VuWall2

Video Wall Control Software - 2.10.4

Video Management Systems Integration

Oct 2019

www.vuwall.com

Simplicity in AV networks & video wall management

Table of Contents

Configure Genetec Security Center for VuWall2 Integration

"Security Center is a unified platform that blends IP video surveillance, access control, and license plate recognition systems within one intuitive solution. Simplify your operations, achieve greater situational awareness, and take advantage of a highly flexible and secure platform that evolves with your organization."

- Extract from Genetec Security Center brochure.

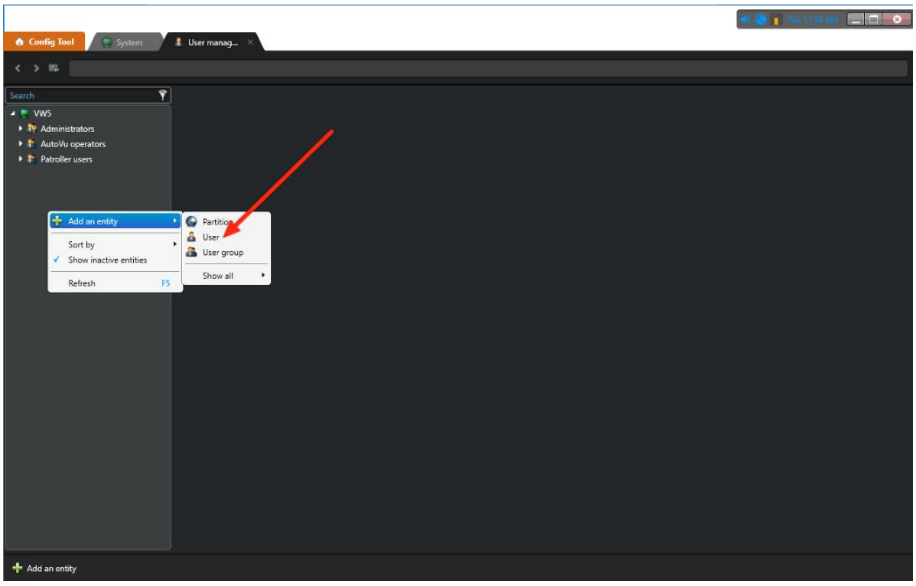
VuWall2 can integrate cameras managed by Security Center. These cameras will appear as IP device sources available to be simultaneously mixed with other types of content that VuWall2 supports.

Requirements

- Access to a Genetec Security Center server version 5.4 or above
- Genetec Security Center server option part no. GSC-1SDK-VuWall-VuWall2
- Genetec Security Desk 5.4 or above on a workstation for configuration
- Genetec Security Center administrator class user, able to create entities
- VuWall2 Server 2.9 Pro or above
- VuWall2 Client installed on a workstation computer for configuration

Note: Genetec Security Desk & VuWall2 Client can co-exist on the same workstation.

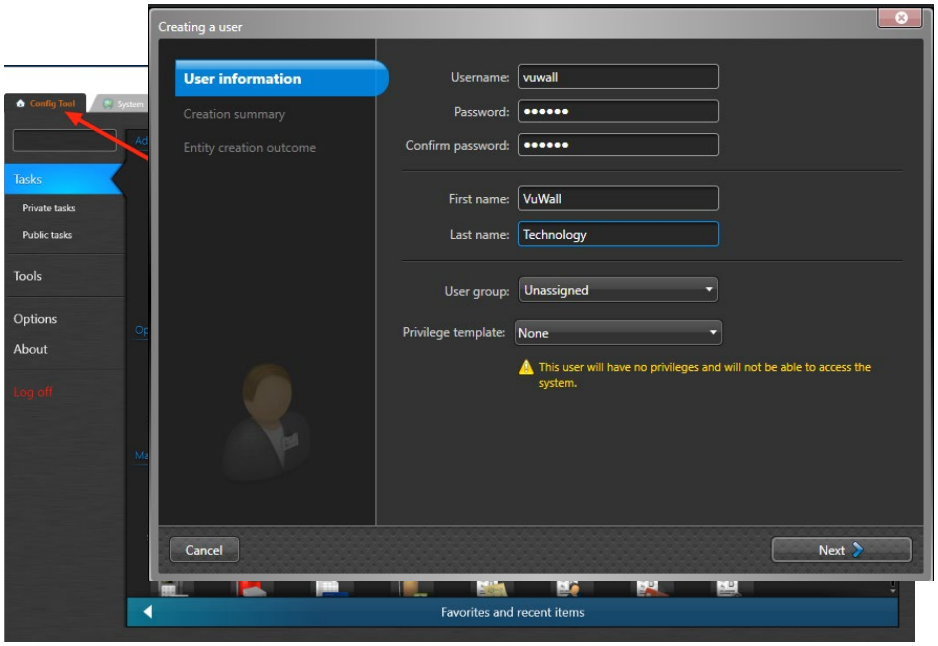
Create a user account in Security Center



