NetworkOptix
VIDEO. POWERED.

Nx Witness User Manual

Nx Witness User Manual

Nx Witness

User Manual

Version 6.1.0

Fundamentals

Nx Witness architectures consists of software defined Media Servers that manage video data and device connections and software clients that are used to configure the Media Servers, users, devices, and operational settings of the Video Management System.

This Desktop Client user manual makes reference the cloud client, the local, browser based Web Admin interface, and the mobile client when there is specifically relevancy or interactivity.

The following icons are used to illustrate the functional components and how they work together as a Site:

 Site

 User(s)

 Server(s)

 Camera(s)

 Client(s)

 Nx Cloud

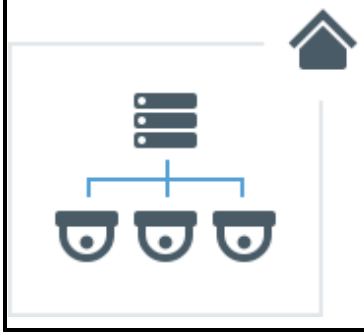
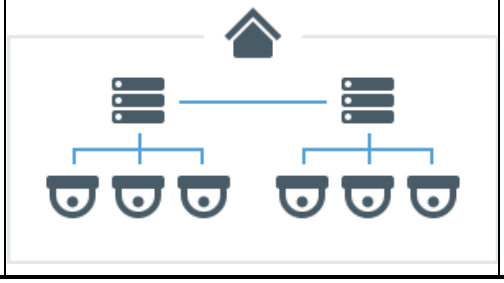
Site:

- One or more Media Servers,
- All devices and streams connected to the server(s),
- Mass storage available to the server(s) (physically attached and/or network addressable), and
- Clients in use (Desktop, Mobile, the Web Admin interface, and/or the Cloud Portal).

The maximum recommended single Site size is 10 servers with 256 video streams per server, and 2,000 TCP connections. Sites can be connected together as an Organization to endlessly expand the total size. Performance will vary significantly depending on specific environmental factors and the equipment in use.

> **NOTE**: It may be possible to configure lower streaming limits or deploy a reduced feature set to meet operational objectives.

Please consult your sales or support team for assistance when a design or installation approaches the maximum recommended Site size.

A Site can have just one server	A Site can have several servers	A server by itself is a Site
		

If there is only one server, there is little difference between the Server and the Site, and they can be considered equivalent. However, with more servers in a Site the differences will become significant.

All Servers in a Site are equal and they share information about all Cameras, Users, and settings in the Site. Video archives are not shared as recorded video is stored only on the Server connected to the video source.

Therefore, when one server in the Site with a new one (e.g., for an update or repair), all Site settings will be retained – but the video archive recorded on the old server is not and must be moved to the new server..

User(s)

Every site contains a user database that associates identity information (Name, Email, User Type) with specific Permissions. Each user is created in or added to the Site with a particular User Type (Cloud, Local, LDAP, or Temporary) that cannot be changed once set. A user must be deleted and recreated to change the User Type.

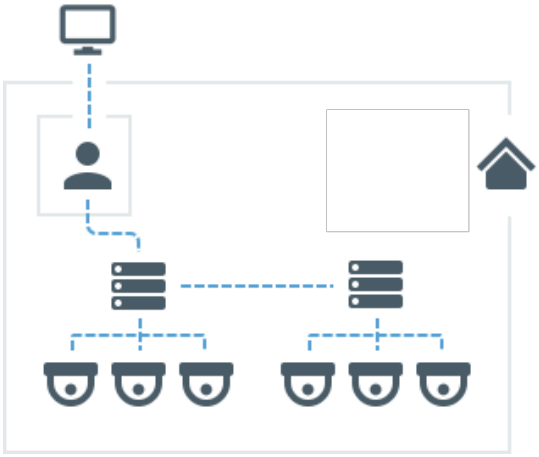
User Management can be done at the User level or by placing Users into Groups with configurable Permissions and Notification settings. Similar to the User Type, the Group Type (Built-In, Custom, LDAP) defines how the Group can be configured and the User Types that can be members of the Group. Groups can be nested to inherit Permissions.

A Site Administrator is defined during setup. This Admin User has full control over the Site and all other Users. There can be only two Administrator accounts on any Site; one is a **Local User** and the other is an optional **Cloud User** available for Cloud Connected Sites. Administrators add or create Power Users to perform limited Site and User Management tasks. All other Users are Viewers with a configurable set of Permissions that include access video streams, managing bookmarks, export from the Archive, interacting with Site monitoring tools.

Users can change Camera settings if granted the "Edit Settings" permission (see Permissions Management).

Cloud Users are unique as their core attributes (Email and password) are stored in the Nx Cloud. Cloud Users are granted access to or removed from Sites where the other User Types are added to or deleted from a SIte.

Removing a Cloud User from a Site does not delete the Cloud User – deleting a non-Cloud User from a Site completely removes the User and their Audit Trail of User Actions.

Administrator has full access to all servers and all devices	Users in a group have a common permission to servers and devices.
	

The term "User" can mean the same thing as the term account, or it can refer to a physical person. A physical person can have multiple accounts and many physical people can share an account. For example, a person has different accounts to access different Sites or multiple people can share a single Admin User account.

See "Users and Groups" for details.

Server(s)

"Server" in this manual can refer to either the server application (called the Media Server) or the computer on which the Media Server application is installed. The maximum recommended number of video sources per server is 256.

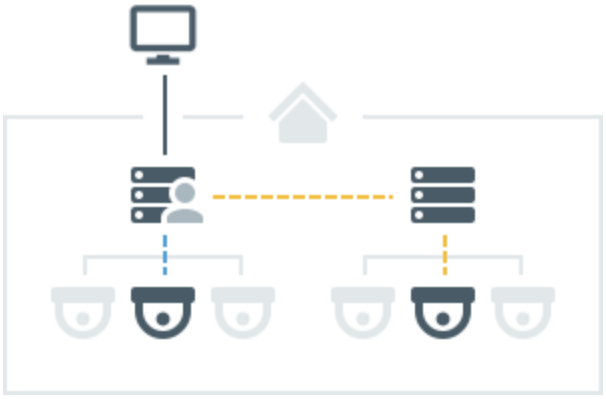
Servers can:

1. Receive video streams from cameras.
2. Manage camera settings.
3. Record video from cameras to internal or external storage.
4. Process and analyze video – for example, detect motion.
5. Manage User database and access levels.
6. Track certain events and react to them.
7. Work with different hardware devices – for example, NVRs, I/O modules, or door locks.

Client(s)

Client applications can connect to servers, and can show live or recorded video from cameras in the Site. Clients are also used to manage the Site, the server(s), and device settings. A client can connect to different servers, but only to one at a time.

Any number of clients can be connected to one server at any time. If the client is connected to a single server in the Site, it has access to the entire Site through this server, including settings applied to others servers and device in the Site.



The following Client applications allow operators to access and manage their Site(s) with an intuitive GUI:

- *Nx Witness Desktop Client* – The most powerful Client application. Available on Windows, MacOS and Ubuntu Linux.
  - Connect to any server.
  - View live streams.
  - Playback recorded video and local video files.
  - Playback up to 64 videos simultaneously.
  - Advanced camera controls – PTZ, 2-way-audio, I/O ports, etc...
  - Built-in web browser.
  - Manage users, cameras, Site, and Server settings.
  - View event logs and User behavior logs.
- *Nx Mobile Mobile Client* – Available on Android and iOS.
  - Connect to any server.
  - View live streams.
  - Playback recorded videos.
  - Camera controls – PTZ, 2-way-audio.
  - Smart Search.
  - Push Notifications.
- *Nx Witness Server Web Admin*– Also called "Web Admin". Can be opened in any modern web browser.
  - Server specific connection.
  - View live streams.
  - Playback recorded videos.
  - Access Health Monitoring.

- Manage Users, Cameras, Site, and Server settings (see Opening the Web Admin for details).

- *Nx Witness Cloud Admin*

Nx Cloud Portal

An important part of Nx Witness is Nx Cloud. It is a cloud service hosted on the Internet and extends functionality of Nx Witness Sites.

In addition to the default functionality, Nx Cloud also gives the ability to:

1. Log in to multiple Sites with a single account.
2. Connect to servers through the internet even though they don't have an external IP address.
3. Add users to your Sites via an Email invite.

To access Cloud features, a Site must be connected to the cloud – which makes it a *Cloud* Site (as opposed to a L*ocal Site*).

Create a Cloud account to interact with Nx Cloud. You can do the following with a Cloud account:

1. Log in to Cloud Sites in the same way as with a regular User account.
2. Log in to Cloud Sites from desktop and mobile clients.
3. Logging in to Nx Cloud.
4. Connect your Sites to Nx Cloud.
5. Restore a password using your Email address.

Users with Cloud accounts are also referred to as Cloud Users. Users with regular accounts or local accounts are referred to as Local Users.

Local accounts belong to the Site, and cannot be moved elsewhere or used in the different services.

Cloud accounts do not belong to any Site, so Site Administrators are not able to create a new account – they can just add an account to their Site, and place the user in a permission group.

In the diagram below, users 1–5 are Local User accounts – they exist only in Site databases and are managed by Site Administrators. User 6 is a Cloud User – the account is the same for both Sites, and is managed on the Cloud Portal by the cloud account Owner. The Site database has information about this account but cannot manage it.

To connect a Site to Nx Cloud, you must log in to the Site using the administrator account. In the Nx Cloud tab of the Site Administration dialog, specify the Cloud account that the Site will be associated with. This account will also receive administrator access permissions and be displayed in the interface as the Site administrator.

After a Site is connected to Nx Cloud, it has access to all Cloud features, and can be disconnected from Nx Cloud at any time. After being disconnected, a Site becomes a local Site again. The Cloud Owner and all other Cloud users will be deleted, but other settings and video archive will not be affected.

Benefits to using the Cloud Portal:

1. Cloud accounts can be created on the Cloud Portal – a web service which is independent of any Site and available to everybody.
2. On the Cloud Portal you can see all your Cloud Sites, view video, and edit some of the settings.
3. You can log in to all Sites associated with your Cloud account from the client Welcome Screens.

Launching the Desktop Client

Click on the Nx Witness shortcut icon on your PC or mobile device interface to launch the Welcome Screen.

To launch the latest version of Nx Witness Desktop Client using other methods

If for some reason you need to use an executable file, locate the **applauncher** executable which launches the newest installed version of the Desktop Client.

- *Windows*
  - Open the **Windows Desktop** and double-click the **Nx Witness shortcut icon**.
  - Open the **Windows Start Menu** > **Programs** > **Network Optix** > **Nx Witness**
  - Open the **Nx Witness installation folder** (the default location is `C:\Program Files\Network Optix\Nx Witness\Client\<VERSION>\HD Witness Launcher.exe`) and open the **Nx Witness executable file**.
  - Automatically launch Nx Witness when a computer starts up:
    a. Open **Main Menu** > **Local Settings** > **General.**
    b. Check the **Run Application when PC boots up** checkbox.
    c. Click **Apply** to accept changes, **OK** to save changes and close the dialog, or **Cancel** to discard changes.

    NOTE: This option is only available on Windows.
- *Linux*
  - Click on Nx Witness shortcut icon
  - From the installation folder: `/opt/networkoptix/client/<VERSION>/bin/applauncher`
- *macOS*
  - Use the Nx Witness shortcut icon located in Applications or Launchpad
  - From the installation folder: /Applications/Nx Witness.app/Contents/MacOS/applauncher

NOTE: In order to display video and graphics properly, it is important to have the video drivers installed. If compatible video drivers are not installed, a warning will display prompting you to update your installation. Windows based installations may be prompted with an option to use Microsoft DirectX in place of the default rendering engine.

Launching in Configuration Mode

The Nx Witness Client detects the configuration of the host platform and if the CPU and/or GPU are insufficient to render all graphics, the Client will launch in *configuration mode*. This mode restricts functionality as follows to limit CPU load and graphics usage:

- Only one video can be viewed at a time
- Notifications are disabled in the client
- Movement of interface elements is disabled

To Close Nx Witness Desktop Client

- Click on the "**X**" button in the top corner of the application window.
- Go to **Main Menu** > **Exit.**

Automatic Session Timeouts

You can set the Desktop and Web Admins to automatically close a User session after a specified amount of time. All User sessions will close automatically after the specified amount of time regardless of activity level or interaction status within the application.

The full log in and authentication process must be completed after a session time has been reached.

Desktop Client

1. Open **Main Menu** > **Site Administration** > **Security**.
2. Check the **Limit session duration** checkbox.
3. Enter a timeout length of up to 99, and select **days, minutes** or **hours**.
4. Apply changes.

Web Admin / Cloud Portal

1. Open **Settings** > **Site Administration** > **Security**.
2. Check the **Limit session duration** checkbox
3. Enter a timeout length of up to 99, and select the unit of **days**, **minutes** or **hours**.
4. Apply changes.

NOTE: Cloud users can also be subject to the same session duration limit as local users by selecting the "*Apply the session duration limit to Cloud users*" checkbox. If this option is enabled, Cloud users will be disconnected from the Site when they reach the session duration limit. However, reaching the session duration limit will not log users out of other active Cloud sessions or other Sites connections.

Launching from command line interface

The Desktop Client can be launched with a command line parameter to define an initial layout. Please contact Support to learn more about launching the Desktop Client from the command line interface.

Retained Settings

Retained settings are restored automatically. To turn off this feature, disable **Main Menu > Local Settings > Automatically restore saved windows configuration**.

The following values are saved locally and restored when the Desktop Client is relaunched:

- Layouts and tabs opened in the main window
- Stream resolution of items on a layout
- Visibility and pin state of the Timeline and Navigation Panel
- Current tab in the Notification Panel

By default, automatically retained settings are only applicable to a single active Desktop Client window at a time. To manually save the settings for multiple Desktop Client windows, when no saved configuration is saved, open **Main Menu > Save Windows Configuration**.

When there is already a Desktop Client window configuration saved, the following sub-menu options will show in the **Main Menu > Windows Configuration >**

- **Save Current State** will update the saved state with the current window configuration.
- **Restore Saved State** will replace the current window configuration with the saved window configuration.
- **Delete Saved State** will remove the saved window configuration and hide the Window Configuration sub-menu until an Window Configuration is saved again.

Initial Site Configuration

When Nx Witness is installed, some initial configuration is required. A newly installed server will be displayed as *New Site* on the Welcome Screen.

To Setup a New Site or Add a Server to an Existing Site:

1. Click on the tile for the new Site to launch the setup wizard.
2. Choose one of the two options:
   - **Setup New Site** – specify a Site name and *Administrator* password. Sometimes, the **New Server** tile may not be displayed if the Desktop Client did not detect the Server. When this happens, use the "Connect to Server" Main Menu item (see "Connecting to a Specific Server"), and provide the Server IP, Port and use **`admin/admin`** as the login/password combination for the new Site.
   - Use the Advanced Site Settings to configure these additional parameters:
     - Enabling and Disabling auto-discovery (see "Automatic Device Discovery").
     - Enabling and Disabling device setting optimization (see "Preventing Nx Witness from Changing Device Settings").
     - Enabling and Disabling anonymous usage statistics (see "Sending Anonymous Usage and Crash Statistics").
     - Configuring Secure Connections.
   - **Add to Existing Site** – if a Site contains multiple Servers (see "Configuring Multi-Server Environment"), specify:
     - Site URL – this value can be auto-discovered. If it is not, the URL format is *http://<host>:<port>*, where <host> is the name or IP address of the Server and <port> is the Server port (usually 7001).
     - Login and Password for the existing Site.

Configuring Storage, Devices, and Recording

Whether the server is connecting to a new Site or an existing Site, the following settings will be required:

- Configuring Server and NAS Storage”
- Device Management (Cameras, Encoders and I/O Modules).
- Enable Recording" – A sufficient number of Licenses or Services must be available (see "Services and Licenses").

Creating User Groups and Layouts

Once storage, device, and recording configuration is complete it is possible to configure the following:

- Users and Groups.
- Layout Management.
- Permissions Management.

Site ID

- All Servers in a given Site have the same ID value. This parameter cannot be viewed or edited, it is required for internal processing when servers are merged.
- If you select "Setup New Site," the Site ID is assigned during initial configuration.
- If you select "Add to Existing Site," the Site ID is taken from the existing Site.

To enable Cloud connectivity feature it is necessary to Connect the Site to Nx Cloud.

If your reseller provides Service Subscription (SaaS) Model, you may need to Connecting the Site to an Organization.

Finally, to use full functionality of, you need to obtain Services or activate Licenses. See "Services and Licenses" for details.

Compatibility Mode

Compatibility mode lets you launch a compatible version of the client application in order to connect to a server running a different version of Nx Witness. The Client downloads another version of itself to match the server version using the same method as an auto-update.

This would be necessary, for instance, when Nx Witness is installed at multiple locations (factory, store, warehouse, etc.) and only one installation has been updated to the current version. In that particular case, the Site will have different versions and one Desktop Client should connect to another Site (i.e. Client at a store connects to the Site in a factory). Site with differing versions are highlighted in red in the log in dialog and in yellow on the Welcome Screen.

When the Desktop Client connects to a server, all component versions are checked and a warning is displayed prompting the user to restart in compatibility mode if the component versions differ from one another. Click **Restart** to connect to the Server in Compabilitiy Mode.

In some instances, it may be necessary to download additional files for the compatibility pack. Once the download is complete, the client should be restarted.

> **NOTE:** It is highly recommended to maintain the product version on all Site components. There may be operational issues when some components (Media Server or Client) in a multiple-server Site have different software versions installed.

See Updating Nx Witness for more information.

Updating a Site or Client

Nx Witness provides users with a one-click method to update all servers in a Site.

Updates can be performed over the internet using the latest build available, a specific build number, or locally from a downloaded file or a file on a USB drive. For internet updates at least one Site component must have an internet connection, whether it is the client or another server.

By default, the client and each Server downloads the update independently from each other. But, if the Server doesn't have internet access, the update can be downloaded via another server that has an active connection. In the event that all available servers are without internet access, the client will provide each Server with the desired update file.

The Desktop Client can be updated without needing to update the Server. This allows for Network Optix to deliver quicker updates for Desktop Client specific issues.

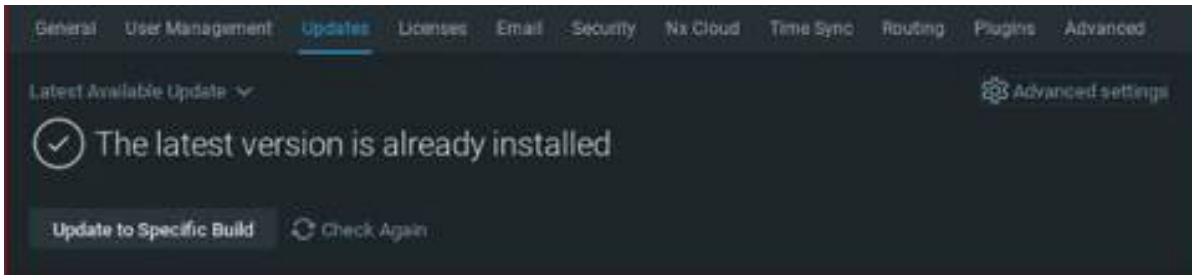
When the download is distributed, servers are tracked with a "ready", "skipped", or "failed" status. The administrator or power user who initiated the update receives specific notifications such as "*Failed to push upgrade package to all servers. Not all servers will be upgraded. Continue?*" This way updating of the Site as a whole does not fail because one or more individual servers is offline or unavailable. Download progress is reported graphically on the *Updates* tab for each server.

It is also possible to initiate a manual update for a specific server. If a new product version does not support the current operating environment for a server, then the update process will not start.

Update files are stored for both the current and target version. This allows clients to update themselves when an installation is started but not finished, or when an old Client tries to connect to a Site. Servers will delete files for the current version when a new update is started. Similarly, files for the target version are deleted when the target version changes, for example because the update is canceled or another target version is set. Desktop Clients do not delete update files and are not used to update other clients.

To Configure Updates Settings

> Open **Main Menu** > **Site Administration** to the **Updates** tab for update controls. The tab either displays that the latest version is installed, or it will show which version number is currently installed if a new version is available.



Advanced Settings

Click on **Advanced settings** in the upper-right corner to configure update settings:

- *Notify about available updates* – If enabled, performs automatic update checks so that when a new version of Nx Witness is released, a notification will open in the Desktop Client.
- *Automatic Client Updates* – Enabled by default. Connecting clients will be automatically updated to the new version when it's available.
- *Check for updates* provides on-demand update checking. This function is unavailable when the *Automatic client updates* toggle is disabled.

Update to a Specific Version

In the upper-left corner is a drop-down for choosing which version to install:

- *Latest Available Updates* – Selects the latest product version available.
- *Specific Build* – Opens a dialog where you can enter a specific *Version* and *Password* (available from your support team).
- *Browse for Update File* – Lets you search for a local update package that has been downloaded (see Offline updates below).

Update Status Indicators

- A yellow exclamation mark on the Server icon in the Resource Panel indicates that the Server version is incompatible with versions of other servers in the Site. (These incompatible servers must be updated separately).
- If the version number is shown in green, the current version is the latest one installed on the Site.
- If the version number is shown in yellow, it does not have the latest build but can be updated.
- If the version number is shown in red, it does not have the latest build and cannot be updated. (Usually because the update for the particular Server is not found. It is possible the Server OS is no longer supported or the package for such a platform was not published).

Online Update

1. Open **Main Menu** > **Site Administration** > **Updates** tab.
2. Click on **Download.**

3. Wait for the update to download and then click on **Install Update**.

Offline Update to the Latest Available Version

1. Open **Main Menu** > **Site Administration** > **Updates** tab.
2. Click on **Get Update File** and choose **Copy Link to Clipboard**.
3. Save the link to an external drive so it can be transferred to a computer with Internet access.
4. Paste the copied link into a browser on a computer with Internet access and use it to download the update file.
5. Save the update file to an external drive, then copy it onto the Client PC that is in a private network.
6. On the offline Client PC, open **Main Menu** > **Site Administration** > **Updates** tab.
7. Click the arrow on the *Latest Available Update* menu and choose **Browse for Update File**.
8. In the file browser that opens, navigate to the external drive where the update file is saved and open it to start the update process.

Offline Update to a Specific Build

It may be necessary to accept a newer version of the end User License agreement (EULA) to proceed with installation. During the downloading phase it is always possible to cancel an update. During the installing phase the update cannot be canceled. After all online servers receive "Install" status, a confirmation dialog displays and you will be prompted to restart the Client to the updated version.

1. Open **Main Menu** > **Site Administration** > **Updates** tab.
2. Click on the **Latest Available Update** menu and choose **Specific Build**.
3. In the dialog that opens, enter the build number and a password (provided by support team), then click **Select Build**.
4. In **Main Menu** > **Site Administration** > **Updates** tab, click on **Get Update File** and choose **Copy Link to Clipboard**.
5. Follow steps 3 through 8 from the above instructions.

Web Admin Client

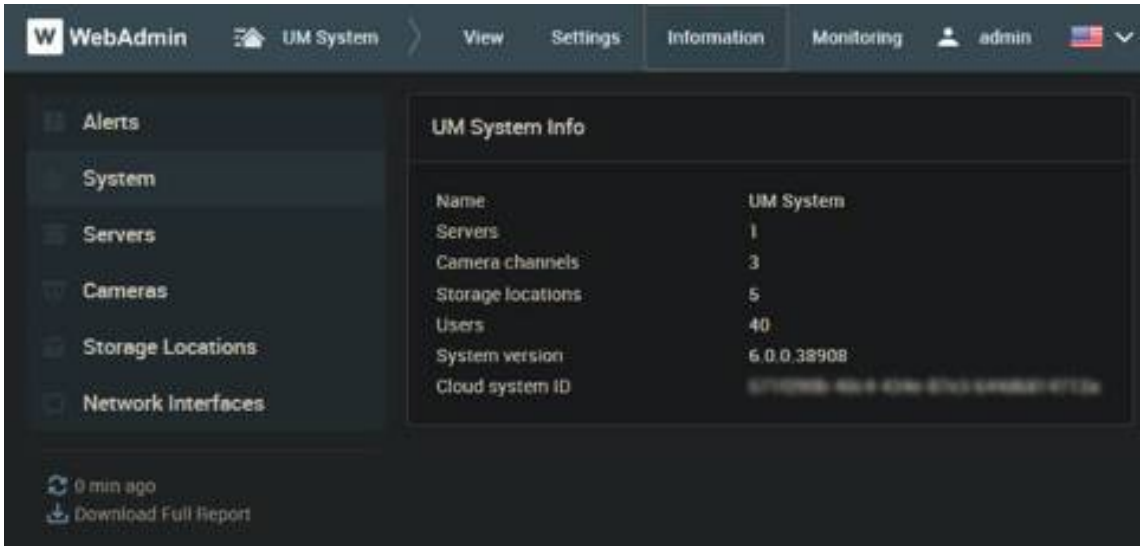
Key The Nx Witness Web Admin client provides the following features:

- Administrator-level Server and Site controls.
- Live stream viewing.
- Playback of archived video.
- Camera management (view camera information and configure motion settings).
- Server Health Monitoring and Log viewing.
- Storage management (view storage information and add external storage).

- User management (add cloud users, remove local/cloud users and change access level).
- View and activate Licenses.
- Access to developer tools and API documentation.

The Web Admin Client Layout presents menus and options that are contextually aware and will change based on selections made, Site configuration, and user permissions.

- A menu positioned along the header area includes tabs for enabled functions (View, Layout, Bookmarks, Settings, Information, Monitoring, Services).
- The tabs displayed vary depending on product version and user permissions.
- The left panel provides for second-level menus choices, filters, or resource selection controls.
- Information refined by the menu selections is displayed in the center display panel.



Configuring the Email Server

An Email service must be configured for the Site to be able to send Emails (see "Mail Notifications").

Nx Witness provides a Cloud based solution to directly push Email notifications to Users or a private SMPT service can be configured to provide delivery of Email notifications using an authorized Email account and corresponding password.

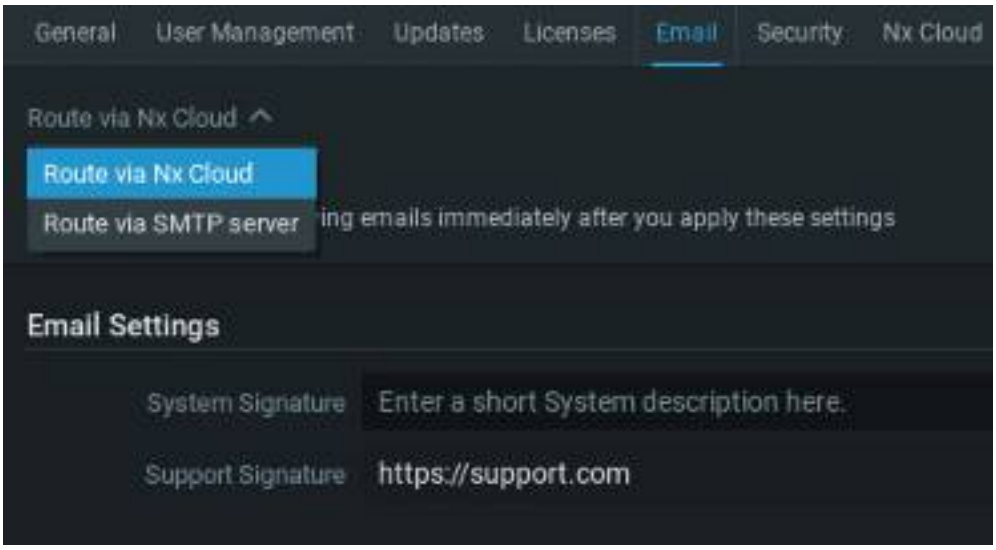
Review the terms and conditions published by SMTP Email service provider to ensure the account is not rate limited or employing a rolling password that could delay or prevent Email notifications from being sent.

To Enable the Cloud Email Service

1. Open **Main Menu** > **Site Administration** > **Email** tab.
2. Select **Route via Cloud** in the drop-down menu.
3. Enter a signature and support URL for the notification messages.

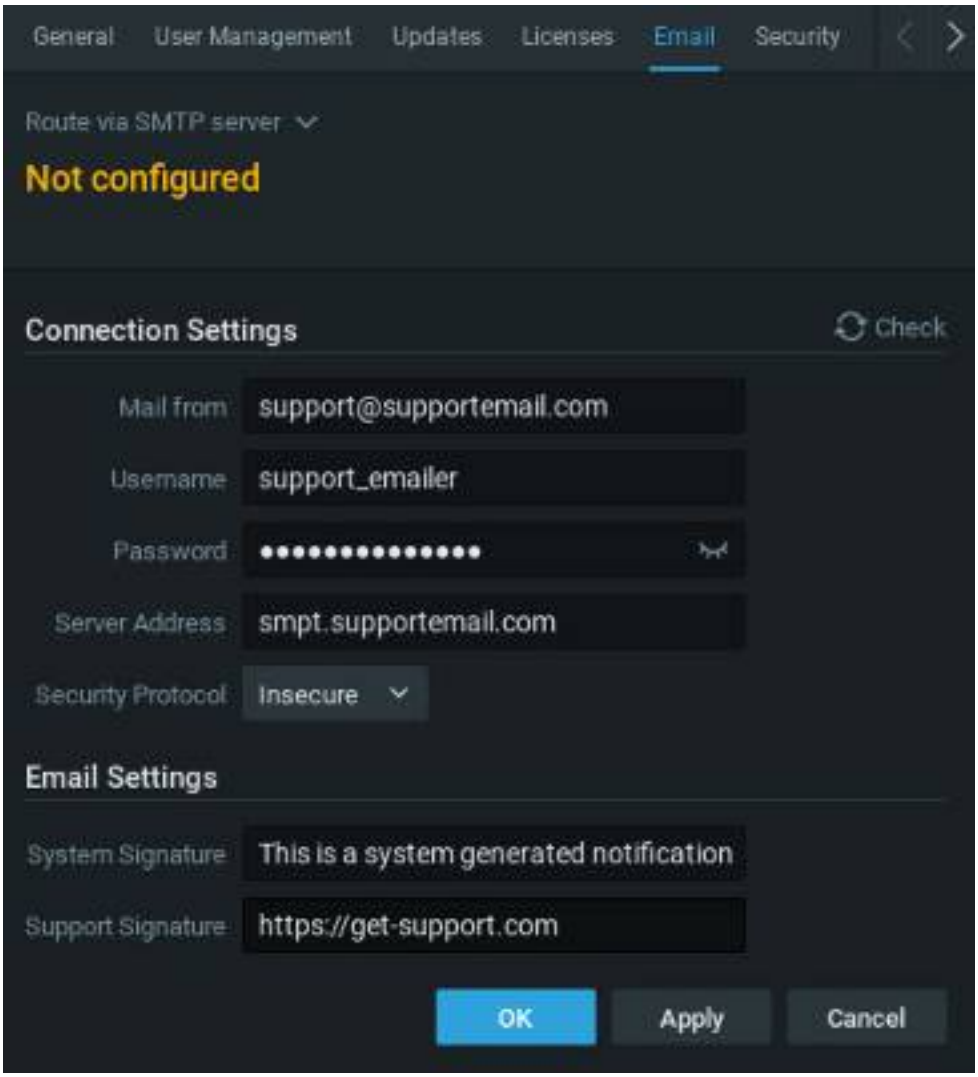
4. Click **Apply** to commit changes and keep dialog open, or Click **OK** to save and close the dialog.
5. Message delivery will immediately be enabled.

NOTE: When using the Route via Cloud service, only Cloud users added to the applicable Site will receive emails. Local users and additional recipients (configured in the rules engine) will not receive emails.



To Configure a SMTP Connection Settings

1. Open **Main Menu** > **Site Administration** > **Email** tab.
2. Enter the following:
   - *Mail from*– Email address to use for outgoing mail.
   - *Username* – Email or login of the outgoing account on the Email server.
   - *Password* – Password for the outgoing Email account.
   - *Server Address* – Email Server address or Gateway.
   - *Security Protocol* – Choose secure connection using TLS, secure connection using SSL, or an insecure connection.
   - *Signature* – User defined description that will identify the Site in outbound Emails.
   - *Support Signature* – Support website for the Nx Witness installation.
3. Click the **Check** button to test the Email Server connection.
4. Click the **Apply** button to save changes to the Email Server configuration.



Web Pages and Integrations

Webpage integrations in Nx Witness allow for interaction with external services and the display of HTTP-based information within a layout cell, a scene, or a dedicated window. For instance, you could place a camera's embedded web-based configuration tools directly alongside its video stream. Plugin Integrations serve as data connectors that facilitate the exchange of analytical metadata and configuration settings between the Desktop Client and a specific camera.

Key Concepts:

- Adding a web page as an integrations enables to web page to interact with the Nx Witness API.
- Web pages and integration can be added through the **Main Menu** or the contextual menu.
- Web pages and integrations can be opened by clicking on the title within the resource panel, or right-click on the title to display a context menu that includes opening in a new tab (within

the active client), opening in a new (Desktop Client) window, or opening the web page / integration in a dedicated (pop-out) window.

- Web pages and integrations can be configured to always open in a dedicated window (see *advanced settings* below).
- Right-click on a web page or integration and toggle the *Show Info* option show or hide the URL as available controls.
- A web page (resource) added within a scene or layout will be rendered using the built-in Chromium browser. Examples:
  - Placing the built in settings (configuration web page) for a device on a layout near the device stream.
  - Display a 3rd party web page that counts cars in a lot next to a camera viewing the entrance and exit gates.
- Each instance of a web page within a layout is treated as a unique session; data and cookie sharing policy is defined by the web page.
- Integrations are web site or browser-based services that can interact with the Desktop Client using API or HTTP methods. Examples:
  - A service that places a camera snapshot over a map, at the location of the camera.
  - An integration could be created to run complex actions based on a Site event or soft trigger.
- Depending on where the context menu to opened, the following options may be available:
  - Toggle an overlay (show information) that includes the URL and available controls (refresh, back, full screen toggle).
  - Open the settings dialog for a web page or integration.
  - Refresh or reload the selected web page or integration.
  - Additional options to open the web page or integration in a new tab or a new window (client or dedicated).
  - Save the web page to an accessible location.
- Log in credentials entered on any web site or integration will be saved between browsing sessions unless you manually sign out of your account before the end of a browsing session.
- Integrations can be programmed to interact with the Desktop Client using JavaScript API.
- The HTML code of the web page or integration can define the opening size and displayed title of the window.
- The API documentation can be opened by right-clicking on an integration that is placed within a layout, and then selecting **JavaScript API** from the context menu.

To Add a New Web Page Item

1. Open **Main Menu > Add > Web Page** or right-click on the *Web Pages* icon in the Resource Panel and select **New Web Page...**

2. In the dialog that opens, enter the destination **URL** and a common **Name** for the *web page*. The **Name** will be displayed within the *Web Pages* folder in the Resource Panel and on the header of the web page within a Layout.
3. To make a web page accessible on client machines that do not host the server, select the advanced option to "**Proxy this web page through the server**" and select which server to use as the proxy.
4. The *Web Page* will open as a new item in the current *Layout* and be added to the Web Pages section of the *Resource Panel*.

In a web page item, the in the bottom left corner of the cell. You can use the **Web Page Settings** option from the item's context menu to change the name or URL.

To Add a New Integration

1. Open **Main Menu> Add > Integration** or right click on the *Integration* icon in the resource panel and select **New Integration...**
2. In the dialog that opens, enter the destination **URL** and a common **Name** for the *integration*, the **Name** will be displayed within the Integration folder in the Resource Panel and on the header of the integration within a Layout.
3. To make an integration accessible on client machines that do not host the server, select the advanced option to "**Proxy this integration through the server**" and select which server to use as the proxy.
4. The integration will open as a new item in the current *Layout* and be added to the integration section of the *Resource Panel*.

   NOTE: An integration may interact with the Desktop Client and request access to the user session. Contact support for additional information (see "Contacting Support").

To Clear Browsing Data Saved Between Sessions

1. Open Main Menu, go to Local Settings > Advanced and press Clear Local Cache.
2. Restart the Nx Witness Desktop Client.

Advanced Settings

The following settings are found on the *Advanced* tab within the web page and integration settings dialog presented when creating a new entry or opened by using the context menu on a web page or integration resource.

- *Allow opening web page without SSL certificate checking* – If enabled, Nx Witness will not check the web page's security certificate. No warning will be shown if the certificate is not secure.
- *Proxy all requested contents* – If enabled, any service or device on the server's network can be accessed by the users of the web page. This setting is only available if "Proxy this web page via server" is enabled.

- *Force open in a dedicated window* selecting this option will open the web page or integration in a dedicated window instead of adding it the the active scene or open layout.

Using Encryption for Site Security

Nx Witness provides HTTPS encryption for client-server data exchange and, separately, for RTSP video traffic streams.

HyperText Transfer Protocol (**HTTP**) is a universally agreed upon convention for network information exchange that is easy to intercept and read. HyperText Transfer Protocol Secure (**HTTPS**) is a safer connection that includes encryption to protect the information exchanged over networks. The encryption is performed using a Secure Sockets Layer (SSL) or TLS (Transport Layer Security) certificate. When an SSL/TLS certificate is issued it means the sending and receiving websites have been authenticated, and a secure connection has been established between the web Server and the browser that connects to it. When you have a secure connection, the website's URL is prefixed with "https" instead of "http," and a padlock icon will display on the address bar.

By default, Nx Witness encryption is disabled. Without encryption, API requests and the Server Web Admin interface can be intercepted and analyzed, and video streams (live and playback) can be intercepted and viewed.

The **Allow only secure connections** checkbox forces all servers in the Site to accept only secure HTTPS connections. When it is enabled, you have the option to also force video traffic encryption.

The **Encrypt video traffic** checkbox applies encryption to RTSP/S format, HLS format, and requests that start with a /media prefix.

NOTE: Encrypted video transfer requires intensive CPU processing, so overall Site performance can be severely impacted, particularly on smaller or weaker hardware such as ARM devices.

IMPORTANT: Due to self-signed certificates, explicit HTTP integrations, or other configuration settings, all integrations configured to work with HTTP need to be tested, and may need to be updated for compatibility with this feature. For example, you will need to disable HTTPS support in order to merge a secured Site with one that does only supports HTTP. Similarly, some third-party products may not support RTSPS and may therefore cause integration issues.

To enable HTTPS encrypted client-server connections

1. Open **Main Menu** –> **Site Administration** (shortcut **Ctrl**+**Alt**+**A**).
2. In the **General** tab, check the **Allow only secure connections** checkbox.
3. Once HTTPS is enabled, the first time you attempt to log onto a server's web page, the browser may first display warnings that indicate a bad certificate and insecure connection ("Your connection is not private. Attackers might be trying to steal your information..."). This is not the case. The warning is a safety feature due to a self-signed certificate on the server, the connection will in fact be more secure.

4. To proceed using an HTTPS connection, click on the word **Advanced**, then click the **Proceed to [xxx.x.x.x] (unsafe)** link to log in. You should only need to do this the first time the HTTPS connection is established.

   NOTE: Although it may have a line through it, as long as https is displayed in the address bar, the connection is secure.

To enable RTSPS encrypted video traffic

1. Open **Main Menu** –> **Site Administration** (shortcut **Ctrl**+**Alt**+**A**).
2. In the **General** tab, check the **Encrypt video traffic** checkbox.

   NOTE: Encrypting video traffic will significantly increase CPU and bandwidth usage because data packets must be encrypted by the server and decrypted by the client.

Connecting to a Site

In order to gain access to Cameras and other Devices, a User must be connected to a Nx Witness Site.

Connection can be made via the following Nx Witness components:

- The Desktop Client (on the Welcome Screen or Specific Server forms).
- Nx Cloud Portal.
- Server's Web Admin.
- Mobile Client.

Connecting to a known Server

Sometimes the term "log in to a Site" is used interchangeably with "connect to a server". In fact, to establish connection with a Nx Witness Server you must do both – connect to the Server using its IP address and a specific port, then log in to the Site with a set of user credentials.

To connect to a Server you must specify the Server (i.e. host) IP address and port, then provide your Nx Witness account login and password.

In Desktop and Mobile Clients, the Server address is entered into a designated field.

In the Web Admin, you enter the Server IP address and connection port in the address line of an Internet browser to access the Web Admin connection dialog.

Both Cloud and Local accounts can be used to connect to a Server in this way. In rare cases, Cloud accounts may not work if the Site you are connecting to doesn't have connection to the internet and you never used the the account of the Site.

Local accounts will always work.

Connecting after you have logged into Nx Cloud.

Another way to connect to a Server, if it belongs to a Site which is connected to Nx Cloud, is to log in to Nx Cloud in the client. After that, if you are not currently connected to a Server, you will see a list of all your Cloud Sites, and be able to log in to any of them by simply clicking on the associated icon.

Your Cloud account will be used as your login, and because you are already logged in to the Client with that account, you will not have to enter your login access credentials again.

The Server to which you will be connected will be determined automatically based on which Server has the best connection. If your Site is connected to the Cloud, you still can connect to a known Server by entering its address and the appropriate credentials.

Reconnecting after session has expired

An informative dialog box will be presented after Cloud sessions are automatically disconnected in accordance with the Automatic Session Timeouts settings.

The Welcome Screen

When Nx Witness Client is first launched, the *Welcome Screen* (shown below) automatically detects and displays the Sites in your local networks and Sites that have been recently accessed. Local Sites can be accessed with a username and password. If a User is logged into Nx Cloud, Cloud Sites are also displayed.

Click on the "**Log in to Nx Cloud**" tile on the welcome screen, or the Cloud icon in the application header, to open Nx Cloud portal. See "Logging in to Nx Cloud" for details.

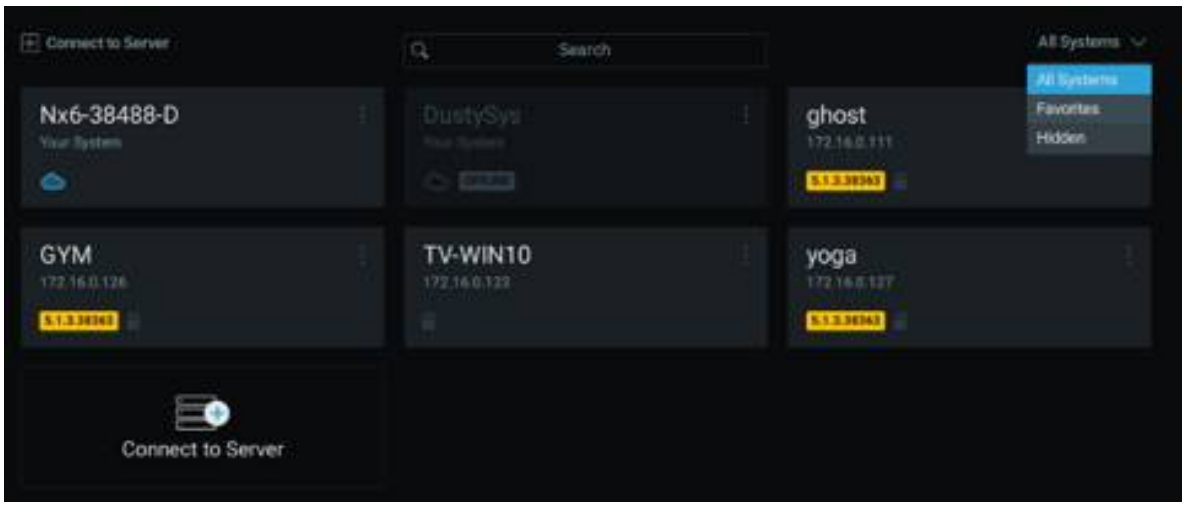
NOTE: When accessing a Cloud connected Site with multiple servers, the Desktop Client attempts to connect to the Server with the best uplink. Alternatively, a specific Server can be chosen in the Site the Desktop Client will connect to, if unreachable, it attempts to connect to another Server.

The number of Site tiles displayed on the Welcome Screen is determined by your screen and window size.

Use the search bar above the tiles to search for a specific Site by certain attributes:

- Site name.
- Server name.
- IP address.
- Site Owner (cloud only).
- User's Email (cloud only).

Unavailable sites appear grayed out on the Welcome Screen and can be deleted. Hidden Sites are only visible when "Hidden" display mode is selected. The option to hide tiles becomes available when the Welcome Screen is excessively populated. Hiding Site tiles is not a security feature; it is intended solely for organizing the Welcome Screen.



The Client can connect to Sites running different version of Nx Witness. The product version is displayed in a yellow block within the Site tile if it is not the same version as the Client. If a Site is incompatible with the Client, the block will be red.

See "Launching Nx Witness in Compatibility Mode" for information on establishing connections when the client and Site/servers have are not the same version.

NOTE: Compatible hardware supports *safe mode* booting where the hardware boots up in *safe mode* if an error or other unexpected event happened during a previous boot. In this case it is possible to connect to a server, but it is not possible to perform any configuration.

To Connect to a Site

Click on the tile for the desired Site. If it is compatible with the client a connection dialog will open.

1. Enter a login and password.

   NOTE: Optionally, check **Remember me** so in the future clicking on the tile will connect directly to the Site using saved credentials.

2. Click **Connect**.

If there are 10 or more unsuccessful attempts to log in from a given IP address within 5 minutes, all log in attempts from that IP address will be denied for 1 minute.

Display Modes

The Welcome Screen has three display mode options which can be accessed in the upper-right corner.

- *All Sites* – displays all Sites on the network that have not yet been hidden or removed (default display mode).
- *Favorites* – displays all Sites added to the list of Favorites.
- *Hidden* – displays all Sites marked to be hidden from other display modes.

To Edit, Hide, or Favorite a Site Connection

For local Sites that are online, you can click on the tile to expand the connection details.

Also, context menu lets you edit the Site tile by clicking on the three dots in the upper-right corner.

- *Hide* – moves the Site tile from the default All Sites display mode to the Hidden display mode.
- *Add to Favorites* – moves the Site tile up in the list when in *All Sites* mode and adds the Site tile to the *Favorites* display mode for easy access.
- *Delete* – removes the Site completely (option only appears for offline and incompatible Sites). The tile won't appear on the Welcome Screen again unless the Site is online.

Working Offline

Even when you are not connected to a Site, the Welcome Screen main menu provides the following:

- *Connect to Server* – lets you connect to a specific Server using its IP address (see "Connecting to a Specific Server").
- *Browse Local Files* – use the Welcome Screen as a media player (see "Playing Local Video Files in Nx Witness").
- *New* – launches a Welcome Screen in a new window.
- *Start Screen Recording* – toggles the recording of the entire screen (see "Screen Recording (Windows Only)").

- *Local Settings* – opens the Local Settings dialog where you can choose language, display time and other global setting (see "Customizing Look and Feel of Nx Witness").
- *About* – displays important Site and network configuration information (see "Collecting Additional Information").
- *User Manual* – open the User Manual.
- *Exit* – closes the window (Alt+F4).

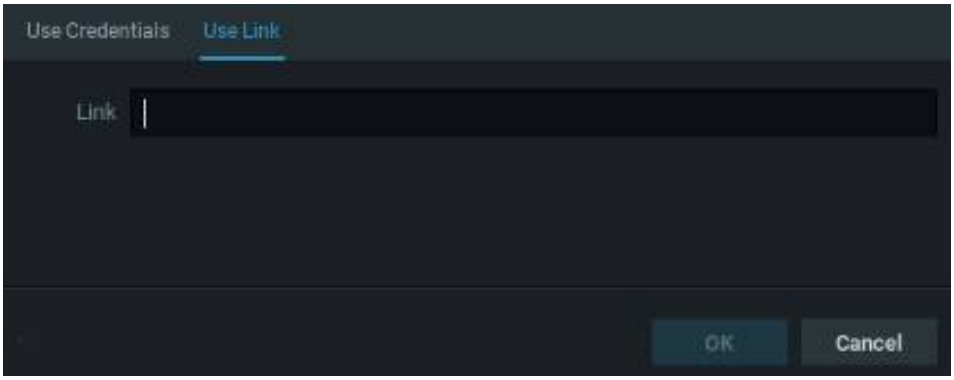
Connecting as a Temporary User

Temporary users are granted limited-duration access to either Local or Cloud-Connected Sites. Anyone with the Temporary User link can access the associated Site.

See "Managing Users" for Temporary Users limitations and "Adding Users" to create a Temporary User.

Connect to a Site or Server using the Desktop Client

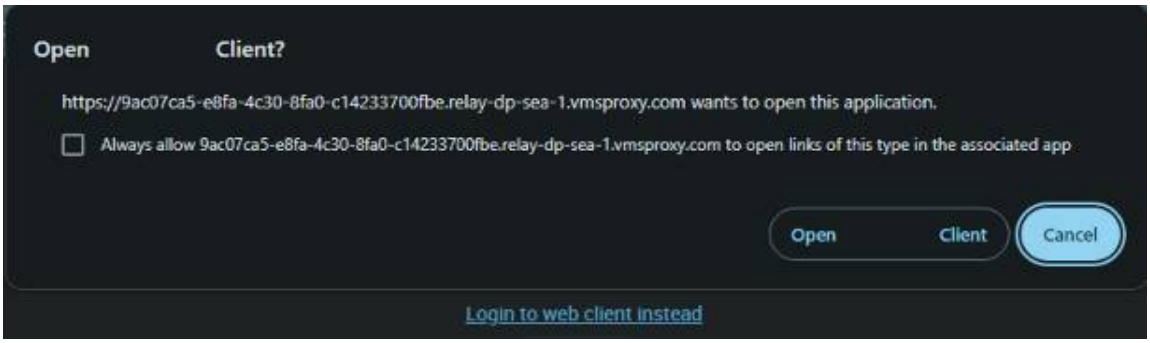
1. Have the Temporary User link provided by the Site Administration team.
2. Open the Desktop Client, Select **Connect to Server**, Select the Use Link tab.
3. Enter the link into the dialog box and press **OK**.
4. The Desktop Client will open to the target Site with no further action needed.



Connect to a Site or a Server using an Internet Browser and the Web Admin

1. Enter the provided Temporary User link into a browser.
2. Depending on local Site configuration there may be prompts to launch the Desktop Client or use the Web Admin.
3. Select Web Admin to open the Site.

Depending on permission granted to Temporary User, the Web Admin may offer less functionality than the Desktop Client.



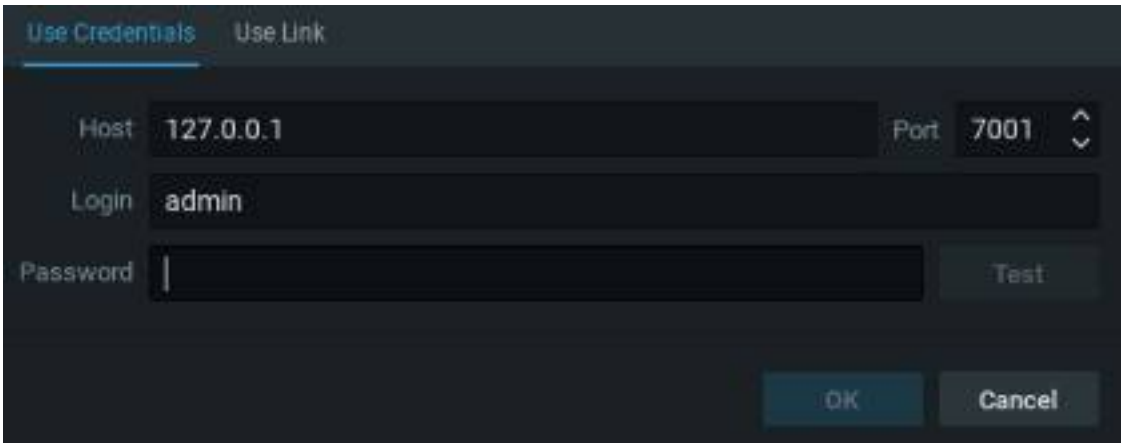
Connecting to a Specific Server

If the Site is not connected to Nx Cloud (see "Connect your Sites to Nx Cloud"), you will have to connect to a specific Server via its IP Address, Hostname, or a provided Temporary User Link.

To Connect to Specific Server via IP or Hostname:

On the *Welcome Screen* or in the *Main Menu*, click *Connect to Server* to open the connection dialog shown below. The *Connect to Server* dialog enables connecting via an IP Address and the use of different User credentials.

If the operation is canceled, the current User will still be connected to the Server.



The following connection details are required:

- *Host* – IP Address or address of the computer Server is installed on (`localhost` or `127.0.0.1` for All-in-One installation).
- *Port* – IP Port for access to Server (`7001` by default).
- *Login* – Account username used to connect to a server. If connecting for the first time, use "`admin`" as the login name.
- *Password* – Account password used to connect to a server. Use the same password that was set up during the initial installation.
- *Test* – Press this button to check connectivity to a server. The following may cause connection errors:
  - Server is not available

- Specified IP Address is incorrect or inaccessible
- Specified port is incorrect
- Server is stopped
- Login and/or password are incorrect
- Server and client are incompatible with each other because they are running different Nx Witness versions. In this case compatibility mode will be suggested.

NOTE: Users can only access *Local Files* when the Desktop Client is not connected to a server (see "Playing Local Video Files in Nx Witness").

To Log Out

Open the **Main Menu** and choose **Disconnect from Server**.

Log in to Nx Cloud

Nx Cloud is a cloud service hosted on the Internet that extends the access to Nx Witness Sites. See "Working with Nx Witness" for more information about Nx Cloud.

The cloud icon in the Navigation Panel opens a dialog where you can log in or log out of Nx Cloud, or create a Nx Cloud account.

To obtain all benefits of Cloud connectivity, the Site should be linked to Nx Cloud. See "Connect your Sites to Nx Cloud" for more details.

To Log In to Nx Cloud from the Desktop Client

1. Click the icon in the Navigation Panel.
2. Enter your Email and Nx Cloud password, then click on the **Log In** button.

Once connected, your Email address will be displayed next to the cloud icon, and you can click on it to open the Nx Cloud portal, log out from Nx Cloud, or change your Cloud account settings.

NOTE: It is possible to connect to a server using the Nx Cloud login even if the internet connection is temporarily unavailable. After several unsuccessful attempts to log in, connect to, or disconnect from a Cloud account, all log in attempts will be denied for 1 minute.

To log in to the Nx Cloud Portal Interface

1. Open the Nx Cloud portal homepage and click **Log In**.
2. Enter your Nx Cloud account credentials and click **Log In**.
3. Select an available Sites to open by clicking on one of the displayed tiles.
4. Choose a tab from the Nx Cloud interface banner to display related information. The most common tabs are:
   - *View* – Show the Resource Panel to select a live viewing device or archive playback.
   - *Layouts* – Display existing and available layouts (Enterprise Edition).
   - *Bookmarks* – View existing and available bookmarks (Enterprise Edition).

- *Settings* – Manage users, Site and security settings, activate Licenses or Services, enable recording, create a motion mask, etc.
- *Information* – Browse detailed data on Site resources (cameras, devices, network interfaces, storage locations).
- *Monitoring* – Open a rolling graph of Site performance metrics (CPU and RAM usage, network and storage I/O, and other available data.

NOTE: Tabs displayed in the Nx Cloud portal are dynamically populated according to configuration and user permissions. Not all tabs are available to all users.

To Create a Nx Cloud Account

When a Site Administrator or power user adds a Cloud User who does not have an established Cloud account, the added user will receive instructions to create their Cloud account.

1. Do one of the following:
   - Open the Cloud Account Creation dialog from the Desktop Client using the icon in the Navigation Panel
   - Open the Nx Cloud Website and find the **Create Account** button in the upper, right-hand corner of the page
   - Open the link provided in the invitation Emailed to Cloud Users who do not have am established Cloud Account
2. Enter your registration information and click **Create Account**.
3. An activation Email will be sent to the Email address specified.

Connect with the Web Admin

There are multiple ways to open the Web Admin interface:

Open Web Admin from the Desktop Client:

1. In the Desktop Client, select **Main Menu > Open > Web Client**.
2. In the Desktop Client, select the Server in the Resource Panel, then use the context menu (Right Click) to select **Server Web Page**.

   NOTE: If a Site contains multiple servers, the Web Admin interface will control the server to which the client is connected (as indicated by the icon in the Resource Panel).

Open Web Admin from an Internet Browser:

1. Enter the server IP address and port into the browser URL address (http://172.142.42.110:7001).
2. In the log in dialog that opens, enter your login and password credentials to open the Web Admin client.

Open Web Admin from the Windows Tray:

1. In the Microsoft Windows operating system, right click the Server Icon in the tray and select **Server Web Page**.

The Mobile Client

Nx Witness *Mobile Client* provides the following features:

- View live streams from cameras
- Search through recorded archive
- PTZ camera control
- Fish-eye camera dewarping
- Two-way audio
- Soft triggers
- Push notifications

The mobile client is available for Android and iOS platforms.

The comprehensive User Guide for the Mobile Client is available as an additional PDF document which is installed in the same location as the PDF version of the Desktop Client User Manual.

Server Certificate Validation

Nx Witness Server certificate validation occurs on the communication between Nx Witness Server, Nx Witness Clients (Desktop Client and Mobile Client), and Nx Cloud to enhance the security of Nx Witness by ensuring you are connecting to a trusted location.

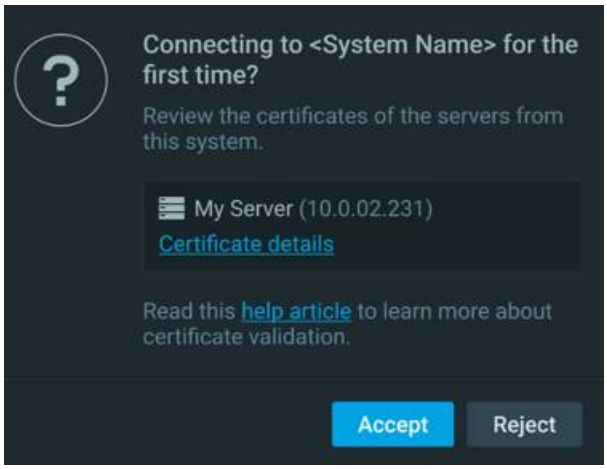
While the Client connects to a Site, the Site provides the public keys from every Server to the Desktop Client for validation. No matter which level is configured, there will be no warning message displayed at all when you connect to a Site having a valid (public) certificate with a matching hostname.

NOTE: A valid certificate must be issued by a public Certification Authority (CA) that contains the completed information of the certificate chain. A public certificate without a certificate chain will be considered invalid in Nx Witness. See "Obtaining and Installing an Authorized Certificate" for details. Trusted Man In The Middle certificates are trusted on the Desktop Client side.

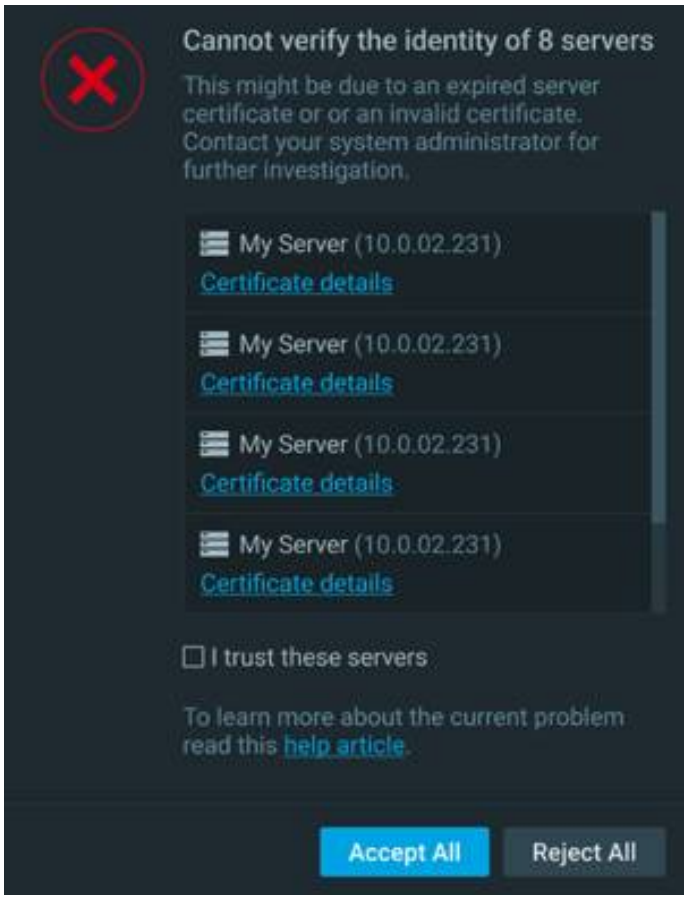
For other types of certificates, the behavior will depend on the Client's validation level:

- **Disabled** – The Client will skip the validation process and connect to the Site directly. The User will not see a warning message. However, it is still NOT recommended to turn the validation off since certificate validation is recommended as a part of the security hardening process of any Site.

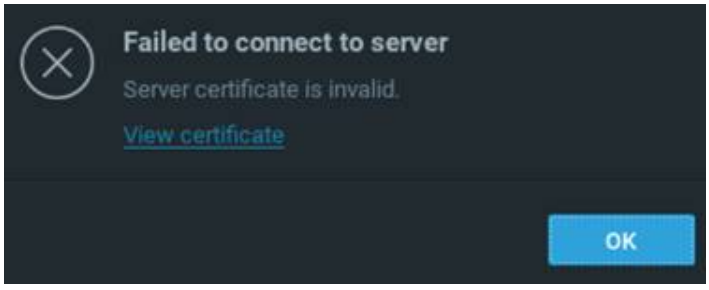
- **Recommended** (default) – Allows users to connect to the Sites with any certificate, but may require the user's confirmation. You may still see the warning message in the following situations:
  - *Connected to an UNKNOWN Sites* – When a Client attempts to connect to a Site for the first time, that means the Client has no information about the servers' certificates before. When the Site provides the certificate(s) that is custom/self-signed, or public certificate without chain information, a "Connecting to Server for the first time?" prompt may appear stating that the SSL certificate could not be verified automatically. Once the Client approves this connection, the certificate will be stored at the Client's end. It is expected that no warning message will pop up again for any further connections until the certificate expires/changes.



  - *Connected to a KNOWN Site* – When a User attempts to use the Client to connect a known Site with a certificate(s) that cannot be successfully verified. For example, mismatched with the Client's pinned certificate, expired certificate, etc. Then the Desktop Client will display the warning message: "Cannot verify the identity of # Server ".
    The User is prompted to take further action and check the certificate's problems. The User can check the *I trust this/these Servers* checkbox and then click *Connect Anyway* to connect to the Servers. This message will be seen every time the User attempts to connect to the Site until the issue with the certificate has been fixed.



- **Strict** – With this mode, the servers that use the default self-signed certificates will also be rejected by the Client. It forces the User to connect to Servers with only a valid (public) certificate and correct hostname. The User will see the warning message below when they attempt to connect to the Site with an invalid certificate or a mismatched hostname.



How to Change the Certificate's Validation Level

To change the validation level in the Desktop Client:

1. Open **Main Menu** > **Local Settings** > **Advanced** tab.
2. Open the **Server certificate validation** drop-down and select a validation level: *Disabled*, *Recommended*, or *Strict*.
3. Apply changes.

NOTE: The Server certificate validation level can also be modified in the Mobile Client.

How to Check the Certificate's Details

To check the Server's SSL certificate validity and information:

Desktop Client

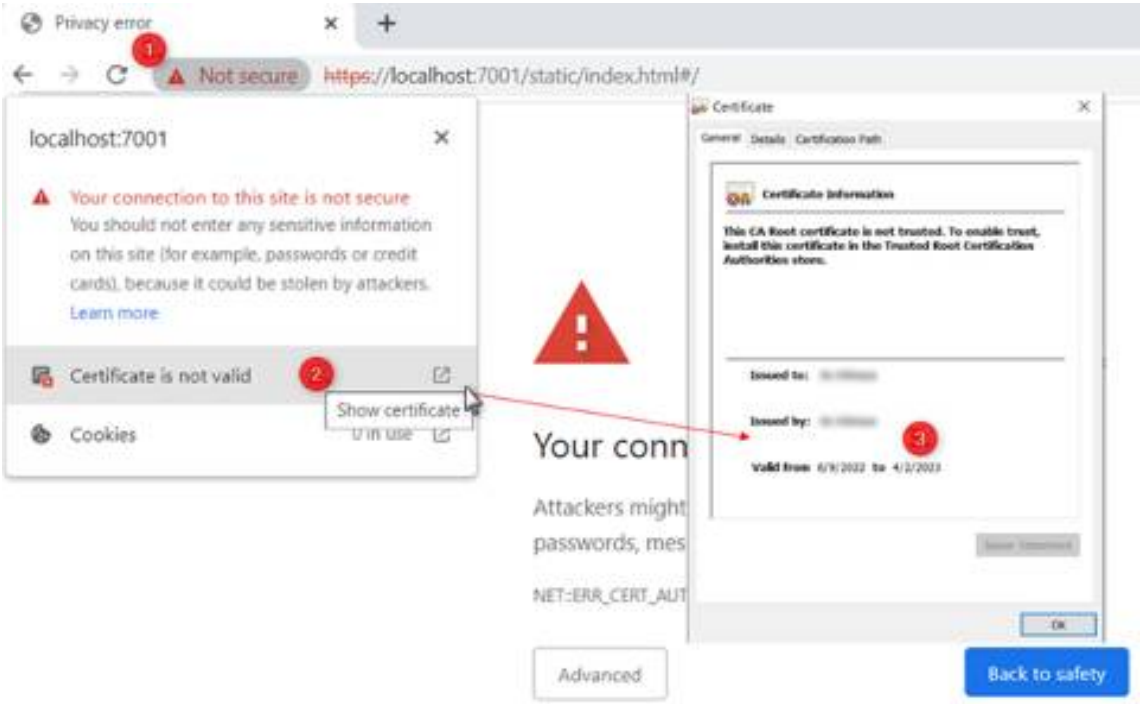
1. Open **Server Settings** > **General**.

   NOTE: Any available pinned/custom certificate will be listed here.

2. Click the certificate to view its details.

Web Admin

1. Visit the Web and click the **Not secure** indicator in the address bar.
2. Click on the certificate's status to open its details
3. Review the certificate's information, such as issuer and expiration date.



How to Renew the Expired Certificate

- Self-signed Certificates from Nx Witness

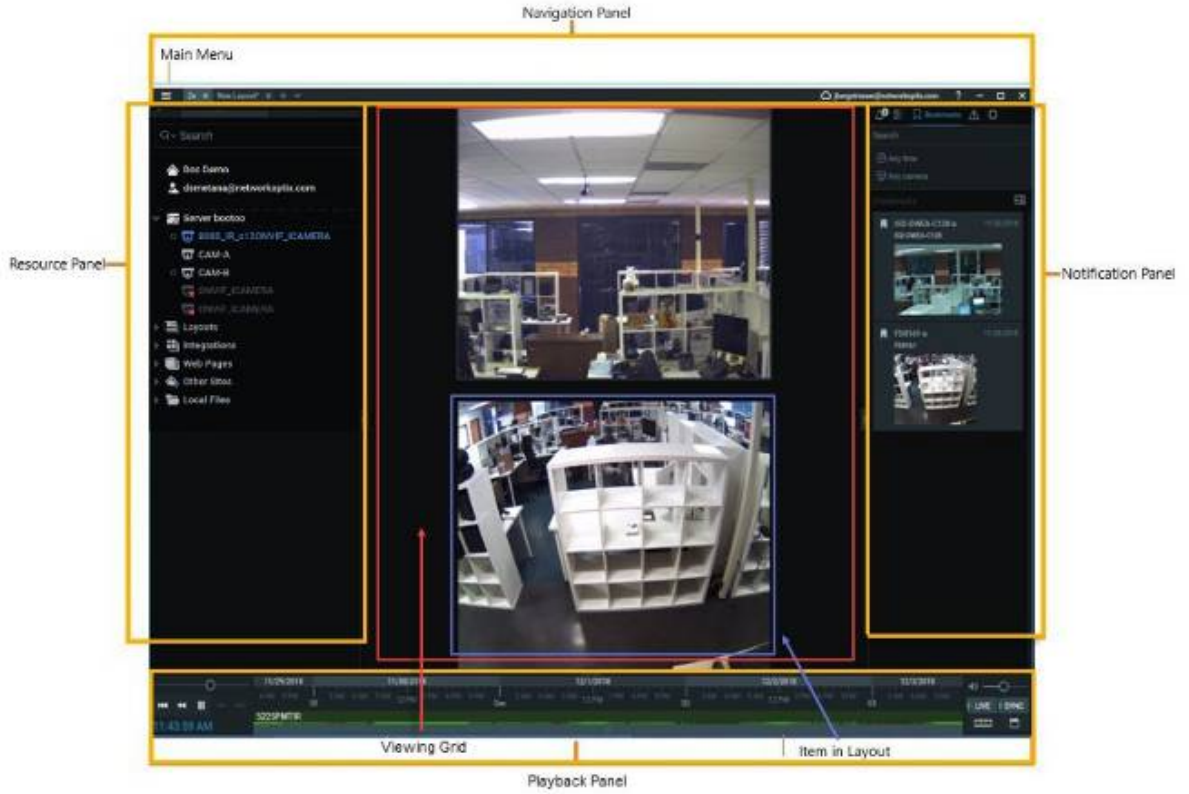
  Restart the Server to renew its certificate and try again.

- Public Certificates / Other Self-signed Certificates

  Contact your administrator to renew the Server certificate.

Desktop User Interface

The Nx Witness Desktop Client User Interface includes the following main regions:



Viewing Grid for Layouts

The central Viewing Grid can display up to 64 individual *Items* – live Camera streams, recorded video files, Web Pages, etc.

An arrangement of items in the Viewing Grid is called a *Layout*. Layouts can be named and saved. Multiple layouts can be open at once, each displayed in a separate tab.

Panels

Sliding panels on each side of the Viewing Grid provide management and display tools. These panels can be resized by dragging the inner edge towards or away from the Viewing Grid, and hidden or opened using the directional arrows.

- *Navigation Panel (top)* – provides access to the Main Menu, tabs for each layout, the Nx Cloud connection form, this User Manual, and standard window sizing controls.
- *Playback Panel (bottom)* – controls playback of local videos and live streams.
- *Resource Panel (left)* – displays all servers, devices (cameras, analog encoders, DVRs/NVRs, IO Modules), Layouts, Showreels, Web Pages, other Sites, and Local files (video and image files) available to the current User (see "Searching and Filtering in Nx Witness" for details about searching and filtering in the Resource Panel.

- *Notification Panel (right)* – contains tabs that display tiles for notifications, motion detection, bookmarks, events, and analytics objects. See "Searching and Filtering in Nx Witness" for details about searching and filtering in the Notification Panel.

Each interface element has a *Context Menu* that provides shortcuts to key actions related to that element. Throughout this User Manual are instructions to use these context menus to access necessary tools. Right-click on an interface element to open its context menu.

Tooltips and Context-sensitive Help

Throughout the Desktop Client application, you can click on the contextual help icon to toggle the mouse pointer into a question mark, then click on a element interest to view related help information. Tooltips and mouse-hover text is also provided though the application.

Keyboard Shortcuts

A set of Keyboard Shortcuts are available to speed up common tasks.

Main Menu

The Main Menu provides access to fundamental Nx Witness settings for server connections, display characteristics, users permissions, device controls, and layout configurations.

NOTE: The items listed in the Main Menu will vary depending on User Permissions and Site settings.

Click on the **Main Menu** button in the upper left corner of the Navigation Panel to access the following:

- *Connect to (Another) Server* (Ctrl+Shift+C) – see "Connecting to Site from the Welcome Screen".
- *Disconnect from Server* (Ctrl+Shift+D)
- *New*
  - *Layout* – creates a new empty tab in the Tab Navigator (see "Layout Tabs").
  - *Window* – opens a new window of Nx Witness (see "Working with Multiple Nx Witness Windows").
  - *Welcome Screen* – opens the Welcome Screen in a new window of Nx Witness (see "Working with Multiple Nx Witness Windows").
- *Open*
  - *File(s)* and *Folder* commands open and play back selected local video files or all video files in a folder, respectively (see "Playing Local Video Files in Nx Witness").
  - *Web Admin* – opens a web browser to an Nx Witness Web Admin login dialog (see "Opening Nx Witness Web Admin").
- *Site Administration* (Ctrl+Alt+A) – opens a tabbed dialog for Site-related settings (see "Site-Wide Configurations").

- *User Management* – opens a dialog for managing Users and User Groups (see "Users and Groups").
- *Lists Management* – site-wide, reusable Lookup Lists that contain variables provide a method to update many Event Rules by changing a single file.
- *Local Settings* – opens a dialog for local client settings (see "Customizing Look and Feel of Nx Witness").
- *Audit Trail* – opens a log that displays all User sessions, actions, and device activity (see "Audit Trail of User Actions").
- *Bookmark Log* (Ctrl+B)– opens a log where you can view, search and manage Bookmarks (see "Searching Bookmarks").
- *Add*
  - Device – opens the dialog where you can specify or search for a connected device, by Server (see "Adding Devices Manually").
  - *User* – creates a new User
  - *Video Wall* – creates new Video Wall (see "Video Wall Management").
  - *Integration* – creates a Web Page frame that can interact with the Desktop Client,
  - *Web Page* – creates a new layout item for a web page,

    see "Managing Web Pages and Integrations".
  - *Showreel* – creates a new tab containing a Showreel layout (see "Showreel (Tour Cycle)").
  - *Virtual Camera* – creates a new Virtual Camera device (see "Setting Up a Virtual Camera").
- *Merge Sites* – starts the process for Merging Sites into a single entity. (see "Configuring Multi-Server Environment").
- *Import From Devices* – this menu item and related data is only displayed supported devices are connected (see "Configuring ONVIF Profiles).
- *About* (F1) – displays product version, hardware, and driver information (see "Collecting Additional Information").
- User manual – Opens this Desktop Client User Manual.
- *Save Window Configuration* – allows for retaining and restoring settings for multiple Desktop Client windows at a time (see "Retained Settings" for more information).
- *Exit* (Alt+F4) – closes the current Nx Witness client session.

Customizing Look and Feel

The Desktop Client can be customized for specific user preferences. These settings are kept locally and apply to the current client instance only.

To Customize the Look and Feel:

Open **Main Menu** > **Local Settings** > **Look and Feel** to set the following global display characteristics:

- *Language* – select the language to display in the user interface.
  - The client must be restarted for this change to take effect.
  - See Configuring Users to change the language displayed in the Notification Panel.
- *Time Mode* – when the Client and Server are in different time zones, use this to select whether *Server Time* or *Client Time* will apply in Client displays (e.g. Timeline, timestamps in Event Logs and Trail, etc). See "Time Synchronization in a Multi-Server Environment".
- *Show additional info in tree* – check this box to include the IP address of devices and servers.
- *Show aim overlay for PTZ cameras* – check this box to enable the alternative UI for PTZ controls, this mode is off by default (see "Alternative PTZ Controls").
- *Tour cycle* – sets the time, in seconds, that each item in a Tour will be displayed.
- *Background Image* – toggle this switch to add an image (typically a logo or map of camera placement) that will display on the Viewing Grid beneath all layouts. Once an image is selected, you can use this switch to toggle the background image on and off.
  1. Click **Browse** to select an image file
  2. Open the **Mode** drop-down and select the desired display mode: *Stretch*, *Fit*, or *Crop*.
  3. Set the **Intensity** level (0%/completely transparent to 100%/completely opaque)

Click **OK** to save changes and exit the dialog or Click **Apply** to save change and remain in the setting dialog, or click **Cancel** to discard changes and exit the dialog. If your changes require a restart, you will be prompted to **Restart Now**, **Restart Later**, or **Cancel**.

NOTE: The Viewing Grid background applies to all Layouts – A background image can be applied to a single Layout (see " Layout Backgrounds and E-Mapping").

Showing and Hiding Panels

Panels in the User interface can be shown or hidden individually, or all at once.

Use the "**>**" and "**<**" arrow buttons at the perimeter of the Viewing Grid to show or hide individual panels.

Press **F11** to simultaneously hide all Panels, and zoom Nx Witness to fill the screen. Press **F11** again to show all Panels – The product window remains maximized.

You can also use Fullscreen Mode to simultaneously hide all four sliding panels and expand the display of a single Item to fill the entire layout.

Searching and Filtering

Nx Witness enable users to search and filter data in various forms (Audit Trail of User Actions, Event Log, Device List, Users etc). The common UI element is a search box. Type any characters there to activate a search. Search results appear in the form immediately as characters are entered. This is because Camera ID strings are so long and contain so many characters they could flood search results without this limitation.

The search functionality in the Resource Panel is a little different than everywhere else in Nx Witness. The Resource Panel display can be filtered in two ways, by type and by text, and these two filters can be applied separately or together. By using this function, the following items can be searched for: Servers, Devices (I/O modules, cameras, etc.), Layouts, Showreels, Video Walls, Web Pages, Users, Local Files, and Groups.

NOTE: The display of server and device IP addresses will change according to the setting of the *Show additional info in tree* option, see the Customizing the Look and Feel section for more information.

Filtering by Resource Type

Only one resource type can be selected at a time. The type filter can be applied by clicking on the magnifying glass () in the Search field to open a drop-down menu. When a type filter is applied, the tree structure changes – all elements become grouped by type, and are displayed without nested elements of a different type (for example, cameras under layouts under users).

You can select a group from the search results **(Shift + Click)** or select multiple items sequentially **(Ctrl + Click)**. You can add items from the search results to the existing layout **(Enter)** or open all selected items into a new layout **(Right-click > Open in New Tab)**.

NOTE: The cursor must be in the search field for these add-to-layout functions to be available.

Filtering by Text

Any text entered in the Search field filters the existing resource display. Multiple keywords are treated as a Boolean "AND". For example entering **abc def** returns only resources which have **abc** and **def**. If the filter returns a large number of results, only the first 64 results will be displayed. Camera ID fields are only searched if a query is 4 symbols or longer.

Search Syntax

Search syntax in Nx Witness search fields is generally the same across all Nx Witness resources, but additional search features are available in a few places.

The standard search syntax includes the following:

- Single word search (not case-sensitive)
- Two word search (not case-sensitive and the search terms' order does not matter)

Search Fields That Use the Standard Search Syntax

- Server Web Admin
- Desktop Client
  - Resource Panel
  - Event Rules (Indexed field: Source)
    NOTE: Events with more than one camera set will show up in your search results if one of the cameras match the search term, but the exact camera name will not be visible until you click on the list of cameras for that event.
  - Event Log (Indexed field: Description)
  - Cameras list (Indexed fields: Name, Vendor, Model, Firmware, IP, and MAC address)
  - Audit Trail (Indexed fields: Camera name, User, IP, Activity, Description, Session ends)
- Cloud Portal

Search Fields That Do Not Use the Standard Search Syntax

The following places in the Desktop Client have an exception or additional search features.