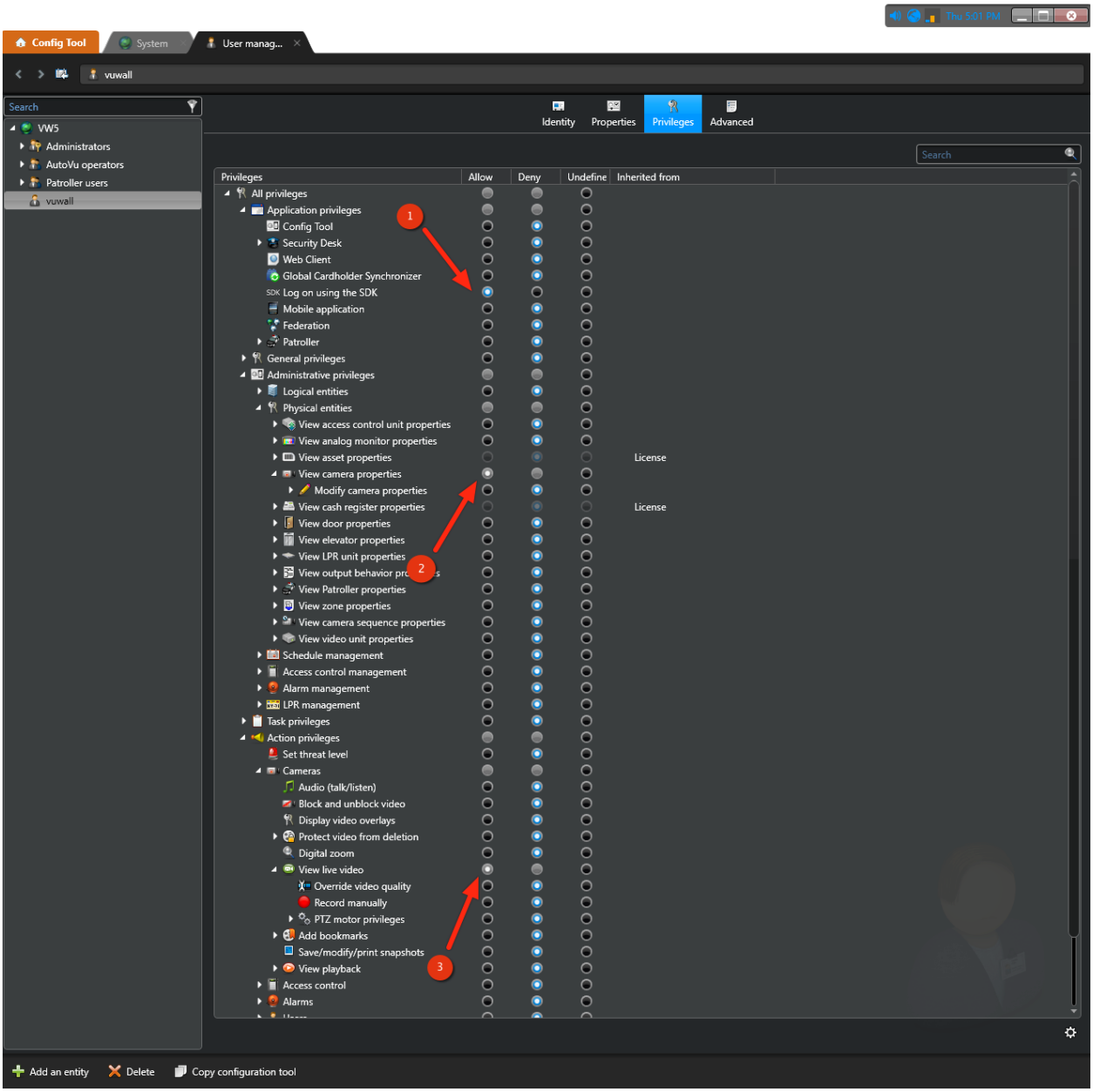
We recommend creating a dedicated user for VuWall2 integration in Security Center. Launch "Genetec Config Tool", click on the "Config Tool" tab and click on "User Management" icon.

Put your mouse cursor anywhere in the left column, right-click to **"Add an entity"**, and select **"User"**.

Fill-in the user credentials and click **"Next".**



Click on **“Next”**, then on the **“Creation Summary”** step click on **“Create”**. On the **“Entity Creation Outcome”** step, click on **“Close”**. Then the following screen will appear:

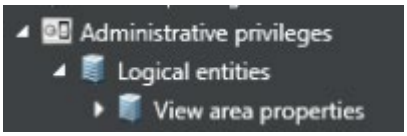


For our new user to view the camera(s), a strict minimum of **3 privileges** is required.

1. “Log on using the SDK”
2. “View Cameras properties”
3. “View live video”

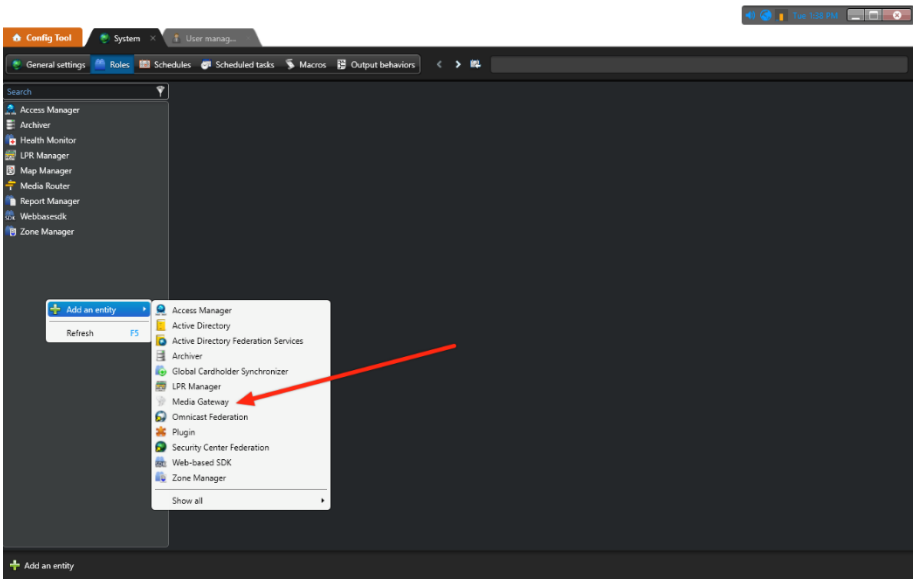
Once completed click on **“Apply”** (bottom right corner) to set the privileges.

Note: In order for users to see the same set of folder structures used in Genetec in the VuWall2 interface an additional permission: **"Administrative privileges > Logical entities > View area properties"** must be set to **"Allow"**



Create the RTSP Gateway entity

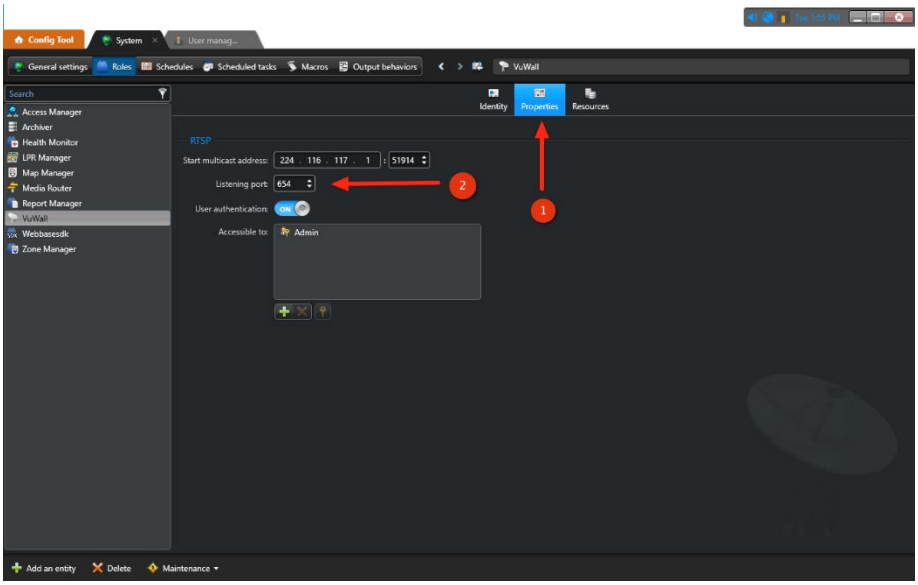
Now, click on the **"System"** tab, anywhere in the left column, right click and select **"Add Entity"**, then select **"Media Gateway"**.



On **"Basic Information"**, enter something meaningful to identify this entity and click on **"Next"**.

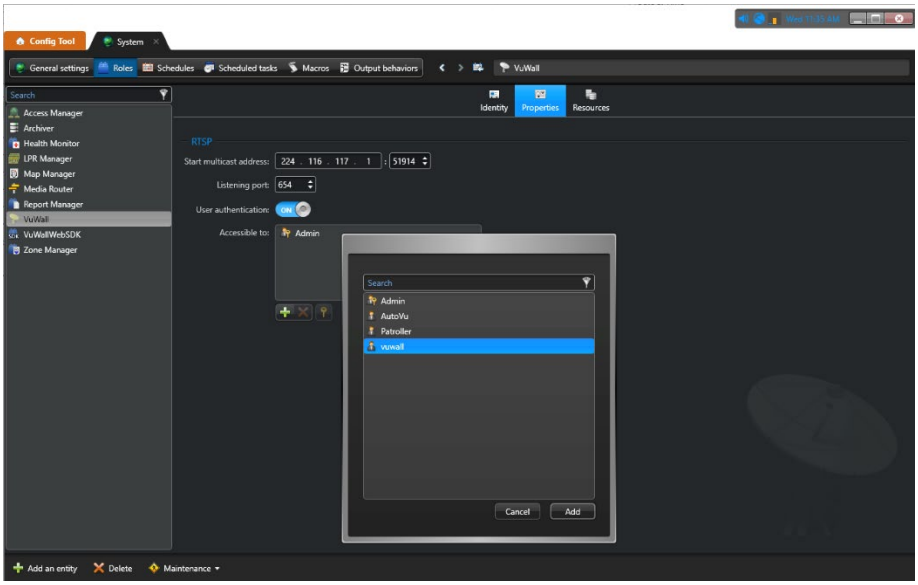
On **"Creation Summary"** click on **"Create"**. On **"Entity Creation Outcome"** click on **"Close"**.

Select the entity you just created and click on its ❶ **“Properties”**, and take note of the ❷ **“Listening Port”**



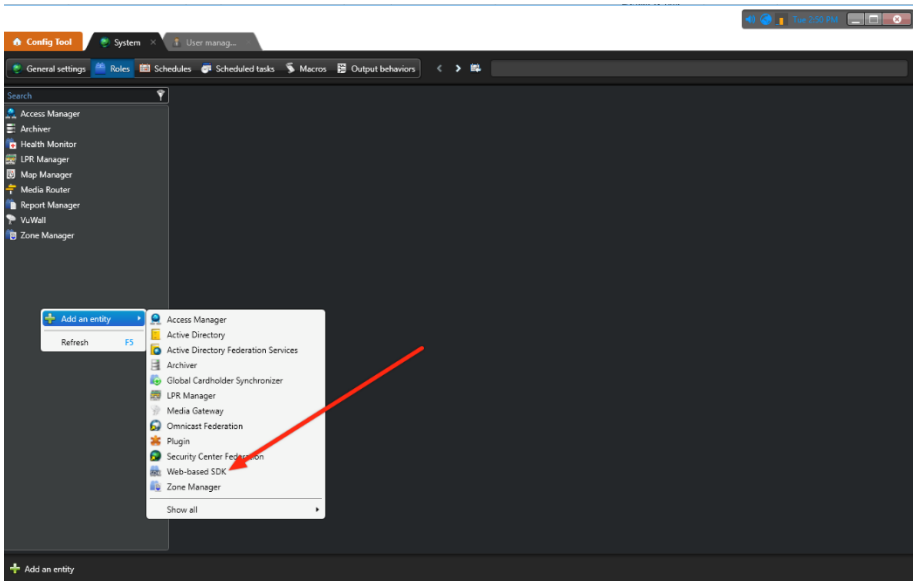
Give your user access to the gateway

While still accessing the properties of the gateway, in the **"Accessible to"** box, click the plus sign below, select the user you have previously created and click on **"Add"**.