- User Manual
  - Two word search terms will provide results for both search terms together and separately.
  - An asterisk (*) can be used in any position to any number of symbols.
  - A question mark (?) can be used to substitute a single character.
  - A hyphen (-) can be used in front of the second search term to search for lines that contain the first term but not the second term.
- User Management
  - Unlike two-word searches across our other resources, only results matching the exact order of search terms will show up.
  - A question mark can be used to substitute a single character.
  - An asterisk can be used in any position to any number of symbols.
- Bookmark Log – (Indexed fields: Name, Description, and Tags)
  - Quotations can be used to find results with the search terms in the order specified.
- Notification Panel, Bookmarks tab (Indexed fields: Name, Description, and Tags) and Objects tab (Indexed fields: Object type and Object text attributes)
  - Quotations can be used to find results with the search terms in the order specified.

Navigation Panel

The **Navigation Panel** provides access to frequently used tools and features, as well as the layout tabs. Like all panels, it can be shown and collapsed.

The Navigation Panel contains the following controls:

- *Main Menu* – use to configure fundamental behavior such as Site Administration, Users and Groups, Local Settings, etc.
- *Layout Tabs* – all open tabs are displayed and can be navigated through.
- *Cloud Connect Button* – connects to Nx Cloud. This button indicates the current Nx Cloud connection status and allows you to connect/disconnect to Nx Cloud and open the Nx Cloud Portal.
- *Help Button* – Toggles the cursor into a (?) that will open a related help topic when clicked on a User Interface element.
- Standard window sizing buttons – Minimize, Maximize, Exit.

Resource Panel

The *Resource Panel* displays all servers, cameras and devices, layouts, Showreels, Video Walls, web pages, local files and other Sites available to the current user. What is shown in the Resource Panel depends on the user's permission level.

NOTE: To access the Resource Panel from the Web Admin, open the **View** tab.

Resource Panel Display

Levels can be expanded to show additional information. For example, servers at the top-level expands to show each server in the Site, and expanding a server shows the connected devices. Use **Ctrl (Cmd) + F** to search through the Resource Panel. The **+** and **-** keys expand/collapse Resource Panel sections and the arrow keys can navigate through and select resources.

Resources that are placed in the active layout are accented in bold font when viewing the Resource Panel list. The currently selected resource is shown in blue in the Resource Panel. Display of server and device IP addresses can be toggled on or off in the Look and Feel dialog.

Each resource and resource type has a related context menu. You can highlight the name and click **F2** as a shortcut to rename a resource.

– *Servers:* Lists the servers registered in the Site. A Server may have several network interfaces, so it is possible for different IP addresses to be displayed for the same server. Server icons indicate the following statuses:

Client is connected to this server

Server is offline

Server version is incompatible with other servers in the Site (see "Updating Nx Witness")

Server is unauthorized. In this very rare situation, the password for the Administrator does not coincide with other servers, so this server is not able connect to the Site. To fix this

issue, open the **Server Web Page** in the Server context menu, open the **Server Settings**, select the corresponding server, and click on **Reset to Defaults**. Then reconnect to the Site (see "Using a Server's Web Interface").

Devices (various icons)**:** Each server shows a list of the attached devices. When a mouse cursor hovers over a device icon in the Resource Panel, a thumbnail of a frame taken by that device will open (thumbnails update every 2-3 seconds). Devices attached to a Server can include:

 Cameras

 Virtual Cameras

 I/O Modules

 Multi-Channel Cameras

 Recorders

 Groups: Two or more of the above devices organized into a group. To create a group, select two or more resources, right-click the selection, and click **Create Group**.

Device icons indicate the following statuses:

 or  – Device is offline (see "Diagnosing Offline Devices").

 or  – Device is unauthorized (see "Configuring Device's Authentication").

Icons to the left of a device name indicate the following:

● – Device is currently in recording mode.

○ – Device is configured for recording but is not recording at the moment.

○ – Indicates camera is not recording but there a recorded archive is available.

! – Device is experiencing network issues (see "Device Disconnection/Malfunction" or "Working Around Device Issues (Expert Settings)").

NOTE: "Preview is outdated" message is displayed over the video preview thumbnail of a device if the thumbnail has not been updated in over 15 minutes.

 – *Layouts:* Contains resources (devices and local files). Owned by the user.

 *Cloud Layouts* – Layouts that are available to the user from within the Cloud Portal.

 *Shared Layouts* – Layouts created by an administrator or power user and made available to a User or Groups of Users.

 Locked Layouts – Layouts that cannot be changed (see "Locking Layouts").

 – *Showreels:* Cycle display through a sequence of layouts (see "Showreel (Tour Cycle)").

 – *Integrations:* Show the viewing cells containing an Integration (see "Adding a Web Page as an Integration").

– *Web Pages:* Show the viewing cells containing a web page (see "Adding a Web Page as an Item").

– *Video Walls:* Control multiple displays remotely (see "Video Wall Management").

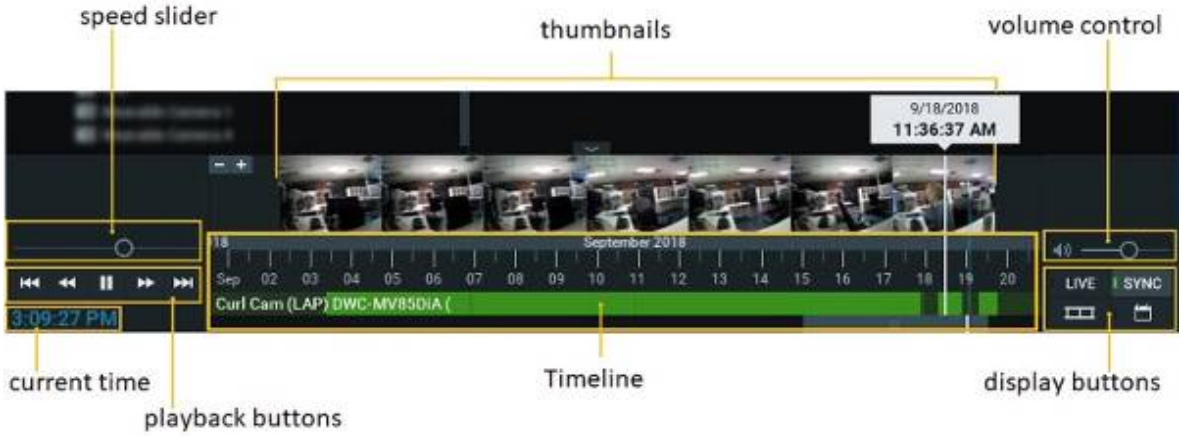
– *Other Sites:* Shows servers on local network that belong to different Sites and currently available Cloud Sites (see "Configuring Multi-Server Environment").

– *Local Files:* Displays the following file types:

- Local Video files (see"Playing Local Video Files in Nx Witness").
- Exported Video Files (see "Exporting Video").
- Exported Multi-Video Files (see "Multi-Video Export").
- Screen Recordings (see "Screen Recording").
- Images.
- Screenshots (see “Taking Screenshots”).

Playback Panel

The *Playback Panel* provides archive and local file playback controls, extensive search capabilities, and seamless transition from live to archived footage.



- *Current time* – displays the current time from your computer.
- *Playback buttons* – use to start, stop, and control playback speed.
- *Speed Slider* – alternate control for playback speed.
- *Timeline* – controls navigation through archive footage. See "Using the Timeline".
- *Thumbnails* – drag the upper edge of the Timeline upward to display preview thumbnails. See "Using Thumbnails".
- Display buttons:
  - *LIVE* – switches selected camera(s) to live playback mode. See "Parts of the Timeline".

- *SYNC* – performs time synchronization of all cameras displayed on the current layout. See "Synchronizing Playback".
-  – use to filmstrip icon to show or hide thumbnails above the Timeline.
-  – use to calendar icon to open the archive navigation Calendar Control".

- *Volume control* – adjusts audio volume of the client application. See "Adjusting Volume".

NOTE: Users must have the Play Audio permission, either directly assigned, or through group membership to play audio.

Notification Panel

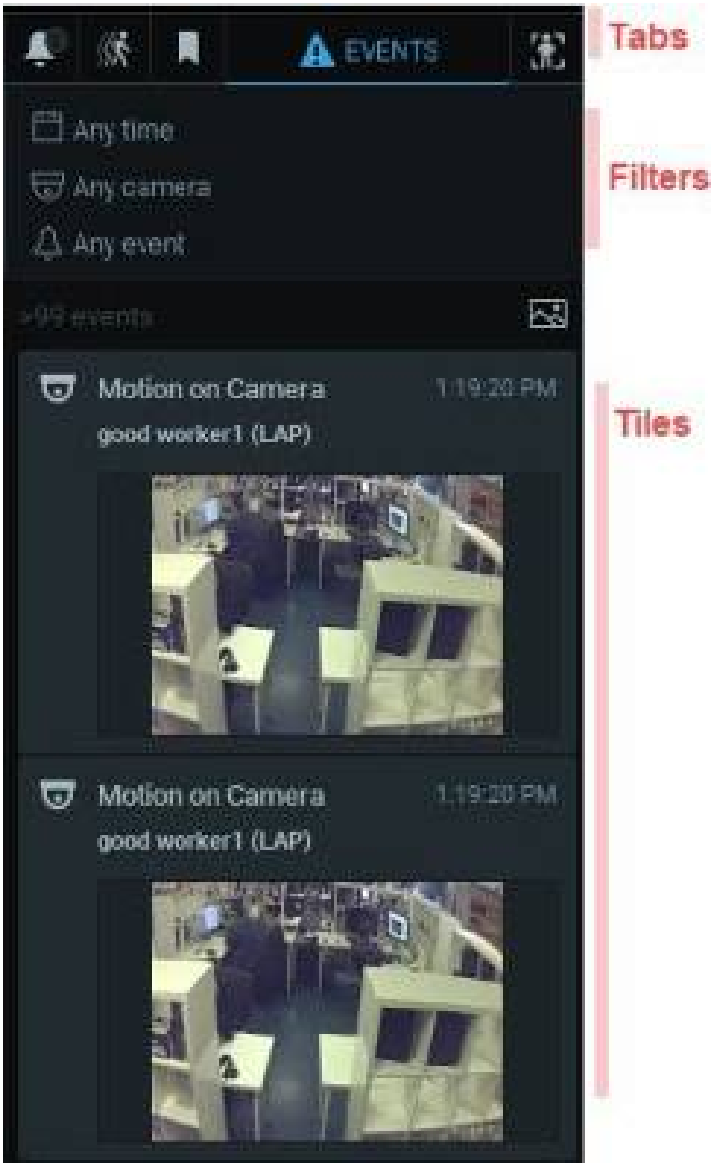
The Notification Panel is constructed of multiple tabs that group information into the following subjects:

- *Notifications*
- *Motion*
- *Bookmarks*
- *Events*
- *Objects*

Having these informational elements together enables efficient search, filter, and awareness to detected events and alerts without leaving playback mode, layout view, or needing to open another window.

The Notification Panel has three main sections:

- Tabs
- Filters
- Tiles.



NOTE: The language displayed in the notification panel is set in the Configuring Users dialog.

Panel Behavior

The Notification Panel can be minimized/maximized by clicking on the arrow dividing the panel from the Viewing Grid.

Right-clicking on the background in any tab opens a generic context menu with these options:

- *Open the* Event Log
- *Event Rules* – see "Event Rules"
- *Filter* – see "Global Notifications"

Tab Behavior

Only one tab can be active at a time. Each tab can be searched and filtered independently by time period, camera, or other parameters as applicable to the given tab. Tab visibility depends on the state of the Site and user permissions. For example, the Motion tab is only available if the user has permission to view archive; the Objects tab is only visible if there is an analytical plugin on the Site that can detect objects, or if there is a database of detected objects from a previously attached plugin.

Filters

The filter section has a set of controls which will differ by tab. The state of filter controls is independent and persistent for each tab when configured in the Notification Panel. The filter options to choose from are – time, camera, area for motion detection, event type for events, object type, and area selector for objects. See "Searching and Filtering" for more details.

Click on a filter control to open a menu of options. When a filter is applied it will be highlighted. Some filters can also be added by selecting an item outside of the Notification Panel, such as clicking on a camera tile or selecting an area on a camera tile to filter motion detection. Click on the **X** to clear a filter.

- *Time selector* – The following options are available:
  - *Any time* (default)
  - *Last day*
  - *Last 7 days*
  - *Last 30 days*

  NOTE: If a segment is selected on the Timeline, that segment becomes the time filter and it is applied to all tabs.
- *Camera selector* – The following options are available:
  - *Any camera* (default)
  - *Current camera*
  - *Cameras on layout*
  - *Choose cameras*
- *Area selector* – Available to the Objects and Motion tabs only, with the prompt to "*Select area on the video to filter results*" if an area is not selected, or in filtered state "*In selected area*". In the Motion and Objects tab, selecting an area simultaneously selects the related camera.
- *Event selector* – Available for the Events tab only and has a two-level menu where the second level menu options are dependent on the top-level selection. Available events are:
  - *Any event*
  - *Motion on Camera*
  - *Input Signal on Camera*
  - *Soft trigger*

- *Plugin Diagnostic Event*
- *Generic Event*
- *Analytics Event*
- *Camera Issues*
- *Server events*

- *Plugin selector* – Only available while in the Objects tab. Its options depend entirely on the third-party products integrated with your Nx Witness Site.
- *Object selector* – Only available while in the Objects tab. Its options depend entirely on the third-party products integrated with your Nx Witness Site.

Event Counter

The event counter shows the number of events displayed in the tiles section. Click the image button () to toggle thumbnails on and off, and in the Objects tab, you also have the option to click the information button () to toggle thumbnail information on and off.

Tile Behavior

Tiles display is always ordered with the most recent tile on top. If the source camera is not in the current layout, double-click to add it or open it in a new layout tab (Right-click). If the source camera is open in the active layout and SYNC mode is turned on, the archive playback for all items in the layout will be synchronized to that camera's Timeline. Clicking on a tile opens the related archive and moves the Timeline marker to the start of the Bookmark.

All tiles have one of four priority types, as indicated with color:

- *Default*
- *Success*
- *Alert*
- *Critical*

The Notifications and Event tabs handle tiles a little differently depending on the event type. A notification tile may open because of an event and then close, or may open and only close when the triggering event ends or the triggering Site state changes. However, Desktop Notifications have an option **Forced Acknowledgment** setting that prevents their closure until required actions are complete.

Search Field

When there is a search field, text input filters all results so only the tiles that meet the search criteria are displayed.

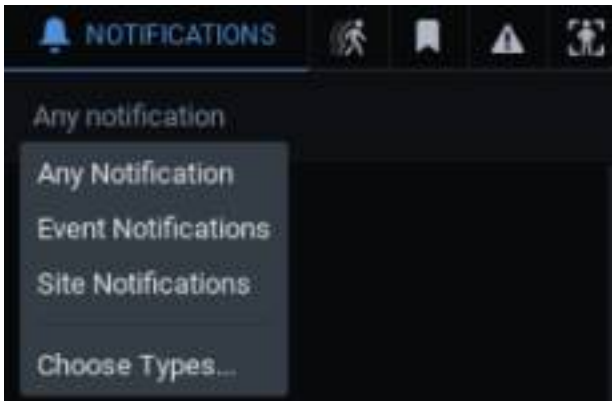
Responding to a Notification

While in the Notifications tab, hovering the cursor over a notification displays additional information according to the notification type.

Clicking or double-clicking on a notification displays additional information and triggers a corresponding action. For example, clicking on a "network issue on device notification" displays the last frame received from that device and opens the *Device Settings* dialog.

Notifications Tab

Users can select to receive any notifications, one of two types of notifications, or a customized list of selected notifications by clicking on the notification types listed below the notifications icon and label.



Types of notifications:

- *Event Notifications* are generated when an event rule is true and valid.
- *Site Notifications* are generated when specific Site conditions are present.
  - *Site Notifications are* pinned to the top of the tile section display and include the state of a Site component.
  - Most tiles will open the related settings or dialog screen when clicked.
  - Resolution suggestions are provided where possible/

NOTE: Users can disabled selected notifications using the Notification Suppression dialog.

Cross Site Notifications:

Sites that are connected within a common Organization will display notifications and informers from all Sites in the Organization, when Cross Site Notifications are enabled.

Key Concepts:

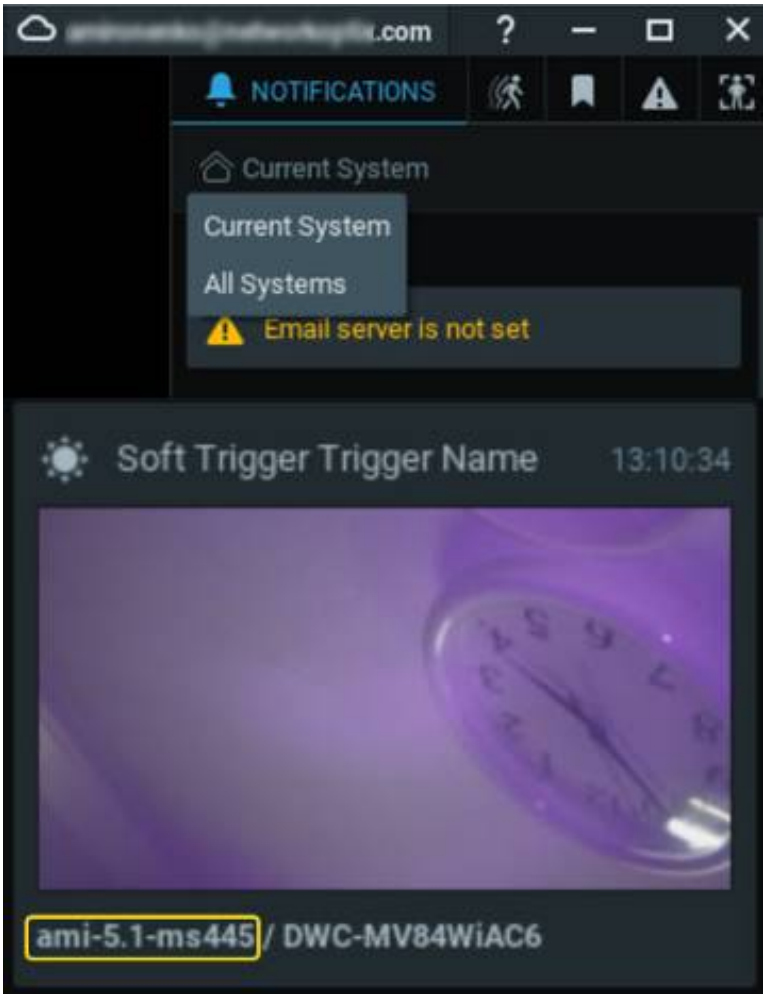
- Users must be logged into the Cloud to receive Cross Site Notifications.
- The Desktop Client will only display communications from Sites that the current user has access to.
- The Cross Site Notification selector is only displayed while logged into the Cloud and when compatible Sites are available.
- Cross Site Notifications must be enabled each time the Desktop Client is restarted – this setting is not saved.

- Notification footers are prefixed with the Site ID instead of the Camera IP Address provided with local Notifications.
- Cross Site Notifications are initiated by the Event Action Show Desktop Notification and adhere to other Event Rules (distribution, timing).

NOTE: If 2FA is required on the Site generating a cross site notification and the receiving user is not authenticated, then the user will be provided an informative dialog and the option to authenticate and enable receipt of notifications from the Site generating (2FA) notifications.

To enable or disable Cross Site Notifications

1. Select the Notifications tab in the right panel.
2. Under the tab title (Notifications) select All Sites to enable or Current Site to disable Cross Sites Notifications.



Site Notifications

The following Site Notifications serve to inform users when current settings or operational factors may limit Site features or performance.

Each of these Notifications can be suppressed per user.

Notifications Common to all Versions		
Notification Title	**Additional Information**	**Click on Notification Action**
Email address is not set	Email delivery of notifications to the logged in user are not possible.	Opens Edit User dialog window dismiss the notification.
Email server is not set	The Site cannot send Email notification until an outgoing Email server is configured.	Opens the Email server configuration dialog or dismiss the notification.
Some user have not set their email addresses	Provides a list of users without valid email addresses. user--1 user--2	Opens the user dialog window for the first user in the list or dismiss the notification.
Error while sending email	Outgoing message were not processed by the Email server.	Opens the Email server configuration dialog or dismiss the informer.
Storage is not configured	Provides a list of server where storage is not configured. server--1 server--2	Opens storage management dialog or dismiss the notification.
Rebuilding the archive index is complete	Provides a list of server where archive index has been rebuilt.	Opens storage management dialog or dismiss the notification.
Rebuilding the archive index is canceled by user	Provides a list of server where archive index rebuild was canceled before completion.	Opens storage management dialog or dismiss the notification.
Archive integrity problem detected	Event occurs when archive files are removed, renamed, manually changed, or when a file has a incorrect time data.	Dismiss the notification
Site has no internet access for time synchronization	No online server in the site has internet access for time synchronization	Opens time settings dialog or dismiss the notification.
Backup storage is not configured	Provides a list of server where backup storage is not configured.	Opens storage management dialog or dismiss the notification.

Notifications Common to all Versions		
	server--1 server--2	
Camera recording schedule is invalid	Some cameras are set to record in a mode they do not support.	Opens camera settings window dismiss the notification.
Storage for analytical data not set	A storage location for analytical data has not been configured.	Opens storage management dialog or dismiss the notification.
System partition is used for analytics data	Analytics data can take up large amounts of space. We recommend choosing another location for it instead of the system partition.	Opens storage management dialog or dismiss the notification.
Intercom call	Incoming intercom call (signal) received	Opens intercom dialog
Intercom call missed	An incoming intercom event was not answered.	
Recording disabled	Recording is disable	
Enterprise Version		
Notification Title	**Additional Information**	**Click on Notification Action**
Local recording services overused	The number of services in use exceeds the number of services available	
Cloud storage services overused	The number of services in use exceeds the number of services available	
Paid integration services overused	The number of services in use exceeds the number of services available	
Site suspended	The Site has been suspended – contact your channel partner for assistance	
Site shutdown	The Site has been suspended – contact your channel partner for assistance	

Notifications Common to all Versions		
Site will stop functioning soon	Site is schedule to be suspended or shutdown in less than 30 days	
Cloud storage backup disabled	Cloud backup is configured, yet disabled	
Paid integration services disabled	A paid integration services is available, yet currently disabled and not in use	
Professional Version		
Notification Title	**Additional Information**	**Click on Notification Action**
Remote archive synchronization failed	Remote archive synchronization has been started for resource: {device.ID}	
No licenses	No licenses are available and recording is prohibited.	Opens the license configuration dialog or dismiss the notification.
Deprecated Notifications – May Appear in Historical Logs		
Site Notification Title	**Additional Information**	**Click on Notification Action**
Archive Backup Finished		N /A
Remote archive synchronization failed	Remote archive synchronization has been started for resource: {device.ID}	N /A
Remote Archive Synchronization	Started synchronization of data on remote device to the Site archive.	N /A
Site in Safe Mode.	Site operating in safe mode after experiencing an unanticipated event.	N /A

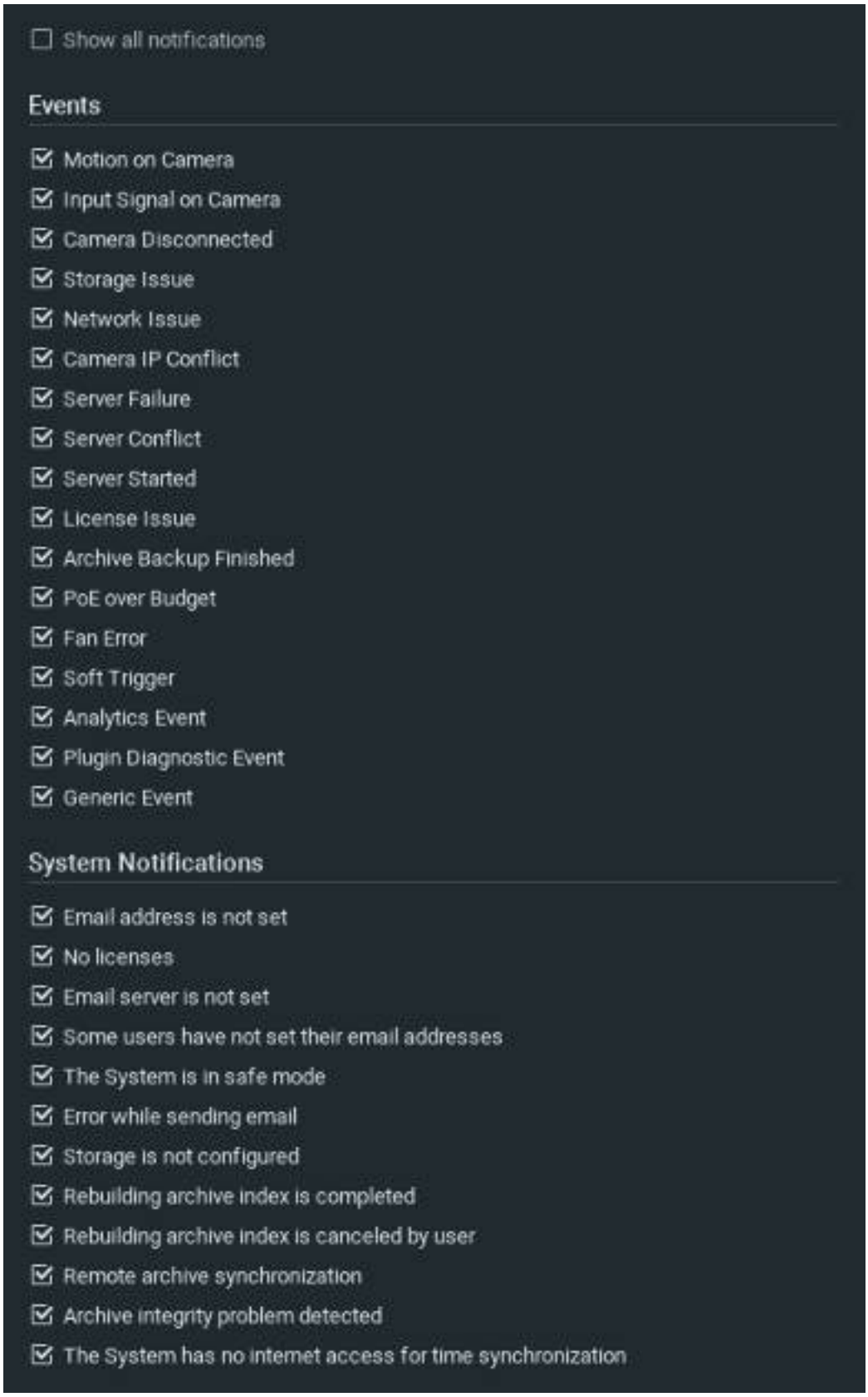
Disable Notifications

Individual event notification can be disabled by the user without effecting the event rules or notifications received by other users of the Site. This can reduce use distractions related to certain domains at the risk missing a relevant notification, and thus should be used with caution.

To select the displayed notifications for a user, first select the Alerts tab in the Notification Panel and then open the label below the notifications tab and select one of the following choices from the menu:

- Any notification to automatically select the *Show all notifications* checkbox atop the list of notifications
- Event notifications to automatically select all event notifications and deselect all Site notifications.
- Site notifications to automatically select all Site notifications and deselect all event notifications.
- Choose Types... to open the individual notification selection dialog.

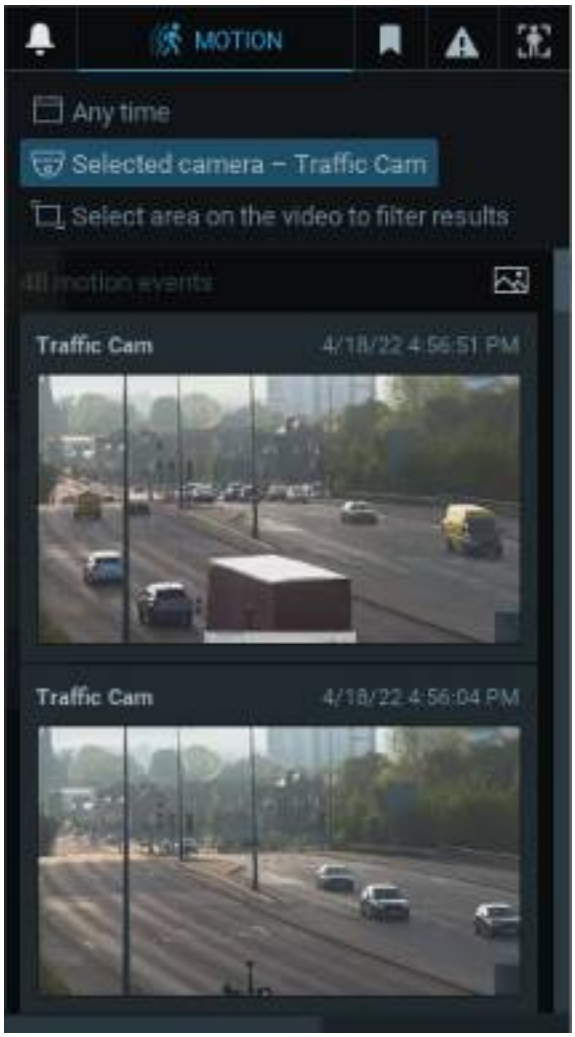
NOTE: The checkbox for *Show* all notifications must be cleared to enable individual notification selection.


Show all notifications
Events
Motion on Camera
Input Signal on Camera
Camera Disconnected
Storage Issue
Network Issue
Camera IP Conflict
Server Failure
Server Conflict
Server Started
License Issue
Archive Backup Finished
PoE over Budget
Fan Error
Soft Trigger
Analytics Event
Plugin Diagnostic Event
Generic Event
System Notifications
Email address is not set
No licenses
Email server is not set
Some users have not set their email addresses
The System is in safe mode
Error while sending email
Storage is not configured
Rebuilding archive index is completed
Rebuilding archive index is canceled by user
Remote archive synchronization
Archive integrity problem detected
The System has no internet access for time synchronization

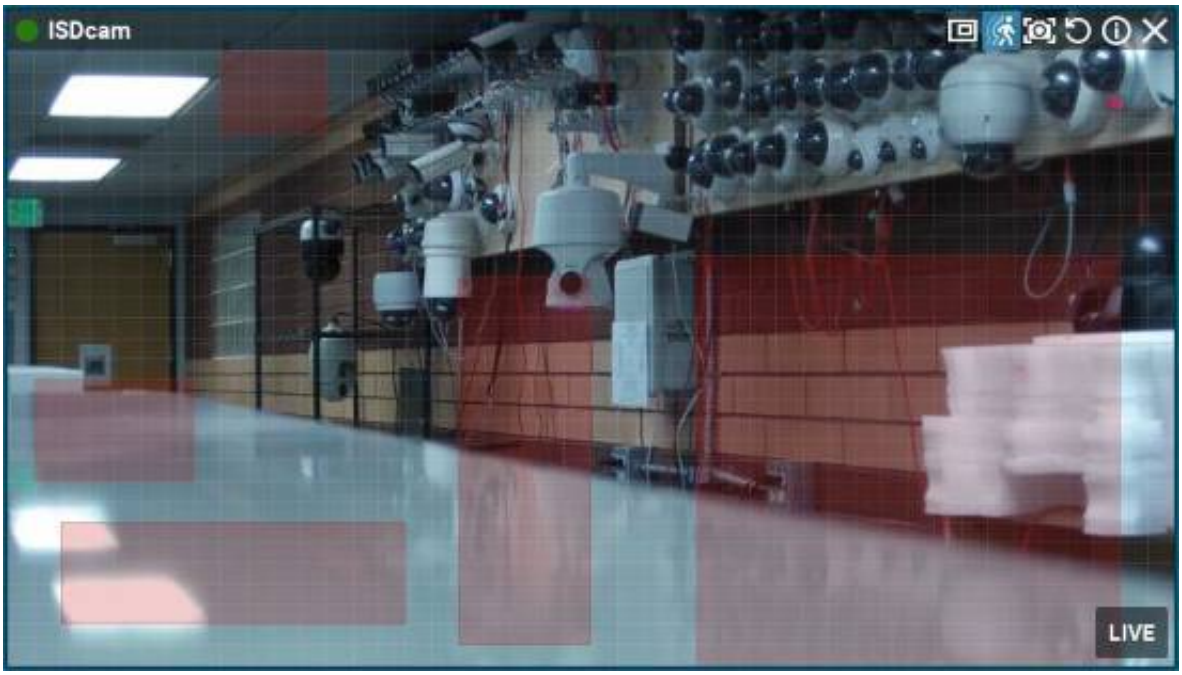
Motion Tab

When the *Motion* tab is active, the Client enters *Motion Search* mode. Conversely, any other method of entering Motion Search mode will launch the Motion Tab. In this mode, items in the active layout have a a semi-transparent Motion Smart Search grid placed over the image. The default filter display is any time and the currently selected camera.

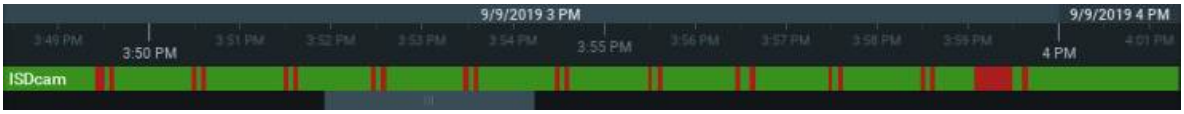
NOTE: Motion search is limited to a single device at a time.



When you click-and-drag on an item display, a red rectangular area is created in which motion will be detected for that camera. Multiple search areas can be created by holding down the Ctrl button while drawing. Selecting a detection area also sets the filters to the states *Selected Camera* and *Selected Area*.



Archive segments on the Timeline that have motion in the selected area are highlighted in red. It is possible to have a motion detection area in as many layout items as you like. When you shift focus to a different camera, the motion search display switches accordingly.



To enter Motion Search mode from layout

- Right-click on the item and choose **Show Motion/Smart Search** option from the context menu.
- Click the **Smart Motion Search** button ( ) in the top right of the item tile.
- Press the Motion tab shortcut on your keyboard (the *m* key*)*.

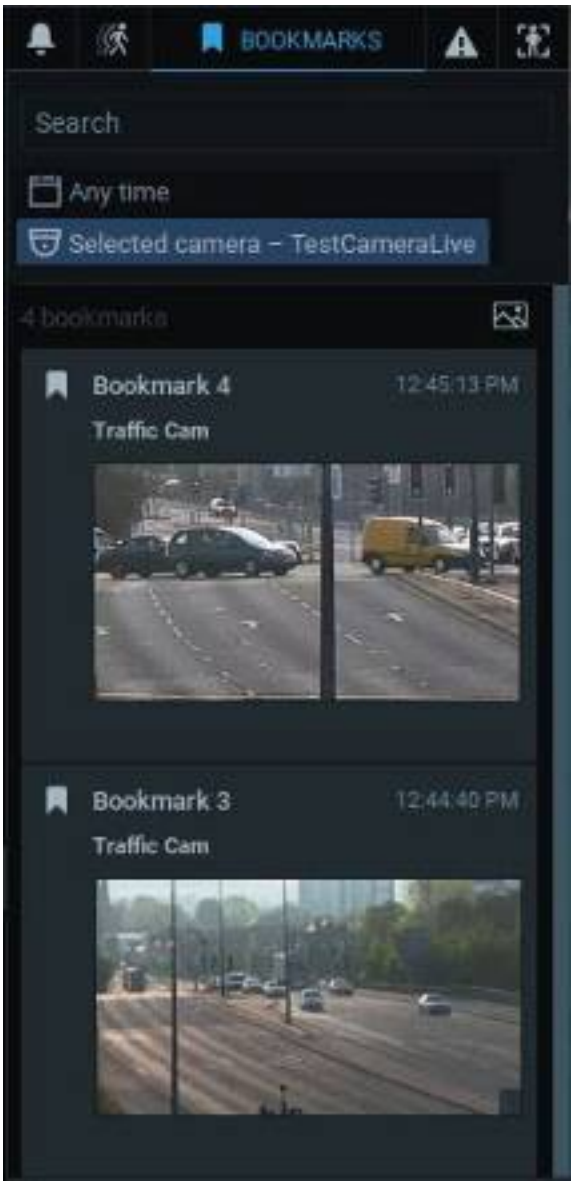
Bookmarks Tab

The *Bookmarks* tab in the Notification Panel provides a visual interface for searching and viewing Bookmarks. All information from the Bookmark dialog is displayed with a thumbnail image from approximately the middle of the Bookmark video.

Key points about using bookmarks:

- When a camera is selected, Bookmarks in the archive will be shown in descending order by archive timestamp.
- Clicking on a Bookmark will move the Timeline marker to the start of the Bookmark.
- The default filter display is any time for any camera on the layout.

- Use search to find a Bookmark Names, Descriptions, and Tags (See "Searching and Filtering " for more details).
- Bookmarks can be shared from within the Cloud Portal.



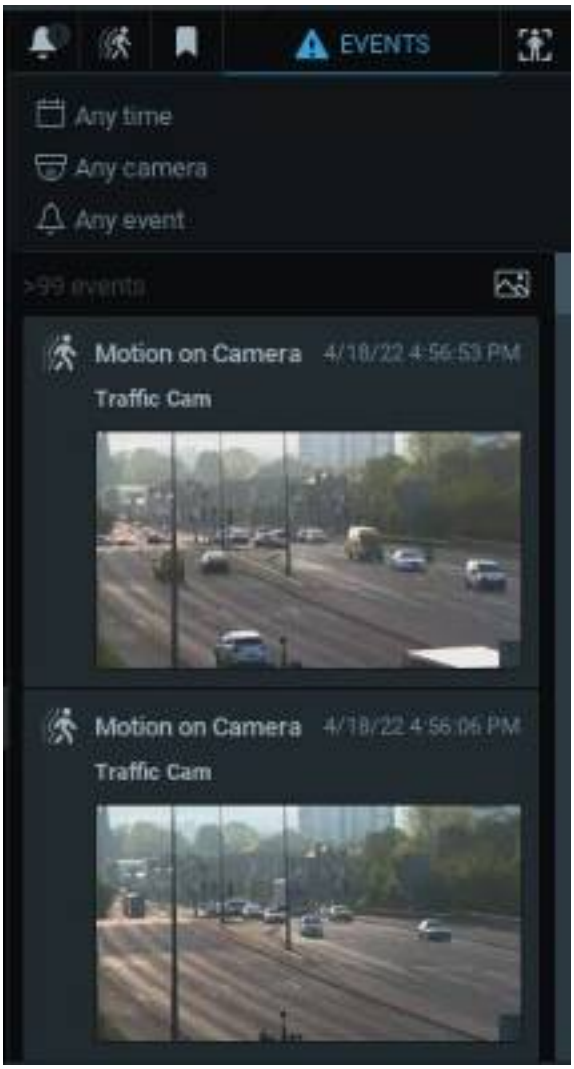
When the Bookmarks Tab is active, blue bookmark segments will display in the Timeline (see "Using Bookmarks" for more details.)

Events Tab

Key Concepts:

- The *Event* tab is only available to users who have permission to view the Event Log.

- This tab provides a summary and visual display of the Events Log content (see "Viewing and Exporting the Event Log").
- Default filter display is any time, any camera, and any type of event.



Objects Tab

Key Concepts:

- The objects tab is provides access to the configuration controls and display of object-based analytical searches.
- Options and controls available are dependent on the permissions granted to the current user and the abilities of the (analytical) plug in used.
- Visibility of the *Objects* tab depends on the existence and type of analytical service available to the device or Site, and the user's permission level.
- The object filter will refine to results using specific object types; with "Any" being the default for all fields.

- Selectable object types (e.g., car, human, bicycle, etc.) vary between plugins and the hosting, source device.
- Newly detected objects on the video source will appear hen an analytical plugin is enabled or the plugin settings are changed.
- Object detection can be applied to a video source that is being viewed, with or without recording being active.
- Detections not recorded to the archive will be lost after closing the Desktop Client.
- Previously detected objects stored in the archive will also appear as tiles.
- Detected objects are outlined by bounding boxes that can be seen in the thumbnail that appears when hovering over the tile.
- The color used for bounding boxes can vary between object types and the analytical plugins used.
  - Some analytical plugins allow for the customization of the bounding box color or other elements - plug in options vary by version and source device.
- The Search tool will search through object types and object text attributes (e.g., color, make, travel speed, etc.).
  - See "Searching and Filtering", "Analytics: Region of Interest", and Advanced Object Search for more details.

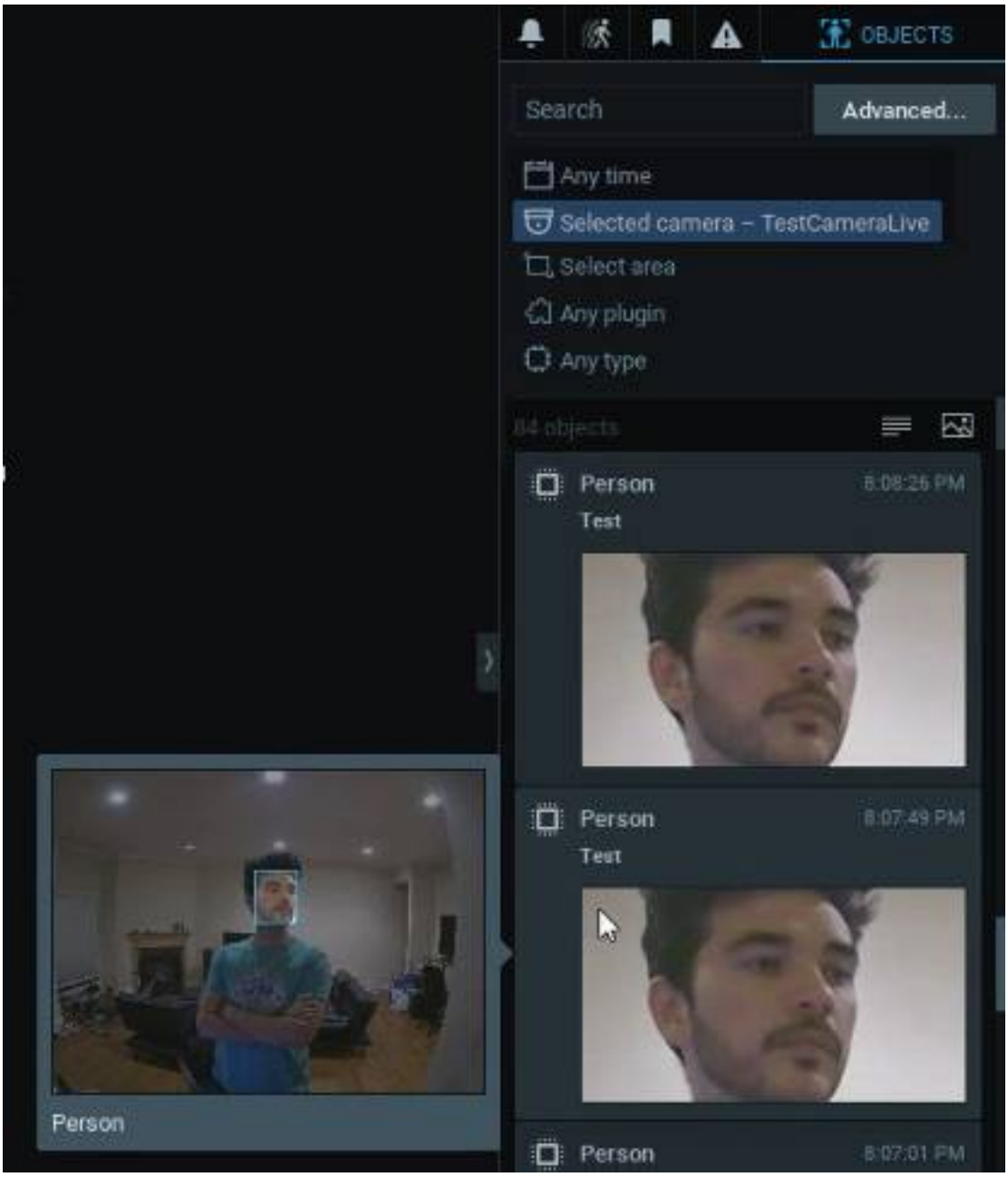
  NOTE: The device filter in Advanced search inherits the device filter from the Objects tab and is limited to one device when using a Cross-Site Layouts.

General Object Search Example:

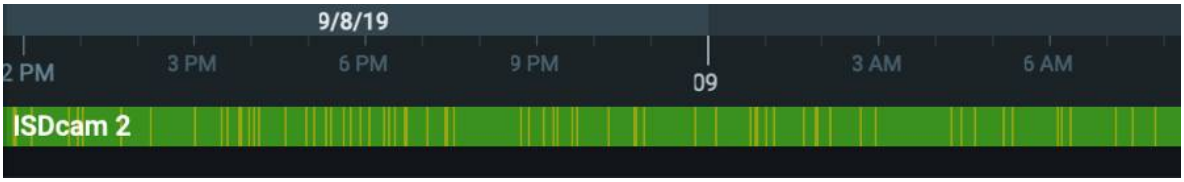
In the following example:

- The object "Person" was detected within the testcamera feed twice.
- All available parameters are set to "Any", including the region of interest (area) of the video.
- The detection bouncing box and event time is shown while the user hovers over the detection tile.

  NOTE: Fields from an *Analytics Event* can be used to automatically fill in certain parameters when creating a HTTP(s) Request.



- Detected objects are indicated with yellow segments in the Timeline.



1.3.7.7.1 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:

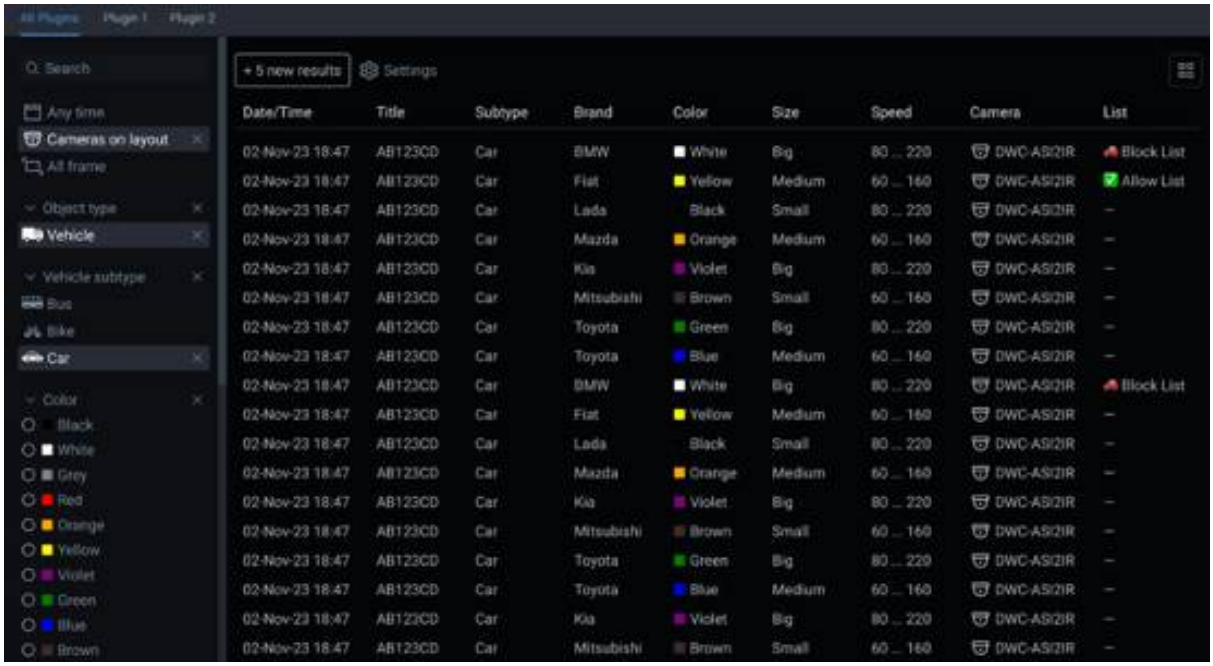
1. Select the Objects Tab from within the Notification Panel.
2. Click on the **Advanced** button to open the Advanced Object Search dialog.
3. Select the active plug-in from header menu or select **All Plugins** – all plugins may not support all select object attributes.
4. Configure the search and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



Working with Multiple Windows

It is possible to open multiple client windows in a single or multiple monitor environment.

To open a new window, click on **Main Menu** > **New** > **Window**. You can select Items from the Resource Panel or Viewing Grid and drag them to the new window.

You can also select an item and open it directly in a new window:

1. Select desired Items in the *Resource Panel* or on the *Viewing Grid*.
2. Select **Open in New Window** from the context menu.

Video Wall Mode provides further control of multiple displays and broadcast capability.

Keyboard Shortcuts

These Keyboard Shortcuts are for Windows and Ubuntu clients – many also work for macOS by replacing "CTRL" with "Command" key.

Keyboard shortcuts only affect the active item and may not have a global response from within the Desktop Client.

Action	Windows Shortcut	macOS Shortcut
About	F1	F1
Alarm / Event Rules	CTRL + E	CMD + E
Archive selection end	]	]
Archive selection start	[	[
Bookmark Log	CTRL + B	CMD + B
Exit item's fullscreen mode	Esc	Esc
Check File Watermark	Alt + C	Option + C
Close layout	CTRL + W	CMD + W
Connect to another Server	CTRL + Shift + C	CMD + Shift + C
Create new Layout	CTRL + T	CMD + T
Device List	CTRL + M	CMD + M
Disconnect from Server	CTRL + Shift + D	CMD + Shift + D
Duplicate item on layout	CTRL + drag-and-drop	CMD + drag-and-drop
Enable Smart Search	Shift + Left click + drag area	Shift + Left click
Enable/disable Image Enhancement	Alt + J	Option + J
Event Log	CTRL + L	CMD + L
Exit Desktop client	Alt + F4	Option + F4
Fisheye dewarping (toggle)	D	D

Action	Windows Shortcut	macOS Shortcut
Hide all panels and switch to Fullscreen Mode	F11	F11
Hotspot toggle	H	H
Information on Item (toggle)	I	I
Maximize/minimize item	Enter	Enter
Move entire scene	Alt + arrows	Option + arrows
Move PTZ/fisheye camera angle	←, ↑,→, ↓	←, ↑,→, ↓
Mute	U	U
Next layout in tour	→, ↓, PgDn, Space, or Enter	
Next recorded chunk	X	X
Open Bookmarks tab (from Notification Panel)	CTRL + B	CMD + B
Open Events dialog	CTRL + E	CMD + E
Open local file	CTRL + O	CMD + O
Open Motion tab (from Notification Panel) Smart Search Toggle	M | Alt + M to toggle	M | Option + M to toggle
Open new window	CTRL + N	CMD + N
Open Notifications tab (from Notification Panel)	N	N
Open Objects tab (from Notification Panel)	O	O
Play/Pause video	Space	Space
Playback slow down (on play) / previous frame (on pause)	CTRL + ←	CMD + ←
Playback speed up (on play) / next frame (on pause)	CTRL + →	CMD + →
Playback – forward 10 seconds	→	→
Playback – rewind 10 seconds	←	←
Previous layout in tour	←, ↑, PgUp, Backspace	
Previous recorded chunk	Z	Z
PTZ (toggle)	P	P

Action	Windows Shortcut	macOS Shortcut
Remove item from layout	Delete	Delete
Rename Resource	F2	F2
Rotate item	Alt + Click-and-drag	Option + Click-and-drag
Rotate with 15-degree step	CTRL + Alt + Click-and-drag	CMD + Option + Click-and-drag
Save layout	CTRL + S	CMD + S
Save layout as	CTRL + Shift + S	CMD + Shift + S
Screen Recording (toggle) – Windows Only	Alt + R	Option + R
Screenshot from selected item	Alt + S	Option + S
Search Resource Panel	CTRL + F	CMD + F
Select camera on layout	Shift + ←, ↑,→, ↓	Shift + ←, ↑,→, ↓
Shift selection in Resource Panel	↑, ↓	↑, ↓
Start tour on layout	Alt + T	Option + T
Switch Layout	CTRL + Tab	CMD + Tab
Switch to LIVE	L	L
SYNC on/off	S	S
Site Administration	CTRL + Alt + A	CMD + Option + A
Volume down	CTRL + ↓	CMD + ↓
Volume up	CTRL + ↑	CMD + ↑
Windowed mode/Fullscreen	Alt + Enter	Option + Enter
Zoom in/out on PTZ or a fisheye camera	[+]or [-] + Mouse Scroll Wheel	[+]or [-] + Mouse Scroll Wheel
Zoom window (create)	W	W

Getting Context Help

Nx Witness includes an integrated User Manual.

To launch the User Manual using contextual clues, click on the **Help** button "**?**" in the Navigation Panel, then click on the desired interface element. The User Manual will open in a web browser and display the topic most relevant to the element clicked on.

Pressing the **F1** button at anytime will also open the *About Nx Witness* dialog, which displays important platform and network configuration information (see "Collecting Additional Information").

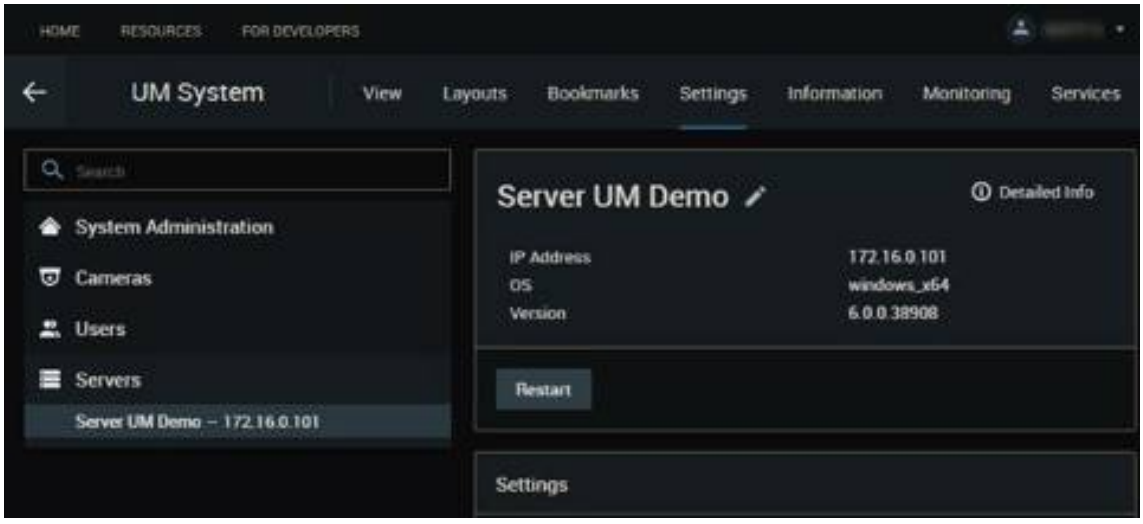
Nx Cloud Portal

Nx Cloud is an important part of Nx Witness that extends functionality of Nx Witness Sites.

Once a Site is linked to Nx Cloud, it becomes possible to access the Site from virtually any Internet browser. Depending on your Site configuration, the Nx Cloud can display Bookmarks and Cloud Layouts that contains devices from different Sites. See "Connecting Site to Nx Cloud" and "Logging in to Nx Cloud".

The Cloud Portal menus and options are contextually aware and will change based on selections made, Site configuration, and user permissions.

- A menu positioned along the header area includes tabs for enabled functions (View, Layout, Bookmarks, Settings, Information, Monitoring, Services).
- The tabs displayed will vary depending on the version of software and permission of the active user.
- The left panel provides for second-level menus choices, filters, or resource selection controls.
- Information refined by the menu selections made is displayed in the Center display panel.



Setting Up 2 Factor Authentication

Improve the security of your Nx Cloud account and prevent unauthorized access by enabling Two-Factor Authentication (2FA). Logging into an account with 2FA turned on requires a verification code generated by a mobile authentication app (e.g. Google Authenticator, Microsoft Authenticator, or Duo Mobile) in addition to your *Nx Cloud* password to be entered.

NOTE: When 2FA is enabled, a TOTP verification code will be required for a Cloud user to change their password.

To Turn On Two-Factor Authentication

1. Install Google Authenticator, Microsoft Authenticator, or Duo Mobile on your mobile device.
2. Open Nx Cloud Portal and log in to your account.
3. Open the Account Settings drop-down menu and click **Security**.
4. Enable **Two-factor Authentication**.
5. Enter your Nx Cloud account password.
6. Open the mobile authentication app 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.

NOTE: For additional security, enable *Ask for verification code on every log in with Nx Cloud account,* or generate single-use backup codes to keep somewhere safe that can be used to log in if you lose access to the mobile authentication app.

To Require Cloud Users to Have 2FA Enabled

1. Open Nx Cloud and log in as a Site Administrator.
2. Navigate to the **Site Administration > Security page**.
3. Select the option "*Mandatory two-factor authentication for cloud users*".

   Cloud users without two-factor authentication will not be able to log into the Site. This setting does not affect local and LDAP users.

To Turn Off Two-Factor Authentication for a Cloud User

1. Open Nx Cloud Portal and log in to your account.
2. Open the Account Settings drop-down menu and click **Security**.
3. Click the **Disable** box.
4. Enter the TOTP verification code generated by the mobile authentication app.
5. Click the **Disable** box to complete the action or select **Cancel**.

To Generate Backup Codes

Backup codes can be used when mobile cannot be used.

1. Open Nx Cloud Portal and log in to your account.
2. Open the Account Settings drop-down menu and click **Security**.
3. Click the **Generate Backup Codes** button.

NOTE: Any previously generated backup codes will be invalidated.

   a. Click the **Copy All** button to copy the backup codes to the clipboard.
   b. Paste the backup codes into a recovery file and save it to a secure location.

To Authenticate using Backup Code

1. Open Nx Cloud Portal and log in to your account.
2. When prompted for the verification code, click the link at the bottom of the dialog box labeled **No access to authentication app?**
3. Enter one of the previously generated and saved backup codes
4. Click the **Log In** button.

   NOTE: Each Backup code can only be used one time. Remember to regenerate new codes if they are frequently used to access Sites.

Site-Wide Configurations

The Site Administration dialog (Ctrl+Alt+A) is used to manage Users, configure Devices, maintain Licenses status or allocate Services, a setup up outgoing Email services, and create the events Nx Witness will track,.

The dialog contains the following tabs and sections:

- *General*
  - *Event Rules* – opens the dialog when to configured events and corresponding actions can be configured.
  - *Event Log* – opens the list of events that occurred.
  - *Device Camera List* – opens the list of devices in the Site.
  - *Audit Trail* – opens the list of users' actions. Can be enabled and disabled.
  - *Bookmarks* – opens the Bookmark log.
  - *Site Settings* – selectable options displayed on the General Tab:
    - Enable Automatic Device Discovery.
    - Send anonymous usage and crash statistics.
    - Preventing Nx Witness from Changing Device Settings.
    - Custom language for Cloud notifications.
- *User Management* – access the configuration dialogs for Users and Groups.
- *Updates* – tools to manage versions and updates.
- *Licenses* – view, activate and manage Site Licenses (Professional Edition only).
- Services – view, activate and manage Site Services (Enterprise Edition only).
- *Email* – enable the Cloud Email service or configure an outgoing Email server.
- *Security:*
  - Use only HTTPS to connect to cameras.
  - Force servers to accept only encrypted connections.
  - Encrypt video traffic.

- Archive encryption.
- Adding a User Watermarks.
- Enable Audit Trail.
- Limit session length.
- Remote Access Tool.

- *Nx Cloud* – use this tab to create or connect to a Cloud account.
- *Time Synchronization* – lets you choose or synchronize Server time.
- *Routing* – shows Site servers and their IP addresses.
- *Plugins* – this tab lists the analytics plugins on the Site, in alphabetical order by device manufacturer.
- *Advanced*:
  - Logs Management – enables users to specify log levels and download log files.
  - Backup and Restore – creates or restores a backup database of the Site configuration (server and camera settings, users, event rules, etc.).

Site Nx Cloud Connections

Connecting a Site to a Cloud Account will enable Nx Cloud features and additional connection methods. Sites can be connected using the Desktop Client or the Nx Witness WebAdmin Interface.

When User log into Nx Cloud are able to access all the Sites that are connected to their Nx Cloud account (see "Connecting to Site from the Welcome Screen").

The following operations are possible with the Cloud:

- Log in to any Cloud Site without reentering credentials.
- Share access to Nx Cloud with other Cloud Users.
- Share Sites with users and add users to Permission Groups. This action is logged in the Audit Trail of User Actions.

To Connect a Site to Nx Cloud

It is necessary to have a Nx Cloud account first (see "Creating a Nx Cloud".)

Desktop Client

1. Open **Main Menu** > **Site Administration** and go to the **Nx Cloud** tab.
2. Click **Connect Site to Nx Cloud** and log in the Nx Cloud where the Site will be connected.

Web Admin

1. Open the Web Admin and log in.
2. Go to **Settings** > **Site Administration** > **General**.

3. Click **Connect to Nx Cloud** and log in to Nx Cloud where the Site will be connected.

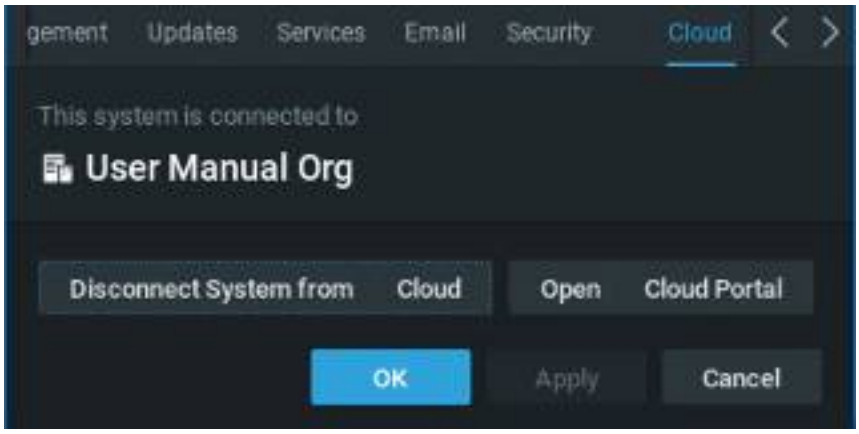
Once connected, the Site will be displayed in the Nx Cloud Portal and will be accessible when logged into the Cloud.

To Disconnect a Site from Nx Cloud

NOTE: Disconnecting a Site will remove access for all Cloud Users that this Site is shared with.

Desktop Client

1. Log in as a Site Administrator.
2. Open **Main Menu** > **Site Administration** and go to the **Nx Cloud** tab.
3. Click **Disconnect Site from Nx Cloud** and authenticate if prompted.
4. Confirm Disconnection and the removal of all Cloud Users from the Site.



Web Admin / Cloud Portal

1. Open the Web Admin and login as a Site Administrator.
2. Go to **Settings** tab in the header menu.
3. Select **Site Administration** > **General** on the left panel.
4. Click **Disconnect Site from Nx Cloud** and authenticate if prompted.
5. Confirm Disconnection and the removal of all Cloud Users from the Site.

Site Organization Connections

Connecting a Site to an Organization will upgrade existing Professional Editions of HD Witness to the Enterprise Edition.

Key considerations before connecting a Site to an Organization:

1. Each recording license key will be converted into a 24-month credit for a Local Recording Service.
2. It is not possible to recover license keys once they are converted into Subscription Service credits.

3. Sites that are disconnected from an Organization will require new recording license keys.

Contact your local Nx Witness reseller or Network Optix customer service team for more information on the benefits of using Organizations.

There are two ways to connect a Site to an Organization:

- Transfer ownership of a Cloud Connected Site from a Cloud Account to an Organization.
- Connect a local Site to an Organization.

Both methods require a Site Administrator and an Organization Administrator to approve the connection.

Transferring Cloud Connected Sites to an Organization

Prerequisites:

- An Organization must be available.
- The Site to transfer must be accessible via the Cloud Portal.

Transfer Process:

1. Open the Cloud Portal and connect to the Site to be transferred.
2. Switch to the **Settings** tab in the Cloud Portal.
3. Click the (change) owner text under the Site Name.
4. Select the **To Organization** in the **Transfer Ownership** dialog.
5. Select the Organization the Site will be transferred to.
6. Confirm the Transfer action.
7. A Site Administrator and the Organization Administrator must authenticate and approve the transfer.

To Connect a Local 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.
5. Select the Organization the Site will be connected to.
6. A Site Administrator and the Organization Administrator must authenticate and approve the transfer.

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.
6. Select the Organization the Site will be connected to.
7. The Site Administrator and the Organization Administrator must authenticate and approve the transfer..

Once connected, the Site will be displayed in the Nx Cloud Portal and will be accessible by Cloud users granted access to the Site.

To Disconnect a Site from the Organization

NOTE: Disconnecting a Site from an Organization will remove access for all Cloud Users that this Site is shared and all Services will be removed from the Site.

The process of disconnection is the same as Disconnecting a Site from Nx Cloud.

Changing Cloud Owner

This topic provides instructions to change the owner of a Cloud Site to another account.

Key Concepts:

- This process will assign a new owner to an existing Cloud Site.
- Ownership of a Cloud Site cannot change is the Site is part of an Organization.
- The to-be Cloud System must be an existing user of the Site to transfer.
- The current owner will be removed from the Site during the transfer process.
- Previous owner must be added as a new user to regain access to the Site.

Instructions for the CURRENT cloud Site owner:

1. Navigate to the Nx Cloud portal and log in as the current Site Owner.

2. Select the **Settings** tab in heading menu.
3. Select the **General** tab under the *System Administration* heading on the left.
4. In the middle of the screen, you'll see the system name followed by the text "owner - you (change)".
5. Click on **(change)** to open the new owner selection dialog.
6. Select the To user (new owner) field and enter or select the new Cloud Owner email address.
7. Select Transfer and authenticate as the current Cloud Site owner.
8. The new owner of the Cloud Site will receive an email to accept the ownership transfer.

Instructions for the NEW cloud Site owner:

1. Open the email account associated with your Nx Cloud account.
2. Locate the automated email generated when the current Owner requested ownership transfer.
3. Navigate to the Nx Cloud portal and log in with the new Site owner account.
4. Select the **Shared with me** tab in the heading menu,
5. Select the Site where ownership is being transferred.
6. Select **Accept** to finalize the transfer; or Reject to refuse the Site ownership transfer.
7. The previous Cloud System Owner receives an email after the transfer is accepted.

NOTE: Optionally add the previous Site owner as a new user, and set their permissions, if they will retain access to the Site.

Upgrade to Enterprise

This topic outlines the process to upgrade an existing Cloud-Connected Professional Edition Site to an Enterprise Edition Site.

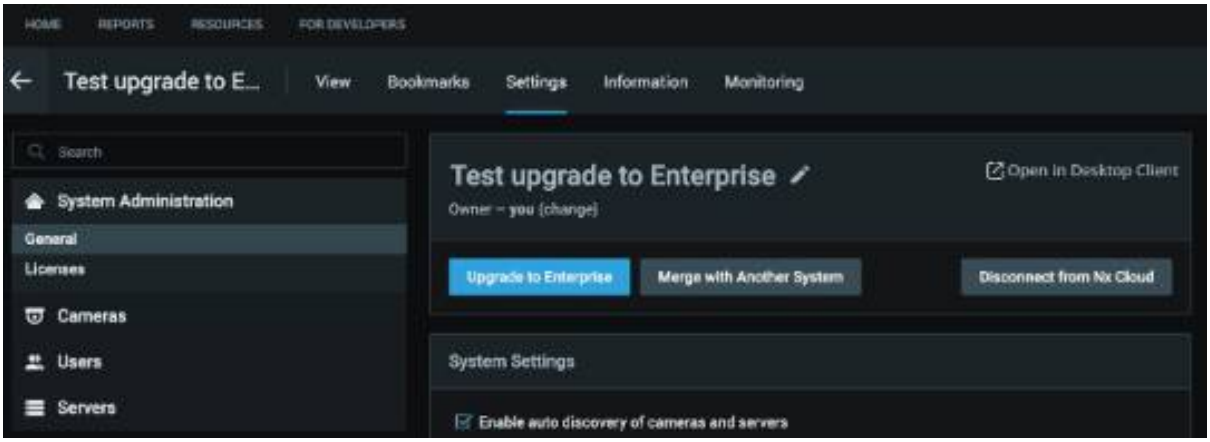
Key Concepts

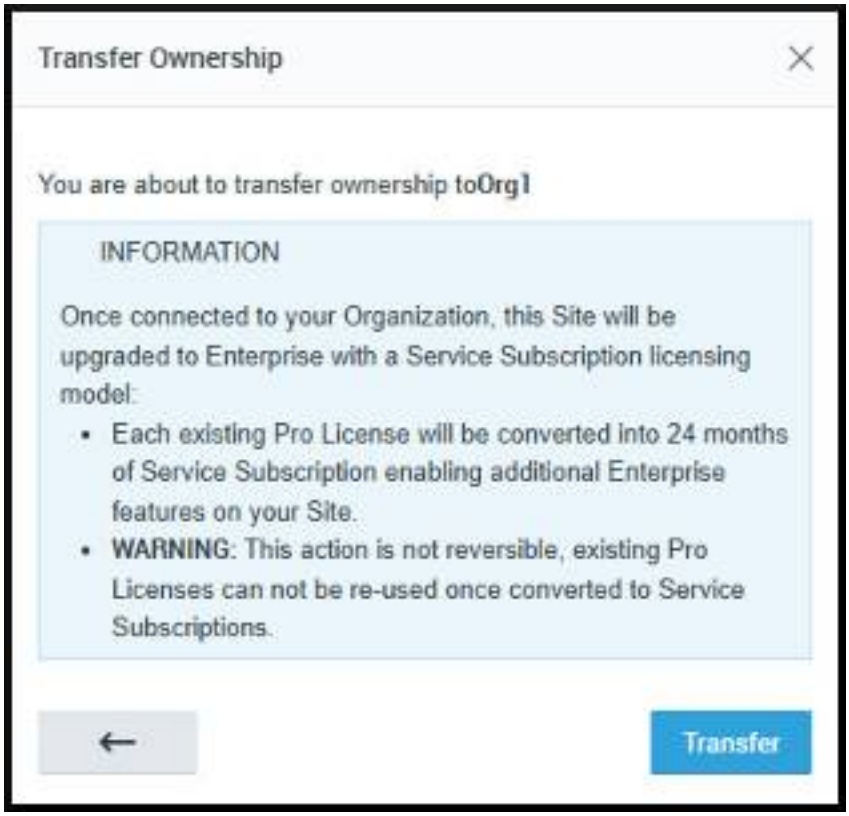
- Once a Professional Edition Site is upgraded to an Enterprise Site, it cannot be undone.
- The Professional to Enterprise upgrade can only be performed in the Cloud Portal.
- Upgrades can only be performed by Organization Administrators.
- Each Professional License will be converted into 24-months of Subscription credits.
- Only the Enterprise Editions provides these features, and more:
  - Unified notifications across all Sites in an Organization.
  - Unified user management and Site access controls.
  - Access to management tools for Subscription Services.
  - Video Wall licenses are included with Enterprise Edition.

- Unlimited Site scalability using the Organization structure.
- Designed to support new features, services, and integrations.

How to Upgrade from Professional to Enterprise Edition

1. Change the Cloud Owner of the Professional Site to an Organization Administrator.
2. Log in to the Nx Cloud Portal as an Organization Administrator.
3. Navigate to the Professional Edition Site that will be upgraded to Enterprise Edition.
4. Select the **Settings** tab in heading menu.
5. Select the **General** tab under the *System Administration* heading on the left.
6. Click the **Upgrade to Enterprise** button found just below the Site name.
7. Review the summary of benefits and support options; click **Next**.
8. Select an Organization to join from the list provided; click **Next**.
9. Accept the transfer terms by clicking the **Transfer** button.
10. A confirmation screen will be presented after successful transfer.





Merging Sites

Merging Sites can increase operational efficiency by placing servers, devices, archives, and users within a single entity (server hive) so an operator does not need to connect to multiple, isolated sites to perform tasks or repeat the same task in multiple Sites. Merging Sites can also increase the device fail-over capacity and improve connectivity by providing additional proxy options.

Key Concepts:

- Site mergers are initiated from the primary Site.
- The Merge process cannot be undone once completed.
- Site backups are automatically created before the merge process begins.
- The following types of Sites can be merged:
  - Local Site to a local Site.
  - Local Site to a cloud Site, when cloud is the primary site.
  - Local Site to a organization – the local site inherits settings from the organization.
  - Cloud Site to a cloud Site when the merger is initiated by the Site owner from within the Cloud Portal.
- The following types of Sites mergers are forbidden:
  - An organization Site and a cloud Site.

- An organization Site and a organization Site.
- Sites that have one or more pending servers cannot be merged.
- Sites that have any Servers using the same Server ID cannot be merged

- Nx Witness will perform a merge assessment after the secondary Site is specified.
  - Merge can continue when only warnings are identified.
  - Merge cannot continue when errors are identified.
- Depending on the size of each Site, a merge can take a few minutes or multiple hours to complete.
- After a successful the merge, all servers, devices, users, archived data, bookmarks, and event rules from both Sites will be available.

The following table provides a summary of the types of Site mergers that are available. It may be required to disconnect a Site from an existing Cloud account or Organization before it can be merged with a different Site or Organization. Cloud to cloud mergers must be done from within the Nx Cloud portal.

		Primary Site Type		
		Local	**Cloud**	**Organization**
Secondary Site Type	**Local**	Yes	Yes	Yes
	Cloud	No	Yes	No
	Organization	No	No	No

To Merge Local Sites

Desktop Client

1. Launch Nx Witness Client and connect to any Server in the Primary Site.
2. Right-click on the Site name in the Resource Panel and choose **Merge Sites** from the context menu.
3. In the *Merge Sites* dialog, enter the URL of the secondary server to be merged (any Server in the Secondary Site, or a remote server) in the **Server URL** field. Use the drop-down menu to find Sites in the local network. For a remote server, enter `http://<ip>:<port>`, where:
   - `<ip>` – IP address of Server (the current computer should be able to connect to this server)
   - `<port>` – network port of Server (default `7001`).
4. Enter the **Password** to the Secondary Site (or the remote server) and click **Check** to validate that a merger is possible

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 using the following syntax: `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 information for the secondary Site and click **Find Site)** then click **Next**.
   - Secondary Site URL (<server_ip>:<server_port>).
   - Secondary Site administrator Login/Password.
5. Fill in the Current Password (for this Site) field.
6. Select which Site's name and administrator password will be kept.
7. Click **Merge Sites**.

NOTE: Nx Witness creates a Site database backup automatically before merging Sites. See "Backing up and Restoring the Site Database".

To Merge Cloud Sites

Cloud Portal

1. Open Nx Cloud.
2. Click on the primary Site where the merge process will be initiated; this will open the Site's page.
3. Click on **Merge with Another Site**.
4. Choose the secondary Site to merge with from the drop-down menu.
5. Select which Site's name and settings will be kept and click **Next**.
6. Enter the Cloud account password and click **Merge Sites**.

Desktop Client and Web Admin

See "To merge Local Sites" at the top of this page.

Services and Licenses

Nx Witness allows users to create layouts displaying live video feeds and perform Site configuration tasks immediately after installation. Some advanced features related to recording, archiving and analyzing video require either a License Key or a Subscription Service.

The highlights listed below outline the primary differences between the Licensing and Services model to assist with planning and preparation for Site migration. Please contact your customer service team for more information.

Subscription Service Model

- Services are pooled within an Organization and easily moved between devices within the same Organization.
- Each Recording License is converted into 24 months of local recording service when a Site connects to an Organization.
- Organization wide reports show overall Services usage and Services changes over time.
- The total number of available Services can quickly adjusted to match the needs of a changing Site configuration.

License Model

- Each installation comes with four free, 30-day license keys to record video.
- License keys are activated and linked to Servers using unique hardware identifiers.
- Keys must be activated over the internet or by using an off-line, email based activation service.
- It is possible for License Keys to become invalid when the linked hardware is offline; these can be recovered.
- License keys are considered in use when assigned to a Server, even if the function enabled by the license is not active.

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.

Nx Witness Services

The Enterprise Edition of Nx Witness provides a suite of subscription services, include the the recording of a device stream.

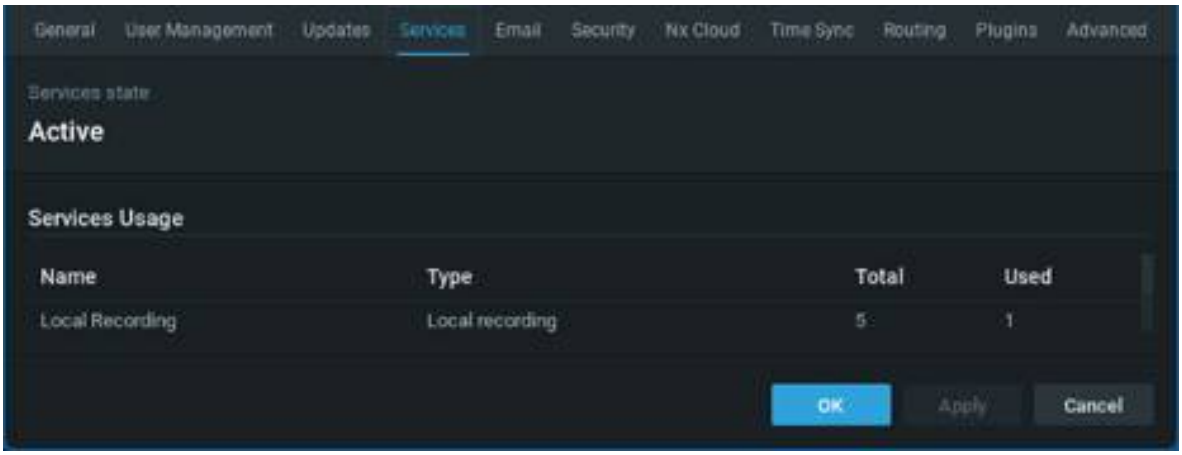
The following conditions must be set before a Site can use available Services:

1. The Site must support Subscription Services by joining an Enterprise Edition Organization. See "Connecting a Site to an Organization".
2. There must be Services available to the Site.

One Recording Services is marked as in-use for each camera where recording is enabled. See "Recording".

Sites that are connected to an Organization have a tab labeled *Services* within the **Site Administration** dialog. This tab displays the state of the Services, the names of available Services, and a count of total and used Services for each Service type.

NOTE:Remove Services from Site devices before an Organization Administrator or Channel Partner reduces the amount of total available Services to prevent the Site from auto-selecting the devices that have Services removed.



Services provided to an Organization can be set to the following states:

State	Functional Description
Active	This is the fully operational State for Sites in an Organization. All users can access their Sites via the Cloud Portal, the Desktop Client, and the Web Admin (when on the same local network as the Site). Recording Services are running as configured within the Camera Settings.
Suspended	Limits access to Sites while keeping all Services running. User access via the Cloud Portal is not permitted. Only the Desktop Client or Web Admin interface can be used to access Sites over the local network.
Shutdown	Stops all Services and disables all Cloud Portal access. Site can only be access by using the Desktop Client or Web Admin (when on the same local network as the Site).

Nx Witness Licenses

The Professional Edition of Nx Witness uses perpetual License Keys to provides a suite of services, include on that enables the recording of a device stream.