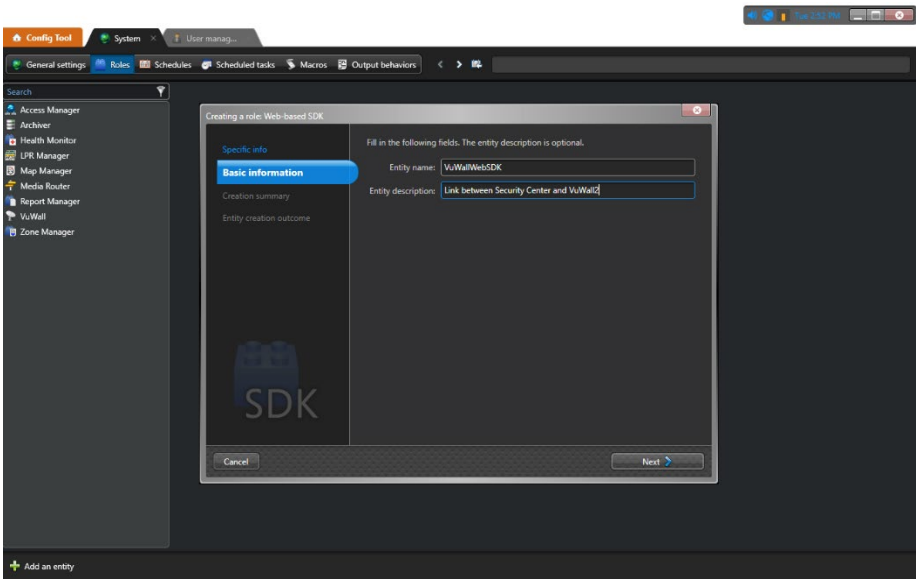


Create the WEB SDK entity

Still under the **"System"** tab, place your mouse cursor on the left column and right click, then select **"Web-Based SDK"**.

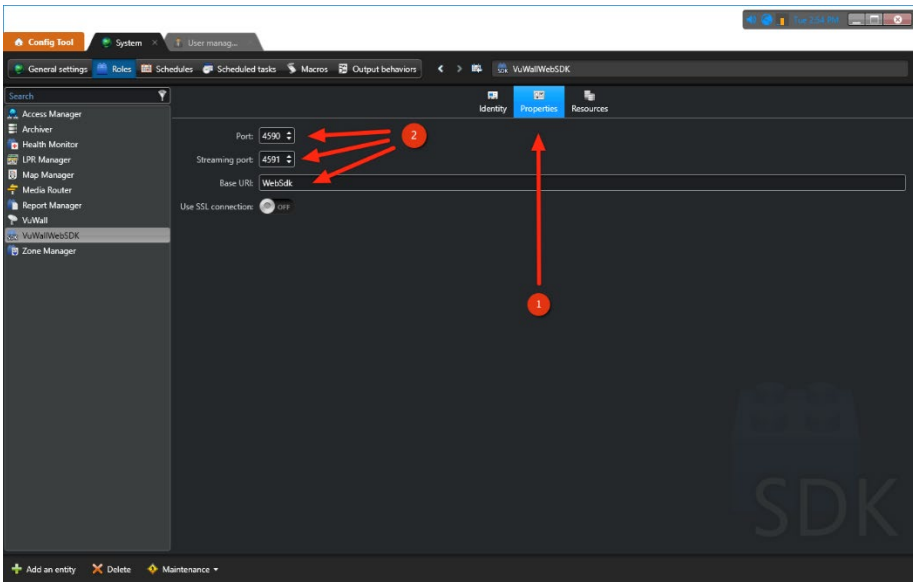


Enter a meaningful **"Entity Name"** and **"Entity Description"** in **"Basic Information"** and click **"Next"**.



On **"Creation Summary"** click on **"Create"**. On **"Entity Creation Outcome"** click on **"Close"**.

Select the entity you just created and click on its ❶ **“Properties”**, ❷ take note of the **“Port”, “Streaming Ports”** numbers and **“Base URI”** name.



NOTE: You may change the name of the “Base URI” if need be.

Configure ISS SecurOS for VuWall2 Integration

"SecurOS™ is the nucleus of a complete security Eco-System. It provides an integration platform, which ties together video, ISS native video analytics, and third-party systems such as access control, fire alarm, and building management. The SecurOS system is suited for large mission critical applications that involve hundreds or thousands of security devices unified into ONE platform."

- Extract from ISS SecurOS brochure.

VuWall2 can integrate cameras managed by ISS SecurOS. These cameras will appear as IP device sources available to be simultaneously mixed with other types of content that VuWall2 supports.