One License is required to record video from a device – One License enables one video stream from an IP camera, an RTSP stream, or an HTTP link to be recorded, therefore one Recording License is needed per Camera.

License Types

- A Free License is a no cost, time based license which expires after a certain length of time.
- A Professional License will not expire.
- I/O Modules require a specific type of license. See "Setting Up I/O Modules".
- A specific type of license is also required for Video Walls. Each license allows a Video Wall to be extended to 2 monitors. For instance, 4 licenses allow a Video Wall to be displayed on 8 monitors. See "Video Wall Management".

A specific *Bridge* license may be required to view video streams from Hanwha NVRs. See "Working with NVRs".

Licenses and Hardware ID

Every Nx Witness license, when activated, is locked to the hardware ID of the computing device upon which it is installed. The hardware ID is a unique 34-digit identifier generated when the Server is installed on a Windows, Ubuntu Linux, or ARM device. The hardware ID is based on the following:

- Motherboard
- MAC Address

After installing Nx Witness on a server, any modification in the components above will result in a change to the hardware ID and invalidation of licenses attached to that device (see "Expired and Invalid License Keys").

To Determine Hardware ID

1. In the Nx Witness Desktop client, open **Main Menu** > **Site Administration**.
2. Go to the **License** tab.
3. Select a license attached to the Server for which you want to see the hardware ID.
4. Click the **Details** button.
5. The *License Details* dialog that opens will display the *License Type*, *License Key*, *Hardware ID,* and the number of archived streams allowed on that device.
6. To copy the license information press the **Copy to Clipboard** button.

NOTE: Mobile and Server Web Admins do not have the ability to locate licensing information.

The following sections describe how to obtain, activate, and deactivate licenses:

- Obtaining and Activating Licenses
- Expired and Invalid License Keys

1.5.6.2.1 Obtaining and Activating Licenses

Nx Witness comes with four trial licenses. A trial license is active for 30 days.

NOTE: Licenses for Servers in a multiple Server Site are activated on the Server to which the client is currently connected. If this Server is offline, those licenses will be invalid until the Server is back online.

NOTE: Licenses that are activated on different servers will be combined if the servers are merged into a single Site.

To Activate a Free License

To get additional licenses, contact your local Nx Witness reseller or Network Optix customer service.

Desktop Client

1. Open **Main Menu** > **Site Administration** and go to the **Licenses** tab.
2. Click **Activate Free License**.

Web Admin / *Cloud Portal*

1. Open **Settings** > **Licenses.**
2. Click **Activate Free License.**

NOTE: You will be warned when a Free License is about to expire.

To Activate a License over the Internet

The server the client is connected to (as indicated by the current server  icon in the Resource Panel) will have the license key bound to it. If it is necessary to activate the license key on a different server, disconnect and connect to a desired one. If Nx Witness is not connected to the Internet, then licenses can be activated offline.

Desktop Client

1. Select the **Licenses** tab in **Site Administration**.
2. Go to the **Internet Activation** tab.
3. Enter or paste in the License Key value and click **Activate License**.

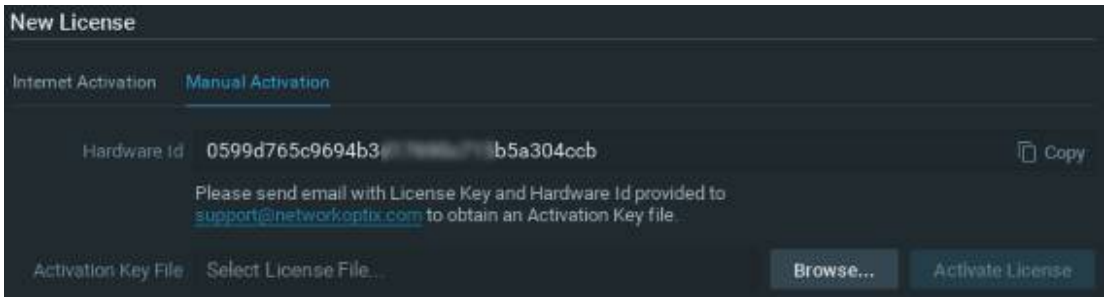
Web Admin / *Cloud Portal*

1. Open **Settings** > **Licenses**.
2. Enter or paste in the *License Key* value and click **License.**

To Activate a License (Trial or Commercial) Offline

In situations where an Nx Witness Site is installed on a device that does not have Internet access, users will be required to perform an Offline (or Manual) license activation. Launch the Nx Witness Client and connect to the Server on which you wish to do an Offline (manual) Activation. The Nx Witness Desktop Client is required – mobile or Web Admins do not have the ability to locate licensing information.

1. Go to **Licenses** tab in **Site Administration**.
2. Go to **Manual Activation** tab.



3. Press the **Copy** button to copy the hardware ID.
4. Email Network Optix customer service to request an activation key, include the Hardware ID and License Key you received in the Email.
5. As soon as you receive the activation key, click **Browse** to import it to the target computer.

To Export a List of License Keys

It is possible to export a list of license keys to a .CSV or .HTML format file. It may be necessary, for instance, if re-activation is needed. To do so, click on *Export* (near the upper right corner) and select the target file.

Nx Witness allows for license deactivation as well. See "Expired and Invalid License Keys".

NOTE: When recording is enabled for a device, the license is considered in use even if the device is not currently recording (as indicated by the empty circle ○ icon to the left of device in the Resource Panel).

Insufficient Licenses Available

An error message or information banner will be presented when there are insufficient licenses to support the selected configuration.

1.5.6.2.2 Expired and Invalid License Keys

Under some circumstances, a license may become invalid. For instance, when a Server is removed from the Site or goes offline, the licenses tied to the hardware ID of that Server will become invalid. When the Server is back online or reconnected to the Site, the licenses will be active again without configuration.

However, if a server change results in a hardware ID update, all licenses tied to the previous hardware ID will become invalid and can only be activated on the new hardware ID by contacting support. If a hardware change is planned, the best approach is to contact support prior to the update so licenses can be intentionally deactivated before the hardware change, while they are still active and valid, and reactivated once the new hardware ID is established.

NOTE: A trial license cannot be deactivated nor reactivated once it expires.

Under certain conditions, such as when a recording license is invalidated, or when a Server fails in a failover-enabled Site (see Configuring Failover), a 30-day grace period is granted to prevent gaps in recording and allow you enough time to resolve the Server or license issue. Once the original Server comes back online, or the license issue has been resolved, the recording will continue normally with the original license(s).

Similar functionality exists for Video Wall licenses, where a seven day grace period is granted to prevent any interruptions in the Video Wall and allow you enough time to resolve the license issue (see Video Wall Mode).

To Deactivate a License

Users can deactivate and move a license a maximum of 3 times. The operation must be performed from the Desktop Client and requires an active Internet connection in order to execute. Trial licenses cannot be deactivated.

1. Go to **Licenses** tab in **Site Administration**.
2. Select a license, click **Deactivate** and confirm the action in the dialog that opens.
3. Enter your name, Email address, and select the reason for deactivation from drop-down list to confirm and explain the action.

It will now be possible to activate this license key on another computer.

To Remove a License

If you are absolutely certain a license is no longer needed, it is possible to remove it. Only invalid (red) licenses can be removed.

1. Go to **Licenses** tab in **Site Administration**.
2. Select the license you want to remove and click the **Remove** button.

Secure Connections

Nx Witness includes many protections for network communications over both secure (e.g. LAN/WAN/VPN) and unsecure (e.g. Internet) networks:

- Authorized Certificate on Server.
- Secure Connections to Cameras over HTTPS.
- Secure Connections between Client and Server.
- Video Traffic Encryption.
- Archive Encryption.

The basic security configuration can be done at the Initial Site Configuration stage. Click **Advanced Site settings** and choose **Security Level**:

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.

NOTE: The Security Level cannot be changed after the initial configuration is set.

Authorized Certificates

By default, the Nx Witness server is installed with a generated self-signed certificate which has the lowest security level. If you use this certificate and use a web browser to connect to the Server through HTTPS, a warning message will appear stating that the connection to the site is not secure (see "Server Certificate Validation"). This means that using the self-signed certificate is not recommended, even though a secure connection is used. It is therefore recommended to obtain a certificate from an authorized certificate provider and install it on the Server that is used for public access (from outside of the local network).

To Obtain and Install an Authorized Certificate

1. Obtain a certificate from any certificate provider (for instance, see the list of top ones here: https://www.techradar.com/news/best-ssl-certificate-provider).
2. Create a file **cert.pem** with the Private Key and Entire Trust Chain (see the instructions on the certificate provider's web site).
3. Place the **cert.pem** file in the following folder:
   - Windows: `C:\Windows\Site32\config\systemprofile\AppData\Local\Network Optix\Network Optix Media Server\ssl`
   - Linux: /opt/networkoptix/mediaserver/var/ssl
4. Restart the server.

For Servers within the local network it is recommended to install the Self-Signed SSL certificate into the Trusted Root Certificate Authorities Store (https://specopssoft.com/support-docs/specops-password-reset/reference-material/installing-the-self-signed-ssl-certificate-into-the-trusted-root-certificate-authorities-store/).

To View A Server's Security Certificate

1. Right-click on a Server and select **Server Settings**.
2. Find the *Certificate* field and click on the **Nx Witness** hyperlink.
3. A dialog displaying the following information about the SSL certificate will appear:
   - Certificate signer (e.g. Self or Trusted CA)
   - Fingerprints
   - Certificate data

- Expiration date

To Set Server Certificate Validation

This option prevents the Desktop Client from connecting to untrusted servers (the ones not having a valid certificate). This is set individually for each instance of the Desktop Client.

1. Open **Main Menu** > **Local Settings** > **Advanced** tab.
2. Click on the **Server certificate validation** drop-down menu and choose one of the following options:
   - *Disabled* – Any certificate is allowed. No warnings are displayed.

   NOTE: This may lead to privacy issues.
   - *Recommended* – Your confirmation will be requested to pin self-signed certificates.
   - *Strict* – Only trusted certificates are allowed (i.e. no self-signed certificates).
3. Apply changes.

To Get Notifed about Certificate Validation Issues

If a certificate is invalid, the "Server Certificate Error" event is triggered.

Cameras over HTTPS Only

This setting will ensure the server only connects to cameras using HTTPS, preventing management traffic between the camera and Server from being intercepted and analyzed.

To Connect to Cameras over Only HTTPS

1. Open **Main Menu > Site Administration > Security** tab.
2. Check the **Use only HTTPS to connect to cameras** checkbox.
3. Apply changes.

NOTE: Any cameras on the Site that do not support HTTPS will appear offline.

Forcing Secure Connections

Forcing secure connections ensures clients only connect to servers in the Site using HTTPS to prevent management traffic (users accounts, device access credentials, Web Admin packets) from being intercepted.

This setting is enabled by default.

To Force Secure Connections

Desktop Client

1. Open **Main Menu** > **Site Administration** > **Security** tab.
2. Check the **Force servers to accept only encrypted connections** checkbox.
3. Apply changes.

Web Admin / *Cloud Portal*

1. Open **Settings** > **Site Administration** > **General**.
2. Check the **Allow only secure connections** checkbox.
3. Apply changes.

NOTE: This setting is turned on by default and will affect the following:

- Generic Events with external connections should be reconfigured and validated.
- All integrations configured to work with HTTP need to be updated and tested.
- API calls – all external connections that use API for integrations should be re-configured to use HTTPS and then tested.

Once HTTPS is enabled, the first time you attempt to log onto a server's web page, the browser may first display warnings that indicate a bad certificate and insecure connection ("Your connection is not private. Attackers might be trying to steal your information..."). This is not the case. The warning is a safety feature due to the self-signed certificate on the Server. The connection will in fact be more secure.

NOTE: Most browsers will generate a prompt or confirmation dialog to proceed using an HTTPS connection. While the specific text will vary by browser version, a common sequence it to click on the word **Advanced**, then click the **Proceed** to [xxx.x.x.x] (unsafe) link to log in. Local machine and application define when this authorization must be repeated.

Enabling Encrypted Video Traffic

This setting prevents video streams (live and playback) from being intercepted and viewed by third parties. This option is only available on Sites that are configured to use Secure Connections.

To Enable Encrypted Video Traffic (Only Available If Site Is Configured to Use Secure Connections)

Desktop Client

1. Open **Main Menu** > **Site Administration** > **Security** tab.
2. Check the **Encrypt video traffic to desktop and mobile clients** checkbox.
3. Apply changes.

Web Admin / Cloud Portal

1. Open **Settings** > **Site Administration** > **General**.
2. Check the **Encrypt video traffic to desktop and mobile clients** checkbox.
3. Apply changes.

NOTE: Encrypting video traffic can significantly increase CPU usage of the Media Server.

Enabling Archive Encryption

By default, Nx Witness stores recorded video without any access controls and it can be viewed by anyone with access to the files.

Enabling archive encryption will prevent the recorded archive from being viewed outside of a Nx Witness client.

To Enable Archive Encryption

1. Open **Main Menu** > **Site Administration** > **Security** tab.
2. Toggle the **Archive encryption** switch.
3. Set a password to encrypt the archive. The encryption password will be required to restore the archive on another Site but will not be required to enter the encryption password to view the video archive within the Site.

NOTE: Do not lose this password as it cannot be reset and the the archive cannot be accessed or recovered with the password.

Server Settings

In addition to the settings that are entered during initial configuration, Administrators can also view and edit these other server parameters.

See the following topics for advanced information concerning Nx Witness storage behavior:

- Archive Distribution and Retention
- Archive Indexing
- Archive Reindex and Scan
- Archive Backup

To configure server parameters, select the desired server in the Resource Panel, open its context menu, and choose **Server Settings**.

General tab

- *Name* – Server can be renamed here or in the Resource Panel
- *IP Address* – cannot be changed (IP address display in the Resource Panel can be turned on or off using the Show additional info in tree flag).
- *Ping* – click to open a terminal window and ping the server.
- *Port* – this value is display only but can be changed from the Web Admin.
- *Certificate* – Name of certificate is displayed; click to display further details.

Server Hardware Option

- *Autodetect USB and web cameras* – if enabled, Nx Witness automatically discovers built-in and USB webcams.
- *Remote Access* - this section displays currently configure remote access services.
- *Server Web Page* – provides a path to Connect with the Web Admin interface.

Storage Management tab

- *Storage Locations* – add and configure main, external and backup storage locations (see "Configuring Server and NAS Storage, Configuring Backup and Redundant Storage and Configuring Analytics Storage").
- *Reindex Archive* or *Reindex Backup* – restores recorded footage if it is moved (see "Reindexing and Fast-Scanning Archives").

NOTE: Displayed statistics will refresh periodically – a manual Refresh button is also provided along the right side of the header menu.

Storage Analytics tab

- To view detailed storage statistics (see "Analyzing and Predicting Storage Usage").

Backup tab

- Backup duplicates the footage in an archive and saves it to other available locations (see "Configuring Backup and Redundant Storage").

Failover tab

- Properly set failover allows a Server to automatically discover and attach cameras from a failed Server (see "Configuring Failover").

Archive Management

In addition to the settings that are entered during initial configuration, Administrators can also view and edit these other server parameters.

See the following topics for advanced information concerning Nx Witness storage behavior:

- Archive Distribution and Retention
- Archive Indexing
- Archive Reindex and Scan
- Archive Backup

To configure server parameters, select the desired server in the Resource Panel, open its context menu, and choose **Server Settings**.

Archive Distribution and Retention

Video from a camera is always written to the Server to which the camera is connected. Cameras can be moved between servers but the recorded video stays where it was and never moves with the camera. New video is written on the new server. Recorded video is called *archive***.**

If a server has multiple drives, video archive is divided between them in order to improve reliability and balance the load on each drive. Nevertheless, even when different parts of the archive are stored on different drives or on different servers, video playback is seamless.

Other data is storage space occupied by data that isn't from the VMS, this storage space is never recorded on. In addition, 10% capacity is *reserved space* that will not be used for recording.

Available Space

The remaining disk storage is considered *available space* – whether it is currently recorded on or is currently free space. Archive is recorded according to available space.

If there is no free space on a given storage device, the Site will automatically delete outdated recordings in order to free space for new archive. By default the oldest archive is deleted first. However, there are two special properties a given camera can be granted that affect archive retention. One prevents archive from being deleted before a certain number of days has elapsed. The other requires that archive be deleted after a certain number of days has elapsed. These are the only cases in which the Site will actively determine storage deletion.

Schematically, storage life cycle can be illustrated like this:

Storing Archive on Multiple Drives

Servers can have any number of storage devices. Recording to some can be disabled manually, or automatically when they are too small or are the main OS partition. USB drives are disabled by default, but can be enabled manually (though for ARM devices they can be enabled by default).

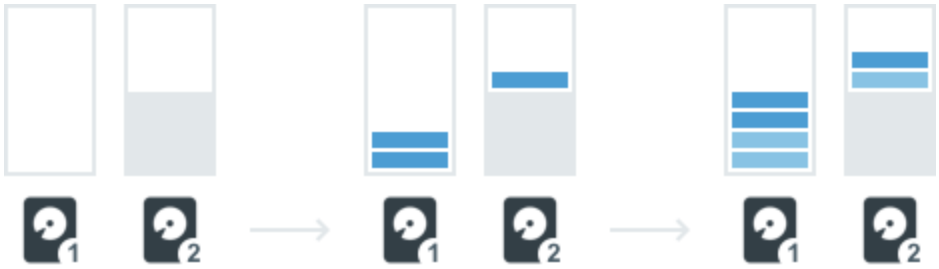
Enabled drives can be one of two types – *main* or *backup* type. Main storage is used to record archive, backup is used to store extra copies of some recordings. At any given moment, a drive can be assigned only one type, but because it is possible to change a drive's type, it is therefore possible to have different types of recording (main and backup) on one drive.

If there are multiple storage locations of the same type (main or backup) on a server, recorded archive will be split between them in proportion to their available space, as shown below:

NOTE: When there are multiple storage locations of the same type on a Server, recorded Archive is distributed separately by type in proportion to the available space for each type.

Write **bitrate** (the amount of data that is processed per unit of time) will correlate with the amount of the available space – in the illustration above disk 1 will have a higher bitrate than the others.

Remember that the distribution of recorded data is dependent on the amount of the available space, not free space. If you have two similar drives, but part of drive #2 is occupied by some other data, recording speed will be higher for the drive #1 because the amount of available space for this drive is higher. Also, because archive recorded by the Site does not reduce the amount of available space, recording speed doesn't depend on how much available space is currently used.



For example, you have two similar drives, and both are already full. You add a third drive with the same amount of available space as the first two but completely empty. Distribution of recorded data is dependent on the amount of available space, so new recordings will be distributed evenly between all three drives. Even though there is plenty of free space on the third drive, outdated footage on the first two drives will be deleted to free up space for new recordings – archive must to be split evenly between all three drives because they have the same amount of the available space.

This is done to balance drive usage and to avoid a situation where all cameras are being written to one drive, which might not have enough speed to record such an amount of data.

Servers Sharing the Same Drive

It is possible to set up recording from multiple servers to the same drive. However, it is very important to split the drive into different partitions and attach separate partitions to each Server so that archive written by one Server cannot be deleted by another.

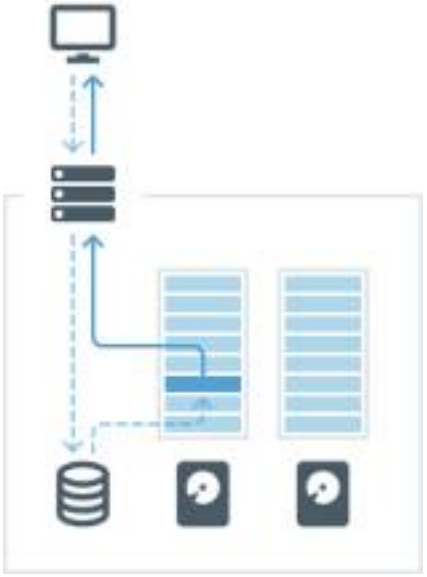
If you add one partition to multiple servers, they both will treat free space on that drive as available and will use it for recording. Data recorded by one Server will be considered “other data” by the other server, and will reduce the amount of available space but will not be overwritten. However, if multiple servers use the same folder and the archive for any one of them is reindexed (see "Reindexing Archive") archive footage from the other servers can be deleted.

If different servers have different recording speeds, it will lead to a situation where storage is divided unequally. After storage is filled with archive, each Server will manage only the space that is occupied by its own data, as shown in the diagram below.

Archive Indexing

The *archive index* is a special database that stores mapping information for video archive. This database includes which cameras are archived, for which times, and in which chunks exactly the archive is stored. *Chunks* are the building blocks of video storage, see "To find archive on a storage device".

The client application pulls storage chunks to the Timeline based on the information in the archive index database. When you click on the Timeline to play a given recorded segment, the client sends the Server a request for that video. The Server checks the archive index to determine where video for that particular moment is stored – on which drive and in which exact chunks. The Server reads that particular video and sends it to the client to display.



– Client

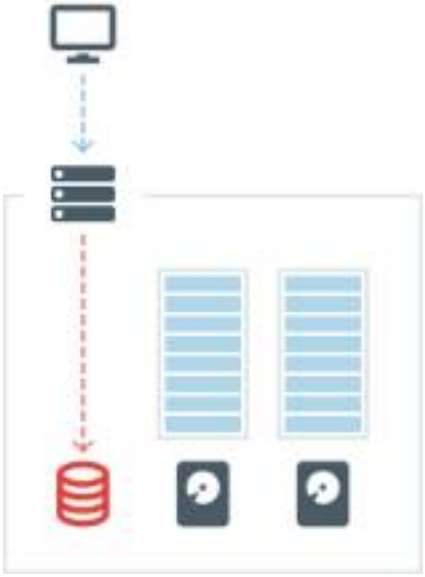
– Server

– Archive Index database

– Storage disk

There can be situations when information in the archive index doesn't reflect the actual video archive. For example, if archive has been deleted or manually relocated, the information about that archive will still be in the index database, but the Server will not be able to read such archive because it is no longer where the archive index last found it.

Similarly, sometimes there is no information in the archive index about archive that does exist in storage. This can happen if the index database file is corrupted or deleted, or when archive video is added to a storage location manually.



These problem can be fixed by *archive reindexing*. During this process, the Server will scan all recordings on all drives and update the archive index database with the current information. Archive reindexing is initiated from the Storage Management dialog for each server, and can be performed for main or backup storage locations (see "Reindexing and Fast-Scanning Archives").

Archive Reindex and Scan

A Nx Witness server creates a database that stores an index mapping the relationship between archive filenames and the physical location of the archive files on the storage drive. When an archive is damaged, administrators will receive a notification when attempting to view that archive. The notification indicates the storage path where the problem was detected.

NOTE: Archives can be saved to one or more backup storage locations to protect against the possibility of complete loss or removal.

The re-index procedure restores the relationship between the database and archive files. This process can take up to several hours, depending on the size of the archive. The Site can still be used during this process and will continue recording while the archive is running the re-index process, as long as the storage drive has enough capacity to do both simultaneously (performance may be affected).

The following events that damage an index:

- A camera is deleted.
- A storage device is moved, renamed, or deleted.
- An archive file is removed, renamed, has an incorrect timestamp, or is otherwise corrupted.

To Reindex an Archive:

1. Do one of the following:

- *Desktop Client:* Right-click on a Server in the Resource Panel, choose **Server Settings** and go to the **Storage Management** tab.
- *Web Admin* / *Cloud Portal:* Open **Settings** > **Servers** and select a server.

2. Click on **Reindex Archive** to restore the index for all Main storage locations. Click **Reindex Backup** to restore the index for all Backup storage locations.
3. A message will open with the warning "**Hard disk load will increase significantly**". Depending on the size of the archive, a full re-index can take several hours to complete. The Site will continue recording while the archive is running the re-index process, but performance may be affected.
4. Click **OK** to continue. When the window closes, reindexing will to run in background. A progress bar will indicate status, and you will see a message when reindexing is either complete or has been canceled.

   NOTE: Reindexing can be canceled at any point, which will trigger the "Reindexing Archive Canceled" event. However, an incompletely indexed archive may be partially or entirely inaccessible. **It is strongly recommended that the archive reindex process be completed**.
5. When reindexing is complete, a "Reindexing Archive Complete" event is triggered.

   To protect against the possibility of complete loss or removal, archives can be saved to one or more backup storage locations. See "Configuring Backup and Redundant Storage".

Fast Archive Scan:

A fast archive scan checks to see that the database is intact and matches the archive. This process usually only takes a few seconds and occurs automatically when the Server is initially started or restarted at any point afterward, an archive file closed improperly, or the index files cannot be read. During a fast archive scan, recording will be put on hold and resume after the process is complete.

There are a few situations where a fast archive scan may take much longer than anticipated, such as when there is an extremely large archive, the Server database was moved while the Server was offline, or an archive from another Server was transferred over to this Server prior to its initial launch.

Archive Backup

Some disks on a Server can be designated as *backup storage*. They will store a copy of the archives recorded to the main storage on the same server.

NOTE: Only archives from main storage of a given Server will be backed up. If there is archive on some other Server you want to backup, you should configure backup storage for that Server as well.

With Backups enabled, the bandwidth restrictions can be configured in three ways: *No Limit*, *Schedule*, or *Fixed* (see "Configuring Backup and Redundant Storage" for details).

Because large amounts of data are being copied during backup, it is possible to set bandwidth limitations or to schedule regular backups at specific times (i.e. *schedule*), to minimize the negative impact of loading the network.

With the *No Limit* bandwidth option enabled, existing archive will be backed up. Afterward, live streams will be continuously recorded in backup storage.

Outdated archive is deleted from backup drives in the same way as from main ones, but independently of the main storage. In other words, if the backup storage has higher capacity, the maximum archive age on it will also be greater.

The opposite is also true – if backup storage is smaller, archive age will be less.

In order to save storage space, a Site can be configured to backup only archive from certain cameras or only certain streams (see Configuring Backup and Redundant Storage for details). Camera recording is backed up only if the camera is selected in backup settings and backup storage is configured on the Server that camera is currently connected to.

Server Storage Configurations

The following topic cover available storage options and configurations.

- Server Attached and NAS Storage
- Configuring Analytics Storage
- Backup and Redundant Storage
- Predict and Analyze Storage Usage

Server Attached and NAS Storage

Each server can use an unlimited number of local, non-local (network), and cloud storage solutions. The server will automatically balance space and consumption across drives when more than one storage location is available (see "Background: Archive Distribution and Retention").

> **NOTE**: USB storage is not enabled by default. Nx Witness will show a warning when a user is attempting to record to a USB device; USB devices can only be used for archive data.

Each server writes to its own sub-directory, using a unique GUID in the storage, and every storage location (devices or folder) has a configurable read-write policy.

Storage Considerations:

- Each local hard disk partition is considered a possible, least preferred, storage location.
- It is recommended to NOT use a primary drive for any archive, index, or analytical data storage – Use an independent partition on a separate physical drive for best results.
- A local drive with a single partition containing an operating environment can be used for recording.
- Nx Witness does not allow recording to drives that are less than 10% the size of the largest drive in the system.
- 10% of available space is reserved on each storage location.
- Storage locations must be detected by the operating environment and be available to Nx Witness applications.
- Storage device activity levels (read, write, scan, clear) are directly related to storage availability, as less capacity generates more frequent reuse of a smaller space.
- Cloud storage can only be used as a backup location.

- When local storage is added to a server, and an extended partition is created with 5 times the storage capacity than the primary storage, or if the total sum of available (non-primary) storage capacity is **5 times** that of the primary storage, the primary partition will be disabled for recording and Nx Witness will record data to the extended partition(s).
- If a primary partition is used, the "Local storage is used for analytic and motion data (Site)" event will be triggered.
- Example storage scenario:
  - Camera A in Site A records in Folder A on a NAS device,
  - Camera B in Site B records in the Folder B on the same NAS.

  The Read-Write policy for this NAS must be Shared or Exclusive. After a manual re-index of the Archive in Site A, Camera B will shown in Site A and similarly, Camera A will be shown in Site B. After that all archive chunks will be updated automatically.

  NOTE: Encrypted archives function the same way as described above.

Data Types Stored:

- **Video Archive**: The recorded audio-video streams provided by a device or camera.
- **Index Data**: Motion, Bookmarks, and proprietary metadata resides at the same drive as the corresponding archive.
- **Analytical Data**: By default, the largest, local, non-primary drive is used for analytical data storage (see "Configuring Analytical Storage").

Read-Write Policies:

1. **Exclusive**: The 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 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 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.

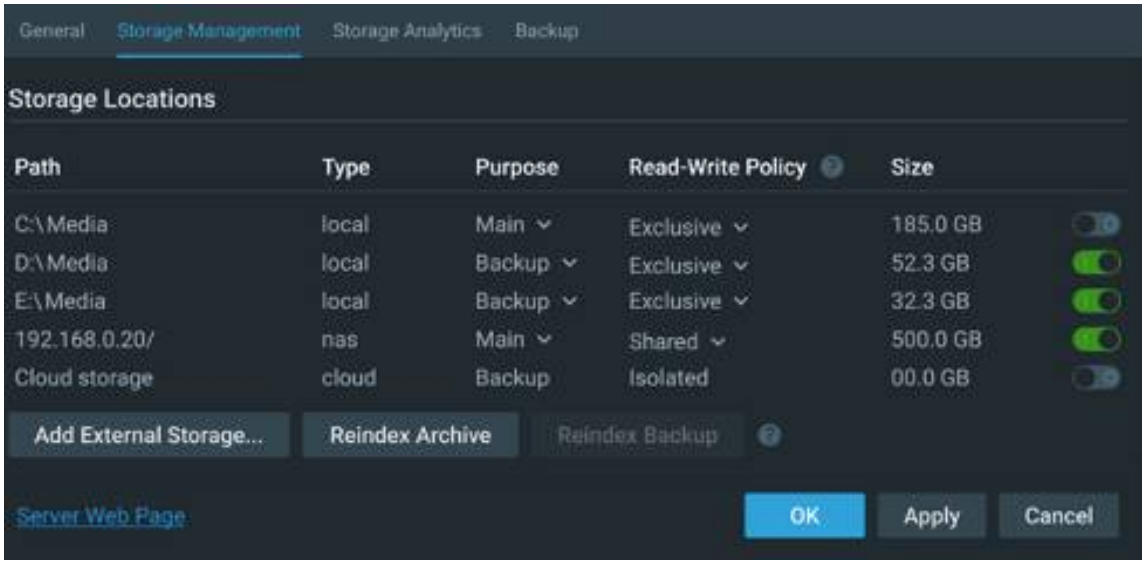
To Configure Server Storage

1. Do one of the following:

- *Desktop Client*: Open the Server context menu and go to **Server Settings > Storage Management** tab.
- Web Admin / Cloud Portal: Open **Settings > Servers** and select a server.

Nx Witness will displays all known and discovered resources available as local storage.

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:
   a. The server has three local partitions (C:, D:, E:).
   b. Disk C (operating system) is currently disabled.
   c. Disk D and Disk E are backup partitions with an exclusive policy.
   d. The NAS is used as main storage using the shared policy.
   e. Cloud storage is an isolated backup location (shown as disabled).



NOTES:

a. There must always be at least one **Main** storage location. Once a main storage location is configured, any other storage location you may have can be set as **Main** or **Backup**.
b. At least one drive must be defined as Backup for archive backup to be possible.
c. Nx Witness will check all storage locations for validity and confirm the ability to write to each. If a drive is not available or has insufficient space, a warning will be displayed.
d. Displayed statistics will refresh periodically and may have a small lag – a manual Refresh button provided in the header menu.
e. Some cameras record directly to their own internal storage, Nx Witness must periodically download archive from the camera's internal storage to Nx Witness servers. See "Remote Archive Synchronization".

f. Recycling bins and similar concepts (Trashboxes, trash bins) **must be disabled** as a part of the configuration step. Nx Witness Server will start overwriting data when the "Reserved Space" limit is reached. To do that, it sends standard SMB-delete requests to the NAS drive. NAS will put files in the bin if the recycle bin is enabled. The Nx Witness Server will not get the necessary space, sending new delete commands instead. Eventually, it will end up with a full drive and the inability to record data until the recycle bin is emptied.

To Add a Network Storage

External storage must use one of the supported storage protocols: CIFS, SMB, NFS, or iSCSI.

NOTE: Make sure NAS is available and accessible through the network on which the computer server is installed.

1. Do one of the following:
   - *Desktop Client:* Open the server's context menu and go to **Server Settings** > **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 it on or off.

To Find Archive on a Storage Device

The storage structure on a partition is as follows:

- *<drive>/HD Witness Media/$GUID/$Resolution/$ID/$YYYY/$MM/$DD/$HH*

where:

- *$GUID* – Unique identifier for the server
- *$Resolution* – can be *hi_quality* (high resolution streams) or *low_quality* (low resolution streams)
- *$ID* – if reported, the MAC address of the recorded device, otherwise the Camera ID
- *$YYYY* – year recorded
- *$MM* – month recorded
- *$DD* – day recorded
- *$HH* – hour recorded

Configuring Analytics Storage

By default, Nx Witness utilizes the largest, non-primary, local storage device analytical data. However, there may be instances where you would prefer to use a different drive for this purpose.

NOTE: Network (CIFS/Samba/NFS) cannot be used for storing analytic data and the Analytics Database cannot be located in a Backup storage location.

Particularly in Sites with a high volume of events, it proves advantageous to employ a faster and dedicated drive specifically for this purpose. For example, SSD, NVMe, and PCIe drives offer significantly faster read/write speeds compared to mechanical HDDs, enabling them to effectively handle the incoming analytic events without performance degration.

Nx Witness enables you to predict the storage usage based on the current data recorded. See "Analyzing and Predicting Storage Usage" for details.

To change the Analytics storage location:

1. Navigate to the Server Settings menu, tab Storage management.
2. Hover with your mouse over the available drives and select Store analytics data.
3. If any data has been recorded to the previous drive, decide to **Delete** or **Keep the current analytics data**.

To Fix the Analytics Storage Database Error

The error “Storage Issue: Analytical storage DB error. Insufficient permissions on the mount point” typically occurs on **Ubuntu** servers when trying to store analytical data on a drive that the Nx Witness Server application is not able to properly access due to having inadequate permissions. Your Server is likely missing the following permissions to the storage drive:

- Read (the capability to read the contents of the file)
- Execute (the capability to execute a file or view the contents of a directory)

Fix the storage issue by enabling the option *forceAnalyticsDbStoragePermissons* in the Nx Witness Web Admin interface. This option grants the Nx Witness Server application the necessary read and execute permissions for that storage drive.

By default, the option is enabled, but it may not be enabled if you have upgraded from a previous version. To enable it manually:

1. Open the Nx Witness Web Admin advanced page (i.e., http://<server ip>:<server port>/#/settings/advanced).
2. Log in to as an Administrator or Power User.
3. Check the box for **forceAnalyticsDbStoragePermissons**.
4. Click the **Save** button at the bottom of the page.

NOTE: If the Server still does not have the appropriate permissions after enabling *forceAnalyticsDbStoragePermissions*, the error "Storage Issue: Analytics storage DB error. Insufficient permissions on the mount point" will still appear in the Notification Panel.

Backup and Redundant Storage

Key Concepts:

- Storage backup duplicates the footage in an archive and saves it to another available location.
- Backup locations can be separate physical drives in the server, network attached storage, or addressable remote locations (FTP).
- The Enterprise Edition of Nx Witness can select a cloud storage service for (video) archive backup.
- Each Server only performs backups from it's own storage archives.
- Every Server in a multiple Server Sites must specify a location to backup footage.
- 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.

Once a backup has been executed, backup archives can still be directly played and accessed via the Client. For example, a Site can be configured to use local storage for 7 days of footage and backup storage for 30 days. If the local storage is backed up once per week then users could still access all backed up video.

NOTE: To configure either backup or redundant storage it is necessary to define at least one main and one backup storage location as described in "Server Attached and NAS Storage".

To Configure Storage Backup

Make sure to backup storage location has been added to the server. Backup settings cannot be changed if a backup storage location is not defined or is not currently attached. A small alert displays under the *Backup Archive* section of **Server Settings** > **Storage Management** if there is no backup storage drive or if no cameras have been selected.

1. Right-click on a Server in the Resource Panel and choose **Server Settings**.
2. Select the **Backup tab** within the **Server Settings** dialog
3. Select the cameras to backup by toggling the switch on the right side. Toggle the **New added devices** option to automatically begin backing up a device once it has been added to the Site.
4. Use the **What to backup** menu to select what aspect of the camera's archive should be backed up:
   - All archive
   - Motion
   - Objects

- Bookmarks
- Motion and Objects
- Motion and Bookmarks
- Objects and Bookmarks
- Motion*, Bookmarks, and Objects*

5. Use the **Quality** menu to select which streams to backup:
   - *All streams*
   - *Low-res*
6. Use **Bandwidth Limit** to set the bandwidth limit for your backups:
   - *No Limit* (redundant) – Footage is written to main and backup location(s) immediately and simultaneously with no bandwidth restriction.
   - *Schedule* – Backup is performed only during the selected days and hours. Fill in the cells of the schedule using the following options: **Unlimited, No backup**, and **Limited to** (limit to a certain Mbit/s, but remember that too tight a bandwidth constraint can cause the entire backup to fail). The footage will be backed up since the last time backup was completed. If network bandwidth is insufficient, the backup may not be fully completed within the specified time frame. In this case the date and time of the footage that was backed up will be clearly indicated (*Archive backup complete until...*).
   - *Fixed* – The bandwidth remains a specified Mbit/s across all days and times.

   NOTE: If *Skip Current Queue* is clicked, the backup process will ignore existing footage and only backup recordings after that point.

After the backup is finished, an internal archive integrity check occurs so that if an archive file is changed or removed, users who are actively viewing that archive will be notified. See "Archive Integrity Check Failure".

To Configure Redundant Storage

With this structure, each Server will back up footage to all other servers in the Site. This will reduce the overall amount of stored footage but provides healthy redundancy.

NOTE: Each Server backs up the archive for selected cameras, but if a camera is moved to a different server, backup will include only the portion archived before the camera was moved.

1. Make sure each Server is available and accessible through the network.
2. On each server, create a shared folder (**\\server\shared**) on a separate HDD to prevent Site malfunction.
3. Make **\\server\shared** accessible through the network with the WRITE permission.
4. Go to **Server Settings** and add all shared folders as NAS devices.
5. Set to **Backup** for each one added.
6. Repeat the above steps on all servers.

7. Configure backup parameters as described above. It is best that servers perform their backup at different times, otherwise recording speed may be too low. When many servers use the same drive for recording it can lead to I/O errors or insufficient write speed.

Predict and Analyze Storage Usage

Due to differing stream bitrates, different cameras may require different amounts of storage space to save data for the same time interval. Nx Witness uses special algorithms to balance storage needs so that cameras with high storage needs do not prevent archive from other cameras from being recorded. Nx Witness storage analytics are available in the Desktop Client to help users estimate and predict storage usage.

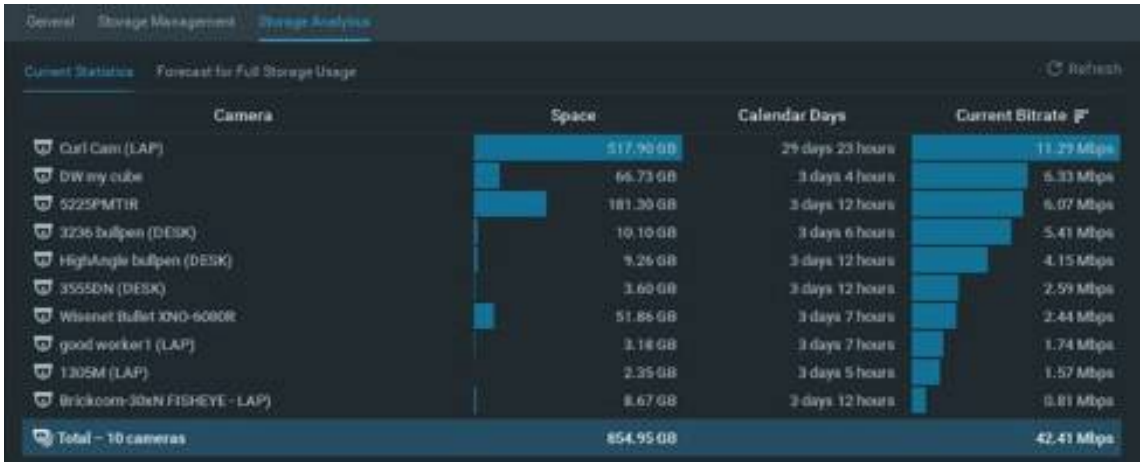
NOTE: For any given camera, Administrators have the option of setting a minimum or maximum number of days that data is archived (see "Configuring Minimum and Maximum Archive Storage").

Some common ways storage analysis can be used:

- Identify camera(s) that stream at extremely high bitrates.
- Estimate the amount of time a Server can store data from a given device in days and hours.
- Assess the storage space that each camera consumes.
- Predict the amount of time a Server can store recordings if additional storage is added.

To View Storage Statistics for a Server

Open **Server Settings** from the Server context menu and go to the **Storage Analytics** tab. The *Current Statistics* tab shows the total number of cameras, total space used for archive and total streaming rate at the bottom of the list, and there is a link to open the Server web page on the lower left corner of the page.



Each of the columns can be sorted in ascending or descending order:

- *Camera* – Camera name.
- *Space* – the amount of storage currently consumed by recordings from a given camera.

- *Calendar Days* – the amount of time recorded data is available for this camera.
- *Current Bitrate* – the current bitrate at which the camera is streaming.

To Predict Storage Needed for a Server

Forecast data is only available for Cameras with recording enabled.

1. Click on the **Forecast for Full Storage Usage** tab in **Server Settings** > **Storage Analytics**. The total number of cameras and total space required for archive is shown at the bottom of the list.
   Each of the columns can be sorted in ascending or descending order:
   - *Camera* – Camera name.
   - *Space* – the amount of storage that will be required.
   - *Calendar Days* – the duration of time that there is for the archive.
2. In the **Base forecast on data recorded during** field, set the window of past history that will be used to calculate future storage needs from the options:
   - *Last 5 minutes.*
   - *Last 60 minutes.*
   - *Last 24 hours.*
   - *Longest period available.*
3. Use the **Additional Storage** field or slider to select an amount of storage that would be added, in Terabytes (TB).

The amount of space and archive duration will update as values in the two settings change.

NOTE: Displayed statistics will periodically refresh – a manual Refresh button is provided along the right side of the header menu.

Monitoring Servers

Nx Witness provides a real time Server Health Monitor display that can be added to layouts, opened in separate tabs or a new window.

Access to Ste Health Monitors is granted to all Built-In Groups. The Built-In Group *Site Health Monitor* is configured to only allow viewing of Site Health Monitors and notifications. Custom Groups can be granted access to Site Health Monitors by using the Permission Resource control or adding the *Site Health Monitor* Group as a member of the Custom Group.

To Monitor Site Health in the Desktop Client

- Click-and-drag the **s**erver from the Resource Panel into a new or existing layout.
- Open the server context menu and choose:
  - **Monitor** will add the server to the current layout.
  - **Monitor in New Tab** will add the server to a new layout.
  - **Monitor in New Window** to open the monitor in new Nx Witness session.

- Multiple Servers can be selected at once by using CTRL+Click to select before opening as previously described.

The following traces are displayed by default and can be toggled off and on by clicking the checkbox in the legend at the bottom of the display:

- CPU load.
- RAM memory usage.
- Hard disk partition usage (for example, C: and D:).
- Network interfaces usage.

The following details can be toggled to always be displayed by clicking the **(i)** icon in the upper right corner of the graph or by opening the graph context menu and selecting **Show on Item > Info**:

- Server name and current up-time since Server was last re/started.
- Percentage of capability being used displayed on the right side.
- Legends and chart color key.

To Monitor Server Health in Web Admin or Cloud Portal

1. Connect to the Server
2. Select **Monitoring** from the header menu
3. Choose to view the *Graph* or *Log*

NOTE: Review the "Health Monitoring" topic for additional options to monitor the performance of Site components.

Using a Server's Web Interface

Nx Witness provides a simple and convenient way to control servers remotely through the server's web interface.

To access a server's web interface from a browser, see "Opening Nx Witness Web Admin".

NOTE: In merged Sites, a Server web page may be inaccessible if it is located on a different network. See Adding a Web Page as an Item for information on accessing such web pages via proxy.

To Access a Server's Web Interface from the Nx Witness Client

1. Right-click on a Server and choose **Server Settings** from the context menu.
2. Click on the **Server Web Page** link on the bottom left of the dialog.
3. The **Server Web Page** can be opened using server's context menu in the Resource Panel.

The menus and settings available in the Web Interface will vary by installation and user permissions:

View:

- See all connected servers and devices.

- View live and recorded video.

NOTE: See "Searching and Filtering in Nx Witness" for information about searching and filtering connected servers and devices.

Settings – Site Administration (General).

- Rename Site.
- Merge Sites.
- Connect to Nx Cloud.
- Allow only secure connections.
- Encrypt video traffic.
- Limit session duration.
- Disable Audit Trail.
- Disable automatic device discovery.
- Preventing Nx Witness from Changing Device Settings.

Settings – Site Administration (Licenses).

- Activate licenses.
- View license information.

Settings – Cameras.

- Select image aspect ratio.
- Select image rotation.
- Enable audio.
- Edit authentication credentials.
- Configure motion detection.

Settings – Users.

- Delete or Remove Users.
- Modify User information (name and Email).
- Change User password.

Settings – Servers.

- Change port.
- Restart Server.
- Restore factory defaults.
- Detach from the Site.
- Choose Main or Backup storage.
- Add external storage.
- Reindex main storage.
- Reindex backup storage.

Information.

- View Health Monitoring information and download a report.

Settings – Footer Links.

- Download Nx Witness.
- API documentation.
- Download SDK.
- Support link.

Session and Digest Authentication

Nx Witness offers different authentication methods for the different aspects of Nx Witness. HTTP Bearer Session authentication is the default option due to its improved security over HTTP Digest authentication. Digest authentication is deprecated in Nx Witness but still usable if enabled on a user-by-user basis.

To Enable HTTP Digest Authentication for a User

1. Launch the Desktop Client.
2. Open Main Menu > **User Management**.
   a. Click **Add User** if adding a new user with Digest Authentication.
      or
   b. Click on an existing user to **Edit** their Digest Authentication setting.
3. Within the user properties dialog, tick the box to **Allow (insecure) digest authentication**.
4. A notification will show when Digest Authentication is enabled for a user.
5. Apply the changes.

NOTESs:

- A warning text will appear in the Security tab (**Main Menu > Site Administration**) stating that Digest Authentication is not secure and the number of users with access to it.
- Username must be lowercase when using Digest Authentication.

Multi-Server Environments

Nx Witness allows many servers to work together, in one or more Sites, for complete scalability.

Servers are identified and merged according to a **localSystemId** value that is assigned to a Server during initial configuration in the Setup Wizard. If "Setup New Site" is selected in the Setup Wizard, a new localSystemId is generated. If "Add to Existing Site" is selected, the localSystemId is taken from the remote Site.

If servers are in different subnets, it is necessary to specify the other server's IP to allow them to merge in separate networks (behind NAT or over the Internet).

When servers are merged, they constantly synchronize all settings so it doesn't matter which Server the client is connected to. If video from a remote Server is requested, the client tries to connect directly to it and if it fails, the current Server will act as a proxy between the client and the Server with the video data.

Licenses are combined as well: if 4 licenses were activated on Server A and 10 licenses were activated on Server B, the Site will have 14 licenses total after the servers are merged.

Based on lab testing results, the maximum recommended scale for a single Site is approximately 10 servers and 1,000 users. However, this will vary significantly depending on specific environmental factors and the equipment in use.

It is recommended to contact the Presales Team for assistance with large-scale deployments and performance optimizations.

The following topics this section describes how to manage multi-Server environments to maintain maximum Site reliability and performance:

- Moving One Server to a Different Site.
- Merging Sites.
- Detaching a Server.
- Configuring Failover.
- Configuring Routing in a Multi-Server Environment.
- Configuring Time Synchronization in a Multi-Server Environment.

Multi-Server Architecture

Each Server has a unique identifier, the "systemid," that allows servers to group together. If a server discovers another server, with the same Site name, in a local network, they will be merged automatically.

If Site names are different, the Sites will be added to the Resource Panel under *Other Sites*.

If servers are in different subnets, it is necessary to specify the other server's IP to allow them to merge in separate networks (behind NAT or over the Internet).

When servers are merged, they constantly synchronize all data so it doesn't matter which server the client is connected to. If a video is requested from a remote server, the one the client is connected to will be proxying the video traffic.

Licenses are shared as well: if 4 licenses were activated on Server A and 10 licenses were activated on Server B, the Site will have 14 licenses total after the servers are merged.

Services are set at the Organization level and can be activated on any (Site) device within the Organization.

NOTE: Nx Witness creates a database backup automatically before merging Sites. See "Backing up and Restoring the Site Database".

Moving Servers Between Sites

Use this action to move a single server to a different Site in the same local network.

NOTE: If it is necessary to join several servers in a different Site to the current one, this method is not an option. Also, this method won't work if the server that should be connected is outside the local network. For these cases use "Merging Sites".

Using the Client to Join a Server

1. Expand **Other Sites** in the *Resource Panel* and locate the destination Site where the Server will be moved to.
2. Expand the desired Site and locate the server that will be moved to the currently connected Site.
3. Open the context menu of the Server you want to move and choose **Merge to Currently Connected Site**.
4. Enter the admin password of the destination Site.

Site Database Backups

You can create a backup of the database of Site settings, User rights and settings, and device configurations, which can be restored in case of failure. If a User creates the backup in the Client, the file is saved as a ***.db** file. Nx Witness creates a database backup automatically every 7 days, whenever the product version is updated, and when Sites are merged (see "Merging Sites"). If the backup is created automatically, the file is saved as a ***.backup** file. More details about backups can be found on the Support Portal.

The Site database does not include archives, Server data, or local settings.

The default database backup location:

- *Windows*

  `C:\Windows\System32\config\systemprofile\AppData\Local\Network Optix\Network Optix Media Server\backup`

- *Linux*

  `/opt/networkoptix/mediaserver/var`

NOTE: It is best to backup and restore the database on the same computer.

To Back up Nx Witness Database

1. Go to **Main Menu** > **Site Administration** > **Advanced.**

2. In the **Backup and Restore** section, click **Create Backup**.
3. In the dialog that opens, choose a file location and enter a file name for the backup.
4. Click **Save**.

To Restore Nx Witness Settings from Backup

1. Go to **Main Menu** > **Site Administration** > **General.**
2. In the *Backup and Restore* section, click **Restore from Backup**.
3. In the dialog that opens, find the desired database backup file (*.db), then click **Open**.
4. Click **OK** in the confirmation dialog to restore the database.

Servers will restart automatically when the Site is restored from backup.

NOTE: It may be necessary to restart Nx Witness clients after restoring a database.

Detaching a Server

This action can be useful if it is necessary to isolate a Server from the current Site. This operation is rarely performed.

NOTE: If licenses have previously been activated on the Server being detached, it will be disabled with the error "Server not found."

To Detach Server from the Site Using a Server's Web Interface

1. Log in to the Web Admin interface of the Server that should be detached from the current Site.
2. Open the **Settings** tab and click **Detach from the Site**.
3. Enter the Server password and confirm the action.

NOTE: All Nx Cloud users including the Cloud Site Owner will be deleted when a Server is unlinked from the Cloud Site. **Only the local administrator and local users will remain.**

To Detach Server from the Site by Restoring a Server's Factory Defaults

1. Log in to the Web Admin interface of the Server to be detached.
2. Go to the **Settings** tab and click **Reset to Defaults.**
3. A confirmation dialog box will displayed and a Server password may be required.

Deleting a Server

In some instances, it may be necessary to delete a server from the Site.

A Server can only be deleted when it is offline. To delete a server, locate it in the Resource Panel, **right-click** to open the context menu and select **Delete**.

NOTE: All devices that are hosted on a deleted Server will be deleted as well. Recorded data will remain in the server's storage.

A Server will automatically discover all devices and start operating once it is back online, and archives from previously attached cameras will remain available. However, storage settings and device configurations are not saved and will have to be re-entered.

Configuring Failover

Automatic failover allows a Server to automatically discover and attach cameras from a failed Server. The failed and the functional Server(s) must be within the same Site. When a Server power, networking failure, or failure to the last remaining storage drives occurs, devices are transferred to the first available failover-enabled Server, and the Client is automatically reconnected.

NOTE: A 30-day grace period is granted to the failover-enabled Server to allow the Cameras to continue recording seamlessly (see Expired and Invalid License Keys).

Failover requires that at least two Servers be enabled. However, to adequately protect a Site, all Servers should be failover-enabled. This is to protect any given Server and because failover success depends on the device capacity of the individual servers.

For example, in a Site with three servers, Server A has maximum capacity of 256 cameras and is actively recording 160 cameras, Server B has a maximum capacity of 256 cameras and is actively recording 128 cameras, and Server C has a maximum capacity of 256 Cameras and is actively recording 176 cameras. Therefore Server A has a failover capacity of 96 devices (256 -160), Server B has a failover capacity of 128 devices (256-128), and Server C has a failover capacity of 80 devices (256-176).

If any one of these Servers were to fail, both the other Servers would be required to capture all of the disconnected devices. For example, a failure of Server A would require space for 160 devices. Server B has failover capacity for 128 devices and Server C has failover capacity for 80 devices, so neither alone would be sufficient ($128 + 80 \geq 160$). Similarly, A (96) plus C (80) are needed for the 128 cameras on B if it were to fail, and A + B are needed for the 176 devices on C ($96 + 128 \geq 176$).

Failover takes approximately 1 minute to complete in the instance of a network or power failure. Archive playback from the failed Server will not function until the Server holding the archive becomes available.

To Configure Failover on a Server

The failover priority setting is a Site-wide option and is synced across all servers in the Site.

1. Right-click on the desired Server in the Resource Panel and choose *Server Settings*.
2. In the *General* tab of the *Server Settings* dialog, enable **Failover**.
3. Enter the maximum number of cameras that can be attached to the Server (256 maximum on Intel/AMD CPUs, 12 maximum on ARM CPUs).
4. Set the **Server Location ID**. By default, this value is 0 for all servers with failover enabled. Servers that share the same Location ID can failover to one another but not to servers

with different Location IDs. This ensures that failover occurs between appropriate servers (for example, you may want to set servers near one another to the same Location ID and severs that are further away to a different Location ID).

5. Click *Apply* or *OK*.
6. Repeat steps 1 – 5 to enable additional failover servers.

To Configure Failover Priority for a Specific Camera

Failover Priority can specify the most important streams that will be transferred first, lower priority devices after that, and inessential devices can be set to not transfer at all.

By default all cameras in a Site are set to "Medium" failover priority. To turn off the failover feature for a given cameras, set it to "Never".

1. In the *General* tab of the *Server Settings* dialog, click **Failover Priority** checkbox.
2. Expand each Server to list the attached cameras and reveal the Failover Priority checkbox. The default setting is medium.
3. Check the desired camera and click one of the buttons – **Never**, **Low**, **Medium**, or **High** – at the bottom to set the desired priority.
4. Repeat steps 2 – 3 for all cameras that should be given a failover priority.
5. Click *OK* to apply changes in the Failover Priority dialog.
6. Click *OK* or *Apply* in the Server Setting dialog.

Routing with Multiple Servers

Nx Witness provides a built-in automatic routing mechanism that enables users to seamlessly work with large sites as a single cluster.

Initially Nx Witness tries to discover all available IP addresses of servers, including public ones. However discovery is not always possible in some network environments. There may be custom network configurations that require custom routing settings. Sometimes servers have several IP addresses (public and private) and it may be necessary to allow or restrict traffic flow for some of them. For instance, a Server can have a public IP address connected to the Internet via 100 Mbit network and a local NIC with local IP address (1Gbit). If it is not necessary to provide public access to this server, it may be useful to restrict traffic flow through the public IP.

To add, enable, and disable routing, open **Main Menu** > **Site Administration** and go to the **Routing** tab.

The left panel displays a list of all connected servers. Click on a Server in this list to show all available interfaces on the right side of the dialog.

- To add an address manually, click the **Add** button and enter a URL using the format http://<ip>:<port>:
  - ***<ip>*** – the desired IP address or DNS name of server.

- ***<port>*** – network port Server is listening on (default **7001**).

- To allow/deny traffic via a specific network interface, click the toggle button for that connection.

Time Synch with Multiple Servers

In large Sites, different components may reside on different locations or even in different time zones. There are a few Site components that the time settings are important for:

- Servers.
- Desktop Clients.
- Cameras.

To Control Time Synchronization between Servers

Some archive potion may become unavailable if the time difference between servers is greater than 10 seconds. Nx Witness can be set to take the current time either from the Internet or from a given server to which all other servers will synchronize.

1. Open **Main Menu** > **Site Administration**.
2. Go to the **Time Sync** tab where the current Site time and configuration information is displayed.
   - To synchronize Site time with the Internet, enable the **Sync time with the Internet** selector. Time cannot be synchronized if there is no Internet connection or if the time Server is offline.
   - To synchronize with local time on a given server, disable the **Sync time with the Internet** toggle and click on the name of the desired server.
   - To allow each Server to use its own local time, choose the **Do not sync time among servers** option (not recommended).
3. Confirm changes.

To Control Time Displayed on Desktop Clients

It is important to configure time in the Desktop Client, if Client and Servers are in different time zones (especially if there are multiple Servers in different time zones).

Desktop Client can display its local time or Server time when browsing the archive, Event Logs, Audit Trail of User Actions, etc.

To specify:

1. Open **Main Menu** > **Local Settings** > **Look and Feel**.
2. In **Time Mode**, choose: *Server Time* or *Client Time.*
3. Confirm changes.

NOTE: This operation should be done on each Desktop Client independently.

For Sites where time is not synchronized, offsets are displayed for both Server time and VMS (Global Site) time.

The time offset is relative to the Server the cursor is hovered over.

For Sites where time is synchronized with a local server, offsets are shown for Server OS time only, relative to the Server OS time on the selected server.

Additionally, it is possible to synchronize time with cameras. However, in some cases it may be necessary. See "Time Synchronization between Servers and Cameras".

Device Management

The following are the most common device types naively are supported in Nx Witness with additional integrations:

- Cameras.
- Encoders.
- DVRs.
- I/O modules.
- NVRs.
- Virtual Cameras.

All connected devices are listed in the Resource Panel and can be accessed, configured and grouped there.

The following settings are required for a device to be able to record:

- Authentication.
- Setting a Recording Schedule.
- Recording Mode.

This section describes the following functions related to devices:

- Viewing Full Device List.
- Adding Cameras and Streams.
- Setting Up Cameras and Devices.
- Accessory Devices.
- Replacing a Camera.
- Diagnosing Offline Devices.
- Working with NVRs.
- Working With Intercoms.

- Image Controls.
- Recording
- Advanced Device Settings
- Camera Plugin Integrations.

NOTE: Most device parameters can only be configured by a Users with the Power User or higher permission level (see "Users and Groups").

Viewing Full Device List

The *Cameras List,* also known as the *Devices List,* provides a view and manage all devices registered in the Nx Witness Site.

To Open the Device List

Open the **Site Administration** dialog and select **Camera List** (**Ctrl**+**M**).

Recording	Name	Vendor	Model	Firmware	IP/Name	MAC address	ID	Server
Continuous	Brickcom-30xN	G-version	Brickcom-30xN	v3.2.3.5.6	192.168.0.168	98-3B-16-4B-AB-F0		Server DESKTOP-DJN3241 (192.168.0.160)
Continuous	IPcameraadmin	IPcamera	admin	V1.04.01-140606	192.168.0.115	00-2A-2A-30-44-7B		Server DESKTOP-DJN3241 (192.168.0.160)
Motion + Low-Res	LR01IPC	LR01	IPC	V0.1.51_H	192.168.0.72	00-B0-FF-C3-92-4F		Server DESKTOP-DJN3241 (192.168.0.160)
Continuous	LR01IPC	LR01	IPC	V0.1.51_H	192.168.0.156	00-86-3D-2D-93-08		Server DESKTOP-DJN3241 (192.168.0.160)
Continuous	IS-DM220	Sentry	IS-DM220	sr20121213NSA	192.168.0.140	00-50-C2-0E-C3-63		Server DESKTOP-DJN3241 (192.168.0.160)
Continuous	AXISM3007	Axis	AXISM3007	lfp-15.30.2	192.168.0.178	AC-CC-8E-19-FB-60		Server DESKTOP-DJN3241 (192.168.0.160)
Motion only	VIVOTEKFD8161	VIVOTEK	FD8161	FD8161-VVTK-0105b	192.168.0.133	00-02-D1-20-DB-51		Server DESKTOP-DJN3241 (192.168.0.160)

- *Recording* – current Recording Mode of the device.
- *Name* – Device name reported by the device.
- *Vendor* – Device manufacturer/maker. When interacting with a 3rd party device via ONVIF protocol, *Onvif Device* is displayed.
- *Model* – *Model* of the device
- *Firmware* – The current firmware version
- *IP/Name* – Device IP address
- *MAC Address* – Device MAC address. If it is not possible to determine the MAC address, a unique identifier is shown (i.e. **`urn_uuid_207f19b2-d5a6-407f-8fec-6265a311058b)`**
- *ID* – 1 to 999999 digits for Logical ID (see "Expert Device Settings").
- *Server* – Server hosting the device

The following controls are available:

- Sort data – Data in each of the columns can be sorted in ascending or descending order by clicking on the header.
- Filter data – Text entered in the *Search* field applies to all data in the list. Results refresh as characters are entered. To disable filtering, clear the field.
- Select data – To select multiple rows use **Ctrl+Click** or **Shift+Click**. Use **Ctrl+A** to select all devices.

The following tools are available from the **Camera List** context menu:

- *Open* – Choose *Open*, *Open in New Tab*, or *Open in New Window*.
- *Delete* – Disconnects the selected device(s) for the Server host.
- *Check Camera Issues* – Opens the "Event Log" for the selected device.
- *Camera Rules* – Opens the "Event Rules List" for the selected device
- *Camera Settings* – Opens the Camera Settings dialog for the chosen device. If multiple cameras are selected before clicking this setting, the dialog that opens will be feature restricted.
- *Select All* – Selects all the cameras in the list
- *Export Selection to File* – Opens the *Export* dialog. Enter a file name and select a format (HTML or CSV text file).
- *Copy Selection to Clipboard* – Copies the column data for each selected camera to clipboard, from which it can be pasted into a text editor or spreadsheet application.

NOTE: A camera can be renamed by opening the Camera Settings dialog for a single device and editing the title.

Device Groups

Devices can be placed in Groups to organize how they are displayed in the Resource Panel, this is very useful for Sites with many devices.

Device Groups:

- Are only used for the visual display and organization of resources within the Desktop Client.
- Cannot be used for device settings or permission management.
- Can be nested 8-levels deep with the same Group name used at each level.
- Cannot have a blank name; the Group name must be at least one character and leading spaces will be removed.
- Do not support a single device being within multiple device groups.
- Only Site Administrators and Power Users can create and modify device groups.

To Create a Device Group:

1. **Right Click** on a device or group in the Resource Panel to open the context menu, or use the hotkey (**CTRL+G**) while a device or Group is selected.
2. Rename the Group or press **Enter** to accept the Site generated name.

To Add or Move Devices Between Groups:

Use drag-and-drop to move the device to the desired group.

To Remove a Device from a Group:

Use drag-and-drop to move the device underneath the Server.

To Delete a Device Group:

Right Click on a group to open the context menu and select **Delete** or use the **DEL** hotkey.

NOTE: Devices are moved up one group level when their current group is deleted.

Adding Cameras and Streams

This section provides information on how to add various devices (cameras, encoders, I/O Modules) to the Nx Witness resource list.

Choose one of the following methods:

- Automatic Device Discovery
- Adding Devices Manually
- Adding Streams as Cameras
- Adding a Webcam or Pi Camera
- Replacing a Camera
- Deleting a Device

See also:

- Setting Up a Virtual Camera
- Setting Up an I/O Module
- Setting Up an Analog Camera
- Device Groups

Automatic Device Discovery

As soon as a server is started and connected to a Site, it automatically performs device discovery in its network for devices that are accessible via broadcast. Once a device is discovered, it is displayed in the Resource Panel.

By default, this feature is turned on. It can be disabled during the Initial Site Configuration or later (see below).

If a device does not transmit media data, it is marked as offline. If a server is offline, all devices the Server is hosting are automatically switched to the offline status.

Some devices require that a password be created or entered upon the first attempted access. They will be displayed in the Resource Panel but an error message will be displayed when an attempt is made to view streams from such devices.

NOTE: For Axis cameras only — if the "People Counter" function is enabled, automatic discovery will not work!

If a device was deleted and connected again, it will be re-discovered. See "Deleting a Device" for details.

NOTE: Once a device is discovered, Nx Witness adjusts the manufacturer's preset image quality settings and streaming configuration for optimal performance in the Nx Witness Site. See "Preventing Nx Witness from Changing Manufacturer Settings" to disable these changes.

If the auto-discovery is turned on, once a device is discovered it cannot be deleted unless physically disconnected from the network. If deleted, it will be discovered and added back automatically.

To avoid that and add only desired devices, you can turn the auto-discovery off.

To Disable Automatic Device Discovery

Desktop Client

1. Open **Main Menu** > **Site Administration** > **General** tab.
2. Uncheck **Enable devices and servers auto discovery** in the *Site Settings* section.
3. When finished, press *OK* to apply or *Cancel* to discard changes.

Web Admin / *Cloud Portal*

1. Open **Settings** > **Site Administration** > **General**.
2. Unheck the **Enable auto discovery of cameras and servers** checkbox.
3. Apply changes.

NOTE: Once auto-discovery is disabled, new devices and servers must be added manually.

Adding Devices Manually

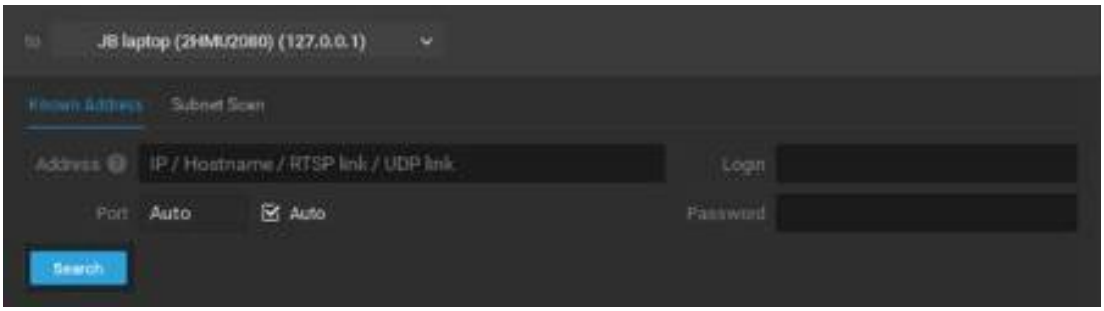
If a device is not accessible via broadcast, for instance if is located in a different network or can only be accessed via internet, it will not be discovered automatically. In this case Nx Witness provides an ability to add a device manually. It is also possible to add several devices simultaneously by scanning a range of IP addresses. You can also specify a device by IP Address, Host Name, or generic RTSP/HTTP/UDP link (see "Adding Multicast, RTSP or HTTP Streams as Cameras").

NOTE: For Axis cameras only — if the "People Counter" function is enabled, neither automatic or manual discovery will work in Nx Witness software.

To Add One or More Devices

1. Open the **Add Device** dialog by doing one of the following:
   - Open **Main Menu** and select **Add > Device**.
   - **Right-click** on the desired Server in Resource Panel to open its context menu.
2. Select the desired Server in the **To** field.

3. If the device requires, specify authentication parameters in the **Login** and **Password** fields. Once a device is added you can use the **Edit Credentials** button in **Camera Settings > General** to change this password.
   - Some devices may be discovered without specifying credentials, but often it is necessary to specify at least the default login and password.
   - Other devices may not require credentials for discovery but will require credentials when they are accessed for the first time. In this case, they will be displayed in the Resource Panel, but you will be prompted to enter credentials in order to view streams from these devices.
4. If needed, specify a discovery **Port**. The default **Auto** setting is recommended. Most devices are discovered on port `80`.
5. Choose one of the following:
   - Select the **Known Address** tab (to add a single device):
   a. Enter either the IP address, Host Name the device can be resolved on, or an RTSP, HTTP, or UDP link for the device in the **Address** field.
   b. Mouse hover over the icon near the Address field to see some syntax examples.



   - Select the **Subnet Scan** tab (to add several devices at once):
   a. Enter the desired **Start IP** and **End IP** values. (By default, addresses 0-255 of the same subnet are suggested so that the entire network will be scanned.)
   b. Press **Scan** to initiate the search. This can take some time, especially when an IP range is being scanned.
   c. If devices are located they will be displayed showing the brand, model and IP address. If a device is already registered it will display in the list as *Added*. Previously added devices, that were later removed, may be re-added.
6. Select the desired devices and click on **Add all devices**.The total number of devices being added will display in a banner at the top of the window.

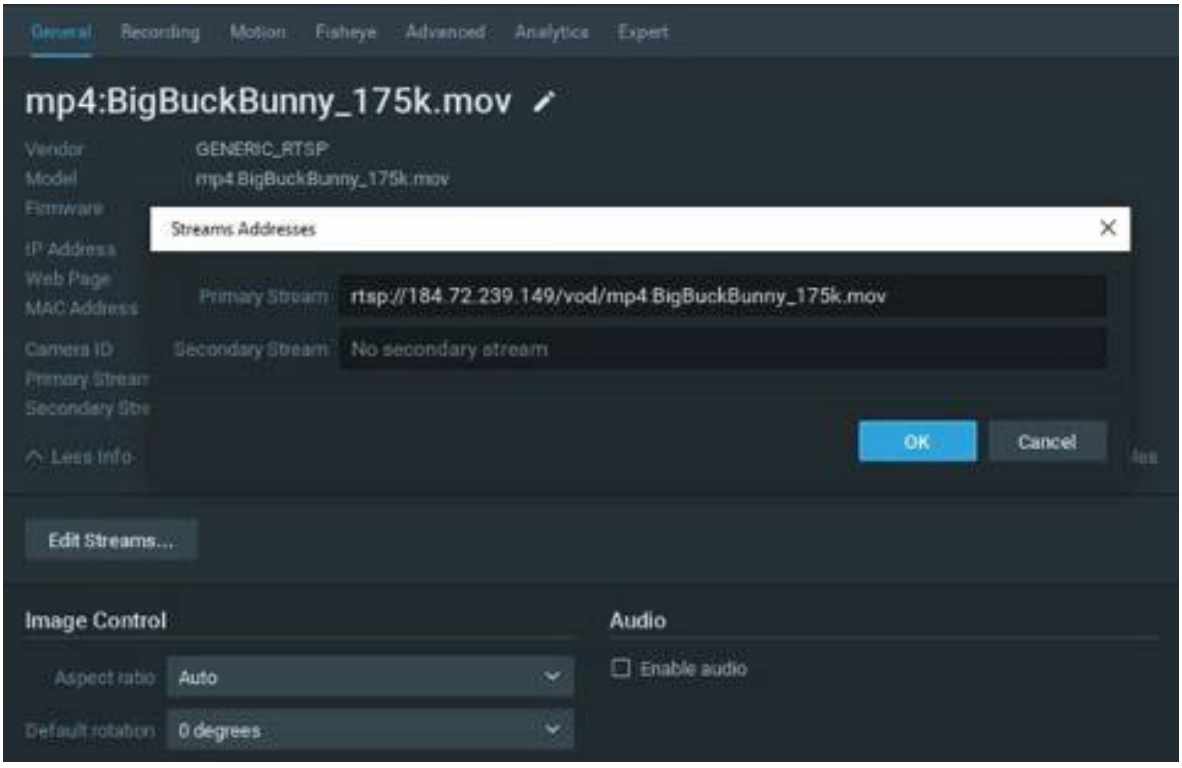
Adding Streams as Cameras

Occasionally a camera cannot be automatically discovered, or will not work properly in Nx Witness because it is not fully compatible with ONVIF. These devices can instead be added using their RTSP, HTTP, or UDP multicast URL stream address. Once added, such a camera can be successfully viewed and recorded in Nx Witness, including audio output over RTSP for devices that record audio.

It is possible to add two streams when creating an RTSP/HTTP camera, which enables dual streaming and adaptive scaling (see "Dual Stream Processing"). Dual-stream cameras from RTSP, HTTP, or UDP streams allow for the integration of third party legacy IP Cameras, DVRs, and NVRs with full Nx Witness adaptive scaling capabilities for reduced CPU and network usage.

NOTE: You must know the exact RTSP/HTTP/UDP URL of the stream. This information can be found in the camera manual, on the camera web page, or by contacting the manufacturer.

Follow the steps described in "Adding Devices Manually" for a single device to add the desired stream value in the **Address** field. Once added, the camera will be displayed in the Resource Panel as a "GENERIC_*stream type_stream name*". You can then use **Edit Streams** in **Camera Settings** > **General** to add or edit either stream value. Not all RTSP devices are compatible with the quality and FPS selection capability in the Client.



NOTE: If the lowest resolution is greater than 1024x768p, software motion detection will not be available.

Adding a Webcam or Pi Camera

Non-IP cameras such as built-in Raspberry Pi cameras or USB webcams are supported on Windows, Ubuntu Linux, and Raspbian operating enviroments with dual-streaming and audio support when the *Autodetect USB and web cameras* option is enabled (see "Configuring Server Settings").

These cameras will be automatically detected and added as a Nx Witness resource available for live and recorded viewing.

When the Nx Witness Site is installed on a Raspberry Pi machine with a Raspberry Pi camera module, the Site will function as a Server with a smart IP camera, capable of operating as a stand-alone Site for demonstrations or as part of a larger Site.

NOTE: Audio is not supported for the Raspberry Pi camera.

Replacing a Camera

The camera replacement feature facilitates the transfer of data from an existing camera to a new one. This allows the new camera to access the original camera's archive, recording schedule, and primary settings, provided the models exchanged are compatible.

Key Concepts:

- Camera replacement only supports single-channel cameras when replaced by another single-channel camera on the same Server.
- This camera replacement process can only be initiated by Administrator and Power Users.
- Camera replacement cannot be undone – a repaired camera should never be reinstalled on it's previous server.
- Available options and a summary of the data transfer plan will be presented for acceptance before the transfer is started.
- The following data and settings can be transferred:
  - Archive.
  - Camera’s name.
  - Access rights.
  - Analytics.
  - Event rules.
  - PTZ settings.
  - General settings.
  - Recording settings.
  - Advanced settings.
- The following data and settings cannot be transferred:
  - Motion Detection settings.

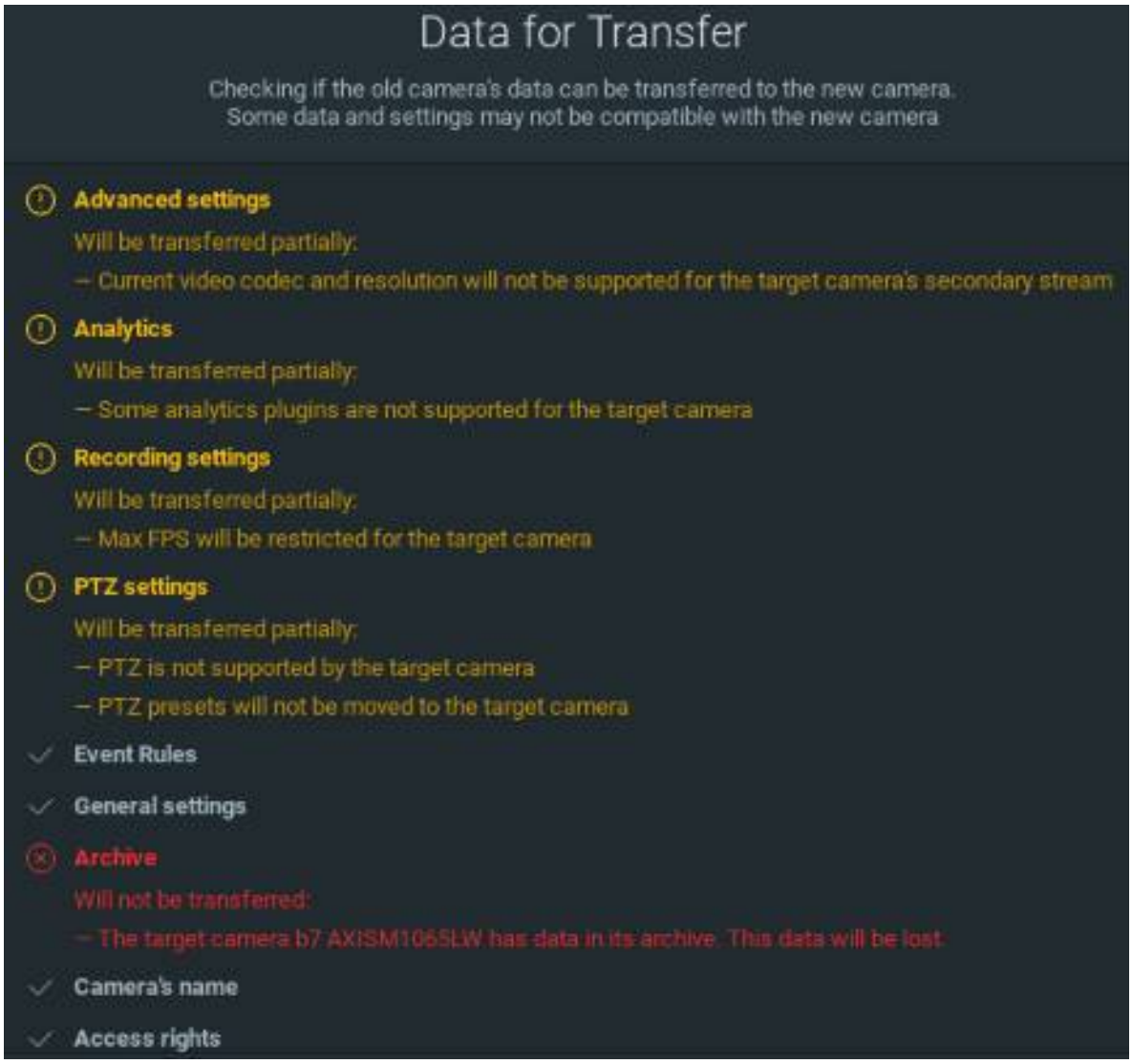
- Two-Way audio.

- Camera replacement does not support the following device types:
  - Multi-sensor cameras.
  - Virtual cameras.
  - Speakers.
  - NVRs.
  - Unauthorized Cameras.
  - IO modules.
  - Offline cameras that appeared after an Archive Reindex and Scan was performed.
  - Cameras that were previous replaced.

How to Replace a Camera

1. Make sure the camera to be replaced is disconnected and appears as offline in the Site.
2. Right-click the desired offline camera in the Resource Panel.
3. Select the **Replace Camera** option.
4. Select a camera to replace the current one.
5. Apply changes.

A transfer summary is presented before the transfer begins.



Deleting a Device

To delete a Device

1. Expand the server hosting the desired device in *Resource Panel*.
2. Find and select the device.
3. **Right-click** for the context menu and choose **Delete** (or the ***Del*** button on a keyboard).
4. Click **Delete** to confirm.

If a camera is disconnected or deleted, its archived footage becomes unavailable. However, it can be restored (see "Viewing Archive from Deleted Cameras").

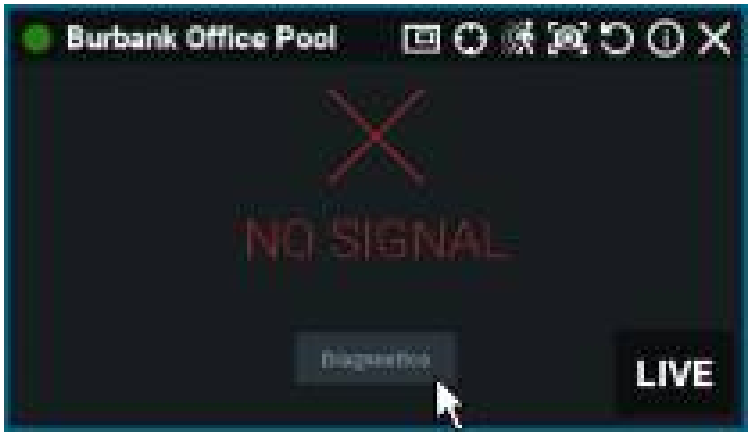
NOTE: If a device is online it will be auto-discovered again unless it was added manually. To avoid auto discovery, either unplug the device or Disable automatic device discovery.

If the device is back online, it will start working immediately and its recorded archive will be available. However, a User will need to reconfigure the **Device** as its settings have been erased.

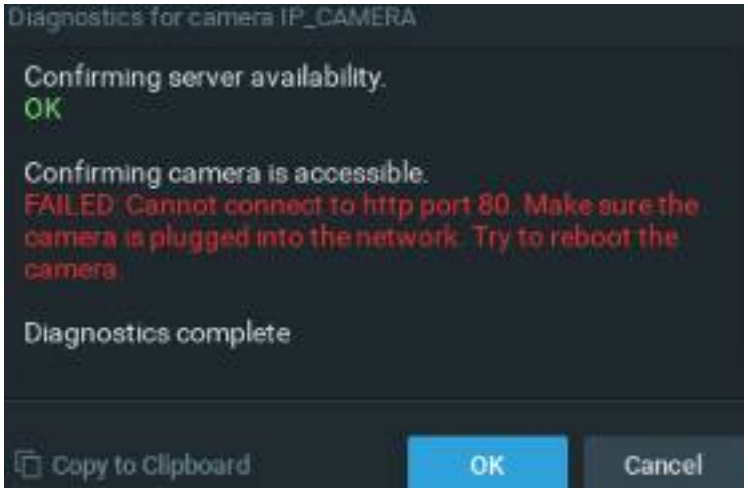
Diagnosing Offline Devices

Nx Witness can perform basic diagnostics to determine why a camera is offline. If you cannot fix the problem yourself, it is important to run a diagnostic test prior to contacting support, and provide them with the results.

A camera that is offline will be have an offline icon ( ) in the Resource Panel and will display **NO SIGNAL** in layout. Diagnostics can be invoked by pressing the **Diagnostics** button on the item:



Once diagnosis is complete, the analysis and recommended actions will be displayed:



Follow the instructions to resolve the issue. If unsuccessful, contact support (see "Contacting Support").

NOTE: Make sure to click *Copy to Clipboard* and paste the data into your message prior to sending it to support.

Setting Up Cameras and Devices

Cameras and Devices contain internal settings specified by the manufacture and Site settings that HD Witness applies outside of the Device. An example is Camera Resolution being set and defined within the Camera while Camera Hotspots are defined and contained within the Desktop Client. The devices settings and options available through the Site will vary depending on device model, firmware installed, and compliance with industry standards.

Users must be a member of a group having **Edit Device** permissions or have been granted permission to **Edit a Device** to perform the tasks outlined in this topics (see "Users and Groups").

NOTE: It is possible to configure image controls, audio, recording schedule, authentication credentials, etc. – for several devices simultaneously. See "Applying Parameters to Multiple Devices".

Device Set Up

- Obtaining Basic Device Information.
- Device Authentication.
- Renaming a Device.
- Setting Camera Orientation.
- Setting Camera Aspect Ratio.
- Hot Spot and Camera Linking.
- Events Log.
- Event Rules List.

Image Control

- Image Enhancement.
- Pan, Tilt, and Zoom Controls.
- Dewarping Controls.
- Saving and Restoring PTZ Positions.
- Setting Up PTZ Tours.

Configuration Settings

- Configuring Audio on a Device.
- Setting Up a Virtual Camera.
- Setting Up an I/O Module.
- Setting Up an Analog Camera.
- Setting Up Motion Detection.
- Setting a Recording Schedule.
- Recording Modes.
- Configuring Minimum and Maximum Archive Storage.

Device Information

Every connected camera has a some identification and configuration data set by the vendor, the active network, and the Nx Witness platform that can be displayed in the Desktop Client, the Web Admin Client, or the Cloud portal, for cloud-connected Sites. While the informational fields displayed between camera vendors and clients may vary, the factual value for every field remains consistent across clients.

To Display Camera Information

Desktop Client

1. Select the camera of interest and open the context (right-click) menu.
2. Click **Camera Settings** from the context menu.
3. Select the **General** tab within the camera settings window.
4. Review the essential information provided.
5. Click the **More info** text to expand the panel and display all available information.

Web Admin / *Cloud Portal*

1. Select the **Settings** tab within the heading menu.
2. Choose **Cameras** within the left panel control.
3. Select a camera from the list displayed.
6. Review the essential information provided.
4. Click the **Detailed info** text to open the *Information Tab* for the camera which displays all available information.

Commonly Available Information

- *Camera name* – click the pencil icon to edit the camera name.
- *Vendor* – retrieved from the camera.
- *Model* – retrieved from the camera.
- *Firmware* – retrieved from the camera.
- *IP address* – the Desktop Client includes a **Ping** button to test camera response.
- *Web Page* – link launches embedded configuration tool, when available. Use caution when changing camera settings in embedded camera tools and clients at the same time.
- *MAC address* – retrieved from the camera.
- *Camera ID* – a UUID that the Site assigns to each camera, including virtual and test cameras. The format is similar to f93369eb-e530-27b7-78ba-16978cbd3061.
- *Primary stream URL* – retrieved from the camera.
- *Secondary stream URL* – retrieved from the camera.

Advanced Information

- ID based on hardware – a unique signature generated from device metadata.

- Availability – includes status and a count of events generated for IP conflicts, offline status, or other issues.
- Stream Resolutions – often includes resolution, FPS metrics, and amount to archived storage consumed.

Authenticating Devices

Most all cameras are created with a predefined login and password combination. During the discovery process, Nx Witness attempts to use the manufacturer's default credentials to access a device and acquire media streams. However, default login and passwords can vary between models or product lines, or may have already been changed.

If Nx Witness cannot access a device using the default authentication, the device is shown as **Unauthorized** () in the Resource Panel and the following message will appear when a User attempts to view a live stream: "UNAUTHORIZED Please check authentication information."

Some devices require that a non-default password be created if they are discovered using default credentials. In this case, the device is displayed within the Resource Panel but an "unauthorized" message will be displayed when attempts are made to view streams from such devices.

To Manage Authorization Credentials

Desktop Client

1. Select the camera of interest and open the context (right-click) menu.
2. Click **Camera Settings** from the context menu.
3. Select the **General** tab within the camera settings window.
4. Click the **Edit Credentials** button located below the Authentication heading.
5. Confirm or update the login and password fields.
6. Click **OK** to apply the changes and attempt to authenticate on the camera.

Web Admin / *Cloud Portal*

1. Select the **Settings** tab within the heading menu.
2. Choose **Cameras** within the left panel control.
3. Select a camera from the list displayed.
4. Click the **Edit Credentials** button located below the Authentication heading.
5. Confirm or update the login and password fields.
6. Click **SAVE** to apply the changes and attempt to authenticate on the camera.

Changing Device Server

Key Concepts:

- The Resource Panel of the Desktop Client can be used to move a device from one Server to another Server.
- Both Servers must be on the same network, otherwise moving a device across networks will take the device offline.
- Changing Servers on the same network will retain device settings and the video archive will be combined seamlessly.
- Only the Desktop Client can change which Server a device is connected to.
- Recording will automatically restart and the live stream will be available.
- When changing Server networks, you will be given the option to Move it anyway, Skip (the specific camera, if more than one is selected), or Cancel the operation.
- Moving devices between Servers is an efficient way to manually balance Server loading.
- Devices can also be automatically moved in the event of a Server failure by Configuring the Failover feature.
- An offline camera will still required a license or service, even though the device is not recoding at the moment.

To Move Devices to Different Servers

1. Open the Resource Panel
2. Select the devices to be moved; selecting multiple devices is permitted.
3. **Drag-and-drop** the selected devices over the name of the new Server.

Renaming a Device

When a device is discovered automatically, it is displayed in the Resource Panel as either "model" or "manufacturer + model". As a result, all cameras with the same make and model will have the same name – only the IP address will differ. Display of the IP address is optional (see "Show additional info in tree").

A device can be renamed for easier identification or any other reason.

In the Resource Panel right-click on the device and use the context menu option **Rename** (**F2**), or from **Camera Settings** > **General** click on the pencil icon in the camera name field to make it editable.

Setting Up Motion Detection

The Nx Witness server is able to perform software motion detection. Motion detection on the software side allows for adaptive scaling, which is dynamic resolution switching that yields bandwidth savings and optimizes the processor load.

By default, the secondary stream will only be used for motion detection if its resolution is less than 1024x728. If the secondary stream resolution is higher than this, the primary stream will be used if its resolution is less than 1024x728.

If both the primary and secondary stream's resolution is higher than 1024x768, then no motion detection will be enabled.

NOTE: If the secondary stream is high-resolution, motion decoding may consume most or all of the Server CPU. See "Forcing Motion Detection to a Specific Stream" to adjust for this issue.

Software-side detection also makes it possible to define regions in which motion detection is performed, with a range of sensitivity levels that include complete **motion masking**, where motion detection is blocked. With **hardware motion detection**, a motion mask can be applied, but sensitivity levels may be unavailable. In some cases it may be possible to use the **Camera Settings** > **General** tab to instead configure device parameters (see "Configuring Device Advanced Settings Using Nx Witness").

NOTE: Arecont Vision devices are set to hardware detection mode automatically.

Motion Detection Indicators

Nx Witness provides motion detection indicators in the form of a temporary red outline on grid cells when motion is detected. This feature is especially useful for highlighting motion that is easily detected by cameras but often filtered out by humans – for example, trees moving in the wind, the motion of shadows, sudden changes in light level, etc.

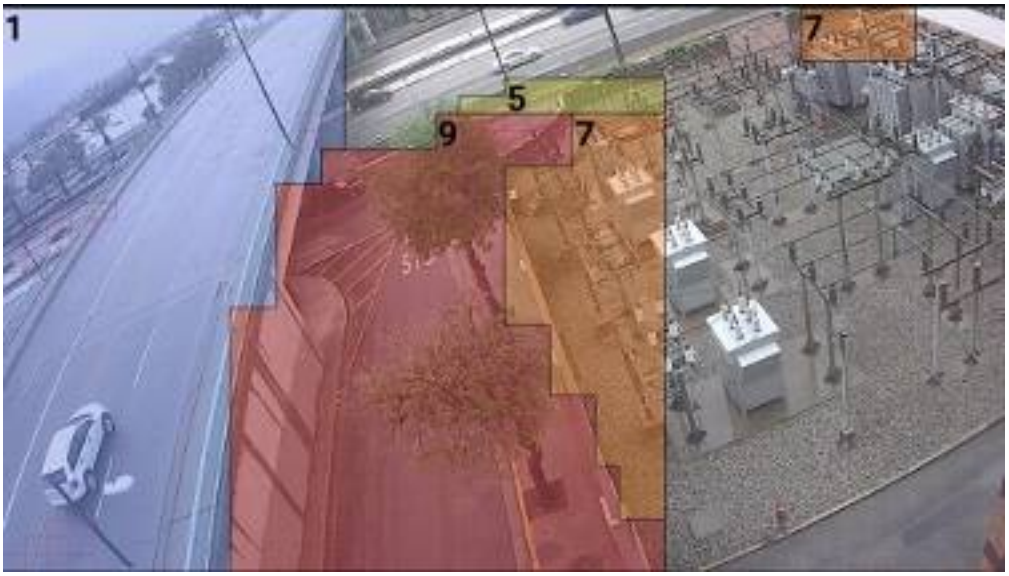
To Configure Motion Detection

1. Do one of the following:
   - *Desktop Client*: Open **Camera Settings** and go to the **Motion** tab, then click the **Motion Detection** button to enable detection (green) for the device.
   - *Web Admin* / *Cloud Portal*: Open **Settings** > **Cameras** and select a camera and Click the **Enable motion detection** button.

     NOTE: Cells in the motion detection grid are briefly highlighted in red when motion is detected. The greater the intensity of brighter these red indicators, the higher the level of motion detection that is set.
2. Click on a number in the *Sensitivity* section, where **0** is no sensitivity to motion (motion mask), **1** is minimal sensitivity, and **9** is maximum sensitivity.
3. The motion detection grid is 42 x 32 cells. Use the following actions to apply the selected sensitivity to cells:
   - Click and Drag to select a rectangular area.
   - Click on a cell (the entire area that the cell is associated with will be filled, not just the individual cell).

4. The sensitivity level remains active until a new one is selected. Continue to select and apply sensitivity levels as desired. If necessary, you can use **RESET** to return the entire field to the default level of 5.
5. Apply changes.

For Example



The above image contains the following motion detection regions:

- Grey (un-numbered) is motion mask
- Blue (**1**) has very low sensitivity to motion
- Yellow (**5**) will capture motion with moderate sensitivity (5 is the default setting)
- Orange (**7**) will be highly sensitive to motion, red (**9**) offers the maximum sensitivity

You can also see some of the red motion indicators on the left side of the image.

Setting Camera Aspect Ratio

Occasionally, cameras will report an incorrect aspect ratio. If Nx Witness cannot make an automatic correction you can do so manually.

NOTE: This correction will require transcoding of videos that are exported from the camera.

To Specify an Aspect Ratio

Desktop Client

1. Open **Camera Settings** and go to the **General** tab.
2. In the **Image Control** section, click on the **Aspect Ratio** drop-down menu.
3. Select the desired aspect ratio from the available options: **16:9**, **1:1**, or **4:3**. Select **Auto** for Nx Witness to determine the aspect ratio.
4. Apply changes.

Web Admin / *Cloud Portal*

1. Open **Settings** > **Cameras** and select a camera.
2. Click on the *Aspect Ratio* drop-down menu.
3. Select the desired aspect ratio from the available options: **16:9**, **1:1**, or **4:3**. Select **Auto** for Nx Witness to determine the aspect ratio.
4. Apply changes.

NOTE: If the aspect ratio is set to **Auto** in the Camera Settings dialog, the aspect ratio of the secondary stream will be modified to match the aspect ratio of the primary stream.

Configure Multiple Devices

To simplify the configuration process, you can apply the same parameters to multiple devices at once. Not all settings and devices

1. Select the desired devices from the Resource Panel or layout.
2. Open the device context menu and go to **Device Settings**. The following settings can be configured when multiple devices are selected:
   - Authentication credentials.
   - Aspect Ratio.
   - Default rotation.
   - Audio (enabled or not).
   - License Activation (Recording on or off).
   - Recording Schedule.
   - All **Expert** tab settings except **Logical ID** (see "Expert Device Settings").
3. Enter the desired parameters.
4. Apply changes.

Camera Audio Settings

Nx Witness allows for audio recording from devices that are audio-enabled and have a microphone connected (see "Audio in Nx Witness").

A user must have the Play Audio permission and the device must have audio enabled for the audio service to fully function. Users with the "Edit Settings" permission and members of the Built-In Administrators and Power User groups the can enable or disable audio on a device.

To Configure Audio

Desktop Client

1. Context (right) click the **camera > Camera Settings > General** tab.
2. Check the *Enable audio* checkbox and choose between the two options:

- **Use audio stream from this camera** – use the audio input from the current camera.
- **Use audio stream from another camera** – select a camera or device with audio input to use instead of the current camera's audio input.

3. Apply changes.

Web Admin / *Cloud Portal*

1. Open **Settings** > **Cameras** and select a camera.
2. Check the *Enable audio* checkbox and choose between the two options:
   - **Use audio stream from this camera** – use the audio input from the current camera.
   - **Use audio stream from another camera** – select a camera or device with audio input to use instead of the current camera's audio input.
3. Apply changes.

NOTE: Only devices connected to the same Server can provide their audio stream to another camera.

Defining Hotspots

Hotspots are click-able icons placed over a video stream that allows users to quickly navigate to another device or shared layout. This feature is useful for tracking an object of interest as it travels between the view of multiple cameras or to quickly view a location from different perspectives.

Hotspot Features:

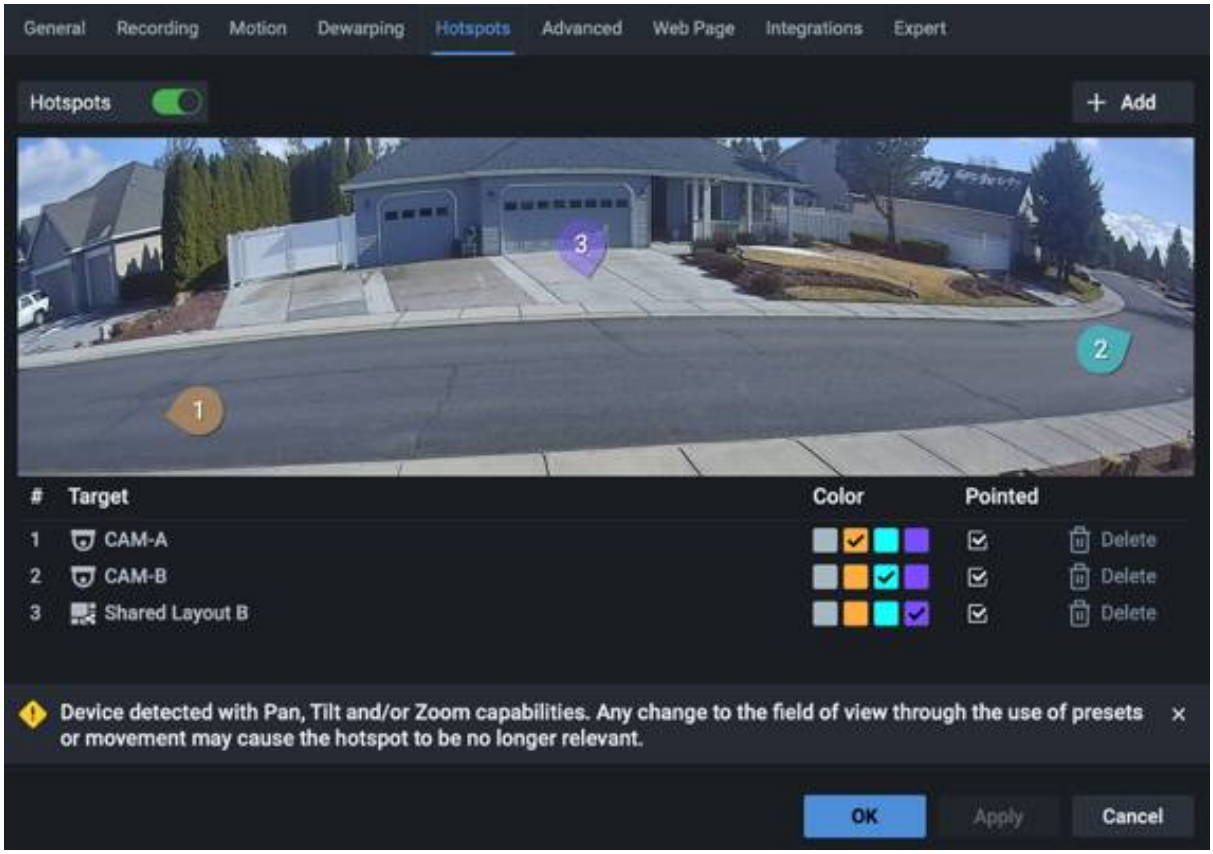
- Hotspot are moveable, freely positioned icons that reside on a video stream overlay.
- Hotspot icons can include a optional directional pointer and color tint.
- Only Administrators and Power Users can create, edit, or delete Hotspots.
- While there is no limit to number of Hotspots created for a camera, only so many will Hotspot icons fit over a video stream.
- All users who can view the device or camera can toggle the Hotspot layer (see "Users and Groups").
- Hotspots respond to mouse hover, mouse click, and will present a context menu on mouse right-click.
- Hotspots are disabled by default and must be enabled for each device or camera in the Site (see "Setting Up Cameras and Devices").
- Hotspots are only available in the Desktop Client and do not exist in other Nx Witness clients or services.
- Each instance of a camera or video stream can be independently be configured to have the Hotspot layer active and displayed, or disabled and hidden.
- Hotspots remain in a fixed X-Y position over the display and are not affected by Image Controls or Pan, Tilt, and Zoom movements.

- Use a PTZ preset to record the the camera position that is aligned with precisely placed Hotspots.

To Add or Edit a Hotspot using the Desktop Client

1. Open **Camera Settings** by doing one of the following:
   - Navigate to **Main Menu > Site Administration > Camera List** and either double click a camera, or right click on a camera in the *camera list*, and select **Camera Settings...**
   - Right-click on a camera name in the resource panel or right-click on a camera stream placed in a layout to open the context menu, then select **Camera Settings...**
2. Select to the **Hotspots** tab in the *Camera Settings* dialog.
3. Set the switch for *Hotspots* to the on (visible and active) position.
4. Click the **Add** button and the next sequential Hotspot number is added to the center of the Camera display.
5. Drag the Hotspot to any available, non-overlapping location on the Camera display.
6. Select a Hotspot to configure from the list:
   - Select a target for the from the list of resources presented.
   - Choose a color tint for the Hotspot
   - If the **Pointed** icon feature is enabled, set the direction of the target.
7. Select a Hotspot from the list to configure it, and then a
   a. Repeat this step to reconfigure any Hotspot labeled *Select Camera*.
8. **Apply** changes to remain in the Hotspot dialog or click **OK** to apply settings and exit the *Camera Settings* dialog.

   NOTE: All created Hotspots not linked to a target will be removed when the *Hotspot* dialog is closed. Removed Hotspots will logically decrement remaining Hotspot numbers.



Using Hotspots

- If not displayed, activate the Hotspot layer using Keyboard Shortcut (**"H"**) or by Clicking the Hotspot icon in the display title bar.
- Hovering the mouse pointer over a camera Hotspot will present a preview of the target.
- Hovering the mouse pointer over a Layout icon will display the title of the shared Layout. Layout Hotspots do not provide a preview or thumbnail.
- Clicking on a camera Hotspot will highlight the target camera on the active layout, or add the target camera to the active layout if it is not already present.
- Right Clicking will open a contextual menu based on where it is opened:
  - The context menu for a camera hotspot includes the option to open the camera, open the camera in a new tab (of the active client), or open the camera in place (replace current grid item with the target camera).
  - The context menu for a shared layout hotspot offers to open the target layout in a new tab.

To Delete a Hotspot using the Desktop Client

1. Open Camera Settings by doing one of the follow:
   - **Main Menu > Site Administration > Camera List** and double click a Camera.

- Open **Camera Settings...** using the context menu on the Viewing Grid or a Camera name in Resources Panel.

2. Change to the Hotspots tab in the *Camera Settings* dialog.
3. Remove Hotspots using the **Delete** (trashcan) icon above the list of Hotspots.

NOTE: Deleted Hotspots cannot be restored.

ONVIF Profiles

Nx Witness automatically discovers devices and configures the optimal streaming parameters to fetch data from devices. For this purpose, the ONVIF protocol is used. The information below is generally applicable to the Advanced and Expert settings dialogs of a camera, the can reached by selecting a camera, activating the context menu (right-click), and then select the tab that contains the relevant information.

The communication is configured according to the **ONVIF Network Interface specification**.

Nx Witness supports different ONVIF Network Interface specifications:

- **Media** – the older one (is supported by all ONVIF devices)
- **Media2** – the newer one.

If the device reports that Media2 is supported, Nx Witness will try to use it.

The audio and video communication is configured through **stream profiles.**

A profile describes the set of parameters related to audio/video transport from a device to the Nx Witness Server:

- A/V Codec
- Bitrate
- Resolution
- Additional parameters.

Usually, cameras provide 2 independent stream profiles:

- Primary stream (Hi-Res)
- Secondary Stream (Lo-res) – used for motion detection, browsing archive etc (see "Dual Stream Processing" for details).

Cameras may provide additional stream profiles (more than 2) but Nx Witness uses only Primary and Secondary ones.

In some cases, the profiles can be fetched and identified incorrectly. In this case it may be necessary to configure stream profiles manually.

To access those settings, use the camera's context menu to open **Camera Settings** > **Expert > Media Streaming**:

- **Primary** and **Secondary Stream Profiles** – specify the stream profiles for Primary and Secondary streams.

  The available profiles may vary depending on the vendor or model of the device used.

  By default, Nx Witness configures the optimal parameters for the stream profiles but it can be turned off and the settings setup on Camera can be used unchanged (see "Preventing Nx Witness from Changing Device Settings").

- **Use Media2 to fetch profiles** – in some case Media2 can work incorrectly. In this case it is possible to select the following options:
  - **Never** – always use Media to configure stream profiles
  - **Use if supported** – use Media2 if the device indicates its support
  - **Auto** – use the built-in method to discover if the device supports Media2.

Profile M - Key Concepts:

- The ONVIF Analytical Plugin integrates ONVIF Profile M analytics into Nx Witness for compatible devices.
- Profile M enables real-time event subscriptions and ability to processes ONVIF event notifications.
- The Primary functions are event parsing and topic tree management for analytics events.
- Real-time Pull-Point Notification Interface supports the latest and most common ONVIF subscription types.
- The Plugin subscribes to all events, without any filtering, as to receive any and all events supported by a camera.
- Filtering is done inside the plugin, allowing only the event types mentioned in user-created Event Rules.
- The profile M functionally provided is defined by the available devices and will vary between devices..

NOTE: Profile M support can be limited and may not be available for all devices that claim to be compatible.

Profile G Key Concepts:

- An option to enable the *Import from Device* service will appear in the **Camera Settings > Expert** tab for supported devices.
- The Main Menu will include an entry to open the *Import from Devices* dialog window when supported devices are connected.
- Only camera or server offline periods that occurred after enabling the *Import from Device* option will be imported automatically.
- When the *Import from Device* is disabled, any offline periods that have not yet been imported will be lost and cannot be recovered.

NOTE: Profile G support is provided for the following cameras:

- Hanwha XND-C9083RV
- Uniview IPC2325SB-DZK-I0
- Vivotek FD/IB9391-EHTV-v2 series
- Vivotek FD/IB9365-EHTV-v2 series

See also:

- Disabling Recording of a Specific Stream
- Disabling a Secondary Stream

Accessory Devices

A joystick is a peripheral device that provides programmable hotkeys and accurate analog control over the pan, tilt, and zoom functions of compatible PTZ cameras in Nx Witness.

This functionality is officially supported on **Microsoft Windows only**. Other OS may work but issues might occur.

The following joysticks are officially supported:

- Axis T8311
- Hanwha Techwin SPC-2000

Other USB joysticks are also supported, but may provide limited functionality.

Initial Setup to start using a joystick in the Desktop Client

1. Close the Desktop Client.
2. Plug in the joystick to the computer that you will be using. Windows will automatically detect the device and install the necessary drivers.
3. Open the Desktop Client.
4. Open a PTZ camera and click on the PTZ icon with your mouse.
5. Use the joystick to pan, tilt, and zoom the camera.

Common Joystick Usage

Stick movement – controls PTZ

Stick rotation – controls zoom in/out.

NOTE: When controlling a PTZ IP camera via analog joystick controls, expect latency from physical movement of the joystick to the resulting PTZ action of the camera. PTZ actions are only applied to items that are selected on the scene in the Desktop Client.

Advanced Configuration

Supported joysticks can access additional configuration settings in the Desktop Client (**Main Menu > Joystick Settings**). Joystick Settings contains two tabs: Basic Actions and With Modifier.

Basic Actions

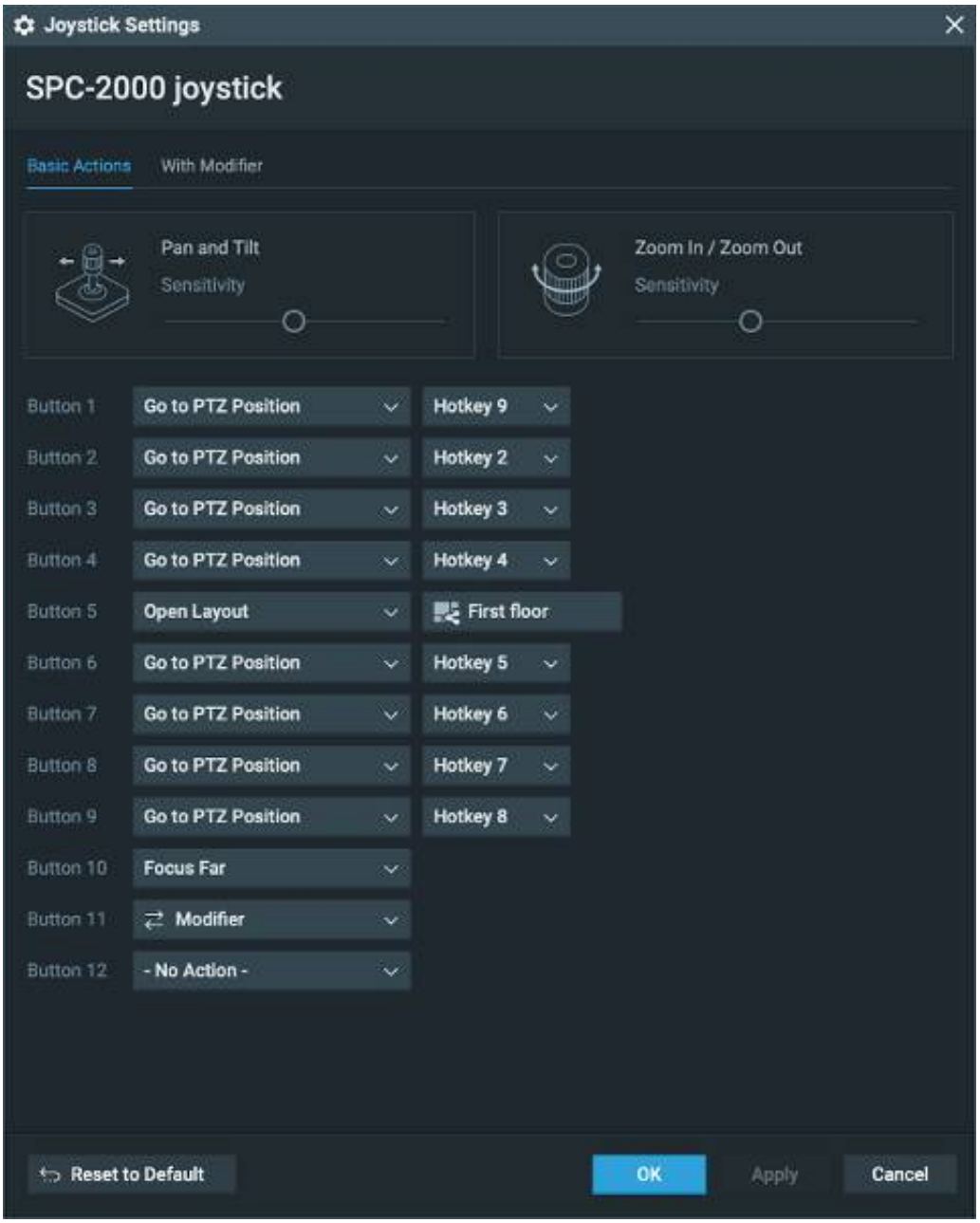
Adjust PTZ sensitivity and configure joystick buttons in this tab. To adjust the sensitivity of PTZ controls, move the slider to the left to reduce sensitivity and move the slider to the right to increase sensitivity.

NOTE: If joystick has only two axises, Zoom sensitivity control is not shown.

Each joystick button has a drop-down menu associated with it where you can assign one of the following actions to the button:

- Focus Near
- Focus Far
- Autofocus
- Go to PTZ position (requires you to select the hotkey/PTZ position)
- Open Layout (requires you to select a specific layout)
- Set to Fullscreen
- Next Camera on Layout
- Previous Camera on Layout
- Modifier (requires additional configuration in the With Modifier tab)

NOTE: All changes must be saved by clicking Apply or OK before exiting the settings dialog.



With Modifier

The With Modifier tab is disabled unless at least one of the joystick buttons is set as a modifier in the Basic Actions tab. Select a secondary action for each joystick button in this tab. The secondary action will activate while the modifier button is held down.

For example: If you set button 11 as a modifier and open the With Modifier tab, you can configure button 1 to open a layout any time button 11 is held down. Button 1 will still retain its standard action of going to a PTZ position when button 11 is not held down.

NOTE: All changes must be saved by clicking Apply or OK before exiting the settings dialog.

Using Joysticks

A joystick is a peripheral device that provides programmable hotkeys and accurate analog control over the pan, tilt, and zoom functions of compatible PTZ cameras in Nx Witness.

This functionality is officially supported on **Microsoft Windows only**. Other OS may work but issues might occur.

The following joysticks are officially supported:

- Axis T8311
- Hanwha Techwin SPC-2000

Other USB joysticks are also supported, but may provide limited functionality.

Initial Setup to start using a joystick in the Desktop Client

1. Close the Desktop Client.
2. Plug in the joystick to the computer that you will be using. Windows will automatically detect the device and install the necessary drivers.
3. Open the Desktop Client.
4. Open a PTZ camera and click on the PTZ icon with your mouse.
5. Use the joystick to pan, tilt, and zoom the camera.

Common Joystick Usage

Stick movement – controls PTZ

Stick rotation – controls zoom in/out.

NOTE: When controlling a PTZ IP camera via analog joystick controls, expect latency from physical movement of the joystick to the resulting PTZ action of the camera. PTZ actions are only applied to items that are selected on the scene in the Desktop Client.

Advanced Configuration

Supported joysticks can access additional configuration settings in the Desktop Client (**Main Menu > Joystick Settings**). Joystick Settings contains two tabs: Basic Actions and With Modifier.

Basic Actions

Adjust PTZ sensitivity and configure joystick buttons in this tab. To adjust the sensitivity of PTZ controls, move the slider to the left to reduce sensitivity and move the slider to the right to increase sensitivity.

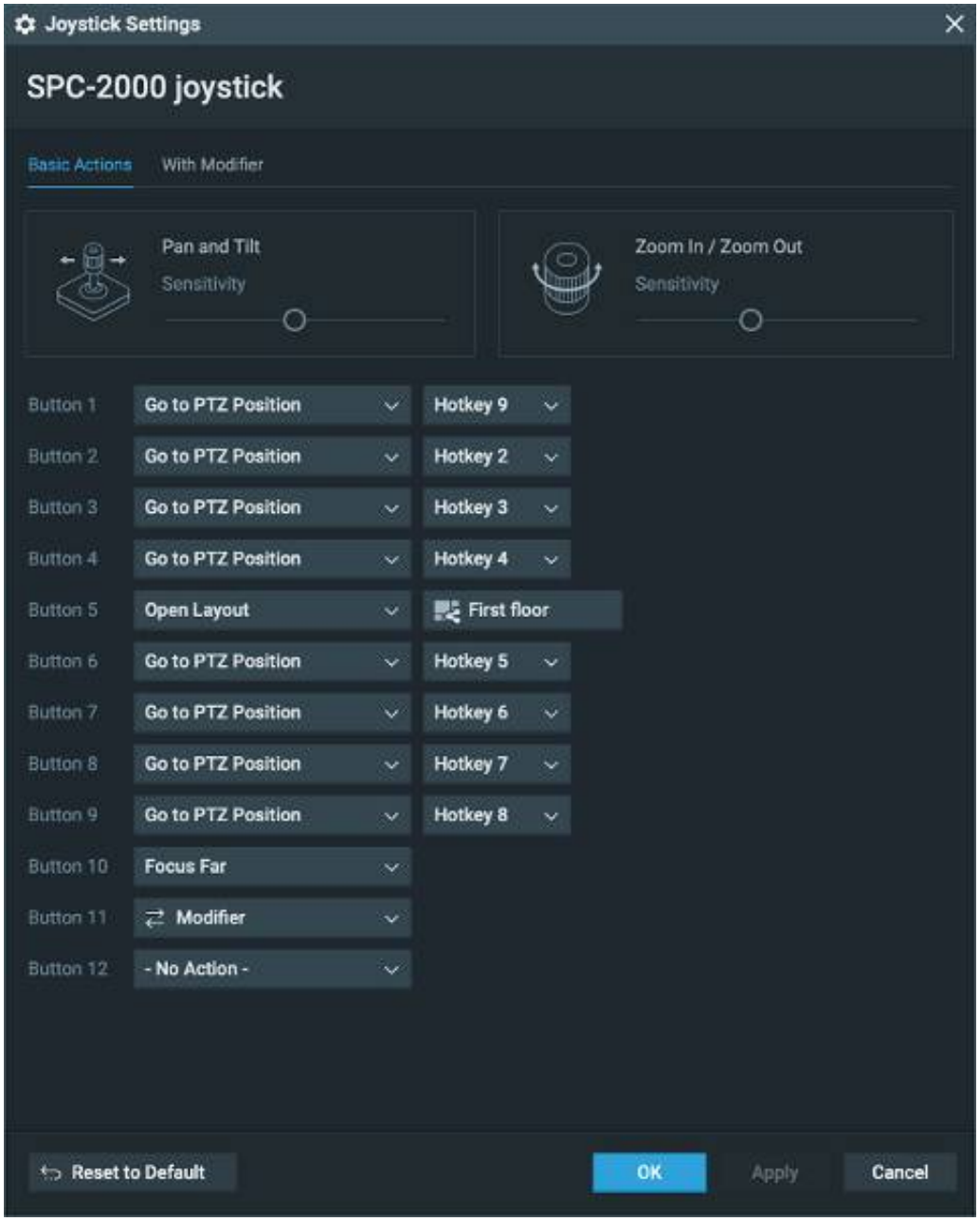
NOTE: If joystick has only two axises, Zoom sensitivity control is not shown.

Each joystick button has a drop-down menu associated with it where you can assign one of the following actions to the button:

- Focus Near
- Focus Far
- Autofocus

- Go to PTZ position (requires you to select the hotkey/PTZ position)
- Open Layout (requires you to select a specific layout)
- Set to Fullscreen
- Next Camera on Layout
- Previous Camera on Layout
- Modifier (requires additional configuration in the With Modifier tab)

NOTE: All changes must be saved by clicking Apply or OK before exiting the settings dialog.



With Modifier

The With Modifier tab is disabled unless at least one of the joystick buttons is set as a modifier in the Basic Actions tab. Select a secondary action for each joystick button in this tab. The secondary action will activate while the modifier button is held down.

For example: If you set button 11 as a modifier and open the With Modifier tab, you can configure button 1 to open a layout any time button 11 is held down. Button 1 will still retain its standard action of going to a PTZ position when button 11 is not held down.

NOTE: All changes must be saved by clicking Apply or OK before exiting the settings dialog.

Setting Up an I/O Module

Nx Witness handles I/O devices as it does cameras, with some specific functionality adaptations. Like all other devices, I/O modules are discovered automatically or with the user's help and then displayed in the Resource Panel.

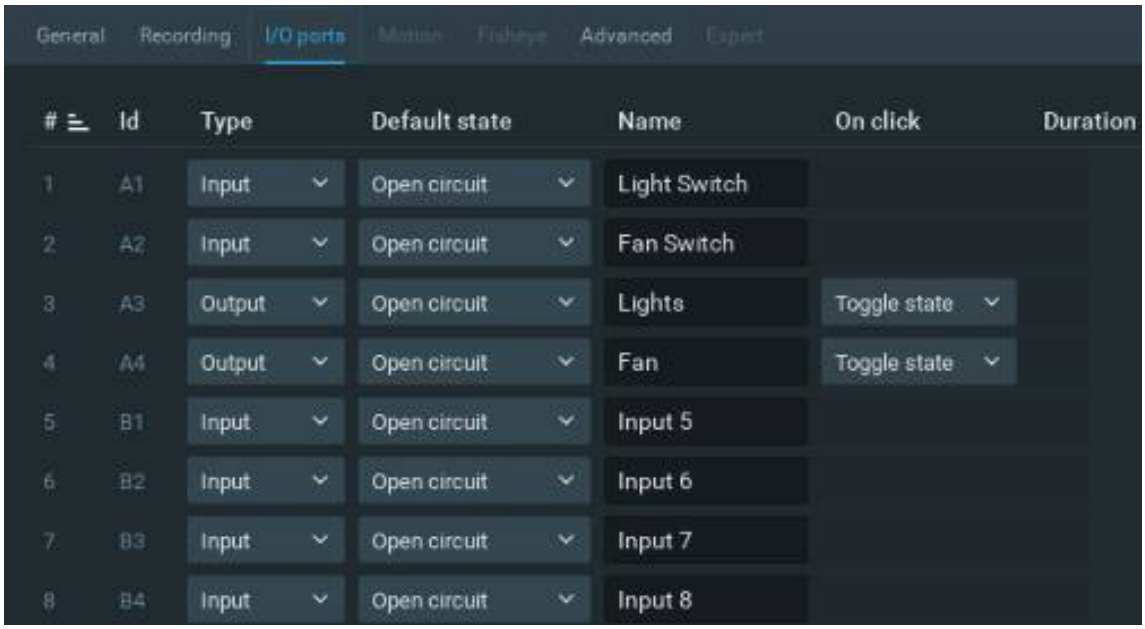
However, to start working with an I/O Module it is necessary to obtain and configure an *I/O Module License* (otherwise the "Device Disabled" message will be displayed). After the license is activated, the module will be displayed with the available inputs and outputs.

I/O Module permissions vary depending on the user's role (see "Permissions Management").

- Any User in the Site that has access to the I/O Module can view its inputs and outputs.
- Administrators, Power Users, and Custom Groups or Users with the "Edit camera settings" permission can configure I/O Modules.
- Administrators, Power Users, Advanced Viewers, and Custom Groups or Users with the "User Input" permission can trigger IO Module outputs.

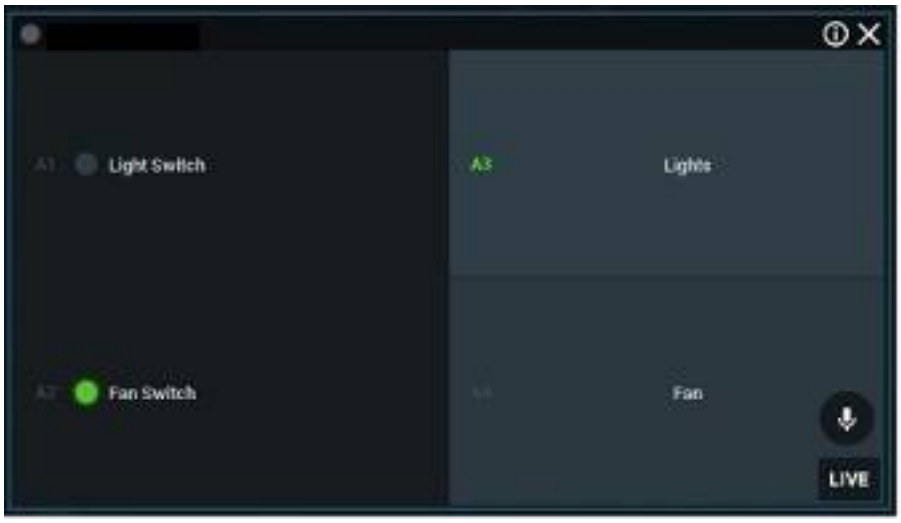
I/O Modules Require the Following Setup Steps

1. Right-click on the device in the Resource Panel and click on **I/O Module Settings**.
2. Go to the **I/O ports** tab and enter the following parameters:
   - *Type* – Input or Output.
   - *Default State* – Default state of the circuit depending on the I/O Module: *Open circuit* or *Grounded*.
   - *Name* – Name of the port.
   - *On click (output only)* – Select the desired action to occur on button click.
     - *Impulse* (requires Duration) – The length of time the signal will be generated (with 100ms steps). Clicking the button changes the port state to Duration time.
     - *Toggle state* – Clicking the button changes the port state until clicking the button again.
   - *Duration* – Time in milliseconds.



After the I/O module is configured, you will see Input ports on the left and Output ports on the right. The state of each port can be seen. The I/O module will be displayed as shown below:

If you are using multiple Inputs and Outputs from the device we recommend using the "Enable tile interface" option in the lower left hand corner of the dialog. This option will generate a responsive tiled interface for the I/O in the Viewing Grid, offering a different visual experience for triggering ports and seeing their state.



The following actions can be performed with an I/O Module:

- *Record Audio from I/O Module* – Only if a microphone is connected. See "Recording Modes" and "Audio in Nx Witness" for details.
- *Playback Audio Archive Recorded from I/O Module* – Only if a microphone was connected during recording. This is similar to viewing archive from cameras (see "Parts of the Timeline").
- *View Inputs State* – Information regarding the inputs state of the device depending on the settings you configured. For example, when the circuit is grounded, the appropriate sensor turns green. Alternatively, you can also set the sensor to turn green when the circuit is open.
- *Trigger Output* – For this purpose click the corresponding button (A3 and A4 in the image above). The output signal is sent for the amount of time specified in the *Pulse Time* setting unless the output is manually turned on/off.
- *Create Rules* – Using the device's input and output ports as described in Input Signal on Device and Device Output.

Working With Intercoms

An intercom is a visitor-side two-way communication device containing a camera and a microphone. Connected intercoms constantly send audio and video to its Nx Witness Site. Nx Witness does not send audio to intercoms unless the user is in an ongoing call with a visitor using an intercom.

The only supported intercom in Nx Witness is the Hanwha Techwin TID-600R.

Intercom Soft Triggers

The TID-600R intercom has three preconfigured soft triggers:

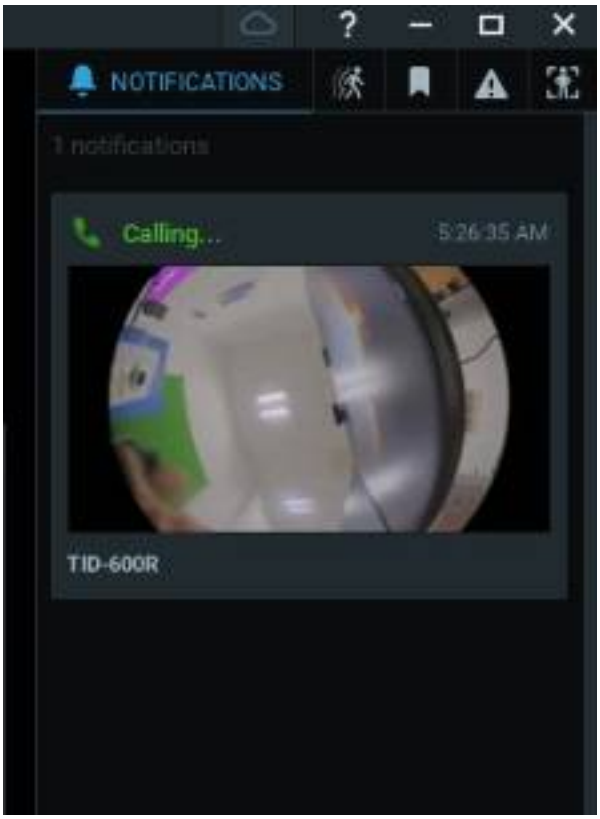
- Push to Talk requires the operator to activate a soft trigger to begin sending audio (see Using 2-Way Audio).
- Door – opens the relay for the door associated with the intercom.
- Heater – turns on the heater function.

Intercom Layouts

When saving a layout containing an intercom or receiving a call, an intercom layout will appear in the Resource Panel called *TID-600R Layout* with the following icon . An intercom layout cannot be deleted unless the intercom is removed from the Nx Witness Site first.

Receiving and Ending Calls

When the visitor initiates a call by clicking a button on the intercom, you will see a notification labeled *Calling...* in the Notification Panel. Click anywhere on the notification to be taken to the intercom layout (it will be automatically created if it does not already exist), where you can click the Push to Talk soft trigger and begin sending audio to the intercom. Release the Push to Talk soft trigger or close the layout when done speaking to the visitor.



Setting Up an Analog Camera

Typically, analog Cameras are connected via analog recorders. Each recorder has a number of channels that indicates the number of analog Cameras it can handle. If a recorder is plugged into the network, it can either be discovered automatically or added manually.

The following types of analog Cameras are supported:

- Analog cameras plugged into an encoder – These cameras behave like any other camera in the Site. It is possible to have a Recording Schedule and Motion Detection configured for Encoder analog cameras.
- Analog cameras plugged into a recorder (DVR) – These cameras are recorded somewhere else so Nx Witness only pulls the desired stream from the recorder. It is not possible to configure a recording schedule or motion detection for recorder analog cameras.

Setting Up a Virtual Camera

It is possible to import offline video files (from wearable Cameras, action Cameras, drones, etc.) into Nx Witness archive and associate that footage with a *Virtual Camera* which can be viewed and processed like any other Camera in the Site. Frames pe Second (FPS) and bitrate recording options are inactive with Virtual Cameras.

NOTE: To be processed as a virtual camera, a imported media must have been produced with timestamp data.

As with any other camera, virtual cameras can be opened, deleted, and renamed. Virtual camera images can be rotated 0, 90, 180, or 270 degrees, can be dewarped, analyzed, and searched to detect motion. Like camera streams recorded by Nx Witness, videos uploaded using the virtual camera feature remain in the archive after the camera is removed from a Server.

> **NOTE**: Motion detection for Virtual Camera footage must be enabled during upload or it will not be available subsequently.

Once storage blocks for a given time period are filled with virtual camera content, they cannot be overwritten. For example, if file "A" was recorded from 11:32 to 11:37, and file "B" was recorded from 11:35 to 11:38 on the same day, if one of the two has already been uploaded, the other file will not be, as they occupy some of the same storage blocks in archive. If the selected file covers a period for which video is already uploaded, you can upload it to a different virtual camera instead.

To Add a Virtual Camera

1. Do one of the following:
   - Open the **Main Menu** and select **Add > Virtual Camera**.
   - Open a Server context menu and select **Add > Virtual Camera**
2. In the dialog that opens, select a Server from the drop-down menu.

   NOTE: Make sure the Server you select has enough storage space for the files being uploaded (see "Analyzing and Predicting Storage Usage"). If there is not enough available storage, the oldest existing archive may be deleted. Or, if the virtual camera footage is older than anything in archive, it will be uploaded and then deleted by the <storage management> service.

3. Enter a name for the virtual camera in the *Name* field.

   NOTE: If you do not enter a name, the default name "Virtual Camera" will automatically be appended with an integer that increments by 1.

4. Click *OK* to save or *Cancel* to exit without saving.
5. In the *Camera Settings* dialog that opens, you can proceed to upload files immediately or at a later point.

To Upload Files to a Virtual Camera

Once added, the virtual camera will be displayed in the Server Resource Panel, and files can be uploaded.

NOTE: Once uploaded, virtual camera files cannot be overwritten.

1. From the camera's context menu choose **Camera Settings**.

   NOTE: In the Camera Settings dialog, make sure to enable all upload setting first. Upload begins as soon as a file or folder is selected and you will not be able to enter settings such as motion detection or fixed archive length at that point.

2. If desired, use the **Default rotation** option to rotate the virtual camera footage by *90, 180* or *270 degrees*.
3. If desired, use the **Ignore timezone in uploaded files** option to make the uploaded file use the Desktop Client's local time instead of the time information found in the file.
4. Check **Enable audio** to include any audio tracks in the original footage.
5. Use the **Fixed Archive Length** fields to assign high or low priority to the virtual camera (see "Configuring Minimum and Maximum Archive Storage").
   - If there is not enough room in Server storage, setting a **Min Days** value will cause archived content with lower priority to be deleted in order to successfully upload files from the higher priority virtual camera. This setting can be crucial for a virtual camera, since oldest footage is deleted first and the virtual camera footage may be much older than material already in archive.
   - **Max. Days** sets an archive duration after which records will *not be saved* for the virtual camera.
6. If desired, check **Detect motion in uploaded video**, which will parse motion detection during file upload.

   NOTE: This option adds significant processing time.

   - If motion detection is checked, you have the option to also adjust the **Sensitivity** setting (see "Setting up Motion Detection").
7. Select **Upload File** to select a single file or **Upload Folder** to select all video files in a given directory.
   - If there is limited storage space on the server, you will get a warning message with a prompt to continue or cancel. There is also an option to cancel upload from *Camera*

Settings once upload is launched. If upload is canceled, any files that have already been uploaded will remain in storage.

- Upload will begin as soon as the file or folder is selected, and runs in background so you can perform other tasks simultaneously. An upload progress bar displays at the top of the *Camera Settings* dialog, and progress percentage is also shown in the Resource Panel.

8. Once upload is complete, the video will launch and play automatically.
   - If only virtual cameras are open in the layout, the Timeline will scale to show only the time interval spanning archive from those cameras. This is especially helpful when virtual camera footage is old and would be difficult to locate with the Timeline fully expanded to the present.
   - If an audio track exists but is not audible, ensure **Enable Audio** in **Camera Settings** > **General** is checked.

Working with NVRs

Nx Witness can work with a wide number of network video recorders (**NVRs**), however there are some special requirements:

- Hanwha NVRs require a specific Bridge License to work (however a professional license will work as well). Each Bridge License allows viewing one channel from the NVR.
- Cameras should be connected to NVRs and properly configured to display in Nx Witness.

After an NVR is configured and added, its channels become visible and it is possible to navigate through its live and archive streams. Some restrictions apply:

- NVRs do not support asynchronous playback, so the SYNC button on the Timeline has no effect.
- Only three simultaneous connections per channel are supported for archive playback. This means only three Nx Witness Client applications may request video from a certain channel. If an additional client tries to view archive from this channel, it will not be accessible.

Image Controls

Item windows display basic device information and provide icons for powerful built-in functions. Information and icons shown depends on whether the item is showing live or recorded video.

Upper Left

The upper left corner displays the camera name for live streams, or the file name for recorded video, and an icon for the current Recording Mode.

– Constant Recording (green circle)

– Motion Recording (red circle)

– Low Resolution always and High Resolution for motion (red circle with green diagonal stripe)

– Not Recording (grey circle)

Upper Right

The upper right corner contains the following buttons:

– Motion Smart Search.

– Screenshot.

– Creating a Zoom Window.

– Dewarping Controls.

– Object Search.

– Pan, Tilt, and Zoom Controls – for live streams, if supported by the device

– Hotspot

– Rotate

– Information – displays additional information about the device settings

– Close – removes the item from the current Viewing Grid.

Bottom Right

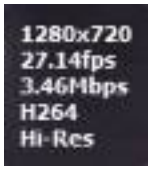
The bottom right corner indicates **LIVE** for live streams, or displays the date and running time for archive. If supported by the device you may also see:

– Using 2-Way Audio button

Custom Soft Triggers

Bottom Left

Click on the Information icon or right-click on any selected item to open the context menu, and choose **Show On Item > Info** (**Alt+I**) to display the following item information:



- Resolution of the stream in pixels
- Frames per second (FPS) of the stream
- Bitrate of the stream. The letter after the bitrate value is the video traffic delivery method indicator – Direct Connect, NAT traversal (N) and Proxy (P).
- Codec (e.g., H.265, H.264, or MJPEG). If "Hardware Decoding" (Intel Quick Sync) is enabled, the stream will display the (HW) indicator to the right of the stream codec.
- Stream in use – Hi-Res or Lo-Res.

Messages in place of Camera feed

- *OFFLINE* (see "Diagnosing Offline Devices").
- *NO DATA* – No recording was performed, no data is available.
- *Loading* – Awaiting data from server.
- *Unauthorized* – Incorrect/missing login or password.

Camera Rotation

Nx Witness can compensate for devices that aremounted upside down or rotated by either 90, 180, or 270 degrees. Rotation correction requires the transcoding of video exported from a Camera.

NOTE: Users must have the Resource Permission to Edit Device Setting grant directly or by Group membership (see "Users and Groups").

To Specify Device Orientation

Desktop Client

1. Open **Camera Settings** and go to the **General** tab.

2. In the **Image Control** section, select the desired rotation adjustment from the **Default rotation** options: *0 degrees*, *90 degrees*, *180 degrees*, *270 degrees*.
3. Apply changes.

Web Admin / *Cloud Portal*

1. Open **Settings** > **Cameras** and select a camera.
2. Open the *Rotation* drop-down menu.
3. Select the desired rotation adjustment from the default options: **0 degrees**, **90 degrees**, **180 degrees**, **270 degrees**.
4. Apply changes.

Image Enhancement

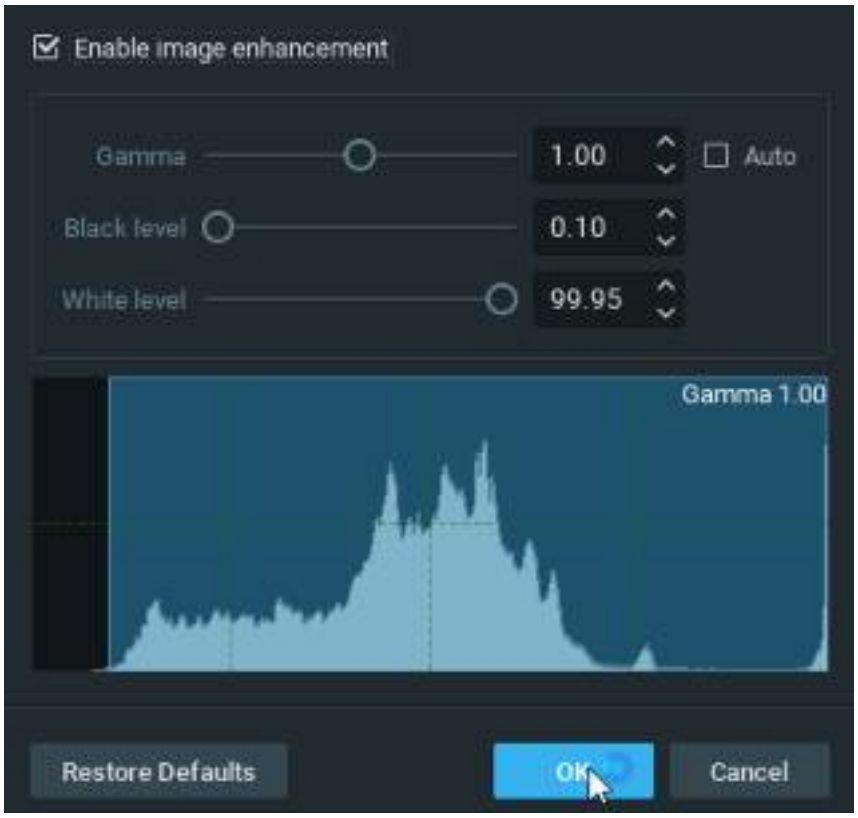
Image enhancement applies a set of adjustments to improve overall image quality. Select an image and open the Image Enhancement dialog using the context menu or hotkey (**ALT+J**).

Automatic Image Enhancement:

Use the default adjustment parameters that Nx Witness calculates (using a standard gamma correction algorithm) or set the parameters manually. In most cases, the default settings are adequate.

To Set Image Enhancement Parameters Manually

1. Right-click on the desired image and select **Image Enhancement** (**Alt+J**) in the context menu.



2. In the *Image Enhancement* dialog that opens, click the **Enable image enhancement** checkbox to turn image enhancement on. This will allow you to see the effect of your changes as they are made.

   NOTE: This setting is persistent and will the applied to all images where manual adjustment in enabled.

3. Set the following parameters:
   - *Gamma* – use the slider to adjust this value, where the lower the value the lighter the image will be. Check **Auto** to allow the gamma value to change to an optimal level as the other settings change.
   - *Black level* and *White level* – use the sliders to adjust these values, noting the impact on the histogram section. It is best to cover as much of the histogram area possible. If too much of the histogram is clipped on the left or right sides, important graphic information will be lost.
3. You can click **Restore Defaults** at any point to restore the default enhancement settings.
4. Click **OK** to save your changes or **Cancel** to discard them.

   NOTE: The current state of image enhancement is always applied to screenshots, and optionally to exported video (it can be turned off in the export settings).

Dewarping Controls

Some specialty lens known as Fish-eye lens capture a very large viewing area but also create a highly distorted image. Nx Witness provides a powerful dewarping algorithm that can be applied to flatten make a fish-eye image making it much easier to view.

Dewarping requires some initial configuration. Once configured a viewer can click on the dewarping icon  when the Camera is in a layout to toggle dewarp mode.

Configuring Camera Dewarping

- Configuring Camera dewarp can only performed by User with Permission to Edit Device Settings (see mode "Permissions Management")
- Keep the Camera open in Layout to view how its image changes as the dewarp settings are adjusted.
- Select the desired camera and open the **Camera Settings** dialog from the context menu.
- In the **Dewarping** tab, click on the **Dewarping** toggle to enable the distortion correction parameters; toggle turns Green with an (1)ON indicator when Enabled.
  - *Dewarping* – select dewarping type: Fisheye or 360° Equirectangular. If 360° Equirectangular, the only fields you can modify are α and β for Horizon correction.
  - *Mount* – indicate the mounting position of the camera to apply the proper dewarping algorithm for the camera's orientation: **Ceiling**, **Wall**, or **Floor/Table.** A wall mount setting allows for only a 180 degree panoramic view while Ceiling and Wall allow for a 360 degree panoramic view.
  - *Angle* – if the camera is not mounted in an exact vertical or horizontal position, you can adjust the mounting angle by -30.0 to +30.0 degrees to fix the distortion.
  - *Lens Projection* – improve fisheye dewarping precision by selecting the most suitable lens projection type:
    - *Equidistant*
    - *Stereographic*
    - *Equisolid*

NOTE: The equidistant dewarping setting can also be used to dewarp compatible 360° panoramic images and videos.

3. If necessary, position the blue calibration circle over the camera's field of view as accurately as possible. Click-and-drag to move the circle and use the mouse wheel to resize it.
4. Click **Auto Calibration** to apply the dewarping algorithm.
5. If needed, you can manually adjust the distortion settings:
   - *Size* – use the slider to change the size of the blue circle. You can also use the mouse scroll wheel to resize it.
   - *X Offset* – use the slider to change the position of the circle horizontally.
   - *Y Offset* – use the slider to change the position of the circle vertically.
   - *Ellipticity* – use the slider to adjust the shape of the lens (panamorph lens support).
8. Click **Apply** or **OK** when finished. To discard changes, click *Cancel*.

   NOTE: Using PTZ controls on a de-warped image does not cause the Camera to move or change PTZ position, only the calculated view is changed.

Viewing a dewarped Camera

Once dewarp is configured and enabled, the dewarping icon will be displayed on the camera image and PTZ-style controls can be used to move around the dewarped image without changing the Camera position (see "Keyboard Shortcuts"). Dewarping mode is disabled while motion search is active, the dewarping state remembered and reinstated when motion search is no longer active.

- Zoom windows created from a dewarped image are dewarped automatically.
- The current dewarping state is applied to screenshots, and it is possible to apply dewarping to a screenshot after it is captured: open the **File Settings** dialog from the context menu and select Dewarping.
- The option to apply dewarping to exported video can be turned on or off in the Export Video dialog using **Apply Filters**.
- Dewarping a camera will set its resolution to **High**.

1. Click the dewarping icon to toggle dewarping mode on and off:

2. Click the **Change Dewarping Mode** button in layout to show the image as a **90**, **180**, or **360** degree panoramic view, as indicated by the button.
3. Use PTZ-style controls can be used to move about the dewarped image without changing the Camera position (see "Pan, Tilt, and Zoom Controls").

   NOTE: Using PTZ controls on a de-warped image does not cause the Camera to move or change PTZ position, only the calculated view is changed.

To Dewarp Fish-eye or 360° Panorama Content

1. Right-click on the image or video file to open the context menu and select **Camera Settings**.
2. Click on the **Dewarping** toggle to Enable (slider turns green) the distortion correction parameters.
3. Configure dewarping as described above.

   NOTE: 360 degree panoramic mode is not available to cameras that are configured as wall mounted, 360° panorama content must use equidistant projection.

Pan, Tilt, and Zoom Controls

Nx Witness will present a PTZ Guide the first time PTZ controls are activated on a Site, unless the Alternate UI for PTZ has been enabled. Once viewed, the PTZ Guide will only be shown after navigating to **Main Menu > Local Settings > Advanced** and clicking on the "**Reset All Warnings**" button.

To the extent supported by a particular ONVIF camera, PTZ controls (Pan, Tilt, and Zoom) are available when the Camera is in Live mode. PTZ controls are also available on archived footage for fish-eye cameras that have dewarping enabled (see "Dewarping Controls").

Cameras that support **ONVIF Absolute Move** have the following features:

- Saving and Restoring PTZ Positions
- Setting Up PTZ Tours
- Relative PTZ

When PTZ requirements are met and enabled, the PTZ icon  will display on the corresponding camera item. See Adjusting PTZ Speed and Selecting PTZ Presets for more configuration options.

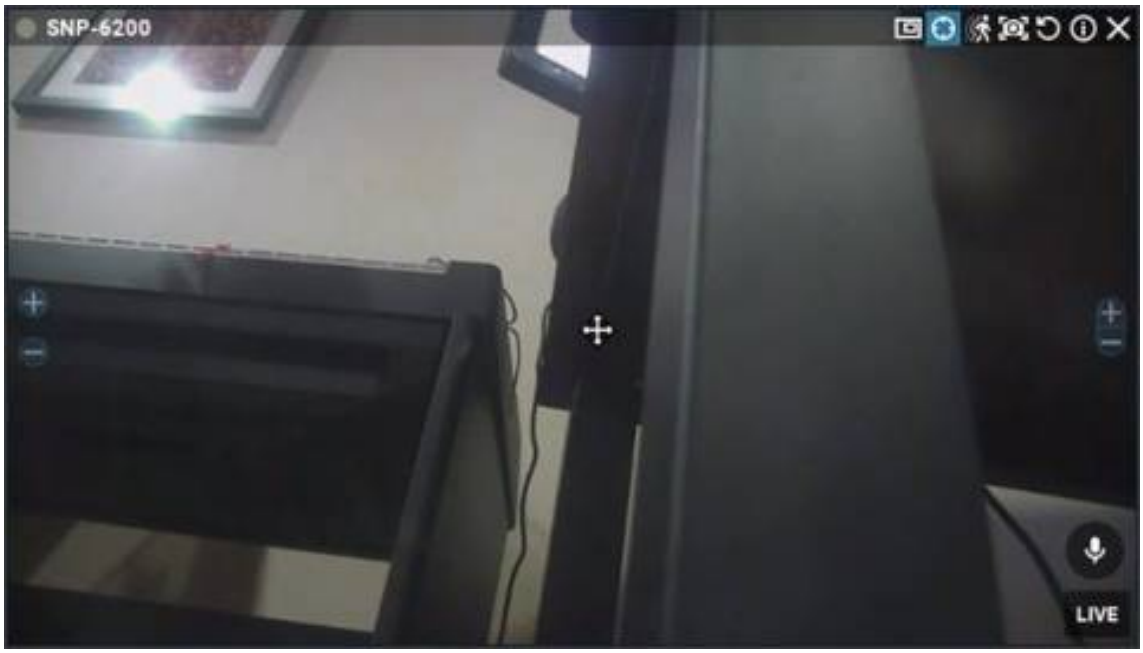
Manufacturer "Native" PTZ Settings

Native PTZ camera presets – those provided in-camera – for a specific camera can maintained by checking **Use camera native presets** in **Camera Settings** > **Expert**. To ignore manufacturer settings in favor of Nx Witness settings, check **Use site presets** instead.

Default UI for PTZ controls

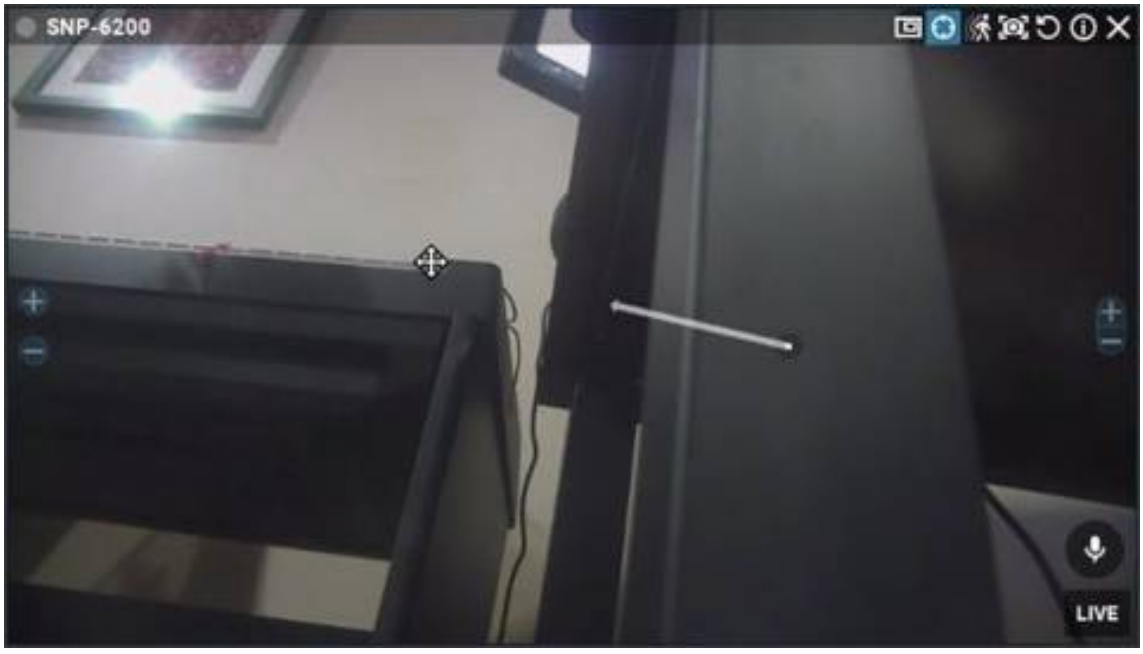
Depending on the camera model, one of the following modes is available when you click on the PTZ icon  .

Simple (**Zoom** only) – Use the mouse wheel or +/- keys to zoom.



Regular (**Zoom** and **Point**) – In addition to the zoom functionality from *Simple* mode, press the arrow keys or drag over any part of the video to point (pan/tilt) the camera.

.



Advanced PTZ (**Zoom**, **Point** and **additional features**) – In addition to the zoom and point functionality from *Regular* mode, *Extended* mode requires a custom product integration and ONVIF Absolute Move support from the camera. Extended mode allows the following additional controls:

- **Shift + Click** anywhere in the field of view to re-center at that position.

- **Shift + Click-and-drag** and draw a zoom rectangle that can be positioned until the mouse button is released.
- **Shift + Double-click** to zoom out all the way.

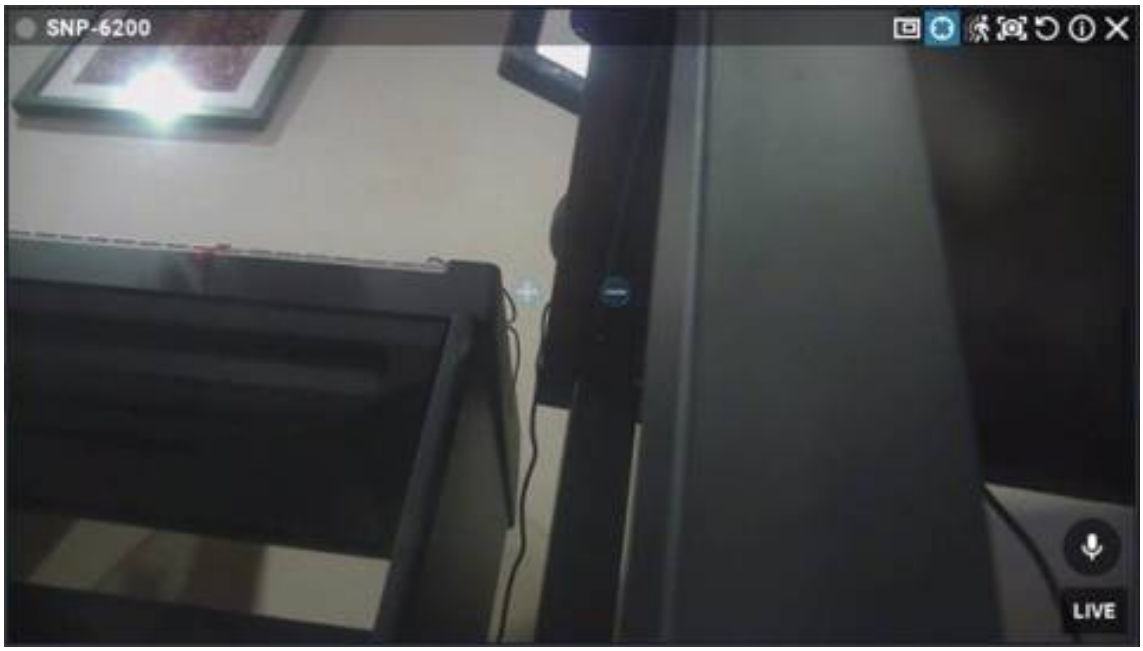
Alternate PTZ Controls

Enable the alternative UI for PTZ controls by selecting the checkbox next to "Show aim overlay for PTZ cameras".

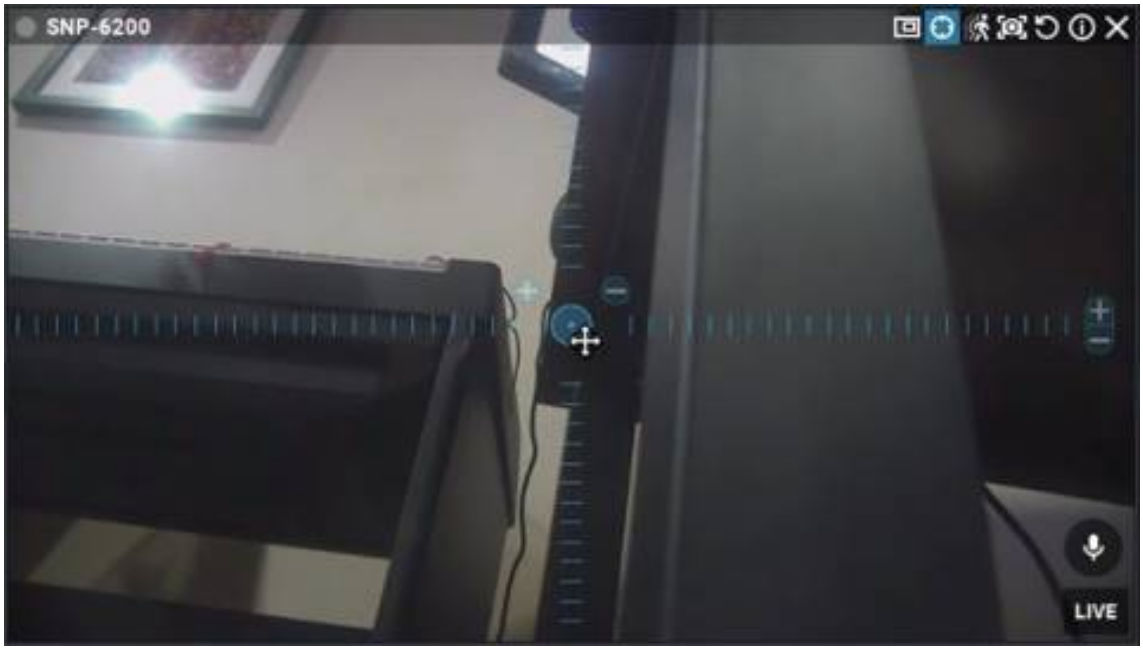
NOTE: The PTZ Guide will not be shown if the Alternate UI for PTZ is enabled.

Depending on the camera model, one of the following modes is available when you click on the PTZ icon .

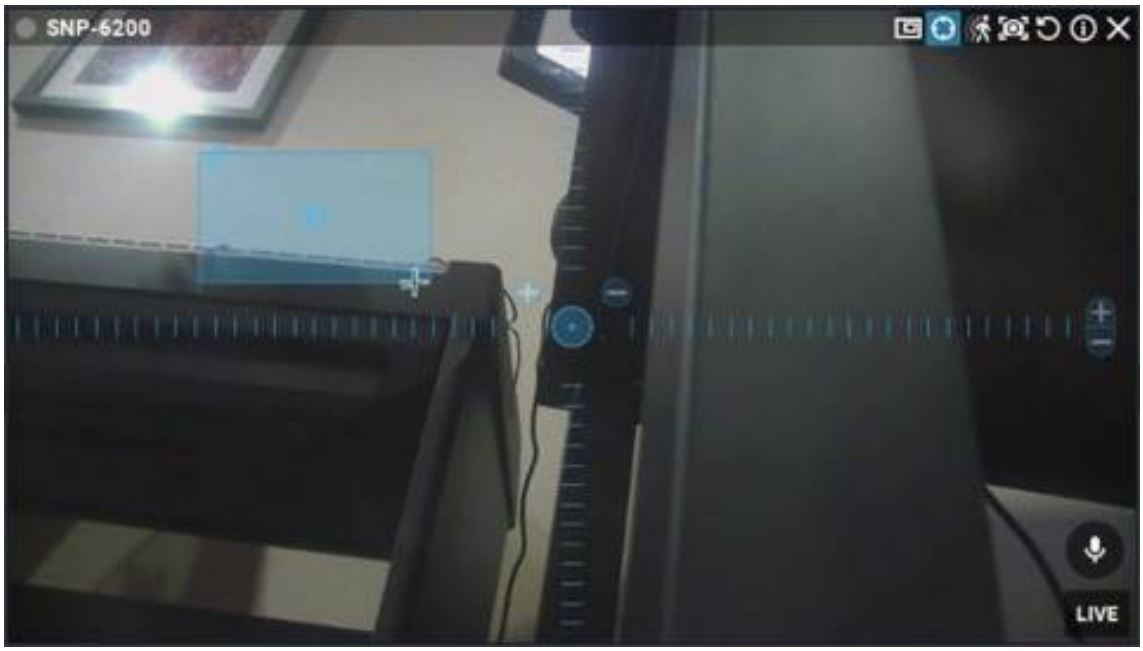
Simple (**Zoom** only) – As shown in the image below, only the **+** and **-** buttons are available to zoom in and out.



Regular (**Zoom** and **Point**) – Use the **+** and **-** buttons to zoom in and out. When there is a center circle as shown below, you can use it to click-and-drag the center of the image to the desired position.