Requirements

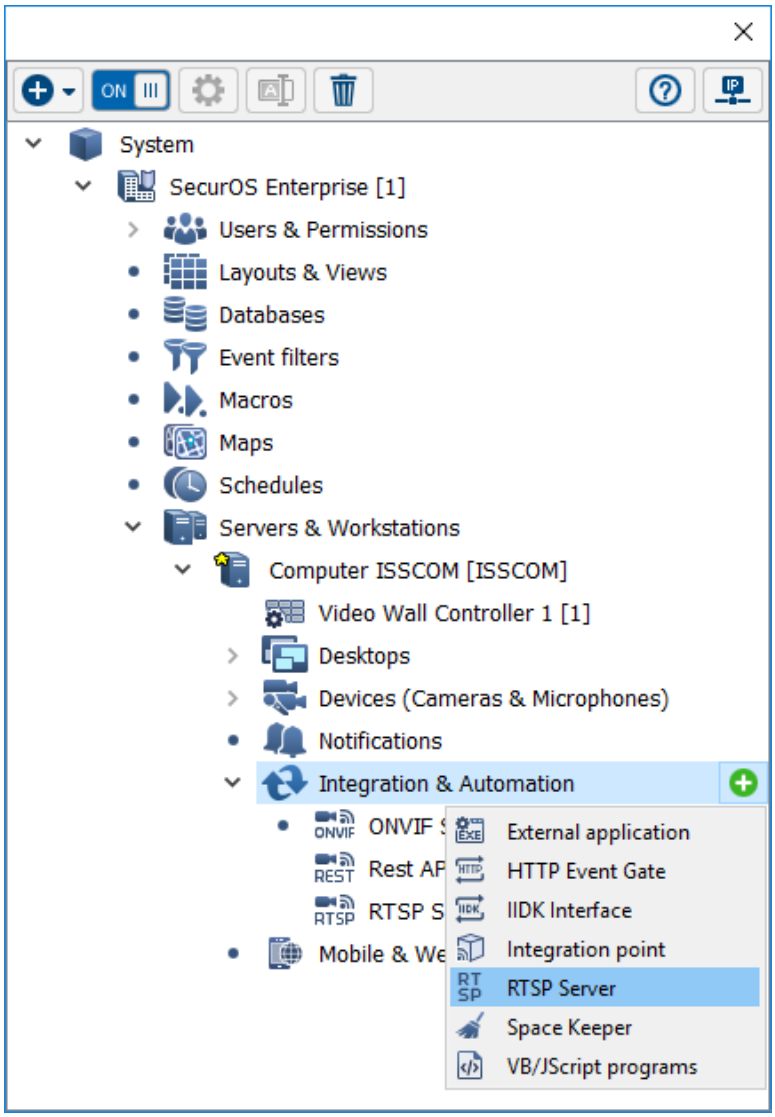
- Access to an ISS SecurOS server version 10.0 or above
- SecurOS Client version 10.0 or above on a workstation for configuration
- SecurOS administrator class user, able to create entities
- VuWall2 Server 2.12 Pro or above
- VuWall2 Client installed on a workstation computer for configuration

Note: ISS SecurOS & VuWall2 Client can co-exist on the same workstation.

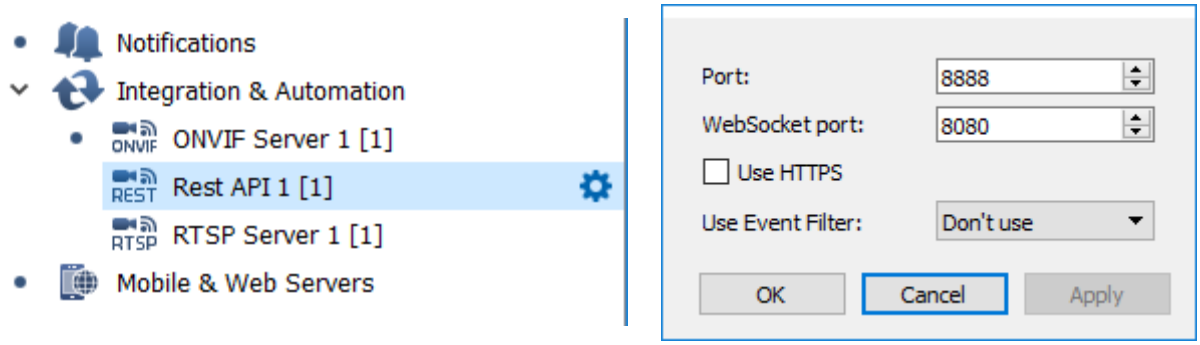
Create the Integration and Automation Entities

First, within the SecurOS Client interface, navigate to the Configuration panel in the top right-corner. Expand the headers until you reach the "**Integration & Automation**" section associated to the SecurOS Server that will communicate with VuWall2. Click that header to highlight it, then select the green **"+"** icon to create the relevant entities. VuWall2 requires the following components:

- "**Rest API**" to retrieve the list of available cameras and their metadata
- "**RTSP Server**" to access the video stream and display on the video wall