Extended (**Zoom**, **Point** and **additional features**) – Requires a custom product integration and ONVIF Absolute Move support from the camera. Allows zooming, repositioning, and the following additional controls:



- **Click** anywhere in the field of view to re-center at that position.
- **Click-and-drag** and draw a zoom rectangle that can be positioned until the mouse button is released.
- **Double-click** to zoom out all the way.

Once a PTZ position is set, press again to hide PTZ controls.

Saving and Restoring PTZ Positions

It is possible to establish predefined PTZ positions that can be restored in just a few clicks or with a Keyboard Shortcut.

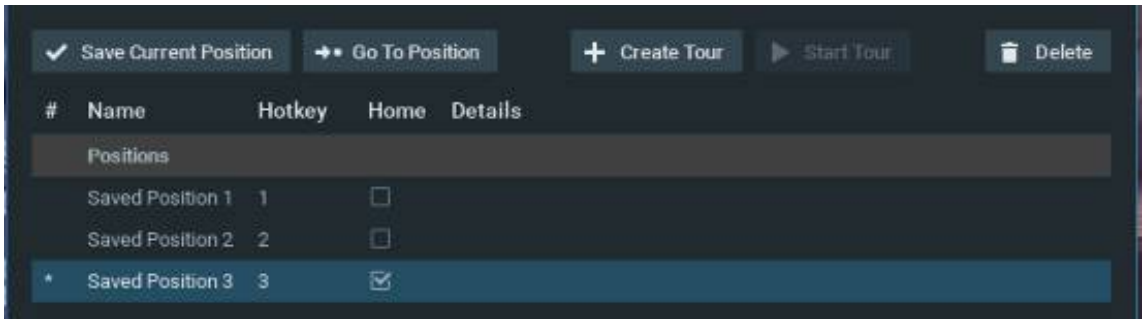
Once defined, a preset PTZ position can serve as the home position for a device, or several presets can be sequenced to create a PTZ tour (see "Setting Up PTZ Tours"). There is also an "Execute PTZ Preset" action for event rules.

To Save a PTZ Position

1. Click on the PTZ icon in layout and go to the desired position.
2. From the camera item in layout, open the context menu and select **PTZ** > **Save Current Position**.
3. Enter a name or accept the default name.
4. Optionally, select a hotkey for the position (**0**-**9**).

To Edit a Saved PTZ Position

1. From the camera item in layout, open the context menu and select **PTZ** > **Manage**. It is a good idea to move the *Manage PTZ* dialog so the camera item is clearly visible in layout.
2. The **Name** and **Hotkey** fields in the *Manage PTZ* list are editable fields.



3. If desired, click the **Home** checkbox to select the position the camera will return when the PTZ position is not changed for 2 minutes. (You can use the **Go To Position** button to preview a preset position.)
4. It is possible to add a new preset by clicking on the PTZ icon in layout and clicking **Save Current Position in** the *Manage PTZ* dialog.
5. Click *Apply* or *OK* when finished. To discard changes, click *Cancel*.

To Restore a PTZ Position

Open the camera context menu and choose **PTZ** > **<position name>** or press the related hot key (**0-9**). The active position will be indicated in the PTZ context menu.

To Delete a PTZ Position

1. Open the camera context menu and select **PTZ** > **Manage**.
2. Select a desired preset and click **Delete**.

   NOTE: If a preset position is included in a PTZ tour, deleting it will make the tour invalid. The tour will remain in the list in the *Manage PTZ* dialog but will not be available from the PTZ context menu.
3. Click *Apply* or *OK* when finished. To discard changes, click *Cancel*.

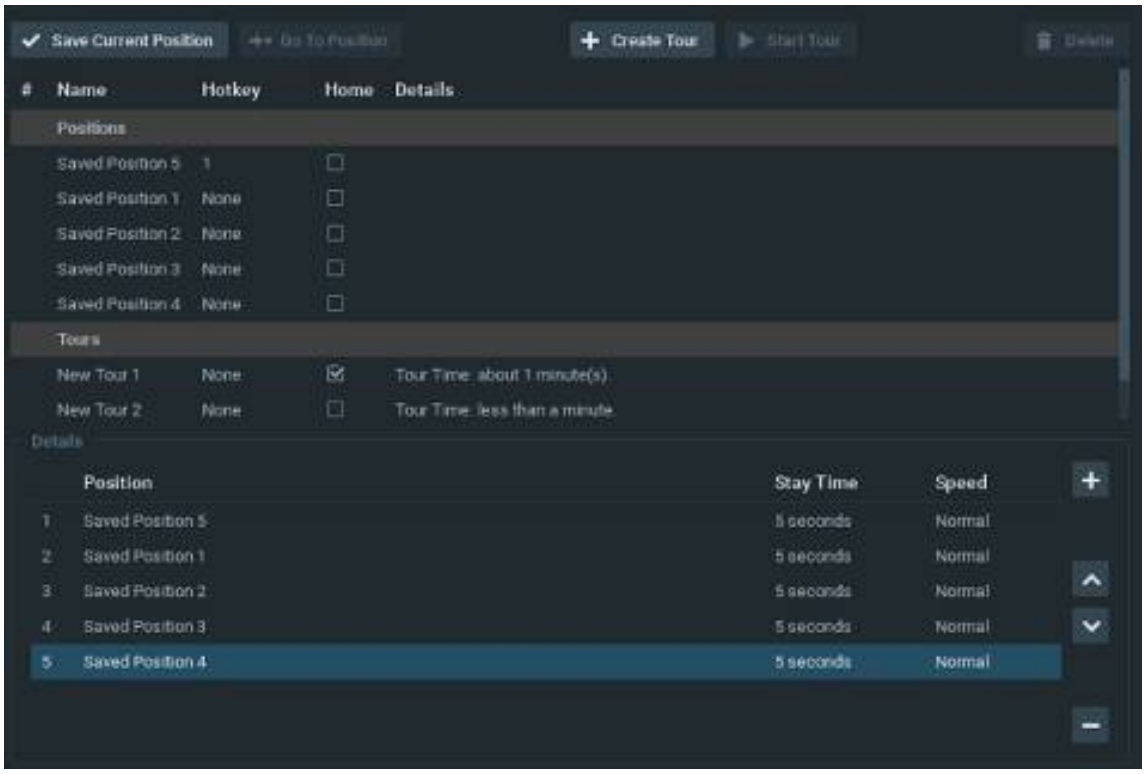
Setting Up PTZ Tours

A **PTZ tour** is a sequence of saved PTZ positions. PTZ tours are useful for observing a broad field of coverage with a single camera. The following requirements apply:

- Can only be applied to a PTZ or fish-eye camera
- Must contain at least two positions
- The same position should not be used consecutively or as both the first and last position. A warning will appear if a tour contains multiple instances of the same position. Instead, define and use slightly different or overlapping PTZ presets.

To Create a PTZ Tour

1. Right-click on the camera item in the layout and select **PTZ** > **Manage** from the context menu.



2. Make sure at least two positions are saved.
3. Click the **Create Tour button**. A *Tours* section will open at the end of the position list, with a default name *New Tour <#>*.
4. In the *Details* form, click the **+** button to add the first position to the tour. Continue to click **+** until you have added all desired positions.
5. Each tour position can be edited as follows:
   - Click on the **Stay Time** field to select the display duration for a position.
   - Click on the **Speed** field to set the speed of the move from one position to the next.
   - Click on the **Position** field to select a different position.
   - Use the **up and down arrows** at the right to change the order of a position in the tour.
   - Click the **+** button to add a position.
   - Click the - button to delete a position.
4. Click *Apply* to save the tour then click the **Start Tour** button to test it.
5. Optionally, rename the tour using the list **Name** field or assign it a **Hotkey**.
6. Optionally, check the **Home** box. The home tour will be activated on a camera automatically if there is no active PTZ tour.
7. Click *Apply* or *OK* when finished. To discard changes, click *Cancel*.

<u>To Start a PTZ Tour</u>

1. From the camera item in layout, open the context menu and select **PTZ**.

2. Select the desired tour from the list of saved tours (which is below the list of saved positions).
3. Alternately, open the context menu, select **PTZ** > **Manage**, highlight the desired tour in the list and click on **Start Tour**.

To Stop a PTZ Tour

A PTZ tour cannot be toggled on and off, it must be replaced with a static PTZ position. Either enable PTZ controls on the camera item and choose a PTZ position manually or choose a saved PTZ position (select one from the context menu or use a hotkey).

Recording

Video archiving begins once you enable recording, set image quality parameters, and specify a recording schedule.

NOTE: Frames per Second (FPS) and quality settings in the recording schedule dictate live stream settings.

Audio can be recorded as well as image if the device has, or is connected to a microphone, and the **Enable Audio** checkbox in **Device Settings** > **General** > **Audio** is checked (see "Configuring Audio on a Device"). It is possible set a recording schedule for an I/O module as well (see "Setting Up I/O Modules").

When recording is enabled, Nx Witness automatically seeks an available License or Service. If one is available, the stream from device will be recorded. If not, you will be warned that the License or Service limit is exceeded and only schedule copy will be available.

See Setting a Recording Schedule for details on the scheduling interface.

Recording Indicators in the Resource Panel

When recording is enabled, the device is marked with a small red circle to the left of its name in the Resource Panel:

- – A solid red circle indicates camera is recording.
- – A red circle outline indicates a recording schedule is established but the camera is not recording at the moment; a License or Recording Service is still being used even though the device is not currently recording.
- – A gray circle outline Indicates camera is not recording but some recorded archive is available.

Setting a Motion Detection Region

You can control the image regions that will trigger motion detection, and how sensitive to motion those regions will be (see "Setting up Motion Detection").

Setting a Recording Schedule

The *recording schedule* is where you define when and at what quality a device will be recorded, using a weekly calendar divided into 1 hour blocks.

The recording schedule is always based on VMS time. When *Motion Detection* is enabled, you can set regions of the image that will register motion, and how sensitive to motion those regions will be (see "Setting up Motion Detection").

NOTE: If recording is *not* enabled, motion detection will only be active when the camera is being viewed in a layout.

Remember that image quality settings in the recording schedule dictate image quality in live playback as well.

> **NOTE**: If no license is available, the "License is required" error will appear above the recording schedule and prevent recording from being enabled. The recording schedule and settings will be inaccessible until a valid license is added.

To Set a Recording Schedule

Desktop Client

1. Select the desired camera(s) in the Resource Panel or in layout.

   NOTE: The Recording Schedule comes with the following settings by default: Motion Only, High Quality, and Max FPS.

2. Choose **Camera Settings** in the context menu and go to the **Recording** tab.
3. Click the **Recording** button at the upper-left to enable recording.

   NOTE: The total number of licenses available and the number of licenses in use is displayed below this button. If the number of available licenses is insufficient, you can click the **Activate License** button and proceed with activation.

4. If desired, set the frames-per-second (**FPS**) rate and **Quality** (*Low*, *Medium*, *High*, or *Best)* that will apply to the device(s). When available for the selected device, you can also adjust the **Bitrate** by clicking on *More Settings*.

   NOTE: If changes to streamed settings are prohibited at the Site level (see "Preventing Nx Witness from Changing Device Settings"), image quality settings in the recording schedule are ignored (the **FPS** and **Quality** fields will be disabled).

5. If desired, check the eye icon to toggling viewing of the **Show Quality** and **Show FPS** to display the respective values in the recording schedule Calendar.
6. If desired, adjust the length of time that will be added to the recording before (**Pre-Recording**) and after (**Post-Recording**) motion or an object is detected. Pre-Recording can be set up to 90 seconds, and Post-Recording can be set up to 300 seconds.
7. If desired, use the *For...* fields to assign high or low priority to the camera's archive.

   NOTE: It is best to leave **Minimum** and **Maximum** set to **Auto** unless you have specific related requirements (see "Configuring Minimum and Maximum Archive Storage").

8. Select the desired Recording Type – *Motion*, *Objects*, or *Motion & Objects*. This selection will change the type of Recording Modes to choose from.
9. Select the desired Recording Mode:
   - *Record Always.*
   - *Motion Only* / *Objects Only* / *Motion & Objects Only.*
   - *Motion + Lo-Res* / *Objects + Lo-Res* / *Motion & Objects + Lo-Res.*
   - *Do Not Record.*

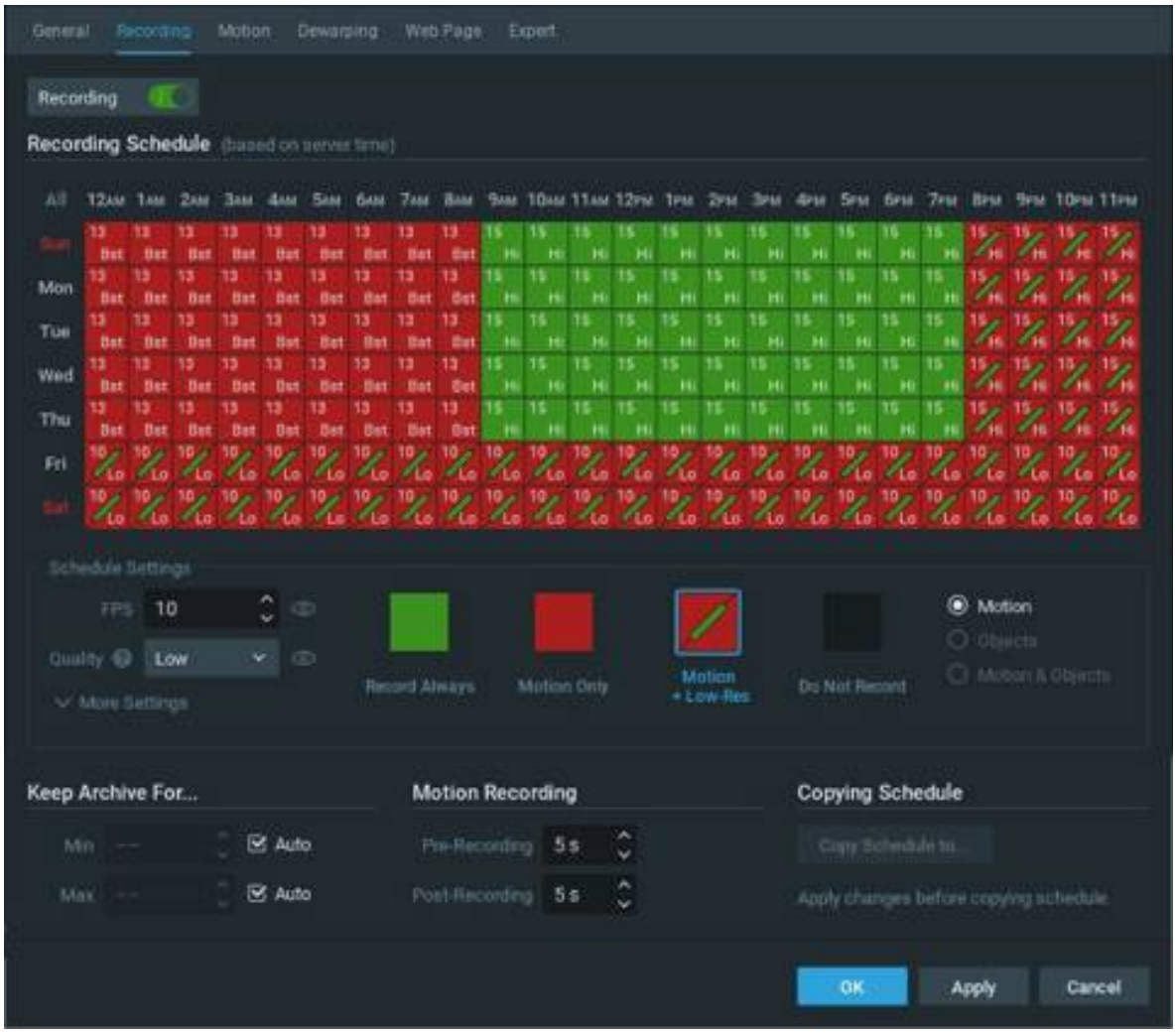
   A blue outline around the button indicates the active recording mode (see "Recording Modes").
10. Once the above parameters are set, click hour blocks in the calendar to apply a recording mode:
    - Click-and-drag to select multiple time blocks.
    - Click on an hour number to select that block of time for an entire week.
    - Click on a day name to select an entire day.
    - Click **All** to select the entire week.

    NOTE:You can use **Alt + Click** to copy the recording mode in a given block so it can be applied to a different block.

    IMPORTANT: First choose FPS, Quality and bitrate values and then apply them to the calendar. Stream setting values are not in effect until time block(s) are selected.
10. Repeat the above steps as desired to schedule other recording modes.

    NOTE: The quality settings are independent of the recording mode. (This is illustrated in the example below, where some Motion + Lo-Res blocks are at 15 FPS/High quality and others are at 10 FPS/Low quality.)
11. Apply changes.

Example



This example uses the following settings:

- Mon – Fri, 9:00 AM-7:59 PM – Record Always, 15 FPS, High quality.
- Mon – Fri, 8:00 PM-11:59 PM – Motion + Lo-Res, 15 FPS, High quality.
- Fri & Sun, 24 hours – Motion + Lo-Res, 10 FPS, Low quality.
- Mon – Fri, 12:00 AM-8:59 AM – Motion Only, 13 FPS, Best quality.

Recording Modes

The recording schedule provides the following modes, which can be applied in 1 hour blocks:

- *Record Always* – Always records.
- *Motion Only* – Recording will start if motion occurs. Requires that the camera support hardware or software motion detection.

 *Motion + Lo-Res* – Records at low resolution unless motion occurs, at which point it automatically switches to recording at high resolution. The camera must support dual-streaming to be able to use this Motion + Lo-Res mode. If it does not, the following warning will be displayed: *Dual-Streaming and Motion Detection is not available for this camera* (see "Dual Stream Processing" for details).

 *Do Not Record* – Never records, unless configured as part of an event.

Remember, image quality settings in the recording schedule dictate image quality during live playback.

For example, if the recording quality in the schedule is set to 4 frames per second and Low Quality, Nx Witness will stream the live image at those settings – even if the camera is capable of higher quality playback. However, when recording is turned off in the schedule, Nx Witness will stream live at the maximum possible quality and frames per second settings for the device.

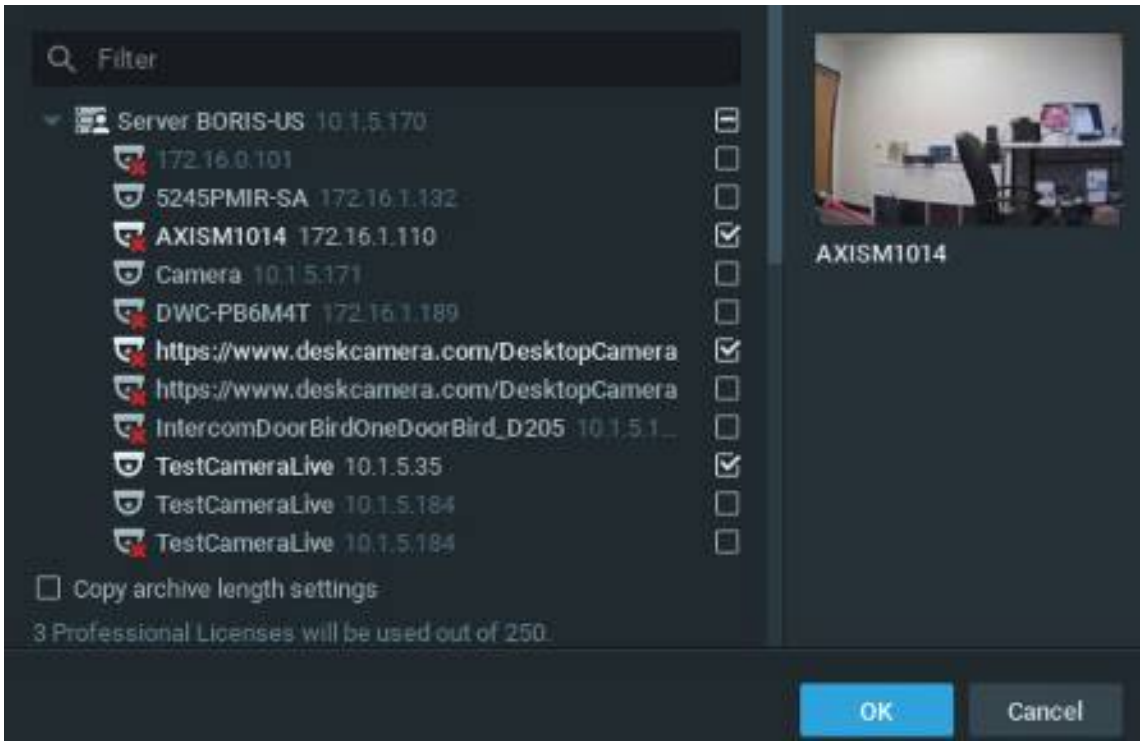
Copying a Recording Schedule

Once a recording schedule is configured for one device the settings can be copied to other devices.

NOTE: A license is required for each device to which the recording schedule is copied. As you select devices, a dynamic message will indicate how many licenses are in use and how many are available.

To Copy a Recording Schedule

1. Open the context menu for the camera where the desired schedule is defined and select **Camera Settings**.
2. In the **Recording** tab, click the **Copy Schedule to** button.



3. In the *Select Cameras* dialog that opens, check the camera(s) to copy the schedule to, or check a Server to copy the schedule to all cameras on that server.

   Use the *Filter* box to filter the device search (see "Searching and Filtering in Nx Witness"). Hover the mouse cursor over a camera name to see a thumbnail of the camera's image.
4. If desired, check **Copy archive length settings** (see "Configuring Minimum and Maximum Archive Storage").
5. Apply changes.

Configuring Archive Storage

Nx Witness provides the ability to set a maximum and minimum storage duration for the archive of any given camera, from the current time going backwards.

Before you use a *Keep Archive For* setting, it is important to understand the impact it will have. The default *Auto* setting means that archived footage for a given camera is treated according to the standard algorithm – the oldest data is deleted first. No controls are placed on when or which archived footage is deleted.

The *Min* and *Max* fields assign priority to a given camera – high priority for Min, low priority for Max. If more than one camera is assigned high or low priority, storage results may not be predictable. Typically the *Min* setting is used for environments with limited storage capacity and a few high-importance cameras, or when a regulation requires that certain footage be stored for a minimum amount of time. *Max* is typically used for environments where storage is limited and there is no need to store records beyond a certain age from certain cameras.

It is not possible to enter a Max value less than the Min value, and vice versa.

Minimum (Days. Hours, Minutes)

Min sets a minimum archive length, in number of days. hours or minutes from the current date, for which Nx Witness gives highest priority to retention of records from a given camera over retention of records from any camera that has the default (*Auto*) archive setting.

For example, a *Min. Days* value of 120 for a given camera means Nx Witness will attempt to preserve the past 120 days of records from that camera.

NOTE: *Be careful when setting a minimum days value.* If more than one camera is assigned a *Min. Days* value, those cameras will have the same priority level – in which case storage results cannot be entirely guaranteed for any of them. If there is insufficient storage space, in order to retain footage as specified with *Min*, Nx Witness will first delete records from cameras that do not have a minimum archive length set, and then the Site may stop recording incoming signals from low and average priority cameras. If storage space is at capacity, no other camera streams will be recorded.

Maximum (Days. Hours, Minutes)

Max sets an archive duration after which records will not be saved for a given camera.

To Configure Minimum and Maximum Storage Duration

1. Go to the camera's context menu from the Resource Panel or layout and open **Camera Settings** > **Recording** tab (or the **General** tab for Virtual Cameras).
2. In the *Fixed Archive Length* section, uncheck the **Auto** checkbox.
3. In **Min**, enter the amount of time for which archive should be retained.
4. In **Max**, enter the amount of time after which archive will be automatically deleted from storage.
5. Click *Apply* to accept, *OK* to save and close the dialog, or *Cancel* to discard changes.

Advanced Device Settings

Nx Witness provides advanced controls so you can view and configure manufacturer parameters such as video stream configuration, image or audio settings, or network configurations either from within the Desktop Client or by opening the manufacturer's device web page.

This section describes the following features:

- Configuring Device Advanced Settings Using Nx Witness
- Configuring Device Using Web Page
- Resetting or Rebooting a Camera

More device settings are explained in the "Expert Device Settings" section.

Configure Device Setting within the Client

To Edit Basic Proprietary Settings

1. Open **Camera Settings** and go to the **Advanced** tab.
2. Available controls are determined by the specific camera model. Settings are grouped by category:
   - *Video Streams Configuration* – Use to control **Codec** and **Resolution** for the primary and secondary streams in addition to **Bitrate** and **FPS** for the secondary stream. These values can be separately **Reset to Defaults** for each stream.
   - *Imaging* – Use to adjust **Exposure** and **Extra Settings** (such as line frequency), if available for the camera.
   - *Audio* – Typically includes audio-in sensitivity and audio-out volume.
   - *Maintenance* – Use to perform various levels of camera reboot. See "Resetting Camera" for details.

   NOTE: If no device settings are displayed, the camera is not ONVIF-compliant and cannot support custom configuration.

In addition, for the most commonly-used cameras, Nx Witness also provides a **Web Page** tab in the **Camera Settings** dialog. This tab launches the device's web page, where you can configure additional proprietary device parameters such as in-camera events, security controls, and network settings – see "Configuring Device Using Web Page".

Configuring Device Using Web Page

Key Concepts:

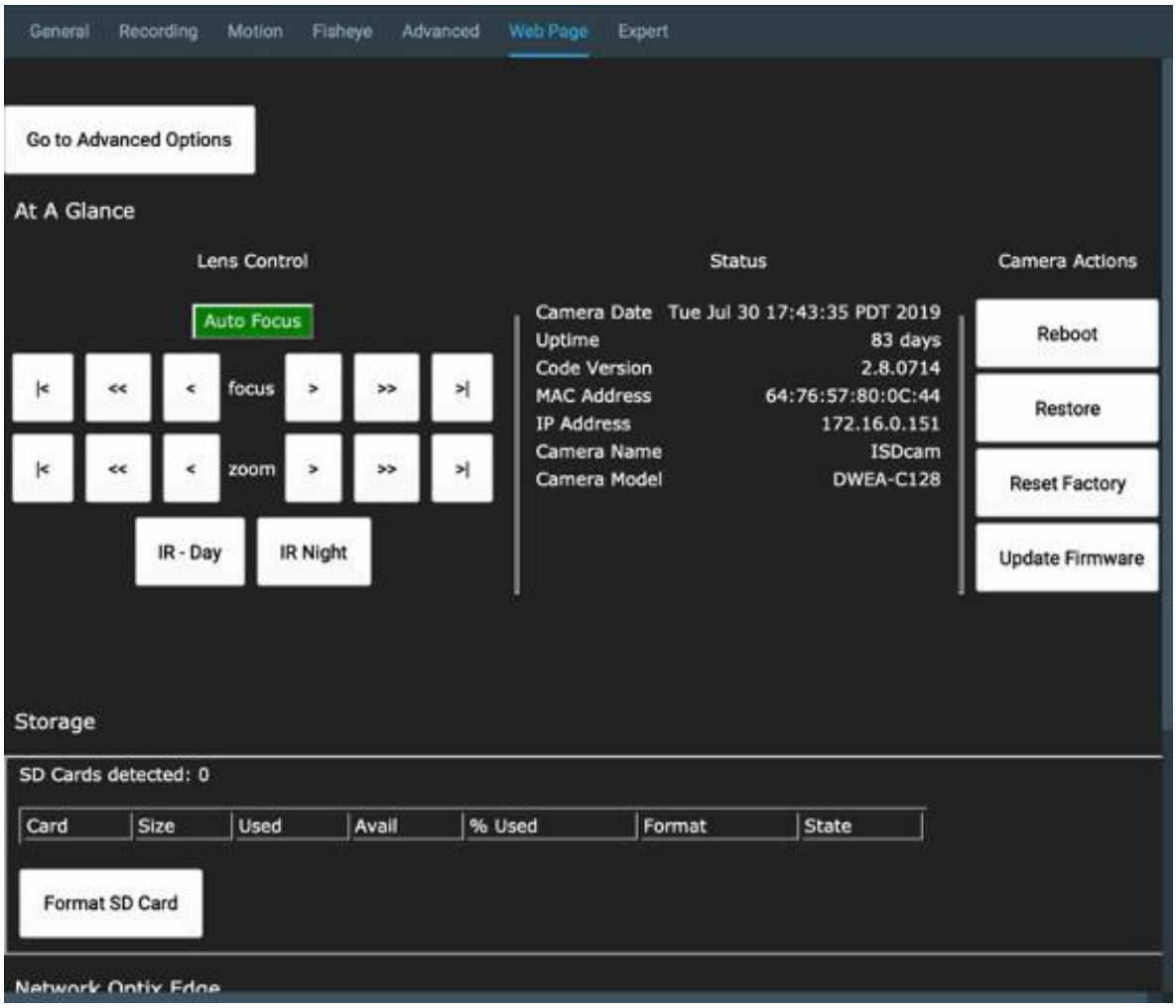
- The Nx Witness can be open most browser-based configuration interfaces that are embedded in devices.
- Any configuration service or interface embedded or hosted within a device must be compatible the Google Chrome.
- Configuration options provided by device hosted interfaces may differ from those available within Nx Witness clients and portals.
- The Server functions as a proxy Server to retrieve the device web page content and display it within the Desktop Client.
- Use either the Web Page in the device settings dialog or a Web Pages and Integrated into web-page integrated to a layout or scene.
- embedded device hosted c

N

For all camera vendors, Nx Witness provides direct access to a camera's web page where users can configure the camera's settings witho ut leaving the Desktop Client. If the device cannot be accessible from the computer Desktop Client is running on, Nx Witness Server acts like a proxy Server to retrieve the device web page content and display it within the Desktop Client.

In some cases, if a custom integration with a camera has been implemented, Nx Witness pulls proprietary device parameters such as authorization, network settings, and displays controls into the Desktop Client where they can be configured directly.

See the below image for one example of such a web page (can vary depending on the manufacturer).



By default, the web page is available on the standard port (80). In case of using a non-standard port, it should be configured in on a device's "Expert" tab (see "Device Expert Tab").

From the General tab

1. Select a camera and open the **Camera Settings** > **General** tab.
2. If the device requires authentication, enter camera credentials in the **Authentication** section (see "Configuring Device Authentication"). You must have the "Edit camera settings" permission to perform this function.
3. Click on the **Web Page** link. The browser will open the device's web page. From here you can control settings such as display size, JPEG refresh rate, PTZ and focus speed, etc.

   NOTE: To check device accessibility, press the **Ping** button prior to opening the web page.

From the Web Page tab

1. Select a camera and open the **Camera Settings** > **Web Page** tab
2. The device's web page will open within that tab.
3. Enter authentication parameters if required.

Resetting or Rebooting a Camera

Most ONVIF-compliant cameras offer a methods to reboot or reset the device. This can be performed using the camera's configuration tool or from within the Desktop Client by following the steps outlined below.

1. Select the camera to reset and open the context (right-click) menu.
2. Open **Camera Settings** and select the **Advanced** tab.
3. Select **Maintenance** in the left side menu under the heading **Category** (This category may be empty for unsupported or non-compliant cameras).
4. Click one of the labeled buttons to instantly send the command to the camera.
   - *System Reboot* – reboots the camera but saves current settings.
   - *Soft Factory Reset* – reboots the camera and restores all settings related to the image but not the IP address.
   - *Hard Factory Reset* – reboots the camera and restores all settings (Network, Authorization, IP address, etc).

NOTE: All options might not be available for all devices.

Expert Device Settings

Nx Witness provides expert settings that can resolve some issues on the device side.

- Configuring Expert Streaming Settings
- Time Synchronization between Servers and Cameras
- Assigning Logical ID
- Adjusting PTZ Speed

- Selecting PTZ Presets

NOTE: Improper configuration may lead to serious Site malfunction! Do not change these settings without fully understanding the potential impact on your Site.

Stream Settings

Nx Witness Server automatically configures the optimal streaming parameters to configure how devices will stream data.

However, in some cases the automatic settings may work improperly and require manual tuning.

This section describes how to set various streaming parameters manually.

NOTE: By default, Nx Witness captures 2 streams from cameras (see "Background: Dual Stream Processing"). Before changing the settings manually, please make sure you understand how the dual-streaming works.

- Preventing Nx Witness from Changing Device Settings.
- Configuring ONVIF Profiles.
- Tuning up Camera Streaming.
- Adjusting Average Bitrate.
- Forcing Motion Detection to a Specific Stream.
- Disabling Recording of a Specific Stream.
- Disabling a Secondary Stream.

1.7.9.1.1 About Dual Stream Processing

Most IP cameras can provide multiple data streams, each at a different resolution and frame rate. Nx Witness requests two data streams, one high resolution and one low resolution, and switches between them for the best image quality with the least impact on processing and network efficiency.

This *adaptive scaling* is one of the most valued features of the Nx Witness:

- *Primary (High-Resolution)* – Streams provide better image quality, but require significant CPU capacity and network bandwidth to view.
- *Secondary (Low-Resolution)* – Streams require far less computing power than typical high-resolution streams, but provide much lower image resolution at a slower frame rate.

When a camera supports dual-streaming, the Site tries to configure the low-resolution stream at or near 640x360 resolution at 7fps (though some cameras may set secondary stream resolution at up to 720p). The secondary stream is used for constant recording, for motion detection (as long as the resolution is less than 1024x768), and to save bandwidth and CPU during playback.

However, if the secondary stream resolution is more than 1024x768, the Media Server will check the primary stream resolution. If the primary stream is less than or equal to 1024x768, it will be used for motion. If it's higher than 1024x768, motion detection will be disabled unless **Force motion detection for the stream** is enabled in **Camera Settings** > **Expert** tab.

Default Nx Witness dual stream settings work well with most cameras. If not, a set of individual controls can be used to manually control stream processing. It is important to understand how these settings behave individually and together, as adjusting them can seriously affect Server and display performance.

NOTE: Do not change image or stream quality settings unless you are absolutely sure of the likely impact on Site performance.

Dual Streaming on the Server

The Server uses the low-resolution stream whenever possible for software motion detection and records both streams to archive unless a different behavior is specified. However, some cameras may not or cannot comply with default Site behavior, usually for one of these reasons:

- Requested settings are not available from the camera.
- The lowest resolution stream is higher than 1024x768p.
- A secondary or low-resolution stream is not provided at all.
- A low-resolution stream is provided as Primary and a high-resolution stream as Secondary.

NOTE: If data is not received from the secondary stream for more than 10 seconds, the Sever will re-initialize the camera.

Dual Streaming on the Client

On the Client, stream resolution for viewing live or archive video is selected automatically.

- High Resolution is displayed under the following conditions:
  - Network bandwidth and CPU load are within normal range.
  - An item is pulled into Fullscreen display.
- Low Resolution is displayed under the following conditions:
  - If network bandwidth between client and Server is insufficient.
  - When image quality is of limited importance: items smaller than 172 pixels, during fast forward or fast rewind playback.
  - When high resolution processing compromises display quality or raises CPU usage to a high level (frames are delayed or dropped during decoding if there are too many streams are open in a given layout).

Settings That Affect Motion Detection

Motion detection is performed on the lowest resolution stream detected, to a threshold of ≤ 1024x768p. Above that, motion detection will not be performed.

- *Motion Detection* – Toggles motion detection on and off for a given camera (see "Setting a Recording Schedule").
- *Disable secondary stream* – If enabled, motion detection will not be performed for the camera, and the secondary stream will not be archived (see "Disabling a Secondary Stream").
- *Force motion detection for stream* – Occasionally, a camera will report its configuration incorrectly and swap the primary and secondary streams. If the secondary stream is high-resolution, motion detection processing will create a very high CPU load. To correct this you can force motion detection to a specific stream (see "Forcing Motion Detection to a Specific Stream").

Settings That Affect Recording and Playback

When certain settings are applied, the Server may or may not archive high-resolution or low-resolution streams.

- *Motion + Lo-Res* – Archives the high-resolution stream when motion is detected and the low-resolution stream when there is no motion, so high-resolution will not always be available for playback (see "Setting a Recording Schedule").
- *Disable secondary stream* – If checked, motion detection won't be performed for the camera, and the secondary stream won't be archived (see "Disabling a Secondary Stream").
- *Do not record primary stream / Do not archive secondary stream* – Use to completely disable archiving of one or both streams (see "Disabling Recording of a Specific Stream").
- *Video Streams Configuration* – Depending on the camera, camera stream settings may be configured in the either of these tabs (Camera Settings > Advanced or Camera Settings > Web Page tab). If you choose to control stream settings from one of these tabs you must do *one of the following*:
  - Open **Camera Settings > Expert** and enable **Keep camera stream and profile settings** to prevent the internal optimization performed by Nx Witness, and causes FPS and image quality settings in the Recording Schedule to be ignored. See "Preventing Nx Witness from Changing Device Settings".
  - Open **Site Administration > General** and disable **Allow Site to optimize device settings**.

Refer to "Configuring Device Advanced Settings Using Nx Witness" and "Configuring Device Using Web Page" for how to use **Restore Defaults** (Expert Tab) to discard manual adjustments and return to native presets.

If performance has dropped significantly after a given layout was opened and some cameras on layout have a fixed high resolution setting, the message "*Set layout resolution to "Auto" to increase performance*" will display across that layout so you can improve streaming quality yourself.

1.7.9.1.2 Automatic Optimization Control

When Nx Witness discovers a camera, it captures the manufacturer's preset image quality settings and streaming configuration, then adjusts these settings to optimize the device for the Nx Witness Site. Manufacturer settings can also be adjusted manually, for example FPS, quality, and bitrate when a recording schedule is defined, or stream settings for a variety of reasons (see "Dual Stream Processing").

However, in some cases, it may be preferable to keep the native settings. For instance, you may want to maintain pre-existing FPS, bitrate, and resolution settings when connecting Nx Witness to another VMS Site. Or, on occasion the ONVIF implementation for a given camera diverges from standard ONVIF enough to make it preferable, or even necessary, to keep the manufacturer settings.

It is possible to prevent the automatic optimization that Nx Witness performs and use native stream and profile settings instead.

To disable automatic optimization for a single camera

1. Open **Camera Settings** and go to the **Expert** tab.
2. Check **Keep camera stream and profile settings**.
3. Apply changes.

NOTES:

- This setting is not available for RTSP/HTTP streams.
- Enabling this flag means FPS and image quality settings in the recording schedule will be ignored.

To disable automatic optimization for all cameras

It is possible to do this during the Initial Site Configuration.

Later, it can be done as follows:

Desktop Client

1. Open **Main Menu** and go to **Site Administration** > **General** tab.
2. Uncheck the **Allow Site to optimize device settings** checkbox.
3. Apply changes.

NOTE: For each camera in your Site, use the web page to set desired image settings.

Web Admin / *Cloud Portal*

1. Open **Settings** > **Site Administration** > **General** tab.
2. Unheck the **Allow Site to optimize device settings** checkbox.
3. Apply changes.

1.7.9.1.3 Camera Stream Tuning

By default, Nx Witness automatically determines the optimal settings that it will use to pull video streams from the camera. However, some cameras use their own proprietary settings that cannot be properly determined. In this case streaming may be unstable.

In this case it is possible to set them manually. To access those settings, use the camera's context menu to open **Camera Settings** > **Expert > Media Streaming**.

NOTE: Do not change these settings unless you are absolutely sure of their potential impact on your Site performance.

The following streaming settings can be manually specified:

- **RTP Transport**. By default, Nx Witness automatically determines the optimal protocol (*Auto*).
- **Media Port**. This is the port used for RTSP communication. By default, **554**.
- **Trust camera timestamp.** By default (disabled), Server puts its own timestamps in the archive, overriding the data coming from cameras. However, if the stream is intermittent, Server may incorrectly put timestamps and this may affect the archive browsing. This option will make the Server trust timestamps coming from the camera, as long as the time difference between the Server and camera is less than 10 seconds. In this mode, network delay doesn't affect the timestamp.

  Also, Server may push time settings to cameras to make sure the timestamps are synchronized. This is especially important for Edge cameras. See "Time Synchronization between Servers and Cameras".

1.7.9.1.4 Adjusting Average Bitrate

Some camera models do not yield the best setting when Nx Witness tries to configure a target bitrate, resulting in poor image quality. If this is the case you can adjust the bitrate calculation for the device manually.

NOTE: This setting will significantly increase bitrate. Use only if the picture quality is noticeably poor.

To Adjust Bitrate

1. Open the **Camera Settings** > **Expert** tab.
2. Check **Calculate bitrate per GOP instead of bitrate per second**.
3. Apply changes.

NOTE: This setting is ignored when "**Keep camera streams and profiles settings**" is checked. See "Preventing Nx Witness from Changing Manufacturer Settings".

1.7.9.1.5 Forcing Motion Detection to a Specific Stream

Nx Witness performs motion detection on the server side by analyzing and decoding the secondary stream from a camera, which is usually a low resolution stream. Occasionally, a camera will report its configuration incorrectly and swap the primary and secondary streams. If this occurs and the secondary stream is high-resolution, motion detection processing will create a very high CPU load.

To correct this, you can force motion detection onto a specific stream.

1. Open the **Camera Settings** > **Expert** tab.
2. Check **Force motion detection for stream** and select **Primary** or **Secondary**.
3. Apply changes.

NOTE: Adjusting these settings can seriously affect Server performance. See "Dual Stream Processing" for details.

1.7.9.1.6 Disabling Recording of a Specific Stream

In some circumstances you may want to disable recording of the primary or secondary stream.

For instance, it may make sense to disable recording of the primary stream to save storage space and instead set the recording type to "Motion Only" and "Low" quality. Or, if the secondary stream bitrate is too high, it may make sense to disable recording so that the Nx Witness Server still performs motion detection but it does not record it.

To disable recording of a specific stream

1. Open the **Camera Settings** > **Expert** tab.
2. Check **Do not archive primary stream** or **Do not record secondary stream**.
3. Apply changes.

1.7.9.1.7 Disabling a Secondary Stream

It is possible to disable the secondary stream entirely. This may be necessary, for example, for very old cameras where the secondary stream has motion detection but does not support H.264 or H.265 Codec. In this case it is helpful to reduce the demand on storage space by disabling the secondary stream so it is not recorded.

NOTE: If the resolution of the primary stream is more than 1024x768, software motion detection will be disabled. If the primary stream resolution is less than or equal to 1024 x 768, motion detection can be performed there.

To completely disable a secondary stream

1. Open the **Camera Settings** > **Expert** tab.
2. Check **Disable secondary stream**.

3. Apply changes.

NOTE: This setting is unavailable if "Allow Site to optimize camera settings is disabled. See ("Dual Stream Processing").

Camera and Server Time Sync

By default, all Servers in Site have the time synchronized (see "Time Synchronization in a Multi-Server Environment"). This ensures the smooth archive recording, indexing and fetching.

By default, Server ignores the time on cameras. However, in some cases it may be necessary, especially for Edge cameras that record archive to the internal storage. In this case it is critical to have the camera time synchronized with Server.

To push time from Server to a camera:

1. Open the **Camera Settings** > **Expert** tab.
2. Unheck **Time Settings** > **Keep Camera Time Settings**.
3. Apply changes.

Additionally, it is possible to force the Server to use timestamps from cameras (may be also useful for Edge cameras). See "Tuning up Camera Streaming" for details.

PTZ Movement Speed

The PTZ speed setting changes how fast the pan or tilt action is completed. The minimum value is 0.1 and the maximum value is 1.0.

In **Camera Settings > Expert** tab, enable **Use different values for pan and tilt** if different speeds for pan and tilt are needed.

PTZ Position Presets

The PTZ presets setting decides which presets the Server will use. Some cameras aren't able to save or activate PTZ presets through Nx Witness (*site presets*) and must process such requests directly on the camera to function correctly (*native presets*).

Choose between two options in **Camera Settings > Expert** tab:

- *Use site presets* – The preset profile and coordinates are saved in the Server's database. When you call the PTZ preset, Nx Witness sends the move request with the absolute coordinates.
- *Use camera native presets* – The preset profile and coordinates are saved in the camera itself. When the PTZ preset is activated, Nx Witness sends the move request with the preset ID. The camera will check the preset configuration by itself and move to the position.

Assigning Logical ID

The Nx Witness Server provides a mapping that lets you assign a six digit *Logical ID* that can be used instead of the much longer Camera ID**.** The Logical ID simplifies device identification when integrating with third-party solutions, and is necessary in environments with input devices that are not capable of entering the full Camera ID. The Logical ID can be used in API calls (including getting RTSP streams etc) to address Cameras. If one is assigned, the Logical ID is displayed on the *General* tab of *Camera Settings*.

To assign a Logical ID

1. Open the context menu for a camera and go to **Camera Settings** > **Expert**.
2. Enter a number in the **Logical ID** field.

   If you are integrating with a Site that is already using 1 to 3 digit identifiers, use the **Generate** button to discover and display the smallest number that is not already in use.

   NOTE: It is also possible to assign a Logical ID to a layout, see "Configuring Layouts".

To remove a Logical ID

Press the **Reset** button. This sets the Logical ID to zero, which the Server equates to having no Logical ID.

Plugin Integrations

Plugins are a type of integration that provides an enhanced data connection between Nx Witness and specific devices. This enables the Desktop Client to receive analytical metadata directly from a a camera and control settings using a common graphical user interface. This is similar to how Web Page Integrations provide a method for the Desktop Client to exchange data with external services.

Key Concepts

- Nx Witness automatically installs a set of plugins for popular cameras from worldwide vendors.
- Plugin vendors, integration developers, and device OEMs provide installation and configuration instructions for their products.
- The Desktop Client will only show plugins and integrations when compatible devices are connected and authorized.
- The Integration vendor defines the level of functionality provided by their plugin and is responsible for application support.
- Integrations can be independently installed, updated, configured, and removed from a Site.
- Plugins directly access the Event Rules engine, APIs, and mediaserver SDK to provide custom analytics and data processing.
- Not all integrations are compatible with all Nx Witness releases nor all device models and firmware versions.

- Camera and device response time will vary with network traffic and the computational capacity of each device.

NOTE: Refer to vendor provided instructions and device-specific documentation for additional information.

Region of Interest

Key Concepts

- Region of Interest (ROI) is a feature often found in cameras with built-in video analysis services.
- ROIs represents an area or line placed over the camera image is part of a defined event or detection alarm.
- A single camera can have multiple ROI and often each ROI has its own settings for sensitivity, time, direction of travel, etc.
- For many cameras the Nx Witness Desktop Client is able to define ROIs and configure detection settings.
- Only one camera stream can be used with the ROI functionality.
- The Analytics Event rule can be used to trigger an Action based on data provided by an integration.

NOTE: This section describes the basic ROI types available through the Stub integration. While these examples are similar to many integrations, each integration vendor defines the tools and settings available through the Desktop Client and directly through software embedded in the camera or device.

Common ROI Types Available in the Stub Integration

The Stub ROI integration provides the following use cases types as examples representing the options available in many integrations.

- The *exclusion polygon* is an area that will be ignored by any other Stub ROI that overlaps the same area on the camera image.
- *Polygons* are closed shapes of between three and six points that can be repositioned on the camera image.
- *Boxes* are four sided shapes created with a click and drag operation. Boxes have the same configuration options as polygons and they can be re-sized and repositioned, but they cannot be rotated and must contain 90 degree angles at each corner.
- *Lines* are limited to two-points of definition that typically include a direction of travel that is part of the event detection configuration.
- *Polylines* can contain multiple points and are often used to define an ROI that aligns with a unique physical environment that must be accommodated. A polyline can cross itself, but it will not create a closed shape and cannot be converted into a polygon.

- The *Size Constraint* function provides a minimum and a maximum bounding box. An object must be between the min and max sizes to trigger a detection event. The min and max bounding boxes do not need to overlap – the minimum box must always be smaller than the maximum box.

Define a Region of Interest

The following outline generally applies to all Stub ROI types while respecting that not all ROI types have the same configuration options.

1. Open the context menu of a supported camera and select > **Camera Settings** > **Integration** to open the dialog.
2. Scroll through the available ROI types and locate the ROI type (Boxes, Lines, Polygon, Size) to be defined.
3. Enter an optional caption-label for the ROI to be displayed when the ROI shape is set to be displayed.
4. Click the empty camera-frame that contains the text "Click to add", or a currently configured ROI snapshot to enter ROI definition mode.
    a. Select a color to be applied to the ROI graphics that will be placed over the camera image.
    b. Place sequential ROI points to create a line or create and close a polygon – click and drag to create a box or to re-size min-max bounding boxes.
    c. Click **Clear** to erase all points and start over, or click **OK** to save the ROI and close the definition dialog.
5. Checkbox to select if the ROI shape is *displayed on video* as an overlay.
6. Set any configuration options for the ROI being defined.

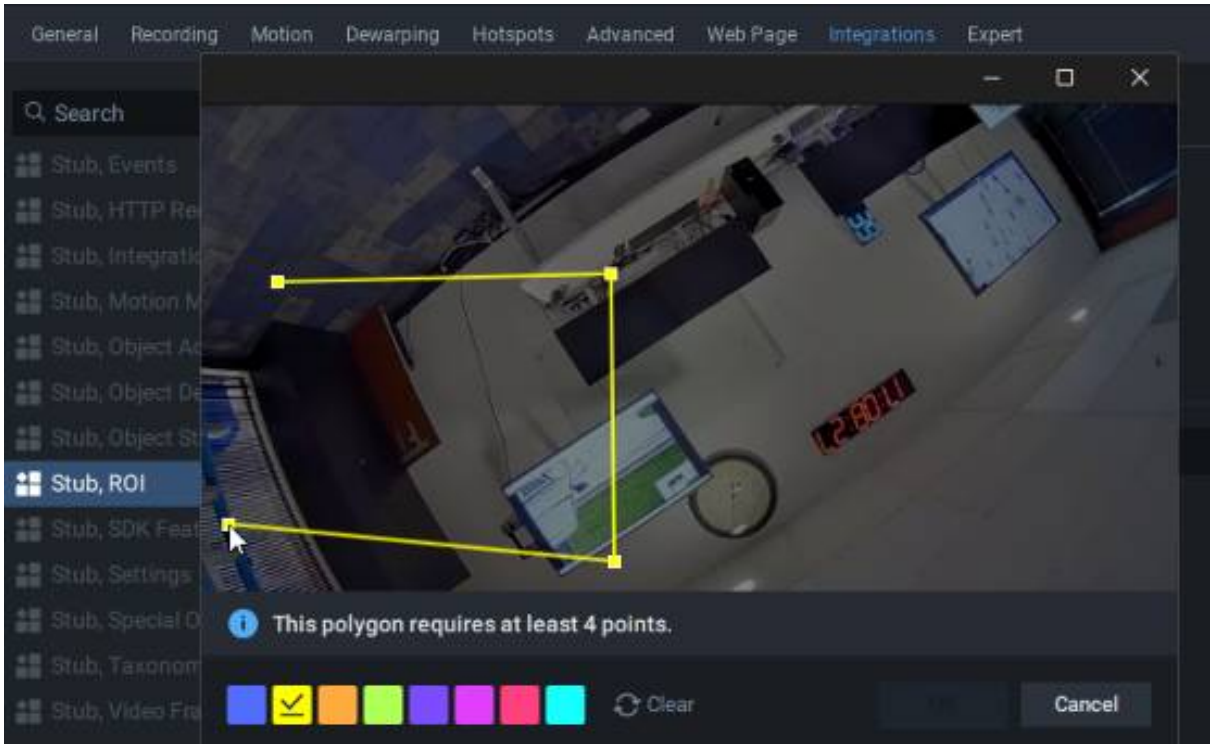
Add Additional Regions of Interest

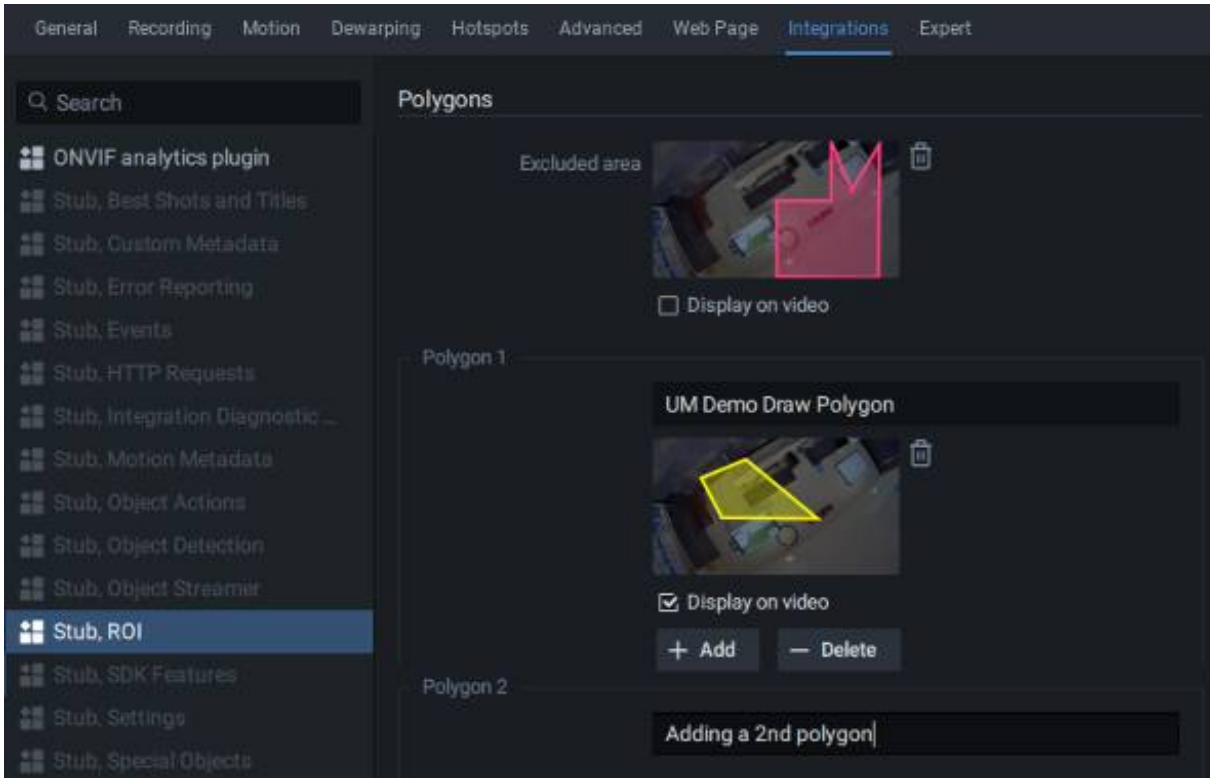
The following steps apply to analytical models that support multiple ROIs.

1. Open the context menu of the camera containing the ROI and select > **Camera Settings** > **Integration** to open the dialog.
2. Locate the ROI to be configured.
3. Use the **+Add** and **-Delete** buttons to add or remove additional ROIs.
4. Repeat the steps to Define a Region of Interest described in the previous section.

Delete a Region of Interest

1. Open the context menu of the camera containing the ROI and select > **Camera Settings** > **Integration** to open the dialog.
2. Locate the ROI to be deleted.
3. Click on the trash can icon to remove the ROI – this cannot be undone.


General
Recording
Motion
Dewarping
Hotspots
Advanced
Web Page
Integrations
Expert
Search
Stub, Events
Stub, HTTP Re
Stub, Integratic
Stub, Motion M
Stub, Object Ac
Stub, Object De
Stub, Object St
Stub, ROI
Stub, SDK Feat
Stub, Settings
Stub, Special O
Stub, Taxonom
Stub, Video Fra
This polygon requires at least 4 points.
Clear
Cancel


General
Recording
Motion
Dewarping
Hotspots
Advanced
Web Page
Integrations
Expert
Search
ONVIF analytics plugin
Stub, Best Shots and Titles
Stub, Custom Metadata
Stub, Error Reporting
Stub, Events
Stub, HTTP Requests
Stub, Integration Diagnostic ...
Stub, Motion Metadata
Stub, Object Actions
Stub, Object Detection
Stub, Object Streamer
Stub, ROI
Stub, SDK Features
Stub, Settings
Stub, Special Objects
Polygons
Excluded area
Display on video
Polygon 1
UM Demo Draw Polygon
Display on video
+ Add
— Delete
Polygon 2
Adding a 2nd polygon

ONVIF Analytic Integration

Key Concepts

- The ONVIF Analytics Plugin integrates real-time analytics events from compatible ONVIF cameras directly into Nx Witness.
- Only events are supported – objects and metadata are not supported.
- Requires cameras with ONVIF Profile M analytics capability.
- Some event types may not be recognized due to camera design or implementation.

Setup

1. Connect Camera: Add an ONVIF-compatible camera to your Site.
2. Auto-Discovery: The plugin automatically detects available analytics event types from the camera.
3. Create Rules: Set up Event Rules to initiate Actions based on analytics events.
4. Automatic Subscription: The plugin subscribes to camera notifications when you create rules.

Health Monitoring Metrics

In addition to the Nx Witness Server Monitoring display, Users with the *Site Health Monitor* permission can view detailed metrics using the Web Admin or Cloud Portal.

Site Health Metrics are parameters of different components of the Site that provides valuable information about the state of each component. Metrics are aimed at helping investigate problems and tune performance. Below are some examples of the parameters available for each component type:

- Alerts – Site, Server, Camera, and Storage related alerts. Event notifications are not shown here.
- Site metrics – The number of Servers, camera channels, storage locations and users, etc.
- Server metrics – CPU/RAM usage, camera channels, Server threads and network connections, etc.
- Camera metrics – Vendor, model, firmware and video quality settings, etc.
- Storage Locations – Capacity, read/write speed and issues, etc.
- Network Interfaces metrics – IP addresses and i/o rates, etc.

To view the Health Monitor:

1. Connect to a Site using the *Web Admin* or *Cloud Portal*.
2. Select the **Information** tab in the heading menu.
3. Select the component to monitor in the left panel.

4. Optionally download the full report for offline review, record keeping, or sharing with technical support.

   NOTE: All metric data is erased when the Server is restarted.

Cloud Connect Issue

Occurs when the server is the master-server and a selected cloud connection condition creates a trigger. This is a default event.

Advanced Parameters:

- *Cloud Database* – this event is triggered when a connection to the Cloud Database could not be established.
- *Cloud Server Socket* – this event is triggered upon a detected issue while listening on the server socket connection.
- *Cloud Mediators* – this event is triggered when a master-server is disconnected from all Cloud Mediators.
- *Cloud Relays* – this event is triggered when a master-server is disconnected from all Cloud Relays.

NOTE: If several values are selected, then the condition for the occurrence of an event works with the "OR" logic where the event occurs if any condition is triggered for at least one selected value.

- Event Scheduling

Troubleshooting Suggestions:

- The user has disabled this type of notification.

Alerts

Alerts are representations of metrics that are presented to the User once metrics pass a threshold where they enter into values that should not be reached for that parameter in a healthy Site.

Alerts can show what's wrong with the Site without having to go too far deep in the details. Below are some examples of the alerts you will receive for each component type:

- *Site alerts* – Maximum number of servers or channels per Site is reached.
- Server alerts – Offline event, high CPU/RAM usage, logging level status, encoding threads greater than 2, etc.
- Camera alerts – Camera offline event, IP conflict, frame drop, etc.
- Storage alerts – Storage inaccessible or offline, storage issue in the last 24 hours, etc.

NOTE: All alerts (including aggregated alerts), are erased after the Server has been restarted.

Site Metrics

The **System** tab contains *System-level* metrics.

The following information is displayed:

- *Servers* – The number of servers in the System.
- Camera channels – The number of camera channels in the System.
- Storage locations – The number of storage locations in the System.
- Users – The number of users in the System.
- System *Version* – The Nx Witness Server version.

Server Metrics

The **Servers** tab contains *Server-level* metrics.

The following information is displayed:

Server Availability

- *Status* – Current status of the sever (online/offline).
- *Events: Server Offline (24h)* – Number of times the server went offline in the last 24 hours.
- *Uptime* – Length of time the sever has been continuously active.
- *Cloud master-server* (flag) – Is current server responsible for connecting to the Cloud (yes=true | no=false)
- *Cloud DB status* – the state of the cloud database can be:
  - Connected, when current server is the master-server.
  - {ErrorMessage} that is related to a cloud database connection.
  - – (dash) when the current server is not the master-server.
- *Events: Cloud DB failures (24h)* – count of cloud database events in a rolling 24-hour window.
- *Cloud Server Socket status* – the current state of the cloud socket.
- *Events: Cloud Server Socket failures* (24h) – count of cloud socket events in a rolling 24-hour window.
- *Cloud Mediator status* – the current Mediator state.
- *Events: Cloud Mediator failures* (24h) – count of cloud mediator events in a rolling 24-hour window.
- *Cloud Mediator URL* – the current internet address of the Mediator.
- *Cloud Relay status* – the current relay state.
- *Events: Cloud Relay failures* (24h) – count of cloud relay events in a rolling 24-hour window.
- *Cloud Relay URL* – the current internet address of the Relay.

Load

- *Total CPU Usage (%)* – CPU usage of the entire machine.
- *CPU used by VMS Server (%)* – CPU usage of the Nx Witness Server application.
- *Total RAM Usage* – RAM usage of the entire machine in GB.
- *Total RAM Usage (%)* – RAM usage of the entire machine as a percentage.
- *RAM used by VMS Server* – RAM usage of the Nx Witness Server application in GB.
- *RAM used by VMS Server (%)* – RAM usage of the Nx Witness Server application as a percentage.
- *Server threads* – Number of threads inside Server processes.
- *Camera channels* – Number of device channels in the Site.
- *Decoding threads* – The number of running decoding threads.
- *Decoding speed* – Total decoding speed in megapixels per second, including thumbnails encoding.
- *Encoding threads* -The number of running encoding threads.
- *Encoding speed* – Total encoding speed in megapixels per second, including thumbnails encoding.
- *Outgoing Primary streams* – The number of primary media streams that are being taken from the Server (including audio-only streams, such as from an I/O module).
- *Outgoing Secondary streams* – The number of secondary media streams that are being taken from the server.
- *Incoming connections* – Number of open incoming sockets, including UDT (TCP over UDP).
- *Outgoing connections* – Number of open outgoing sockets, including UDT (TCP over UDP).
- *Logging level* – The type of logging enabled on the server.

Info

- *Public IP* – Public IP of the server.
- *OS* – Operating System installed on the server.
- *OS Time* – Time as reported by the operating System.
- *VMS Time* – Time as reported by the Nx Witness server application.
- *CPU Name* – Available manufacturer and model information for the CPU.
- *Cores* – The reported number of cores in CPU.
- *RAM* – Amount of RAM (GB) installed on the server.
- *Events count: Time Changed (24h)* – Number of times the server's time had to be synchronized.

Activity

- *Transactions per second* – Represents activity with resources settings and information being changed in the internal database (from a moving average over the last 60 seconds).
- *Event Rules activations per second* – Number of times Event Rules have been triggered (from a moving average over the last 60 seconds).
- *REST API calls per second* – Number of HTTP REST API per second (from a moving average over the last 60 seconds). This number does not include API calls for media streaming and data proxying between servers.
- *Thumbnails per second* – Number of thumbnails decoded per second (from a moving average over the last 60 seconds).
- *Active plugins list* – Numbered list of plugins that are currently working on the server.

Camera Metrics

The **Cameras** tab contains Camera-level metrics.

The following information is displayed:

- *Name* – Name of the device.

Info

- *Server* – Name of the Server the camera is connected to.
- *Type* – The type of device: Camera, Multi-Sensor Camera, Encoder, NVR, I/O module, or Horn Speaker.
- *IP* – IP address of the device.
- *Recording* – The recording status of the device: On, Scheduled, or Off.

Availability

- *Status* – The connectivity status of the device: Offline, Online, Unauthorized, or Server Offline.
- *Events* – Camera Offline (1h) – Number of times the camera went offline over the past hour.
- *Events – Stream Issues (1h)* – Number of times the stream had issues over the past hour.

Primary Stream

- *Resolution* – The resolution of the primary stream.
- *Actual FPS* – Frames Per Second (FPS) of the stream.
- *Avg FPS drop (10 min)* – Difference between the FPS being targeted and the actual FPS (average over the last 10 minutes).

Secondary Stream

- *Resolution* – The resolution of the secondary stream.
- *Actual FPS* – Frames Per Second (FPS) of the stream.

- *Avg FPS drop (10 min)* – Difference between the FPS being targeted (set in the Advanced tab) and the actual FPS (average over the last 10 minutes).

Storage Analytics

- *Archive* – Length of all archived footage associated with this camera.
- *Recording Bitrate (5min)* – Bitrate for the Camera archive (based on the last 5 minutes of recorded archive).

Storage Metrics

The **Storage** tab contains *Storage-level* metrics.

The following information is displayed:

- *Name* – Storage location path.

Info

- *Server* – Name of the Server the storage is installed on.
- *Type* – Types of storage being used (local, smb, etc).

State

- *Status* – Current status of the storage drive.
  - Online – Displays when the storage drive is online and not disabled by the user.
  - Disabled – Displays when the storage drive is online but disabled by the user.
  - Inaccessible – Displays when the storage is offline.
  - Server Offline – Displays when the Server that the storage drive belongs to is offline.
- *Issues (24h)* – Number of storage issue events within the last 24 hours.

Activity

- *Read Rate* – Storage drive read rate per second (from a moving average over the last 60 seconds).
- *Write Rate* – Storage drive write rate per second (from a moving average over the last 60 seconds).

Space

- *Total* – Size of the storage in Gigabyles (GB).
- *VMS Media (%)* – Amount of the storage space occupied by data (as a percentage).

Network Metrics

The **Network Interfaces** tab contains *Network-level* metrics.

The following information is displayed:

- *Name* – Name of the network interface.

Info

- *Server* – Name of the Server the network interface is installed on.
- *State* – Status of the network interface: Up (active), or Down (Disconnected or disabled in the OS).
- *IP* – IPv4-address of the network interface.

I/O Rates

- *IN Rate* – The amount of data received per second on the network interface (in kilobytes).
- *OUT Rate* – The amount of data sent per second on the network interface (in kilobytes).

Event Rules

Key Concepts:

- An *event rule* is a set of conditions that, when true, initiate a defined *action*.
- The event type selected defines the available parameters for both the event and the action.
- Create multiple rules using the same event conditions to initiate multiple actions for a singular event.
- An assortment of frequently used rules and actions are included with the HD Witness Desktop Client.
- Lookup Lists are a Site-wide set of values that enable multiple events and actions to updated at once.
- Certain events will pulse-highlight the device initiating an action to gain the users attention.
- Authorized users can create *event rules* and *actions* that use HTTP methods to interface with third-party services or Site (API) endpoints.
- Authorized users can create on-screen Soft Trigger events to test actions or enable users to manually start an action at their discretion.
- Most e*vent rules* and *actions* can be disabled, deleted, or set to only run on a defined, hourly schedule.
- Event rules with invalid settings are flagged in the event list and invalid options are flagged in the Event Rule Configuration dialog.
- Most actions include an interval setting to limit the frequency of actions taken.

Event Rule Types:

- *User events* – Are events defined by authorized users for specific conditions or integration with third party solutions.

- *Site-generated events* – Are instantaneous and related to platform configuration or operational elements.
- *Default Events* – Run when Nx Witness is open and monitor for device or hardware centric events.

NOTE: Events and actions are either momentary/instantaneous or prolonged, when they contain a duration of time or a start and stop element.

Event Logging:

- Events are automatically recorded in the Site Event Log
- The write to the log action will record events without taking additional action.

Site Metadata:

- Site metadata (device ID, date-time, IP address) is available for use in select actions.

Additional References:

- Open The Event Rules List to explore current *event rules* and *actions* in the Site.
- Use The Event Rules Form to create a new *event rule* and *action* pair in the Site.
- Explore available Site and device metadata that can be used with event rules and actions.
- Review how Lookup Lists can accelerate the maintenance and revision of rules and actions.

Event Rules

Key Concepts:

- The Event Rules dialog provides a summary view (event – source – action – target – comment) of all event rules in the Site.
- Available action-icons and relative to the number of existing rules that are selected.
- Contextual icons to perform event rule tasks.
- Disabled rules are shaded and dimmed in the list of current event rules.
- Clicking the **Reset to Defaults** button will clear all custom event rules and restore the original set of *event rules*. This action cannot be undone.
- Contents of the search box are applied to all visible columns of data
  - Single character (?) and any after (*) wildcards are supported in the search box.

How to Open the Event Rules List:

Use any of the following methods to open the *Event Rules* list and view a summary of all event rules.

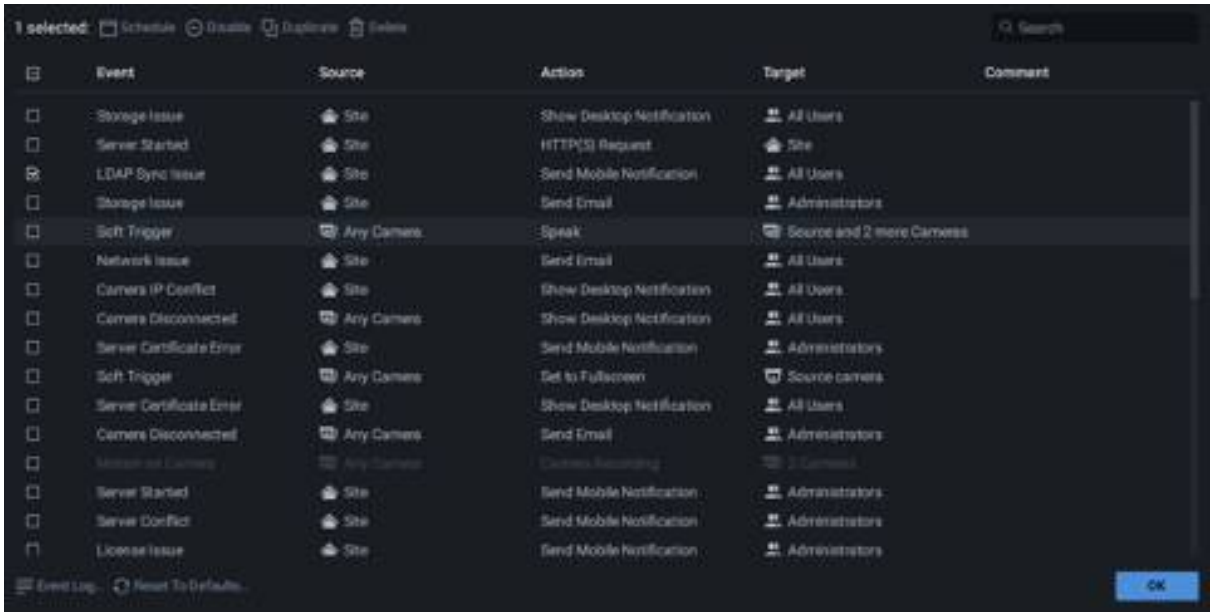
- Open the main menu, select **Site Administration** > **General** tab and click the **Event Rules** button.

- Open the context menu from the Notifications panel and choose **Event rules.**
- Use the device context menu and select **Camera Rules** to display the rules that apply to that specific device.
- Click on the **Camera Rules** button in the **General tab of the Camera Settings** dialog.
- Press the hot-key combination of CTRL + E (Windows) or CMD + E (macOS).

Actions Available in the Event Rules List:

The following actions are available within the dialog box for event rules.

- When no existing rules are selected, the **+Add Rule** button is available to open a blank Event Rule Form.
- Click on any exiting rule to open the Event Rule Form where configuration changes can be made.
- The button to **duplicate** a rule is available only when one checkbox next to an existing event rule is selected.
- If multiple, existing rules are selected, the event Schedule, delete, and enable/disable toggle is available.



Event Rule Form

Key Concepts:

- The event rule form is used to create or modify an event rules and the associated action.
- Some rules can be saved with minor issues that may prevent proper rule execution.
- Rules cannot be saved when required fields and selections are empty.
- Alert icons and banners are displayed near invalid settings or missing selections.

- There are two panel to the Event Rule Form:
  - The WHEN EVENT panel defines the conditions required to make the event rule true and valid.
  - The DO ACTION panel defines what actions the Site will take when the event rule is true and valid.

Common Settings:

The follow setting and options are present for every event rule type while all other parameters are defined by the event type and action type selected.

- A title and comment field provides for unique labeling that can found using search tools.
- Each event rule form includes a slide-switch to enable or disable the event rule.
- Click the schedule icon to opens a matrix of days and full hour increments to set when the event rule will be active.
- Alert icons are displayed near invalid settings in the configuration dialog.
- The configuration dialog uses pull-down menus for key attributes and multiple-selection pick lists for devices and users.
- Selections may be lost when changing the event or action type to one that does not share the same options.

WHEN EVENT (left) Panel:

- The When Event is the left-side panel of the event rule form.
- The top-most selection for the when event is the event type.
- The event type selected defines the parameters and options available for the event rule.
- Site Events are fully defined and do not contain configuration options.
- See the list of Tracked Events and configuration instructions all available event types.

DO ACTION (right) Panel:

- The top-most selection is the action type.
- The action type defines the parameters and options available for the event rule.
- See the list of Actions and the configuration instructions for available actions.

WHEN Events

Actions are initiated when the conditions of a defined event are valid and true within the "Event Scheduling" window of time.

Refer to the particular event description for configuration details and additional information:

User Events:

User event types are defined by Site operators and are not enabled by default or during installation.

- Analytics Event
- Analytics Object Detected
- Input Signal on Device
- Motion on Camera
- Plugin Diagnostic Event
- Soft Trigger

Default Events:

Default events are set during client installation and when **Reset to Defaults** is selected within the Event Rules List dialog.

- Camera Disconnected
- Camera IP Conflict
- Generic Event
- LDAP Sync Issue
- License Issue
- Network Issue
- Server Certificate Error
- Server Conflict
- Server Failure
- Server Started
- Services Issue
- Storage Issue

Analytics Event

The Analytics Event happens when a defined signal type is received from any device listed in the *Occurs At* field and the metadata received from the device also passes all additional requirements of the event rule.

Key Concepts**:**

- Devices that do not provide analytical event signals are not shown unless the *Show all cameras* switch is enabled.
- Devices that do not support *analytics events* are highlighted red when the showing all cameras in the selection dialog.

- The analytic *Of Type* options shown in the selection menu are provided by the devices listed in the *Occurs At* field.
- There are three (3) optional AND conditions that must match for the *analytics event* to be true.
  - The metadata defined in the *caption*, *description*, and *attribute* fields is case sensitive.
  - Empty fields are always processed as a match.

Occurs At**:**

This rule condition defines the devices monitored for the event conditions.

1. Click on the *Occurs At* data field to open the selection dialog.
2. The search box will dynamically filter available devices by name.
3. Selecting a server will automatically select all devices attached to the server.
4. Select/deselect individual devices until the event rule is configured as intended.

Of Type**:**

The values available are provided by the devices listed in the *Occurs At* field.

1. Click on the *Of Type* data field to open the selection dialog.
2. Select the *Of Type* that will be required for this event rule.

And Caption:

This rule requires that all metadata entered in the event rule *and caption* filed exactly matches the corresponding caption field metadata received from the device. Caption metadata is case sensitive and empty fields are processed as a match.

- **Contains Keywords** that are manually entered into the event rule configuration dialog.
- **Not Contains Keywords** that are manually entered into the event rule configuration dialog.
- **Contains list entities** will include the content contained in the selected Lookup List.
- **Not contains list entries** will exclude the content contained in the selected Lookup List.
- **Blank** (keywords) indicates no requirement are set.

And Description**:**

This rule attribute is specific to the Analytics Object Detection event rule and provides the method to provide rule-specific object attributes that can be differ from other detection rules.

- **Contains Keywords** that are manually entered into the event rule configuration dialog.
- **Not Contains Keywords** that are manually entered into the event rule configuration dialog.
- **Contains list entities** will include the content contained in the Lookup List.
- **Not contains list entries** will exclude the content contained in the Lookup List.
- **Blank** (keywords) indicates no requirement are set.

Analytics Object Detected

The Analytics Object Detected event happens when a device listed in the *Occurs At* field finds a match with the object type and attributes specified.

Key Concepts:

- Object Detection events are defined by devices and services that can identify attributes of an object.
- Accuracy and overall detection performance is a factor of the detection models and services used.
- Options and detection parameters vary by device and analytical services in use.
- The values available in the *Of Type* selection menu are defined by the devices listed in the *Occurs At* field.
- Empty fields are always processed as a valid match.

Example of Object Attributes:

- Object *Of Type*: Vehicle
  - Attributes: Color (Green) | Model (SUV) | Size (Small)
- Object *Of Type*: Vehicle
  - Attributes: Color (Blue) | Model (SUV) | Size (Large)

Occurs At**:**

To set the cameras that will monitor for object detection:

1. Click on the *Occurs At* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. If needed, use the search box is filter available cameras.
4. Selecting a server will automatically select all cameras attached to the server.
5. Adjust the list of *Occurs At* cameras until the event rule is configured as intended.

   Selecting the *Source camera* will always include the camera specified in the "Occurs At (camera)" setting within the WHEN panel.

   Devices that do not provide analytical event signals are not shown unless the *Show all cameras* switch is active.

   Devices that do not support *analytics object events* are highlighted red when the showing all cameras in the selection dialog.

Of Type:

The values available are provided by the devices listed in the *Occurs At* field.

1. Click on the *Of Type* data field to open the selection dialog.
2. Select the *Of Type* that will be required for this event rule.

   When *Of Type* values available and selected may not be compatible with all devices in the *Occurs At* selection.

And Object:

This rule attribute requires specific object data to match the selected event rule requirements.

- **Has attributes** are manually entered into the event rule configuration dialog.
- **Is listed** must include the content contained in the selected Lookup List.
- **Is not listed** must not include the content contained in the selected Lookup List.

Camera Disconnected

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this notification.
- Occurs if a device is disconnected for whatever reason (network issue, device malfunction, etc.).
- Devices are considered disconnected if no data is received for 10 seconds.
- If a device is experiencing network issues for over a minute an alert icon will appear next to it in the Resource Panel.
- Device status is automatically changed back to online once data transmission resumes.
- The following, related events may occur for the same device or cause the Camera Disconnected event to become true.
  - Camera IP Conflict
  - *Network Issue*
  - Server Conflict
  - Server Failure

Camera:

This rule condition defines the cameras to be monitored for the event conditions.

1. Click on the *Camera* data field to open the selection dialog.
2. The search box will dynamically filter available cameras by name.
3. Selecting a server will automatically select all cameras attached to the server.
4. Select/deselect individual devices until the event rule is configured as intended.

Camera IP Conflict

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this notification.
- Event Occurs when more than one cameras on the active network have same IP address.
- All but one camera with conflicting (duplicated) IP address will go offline and generate a Camera Disconnected event.

Generic Event

Key Concepts:

- This is a default event.
- Occurs when the Server receives an HTTP request from an external device, service, or environment.
- Users can choose to hide this notification.
- Enables third-party products and services to send an HTTP string to a server, and thus the device, using a *rest/v4/event/generic* API call.
- Pair with the "Site HTTP(s) Request" action to create bidirectional API communications between Nx Witness and external software environments.
- A Generic Event request must follow the proper format in order to be read by the server.
- The fields in the HTTP request must match the corresponding event rule fields to be acted upon.
- Keywords and the contents of all Lookup Lists are case sensitive.
- Empty fields are always processed as a match.