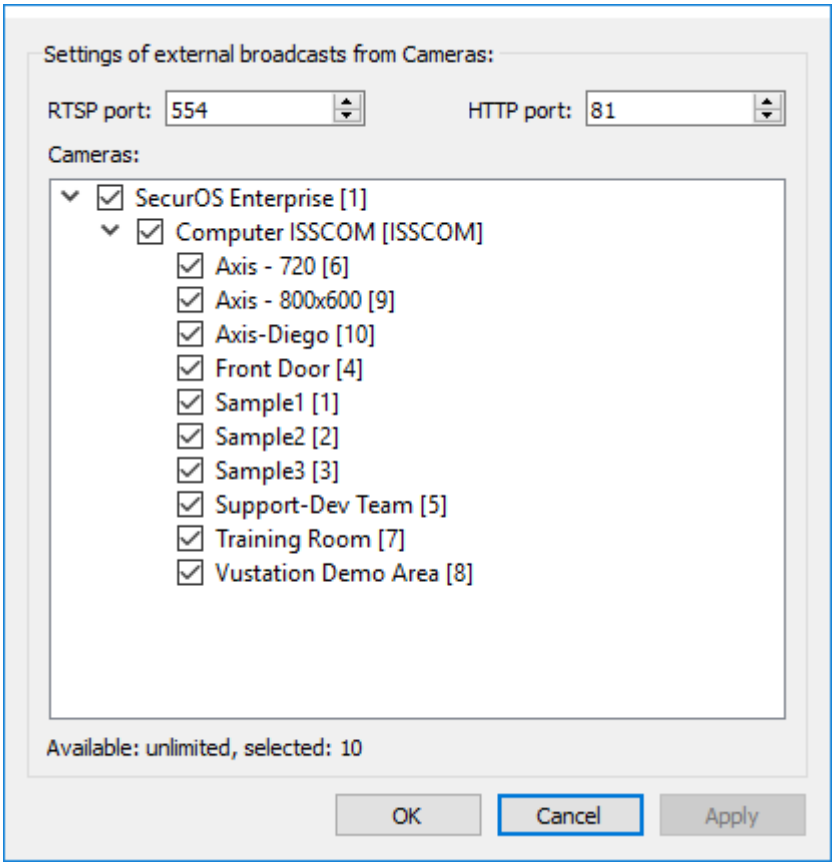


The network-related settings of these new entities will have to be entered into VuWall2 in a later step. To access these settings, and modify them if need be, click on each header and select the "**Gear**" icon.



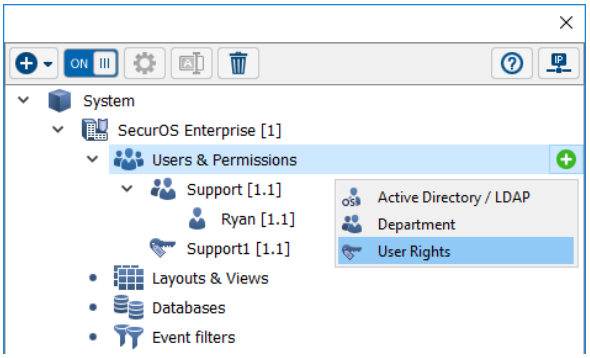
For the "**Rest API**", the "**Port**" and "**Use HTTPS**" settings will need to match those in VuWall2.

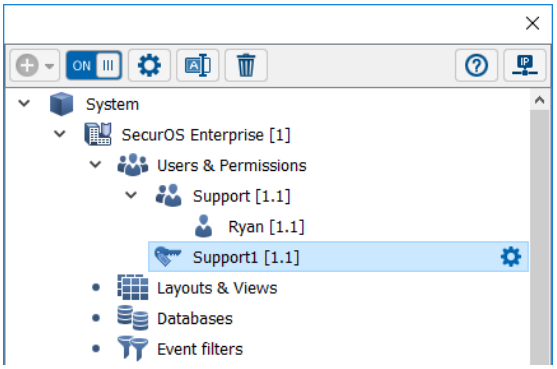
For the "**RTSP Server**", only the "**RTSP Port**" will be necessary. In this form, you can also filter which cameras will be accessible to the VuWall2 Server.



Assign User Credentials for the Integration Entities

We recommend creating a dedicated user account and set of user rights for the video wall integration, which will only be assigned the necessary permissions. For the user rights, click on the "**Users & Permissions**" header, select the green **"+"** icon and choose "**User Rights**". Once that is done, click on that new entity's header and select the "**Gear**" icon.

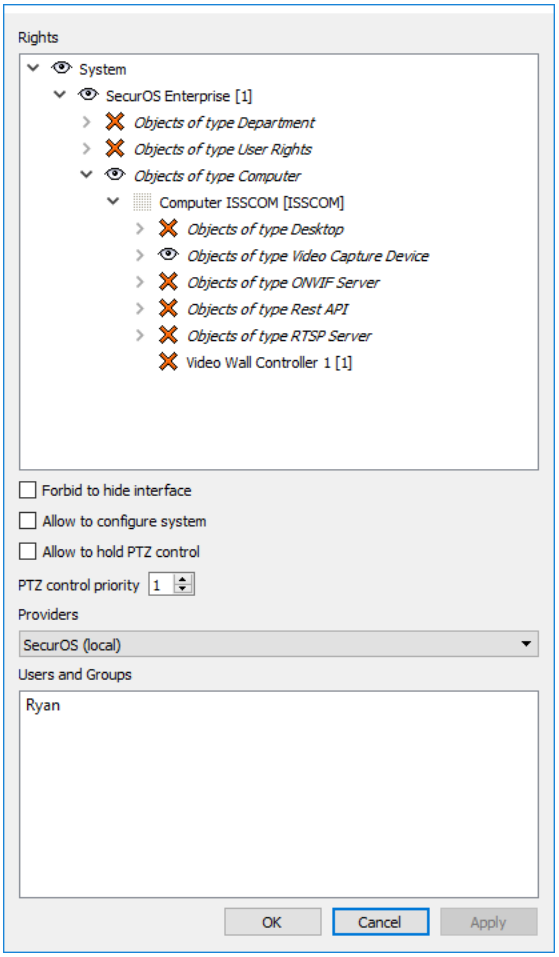




The VuWall2 Server user only needs "**Read**" access to the camera entities; everything else can be forbidden. The "**Rest API**" and "**RTSP Server**" entities themselves do not need to be accessed or managed by that user account. Their functionality will still be available on the network, allowing access to the other entities given the appropriate credentials.

In the "**Users and Groups**" section, enter the account that will be used by the video wall controller.