Basic Parameters:

Each request contains the following fields:

- *Source.*
- *Caption.*
- *Description.*
- *Metadata* – Used to pass a device identifier that will specify devices the event is limited to (cameras, I/O modules, etc). To obtain the device identifier:

  Open the device context menu and click **Device Settings**. In the **General** tab, the device identifier will be displayed as **Camera ID or Device ID**.

  NOTE: It is necessary to specify a device if the generic event is linked to a notification, and the "Force Acknowledgment" option is required. In this case once the notification is

acknowledged, a Bookmark will be created and linked to the specified device. See "Show Notifications" for details.

- *State* – This is an optional field for the `state`.
  - If there is no *state* field in the HTTP request, the event is considered **instant**.
  - If specified, the event is considered **continuous** and the rule requires a *state*=**started** or *state*=**stopped** attribute.
  - If a Generic Event containing *state*=**started** is received, the resulting action will continue until the server receives a Generic Event with the same parameters that contains *state*=stopped.

NOTE: If a continuous action such as "device recording" or "repeat sound" is bound to an instant Generic Event (one without a state field), the rule will not work. See "Configuring Event Rules" for more information about continuous and instant events.

Advanced Parameters:

For detailed information on the advanced parameters available for generic events, which are not covered in this Desktop Client User Manual, users and developers should refer to the API documentation hosted on an available mediaserver using the following syntax:

`https://<serverIp>:7001/#/api-tool/main`

Omit Logging:

When selected, the **Omit Logging** option will not add this specific *generic event rule* from being added to the Event log. This option allows an action that is triggered in rapid succession or with a very high frequency to be performed without a database call or storage action that would cause undesirable "spamming" of the Event Log.

NOTE: Even if the "**Omit logging**" checkbox is selected, a *generic event* with a "Write to log" action will still appear in the *event log*.

Troubleshooting Suggestions:

- The user has disabled this type of notification.
- HTTP request is not correctly written. Refer to the Server API.
- Request is filtered out. Try clearing all fields (Source, Caption, Description) and trigger the HTTP request again.
- HTTP request is bound to a continuous type of action but does not contain the "State" field.
- A device is not specified yet the event is linked to a notification and the "Force Acknowledgment" option is set.

Input Signal on Camera

Key Concepts:

- This is a Site event that cannot be disabled.
- Users can choose to hide this notification.
- Event Occurs when a device provides a detectable signal to Nx Witness.
- Most ONVIF-compliant devices that provide output signals are supported.
- Tje ID names for signals will vary between device models and versions.

Occurs At**:**

Select the cameras that will record during for this event action.

1. Click on the *On* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. If needed, use the search box is filter available cameras.
4. Selecting a server will automatically select all cameras attached to the server.
5. Adjust the list of selected cameras until the event rule is configured as intended.

With ID**:**

This rule condition defines the signal ID to accept from the *Occurs At* devices.

- Click on the *With ID* data field to pop-open the selection dialog.
- Select the signal ID that triggers the event rule.
- See Setting Up I/O Modules for additional information.

Integration Diagnostics

Key Concepts:

- This is a default event that can be disabled.
- Users cannot choose to hide this notification.
- Occurs when a server receives a diagnostic event from an integration within the Site.

Occurs At**:**

Select the cameras using integrations that will be monitored for diagnostic information.

1. Click on the *On* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. If needed, use the search box is filter available cameras.
4. Selecting a server will automatically select all cameras attached to the server.
5. Adjust the list of selected cameras until the event rule is configured as intended.

For Plugin**:**

The values available are provided by the devices listed in the *Occurs At* field.

1. Click on the *Of Type* data field to open the selection dialog.
2. Select the *For Plugin* that will be monitored for this event rule.

And Caption:

This rule requires that all metadata entered in the event rule *and caption* filed exactly matches the corresponding caption field metadata received from the device. Caption metadata is case sensitive and empty fields are processed as a match.

- **Contains Keywords** that are manually entered into the event rule configuration dialog.
- **Not Contains Keywords** that are manually entered into the event rule configuration dialog.
- **Contains list entities** will include the content contained in the selected Lookup List.
- **Not contains list entries** will exclude the content contained in the selected Lookup List.
- **Blank** (keywords) indicates no requirements are set.

And Description**:**

This rule requires that all metadata entered in the event rule *and description* filed exactly matches the corresponding caption field metadata received from the device. Description metadata is case sensitive and empty fields are processed as a match.

- **Contains Keywords** that are manually entered into the event rule configuration dialog.
- **Not Contains Keywords** that are manually entered into the event rule configuration dialog.
- **Contains list entities** will include the content contained in the Lookup List.
- **Not contains list entries** will exclude the content contained in the Lookup List.
- **Blank** (keywords) indicates no requirements are set.

And Level is:

Select any combination of the following optional qualifiers that may be provided by the device:

- *Info*
- *Waning*
- *Error*

LDAP Sync Issue

Key Concepts:

- This is a Site event that can be disabled.
- Users can choose to hide this notification.

- Event Occurs when any issue that prevents successful LDAP synchronization (proxy, connectivity, LDAP Server offline).
- LDAP users will not be able to connect to a Site (see "LDAP Users and Groups").
- All DO actions except Panic Recording and Repeat Sound are permitted actions for LDAP Sync Issue Events.

Troubleshooting Suggestions:

- Unable to reach the or connect to the LDAP server.
- Failed to complete the synchronization within the timeout setting.
- No User accounts on LDAP Server match the synchronization settings.
- Some LDAP users or groups were not found in the LDAP database.
- Changes being made on LDAP Server during Synchronization.
- Incorrect LDAP configuration or misaligned attribute mapping.

License Issue

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this hide this notification.
- This event is only available on Professional versions of HD Witness
- Event Occurs when a trial license expires, the Server on which licenses are activated goes offline, or other license configuration issues.
- The license issue notification containing the affected cameras is is generated once recording has stopped.
- Click on the notification to open the licenses configuration dialog.
- It is not possible to record camera streams without active recording licenses.
- Some analog cameras connected to encoders or I/O modules may remain viewable while license issues persist.

  NOTE: When a Server goes offline, there is a 30-day failover period for the licenses that were in use, during which recording can continue. The Server must be restored or new licenses must be activated during this grace period. After the grace period recording will stop every cameras missing a licenses.

Motion on Camera

Key Concepts:

- This is a default event that can be disabled.

- Users can choose to hide this notification.
- Occurs when motion is detected by a device.
- A Recording Schedule must be enabled on the selected cameras for this rule to be functional.
- The current motion event is considered complete when no motion occurs for 3 seconds.
- Once stopped, a future motion is considered a new motion event.

Occurs At**:**

Select the cameras that be monitored for motion detection signals.

1. Click on the *On* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. If needed, use the search box is filter available cameras.
4. Selecting a server will automatically select all cameras attached to the server.
5. Adjust the list of selected cameras until the event rule is configured as intended.

Troubleshooting Suggestions:

- The user has disabled this type of notification.
- Recording is disabled for cameras being monitored.
- The motion mask is not set properly..
- Too many cameras are monitored, triggering too many events to process.
- Cameras that are monitored are offline.
- Event action is not configured properly to act on the motion detection signal.

Network Issue

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this notification.
- Occurs when the network is unable to transfer data between device and server and packet loss is detected.
- Network issues can cause camera frame rates to drop or off-device analytics to fail.
- If no camera frames are received from a device for 10 seconds the camera disconnected event is asserted.

Server Certificate Error

Key Concepts:

- This is a Site event that can be disabled.
- Users can choose to hide this notification.
- Occurs if the Server's SSL certificate is unable to be verified.
- Click to open server settings.

  NOTE: See "Obtaining and Installing an Authorized Certificate" and "Server Certificate Validation" for details.

Server Conflict

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this notification.
- Occurs when different servers on the same network access and pull data from the same devices.
- This conflict will cause some devices to go offline because they do not provide several streams simultaneously.
- Sever conflict can assert the Camera Disconnected event.
- The notification message contains a list of the specific devices that are used by both servers.

Server Failure

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this notification.
- Occurs when a server is offline, down, or otherwise unavailable.
- Root cause can be a hardware failure, software issue, or manual or shutdown.
- All devices connected to an failed server will go offline.
- Properer configured Server Failover will attempt to reroute cameras to available servers.

Server Started

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this notification.
- Occurs when any server registered in the Site has started.

Services Issue

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this hide this notification.
- This event is only available on Enterprise versions of HD Witness
- Event Occurs when a subscription service become unavailable, expired, or otherwise shutdown or suspended.
- Features that require an active service may stop or have limited functionality.
- Click on the notification to open the configuration dialog for subscription services.

Soft Trigger

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this notification.
- This event type adds an on-screen (icon) button that user can click to initiate an action.
- Event duration is considered valid and ongoing for as long as the click is held.
- The event is treated as instant when clicked and released.
- The contents of the **Name** field are displayed on mouse over.
- A soft trigger with a "Perform HTTP Request" action can signal third-party solutions and devices.
- Notification will be shown if user has permission to activate soft trigger but lacks access to the device.

Occurs At**:**

Select the cameras that will record during for this event action.

1. Click on the *On* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. If needed, use the search box is filter available cameras.
4. Selecting a server will automatically select all cameras attached to the server.

5. Adjust the list of selected cameras until the event rule is configured as intended.

By:

This rule condition defines the users who can activate the soft trigger.

1. Click on the *By* data field to pop-open the selection dialog.
2. The search box will dynamically filter available users by name.
3. Default view for user selection is by group.
4. Toggle the *Show all users* switch to select individual users.

Name:

Enter a brief description of the event that will triggered. Contents of this field are displayed on layout when the cursor hovers over the button.

Icon:

Select an icon for the soft trigger from the menu of available choices.

Storage Issue (default)

Key Concepts:

- This is a default event that can be disabled.
- Users can choose to hide this notification.
- Occurs if a Server is unable to write data onto one or more storage device.

Troubleshooting Suggestions:

Storage issue may be caused by any of the following:

- *Hard disk malfunction.*
- *Insufficient rights* – The permission to write on disk or recorded folder may be restricted by the computer Administrator.
- *Hard disk is too slow* – Too many cameras are attempting to record simultaneously and the hard disk cannot respond quickly enough. Try adding additional drives to the server.
- *Disk is full* – There is a required reserved space of approximately 10%. When available disk space reaches that threshold, the oldest data will be overwritten by new data. If available storage drops below this threshold, the server will write data to the disk but instantly erase it.
- *Primary Drive is Full* – Occurs when the primary partition lacks enough free space to function correctly/

DO Actions

The reaction to a valid event rule is an *Action*.

Each action has its own set of parameters, refer to one of the following action description for more information:

- Camera Recording
- Create Bookmark
- Device Output
- Execute PTZ Preset
- Exit Full screen
- HTTP(S) Request
- Open Layout
- Panic Recording
- Play Sound
- Repeat Sound
- Send Email
- Send Mobile Notification
- Set to Full screen
- Show Desktop Notification
- Show Text Overlay
- Show on Alarm Layout
- Site HTTP(S) Action
- Speak
- Write to Log

Camera Recording

Key Concepts:

- When the event rule is true and valid, this action starts recording on the selected cameras.
- Recording can be set to continue for a fixed duration or a duration of time relative to the event.
- The camera settings in this action will override the operational camera setting for the duration of the action.
- Action can be configured to capture additional time before and after the event rule became true and valid.

On:

Select the cameras that will record during for this event action.

1. Click on the *On* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. If needed, use the search box is filter available cameras.
4. Selecting a server will automatically select all cameras attached to the server.
5. Adjust the list of selected cameras until the event rule is configured as intended.

   Selecting the *Source camera* will always include the camera specified in the "Occurs At (camera)" setting within the WHEN panel.

Quality:

Choose a preset camera quality level.

FPS:

Set the desired target frames per second (FPS) for camera recording by either entering a numerical value or using the up and down arrows.

Additional Settings:

Below the FPS value is the duration mode:

- *For the duration of the event* provides for additional time to be added before and after the event duration.
  - Enter time values and unit of measurement to record before and after the after the event.
- *Of fixed duration* will enable the additional options below:

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

Duration:

Select the duration of the action and the unit of time measurement.

Also Include:

Enter an amount of time, and a unit of measurement, to include prior to the *Begin When* selection.

Interval of Action:

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Create Bookmark

Key Concepts**:**

- When the event rule is true and valid, the Site will create a bookmark on the selected devices.
- Action can persist for a fixed duration or a duration of time relative to the event.
- Bookmarks can be created on the source camera, other available cameras, or both.
- For the bookmark creation to be successful, recording must be enabled on all cameras specified in the "At" field.
- Bookmarks are automatically named using the format "<Event> on <Device>".
- Optional, predefined tags and applied to all bookmarks created with this action.

At:

Select the cameras where the bookmark will be created.

1. Click on the *At* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. The search box will dynamically filter available camera by name.
4. Selecting a server will automatically select all cameras attached to the server.
5. Select/deselect individual cameras until the event rule is configured as intended.

   Selecting the *Source camera* will always include the camera specified in the *Occurs At* (camera) setting within the WHEN panel.

Additional Settings:

Below the *At* field is the duration mode:

- *For the duration of the event* provides for additional time to be added before and after the event duration.
  - Enter time values and unit of measurement to record before and after the after the event.
- *Of fixed duration* will enable the additional options below:

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

Duration:

Select the duration of the action and the unit of time measurement.

Also Include:

Enter an amount of time, and a unit of measurement, to include prior to the *Begin When* selection.

Add Tags: Define any tags that will become part of the bookmark metadata.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Device Output

Key Concepts:

- When the event rule is true and valid, an output signal will be sent to selected devices.
- Action can persist for a fixed duration or a duration of time relative to the event.
- The output options are provided and defined by the selected *At* devices.
- A common **Output ID** can be sent to multiple devices as part of a single action.
- Output is synchronous with, and will stop when motion or input stops with these event rules:
  - Motion on Camera
  - Generic Event

- Analytics Event
- Soft Trigger
- Input Signal on Device.

At:

Select the cameras that will receive the **Output ID** signal.

1. Click on the *At* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. The search box will dynamically filter available camera by name..
4. Selecting a server will automatically select all cameras attached to the server.
5. Select/deselect individual cameras until the event rule is configured as intended.

   Selecting the *Source camera* will always include the camera specified in the *Occurs At* (camera) setting within the WHEN panel.

Output ID:

- Available options are provided by the *At* device.
- Select one I/O Module ID that the output signal will be routed to.

Additional Settings:

Below the *At* field is the duration mode:

- *For the duration of the event* will provide the device output from event beginning to event end.
- *Of fixed duration* will enable the additional options below:

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

Duration:

Select the duration of the action and the unit of time measurement.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.

- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Execute PTZ Preset

Key Concepts:

- When the event rule is true and valid, selected cameras will move to an established PTZ position.
- One PTZ position must be defined on at least one selected (*At)* camera for this action to be valid.
- It is not possible to start PTZ tours using this action.
- Set the interval of action longer than the movement time to prevent restarting the PTZ movement.

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

At:

Select the cameras that will receive the PTZ preset (move) command.

1. Click on the *At* data field to open the selection dialog.
1. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
2. The search box will dynamically filter available camera by name..
3. Selecting a server will automatically select all cameras attached to the server.
4. Select/deselect individual cameras until the event rule is configured as intended.

   NOTES:

   - Selecting the *Source camera* will always include the camera specified in the *Occurs At* (camera) setting within the WHEN panel.
   - No PTZ movement will take place on (*At*) devices that do not have a matching PTZ preset defined.

Interval of Action:

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Exit Fullscreen

Key Concepts:

- When the event rule is true and valid, the selected layout will *exit full screen* mode.
- No action is taken if the selected layout is not in full screen mode.
- All selected layouts are sent the *Exit Fullscreen* command.
- Exit full screen is a companion action to the Set to Fullscreen action.

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

On Layout:

This parameter defines the layouts that will exit fullscreen mode upon a true and valid WHEN EVENT.

1. Click the *On Layout* data field to open the selection dialog.
2. The search box will dynamically filter available layouts by name.
3. Adjust the list of selected layouts until the event rule is configured as intended.
4. At least one layout must be selected to save and enable this event rule.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

HTTP(S) Request

Key Concepts:

- When the event rule is true and valid, a preformed HTTP(S) request is sent to a specified URL.
- The request must be formed with a syntax that is acceptable and actionable by the receiving device.
- Bidirectional communications with external devices or services can be maintained when combined with a Generic Event.
- Multiple receiver-authentication methods and content types are supported.
- The following methods can be sent:
  - Auto
  - GET
  - POST
  - PUT
  - PATCH
  - DELETE

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

URL:

Enter the complete URL where the request (content) will be sent.

Method:

Select the HTTP(S) method to be sent.

Content:

Enter the complete body of the request to be delivered to the URL, including any Event Field Metadata.

Content Type:

Select the content type required by the receiving service:

- *Auto*
- *text/plain*

- *text/html*
- *application/html*
- *application/jsonE*
- *application/xml*

NOTE: Auto selects the best format based on the content entered.

Authentication Type:

Select the authentication type required by the receiving service and provide the credentials to use:

- *Auto, Basic, and Digest* required a Login and Password be provided.
- *Bearer* requires a token to be provided

Interval of Action:

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

Example Content Syntax:

The following example and descriptors are for illustrative purposes only:

http://123.12.8.1:7001/api.clickandcall.com/http/**sendmsg**?**login**=VMSuser&password=123456&**api_id**=3612726$MO=1&**from**-13234567890&**to**=18184493546$**text**=suspicious+motion+at+loading+bay

- *sendmsg* – Sends data to a server at IP Address 123.12.8.1 port 7001
- *login and password* – credentials required by the receiver to allow the request access to their platform.
- *api_id* – required account number with receiving entity.
- *from* – phone number from which the message will be sent.
- *to* – phone number to which the message is sent.
- *text* – the message text, in this case "Visitor is outside front door".

Action Troubleshooting:

- Event is not configured properly to initiate the DO HTTP(S) Request action.
- The request syntax is incorrect or not understood by the receiver.
- External authorization issue from incorrect or missing credentials.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Open Layout

Key Concepts:

- When the event rule is true and valid, a specific layout will open for selected users.
- The list of *To* users can be individuals, built-in groups, custom groups, or all users of the Site.
- No action will take place for users who receive the *Open Layout* action while lacking permission to view the layout.

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

To:

Select the users who will receive the *Open Layout* action:

1. Click on the *To* data field to open the selection dialog.
2. Slide the **Show all users** switch to display individual users – only groups are shown by default.
3. The search box will filter available users and groups by name.
4. Select/deselect users and groups until the event rule is configured as intended.

   NOTE: Selected groups or users without permission to the layout are shown in red text.

Layout:

This field defines which layout will open on event rule for the users listed in the *To* field.

1. Click on the *Layout* data field to open the selection dialog.
2. The search box will dynamically filter available layouts by name.
3. Select the layout to open with respect the the following conditions:
   a. Cross-Site Layouts cannot be used with this event action.
   b. Only shared layouts are displayed when no users or user groups are selected.

c. If exactly one user is selected, their local and all shared layouts will be displayed in the *Select Layout* dialog.
d. A warning message will be displayed when selected users cannot access the layout selection.

Rewind:

The *rewind* feature will move the playback back the footage up by a predefined amount of time when opening the layout.

1. Slide the switch enable or disable the rewind function.
2. Enter an amount **For** how long the camera archive should rewind.
3. Select the unit of time measurement for the amount of time.

Interval of Action:

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Panic Recording

Key Concepts:

- When the event rule is true and valid, all devices will record at their maximum resolution.
- Action can persist for a fixed duration or a duration of time relative to the event.

Additional Settings:

Below the action type is the duration mode:

- *For the duration of the event* will provide the device output from event beginning to event end.
- *Of fixed duration* will enable the additional options below:

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

Duration:

Select the duration of the action and the unit of time measurement.

Interval of Action:

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Play Sound

Key Concepts:

- When the event rule is true and valid, this action will send an audio file to devices and/or users for playback.
- An assortment of audio files are provided.
- Preloaded audio files will play one time.
- Authorized users can upload audio files of up to 30 seconds in length.
- Custom audio files will play (clip/loop) for the duration specified when added to the Site.
- Playback devices must be configured to support 2-way audio.
- Users must have the Play Audio permission.

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

Sound:

This field defines which audio file will be sent to the playback (*At*) device.

1. Click on the the current sound file name, or the *No Sound* text to open the selection dialog.
2. Select the audio file from the choices listed, or
3. Click the **Manage** button to open the sound file management dialog with the following choices:
   a. **Play** – play the selected file on the current client workstation.
   b. **Add...** will open a file selection dialog:
      - .WAV, .MP3, .OGG, and .WMA file types are supported.
      - Enter a custom title for the imported file or default to the imported file name.
      - Set a playback length of up to 30 seconds; longer files will be clipped.
   c. **Rename...** provide a dialog to rename sound file that currently exist in the selection menu.
   d. **Delete...** will delete the currently selected, user uploaded file. System sounds cannot be deleted.

At:

Select the cameras that will receive the audio file for playback.

1. Click on the *At* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. The search box will filter available cameras by name.
4. Selecting a server will automatically select all cameras attached to the server.
5. Select/deselect individual cameras until the event rule is configured as intended.

   Selecting the *Source camera* will always include the camera specified in the *Occurs At* (camera) setting within the WHEN panel.

To Users:

Select the users who will receive the *Open Layout* action:

1. Click on the *To Users* data field to open the selection dialog.
2. Slide the **Show all users** switch to display individual users – only groups are shown by default.
3. The search box will filter available users and groups by name.

4. Select/deselect users and groups until the event rule is configured as intended.

   NOTE: Selected groups or users without permission to the layout are shown in red text.

Additional Controls:

- The *Volume* slider is synchronized with the client volume in the Playback Panel.
- Click the **Test** button to preview playback in the current client session.

Interval of Action:

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Repeat Sound

Key Concepts:

- When the event rule is true and valid, this action will repeatedly send a prerecorded audio file to devices and/or users for playback.
- The *Repeat Sound* action is not available for instantaneous events.
- An assortment of audio files are provided.
- Authorized users can upload audio files of up to 30 seconds in length.
- Playback devices must be configured to support 2-way audio.
- Users must have the Play Audio permission.
- The *Repeat Sounds* action is only available for the following event types:
  - Analytics Event
  - Analytics Object Detected
  - Generic Event
  - Input Signal on Device
  - Motion on Camera
  - Soft Trigger

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

Sound:

Defines which audio file will be sent to the playback (*At*) device.

1. Click on the the current sound file name, or the *No Sound* text to open the selection dialog.
2. Select the audio file from the choices listed, or
3. Click the **Manage** button to open the sound file management dialog with the following choices:
   a. **Play** – play the selected file on the current client workstation.
   b. **Add...** will open a file selection dialog:
      - .WAV, .MP3, .OGG, and .WMA file types are supported.
      - Enter a custom title for the imported file or default to the imported file name.
      - Set a playback length of up to 30 seconds; longer files will be clipped.
   c. **Rename...** provide a dialog to rename sound file that currently exist in the selection menu.
   d. **Delete...** will delete the currently selected, user uploaded file. System sounds cannot be deleted.

At:

Select the cameras that will receive the audio file for playback.

1. Click on the *At* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. The search box will filter available cameras by name.
4. Selecting a server will automatically select all cameras attached to the server.
5. Select/deselect individual cameras until the event rule is configured as intended.

   Selecting the *Source camera* will always include the camera specified in the *Occurs At* (camera) setting within the WHEN panel.

To Users:

Select the users who will receive the *Open Layout* action:

1. Click on the *To Users* data field to open the selection dialog.

2. Slide the **Show all users** switch to display individual users – only groups are shown by default.
3. The search box will filter available users and groups by name.
4. Select/deselect users and groups until the event rule is configured as intended.

   NOTE: Selected groups or users without permission to the layout are shown in red text.

Additional Controls:

- The *Volume* slider is synchronized with the client volume in the Playback Panel.
- Click the **Test** button to preview playback in the current client session.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Send Email

Key Concepts:

- When the event rule is true and valid, this action generates and sends an Email to defined groups or specific users.
- A snapshot image of the camera feed is taken when the event happens.
- The log is updated with an entry for each Send Email action.
- An *Email service* must be properly Configured for this action to complete.
- Email addresses must be current and properly formatted in the setting for each user.
- Email will contain:
  - The event rule that triggered the Email.
  - The server sending the Email.
  - A snapshot from the *At* camera in the event rule.
  - An archive playback link for cloud connected Sites.
  - Available metadata from the event rule (label, date, time, IP address).
  - The support email and website URL configured in the Email Server settings.

Begin When:

The *Begin When* setting appears only for supported events, with options varying by event type.

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.

- *When event stops* is the moment the event rule was no longer true and valid

To:

This field defines which users will receive the Email.

1. Click on the *To* data field to open the selection dialog.
2. By default only user groups are shown with a **show all users** toggle switch available.
3. The search box will dynamically filter available users and groups by name.
4. Adjust the list of selected users until the event rule is configured as intended.

NOTE: An alert icon will be displayed when selected users do not have an Email address configured.

Additional Recipients**:**

- Enter any additional Email addresses to notify.
- Separate multiple addresses with a semicolon (**;**).
- No spaces are allowed in the receiving Email addresses.

Interval of Action*:*

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Send Mobile Notification

Key Concepts:

- When the event rule is true and valid, a push notification is send to the mobile device of selected users.
- The users must connected to the Cloud through the mobile application to receive push notifications.
- Mobile clients v20.1 or later are required to receive push notifications.
- Users can receive push notifications from multiple Sites that are connected to their account.

- Users can toggle or suppress notification on their mobile device.

Begin When:

The *Begin When* setting appears only for supported events, with options varying by event type.

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid

To:

Select the users who will receive the *Open Layout* action:

1. Click on the *To Users* data field to open the selection dialog.
2. Slide the **Show all users** switch to display individual users – only groups are shown by default.
3. The search box will filter available users and groups by name.
4. Select/deselect users and groups until the event rule is configured as intended.

   NOTE: Selected users without cloud accounts are shown in red text.

Header: (optional)

- Provide custom text that will replace the Site generated notification header.
- Find available metadata by staring with a open curly bracket {.

Body: (optional)

- Provide custom text that will replace the Site generated notification body.
- Find available metadata by staring with a open curly bracket {.
- Selecting **Add Source Device name to Body** to increase the information provided to users.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Interval of Action:

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

- Users without an accurate email address set in their profile are unable to receive Email notifications.

Set to Fullscreen

Key Concepts:

- When the event rule is true and valid, a specified camera on specified layout will change to full screen mode.
- Only one camera can be selected to open in fullscreen mode as part of this event.
- The layout selected in the rule must be the active tab or window when the event happens.
- Optionally rewind the archive by up to 5 minutes when opening in full screen

Begin When:

The *Begin When* setting appears only for supported events, with options varying by event type.

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid

Camera:

Select the camera that will open to full screen.

1. Click on the *Camera* data field to open the selection dialog.
2. The search box will dynamically filter available cameras by name.
3. Selecting *Source camera* to have the action camera always be the same as the event source.

On Layout:

Select the camera that will open to full screen.

1. Click on the *Camera* data field to open the selection dialog.
2. The search box will dynamically filter available cameras by name.
3. Selecting a server will automatically select all devices attached to the server.
4. Adjust the list of selected devices until the event rule is configured as intended.

   Selecting *Source camera* opens the *Occurs At* camera defined in the *WHEN* panel, if the Source camera is also on the selected layout.

Rewind:

The *rewind* feature will move the playback back the footage up by a predefined amount of time after opening in full screen.

1. Slide the switch to turn the rewinds feature on or off.

2. Enter an amount **For** how long the camera archive should rewind.
3. Select the unit of time measurement for the amount of time.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Show Desktop Notification

Key Concepts:

- This action with generate a Notification Panel entry for listed users.
- Cross Site Notifications requires a Show Desktop Notification action to cross sites.
- An optional **Forced Acknowledgment** function requires users to create a bookmark to dismiss the notification.
- Hovering over the Acknowledgment button opens a thumbnail with the device name and event time stamp.

Begin When:

The *Begin When* setting appears only for supported events, with options varying by event type.

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid

To:

This field defines which users will receive the desktop notification.

1. Click on the *To* data field to open the selection dialog.
2. By default only user groups are shown with a **show all users** toggle switch available.
3. The search box will dynamically filter available users and groups by name.
4. Adjust the list of selected users until the event rule is configured as intended.

   NOTE: Selecting **Force Acknowledgment** requires users to create a bookmark to dismiss the notification.

Interval of action:

The interval of action can prevent concurrent or incomplete actions when the same rule is re-triggered before action is complete.

- Move the slider switch to enable or disable the interval of action control.

- If enabled, a numerical value for the interval and a unit of measurements is required.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Show Text Overlay

Key Concepts:

- This action will display a text overlay on specific cameras when an event occurs.
- Site or device generated metadata may be available (device dependent).
- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** to discard any changes not applied and close the dialog.

At:

The *At* field defines the devices where the text overlay is rendered.

1. Click on the *On* data field to open the selection dialog.
2. The search box will dynamically filter available devices by name.
3. Selecting a server will automatically select all devices attached to the server.
4. Adjust the list of selected devices until the event rule is configured as intended.

   Selecting *Source camera* will display the text overlay on the source camera, when the event is bound to a (*At*) camera.

Duration Mode:

The *Duration Mode* appears only for supported events, with options varying by event type.

- *Of fixed duration* presents additional fields for when the event begins and the duration in time.
- *For the duration of the event* is define by the event and does not present a duration of time.

Begin When:

The *Begin When* setting appears only for supported events, with options varying by event type.

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid

Duration:

Enter a numerical value for the duration and a unit of time measurements for the text overlay to be displayed.

Custom Text:

- Enter the alphanumeric information to be displayed in the text overlay.
- Some devices and Sites can display metadata contained within { } curly brackets.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Show on Alarm Layout

Key Concepts:

- This action opens specified cameras in a dedicated *Alarms l*ayout tab.
- The *Alarms* layout tab includes the label "Alarms" in the title and an alert icon.
- Only one *Alarm Layout* tab can be open at a time.
- Users cannot manually add any elements to an open *Alarm Layout.*
- If several events are configured to show different cameras on an alarm layout for the same user, the corresponding cameras will be added to the active *Alarms* Layout upon the event occurrence.
- If several events are configured to show different cameras on the *Alarms* layout for different users, each user will see a separate Alarm Layout.
- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** to discard any changes not applied and close the dialog.

Begin When:

The *Begin When* setting appears only for supported events, with options varying by event type.

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid

Cameras:

This condition defines the cameras shown on the *Alarms l*ayout.

1. Click on the camera data field to open the selection dialog.
2. The search box will dynamically filter available cameras by name.
3. Selecting a server will automatically select all cameras.
4. Adjust the list of selected devices until the event rule is configured as intended.

   Selecting *Source camera* will ensure the Event *Occurs At* camera will always be on the *Alarms* layout.

To:

This field defines which users will receive the *Alarm Layout* notification.

1. Click on the *To* data field to open the selection dialog.
2. User groups are displayed by default. An option to **Show all users** is available via a slide switch.
3. The search box will dynamically filter available users and groups by name.
4. Adjust the list of selected users until the event rule is configured as intended.

Force Alarm Layout Opening:

- Selecting this option will force the *Alarms* layout to become the active layout tab and take focus from the current layout.
- If **Force Alarm Layout Opening** is disabled, the *Alarms* layout will open in the background and will not take focus.

Rewind:

The *rewind* feature will move the camera playback position by a predefined amount of time after opening the *Alarm Layout*.

1. Slide the switch to turn the *Rewind* feature on or off.
2. Enter an amount *For* how long the camera archive will rewind.
3. Select the unit of time measurement for the *Rewind* value.

Interval of Action:

Enable the an *interval of action* control to prevent duplicate actions or restarting the action before it is complete/

- Used the slider switch to enable or disable the interval of action control.
- If enabled, a numerical value for the interval and a unit of time measurements is required.
- When enabled, the action will only happen once within the defined interval of action.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.

- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Site HTTP(S) Request

Key Concepts:

- When the event rule is true and valid, a HTTP(S) Request is sent to a Site endpoint.
- This method allows an event to make an internal Site API call.

Begin When:

The *Begin When* setting appears only for supported events and the following options will varying by event type:

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

Endpoint:

Enter the Site endpoint that will receive the content of the request.

Method:

Select the method to be sent:

  - GET
  - POST (default)
  - PUT
  - PATCH
  - DELETE

Content:

Enter the complete body of the request to be delivered to the URL, including any Event Field Metadata.

Interval of Action:

To avoid overlapping actions, enable the *interval of action* and set the *Once in* duration to be longer than the execution time of the action.

- Move the slider switch to enable or disable the *interval of action* control.
- If enabled, a numerical value for the *interval of action* and a unit of measurements is required.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.

- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Speak

Key Concepts:

- This action will pronounce the specified *Text* using machine generated speech.
- Text to speech is performed locally without internet-connected services.
- Speech can be delivered to one or more devices, user groups, and/or specific users.
- Playback quality can be influenced by the configuration of rendering devices.

Begin When:

The *Begin When* setting appears only for supported events, with options varying by event type.

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid

Text:

- Enter the text that will be converted into machine generated speech.
- Use the **Test** button speak the text on the local client.

At Device:

The *At Device* field defines which devices will receive speech file for playback.

1. Click on the *At Device* data field to open the selection dialog.
2. Slide the **Show all cameras** switch to make additional, possibly incompatible cameras appear in red text.
3. The search box will dynamically filter available devices by name.
4. Selecting a server will automatically select all devices attached to the server.
5. Adjust the list of selected devices until the event rule is configured as intended.

   Selecting *Source camera* will ensure the spoken text is always sent to the Event *Occurs At* camera.

To Users:

This field defines the users that will receive the spoken audio for playback in their client.

1. User groups are displayed by default. An option to **Show all users** is available via a slide switch.
2. The search box will dynamically filter available users and groups by name.
3. Selecting a group selects all users in the group.

NOTES:

- Selected users may not have the audio playback permission required.
- Local workstation settings may mute or disable local audio playback.

Additional Controls:

- The *Volume* slider adjusts the amplitude of the transmitted audio file while local workstations and devices, where local audio setting and speaker hardware will also influence the sound playback.
- Click the **Test** button to preview the machine rendered speech on the current client.

Interval of Action:

Enable the an *interval of action* control to prevent duplicate actions or restarting the action before it is complete/

- Used the slider switch to enable or disable the interval of action control.
- If enabled, a numerical value for the interval and a unit of time measurements is required.
- When enabled, the action will only happen once within the defined interval of action.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Write to Log

Key Concepts:

- The action writes a record to the event log when the event rule is true and valid.
- No device changes are made and no user notifications are generated by this action.

Begin When:

The *Begin When* setting appears only for supported events, with options varying by event type.

- *When event occurs* is the moment an instantaneous events occurs.
- *When event starts* is the moment the event rule became true and valid.
- *When event stops* is the moment the event rule was no longer true and valid.

Interval of action:

- Move the slider switch to enable or disable the interval of action control.
- If enabled, a numerical value for the interval and a unit of measurements is required.

- Is a method to reduce concurrent or incomplete actions when the same rule is re-triggered before action is completeBy default, all events mentioned in rules are written to the log.

Dialog Controls:

- Click **Apply** to update the event rule and keep the dialog open.
- Click **OK** to save settings and close the dialog.
- Click **Cancel** or use the close window control to discard any changes not applied and close the dialog.

Event Field Placeholders

Key Concepts:

- The actions Do HTTP(s), Send Mobile Notification, Site HTTP(S) Request, and Speak can use field parameters to insert Site metadata.
- Field parameters must be contained within curly brackets { } and adhere to applicable syntax rules where they are used.
- The resolved content and syntax of the populated parameters can vary per originating device or Site configuration.
- Action field parameters for populated when the the action begins and may be subject to minor lag for time based values.
- When event field parameters are used with the speak action, label will be spoken during tests and the value of the filed will be spoken when the event rule is true is and valid under normal operating conditions.

Available Parameters:

The following examples are provided for reference only, available parameters and contents are subject to device and Site settings.

Parameter Label	Description	Example
{device.name}	• The name of the resource (device) that generated the event. • For Site events this will be {site.name}.	• Hallway camera • Basement server
{device.type}	• The type of the resource (device) that generated the event. • For the Site events, this will be {site.name}.	• Camera • ACME-Site
{event.caption}	• The user-provided caption is used when available (Generic Event, Analytics Event, Integration Diagnostic Event).	• Camera Disconnected • Generic Event • Custom User Caption

Parameter Label	Description	Example
	• For an Analytics Event, if caption is not provided, then the caption is substituted with the event type (Line Crossing, People Detection). • Otherwise, the name of the event that is used in Event rules and Event logs is used.	• Line Crossing
{event.description}	• Generic event or analytics event description. • Will return empty string for all other events.	Description text
{event.name}	Name of the event used in the event rule and the event log.	Camera disconnected
{event.source}	• Generic event source. • The value of {device.name} for all other events.	• Keyword • Custom text
{event.time}	Date and time of the event in ISO8601 format	2024-01-13T09:11:23+00:00
{event.timestamp}	The Current Epoch Unix Timestamp	1644422205
{event.timestampMs}	The Current Epoch Unix Timestamp in milliseconds	1644422205
{event.timestampUs}	The Current Epoch Unix Timestamp in microseconds	1644422205
{event.type}	Same as {event.name}	Camera disconnected
{server.name}	• The name of the server that generated the event. • Or the name of the server connected to the resource that generated event.	• Garage Server
{site.name}	The name of the Site where {server.name} is connected.	Warehouse

Event Scheduling

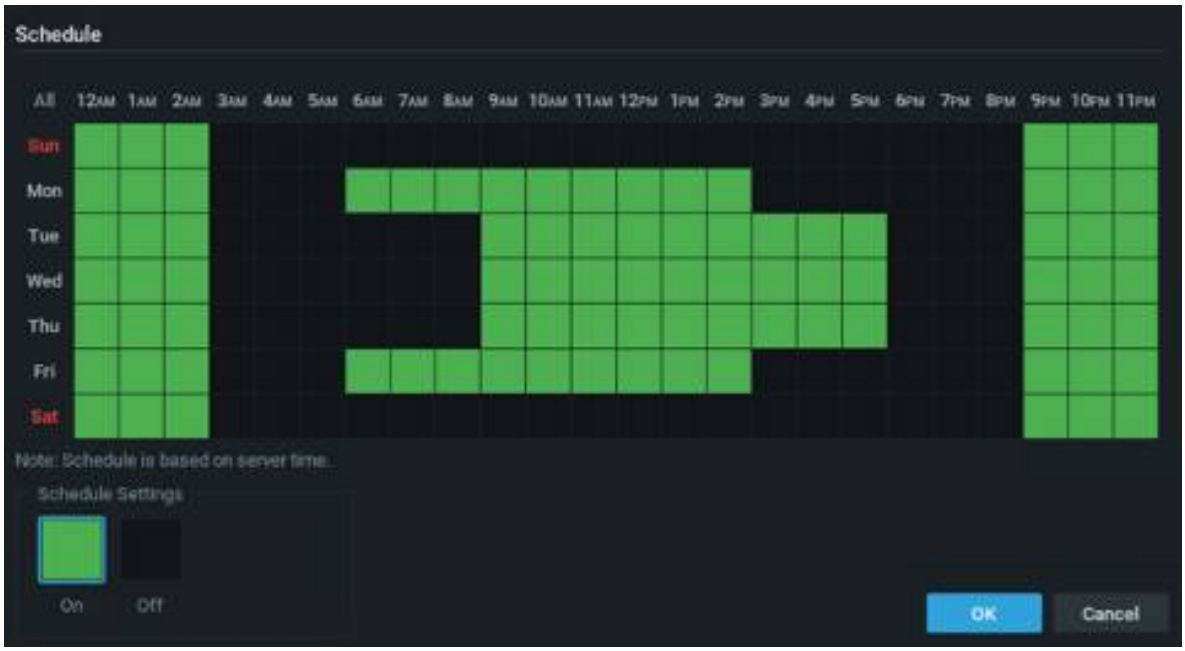
Key Concepts:

- As a default setting, all included and new events are scheduled continuous monitoring (24 hours a day, 7 days a week).
- Site-generated events are always being monitored and cannot be placed on a schedule.
- The monitoring of user-defined events can be set to run in one-hour increments that span a repeating 7 day week.

- A common schedule can be bulk applied to multiple rules when done from the Event Rules List.
- It is possible to disable a rule entirely by setting every hour of the week to be **OFF**.

To Set an Event Schedule:

1. Open the scheduling widget from within the event rule dialog, or from the event list where bulk scheduling is possible.
2. Click the **On** or **Off** button to determine monitoring behavior in specific 1-hour cells from 12AM to 11PM.
3. Click in a cell to apply the selected schedule setting to cells, or use these shortcuts to apply to multiple cells:
    - **Click**-and-**drag** to select multiple cells.
    - Click the hour heading to select an entire column.
    - Click the day of the week to select an entire row.
    - Click **All** to select all cells.
4. Click **OK** to accept or **Cancel** to discard changes.ads



Lookup Lists

Lookup lists expand the functionality of Event Rules by enabling a range of values and wildcards to be applied to decision making logic. This can reduce the effort required to maintain rules and enable fewer rules to cover a greater range of conditions by managing one list instead of multiple rules.

Key Concepts:

- Lookup Lists can only be created and modified by Administrators and Power Users from within the Desktop Client.
- The contents of a Lookup List are continuously applied to all instances where the Lookup List is referenced.
- The wildcards of (?) for an individual character and (*) for all remaining characters are supported in Lookup Lists.
- Lookup Lists can be exported as a .CSV file and imported from .CSV, .TXT, or .TSV file types.
- New installations include empty, generic lists types named Allowed and Blocked that cannot be restored if deleted.

Example User Cases:

- Open a gate when a detected license plate is on an *Allowed* list.
- Trigger an alert when a detected license plate is on a *Blocked* list.
- Execute an action when an object described (size, color, shape) by an Object list is detected.

Types of Lookup Lists:

- **Generic Lists:**
  - Can be used in Analytics Events, Analytics Object Detected Events, Generic Events, and Plugin Diagnostic Events.
  - Are created without association to any specific plugin, device, or rule.
  - Only contain one data field (column) and function similar to a list of keywords.
  - Are tested against any entry on any word in the caption, the source, the description, and on any attribute value for an object.
- **Object Lists:**
  - Can only be created in reference to a supported Object Detection plugin.
  - Are used when there is a need to check for multiple attributes of a detected object.
  - Can only be used in Analytics Object Detected Events and only for the same object type.
  - A compatible camera and object must first be selected before the object list will appear as an option.
  - Are checked for each attribute value from the list entry to the corresponding attribute values from the object, and they all must match.
  - Permit users to select the attributes to include, all others will be ignored when testing for a match.
  - Will treat all empty values as "Any" when testing for a match.
  - Require at least one attribute value to be defined and not empty nor set to any.

Lookup List Attributes:

- *List name* – a user defined label for the list.
- *List type* – select from the following list types:

- *Column* – user defined field ("license plate") that will contain values to be examined.
- *Value* – contains values for a defined column, for example the license plate values to be examined.

Import Export Considerations:

The topic pages for Generic Lists and Object Lists contain list import and export instructions.

Generic Lists

The information provided on this page is specific to the Generic Lookup list type.

Create a Generic List:

1. Open **Main Menu > Lists Management**,
2. Atop the *Lookup Lists* dialog, select the **New List...** button,
3. Enter a name for the new list.
4. Select the *Generic List* type.
5. Enter a name for the list column (data field).
6. Click the **Create** button to progress to the list content dialog.

Configure or Delete a Generic List:

1. Open **Main Menu > Lists Management**.
2. Atop the *Lookup Lists* dialog select an existing generic list from the pull-down menu.
3. Click on the **Settings** icon to edit the list and column name.
4. Use the **Delete** icon to remove the generic list.

Define the Values in a Lookup List:

1. Open **Main Menu > Lists Management**.
2. Atop the *Lookup Lists* dialog select an existing generic list using the pull-down menu.
3. Click the **+Add** button to add a new value to the list.
4. Click on an existing value in the column to edit the value.
5. Use the checkbox to select values to delete, then click the **Delete** icon.

Import Values to a Generic List:

Generic Lookup Lists can quickly be populated using existing data.

1. Open **Main Menu > Lists Management**.
2. Atop the *Lookup Lists* dialog, use the pull-down menu to select an existing (generic) list where the imported data will be placed.
3. Click the icon labeled **Import** that is between the **+Add** button and the icon labeled **Export**.
4. Browse to and select the (list) file to be parsed for import:
   a. .CSV, .TXT, or .TSV file types can be imported.

b. Select the character that is used to separated values within the imported values.

5. Nx Witness will attempt to parse the list and generate a preview within the *Import Options* dialog.
6. Confirm the state of the *Data Contains Header* checkbox matches the file to import
7. Click the **Import** button if the preview is correct.
   a. Imported data will be appended to existing data.
   b. Erroneously imported data and duplicates must be manually removed from the list.
   c. Values in the revised list, after import, can be edited before being committed.
8. Click the **Apply** button to commit and deploy list changes without closing the Lookup List dialog.
9. Click the **OK** button to close the Lookup List dialog.

Export a Lookup List:

The contents of a list can be export for external modification or other usage.

1. Open **Main Menu > Lists Management**,
2. Atop the *Lookup Lists* dialog select an existing list using the pull-down menu.
3. Click the **Export** button.
4. Browse to the location where the file will be exported.
5. Confirm the file-type and file name the list will be exported to.
6. Click **Save** to export the Lookup List.
7. The export confirmation dialog includes an option to open the 'save to' location.

Object Lists

The information provided on this page is specific to the Object Lookup list type.

Create an Object List:

1. Open **Main Menu > Lists Management**,
2. Atop the *Lookup Lists* dialog, select the **New List...** button,
3. Enter a name for the new list.
4. Select the List Type for the new list.
5. Enter a name for the list column(s) in a generic list, or
   Select a predefined name of the column(s) in an object list.
6. Proceed according to the Configure a Lookup List section.

Configure or Delete a Lookup List:

1. Open **Main Menu > Lists Management.**
2. Atop the *Lookup Lists* dialog select an existing list using the pull-down menu.
3. Click on the **Settings** icon to open the List Settings dialog containing the following options:

a. Select the current list name to edit the list name.

b. Click the **Delete icon** to remove the entire list and all data.

c. Use the checkbox to add or remove an attribute column from the Lookup List.

NOTE: All values in the (attribute) column are lost when a column is removed from a list.

Define the Values in a Lookup List:

1. Open **Main Menu > Lists Management.**
2. Atop the *Lookup Lists* dialog select an existing list using the pull-down menu.
3. To add a new entry:
   a. Click the **+Add** button to add a new value to the list.
   b. The *Add Entry* dialog box will open to configure the new list entry.
   c. Attributes with a defined list of values will present a pull-down menu of available choices.
   d. Attributes without a defined list of values will be populated with *Any <attribute>* text – click on the text to enter a custom value.

   NOTE: An entry can be added to an object list by right clicking on the card in objects tab. The list must be of the same object type, only those attributes will be saved, for which a list has columns, any not detected attributes will be treated as empty = "Any". The entry won't be added, if the resulting entry will have all attribute values = "any". Values
4. To edit an existing entry:
   a. With the list contents displayed as a table, click on the attribute data to change.
   b. Columns constrained to a predefined list will present a pull-down menu to value selection.
   c. Click on *Any <attribute>* text to open the free form entry mode and provide a value.
   d. Click the **Apply** button to save and deploy list changes while keeping the dialog open.
   e. Click **OK** to deploy list changes and close the dialog.
5. To delete values, first select the values to remove with the selection boxes, and then click the **Delete** button.

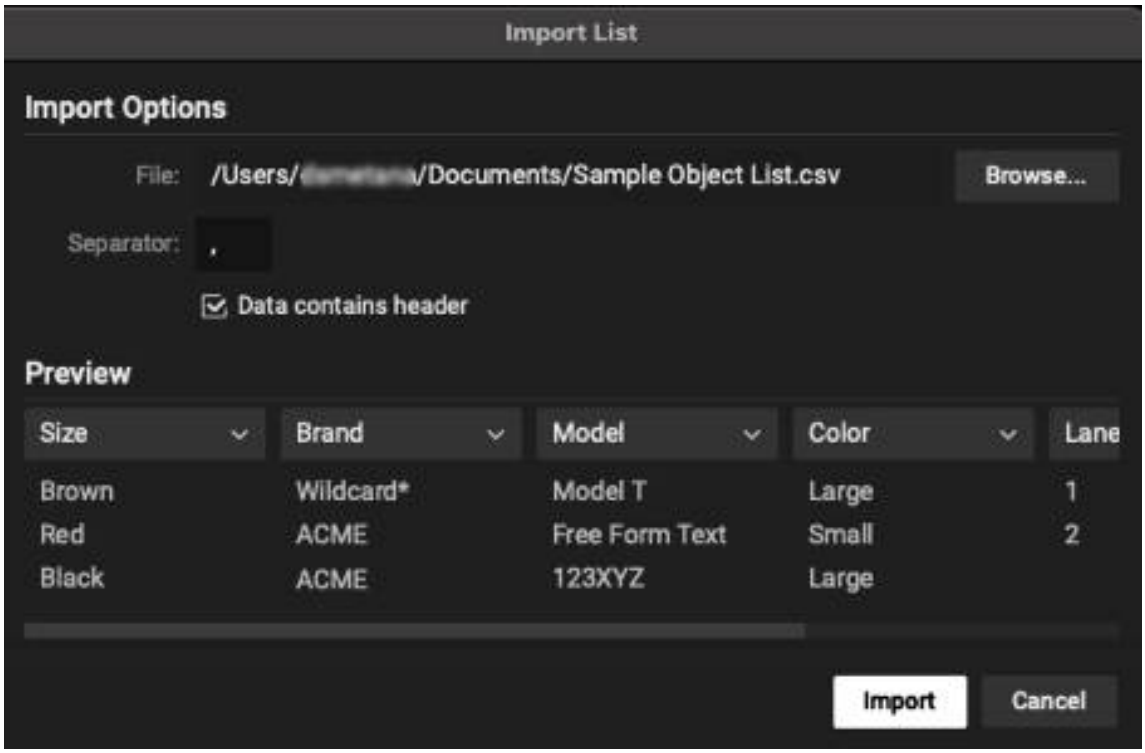
Import an Object Lookup List:

1. Open **Main Menu > Lists Management**.
2. top the *Lookup Lists* dialog, use the pull-down menu to select an existing (object) list where the imported data will be placed.
3. Click the icon labeled **Import** that is between the **+Add** button and the icon labeled **Export**.
4. Browse to and select the (list) file to be imported and click the **Open** button.
   a. The file to import must have same number of columns as the Object list
   b. While any basic alphanumeric character can be a column separator, each line entry must end with a line feed / carriage return.

5. Nx Witness will attempt to parse the list and generate a preview (*Import Options* dialog) using the following defaults:
   a. *Data contains headers* checkbox is selected.
   b. Separator is a comma for .CSV files and the TAB character for .TSV files.
2. Inspect the import preview and make any changes to the data mapping:
   a. The parsed data is previewed as a table within the *Import Options* dialog.
   b. Use the pull-down menus in the Preview headings to correctly map attributes to data columns within the file to import.
   c. Each object attribute can only be used once – aligning an attribute to a different data column will set the previous heading to *Select attribute*
   d. The **Import** button will remain disabled until all headings are either mapped to data, or set as *Do not import*.
   e. A manual mapping dialog is presented when the data parsed from the file to import does not match the available object attributes.

      EXAMPLE: (with mixed headers and data)

      - The attribute type for the left-most column is *size* while the data contains *color* values.
      - The attribute type for the forth column from the left is *color* while the data contains *size* values.
      - Remap the headings by using the pull-down menus.



NOTE: Within object lists, attributes can be manually map to columns if there's an enumeration with fixed set of values, example:

If available color attributes are [brown, red, black], and an imported data "magenta", the user must map this value (magenta = red).

3. Click the **Import** button when all data mapping is set.
4. Imported data will be appended to existing data.
   a. Erroneously imported data and duplicates must be manually removed from the list.
   b. Values in the revised list, after import, can be edited before being committed.
5. Click the **Apply** button to fully commit the list changes and the **OK** button to close the import dialog.

Export a Lookup List:

1. Open **Main Menu > Lists Management**,
2. Atop the *Lookup Lists* dialog select an existing list using the pull-down menu.
3. Click the **Export** button.
4. Browse to the location where the file will be exported.
5. Confirm the file-type and file name the list will be exported to.
6. Click **Save** to export the Lookup List.
7. The export confirmation dialog includes an option to open the 'save to' location.

Viewing and Exporting the Event Log

Each event that occurs in Nx Witness is stored in the **Event Log** and displayed in the "Events Tab". The Event Log make it easy to navigate through past activity and diagnose Device or Server issues.

To View the Event Log:

- Open **Main Menu** > **Site Administration** > **General** tab and click on the **Event Log** button.
- Open the context menu by right-clicking anywhere on the Notification Panel, then choose **Event Log.**
- Use the **Ctrl+L** shortcut.

To search the Event Log:

The search box found at the top right of the Event Log will allow you to search the descriptions of all logged events for your desired keyword(s).

To sort the Event Log:

Events are displayed in the following columns. You can click on any column header to sort the log in ascending or descending order:

- *Date/Time* – Date and time the event occurred.
- *Event* – The type of event.
- *Source* – The resource that initiates the event: device (motion detection, input signal, etc) or Server (storage issue, Server failure, etc).
- *Action* – The action that is performed when the event occurs.

- *Target* – The Users or Devices that are recipient of the action.
- *Description* – Any additional information. For motion detection events, the description includes a hyperlink that will open the device in a new layout and start playback of the event.

To Filter the Event Log using the Header Menus:

- *Start date* and *End date* – Select a day in each of these calendar fields to show only events that occurred during a particular time period. Default display is the current day. Dates are shown in dd/mm/yyyy format.
- *Event type* – From the drop-down menu, select an event category (*Any Event*, *Any Device Issue, Any Server Issue, Analytics Event, Generic Event*), or specific type of event within those categories.
- *Device type* – Display events occurring on a particular device only (applies to Motion, Input and Device Issues).
- *Action* – Display only the events caused by a particular action.

Click the **Clear Filter** button to remove all filter conditions. Click the **Refresh** button to apply additional filter criteria to list that is already filtered.

To Filter the Event Log using Event Fields:

You can also use the context menu of an existing record to filter the Event Log according to that record. For example, if you **right-click** on a specific record and choose **Filter Similar Rows**, only the events occurring on the same source and event will be displayed. To clear all existing filters, click **Clear Filter** at the top right or open the context menu on an existing record and choose **Clear Filter**.

To View the Event Log for a Specific Device or Server:

- *Device* – Open the device context menu and select **Check {*device type*} Issues**.
- *Server* – Open the Server context menu and select **Server Diagnostics**.

Other Event Log Functionality:

Context menus in the Event Log provide different options, depending on the field (event, source, action, etc.) from which they are opened. The following options are available from the context menu for all fields:

- *Select All (Ctrl+A)* – Selects all entries in the log.
- *Export Selection to File* – Saves the selected data to an HTML or CSV text file.
- *Copy Selection to Clipboard* – Copies the selected data to your clipboard.

Context menus in the *Source* field provide several additional functions, depending on the device.

You can drag the mouse or use **Ctrl**+**Click** or **Shift**+**Click** to select multiple and apply the desired option to multiple events.

To Export Event Logs:

This may be requested once contacting technical support. See "Contacting Support".

1. Open **Main Menu** > **Site Administration** > **General** > **Event Log**.
2. If desired, filter by event or camera.
3. Select the events to be exported, or use the context menu to select all.
4. Open the context menu and choose **Export Selection to File**.
5. Choose the save location, enter a file name, and select the file type:
   - *.html*
   - *.csv*
6. Save the file.

Users and Groups

Key Concepts (Users):

- User accounts are defined by both a User Type and a set of Permissions that are granted through Group membership and/or directly granted to the user account.
- A user must log in to a Site before they can perform any permitted actions.
- Once a user account is created, the (user account) type cannot be changed.
- An administrators can create and configure any Site user.
- Power Users can not create or configure Administrators or other Power Users.
- The Desktop Client must be used to create or change Temporary Users.
- Users can be Enabled, Disabled, Deleted (local user), or Removed (cloud user), using the Desktop Client, the Web Admin client, and the Cloud Portal.
- Users imported from a Lightweight Directory Access Protocol (LDAP) Server will use their existing credentials to connect to a Site.
- LDAP Users can be configured as individual users or placed into existing Site groups.

Key Concepts (Groups):

- A group is a collection of users who share a common set of permissions via group membership.
- Built-In groups have a set of predefined permissions that cannot be changed.
- Custom groups can be configured to provide a unique set of Site permission to group members.
- Custom groups can be created and configured by *Administrators* and *Power Users*.
- Permission changes made to a custom group are equally applied to all users in the Group.

- Users in nested groups inherit permissions from every group their group is a (nested) member of.
- LDAP Groups can be imported and managed as a Custom Group (see "LDAP Users and Groups").

See "Managing Users", "Managing Groups", and managing "LDAP Users and Groups" for more information.

NOTE: The dialog to configure User Permissions and Group Permissions is the same (see "Permissions Management").

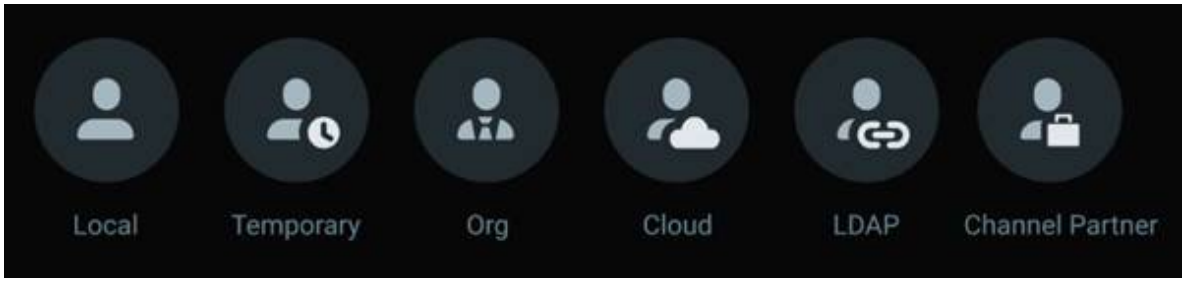
User Management

There are many places where user management tasks can be performed. This section covers the following topics:

- User Types
- Adding Users
- Configuring Users
- Managing Temporary User Access
- Enabling and Disabling Users
- Deleting and Removing Users

User Types

The following types of Users can be present in the Site and are identified in lists with specific icons; grayed out icons indicate that the user account is currently disabled.



- *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, a preset expiration date, and an optional session length 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 connect the Cloud portal.
- Receive a URL to connect to a specific Site; no password is required and the link can be used by anyone.

- *Organization (Org) Users:*
  - Are created outside of the Desktop Client, Mobile Client, or the Web Admin clients.
  - 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 all Sites within the Organization, or only a subset of Sites in the Organization.
  - Permission granted at the Organization level can only be changed by an Organization Administrator.
  - Site-level permissions, including Global Permissions, can be 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, where the user has access permissions.
- *Cloud Users:*
  - Reside in the Cloud and can exist without having access to a Site.
  - Use the Desktop Client, Mobile Client, Web Admin interface, or the Cloud Portal 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 when imported.
  - 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 to Resources and added to both Built-In and Custom Permission Groups.
  - Cannot be permanently deleted from a Site as LDAP users are re-imported during each LDAP sync.

NOTES:

1. LDAP Users will be imported (as disabled) when there is already the same username in the Site.
2. To block access by an LDAP user, the user account must be removed from the LDAP server or disabled in the Site settings.
3. Disable an LDAP user when there is a need to retain user entries in the Audit Trail of User Actions.

- *Channel Partner Users:*
  - Are created outside of the Desktop Client, Mobile Client, or the Web Admin interface.
  - Are managed at the Channel Partner level by the Channel Partner Administrator, and at the Organization level by the Organization Administrator.
  - Are only displayed in User Management dialogs and Site User lists when they are granted Site-level permissions.
  - Inherit permissions from their Channel Partner that cannot be changed by Site Administrators or Power Users.
  - Site-level permissions, including Global 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 where they have access permission.
  - 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.

The following topics are structured around how to perform common User Management tasks:

- Adding Users.
- Configuring Users.
- Managing Temporary User Access.
- Disabling and Enabling Users.
- Deleting Users.

Adding Users

Know the User Type to be added before starting the process as User Type cannot be changed once set. A User must be deleted and added again to change 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 will be Added to a Site without access to Site Resources if they are not a member of a Permission Group, or assigned Permissions using the Desktop Client (see "Configure Users").

Adding a User using the Desktop Client

1. Open the *Add User* dialog by selecting **Main Menu > Add > User.**
2. Confirm the *New User* dialog box is open to the *General* tab.
   - Information on the *General* tab is required to create a user.
3. Select to add a User as Enabled or Disabled (see "Enabling and Disabling Users").
4. Choose the User Type.
   - *Cloud*: Enter the Email address of the User to add. Cloud Users cannot be Temporary Users.
   - *Local*: Enter the following information.
     - Login.
     - Full Name.
     - Email address.
     - Access type – Select **Regular** or **Temporary**.
       - Set time limitations when Adding Temporary Users (see "Managing Temporary User Access").
       - 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. 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.
2. Expand **Users** in the left panel navigation.
3. Click the **Add User** button.
4. Enter the Email address of the User to add.
5. Optional – Select the Permission Groups the Added User will be a member of.
6. Click **Add User** to complete the process. Authentication may be required.

NOTE: Established Cloud Users will see the Site on their Welcome screen and new Cloud Users will receive further instructions by Email.

Configuring Users

Key Concepts:

- There are two components to user account configuration; user identity and user permissions.
- Only Administrators can add or configure Power User accounts.
- Administrators and Power Users can manage others users.
- A user can be granted Site permissions directly to their account and/or through membership in permission groups.
- User management and group permission controls can be accessed from multiple dialog and menu locations.
- The permission configuration screen for users and groups is the same.
- Organization user can be granted access to Site resources and groups using the Desktop Client, Web Admin, and Cloud Portal clients.

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

To Configure a User in the Desktop Client

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 a **User** to open the configuration dialog.
   - User configuration changes are limited to Enabling and Disabling Users when multiple Users are selected.
3. Make changes in the *User Settings* tabs as outlined below.
   - The *General* tab contains:
     - User identity attributes (Name, Email) of non-LDAP Users
     - Current permissions group membership for the user.
     - The user's *Notification Language* selection.

       NOTE: Changing the *Notification Language* selection will only affects new notifications, not existing (active) notifications, the notification panel controls, nor informers. The user interface language selection is located in the Look and Feel dialog.
   - The *Groups* tab selects which Groups the User is a member of.
     - LDAP group membership cannot be changed within the Desktop Client.
   - The *Resources* tab is used to view and Manage Permissions.
   - The *Global Resources* tab defines:
     - If the User is permitted to view the Event Log.
     - If the User is permitted to generate Events.

4. Click **Apply** to save edits and keep the dialog open, or Click **OK** to Apply changes and close the dialog. Authentication may be required.

To Modify a User using the *Web Admin* / *Cloud Portal*

1. Select **Settings** in the page header menu.
2. Expand the list of **Users** in the left panel.
3. Click on a User to open the configuration dialog.
   - Local Users can be Enabled, Disabled, or Deleted – Group Memberships, Name, Password, and Email can be updated.
   - Cloud Users can be Enabled, Disabled, Removed from the Site, or have their Group Memberships changed.
   - Temporary Users can be Enabled, Disabled, or Deleted.
   - LDAP Users can be Enabled, Disabled, and have their non-LDAP Group memberships changed.
   - Organization users can have their Site-level group membership changed.
   - Channel Partner users can have their Site-level group membership changed and they can also be removed from a Site.
4. Configure available User attributes and Click **Save**. Authentication may be required.

NOTES:

- Users inherit Permissions from direct and nested Group Memberships.
- See granting Channel Partner Access to Sites for Channel Partner settings

Managing Temporary User Access

Temporary Users receive a unique URL link that provides access to a Site through either the Desktop Client or the Web Admin. The Temporary User URL does not require a password and can be used by anyone (see Connecting as a Temporary User").

- Only Administrators and Power Users can create or modify Temporary Users.
- Temporary User must be configured with a future expiration date.
- Temporary Users can be added and configured at the Desktop Client only (except Status).
- Temporary Users can be members of any Groups that do not include Administrative or Power User permissions.
- The Audit Trail of User Actions captures the activity of Temporary Users.
- Temporary Users can be Enabled, Disable, or Deleted in the Desktop Client, Web Admin, and Cloud Portal.
  - Disabling a Temporary User disables the Temporary link, it does not change the configuration of the Temporary User.

Generating a Temporary Link

NOTE: Generating a Link for a Temporary User with an existing Link will invalidate the existing link and close any open sessions.

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. Open the User by doing one the following.
   - Clicking on the User name in the list.
   - Selecting the checkbox for the User and clicking the **Edit** icon.
     - Selecting multiple Users will limit the edit dialog to batch Enabling and Disabling of Users.
3. Click the **New Link**… button to open the *New Link* configuration dialog.
4. Select the date the Link is *Valid Until.* Server date is used for this required value.
5. Check the *Revoke access after login* box to define an expiration timer that will start when the link is used (optional).
   - If *Revoke access after login* is selected, than a value between 1 and 999, in minutes, hours, or days must be provided.
6. Click the **Create** button. Authentication may be required.
7. Copy the link and provide it to the intended User (see "Connecting as a Temporary User").

Terminating a Temporary User Link

NOTE: This will quickly log the Temporary User out of an active session.

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. Open the User to modify by doing one the following.
   - Clicking on the User name in the list.
   - Select the checkbox for the User and click the **Edit** icon.
     - Selecting multiple Users will limit the Edit dialog to batch Enabling and Disabling of Users.
3. Click the **Terminate** button to disconnect the User and terminate the previously provided link.
4. Confirm and authenticate if prompted.

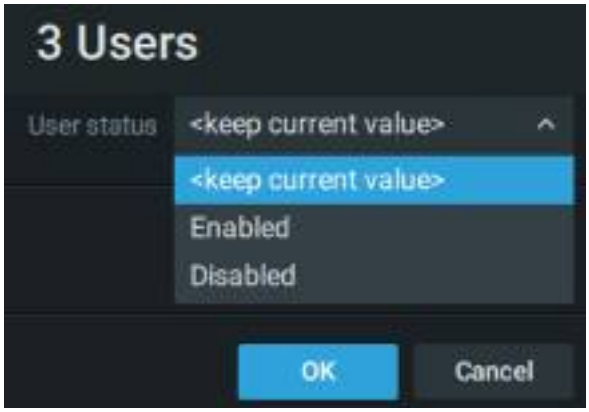
Enabling and Disabling Users

Enabled Users can access the Site according to their Permissions while a Disabled User is prevented from accessing the Site by any method. Unlike Deleting a User, Disabling a User preserves existing User information in the database and the User can again be Enabled with previous Permissions and settings unchanged.

- Administrators and Power Users can Enable or Disable Site Users in the Desktop Client, Web Admin, and Cloud Portal.
- Power Users cannot Enable or Disable Administrators or other Power Users.
- The Audit Trail of User Actions retains all entries for disabled users.
- Disabled Users will be disconnected from the Site and Email notifications will stop.
- Layouts created or shared by disabled users will remain available to other users.
- Organization and Channel Partners users cannot be disabled.

Enabling and Disabling Users in the Desktop Client

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. To disable or enable a single User:
   - Click on the User name in the list, or select a single checkbox and Click **Edit** to open *User Properties*.
   - Change the toggle to Enabled (Green) or Disabled (Gray).
3. To Enable or Disable multiple Users at once:
   - Select the checkbox next to each User to Enable or Disable.
   - Click the Edit button to open the multiple User Enable or Disable dialog.
   - Choose if all selected Users are to be Enabled or Disabled.



4. Click **OK** to Apply changes. Authentication may be required. Disabled Users will be disconnected from the Site.

Disabling and Enabling Users using the *Web Admin* / *Cloud Portal*

1. Select **Settings** in the page header menu.
2. Expand **Users** in the left panel menu.
3. Select a User to display User Properties.
4. Change the toggle to Enabled (Green) or Disabled (Red).
5. Click **Save** to Apply changes. Authentication may be required.

NOTE: Disabled User will be disconnected from the Site.

Deleting and Removing Users

Key Concepts:

- Local Users can be deleted from the Site they reside in while Cloud Users can only be removed from a Site. Removing a Cloud User from a Site does not delete the Cloud User Account.
- Deleting a User from a Local Site is instantaneous, permanent, and complete.
- Deleting a User cannot be undone.
- The Audit Trail for deleted users is retained in the Site data.
- Administrators cannot be deleted or removed from a Site.
- Only Administrators and Power Users can delete or remove users.
- Power Users cannot delete or remove other Administrators, Power Users, or their own account.
- Users can be deleted or removed in the Desktop Client, Web Admin, and Cloud Portal.
- LDAP Users cannot be deleted until the LDAP Server is disconnected.
- In the Desktop Client multiple users can be deleted in one action.
- Deleting or removing a User will close all active sessions and prevent further access to the Site.
- Organization users cannot be deleted or removed from a Site.
- Channel Partners Users can be removed from a Site; this hides the Channel Partner user in the User Management interface while retaining their inherited permissions.
- Layouts available only to the deleted User will be removed from the Site.

NOTE: If "*Do not show this message again*" has been previously checked, you will not be prompted to confirm a User deletion and the action will be instant and permanent. To re-enable confirmations open **Local Settings** > **Advanced** and click the **Reset All Warnings** button.

Delete a User in the Desktop Client

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.

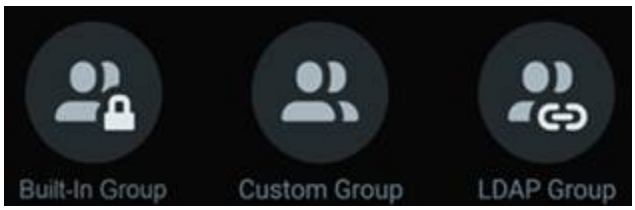
2. Do one of the following
   - Click on the User to open the User settings and then select the **Delete** button on the right side of the dialog box.
   - Click the checkbox next to each User to be deleted, then select the **Delete** Icon in the banner.
3. Confirm if prompted. Authentication may be required.

Delete or Remove a User in the *Web Admin* / *Cloud Portal*

1. Select **Settings** in the page header menu.
2. Expand **Users** in the left panel navigation.
3. If needed, use the *Search* box to narrow the list of users.
4. Select the User to delete or remove, this will open the User Settings dialog:
   - Click **Delete User** to delete Temporary or Local Users.
   - Click **Remove User** to remove Cloud Users from the Site.
5. Confirm if prompted. Authentication may be required.

Group Configuration

Groups are a powerful method to organize Users and simplify Permissions Management. There are three types of groups:



- *Built-In Groups*
  - Provide predefined access to Settings and Resources.
  - Cannot be modified or changed (see "Built-In Groups and Permissions").
  - *Administrators* and *Power Users* are the only Groups that can edit Site settings.
  - There are six predefined, Built-In groups, that are listed in order of decreasing permissions – Built-In groups have the permissions of each group below it.
    1. Administrators
    2. Power Users
    3. Advanced Viewers
    4. Viewers

5. Live Viewers
6. Site Health Viewers

- Except for the Built-In Administrator group, all Built-In groups can contain Custom Groups as members who inherit permissions from the Built-In Group.

- *Custom Groups*
  - Can be configured with a Permission set tuned to business policies and unique operational needs.
  - Are created and managed by members of the Built-in Administrators and *Power Users* Groups.
  - Can be members of the Built-In Power Users Group to access some Site and resource settings.
  - Can be members of any Built-In Group, except for the Administrators Group.
  - Inherit the permissions from all direct-parent groups and all grandparents at any level.
  - Cannot be configured to grant members access to change Site and Server settings.
  - Temporary Users cannot be added to any Custom Group that inherits Power User permissions.
- *LDAP Groups*
  - Can be imported with existing LDAP User members.
  - Can be managed similar to a Custom Group but their membership and group name can be changed on the LDAP Server only.
  - May have a duplicated Group name if a similar Group exists in the Site.

  See LDAP Users and Groups for configuration settings, warning banners, and related details.

The following topics describe the operations that can be performed with Groups:

- Creating a Group
- Configuring a Groups
- Deleting a Group

Built-In Groups and Permissions

The table on this page 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 another 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	✔	see "Security Level"				
Configure Time Synchronization Settings	✔	✔				
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	✔	✔				
Configure Server Settings						
Rename Server	✔	✔				
Auto-detect built-in and USB camera	✔	✔				

	Configure Failover (all settings)	✔	✔				
	Detach Server (from Site)	✔					
	Delete Server (Resource Panel, not online Servers)	✔					
	Reset to Defaults	✔					
	Restart Server	✔	✔				
	Add, Edit, Delete Storage Management	✔	✔				
	Manage Analytic DB Storage	✔	✔				
	Reindex (Archive + Backup)	✔	✔				
	Configure Backup Settings	✔	✔				
	Pin Certificate (in case of certificate error)	✔					
Cameras and Devices							
	View Live all Camera and Devices	✔	✔	✔	✔	✔	
	View Live all Web Pages and Integrations	✔	✔	✔	✔	✔	
	View Live all Server Health Monitors	✔	✔	✔	✔	✔	✔
	Play Audio	✔	✔	✔	✔	✔	
	View Archive	✔	✔	✔	✔		
	Manage Bookmarks	✔	✔	✔			
	User Input (PTZ, 2-Way Audio, Soft Triggers, I/O Buttons)	✔	✔	✔			
	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	✔	✔	✔	✔		
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	✔	✔				

NOTE: Many of the features and functions described in this manual are only available to Users with the appropriate Permissions.

Create a Custom Group

Site Administrators and Power Users can use the Desktop Client to create, manage, and delete Custom Groups.

How to create a Custom Group in the Desktop Client

1. Open **Main Menu > User Management.**
2. Select the *Groups* tab within the *Site Administration* dialog.
3. Click the **Add Group** button to open the *New Group* dialog.
4. Enter the name of the new *Group*.
5. Enter an optional description of the *Group.*
6. Use the Permission Group menu to select if the new group will be a member of any Built-In Groups or Custom Groups.
7. Click **Add Group** to create the group. Authentication may be required.

See "Configuring Groups" for information on granting Resources to Groups and managing Group Membership.

Configuring Groups

Groups are a powerful and efficient method to manage User Permissions. Changes made to the Group are applied to all Group members. Groups inherit permissions when they are a member of another Group, which in turn could be a member of another Group, further inheriting permissions.

- Administrators and Power Users can create, configure, or delete Custom Groups.
- Power Users can only edit Custom Groups that do not contain other Power Users or Administrators.
- Built-In Groups only allow members to be added or removed.
- Groups can only be created, configured, and deleted using the Desktop Client.
- Changes to LDAP Groups are stored in Nx Witness and not pushed to the LDAP Server.

- LDAP Group descriptions and Resource Permissions are configurable.
- Non-LDAP Users and Groups cannot be members of an LDAP Group.
- Deleting LDAP Groups within Nx Witness is not permanent, a deleted LDAP Group will be re-imported during the next LDAP sync unless the link to the LDAP server is removed.
- LDAP Group Name and Membership changes must be made on the LDAP Server.
- An LDAP Group and non-LDAP Group users can be members of the same Site Group.

- The Web Admin and Cloud Portal will display which Groups a User is a member of.
- The Web Admin and Cloud Portal will not display all members of a Group or Group Permissions.
- Changes can be saved on each tab, or on any tab after all changes are completed

To configure Groups:

1. Open the Group Management dialog by selecting Main Menu > User Management dialog and switching to the Groups tab.

- Optionally refine the list of groups by using the search box, filters, and column sorting options.

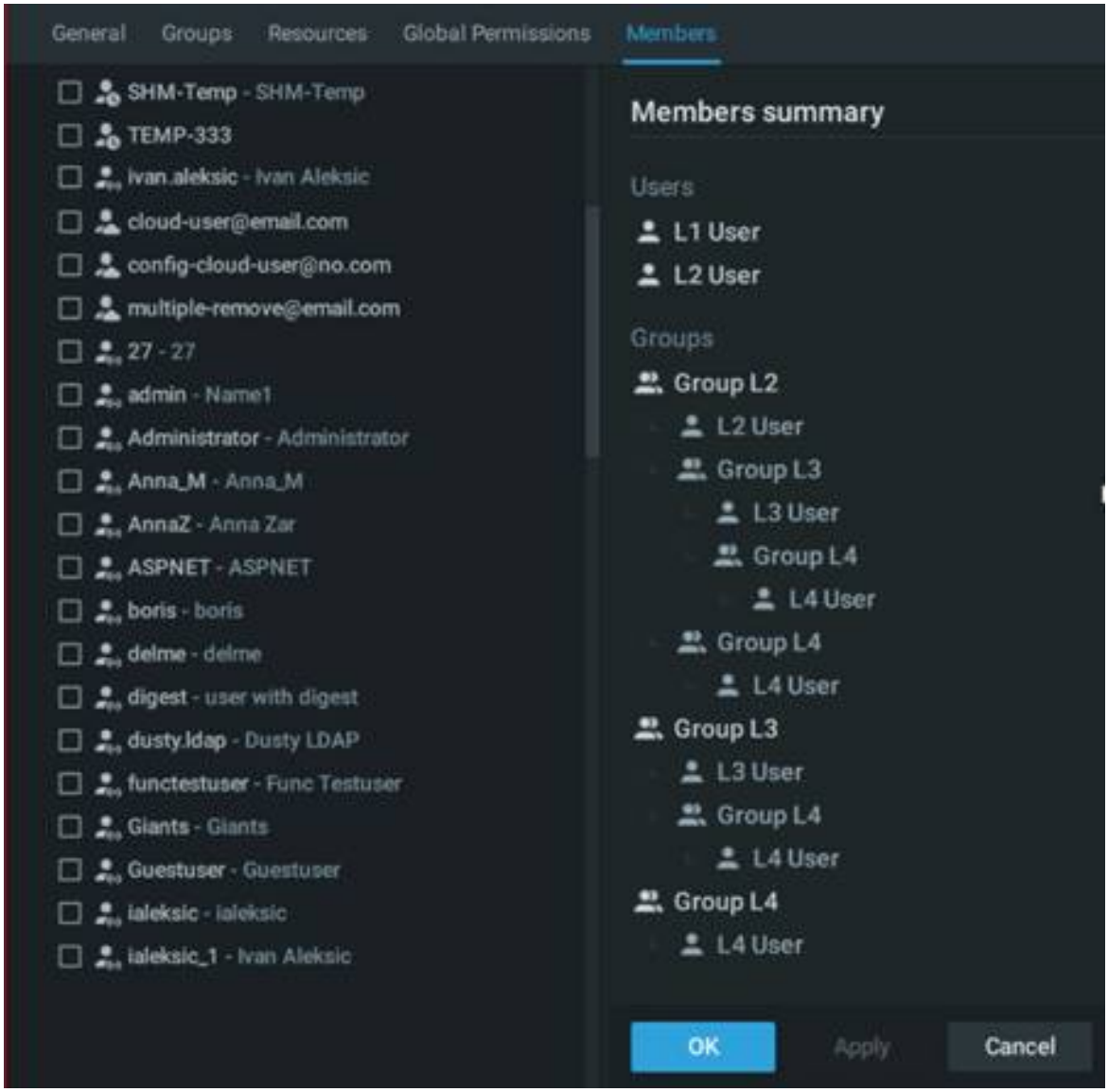
2. Click on a Group to open the configuration dialog.
3. Use the tabs within the Group configuration dialog to make permitted changes.
   - The *General* tab configures:
     - The name of any Custom Group.
     - The description of any LDAP or Custom Group.
     - All Permissions Groups where Permissions are inherited from.
   - The *Groups* tab provides:
     - A view and search function for all Groups this Group can be a member of.
     - A selection checkbox next each available Group which toggles Group membership.
     - Real-Time display of all Groups the current Group is member of.
     - A read-only view of LDAP Groups the current LDAP Group is a member of.
   - The *Resources* tab provides:
     - A grid-view of Permission types and available Site Resources.
     - Visual display indicating if Permissions is granted, inherited, or not authorized.
     - A preview of cascading Permissions that will be included with specific selections.
     - Hover-text that details where permissions are directly inherited from.

     See "Permissions Management" for details.
   - The *Global Permissions* tab defines:
     - If Group members are permitted to View the Event Log.
     - If Group members are permitted to generate non-camera events.
   - The *Members* tab provides:

- A detailed view of all Group members, including Users from nested Groups.
- Selectable checkboxes to add or remove members from the Group.

Groups Memberships Inheritance Example

In the following example:



- *L1 User* and *L2 User* are directly assigned to **Group L1**.
- *L3 User* is a member of **Group L1** via membership in **Group L2** and **Group L3**.
- *L4 User* is a member of **Group L1** via membership in **Group L3** *and* **Group L4**; both being members of *Group L2*.
- **Group L1** will have the same User Members if **Groups L3** and **Group L4** are removed as member of **Group L1** since *L3 User* and L4 *User* are nested in Group *L2.*

NOTE: Be careful with nested Groups as inheritance may grant unintended permissions to a group or user.

Deleting a Group

Built-In Groups and Permissions cannot be deleted. Custom groups can be deleted by Administrators and Power Users using the Desktop Client.

Deleting a group will not delete User accounts that are members of the Group, members of the deleted Group may see a change in the Resources that are available to them if those same Resources are not provided from another Group membership or granted to the User directly.

To delete a Group

1. Open the *Group Management* dialog by selecting **Main Menu > User Management** dialog and switching to the **Groups** tab.
   - Optionally refine the list of users by using the search box, filters, and column sorting options.
1. Select the checkbox next to each Group to be deleted.
2. Click on the **Delete** button to remove the group(s) from the Site.
3. Confirm or authenticate if prompted.

NOTE: A confirmation message will not be displayed if the *Do Not Show Again* option has been selected. **Open Menu Menu > Local Settings > Advanced** and click the **Reset All Warnings** button to again show all confirmation prompts.

Permissions Management

Permissions can be configured for Groups (Custom and LDAP), Channel Partners users, and for individual users (local, cloud, organization, and LDAP).

To configure Permission for a Group

1. Open the *Group Management* dialog by selecting **Main Menu > User Management** dialog and switching to the **Groups** tab.
   - Optionally refine the list of groups by using the search box, filters, and column sorting options.
2. Click on a Group to open the configuration dialog.
3. Choose the *Resources* tab to manage **Resource Permissions** or the *Global Permissions* tab to manage **Global Permissions**.

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 select a single checkbox and Click **Edit** to open *User Properties*.
3. Choose the *Resources* tab to manage **Resource Permissions** or the *Global Permissions* tab to manage **Global Permissions**.

Global Permissions

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.

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

- Devices – Cameras, I/O modules, etc.
- Web Pages and Integrations.
- Server Health Monitors.
- Layouts – may include all of the above Resources. Granting permission for a Layout grants access to all Resources placed on the Layout.
- Video Walls – configure Video Walls based on available Resource Permissions.

The following rules are applied when managing Resource Permissions:

- Clicking on the heading row of any Resource (devices, layouts,web pages, etc.) will toggle all the resources in the Permission column.
- Permissions can only be granted, inherited, or not granted, there is no mechanism to block access to a specific Resource.
- Users and Groups inherit the Permissions from every Group they are a member of.

Resource Control Icons – provide permissions to selected resources:

- **View Live** – Permission to access a live view only.
- **Play Audio** – Permission to Play Audio received from a device. Applies to both live and archived streams.
- **View Archive** – Permission to access the archive.
- **Export Archive** – Permission to export archives.
- **View Bookmarks** – Permission to browse Bookmark.
- **Manage Bookmarks** – Permission to View, Create, Edit, or Delete Bookmark.
- **User Input** – Permission to control PTZ, use Soft Triggers, and 2-way audio.
- **Edit Settings** – Permission to change the available device options.

NOTE: Selecting a permission will automatically select any other permissions it requires in the permission table.

Permission Status Icons:

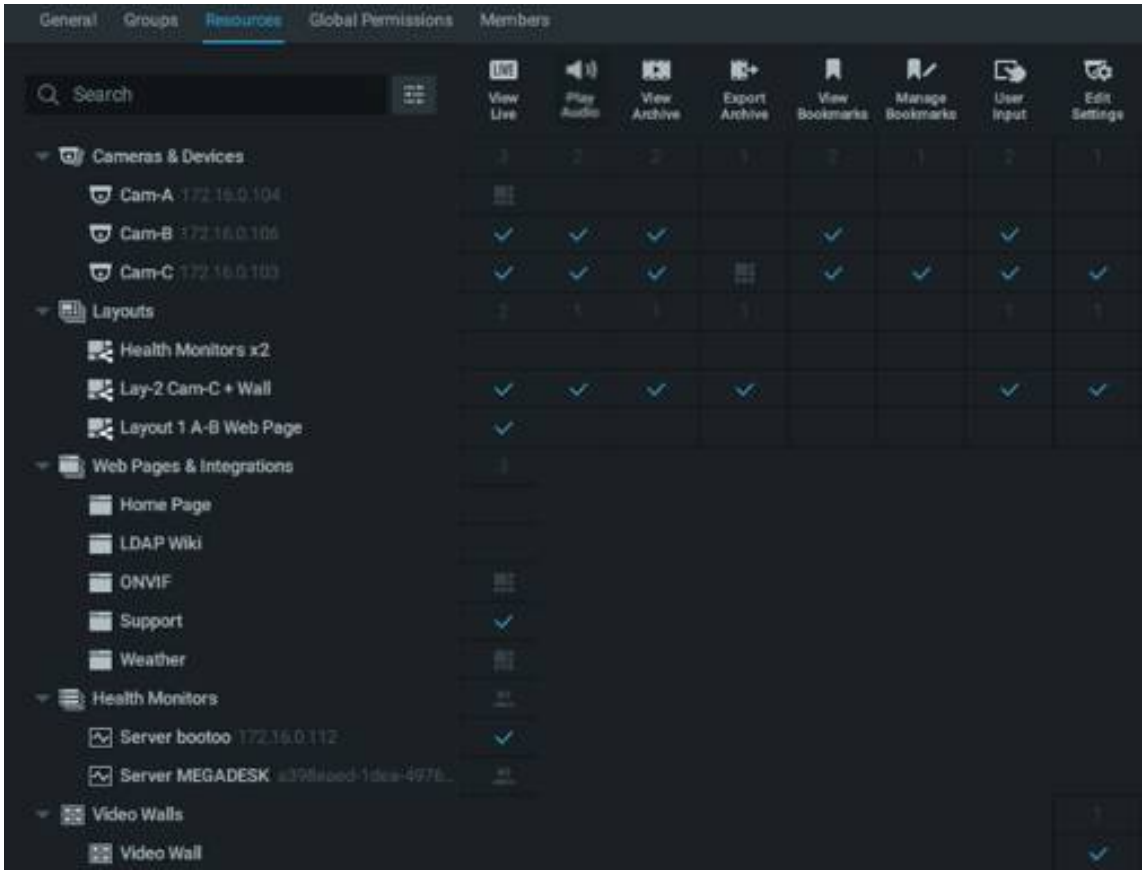
- Empty Space – No Permission granted to this Site Resource.
- Checkmark – An explicitly granted (not inherited) Permission to a Resource.
- A Number – The sum of Resources granted per Permission type displayed in row heading.
- Layout – Permission to the Resource is inherited through a Layout granting Permissions.
- Multiple Users – Permissions are inherited from membership in one or more Groups.

NOTES:

- Mouse-hover Permission Status Icon in the panel to view inheritance details.
- Mouse-hover over the Permission grid to see inheritance rules.

Permissions Panel Configuration Example:

The example below illustrates various combinations of Resource Permissions assigned to Users and Groups:



- **Cameras & Devices**
  - Cam-A – Live View is inherited from **Layout 1 A-B Web Page**.
  - Cam-B – Live View, Play Audio, View Archive, View Bookmarks, and User Input to Cam-B are explicitly granted.

  - Cam-C – Same as Cam B; Export Archive permission is inherited from **Layout Lay-2 Cam-C + Wall** with Manage Bookmarks and Edit Settings permission being explicitly granted.
- **Layouts**
  - No access to **Health Monitor x2 Layout**.
  - **Lay-2 Cam-C + Wall layout** includes all permissions except for View and Manage Bookmarks.
  - **Layout 1 A-B Web Page** is limited to Live View.
- **Web Pages & Integrations**
  - Inherited permission to view **ONVIF Web Page** from **Lay-2 Cam-C + Wall**.
  - Explicit permission to view **Support Web Page**.
  - Inherited permission to view **Weather Web Page** from **Layout 1 A-B Web Page**.
- **Site Health Monitors**
  - Explicit permission to view for **Server bootoo**.
  - Inherited permission to view for **Server MEGADESK** inherited from **SHM Group**.
- **Video Walls**
  - Explicit permission to edit **Video Wall**.

LDAP Users and Groups

LDAP integration allows a Site to import *Users* and *User Groups* from an LDAP Server.

- Users must exist in the LDAP database object tree, match the base selection, and not be disabled in the LDAP Server to be imported.
- LDAP Groups and Users can be assigned Permissions and placed in any existing Site Groups, except the Built-In Administrator Group (see "Configuring Users" and "Configuring Groups").
- LDAP Groups have certain specifics in terms of configuration (see "Configuring Groups").
- LDAP Users can access the Site using their LDAP username and password.
- LDAP users will not be able to log in while the LDAP Server is not available (see "LDAP Sync Failure").
- The following LDAP Servers types are supported:
  - Microsoft Active Directory,
  - Open LDAP Server,
  - JumpCloud.

NOTE: LDAP Users must have Resource Permissions granted (see "Permissions Management") or to be added to a Built-In Group to do anything more than connect to a Site.

Setting Up LDAP Integration

To import LDAP users and allow them to connect to the Site, it is necessary to establish a connection between Nx Witness and the LDAP Server. The LDAP server does not have to be a part of the same LAN the Media Server is on, but it must be available for the Media Server either by LAN or WAN.

- LDAP integration should be performed by, or in cooperation with, the Network (Domain) Administrator.
- LDAP over SSL may require certificates on both the LDAP and Nx Witness Servers.

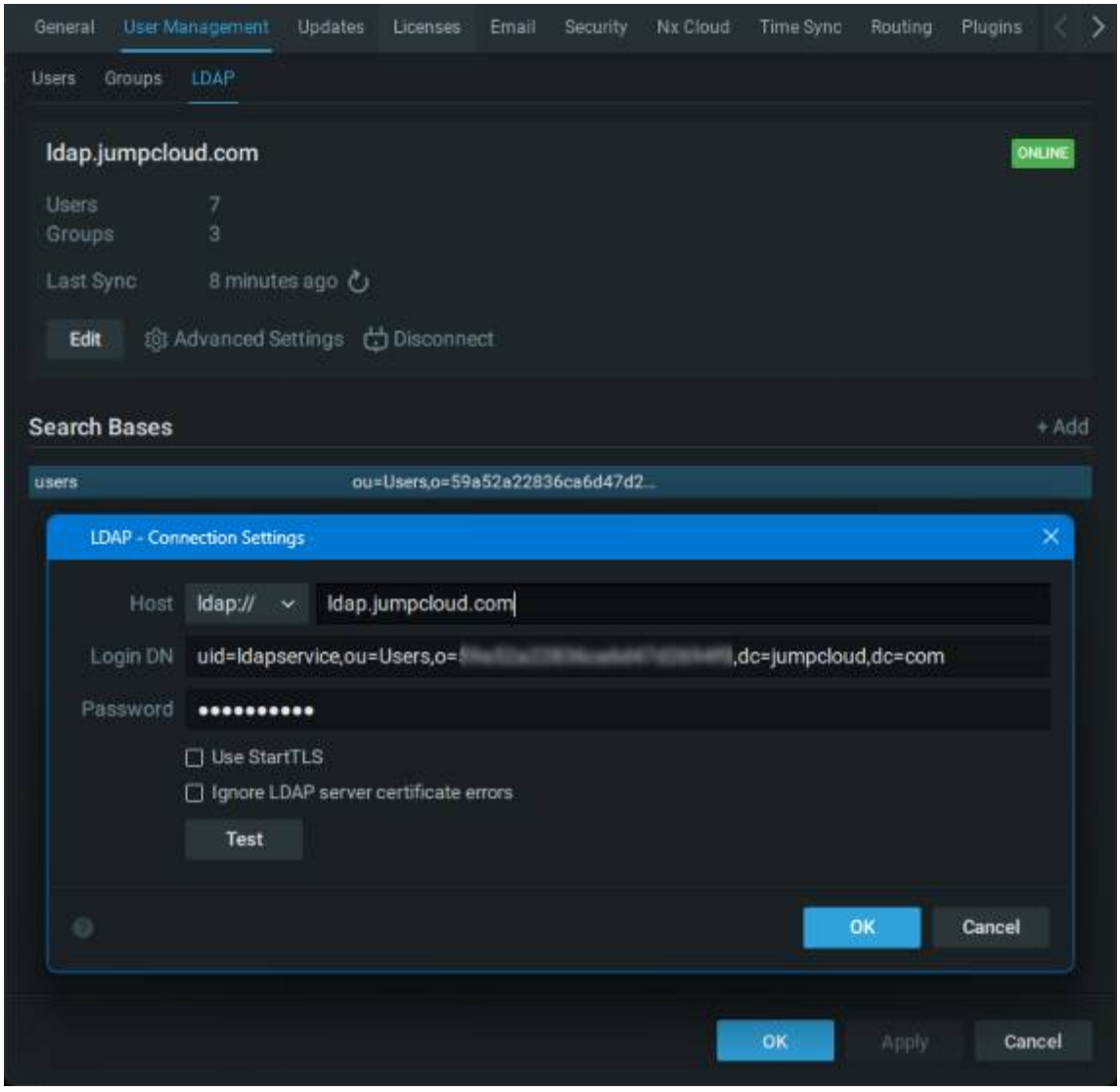
NOTE: When configuring LDAP integration, do not specify the domain's base distinguished name (DN) as a search base, instead specify the organizational units (OU's) underneath the base DN because it is not possible to filter on OU membership, but you can filter on group membership.

To retrieve all users that are members of a specified group, filter on the **`memberOf`** attribute. For example: memberOf=CN=Security Users,CN=Users,DC=DOMAIN,DC=LOCAL.

1. Select **Main Menu > User Management** and go to the *LDAP* tab.
   A **Configure** button is displayed when no LDAP information exists in the Site, otherwise the LDAP dialog displays the following summary information:
   - Server,
   - Server status,
   - the last synchronization timestamp,
   - the numbers of users and groups retrieved.
2. Click the **Edit** button below the summary information to open the *LDAP Connection Settings* dialog.
3. Enter the following information (consult with your Network or Domain Administrator as needed):
   - **Host:** (ldap:// or ldaps://)

     NOTE: If using a Server URL, it should be a fully qualified domain name (FQDN), sometimes also referred to as an absolute domain name. See https://en.wikipedia.org/wiki/Fully_qualified_domain_name for details.
   - **Login DN**
   - **Password**
   - **Options:**
     - Use StarTLS
     - Ignore LDAP Server certificate errors
4. Click the **Test** button to validate the server connection and credentials. One of the following message will be displayed:
   - Connection OK
   - Cannot connect to LDAP Server

5. Upon successful test results click the **Apply** button to save the connection setting and return to the LDAP summary. Clicking **Cancel** will discard all settings entered and exit the *LDAP Connection Settings* dialog.
6. Click the **+Add** button along the Search Bases heading to open the *Add Search Base* dialog; enter the following information:
   - *Name* – often "Users"
   - *Base DN* – the starting point for LDAP searches and synchronization.
   - *Filter* – specific which Users and Groups from the Base DN to are allowed (optional).
7. Click **OK** to close the dialog and return to the *LDAP* tab of the User Management dialog.
8. Click **Apply** to save the Search Base parameters and retrieve User and Group information from the LDAP server. The Users and Groups count will update upon a successful retrieval.



9. Optional – Click on Advanced Settings to review and change defaults for:

- *Synchronize Users* – Always or only at Login.
- *Sync Interval* – a value from 1 to 9999999 in seconds, minutes, or days.
- *Proxy Server* – select a specific Server to connect to the LDAP server, or Select *Auto.*
  - In Auto mode, each server tries to connect to LDAP directly. If the connection fails, then every Server in the Site will try to connect. If a specific Server is selected, but it is unavailable, the Site defaults to Auto mode.
- Users – Deselect *Auto* to provide a specific value; use the checkbox to toggle the *allowing insecure (digest) authentication for imported Users*.
- Groups – Deselect *Auto* to provide a specific *objectClass* value.
- Membership – Deselect *Auto* to provide a specific *Group Members Attribute*.

Importing Users from LDAP Server

LDAP Users and Groups are imported immediately after the LDAP integration is completed and validated. Follow these steps to force an LDAP synchronization:

1. Open **Main Menu** > **User Management > LDAP** tab.
2. Below the User and Group count is the *Last Sync* timestamp and a refresh icon.
3. Click the refresh icon to force LDAP synchronization. The refresh icon is not displayed when the sync interval in Advanced Settings is set to 1 minute or less.
4. Once imported, LDAP users can be enabled or disabled (see "Enabling and Disabling Users"), and assigned User Permissions or placed in Permission Groups (see "Configuring Users").

NOTE: LDAP users must successfully log into the Desktop Client one time before they can use the Web Admin.

Changing or reconfiguring LDAP Servers

Changing or reconfiguring the LDAP Server integration can result in existing LDAP Users becoming invalid and thus disabled in the Site. A warning banner and confirmation dialog is presented when LDAP integration changes may disrupt the validity of existing LDAP Users and Group.

Removing or Deleting an LDAP Server from the Site

- Removing or deleting an LDAP Server connection that has been synchronized at least once will remove all LDAP User and Groups from the Site and clear all data for LDAP User permissions and group memberships.
- The Audit Trail of User Actions retains all history for deleted users.
- Removing or Deleting the LDAP connection cannot be undone.
  1. Open **Site Administration** > **User Management >** *LDAP* tab.
  2. Click on the **Disconnect** button near the **Edit** and **Advanced Settings** buttons.
  3. Confirm to *Disconnect LDAP server and remove all LDAP Users and Groups*.

LDAP Warnings

The following warning may be displayed during LDAP configuration, testing, and update Synchronization

- **Remove existing LDAP Users and Groups**:
  - This warning is displayed for any action that will force the removal of all existing LDAP Users from the Site.
- **Disconnect LDAP Server** confirmation:
  - This dialog is displayed before disconnecting and LDAP Server and removing all LDAP Users from the Site.
- **LDAP Server is offline:**
  - This banner is displayed in the User Management dialog for LDAP and includes a count of how many Users are currently unable to connect to the Site.
- **LDAP User Duplication:**
  - This banner is displayed in the User Management dialog when imported LDAP usernames conflict with existing usernames in the Site. Site accounts have priority and the duplicated LDAP usernames will are disabled.
- **LDAP Digest Authentication:**
  - An informational dialog is presented when changing the LDAP Digest Authentication settings if some Users will also need their User Configuration Settings changed.

Partner Access to Sites

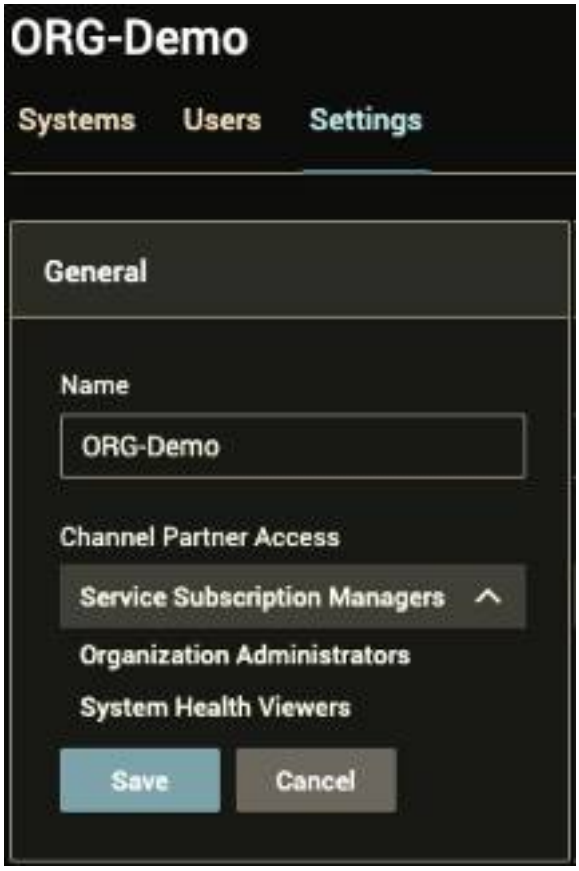
The information in this topic is only applicable to the Enterprise Edition of Nx Witness.

Key Concepts:

- Channel Partners define the type and quantity of Services that are available to their Organizations using a dedicated application.
- An Organization Administrator must grant their Channel Partner one of three access levels:
  - *Organization Administrator* access will grant the Channel Partner complete authority over Sites, encompassing all the permissions held by a Site Administrator.
  - *System Health Viewers* have limited access, enabling them to monitor system health and manage service subscriptions. However, they are restricted from accessing Site resources, devices, archives, bookmarks, user data, logs, notifications, and Site settings.
  - *Service Subscription Managers* can only manage the Service Subscriptions available to Sites. They do not have access to System Health information or any Site resources.
- Channel Partner users with access to a Site are not visible in the Site user management dialogs, unless they have Site-level permission set.
- The Audit Trail of User Actions will capture the actions taken by a Channel Partners.

Setting Channel Partner access to an Organization:

1. Sign into the Cloud Portal as an Organization Administrator.
2. Depending on your Cloud access rights, it may be necessary to activate the Organizations tab to display the available Organizations.
3. Choose the Organization where Channel Partner access will be set by clicking on the Organization tile.
4. Select the *Settings* tab within the banner menu under Organization name.
5. Use the *Channel Partner Access* pull-down menu to select the access Channel Partners will have to the Organization.
6. Confirm the Channel Partner Access change by clicking on the **Save** button.



NOTE: A warning message will appear when a pending Channel Partner Access change will reduce your access. Once your access is lowered, only an Organization Administrator will be able to elevate it again.

Audit Trail of User Actions

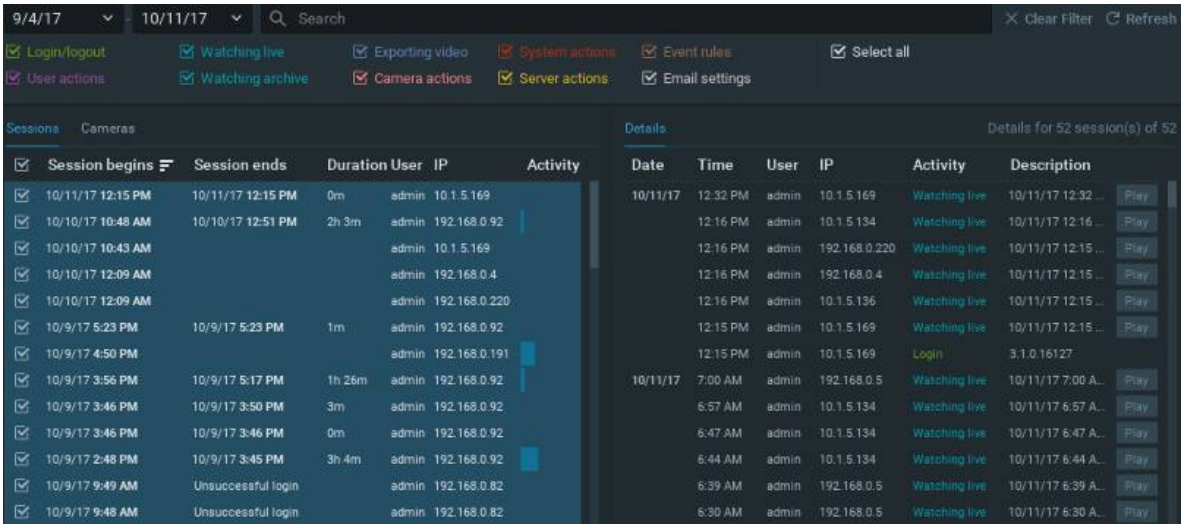
Key Concepts

- Nx Witness tracks all user actions and records them to a log called the Audit Trail.

- To view the Audit Trail log, open **Site Administration** in the main menu, then select the *General* tab and click on the **Audit Trail** button.
- The top panel provides filters and a search tool.
- The initial display is includes all sessions and all cameras selected.
- Selected entries can be copied to the clipboard or exported using the right-click context menu.
- Channel Partner users without site-level permissions will have their email hidden as a string of asterisks (***).
- Audit trail entries for deleted users are retained.

Audit Trail Filtering and Searching

- *Sort* – Data can be sorted in ascending or descending order by clicking on any column header.
- *Filter* – Type a filter criteria in the *Search* field on the top. Select a desired time period using the From and To calendar fields.
- *Show/Hide actions by type* – Use the checkboxes at the top to toggle display of specific action types.
- *Update data* – Data may have changed since the log was opened. Use the **Refresh** to update the display.
- *Export* – To export the log file, select the desired records and open the context menu to choose one of the following:
  - *Copy Selection to Clipboard* – So data can be pasted to another program (ex. Microsoft Excel or Google Docs).
  - *Export Selection to File* – Exports data as an *html* or *csv* file. Click on one or more individual checkboxes to filter the display.



There are two summary panels, **Sessions** and **Cameras**, with a related **Details** panel to the right. Columns in these tabs can be sorted in ascending or descending order. Use the checkboxes to select certain sessions or cameras, or check the box in the header to select all logged activities.

Sessions Tab

Provides a summary of activities during a User session, where a session is defined as the period between a user's log in and log out:

- Session begins and Session ends date and time
- Duration of session
- User ID
- IP address of Client the User logged in from
- Activity bar graph depicting the number of actions performed during a session. Hover the cursor over this graph to see the precise count of actions.

Cameras Tab

Provides a summary of devices used:

- Camera name
- IP address of the camera
- Activity bar graph depicting the number of actions performed with the camera(s) during the selected time period.

Details Tab

For both sessions and cameras, shows:

- *Date and Time* – When each action occurred.
- *User* – The one who performed the operation.
- *IP* – IP address of Client the User logged in from.
- *Activity* – The action performed. For example, watching archive, watching live, Server updated, camera updated, exporting video, etc.
- *Description* – Details of the action performed (start/end times, number of cameras affected, Site version updates, etc.). There may also be a button for direct access to the activity performed. For example, watching activities can be expanded to show the camera(s) that were viewed and a *Play* button that launches the related archive. Similarly, for the "Camera updated" activity, the *Camera settings* button opens the settings dialog of the device modified by the user.

Disabling Audit Trail recording

The Audit Trail is enabled by default.

Desktop Client

1. Open **Main Menu** > **Site Administration** > **Security** tab.
2. Uncheck the **Enable audit trail** checkbox.
3. Apply changes.

Web Admin / *Cloud Portal*

1. Open **Settings** > **Site Administration** > **General**.
2. Uncheck the **Enable audit trail** checkbox.
3. Apply changes.

Disconnect Cloud Account

Key Concepts

- Cloud accounts can be standalone; or connected to a Site, an Organization, or a Channel Partner.
- Disconnecting a Site from a Cloud Account will convert the Site to a local Site.
- A cloud-connected Site can be directly transferred to another cloud account.
- Cloud users can choose to disconnect their account from an Organization or Channel Partner to revoke their own access and disassociate their account from entities they no longer manager or wish to participate in.

Transferring a Cloud Connected Site

See Changing Cloud Owner for further instructions.

Disconnect Cloud Account from a Site

Using the Desktop Client:

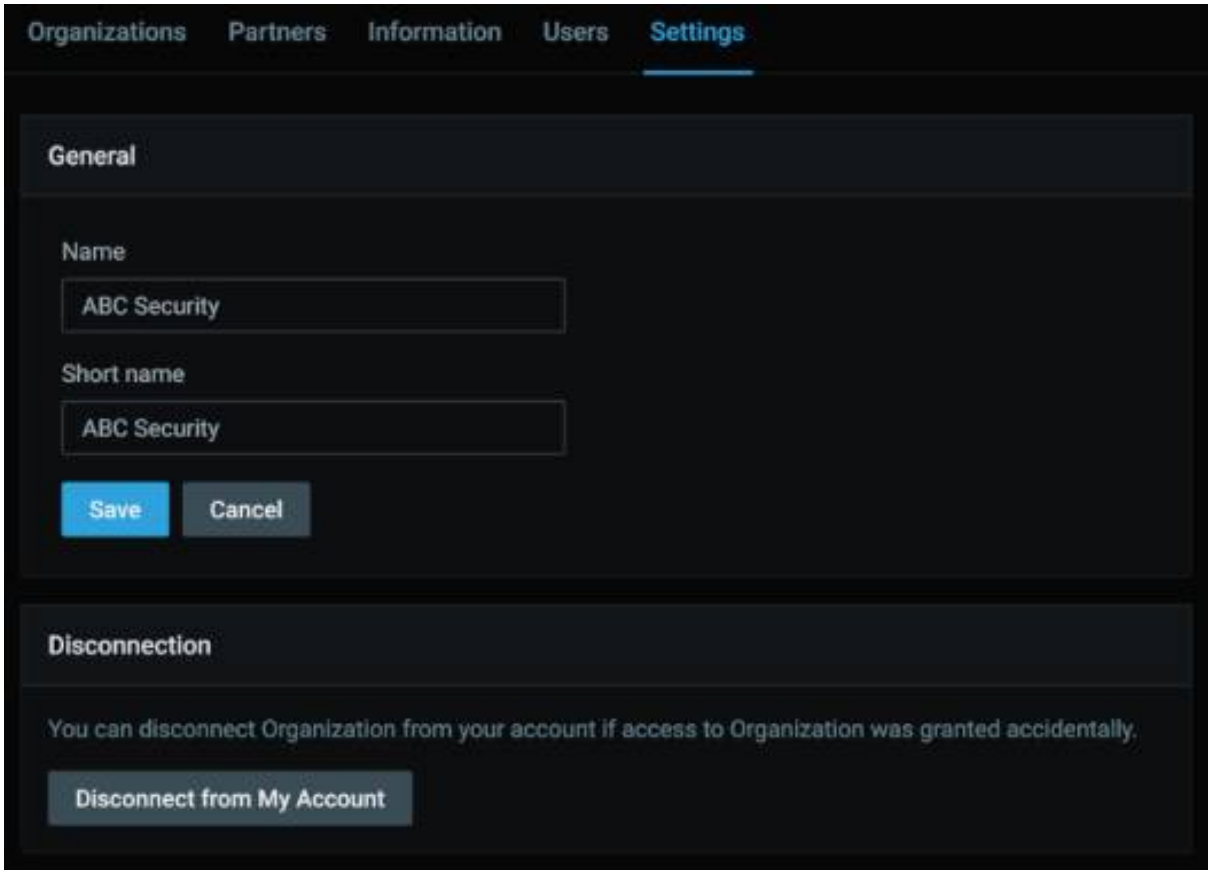
1. Open the **Main Menu > Site Administration** dialog.
2. Select the ***Nx Cloud*** settings tab.
3. Click the **Disconnect Site from Cloud** button.
4. Confirm and complete the action.

Using the *Web Admin* / *Cloud Portal*

1. Open the Site in the Cloud Portal.
2. Select **Settings** in the header menu.
3. Select **General** in the left menu.
4. Click the **Disconnect Site from Cloud** button.
5. Confirm and complete the action.

Disconnect Account from an Organization or Channel Partner

1. Using the *Web Admin* / *Cloud Portal* to open the Site
2. Select set **Settings** tab in the heading menu.
3. Click on the **Disconnect from my Account** button.
4. Review summary of access changes.
5. Click on the **Disconnect** button to complete the action.



Layout Management

Layouts are an integral part of the Nx Witness experience that provides a way to organize Cameras, Devices, and Web Pages for efficient access and viewing. Users can quickly switch between Layouts to follow items of interest or to view an area from another perspective.

- The following types of Layouts are available:
  - Shared Layouts – can be shared with other Site users.
  - Intercom Layouts – are created to support intercom events (see Working With Intercoms).
  - Cloud Layouts – may contain devices from multiple Cloud-Connected Sites.
  - Local Layouts – can only be accessed by the user who created the Layout.
  - Alarm Layouts are configured to open as a responsive action to a specific Event (see " Show on Alarm Layout").
- Layouts are only accessible in the Desktop Client and cannot be viewed in the Web Admin or Cloud Portal.
- A Layout is an arrangement of up to 64 Cameras, Devices, Web Pages, and other elements placed on the Viewing Grid.
- Each Layout is displayed within a separate tab of Desktop Client and Multiple Layouts can be open simultaneously.

- A Layout must be saved after it is created, otherwise it will be lost if the tab is closed or the session has ended.
- Layouts of different types can be grouped together within the Resource Panel.
- *Administrators* and *Power Users* can create and share Layouts with other Users (see "Creating and Sharing Layouts" and "Permissions Management").
- All users with access to the layouts can see the groups containing these layouts. However, if an administrator creates groups of local layouts, they will not be visible to users until at least one layout inside the is converted into a shared layout.
- If not all layouts within a group are shared, uses will only see the layouts they can access within a layout group.
- Changes to Shared Layouts and Cloud Layouts are propagated to all Desktop Client instances and Users who have permissions to the Layout.

Additional Layout Topics

Viewing Grid

The *Viewing Grid* is the empty background of cells into which items are placed to create a layout. Each layout is displayed in a separate tab of the Viewing Grid. Tabs allow you to have multiple layouts open at once.

The cells of the Viewing Grid are only visible when you move or re-size an object in layout. When an item is being moved, a green cell indicates where it can be placed, red cells indicate where it cannot be placed.

The Viewing Grid has a default cell aspect ratio of 16:9, currently the most common aspect ratio of cameras on the market, but will shift to the aspect ratio of the first item placed in a new layout. This is important to consider when designing your layout. Subsequent items added to layout retain their native aspect ratio regardless of the aspect ratio of the Viewing Grid. However, the default aspect ratio for a layout can be changed using **Cell Aspect Ratio** from the Viewing Grid context menu.

It is also possible to control the size of the Viewing Grid cells for specific layouts; see "Configuring Layouts".

The Viewing Grid has a setting for the space between cells (*None*, *Small*, *Medium*, or *Large*) which is useful when you need to make a layout more compact. Access this control from the Viewing Grid context menu by choosing **Change Cell Spacing**.

There is also a setting for the display resolution of the items that are currently displayed (*Auto*, *Low*, *High*), which is controlled from the **Resolution** option in the Viewing Grid context menu (right-click on the camera tile).

Cell Spacing

This feature is used to change the spacing between items in a layout so they can be closer together or further apart.

For example, four individual single-sensor cameras that together form a 180 degree panoramic view would best be displayed without any space between cells.

To adjust the distance between items, open the Viewing Grid context menu and select **Cell Spacing**, or use **Ctrl**+**Mouse Wheel** over the Viewing Grid. Options are *None*, *Small*, *Medium*, or *Large.*

Cell Aspect Ratio

Cameras provide video in a variety of aspect ratio formats. To populate layouts efficiently, Nx Witness attempts to match the default aspect ratio of an Item window to the aspect ratio of its contents.

The Viewing Grid adjusts to the aspect ratio of the first item added. To change the aspect ratio of an entire layout, right-click anywhere on the Viewing Grid, and use **Cell Aspect Ratio** from the context menu to select from the available options (*4:3*, *16:9*, *1:1*, *3:4*, or *9:16*).

Layout Resolution

You can set the resolution for all items in a layout by right-clicking anywhere on the Viewing Grid, and using **Resolution** from the context menu to select from the available options (*Auto*, *High*, or *Low*). Auto allows each device to display at it's own default setting. Once the resolution for an entire layout is set, you can still set the resolution of an individual item as desired, in which case the layout resolution will display *Custom* to indicate that not all items are using the same resolution setting.

Layout Tabs and Groups

Key Concepts:

- The display on initial Site launch is an empty Viewing Grid with tab name “New Layout*”.
- An asterisk at the end of the layout name indicates that the layout has unsaved changes.
- The name if each new layout defaults to *New Layout #* using the next logical, numerical increment.
- One layout tab must always be open, this can be an empty New Layout #* tab.

- If more tabs are open than can fit in the display, "**<**" and "**>**" arrows will be provided to scroll through any tabs that are not visible.

To Open a New Layout Tab

1. **Right-click** on any tab in the Navigation Panel and select **New Layout** (**Ctrl**+**T**) from the context menu.
2. Go to **Main Menu** > **New** > **Layout**.
3. Click on the **+** icon to the right of the last tab in the Navigation Panel.

To Close a Tab

1. Click on the **X** icon next to the tab name.
2. **Right-click** on a tab to open the context menu and select **Close** (**Ctrl**+**W**).

To Close All but the Active Tab

- To close all tabs but the active one, open the tab's context menu and select **Close All But This.**

To Reposition a Tab

- Click-and-drag a tab name in the Navigation Panel to change its position.

To Open an Existing Layout

1. Drag-and-drop the layout from *Layouts* in the Resource Panel onto the Viewing Grid.
2. **Right-click** on the layout in the Resource Panel and choose **Open Layout** (or press **Enter**) from the context menu.
3. **Right-click** on an existing layout in the Navigation Panel and select **Open Layout** from the context menu to open a list of all layouts available to the current session.
4. Click on the **?** icon to the right of the last tab in the Navigation Panel to open a list of all layouts available to the current session.

If you select a layout that is currently open, focus will shift to that tab. If you select a layout that is not currently open, it will open in a new tab. You can use the first two steps to select and open multiple layouts. Each layout will open in a separate tab. (If a layout is already open it will not be reopened in a second tab.)

NOTE: After Nx Witness is closed, all saved layouts that are open will be restored when the User logs back in.

Layout Groups in the Resource Panel:

- All layout groups are expanded by default .
- Each layout can only exist in one layout group at a time.
- All layouts inside a group (folder) are sorted lexicographically.
- Layout groups can be nested 8-levels deep with the same Group name used at each level.

- The collapsed and expanded settings for layout group is saved and restored when user returns to the Site.
- Layout groups cannot have a blank name; the Group name must be at least one character and leading spaces will be removed.
- Only Site Administrators and Power Users can create and modify layout groups.

To Create a Layout Group:

1. Select one or more layouts and then use the context menu (right-click) or the hot-key (CTRL+G/CMD+G) to create a New Group.
2. The created group is automatically named New Group with subsequent groups incrementally named New Group 1, New Group 2, ...
3. Newly created groups are added to the top of the list of all layouts and first displayed in an editable (rename) mode.

To Modify a Layout Group:

1. Drag and Drop Layouts in and out of the group to change the contents of the Layout group.
2. Removing a Layout group, or a nested Layout group, will return all the contained Layouts to the Resource Tree.
3. Use the context menu to rename or remove a Layout group from the Site.

Creating and Sharing Layouts

A new Site is installed without Layouts configured and will open to a blank Viewing Grid. A new Layout can be configured as a temporary one for the current session, saved to the current User for later recall, shared with others Users of the Site, or Saved As a Cloud Layout that can contain Devices from different Cloud Connected Sites.

To Create a New Layout

1. Click on the **+** icon in the Navigation Panel to the right of other open Layout or Site tabs.
2. Configure the Layout to meet the viewing needs.

To Save a Local Layout

1. Right-click on the Layout tab or the Layout name in the Resource Tree to open the Layout context menu.
   - Select **Save Layout** to save the Layout using the current type and name (New Layout # if not changed previously).
   - Select **Save Layout As** to save the Layout as the current type under a new name.

   NOTE: A Layout must be saved once before it can be shared locally or converted to a Shared Layout.

To Convert a Local Layout to a Shared Layout

1. Ensure the Layout is has been successfully saved once and is displayed in the Resource Tree.
2. Right-click on the Layout in the Resource Tree to open the Layout context menu.
3. Select *Convert to a Shared Layout* in the context menu. The Layout icon will update to reflect that it is a Shared Layout.
4. The Layout is now visible to Administrator and Power User who can share it with other Users (see "Permissions Management").

To Save a Layout as a Cloud Layout

1. Site must be connected to the Cloud.
2. Ensure the Layout is has been successfully saved once and is displayed in the Resource Tree.
3. Right-click on the Layout in the Resource Tree to open the Layout context menu.
4. Select *Save as a Cloud Layout* in the context menu. This will **Save a Copy** of the Layout as a *Cloud Layout* under the name provided.

Granting Permission to a Layout

1. Ensure the Layout is has been successfully saved once and is displayed in the Resource Tree.
2. Administrators and Power Users can grant other Users Permission to the Layout (see "Permissions Management").

Saving and Locking Layouts

A layout remains local and will only be available during the current session unless it is saved. Saving a layout saves the position and rotation of all items. Once a layout is saved, it is added to the Resource Panel under Layouts and also the names of the users who have access to it. Saved layouts that were open when a session closed will automatically reopen the next time a User logs in.

- Use *Save Current Layout* (Ctrl+S) to save the layout name with its current name (as shown in the tab header caption).
- Use *Save Current Layout As* (Ctrl+Alt+S) to enter a name of your choice.

To Save a Layout

- **Right-click** on the tab name in the Navigation Panel and select **Save Current Layout** or **Save Current Layout As** from the context menu.
- **Right-click** on the Viewing Grid of the layout and select **Save Current Layout** or **Save Current Layout As** from the context menu.
- Click on the desired layout in the *Resource Panel* and select **Save Current Layout As** to save it with a new name.

A layout can be locked so that no changes at all are permitted unless and until it is unlocked. This includes item rotation, cell spacing, aspect ratio or window zooming.

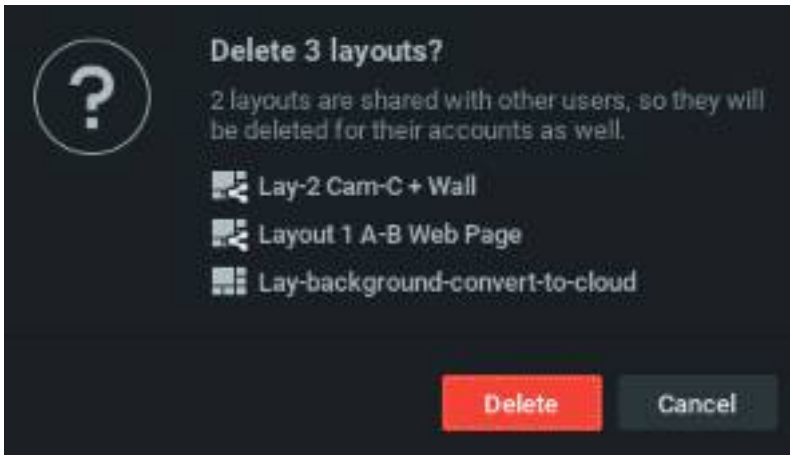
To Lock or Unlock a Layout

1. **Right-click** on the Viewing Grid of the layout you want to lock and select **Layout Settings** in the context menu.
2. In the *General* tab, click the **Locked** toggle.
3. Click *OK* to accept or *Cancel* to discard changes.

Deleting Layouts

To Delete a Layout from the Resource Panel

- Find and select the Layout to delete, or use shift+click to select multiple Layouts in the Resource Panel.
- Invoke the context menu and choose Delete (or use the Del button on a keyboard).
- If the layout is shared, click Delete again in the confirmation dialog.
- The layout will be deleted from all Clients and Users in the Site.
- Locked Layouts cannot be deleted.



Configuring Layouts

Items (Devices, Cameras, Integrations, Virtual Cameras, Web Pages, Local files, etc.) are placed on the Viewing Grid to create a **Layout**. A Layout may contain more than once instance of an Item, up to a total maximum of 64 items.

Permission to Shared Layout are covered in topics about Users and Groups and Permissions Management.

To set Aspect Ratio and Spacing

Right-click on the Viewing Grid of the Layout to open the Layout context menu and select one of the following Layout Configuration choices.

- Resolution expands to offer choices of Auto, High, and Low resolutions.

- Cell *Aspect Ratio* expands to offer quick selection of the most common Aspect Ratios.
  - Cell aspect ratio is adaptive-it depends on the aspect ratio of the first item opened in the Viewing Grid. The default aspect ratio of cell in the Viewing Grid is 16:9 can be changed to other presets.
- *Cell Spacing* expands to offer none, small, medium, and large spacing or padding between layout elements.

NOTE: Cell Spacing, Cell Aspect Ratio, and Layout Resolution can be set for universally for a Layout or use the Layout Settings dialog to adjust them manually.

To change additional Layout Settings

Do one of the following:

- Right-click on the Viewing Grid where there is item of the Layout and select *Layout Settings...*
- Right-click on a Layout in the Resource Panel and select *Layout Settings...*

Settings on the *General* tab:

- Locked slide toggle – See Locking Layouts.
- Minimum Grid Size – Enable this parameter to control item size and placement more precisely. When an item is added to layout, it is always scaled to fit into one cell of the Viewing Grid. As more items are added to layout, the cell size is adaptively reduced so that all items can fit in the display. Cell size gets smaller with each item added, so item size gets smaller. When Minimum Grid Size is enabled, you can set an absolute Viewing Grid cell size, where the greater the value in the Width and Height fields, the more cells there are in the grid. The larger the number of cells in the grid, the smaller each cell is, and therefore the more flexibility you have in positioning items.
- Logical *ID* – enter a custom ID number or use the up and down arrows to define the Layout ID for quick API and integration identification and access.
  - Generate – Will assign the next available, incremental ID number. 1 if no other Layouts are in the Site, or 11 if ten other Layouts exist in the Site.
  - Reset – Clears the Logical ID field.

Settings on the *Background* tab are described in Layout Backgrounds.

Adding Items to Layout

To add item(s) to the current layout, choose from one of the following:

- Double-click on the item in the Resource Panel
- Right-click in the Resource Panel to open the context menu and select **Open**
- Drag-and-drop a device, web page or local file from the Resource Panel into layout

NOTE: that you can Select and add multiple items from the Resource Panel using the **CTRL** or **Shift** keys.

- Open *Local file(s)* or *Folder* – will be added to the current layout.

New items will scale to occupy the available space in layout. Nx Witness adjusts the aspect ratio of Viewing Grid cells according to the aspect ratio of the items in layout to maximize use of display space. See "Cell Aspect Ratio".

NOTE: Viewer-level User and Groups with similar limitations on their authority can add items but not save (update) the shared layout, they can also make their own layout from available cameras.

To Open Items Directly into a New Tab

- Right-click on the desired item(s) in the Resource Panel and select **Open in New Tab** in the context menu.
- Drag-and-drop the selected item(s) from the Resource Panel and onto the Navigation Panel header.

NOTE: It may be difficult to locate and add each device manually. You can use the search pane to help locate items (see "Searching and Filtering in Nx Witness").

To Configure a Layout Using Search

1. Create a new layout (see "Creating and Sharing Layouts").
2. Enter keywords into the Search box. The search results will appear on the Resource Panel automatically.
3. By adding or deleting keywords from the search box, the items on the Resource Panel will vary.
4. Save the configured Layout.

Cross-Site Layouts

Additionally, it is possible to add devices from different Sites you have access to. Some limitations apply:

- The Devices must be connected to Sites that share a common Cloud Account or Organization.
- Users need permissions to view Cameras that are placed on the Layout.

To add a device from a different Site:

1. Find the desired Site in the Resource Panel.
2. Expand the desired Site, choose the device(s) you want to add and add them to the current layout as described above.

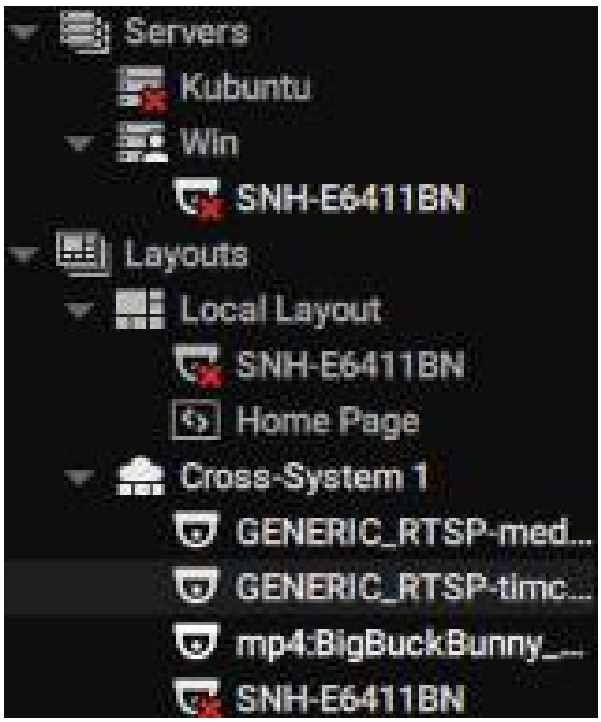
Also items from other Sites may already be in other Cross-Site Layouts in the Resource Panel. In this case, once add them to the current Layout, it will automatically turn into a Cross-Site one.

Once such layout is saved, a few restrictions will apply:

- It can only be displayed in the Desktop Client (not Mobile/Web Admins).
- Cloud Users can set up and save such layouts but cannot share them to other users.

Cross Site layouts cannot be used with VideoWall, Showreels or automated with Event Rules (the "Open Layout" action).

Cross-Site Layouts are displayed in the Resource Panel as follows:



Selecting Items in Layout

Click on an item to select it. The selected Item will expand in the layout. To bring it back to normal, click again. Once an item is selected you can use Shift+Arrow key to scroll selected through all items in a given layout. Items can also be selected from the Resource Panel.

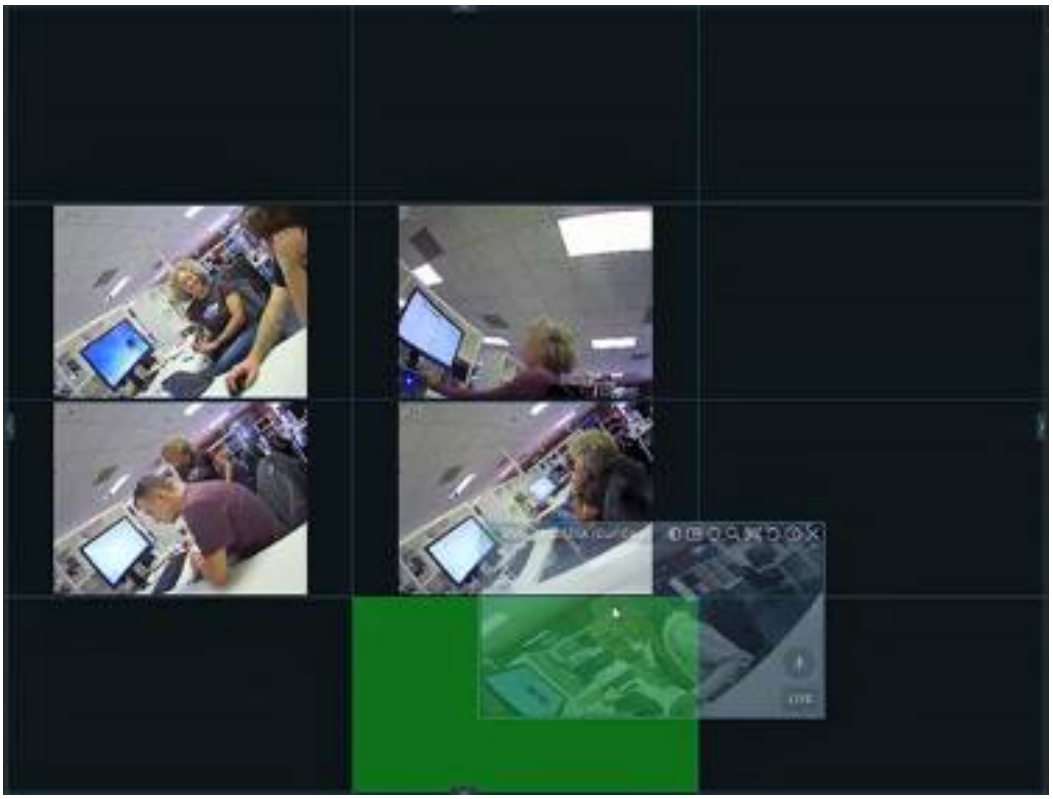
You can also select multiple items. Multiple selected items do not expand, instead they are outlined and given a colored overlay.

To Select More than One Item

- Click-and-drag over items with a mouse to create a selection box.
- Use Ctrl+Click to toggle selection of successive items. Click on any one of multiple selected items to deselect all.
- Use Ctrl+A to select all items on a layout.

Rearrange Layout Items

To move an Item, simply click on it and drag it to a new position. The grid cell borders will be visible while the item is in motion. The grid cell aspect ratio is adaptive and depends on aspect ratio of the first item opened.



If the desired cell position is already occupied, the items will be swapped. If swapping is not possible due to too great a difference in item sizes or aspect ratio, the target cell(s) will be marked red:

If a bigger Item is being replaced by a smaller one, they will swap sizes as well as positions.

You can also use a right-click to move all Items in the layout at once, including the background image if there is one.

Resizing Items

To resize an item, select an edge in layout and click-and-drag the mouse to resize it. If resizing is possible, the new cells are highlighted in green:

If resizing is not possible, the cells will appear red:

In this case the best practice is to move the entire Viewing Grid using a click-and-drag and then resize the Item to occupy the available space, or move the desired Item away from the other items then resize it to occupy the available space.

Rotating an Item

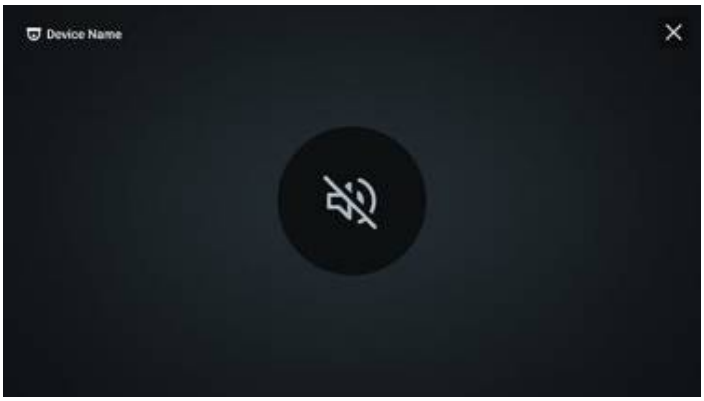
There are several ways to rotate an item in layout. A red directional arrow will indicate that the item is in rotation mode.

- Press Alt + click-and-drag over an item. Release when the item is at the desired angle. You can use Alt + Ctrl + click-and-drag to limit rotation to increments of 30 degrees.
- Click and hold the **Rotate** button ( ), then use the mouse to rotate the item. Release when finished. Press **Ctrl** while holding the **Rotate** button to limit rotation to increments of 30 degrees.
- It is also possible to use **Rotate to** in the item's context menu to choose from the options *0*, *90*, *180* or *270 degrees.*

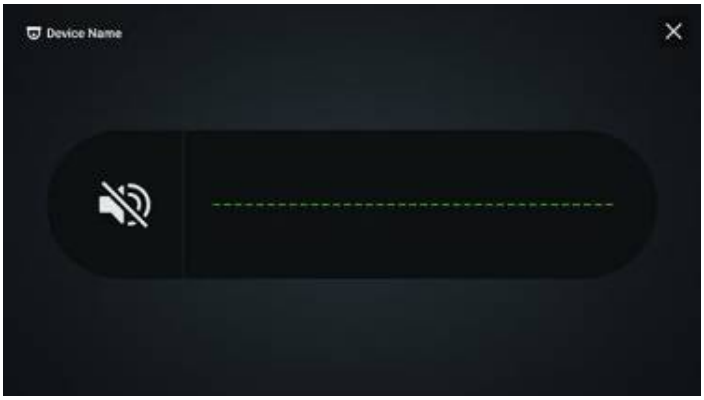
Audio Only Items

Key Concepts

- Audio only devices (speakers, microphones, intercoms) can be arranged on a layout similar to other items.
- Each audio item provides a steams that can simultaneously be played from a layout.
- The icon for an audio only devices is a speaker.
- The audio speaker icon includes a visualizer when active and reverts to simple icon when disabled
- Local workstation settings for volume and available speakers will impact playback options.



Audio Device Muted



Audio Device Active – No Sound

Audio Device Active – Sound Received

Related Topics

- Configuring Device Audio
- Working With Intercoms
- Adjusting Volume
- Using 2-Way Audio

Removing Items from Layout

To Remove an Item from a Layout

1. Open the desired layout.
2. Select the desired item in the layout.
3. Click the close icon  in the upper right-hand corner to remove a single Item.
4. To remove multiple items at once, use **Ctrl + click** to select the desired items then right-click on any item to open the context menu and select **Remove from Layout** (or use the DEL button on a keyboard).

To Remove an Item from a Layout Using the Resource Panel

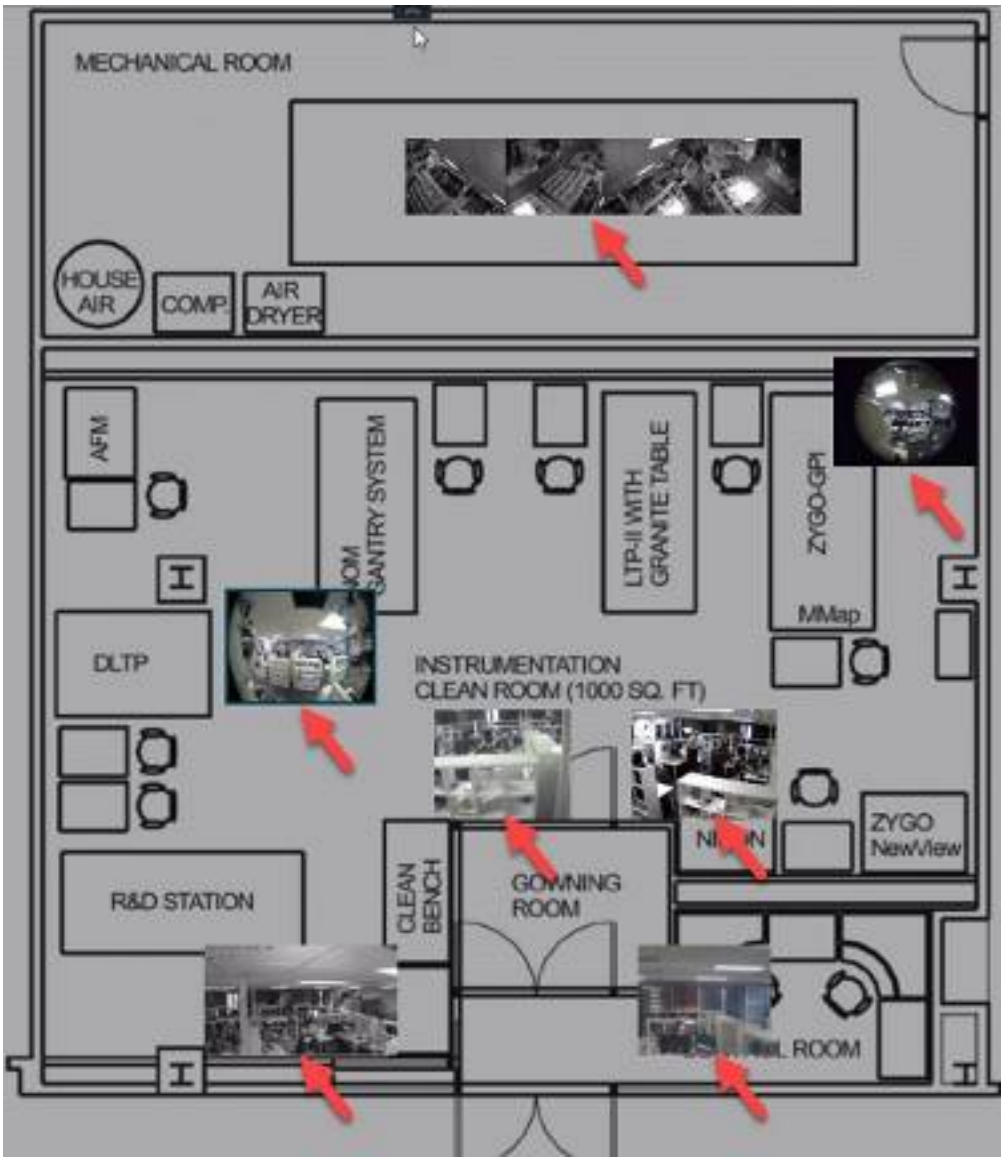
1. In the in Resource Panel, expand **Layouts** or **Users** and locate the desired layout.
2. Select the desired Item(s) under the specified layout.
3. Open the context menu and select **Remove from Layout** (DEL).
4. Confirm deletion by clicking *Yes*.

NOTE: The size of all items will stay the same or change depending on the position or number of remaining items.

Layout Backgrounds (E-Mapping)

User and Shared Layouts can be configured with a custom background image to facilitate Layout organization or provide additional information to the viewer such as a map or floor plan on which device thumbnails can be positioned to indicate their physical location. Users must be granted permission to access shared Layouts (see "Users and Groups" and "Permissions Management").

NOTE: Cloud Layouts do not support background images – they will be removed when a Layout is saved as a Cloud Layout.



To Add a Background Image

You can start with an empty layout or one that already has items. If you start with items in the layout, they will be reduced to thumbnail size they can be positioned as desired.

1. Open the desired picture in layout using **Main Menu** > **Open** > **File(s)** (**Ctrl + O**).
2. Right-click on the image and choose **Set as Layout Background** in the context menu. The image will be added, scaled to fill the entire layout area.
3. Alternately, you can open **Layout Settings** from the Viewing Grid context menu for the layout, open the **Background** tab, then click on *<No picture>* to browse for a background image.

The image types accepted are displayed in the dialog.

To Edit a Background Image

1. Open the layout with the background you want to change.
2. Right-click anywhere on the background and choose **Layout Settings** in the context menu.
3. Select the *Background* tab.
   - Click **Browse** to select a new image file to set as background.
   - Click **Clear** to remove the background image from the layout.
   - Click **View** to open the background image in an editing application.
   - Check **Crop to monitor aspect ratio** to adjust the aspect ratio of the image according to the monitor aspect ratio. For instance, if monitor resolution is 1920x1080 (16:9) and image resolution is 1920x1200 (16:10), then the image will be cropped on both top and bottom.
   - Use **Width** and **Height** to control the exact number of Viewing Grid cells the background image will span.
   - Use **Keep Aspect Ratio** to maintain the original aspect ratio of the background image while changing the width or height.
   - Use **Opacity** to control the translucence of the image (in percent).
5. Apply changes.
6. Make sure to save the layout when you are done.

Expanding to Fullscreen Mode

Fullscreen mode simultaneously expands display of a single Item to fill the entire layout, and hides all four sliding panels. If you expand an item to Fullscreen mode, only recorded fragments related to the selected Item are visible on the Timeline. Use the **ESC** key to exit Fullscreen mode.

You have the option to pin the timeline while in fullscreen mode to prevent it from automatically hiding. If you exit fullscreen mode with the timeline still pined, all other cameras will have the timeline automatically pinned when entering fullscreen mode.

To Toggle Fullscreen Mode on or off, Use One of the Following:

- Double-click or press **Enter** on an Item in layout.
- Open an item's context menu and select **Maximize Item** to expand or **Restore Item** to return the full layout and panel display.
- Create an event rule using the action "Set to Fullscreen".

NOTE: You can use a Tour to loop through Fullscreen display of each item in the active layout.

Zooming an Item or Layout

Use the mouse wheel to zoom the layout in and out, centered on the cursor location within the layout.

Fit in View

- *Fit In View* scales the Viewing Grid so that all items in the layout are visible. It is a convenient way to restore a layout you have zoomed or moved.
- Right-click on the layout background to open the context menu and select **Fit in View**.
- Fit In View is performed automatically when you change to *Fullscreen Mode* (see "Expanding Items to Fullscreen Mode").

Creating a Zoom Window

The *zoom window* feature lets you select a rectangular region in an item's display to instantly open that selected region as a new zoomed-in item on the current layout. You can create as many zoom regions as you like on a given item, and a zoom region can be moved from one camera to another in the same layout. Zoom windows are saved with the layout. Zoom windows can be especially helpful for viewing fish-eye camera output (see "Dewarping Controls").

NOTE: Zoom windows will set the camera's resolution to high.

Zoom regions on the source camera are editable. Click-and-drag inside a zoom region to reposition it, and click-and-drag on the zoom region outline to adjust its size. The related zoom window will adjust dynamically adjust.

Closing a zoom window deletes the zoom region on the source item.

To Configure a Zoom Window

1. Select a camera item.
2. Click on the **Create Zoom Window** icon ( ), then drag a rectangle over the desired area. A new zoom window item will open in the current layout.

Video Wall Mode

Video Wall mode lets you use a session of the Nx Witness Desktop Client to remotely control a display on other monitors in your Site via a LAN, WAN, or an internet connection.

A special Video Wall License is required (see "Nx Witness Licenses"). Each license allows you to display a Video Wall on up to 2 monitors (for example, 4 licenses allow you to display a Video Wall on 8 monitors). When a Video Wall license is invalidated, the *Video Wall Failover* feature kicks in and provides you with a 7-day grace period to prevent any interruptions in the Video Wall and allows you enough time to resolve the license issue (see Expired and Invalid License Keys). A countdown will be shown until your Video Wall license key has been restored or a new one is activated in its place. If no action is taken, the error message "Not enough licenses" will be shown, and your Video Wall will be disabled. Video Wall Failover is automatically enabled after Video Wall is configured.

NOTE: To be able to access, configure and control a Video Wall, a User must be assigned the related permissions (see "Permissions Management").

Layout and Camera settings may be changed while editing video wall screen and settings are saved on the Server or on the machine where video wall is running.

The resolution of a Camera when in the Video Wall mode can be changed via the context menu, but to take effect, this must be done in the *Screen* under *Video Walls* in the Resource Panel, and not in the standard layout.

Video Walls do not display any overlays or performance alerts while a camera is in live mode and do not display the Timeline unless that option is enabled. However, the timestamp is always displayed when a Video Wall camera is in archive mode, and it is possible to add backgrounds to Layouts and to assign a logical ID to a Video Wall Layout.

Video Wall Architecture

A *Video Wall Server* is the computer that hosts the main database of a *Video Wall Cluster*. Video Wall displays can be connected to this Server and it can act as the Video Wall Processor as well. All computers that are part of the Video Wall Cluster (clients and controllers) should be Cloud connected or able to connect to the Server.

The *Video Wall Processor* is the computer that Video Wall displays are connected to. Depending on its configuration it can handle one or several displays. There is no limit to the number of Video Wall Processors that can be combined in a Video Wall Cluster.

A *Video Wall Controller* is any computer that can connect to a Video Wall and control it. It can even be a laptop; the only requirement is that the video adapter should support OpenGL > 2.0.

In order to operate Video Wall properly, Nx Witness should be installed on every computer in the Video Wall Cluster:

- Video Wall Server: Full installation.
- Video Wall Processor(s): Client only installation.
- Video Wall Controller(s): Client only installation.

If all Video Wall components are installed on one computer, choose Full installation.

Initial Video Wall configuration is performed in several steps:

- Configuring a Video Wall Display
- Switching to Video Wall Mode
- Controlling Video Wall Displays

You can also Delete a Video Wall or it's Elements, or Push an Operator's Screen to a Video Wall.

The number of displays available to any single computer is limited by the number of video outputs it has. To extend Video Wall it is necessary to add additional computers and combine them with the Video Wall Cluster. See "Configuring Video Wall on Several Computers".

Configuring a Video Wall Display

Use the Desktop Client running on what will be the display computer to complete the following steps.

Create a new Video Wall

1. Open the **Main Menu** and choose **Add** > **Video Wall**.
2. Enter a name for the Video Wall.
3. Apply changes.
4. The newly created and named Video Wall will be added to the Resource Panel.

Configure Video Wall Layout

To make a computer display part of Video Wall it is necessary to perform the following settings **on that computer**:

1. Right-click on the Video Wall in the Resource Panel and choose **Attach to Video Wall**.
2. Nx Witness automatically detects, numbers, and previews the displays connected to the computer.

3. Click on an item in the dialog (it will change color and be retitled "New Item"). In this state you can drag the edges to resize the item, click-and-drag in the center to reposition it, or click on the "X" in the upper-right corner to remove the screen.

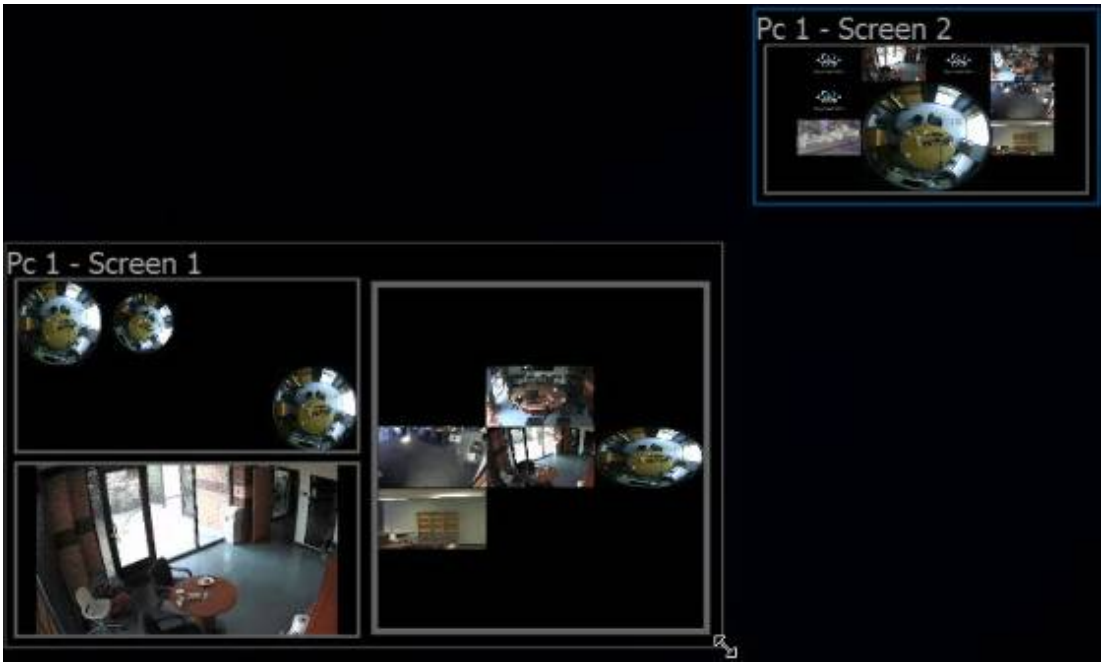
4. Typically, one Virtual screen represents one physical display. It is also possible to stretch one Virtual Screen across several physical displays:

Or, you can design one physical display that contains multiple Virtual Screens, in various combinations:

5. Once the screens are arranged as desired, click OK to save the configuration.

6. At this point you can drag-and-drop resources (devices, web pages, local files, etc.) from the Resource Panel into the Video Wall layout. It is possible to place a single device or an entire Layout into each Virtual Screen.

NOTE: Cross-Site Layouts cannot be used.



- To remove a resource from a Virtual Screen, right-click on it in the Video Wall layout and choose *Clear Screen*.
- To simplify the calibration process it is possible to add identification information of a resource the corresponding physical Display. To do so right-click on the desired Virtual Display and select *Identify.*

7. To save changes, right-click on the Video Wall in the Resource Panel and choose *Save Current Matrix*. The Matrix will be added to the Resource Panel under the current Video Wall, where you can right-click to rename it, load or delete it.
8. Right-click on the Video Wall in the Resource Panel and choose *Save Video Wall* (Ctrl+S).

To finalize configuration it is necessary to Switch Video Wall Processor to Video Wall Mode. After a Video Wall has been started on the Video Wall Processor, the current configuration can also be changed on the Video Wall Controller. To restore a Video Wall view, expand the Video Wall in Resource Panel, right-click on a saved Matrix and choose *Load Matrix.*

To open Video Wall on a Video Wall Controller

- Drag Video Wall onto the layout.
- Right-click on the desired Video Wall in Resource Panel and choose *Open Video Wall.*

Switching to Video Wall Mode

To control a Video Wall it is necessary to switch the Video Wall Processor to Video Wall Mode. **This should be done on Video Wall Processor.**

Usually Video Walls are controlled from a Video Wall Controller, and the computers the displays are connected to are easily accessible. So it is recommended to set up automatic switching to Video Wall Mode:

1. Right-click on **Video Wall** in Resource Panel and choose **Video Wall Settings**.
2. Click on **Launch video wall when Windows starts** and click *OK*.

NOTE: This option is available for Windows PCs only and is enabled by default.

To switch to Video Wall Mode, right-click on **Video Wall** in the Resource Panel and choose *Switch to Video Wall Mode* and click *Close* on the dialog window.

Several instances of the Client will be launched. The Client will be switched to Video Wall mode and will become inoperable. At this point it is possible to change settings and control the Video Wall from the Video Wall Controller.

To switch back from Video Wall to standard mode it is necessary to close all Client instances and relaunch the Client once more. In this case, operator won't be able to control displays connected to this Video Wall Processor and the corresponding screens will be displayed in the Resource Panel as offline.

Configuring Video Wall on Several Computers

To increase the number of Video Wall displays you must to add additional Video Wall processors.

To Add a Video Wall Processor

1. Run the Desktop Client on the PC that should be added to the current Video Wall. Physical displays should be connected to this machine.
2. Right-click on desired Video Wall in the Resource Panel and choose **Attach to Video Wall**.
3. Repeat all steps described in "Configuring a Video Wall Display".
4. Switch to **Video Wall Mode** (see "Switching to Video Wall Mode").
5. Repeat the steps above on each Video Wall Processor.

Video Wall mode will be extended and will include displays connected to the newly attached Video Wall Processors.

Deleting a Video Wall or Elements

To Delete a Video Wall, right-click on it in the Resource Panel and choose *Delete*, then click *Delete* in the confirmation dialog. This action will delete all Screens and configurations related to this Video Wall, and will stop the Video Wall on every single Video Wall Processor.

The Following Video Wall Elements Can Be Deleted

Screen

- Right-click on a screen, within a video wall in the Resource Panel and choose **Delete**, then click **Delete** in the confirmation dialog. This results in stopping the Video Wall in the corresponding physical display.

Matrix

- Right-click on a video wall matrix in the Resource Panel and choose **Delete**, then click **Delete** in the confirmation dialog to delete a saved configuration.

Controlling Video Wall Displays

Users with sufficient rights can change the layouts that are placed on a Video Wall.

As soon as a Video Wall Display is opened on the Video Wall Controller, the User can control it like any other layout – it is possible to change the layout, navigate through archive, perform searches, etc. All changes made on the Video Wall Controller are immediately displayed on the Video Wall itself.

It is also possible to push the Video Wall Controller desktop view to Video Wall. See "Pushing Operator's Screen on Video Wall".

To Control Video Wall

1. Use one of the following to open Video Wall on the Video Wall Controller:
   - Drag Video Wall onto the layout.
   - Right-click on desired Video Wall in Resource Panel and choose *Open Video Wall(s)*.

   NOTE: It is not possible to open videos in this Layout.
2. Double-click on the desired Video Wall Screen to enter control mode. The layout of this screen will be opened and you will be able to perform any necessary operations:
   - Adding Items to a Layout
   - Removing Items from a Layout
   - Selecting Items in Layout
   - Moving and Swapping Items in Layout
   - Resizing Items
   - Cell Spacing

- Cell Aspect Ratio
- Creating a Zoom Window
- Working with Multiple Nx Witness Windows
- Navigating through Archive and Live
- Pushing Operator's Screen on Video Wall.

All changes will be reflected *immediately* on the corresponding Video Wall Display.

Pushing Operator's Screen on Video Wall

For Windows only, Nx Witness provides the ability to push Operator's screen to Video Wall. This is done from the *Video Wall Controller* on a PC:

1. Open Video Wall on Video Wall Controller by dragging the desired Video Wall from the Resource Panel onto the layout, or by right-clicking on the desired Video Wall in the Resource Panel and choosing *Open Video Wall*.
2. Right-click on the desired Screen and choose *Push my Screen*. Everything displayed on the operator's desktop will be sent to the Video Wall screen, including sound.
3. To stop the broadcast, locate the desired Screen in the Resource Panel or on Video Wall Layout, right-click and choose *Clear Screen*.

Playback and Export

Nx Witness provides viewing and playback of the following content:

- *Cameras* – Live and archived footage.
- *I/O Modules* – Sound can be recorded from an I/O module with a microphone connected and played live or from archive.
- *Local files* – Saved video and image files.

In addition to the internal dynamic resolution switching, you can use these manual adjustment features if you are experiencing image stuttering during live streaming, or if there is too much time between actual action and displayed action in Live view:

- Setting Item Resolution
- Setting Layout Resolution
- Configuring Live Buffer Size
- Double Buffering
- Disabling Blur for Intel HD Graphics
- Hardware Video Decoding

There are several tools that make archive search faster and easier:

- Navigating and Searching Video

- Using Bookmarks

This section also describes:

- Playing Local Video Files
- Exporting Video
- Using Audio
- Taking Screenshots
- Tours – Cycles display through items in a single layout.
- Showreels (Tour Cycle) – Cycles display through multiple entire layouts.

Setting Item Resolution

It is possible to override the default image quality for a single item in layout. This is useful, for example, when you need to reduce client CPU usage (in which case you set playback to low-resolution), or to enhance image quality for a given item (in which case you set playback to high-resolution).

NOTE: This setting is saved for each item individually, so it is possible to have the same device playing back at different resolution levels in different layouts. Alternatively, all the items in a layout can have their resolution set at once (see "Setting Layout Resolution").

Fullscreen mode and dewarp mode will always use the primary stream (see "Fullscreen Mode" and "Dewarping Controls" for details).

NOTE: Image quality settings are dependent on the camera's primary/secondary stream settings in Nx Witness and any inherent limitations the camera may have (see "Dual Streaming").