This concludes the setup required in ISS SecurOS, now we will configure VuWall2 to retrieve the cameras.



Configure Milestone XProtect for VuWall2 Integration

"Milestone offers the market's widest portfolio of IP VMS solutions spanning from easy-to-use small, single-server solutions to fully scalable advanced solutions for high-security surveillance and alarm centers. All products in the XProtect portfolio are designed based on the same powerful open architecture, which makes the XProtect products compatible with more IP cameras and video encoders than any other VMS manufacturers."

- Extract from Milestone XProtect VMS brochure.

VuWall2 can integrate cameras managed by Milestone XProtect. These cameras will appear as IP device sources available to be simultaneously mixed with other types of content that VuWall2 supports.

Requirements

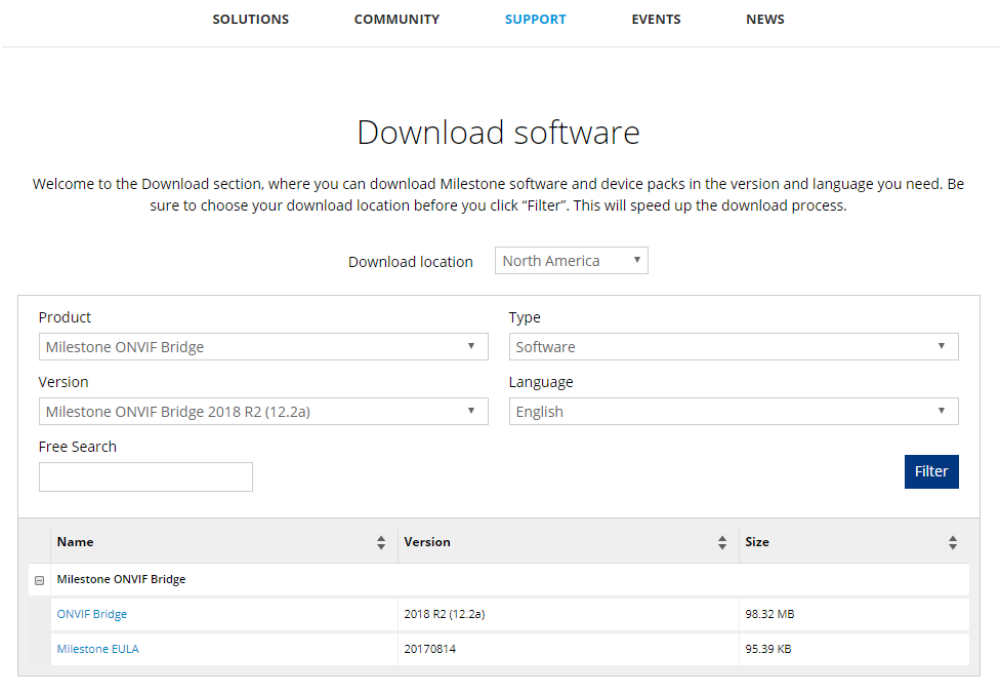
- Access to an Milestone XProtect server version 2018 or above
- Milestone XProtect Client version 2018 or above on a workstation for configuration
- XProtect administrator class user, able to create entities
- VuWall2 Server 2.12 Pro or above
- VuWall2 Client installed on a workstation computer for configuration

Note: Milestone XProtect Client & VuWall2 Client can co-exist on the same workstation.

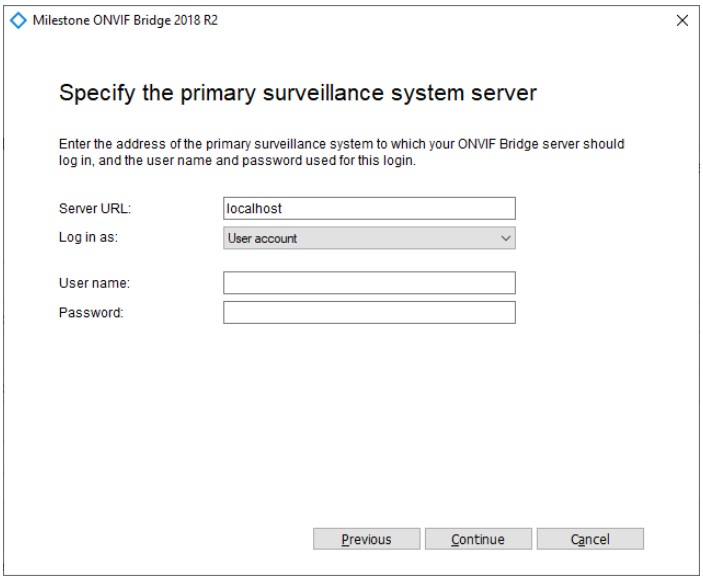
Install the Milestone ONVIF Bridge

Using a web browser, navigate to the Milestone website's download page: https://www.milestonesys.com/support/resources/download-software

There, search for the product "**Milestone ONVIF Bridge**", matching the version of your local Milestone server. Clock on the file named "**ONVIF Bridge**" to start the download.