To Specify Item Playback Resolution

1. Right-click on the item in layout to open the context menu and choose **Resolution**.
2. The default is **Auto**. Select **High** or **Low**.
3. Click the information icon or use the item context menu **Show on Item > Info** (**Alt+I**) to confirm the setting (see "Image Display Controls").

Setting Layout Resolution

Setting Layout Resolution Manually

It is possible to set the resolution for all items in a layout at once. Right-click on the Viewing Grid, choose **Resolution** in the context menu, then select **Low** or **High**. The change is applied at once, but only for the current session. The default setting is **Auto**. The **Custom** setting indicates that one or more items in the layout are playing back at a different resolution than the others.

This can occur when the resolution setting for a specific item has been set manually. See "Setting Item Resolution".

Auto Pausing Video Playback

Nx Witness also offers significant bandwidth savings with the option to automatically pause video playback due to inactivity after a certain period of time. To set this option, open **Main Menu**, go to **Local Settings** > **General** and check **Auto Pause Video**, then set the desired time interval (in minutes).

Configuring Live Buffer Size

On some cameras, live playback may stutter, or there may be a time significant delay between actual actions and the action shown on Live view. For a better viewing experience it may be helpful to adjust the live buffer size from the default of 500ms.

To do so, open **Main Menu**, choose **Local Settings** > **Advanced**, then adjust the **Maximum Live Buffer Length** to the smallest possible value that does not cause issues with live view on all cameras.

- Larger buffer makes playback smoother but increases the delay between real time and the live display.
- Smaller buffer decreases the delay but can cause stutters on playback.

See also "Double Buffering" and "Disabling Blur for Intel HD Graphics".

Double Buffering

On some graphic cards, drivers may have problems with OpenGL drawing, resulting in very high or even 100% CPU load. In this case, the issue may be resolved by disabling double buffering, which is enabled by default.

To disable double buffering, open **Main Menu**, choose **Local Settings** then in the **Advanced** tab uncheck the **Double Buffering** checkbox and restart the Nx Witness client to apply the change.

Disabling Blur for Intel HD Graphics

In some situations the client application may work incorrectly on certain computers where an integrated Intel graphic chip (Intel HD Graphics) is installed. This may result in noticeable frames per second drop or incorrect video playback. In this case it may help to disable the blur effect in client settings.

To do so, choose **Local Settings** (**Advanced** tab), then check **Disable blur**, and click *Apply* or *OK*. The Nx Witness client must be restarted for this change to take effect.

NOTE: Do not disable blur unless the graphic adapter is from Intel and you are experiencing graphic issues.

Hardware Video Decoding

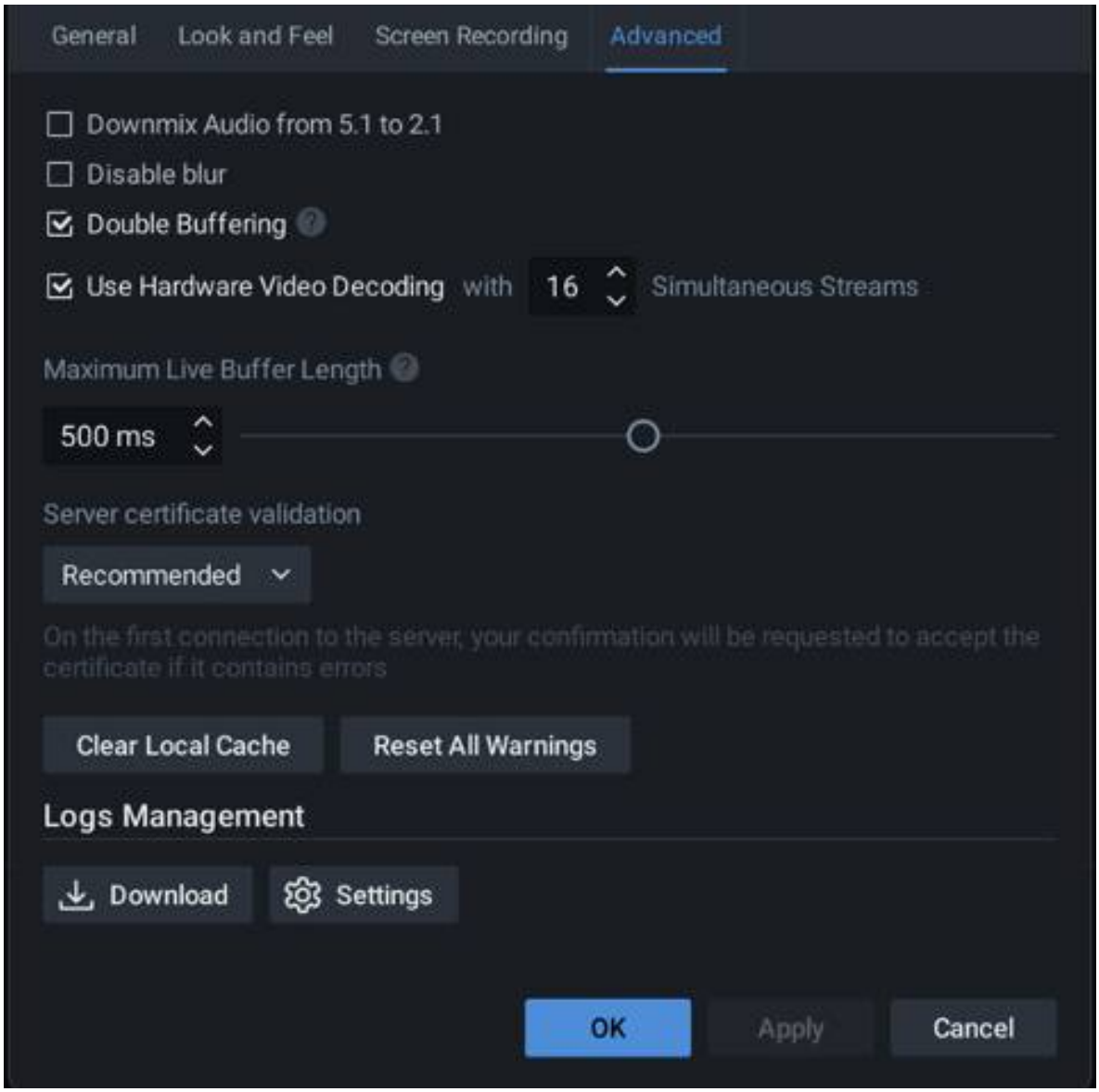
The Nx Witness Desktop Client supports hardware acceleration on Graphical Processing Units (GPU) from NVIDIA and Intel. Enabling hardware acceleration can free up computational resources for other tasks and often improve the performance of lower powered hardware or increase the ability to decode very-high resolution cameras and streams.

To Enable Hardware Acceleration:

1. Open **Main Menu > Local Settings > Advanced**
2. Check the box for *Use Hardware Acceleration Decoding*.
3. Set the number of simultaneous streams that will receive hardware acceleration.
4. Click **Apply** to save changes.

To Disable Hardware Acceleration:

1. Open Main Menu > Local Settings > Advanced
2. Deselect the box for *Use Hardware Acceleration Decoding*.
3. Click **Apply** to save changes.



Navigating and Searching Video

Since an archive may contain a significant volume of video data, the following search methods are available to minimize the time spent searching for a particular event or segment.

- *Timeline* – Speeds navigation through live and archived footage. See "Parts of the Timeline" and "Using the Timeline".
- *Calendar* – Zooms the Timeline to a selected date (see "Using the Calendar").
- *Motion Smart Search* – Selects a region on video, refines the archive, and highlight fragments that include motion (see "Performing Motion Smart Search").
- *Thumbnail Navigation* – Small previews are displayed on top of the Timeline to help locate a particular image or event (see "Using Thumbnails").

- *Preview Search* – Select a region on the Timeline and allow for the application to provide videos that represent a time period based on timestamps (see "Preview Search").
- *Bookmarks* – This feature lets you select a segment of footage from a single device, give it a name, description and tags, and instantly export the bookmark (see "Using Bookmarks").

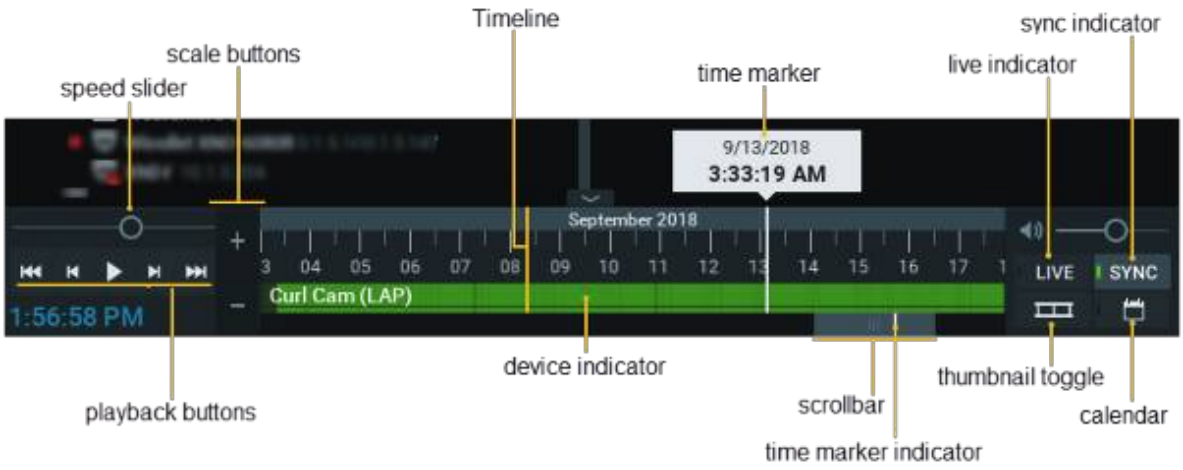
Parts of the Timeline

The Timeline provides a convenient way to navigate through live or archive video and control display speed.

NOTE: Timeline behavior is slightly different for archive and live footage.

- *LIVE* – Click to switch the selected camera(s) to live playback mode.
- *SYNC* – Click to synchronize all items displayed in the current layout to the same date and time. When SYNC is enabled, the speed slider and LIVE button apply to all items in layout. When SYNC is off, the speed slider and LIVE button apply only to the selected item. See "Synchronizing Playback".
- *Thumbnails* – Use to show/hide thumbnail images of the active device above the Timeline.
- *Calendar* – Opens a calendar option for Timeline navigation. See "Using the Calendar".

Timeline for Archive Display



Timeline Scale and Position Controls

- *Timeline* – Controls navigation through archive footage.
- *Time marker* – Indicates the current date and time of the selected video.
- *Scrollbar* – Use to quickly move backwards and forwards along the Timeline. The scrollbar scales with the Timeline zoom level.
- *Time marker indicator* – Indicates where you are on the Timeline relative to the time marker.
- *Scale buttons* – Use to scale date/time display from increments of 100ms to 1 month.

- *Thumbnails* – Click-and-drag the top of the Timeline to see a thumbnail view of the currently selected item (see "Using Thumbnails").
- *Device indicator* – Displays the name of the currently selected device and also indicates archive status, where bright green indicates a recorded segment, gray indicates no recorded footage, blue indicates a Bookmark, and, if Motion Smart Search is active, red indicates regions where motion has been detected (see "Performing Motion Smart Search"). When a layout contains multiple devices, combined status for the unselected devices is shown in a very narrow bar beneath the larger bar.

Timeline Speed Controls

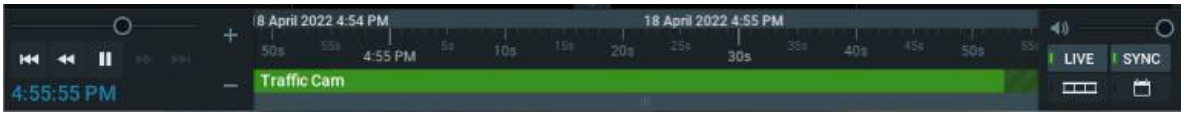
- *Playback buttons* – Use to start, stop, and control playback speed; click forward or reverse to jump 10 seconds.
- *Speed slider* – Provides additional control for playback speed.

Timeline Volume Control

See "Adjusting Volume".

Timeline for Live Display

By default, all devices display a live image when first opened in layout. The last-minute of the archive is generally accessible in Nx Witness. Usually, only the last several seconds will not be available for immediate playback (represented by diagonal stripes on the Timeline).



Using the Timeline

The Timeline itself and the scrollbar respond to a broad set of mouse wheel, mouse click, and button commands.

Click on the desired date and time on the Timeline to select it. If archive exists at that point, the time marker is placed at that point. If not, the time marker jumps to the beginning of the next recorded segment. Playback will begin in real time if playback is active. If playback is paused, the time marker position and content remains static until you click elsewhere on the Timeline.

If the desired point in time is not currently visible there are several ways to locate it.

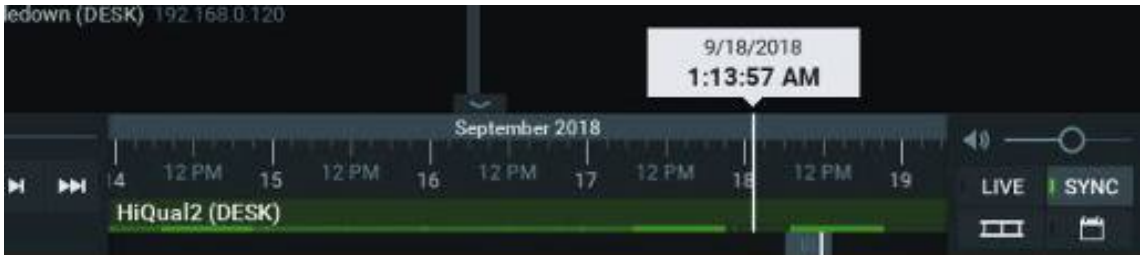
To Scroll the Timeline

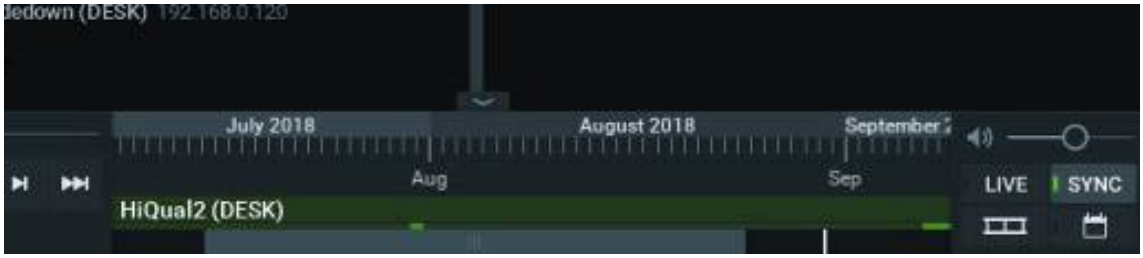
- Click-and-drag the scrollbar back or forth to the desired position.
- Use Ctrl+mouse wheel over the Timeline or scrollbar.

To Scale the Timeline

Scaling is centered on the cursor unless the cursor is at the very end of the Timeline, in which case scaling is anchored to that end point. The scrollbar scales with the Timeline to indicate

how much of the total Timeline is currently visible on screen. The white time marker indicator shows the location of the time marker in relation to the current Timeline display. For example, in the left illustration below, the scrollbar is small because only a small portion of the total Timeline is visible, and the scrollbar overlaps the time marker indicator because the time marker is currently visible. In the right illustration, the scrollbar is large because a large portion of the total Timeline is visible, and the scrollbar does *not* overlap the time marker indicator, because the time marker (which is still at 9/18/2018) is not currently visible.





- Use the mouse wheel over the Timeline or scrollbar to zoom in (smaller time increments) or out (larger time increments).
- Click on the scale buttons to zoom in (+) or out (−) by 10%. Double-click to zoom by 20%.
- Click and hold the scale buttons for rapid zoom.
- Click in the scrollbar background area to scroll "screen by screen" in increments the size of the current display. Double-click to scroll by two screens.
- Double-click on the scrollbar to zoom out to the maximum available view.

<u>During Playback</u>

Long-Press or Double-Press (in one second) Press or Z to jump backwards to rewind to previous chunk.

- If the rewind button is pressed while in Live mode, the mode will switch to archive playback.
- If the fast forward button is pressed while viewing archive, display will switch to Live mode once the current time is reached.
- Use the **Speed Slider** to temporarily change playback speed by draging-and-holding it to the right for fast forward or to the left for fast rewind.
  - The **Speed Slider** can also be set in 2x, 4x, 8x, and 16x increments. Release to return to 1x speed (during playback) or 0x (when paused).

NOTE:When SYNC is enabled, the speed slider and LIVE button apply to all items in layout. When SYNC is off, the speed slider and LIVE button apply only to the selected device.

To Control Playback Speed

- Press **Space** to toggle between play and pause.
- Press  to play at actual speed.
- Press  to pause.
- Press  or **Ctrl**+**Right Arrow** to fast forward. Available speeds are 2x, 4x, 8x, and 16x.
- Press  or **Ctrl**+**Left Arrow** to rewind. Available speeds are -2x, -4x, -8x and -16x.
- Press  or **X** to jump forward to the next recorded chunk.
- Press  or **Z** to jump backwards to the previous recorded chunk.

When Paused

- Press  or Ctrl+Right Arrow to jump to the next frame.
- Press  or Ctrl+Left Arrow to jump to the previous frame.
- Press  or X to jump forward to the next recorded chunk.
- Press  or Z to jump backwards to the previous recorded chunk.
- The speed slider has increments 0.25x, 0.5x, 1x, 2x, and 4x.

To Select a Time Segment

- Click-and-drag on the Timeline.
- Hover over the Timeline and open the context menu to choose **Mark Selection Start** (shortcut **[**), then move to the end location and choose **Mark Selection End** (shortcut **]**).

The selection will be highlighted with blue shading. Once a segment is selected, you can click-and-drag the edges to adjust its length. You can also use the context menu to select *Clear Selection or Zoom to Selection*. If you click outside the selected segment the selection will be lost.

Using Thumbnails

Thumbnails are single snapshots taken from archived video footage. They provide a visual preview of footage to speed and simplify archive searches. Hover the mouse cursor over the Timeline to see a thumbnail for that moment in the Timeline.

To Open the Thumbnail Panel

- Select the desired device in layout then click-and-drag the upper edge of the Timeline to open the thumbnail panel.

- Click on the Thumbnail button ( ) to show/hide thumbnails.

The higher you drag upwards, the larger the thumbnails will be.

A tiny dot near the bottom-center of each thumbnail indicates the exact moment the snapshot was taken. You can click on a thumbnail to jump to the moment in archive when it was taken.

If no thumbnails are displayed, there is no archive available for the selected camera during the visible time period.

To close the thumbnails, click-and-drag the upper edge of the thumbnails panel down or or click on the Thumbnail button ( ).

Synchronizing Playback

All cameras in a layout can be synchronized to a common playback date and time by enabling the SYNC button ( ). When SYNC is on, the speed slider, playback controls (ex. search, fast forward, rewind), and LIVE button apply to all items in layout. If no archive exists for a given camera when devices are synched, that item displays "no data".

When SYNC is off, the speed slider, playback controls, and LIVE button apply only to the selected item. It is possible to view each camera at a different point in time. Thin blue lines on the Timeline will indicate the current position of each camera that has archive. If no archive exists for a given camera, that device will jump to live display.

Using the Calendar

The Calendar is used to navigate the Timeline. The Calendar is displayed is toggled by clicking on the Calendar icon in the lower right corner of the Timeline. The Calendar will overlay the Notification Panel and Viewing Grid or Current Layout when the Desktop Client window is of a small size.

Using visual accents on the Calender

- A blue square outlines the current date.
- Date and Time markers displayed on the calender:
  - Have a green underline where recordings exists and Bookmarks, Notifications, or Alerts are selected in the Notification Panel.

- Have a red underline where motion has been detected and Motion is selected in the Notification Panel.
- Have an orange underline where objects have been detected and the Objects are selected in the Notification Panel

Navigating the Calender

- Click on the Month and Year header to open the Month Picker, or use the arrows to move forward or backward by a month.
- Click on a date and the Timeline will center on the selected date.
- Click on a time and the Timeline will center on the selected hour.
- Use Ctrl + Click to select beginning and ending dates or blocks of time to display.
- Quick jump buttons along the bottom of the Calendar will select Today (date on archive server), the past hour, the past 24 hours, the past 7 days, or the past 30 days.

Performing Motion Smart Search

Smart Motion Search instantly searches archive to discover and highlight the segments that contain motion in a user-selected region of a video image. Simply select the desired region and Nx Witness will display all segments that contain motion throughout the archive (scanning through a yearly archive only takes a few seconds).

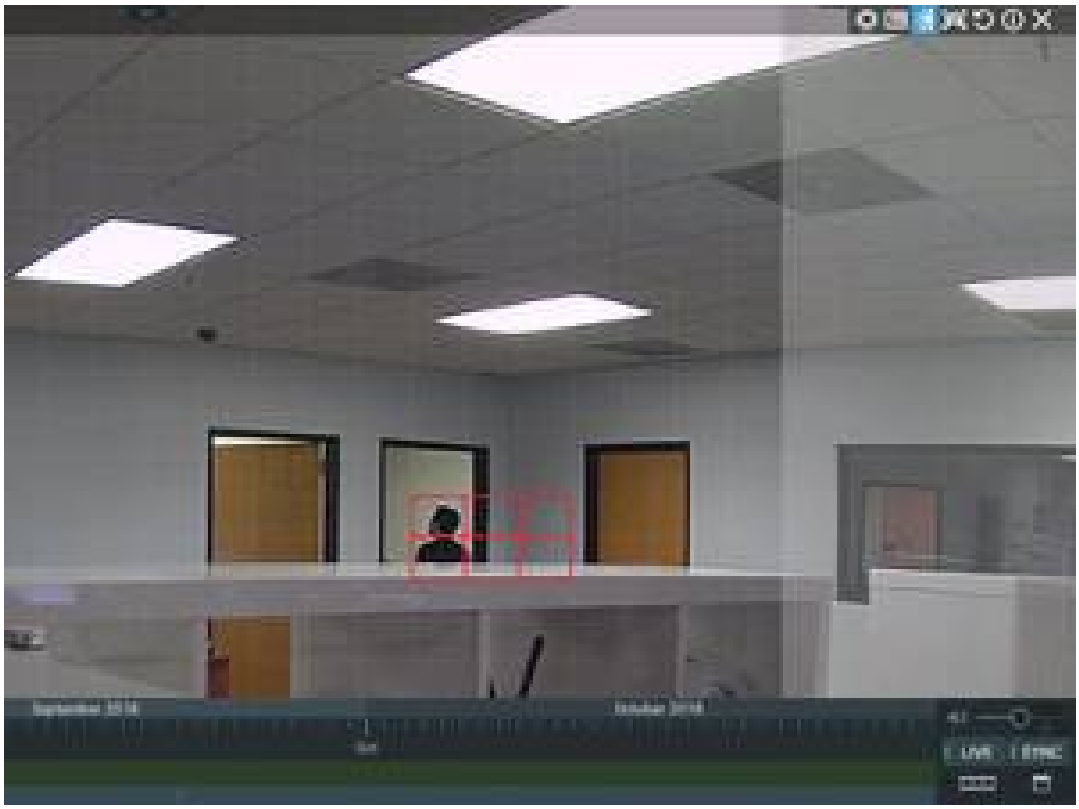
Motion Smart Search requires that the selected camera supports motion detection, and that Nx Witness motion detection be enabled.

NOTE: Motion smart search cannot be applied to Motion Mask regions, where motion detection has been blocked (see "Setting up Motion Detection"). However, if no area is selected, Nx Witness returns results from the entire video region.

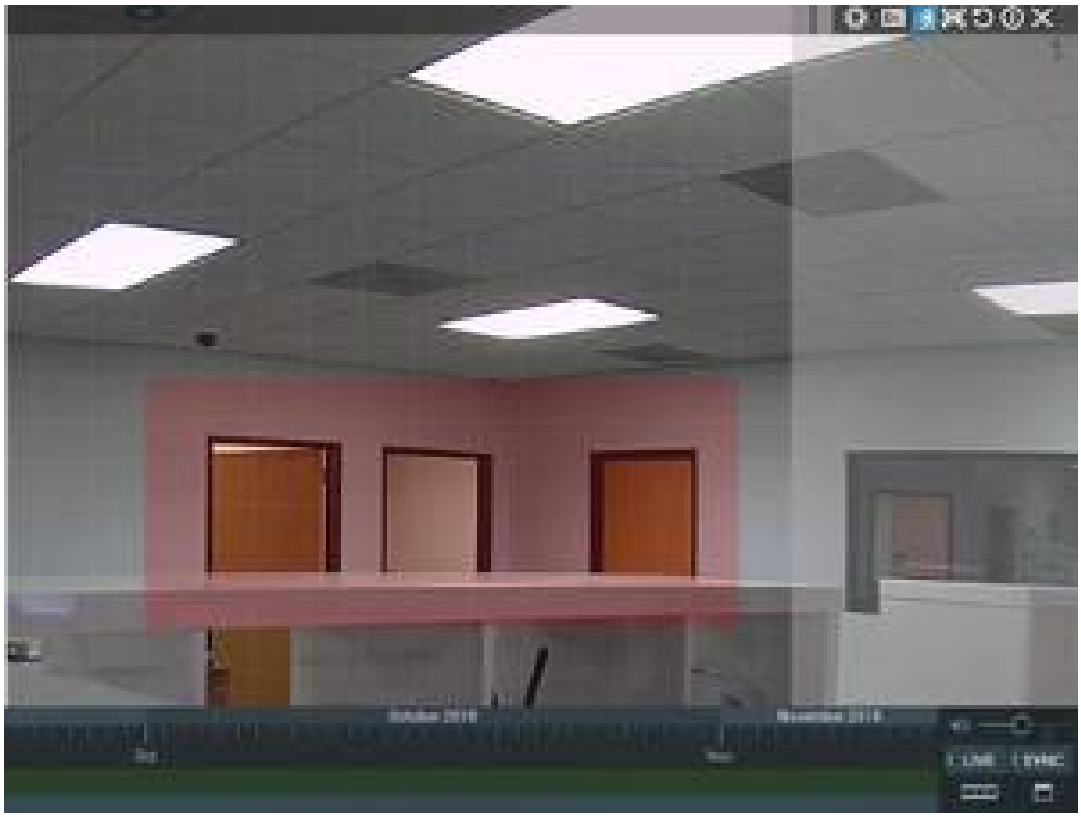
1. Open the camera's motion grid in one of the following ways:
   - Use the  icon on the camera tile.
   - Open the camera's context menu and choose *Show Motion/Smart Search*.

- Select the camera and use the shortcut **M**.
- Use Shift+click-and-drag to simultaneously enable Motion Smart Search and select the desired region.

The motion grid will display as a gray overlay. Red cell outlines indicate that motion is detected:



2. Use Click-and-drag to select the region where motion smart search should be applied or use Ctrl+click-and-drag to select multiple areas.



3. As soon as the region is selected, the Timeline will display red bars, each of which indicates an archive period that contains motion in the selected region.
4. Scroll through the Timeline to the red bars to quickly and easily locate motion in the archive.
5. To disable Smart Motion Search, clear all regions in the motion grid, toggle the button, or use the context menu option **Hide Motion/Smart Search** (**M**).

Preview Search

This feature helps to search through data by breaking a selected time range into smaller segments of equal length and displaying these segments as separate items in a new layout tab. Unrecorded time segments are displayed as grey or an empty space on the timeline.

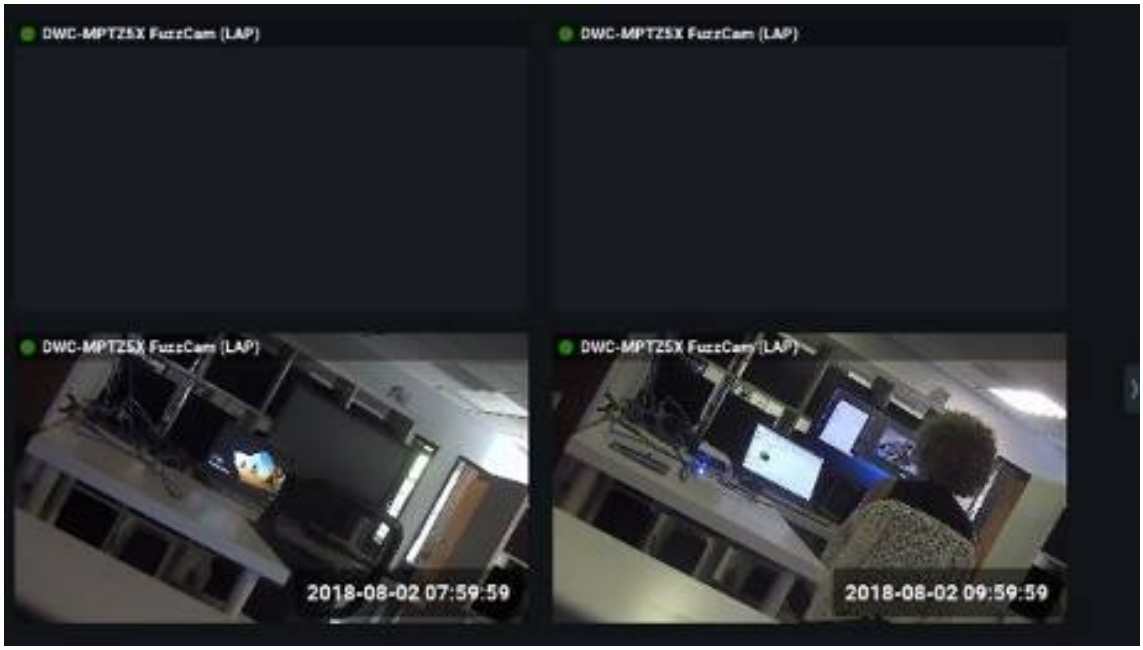
Preview search can be used iteratively until the desired event is located.

For instance, a one month period will be broken down into ten 3-day segments, the 3-day segments will be broken down into nine 8-hour periods, the 8-hour segments into eight 1-hour periods, and so on. It may therefore take three to five iterations to locate a given event within an initial period of several months.

<u>To Perform Preview Search</u>

1. Select the desired camera in layout.
2. Click-and-drag on the Timeline to select a period to search.

3. Right-click on the selection and choose **Preview Search** in the context menu. A new tab will open with multiple items each showing a still of the start of a segment, in time order from upper left to lower right.



4. Click on an item to skip the Timeline to the starting point of the segment shown in the still. The segment will be selected when you click on the item.
5. Click the play button to view the selected segment in that item.
6. If desired, use the Timeline context menu to perform any of the available commands (clear or zoom to the selection, add a bookmark, export video, or perform another preview search).
7. Repeat the above steps as needed.

Viewing Archive from Deleted Cameras

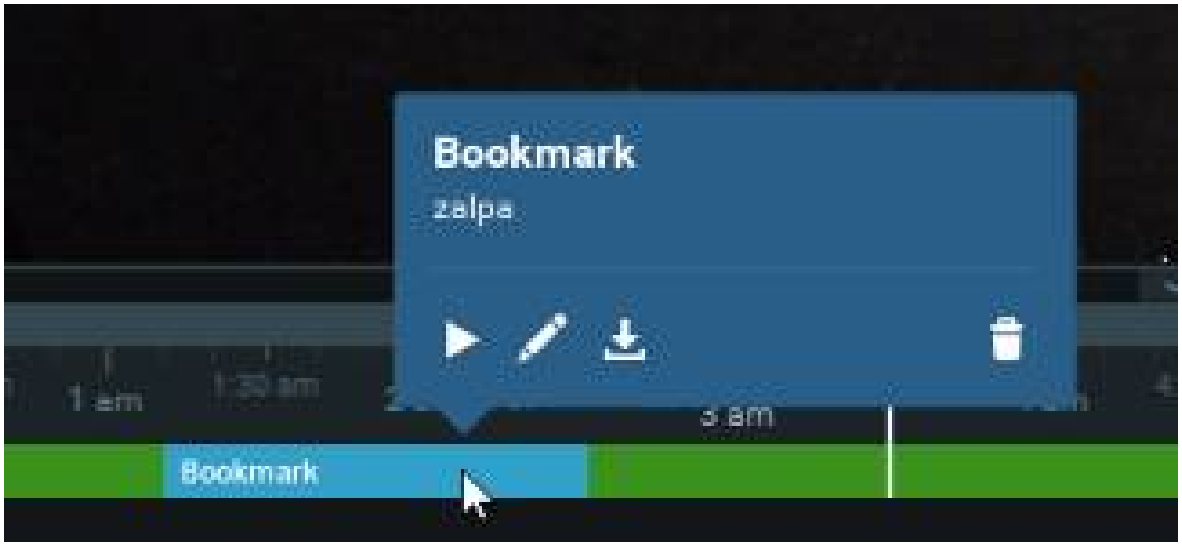
When a camera has been deleted from the Site, access to its footage is lost. To make such footage available again the index that maps the relationship between archive filenames and the physical location of the archive files on the storage drive must be restored – see "Reindexing and Fast-Scanning Archives".

After the archive is restored, the deleted camera will again be displayed in the Resource Panel. Though the device will be marked offline and is not available for live video, it is possible to navigate through its archive.

Using Bookmarks

A Bookmark is a footage in the archive that is marked and named to make it easy to find and review. When the "Bookmarks Tab" of the Notifications Panel is active, Bookmarks for the selected Camera appear as blue segments on the Timeline. Only if the Bookmarks Tab is open and only if a camera actually has Bookmarks can they be displayed. When several items are open in a layout, the Timeline only displays Bookmarks for the selected camera.

Hovering the cursor over a Bookmark segment on the Timeline opens controls for that Bookmark.



– Plays the Bookmark from the beginning.

– Opens the *Bookmark* dialog where the name, description and tags can be edited.

– Opens the *Export Video* dialog.

– Deletes the Bookmark.

Bookmarks can be created manually on the Timeline (see "Creating Bookmarks Manually"), or they can be created automatically as the action of an event rule (see "Create Bookmark"). The action of completing an acknowledgment in response to a notification also generates a Bookmark of the triggering event.

The name, description and tag properties of Bookmarks are searchable and editable (see "Searching Bookmarks"). Bookmarks are exported with the archive of cameras, and can be exported and saved separately (see "Exporting Bookmarks"). When archived footage is deleted, the associated Bookmarks are deleted as well. You can also manually delete Bookmarks (see "Deleting Bookmarks").

To Play a Bookmark

- Hover over the Bookmark in Timeline and click the play icon (opens in the current layout).

- Double-click a single record in the Bookmark Log (opens in the current layout).
- Invoke the context menu in the Bookmark Log and choose **Open in New Tab** (opens in a new tab).

Sharing Bookmarks

- The Enterprise Edition of Nx Witness allows bookmarks to be shared.
- Bookmarks can only be shared from within the Nx Cloud portal.
- Shared bookmarks include an additional icon of 'multiple users' when viewed in the Desktop Client.

Sharing Bookmarks

- The Enterprise Edition of Nx Witness allows bookmarks to be shared.
- Bookmarks can only be shared from within the Nx Cloud portal.
- Shared bookmarks include an additional icon of 'multiple users' when viewed in the Desktop Client.

Creating Bookmarks Manually

To Create a Bookmark Manually

1. Open the desired camera (it must have recorded footage).
2. Select the time span of the Bookmark on the Timeline:
   - Click on the Timeline and drag the time indicator line to mark a segment, which will be highlighted with a blue overlay.
   - Right-Click on the Timeline to open the context menu and select **Mark Selection Start** (shortcut **[**), then Right-Click on the desired end point, and select **Mark Selection End** (shortcut **]**).
3. Once a time segment is defined, you can adjust it by clicking and dragging the edges of the blue block, or it can be removed entirely using **Clear Selection** in the Timeline context menu.
4. Right-click in the blue highlighted area and select **Add Bookmark**.
5. In the *Bookmark* dialog that opens, enter a **Name**, **Description** and if desired, one or more **Tags** separated by commas. (You can use a preexisting tag or create a new one. The most commonly used tags will be suggested.)
6. Click *OK* to accept or *Cancel* to close without saving.

Searching Bookmarks

You can use the *Bookmark Log* to search for and edit Bookmarks (see "Searching and Filtering in Nx Witness"). The "Bookmarks Tab" also provides some search and filter operations.

To Open the Bookmarks log

1. Open the **Main Menu** and select **Bookmark Log** (Ctrl+B).
2. You can sort any of the columns (*Name, Camera, Start time, Length, Created, Creator, Tags, and Description*) in ascending or descending order. You can also filter the Bookmark Log as follows:
   - *Date* – Click on the drop-down arrow to open a calendar popup for the start (left date field) and end (right date field) date filter.
   - *Devices* – Click on **All Camera** to open the standard *Select Cameras* dialog where you can select from the available devices, grouped by server.
   - *Search* – Text entered in this field yields any Bookmarks containing those characters their *Name*, *Description* and *Tags* fields. Returns up to 1000 results. Results can be cleared by clicking **Clear Filter**. See "Searching and Filtering in Nx Witness" for more details.
3. The *Bookmark Log* context menu lets you perform the following operations:
   - *Open in New Tab* – opens a new layout tab and plays the highlighted Bookmark (double-click).
   - *Edit Bookmark* – opens the *Bookmark* dialog where you can edit the *Name*, *Description* and *Tags* for the highlighted Bookmark.
   - *Export Bookmark* – exports a video file containing the Bookmark(s). Available for a single bookmark, or when multiple Bookmarks are selected (see "Exporting Bookmarks").
   - *Copy Bookmark Text* – copy the selected Bookmark's contents in text format.
   - *Delete Bookmark* – deletes the selected Bookmark(s). Available for a single bookmark, or when multiple Bookmarks are selected.

Exporting Bookmarks

Bookmarks are saved to archive and can be exported like any other video. Use one of the following to locate a Bookmark and open the **Export Video** dialog. You can view and manipulate exported bookmarks in the same way as a exported layouts.

NOTE:Bookmarks are included in exported video.

- Open **Main Menu**, choose **Bookmark Log**, right-click on the desired bookmark and select **Export Bookmark**.
- Use the Timeline to find the desired Bookmark (see "Searching Bookmarks"), hover over it and click on the **Export Bookmark** icon in the Bookmark dialog.

Use the Export Video dialog as described in "Single Camera Export".

To Export Multiple Bookmarks

1. Select the desired Bookmarks in the *Bookmark Log* by using Ctrl+Left-click (to select them one by one) or Shift+Left-click (to select all items in-between your clicks as well).

2. Right-click on any of the selected items and choose **Export Bookmarks**.
3. Use the *Multi-Video* tab of the *Export Video* dialog that opens, as described in "Multi-Video Export".
   - Optionally you can apply filters as described in "Single Camera Export".

Deleting Bookmarks

Bookmarks can be deleted individually from the Timeline, or in multiples from the *Bookmark Log* dialog.

To Delete a Bookmark Using the Timeline

- Hover the mouse cursor over the Bookmark to open its control dialog and click  .
- Right-click on the Bookmark and choose **Remove Bookmark**.

To Delete a Bookmark Using the Bookmark Log

1. Open Main Menu and choose *Bookmark Log* (Ctrl+B).
2. Select the desired Bookmarks (use mouse drag or Ctrl+Click or Shift+Click to select multiple rows), open the context menu, and choose **Remove bookmarks**.

Playing Local Video Files

Nx Witness can browse to find and playback recorded videos within the Desktop Client or on the Welcome Screen without launching a Site

You can play almost any video file on your local drive, with most major codecs and containers supported. You can also use Nx Witness to browse local files from the Welcome Screen without connecting to a Site.

Local files include:

- Files found in designated Nx Witness Media Folders.
- Recently opened local files.
- Exported Files.
- Screen Recordings.
- Screenshots.

The Local Files list updates when a source folder is changed or a file in the folder is removed or added.

To Browse and View Local Files from the Nx Witness Welcome Screen

1. Go to **Main Menu** on the Welcome Screen and select **Browse Local Files**.

2. The Nx Witness interface opens to a blank new layout, with all local files found in the specified media folders listed in the Resource Panel.
3. You can add files, arrange items, add new layouts, and use the Timeline from this screen, but will not be able to save layouts.
4. To toggle back to the Site connection page, go to **Main Menu** and select **Show Welcome Screen**.

To Rename Local Files from the Resource Panel

1. Right-click on a local file to open the context menu.
2. Choose **Rename** (**F2**) to make the name editable.
3. Type the desired file name.
4. Press **Enter**.

5.1 Sound Stream Playback (for Local Files Only)

Video files that have a 5.1 sound stream require a special setting in order to play back on stereo speakers.

1. Go to **Main Menu > Local Settings > Advanced** tab and check **Downmix Audio from 5.1 to 2.1**.
2. Click *Apply* to save changes, OK to save changes and close the dialog, or *Cancel* to discard changes.
3. You will need to restart the Nx Witness client for this change to take effect.

See Timeline Navigation for Local Files.

Timeline Navigation for Local Files

Navigation through local files is very similar to navigation through recorded archive, with the following exceptions:

- Items are not synchronized, therefore **Sync** is always disabled.
- Files are not live, therefore **Live** is always disabled.
- The Timeline does not display colored markers for recorded or motion regions.
- ⏮ and ⏭ buttons jump to the beginning or end of a file.

All other operations (seek, play, pause, fast forward, rewind, etc.) are available. as described in "Parts of the Timeline".

NOTE: If a layout contains both live streams and local files, the Cameras are played back synchronously and local files play back independently.

Configuring Local Media Folders

When Nx Witness starts, it automatically indexes the designated local media folders and displays them under *Local Files* in the Resource Panel.

The default media folders (customizable) are:

- *Windows*
  - `C:\Users\<username>\Videos\Nx Witness Media`
- *Linux*
  - `/home/<username>/Videos/Nx Witness Media`
- *macOS*
  - `/Users/<username>/Movies/Nx Witness Media`

To Add or Remove a Media Folder

1. Open **Main Menu** > **Local Settings** > **General** tab.
2. In *Local Media Folders* section, click **Add** and choose the desired path.
3. To delete a media folder, *select* the folder from the list and click **Remove**.
4. Click *OK* when finished or *Cancel* to discard changes.

To Open Local Files That Are Outside the Media Folders

To view local files that are not shown in the Resource Panel, use one of the following:

- Drag-and-drop a video file(s) or a folder from Windows Explorer to copy it into the Nx Witness Viewing Grid.
- Go to **Main Menu** and select **Open** > **Files** (Ctrl+O) then select the file(s) to be opened.
- Go to **Main Menu** and choose **Open** > **Folder** then select a folder to be opened.
- Right-click anywhere on the VieDewing Grid to open the context menu, select **Open** > **Folder** then choose a folder.

Exporting Video

Files from a single device, Bookmarks, and files from multiple devices that are synchronized for simultaneous playback can be can be exported from Nx Witness. Export is performed in background, so it is possible to continue working with Nx Witness until the export is completed. As soon as export is finished, the video will be available under Local Files in the Resource Panel. Exporting motion-only video ignores all gaps between motion events and stitches the separate motion events together to form seamless playback. If they exist for a camera, Bookmarks are included in exported video.

NOTE: **Exported video will only be available as a Local file until the current session ends!** To make it available permanently, the exported video must be saved to the Nx Witness **Media Folder** (see "Configuring Media Folders"). Alternately, you can create and save a layout that contains the exported video(s). See "Viewing Exported Video" for more information.

Exported video can be protected with a password that will be required to be able to log in and view exported.NOV or.EXE files. Videos can also be exported in read-only mode to prevent modifications to Layout and item settings during playback. This protects the chain of custody and authenticity of exported video during investigations.

If a long time segment is selected for export, the following warning message will appear: *You are about to export a long video. It may require over a gigabyte of HDD space and take several minutes to complete.*

The Following File Formats Are Supported

- *MKV* – Matroska (**.**mkv) is a more advanced format that may not be supported on some devices (ex: home media players). It does not restrict video and audio content. (Single camera only.)
- *AVI* – Audio video interleave (.avi) is more widely used, but the codec remains intact (H264). To view exported videos in other players additional codecs may be required. If a codec is not allowed in the AVI format, a warning message will display. (Single camera only.)
- *MP4* – MPEG-4 Part 14 (.mp4) is another advanced format that may not be played back on some devices (ex: home media players). It does not restrict video and audio content. (Single camera only.)
- *NOV* – A proprietary Nx Witness media file (.NOV) that can only be opened by the Nx Witness Desktop Client.
- *EXE* – A platform dependent executable bundle where the Nx Witness Client application is exported with the video file. Used to distribute videos to users who do not have any codecs or media players installed. Can be opened without Nx Witness installed on the computer, but video will be viewable only on the Windows architecture with which video was produced. When the executable is opened, the Client launches and plays the exported video. These files can be edited once exported. Motion detection and data processing in the recorded segments is retained in the export.

NOTE: Export is only available to users with the appropriate permissions. Export archive permission is required for any export operation. See "Built-In Groups and Permissions" for details.

The Following Options Are Available

- Adding a User Watermark – Adds an overlay of the User login to video to identify the recording source.
- Validating Exports – Indicates if any modifications were performed to the footage being exported.
- Read-only – Multi-video files (.exe and.nov formats) can be exported with a read-only option.
- Password Protected Export – Multi-video files (.exe and.nov formats) can be exported with password protection.

- Other options (timestamp, logo, etc.) may be added to single-camera exports.

Single Camera Export

The following option and export overlays are available for *.mkv*, *.avi*, and *.mp4* export formats:

- Export Settings – Check the Apply Filters box to apply image filters (e.g. rotation, dewarping, image enhancement, etc.) from the source recording to the exported video.
- Add Bookmark Info – Toggle this option Check this box to apply your bookmark description to the exported video, you can change area width and font size. (Only available when Exporting Bookmarks.)
- Add Timestamp – Adds a timestamp in Long (day of week, date, month, and year, hour:minute:seconds and UTC differential) or Short (dd/mm/yyyy hh:mm), ISO8601, or RFC2822 format. Font size is also adjustable.
- Add Image – Browse for an image (typically a logo) to add to the exported video.upper left corner. There are sliders for Opacity and Size.
- Add Text – Adds the text of your choice. You can set the Width of the text field and the Font Size.
- Add Info – Check the Camera name box to add the camera's name. Check the Export date box to add the export session's timestamp. You can set the Font Size.
- Rapid Review – Exports video at a higher playback speed than the original recording (see "Rapid Review Export"). Video must be at least 10 seconds long for this option to be available.

NOTE: You may experience playback issues when exporting a video where the primary and secondary streams have different codecs. In such cases, the video should be exported using transcoding or as a multi-video (nov file/executable). See Multi-Video Export for details.

To Export a Video Segment from a Single Camera

1. Select the desired item in the layout.
2. Use the Timeline to select the desired video segment (see instructions for how to select a time segment in "Timeline").
3. Right-click on the selected time segment to open the context menu and choose **Export Video**.
4. Select the *Single Camera* tab in the **Export Video** dialog.
5. Select a **Folder** where the file will be saved and enter a file **Name.**
6. Select a **file format** from the drop-down menu.
7. When available, you can optionally check **Apply Filters** or select from the export overlays described above.

   NOTES:

a) Overlays are inserted at the upper left corner but can be clicked-and-dragged to any other position.

b) Including filters or overlay options requires transcoding, which will increase CPU usage and export time significantly.

8. Click **Export**. A status dialog will display export progress as a percentage. Clicking **Stop Export** will cancel the operation so that no exported data is saved.

   NOTE: An exported video will only be available as a Local File in the Resource Panel until the client restarts. To make it available there for subsequent sessions, save the exported video to the Nx Witness Media Folder (see "Configuring Media Folders").

Multi-Video Export

With multi-video export it is possible to export video and audio from the archives of several cameras or Bookmarks simultaneously (for instance, the last 10 minutes of recorded video from five different cameras).

NOTE: It is not possible to playback local videos files in a multi-video export. If a layout includes both cameras and local files, the local files will not be shown in the *Export Video* dialog and will not be exported in the resulting file. When the selection contains empty archive on a given camera**,** it will be exported and "no data" will be shown when viewing the exported clip.

The exported files are saved either in a proprietary format that can be played by Nx Witness (.nov), or as an executable bundle that can be viewed on any Windows computer (.exe). The proprietary format has many benefits in comparison to single camera export. The exported multi-video layout can be navigated, manipulated, and searched like any other layout (see "Synchronizing Playback" and "Smart Motion Search").

NOTE: An exported video will only be available as a Local File in the Resource Panel until the client restarts. To make it available permanently, save the exported video to the **Nx Witness Media Folder** (see "Configuring Media Folders").

To Export Multiple Items as One File

1. Open the desired layout.
2. Use the Timeline to select the desired time segment.
3. **Right-click** on the selected time segment to open the context menu and choose **Export Video**.
4. Select the **Multi Video** tab.
5. Optionally, you can check **Make read-only** to prevent the exported video from being edited.
6. Optionally, you can check **Protect with password** to require a password to launch and view the exported file (see "Password Protected Exports" below).
7. Select Network Optix Media file (**.nov*) or Executable Network Optix Media File (x64) (**.exe*) format.
8. Select a **Folder** to export to and enter a file **Name**.

9. Click *Export* or *Cancel*.

Password Protected Exports

Exported file types.EXE and.NOV can be protected with a password, which will be required to open the exported layout. To apply a password, use the **Multi-Video** tab of the **Export Video** dialog and check **Protect with password**. Encrypted layouts are indicated in the Local Files list with a locked icon ().

NOTE: The layout remains unlocked until the User session ends unless you choose the *Forget Password* option in the context menu, which closes the layout so that the password will be required to reopen it.

Rapid Review Export

The *Rapid Review* feature lets you export video at a higher playback speed than the original recording. (Sometimes this is called "timelapse" mode). When you specify either the export playback speed or length of the video, the corresponding value and the *Frames interval* will adjust accordingly.

NOTE: The source video must be at least 10 seconds long for this option to be available.

To Apply Rapid Review Export

1. Select the desired device.
2. Select the time span you want to export and use the Timeline context menu to open the **Export Video** dialog (right-click on the newly selected area highlighted in blue).
3. In the **Single Camera** tab, click on the **Rapid Review** button. (It may be necessary to select a different output format to enable the button.)
4. The Rapid Review panel that opens to the right of the preview will show the **Initial video length** of the selected segment for reference. Set a value for each of the following:
   - *Exported video length* – Enter a desired duration in seconds, where the shorter the exported video, the faster the playback speed will be.
   - *Speed* – Use the slider to set the speed increase from **10x** to the maximum available value. (The maximum speed multiplier depends on the initial video length.)

   NOTE: The *Exported video length* and *Speed* values are related. The faster the playback speed and the higher the frame interval, the longer the video will be. Smaller video files are created with a slower speed and a lower frame interval.

Viewing Exported Video

As soon as export is finished, the extracted video clip(s) will be available under Local Files on the Resource Panel.

- AVI, MKV and MP4 files are shown as a single record.

- EXE and NOV files are contained in a folder and will display in a new tab.
- Single camera and Bookmark exports are displayed as a single item.

When an exported Multi-Video is opened, it behaves like a standard layout and normal actions (arranging items, smart motion search, exporting video) can be applied.

Adding a User Watermark

To deter unauthorized or unwanted distribution of video recordings, it is possible to add a watermark to video playback. The watermark consists of the User login as a semi-transparent overlay repeated across the entire image. When enabled, only users with administrator or power user permissions can export video without the watermark.

To Enable Watermark on Exported Video

1. Open **Site Administration**.
2. In the **Security** tab, enable the **Display watermark with username over video** checkbox.
3. Click on the **Watermark Preview** button to adjust the opacity (0 – 100%) and the number of times the username is overlayed (1x1 array – 6x10 array) on the image.
4. Click *OK* to accept or *Cancel*.

NOTE: Video still can be exported without a watermark via the Web Admin, for example. However, the Audit Trail of User Actions can be used to trace the recording event and the responsible user.

Validating Exports

Export validation let you determine whether video exported from Nx Witness been modified since being exported. An internal watermark is checked to verify the file is intact.

NOTE:Attempting to check the validity of a local file that was not exported will result in the watermark "not found".

To Check the Watermark on an Exported Video

1. Open the desired video in layout.
2. Open the item's context menu and select **Check File Watermark** (**Alt**+**C**).
3. A progress dialog will display during the validation. If the file is in its original state, the check will succeed (Watermark Matched):

4. If any modifications took place, the check will fail (Invalid Watermark):

Audio in Nx Witness

Nx Witness provides support for multiple audio devices with audio related controls available at the resource level and both the user and group-level permissions.

Properly configured audio can help users to have a better understanding of what is happening at the scene. In cases where a loudspeaker is present, Using 2-Way Audio enables the option to communicate with resources on site and many analytical solutions include sound detection as a method to trigger an event (seeEvent Rules).

Key Concepts:

- Individual devices can have audio support enabled or disabled (See Configuring Audio on a Device).
- Audio from audio-enabled devices is captured to the archive when recording is enabled for the device.

- Audio will play in live views and from the archive when the user has the **Play Audio** permission (see Permissions Management).
- There can be multiple volume controls (client, workstation, remote connection services) present in a Site (see Adjusting Volume).
- The Desktop Client can simultaneously play audio from all devices open in a layout when Play audio from all cameras on layout is selected in Local Settings.

  NOTE: After enabling audio from all devices in a layout, individually mute devices until only the desired audio streams are active.

Audio-Video Synchronization:

The performance of audio-video synchronization by timestamp relies on:

- To provide what is considered lip-synced audio, Network Optix synchronizes audio and video streams using the same timestamp for both, as received from the device.
- Accurate synchronization timing in the RTSP stream of the devices.
- Available network bandwidth between devices, servers, and clients.
- Sufficient resources are available in the server-client environment.

Supported Audio Codecs:

- *AAC* – Advanced Audio Coding is an audio coding standard for lossy digital audio compression.
- *G.711 (u-Law/A-law)* – an ITU-T PCM speech coding standard providing toll-quality voice compression.
- *G.726* – an ITU-T ADPCM speech coding standard with half the bitrate of G.711.
- *MPEG Audio (MP1, MP2, and MP3)* – an audio coding standard for lossy digital audio compression.

Adjusting Volume

Global volume controls:

The playback panel of the Desktop Client includes a single volume control that applies to all audio sources on layout, scene, and the Speak, Play Sound, and Repeat Sound Site actions that are part of the Event Rules.

To adjust playback volume, use one of the following:

- Click-and-drag the **Volume Slider** to the right of the Timeline.
- Click on the Volume Slide and then adjust with the **Mouse Wheel**.
- Use **Ctrl**+**Up** or **Ctrl**+**Down** volume Keyboard Shortcuts.

NOTE: Click the speaker icon or the Keyboard Shortcut: **U** to toggle the Site-wide mute function.

Muting an active device:

Individual devices will display a mute icon along the top panel buttons when the following Site conditions are set:

- The resource type is a Camera, Virtual Camera, or Input/Output device.
- The resources has all device specific audio services enabled.
- The current user has "Play Audio" permissions to the resource.
- Site Local Settings are configured to "Play audio from all cameras on layout".
- Mute configuration retention:
  - The state of the device-mute control is retained regardless of the global volume mute control.
  - The mute state is saved per layout instance on the grid.
    - If resource 1 on layout A is muted, and resource 1 is opened again (new instance) on layout A or another layout, then the default state (not muted) is set for the new instance.
    - If layout A is closed, and then opened once again, the first added instance of resource 1 will be muted while all additional instances will have the default state of not muted.
    - Device (mute) state is saved per Desktop Client instance. If the same user opens the same Site from from a Desktop Client running on a different workstation, and then opens layout A, both instances of resource 1 will have the default mute state of not muted.
    - The device mute state is saved with the user data such that when another user connects to the same Site from the same Desktop Client, and opens Layout A, both instances of resource 1 will have the default mote state of not muted.

Using 2-Way Audio

Two-way audio (transmitting audio to a camera or I/O device from the Nx Witness client) is possible if you have a microphone connected the workstation running the Desktop Client. Currently this feature is supported on the following devices:

- ONVIF compliant devices.
- Axis cameras with firmware 5.x or higher.
- Sony SNC-CX600.
- The entire Digital Watchdog camera line.
- The entire Hanwha camera line.

If a device supports 2-way audio, you will see a blue microphone button when the device is open in layout, as shown below.

To Manually Transmit Audio to a Device

- Press and hold the microphone icon while speaking. You can use the spectrum analyzer to check the level while the button is depressed. Release the button to end the transmission.
- You can also configure an event rule or soft trigger to play sound or speak text on a device; see the Play Sound, Repeat Sound, and Speak topics for more details.

  NOTE: Error will appear when attempting to manually transmit audio with incorrect audio input parameters.

To Configure 2-way Audio

1. Right-click the camera **> Camera Settings > General** tab.
2. Check the *Enable 2-way audio* checkbox and choose between the two options:
   - *Use this camera for audio output* – Use the current camera for audio output.
   - *Transmit audio stream to another camera* – Select a camera or device to use for audio output instead of the current camera.
3. **Apply** changes.

Taking Screenshots

Nx Witness has a built-in *Screenshot* feature that simplifies still image capture of streaming device and local video files to PNG or JPG output formats. If image enhancement and/or Dewarping Controls were applied to the source, they will be retained in the Screenshot. Screenshot settings are retain as the default for the next screenshot.

To Take a Screenshot from a Video

1. Select an item in a **Layout**.
2. Move to the desired position in the **Timeline** (see "Parts of the Timeline").
3. Click the **Screenshot** button .
4. In the **Save As** dialog that opens:
   a. Chose a directory location

b. Enter a **File name** or use the default file name (i.e. the device name appended with a timestamp).
c. Select one of the file types from the drop-down menu: *JPEG* or *PNG*.
d. To include the playback time, select a timestamp location from the drop-down menu or select *No Timestamp*.
e. To include the camera's name, select a camera name location from the drop-down menu or select *No camera name*.
f. Click **Save**.

Tours

If several Items are open in the Viewing Grid, you can create a *Tour* that loops through Fullscreen display of each item like a slide show.

To start a tour, open the Viewing Grid context menu and select **Start Tour** (**Alt**+**T**). To stop a tour, press **Escape** or double-click the mouse.

To Set Item Display Length in a Tour

1. Open **Main Menu** and select **Local Settings**.
2. In the **Look and Feel** tab, use **Tour Cycle** to specify the desired duration (in seconds).

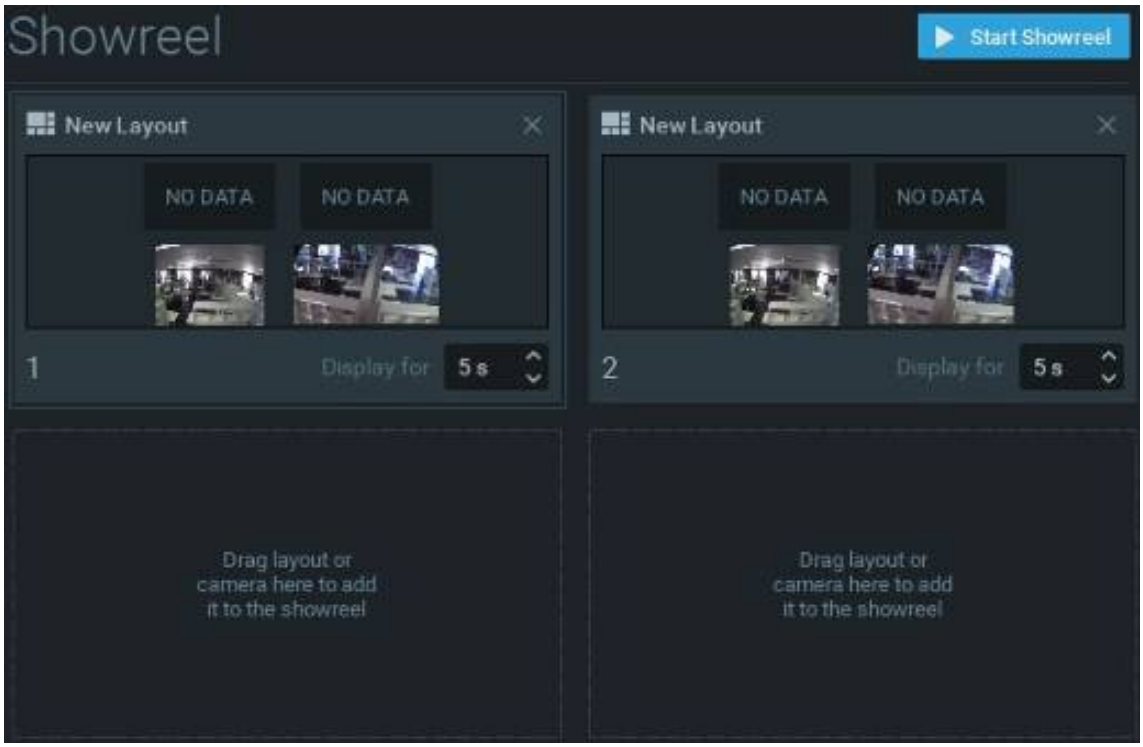
   It is also possible to cycle through layout tabs – see "Showreel (Tour Cycle)".

Showreels (Tour Cycle)

In addition to Tours, which cycle in Fullscreen mode through open items in a single layout, you can create a *Showreel* that cycles in Fullscreen mode through several entire layouts.

To Configure a Showreel

1. Open Main Menu and select **Add > Showreel**.



2. Drag any of the following resources into the Showreel cells:
   - Layout(s) from Resource Panel (Cross-Site Layouts cannot be used)
   - Individual Resources (Cameras, Local Files, other Devices, Web Pages) from Resource Panel
   - Servers (monitoring item will be displayed) from Resource Panel
   - External video files, or folders containing video files – right-click in an empty cell to open the Showreel context menu and choose **Open** > **Files** or **Open** > **Folder.**
3. Click-and-drag cells to set the display order by repositioning them in the layout. (Showreel order is left to right, top to bottom.) Click the **X** in the upper right corner to remove a cell.
4. Use the scrolling *Display for* field to set the display time, in seconds (1 to 99), for each cell.
5. If you do not want the Showreel to cycle automatically, open the context menu and check **Settings** > **Switch with Hotkeys**. Once the Showreel is started, it can be cycled manually using the right arrow key to go forward and the left arrow key to go backwards. For automatic continuous cycling, check **Settings** > **Switch on timer**.
6. Showreels are displayed in the Resource Panel and can be opened, deleted, renamed or started using their Resource Panel context menu.

To Display a Showreel

1. To start a Showreel, click the **Start Showreel** button in the upper-right corner of the showreel layout, or open the Showreel context menu from the Resource Panel and choose **Start Showreel** (shortcut **Alt+T**). To stop a Showreel, press **ESC**.

2. Once a Showreel is running, whether automatically or manually, you can use the right and left arrow keys to move through the cycle.

Screen Recording

Desktop Clients running on the Microsoft Windows operating system can use HD Witness to record screen content to a file that may include audio, depending on Site, Server, and device configuration.

Screen recordings can be saved in the following formats:

- *MPEG4 Part 2 (Video)*
- *MP3 LAME Audio Codec (Stereo Audio)*
- *AVI (Container)*

NOTE: Screen Recording is a CPU intense task. If you experience issues, try to change the capture resolution and quality.

Setting up Screen Recording

1. Open **Main Menu** and choose **Local Settings**.
2. Go to the *Screen Recording* tab to configure parameters:
   - *Temporary Folder* – The folder that stores temporary files. FIles are stored during recording, then are copied to a specified folder to be saved.

   NOTE: This folder must be accessible and writable.
   - *Screen* – If several monitors are installed, choose the desired one.
   - *Resolution* – Select screen resolution. The lower the resolution, the higher the performance.
   - *Recording Quality* – Select *Performance* for best performance. Select *Best* for best quality. Select *Average* to balance performance and quality.
   - *Capture Cursor* – Select this checkbox to include the mouse cursor during recording.
4. Click *OK* when done or *Cancel* to discard changes.

To Select an Audio Source

1. Go to the *General* tab in **Local Settings**.
2. Select **First Source** and **Second Source**. Audio will be mixed from both devices. The best practice is to select the sound card as primary and a microphone as secondary source. In this case, both sounds from Nx Witness (i.e. video clips) and microphone will be recorded simultaneously.

To Configure an Audio Source

1. Set up audio input card parameters in Windows and ensure the selected source is the default input device.
2. Test recording using the Windows Recorder or any other sound recording application.

Performing Screen Recording

1. To record the entire client screen, open Main Menu and select Start Screen Recording (Alt+R).
2. Screen recording will begin in 3 seconds.

   NOTE: See Setting up Screen Recording for instructions on setting up and testing an audio device.
3. To stop recording, open Main Menu and select Stop Screen Recording (Alt+R).
4. Choose the desired file name and location and click *Save* (*Cancel* will close the dialog and data will not be saved). File and folder operations are performed in the same manner as in Windows Explorer. As soon as the file is saved, it will be available in local files.

   NOTE: The screen recording will only be available as a Local File until the client restarts. To make the screen recording available during subsequent sessions, save the recorded video to **Nx Witness Media Folder** or create and save a layout containing the video.

Contacting Support

Some issues can be resolved without support, such as

- A camera that is not working properly can be diagnosed (see "Diagnosing Offline Devices"), and
- An archive that is lost can be restored (see "Reindexing and Fast-Scanning Archives").

NOTE: This section and the following sub-sections apply only to Site Administrators:

Collecting Basic Information

Collecting Logs

Providing Remote Access

Sending Anonymous Usage and Crash Statistics.

When posting an issue to support, describe the problem in as much detail as possible. At a minimum, please provide the version, hardware, and environmental properties of the Site as found in the About screen (see "Collecting Basic Information"). Support may request additional information such as log files, network configuration, etc. (see "Collecting Logs" and "Viewing and Exporting the Event Log"), or ask that you provide Administrator login credentials.

For a more in-depth look at the state your Site is in, see "Health Monitoring". Health Monitoring will display Site performance and error information. It will be helpful to include some of the information on that page when submitting a support request.

To expedite investigation, it may be useful to provide remote access. If it is not possible to provide remote access for security reasons, or if an issue is difficult to replicate, a supporting video clip can help the support team understand and investigate the issue. Use the screen recording function to create a video clip, and attach the video to your support ticket.

If the issue is related to compatibility of a specific device, the support team might provide a specific build that can solve the particular issue. See "Updating Nx Witness" for more information.

Collecting Basic Information

To display product version, hardware, and driver information, go to **Main Menu** and select **About** (**F1**).

The *About Nx Witness* dialog will display:

- Version and platform information.
- A list of external libraries used.
- Graphical Processing Unit (GPU) information.
- Site Servers.
- Nx Witness components and driver versions.
- Customer Support contact information.

This data is required by the support team and should be provided in your support ticket in addition to other pertinent details. (Similar information can be acquired with standard Windows tools such as **ipconfig**, but *About Nx Witness* is more direct and specific to the product).

Collecting Logs

Log files track the internal actions performed by Nx Witness components. They are crucial part in the process to help developers to deeply understand the problem and causes.

The following logs may be requested as part of a support ticket:

- Site Logs.
- Client Logs.
- Update Logs.

NOTE: Desktop Client logs are disabled by default.

To manage log files:

- all: **Main Menu -> Site Administration** > **Advanced** > **Logs Management.**

- Client only: **Main Menu -> Local Settings** > **Advanced** > **Logs Management** (does not require to be logged into a Site).

Before downloading log files, it is necessary to understand Log Level – the amount of information that the Site components record to the log files.

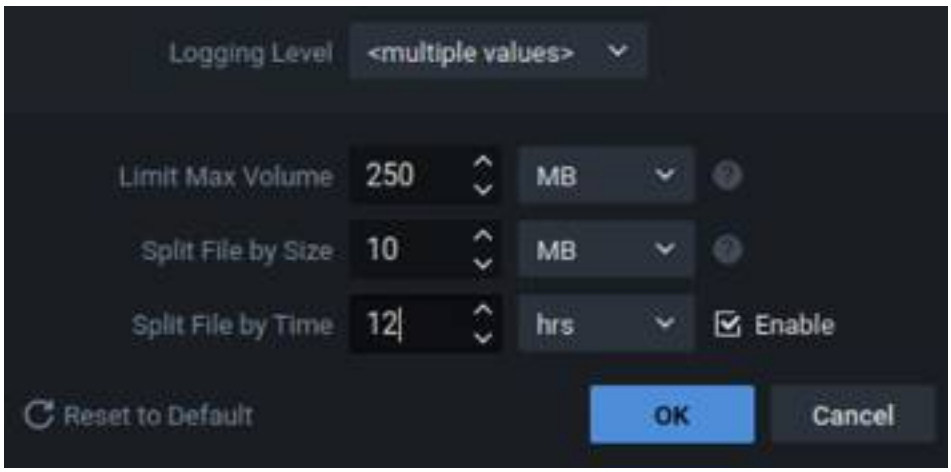
Each component has the following log levels:

- **NONE** – no log files are written (default for Desktop Client).
- **ERROR** – only errors and critical failures are written.
- **WARNING** – warnings (predefined messages from developers), errors, critical failures.
- **INFO** – same as **WARNING** plus informational messages predefined by developers (default log level for Servers).
- **DEBUG** – same as **INFO** plus auto generated messages about the actions performed by the application (recommended when reporting an issue).
- **VERBOSE** – same as **DEBUG but records** full track of everything that the application does (very big amount of data). Slows down the application so definitely not recommended for a long-term run. Might be requested by developers. In this case switch to this log level, collect the log files once the issue is reproduced and switch back immediately after.

Log level and additional parameters can be configured in **Logs Management -> Settings:**

- for Client and Server: select the components that you want to configure (It is not possible to configure logs on offline servers) and click **Settings.**
- for Client only: Click **Settings** in **Local Settings** > **Advanced** > **Logs Management**.

The following settings can be configured:



- **Logging Level** – explained above
- **Limit Max Volume** – the maximum total size of the log files. Once the size hits the limit, the oldest records will be erased.

- **Split File by Size** – size of the single log file. Once the size hits the limit, the new file will be created until the **Max Volume** limit is reached by all log files.
- **Split File by Time** – if enabled, the new file will be created once in a specified period of time (12 hours at the example above) until the **Max Volume** limit is reached by all log files.
- **Reset to Defaults** – to revert settings to the original ones.

The changes will be applied once you click **OK**.

To view Server Logs view in browser, right-click on the desired Server in Resource Panel and choose **Server Logs** from the context menu. The log will open in a web browser.

To Obtain Server and/or Client Logs

1. Open **Logs Management**.
2. Select the components that you want to download log files for.
3. Click **Download**.
4. Choose the folder which will be used to save log files.

To Obtain Client Logs (alternative way)

1. Open **Logs Management**.
2. Click Download.
3. Choose the folder which will be used to save log files.

Log files are downloaded as zip archives with the following names:

- **`client_<date> - <time>.zip`** – client logs
- **`<server_name> - <server_guid> - <date> - <time>.zip`** – Server logs (for each Server in the Site)

Server logs archive contains the following:

- **`system_XXX.log`** – System events (licenses related events Server start/stop, critical issues).
- **`main_XXX.log`** – Server events (everything else).

Providing Remote Access

Nx Witness servers supports simple remote access services that do not require port forwarding, or the Desktop Client will provide port forwarding when the Remote Access Tool is enabled.

Remote Access Key Concepts:

- User accounts configured for Digest Authentication are not allowed to make remote access connections.
- Only Site administrators can change the remote access settings.
- All remote access connections are logged in the Audit Trail of User Actions.

- A remote access service must be installed on the same machine as the server to be shared.
- The Remote Access Tool enables port forwarding for the Desktop Client and may not be required for all remote access solutions.

Supported Remote Access Services:

The following remote access services have been tested and many others will likely work without issue:

- Team Viewer.
- NoMachine.
- SSH Protocol (openSSH).
- VNC – RealVNC, TightVNC, or UltraVNC.
- RDP – Windows Remote Desktop (Requires Public IP).

Remote Access Requisites:

- The connecting user must be a member of the Site Administrators permissions group, or a member of the Power User group when remote access is granted to power users.
- The **Remote Access Tool** must be enabled (default) for the Desktop Client to provide port forwarding.
- The server that will receive the remote connection request must be active and online.
- A remote access configuration files must be present in the server's available resources.
- The remote access client must have a network path to the Media Server.
  Router, Gateway, and other network settings are not covered in the Nx Witness user manual.

Create a Remote Access Configuration File:

Follow these steps to create a remote access configuration file on the server to be accessed or shared.

1. Create a file called **`port_forwarding.json`** in the following location per the operating system in use:
   a. Windows: **`C:\Windows\System32\config\systemprofile\AppData\Local\Network Optix\Network Optix Media Server`**
   b. Linux: **`computer/opt/Network Optix/mediaserver/var`**
2. The port_forwarding.json file must contain the following structure

```
[
    {
        "name": "RDP",
        "port": 3389,
        "login": "admin",
        "password": "123"
    },
    {
```

```
            "name": "SSH",
            "port": 22,
            "login": "root",
            "password": "456"
        }
    ]
```

3. The `port_forwarding.json` file uses the following parameters:

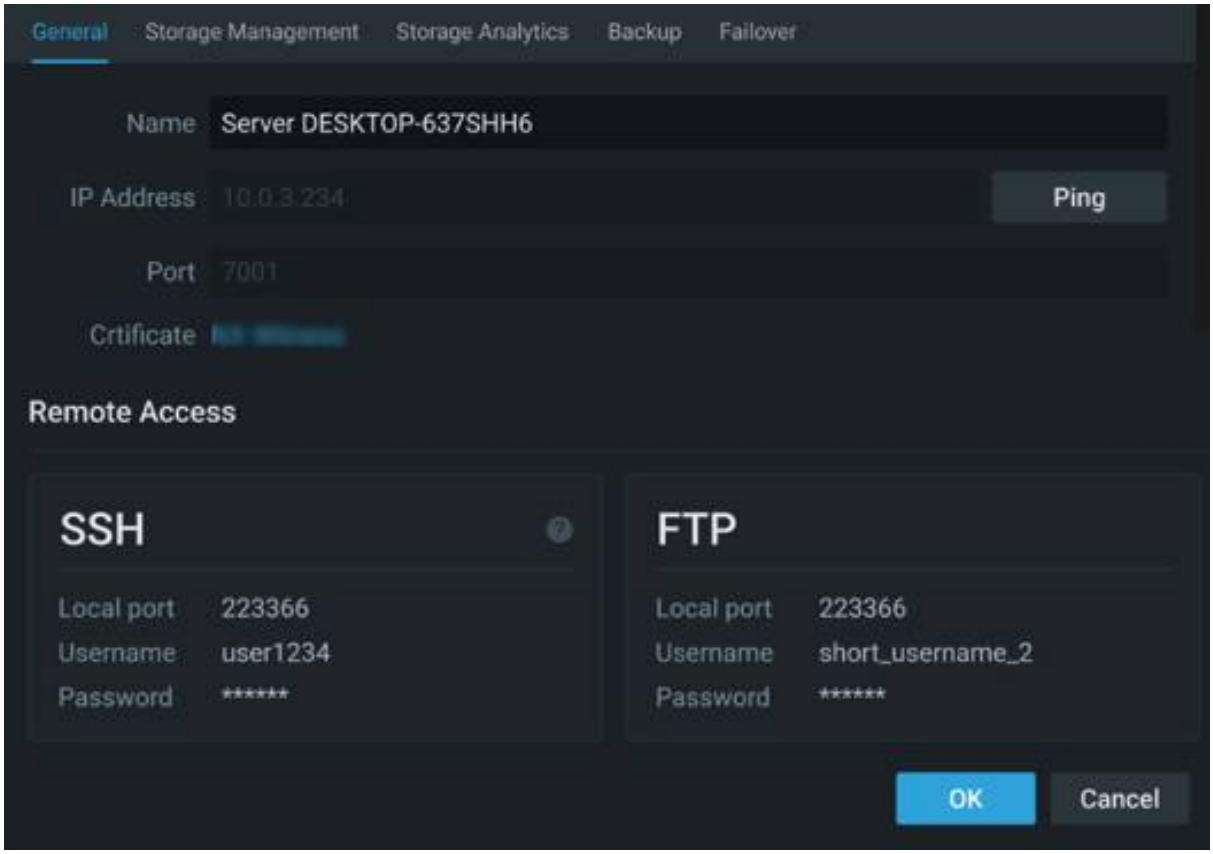
Parameter Name	Required or Optional	Description
`name`	Optional	Name will be displayed in the Desktop Client within the **Server Settings -> General** tab.
`port`	Optional	The port of the remote access service – some remote access services do not require this parameter and it is only used for port forwarding by the Desktop Client.
`login`	Optional	Login for the remote access user (add to the port_forwarding.json file for convenience) – can also be entered at the time of remote access connection.
`password`	Optional	Password for the remote access user (add to the port_forwarding.json file for convenience) – can also be entered at the time of remote access connection.

NOTES:

1. The login and password are for the machine providing the remote connection and not the login and password of server being shared. Credentials must be entered to complete the connection, these can be entered when establishing a remote connection or optionally placed in the configuration file so end-users can copy the login and password from the **Server Settings -> General** dialog.
2. The availability of the remote access feature and the path for the port_forwarding.json file will vary depending on the Edge server and is specific to each vendor. Refer to vendor documentation or support services for additional guidance.

Establishing a Remote Access Connection:

1. Open the **Main Menu -> Site Administration -> Security** dialog.
2. Ensure the **Remote Access Tool** switch is set to enabled.
3. Close the **Site Administration -> Security** dialog.
4. Select a server in the resource panel using the context menu (right click).
5. Open the **server settings** dialog from the menu and select the **general** tab.
6. The Desktop Client will display tiles with the remote connection parameters.
7. Use the port, login (username) and password to establish remote connection using chosen remote access service.
8. Close the Remote Connection when all remote tasks are complete.



Sending Anonymous Usage and Crash Statistics

Nx Witness helps developers and support enhance the product by sending the following information anonymously:

- Events rules with details on all settings.
- Cameras with details for the vendor, model, firmware, max FPS, PTZ capabilities, etc.
- Information about saved layouts and the cameras they contain.
- License information – key, license type, camera count, expiration, etc.
- Media Server software information:
  - Version.
  - Failover with max cameras.
  - Status.
  - SystemID.
  - User access rights.
- Features usage:
  - Button clicks for each camera widget button.
  - Button clicks for each timeline button (sync, calendar, play/pause, etc).
  - Count of dialogs opened (per dialog) and opened tabs count.

  - Preview search time and count.
  - Percentage of time when the window is in fullscreen mode.
  - Motion search time and count.
  - Percentage of time when the window is active.
- Total session time.
- Internet network usage.
- Client hardware information:
  - "openGLRenderer" (ex. GeForce GT 730/PCIe/SSE2)
  - "OpenGL vendor" (ex. NVIDIA Corporation)
  - "OpenGL version" (ex. 4.4.0 NVIDIA 331.113)

Statistics reports are sent once a month. This feature is enabled by default.

To Disable Statistics Reports

It is possible to do this during the Initial Site Configuration. To do this later:

1. Open the **Main Menu->Site Administration** dialog and select the *General* tab.
2. Clear the *Send anonymous usage and crash statistics to software developers* checkbox and click **OK**.

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