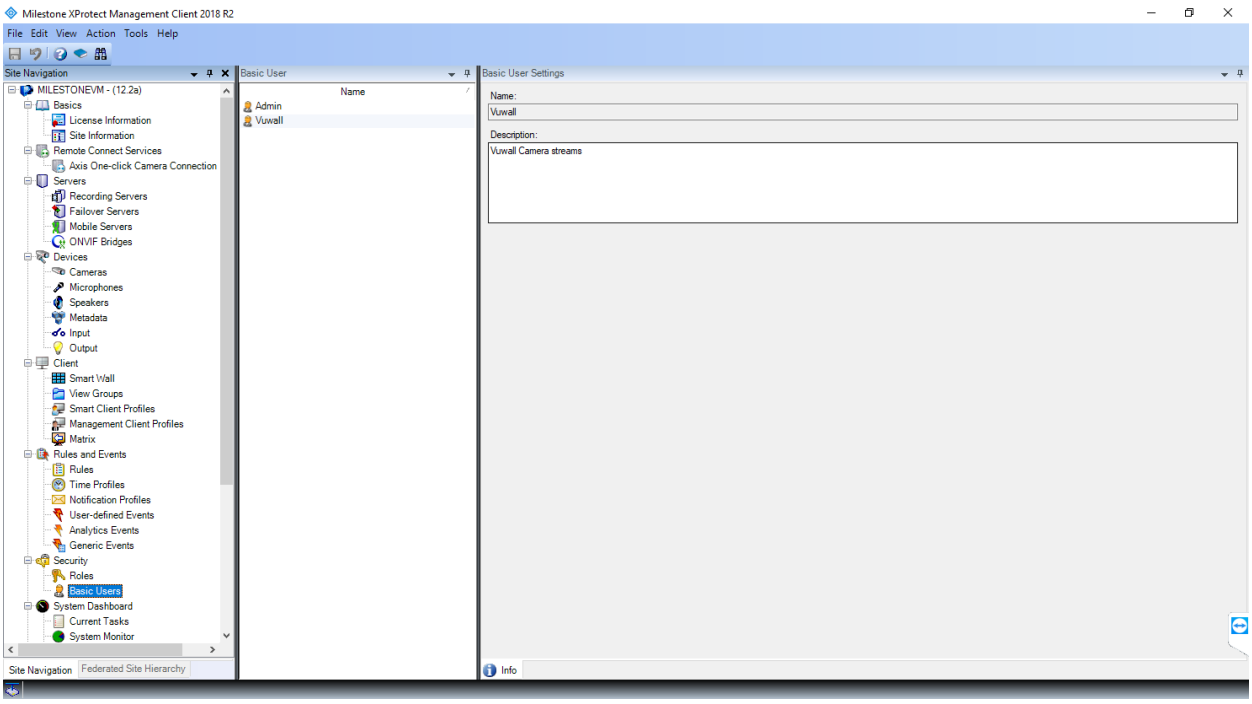


Once downloaded, copy the file "**VideoOS.ONVIF.Installer.exe**" onto the computer running the Milestone Server, execute it and follow the instructions. No customization is necessary during this installation. Along the way, you will need to specify the primary server and enter its administrator credentials.

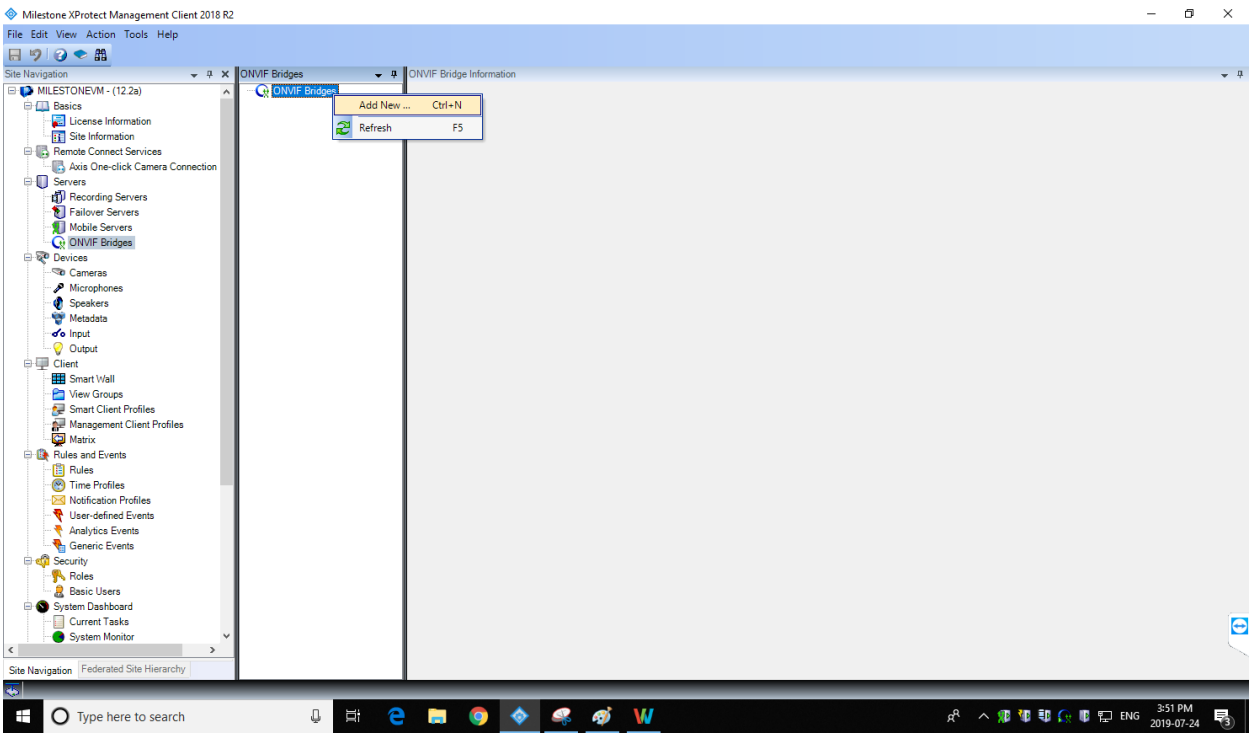


Activate access to the ONVIF Bridge Server

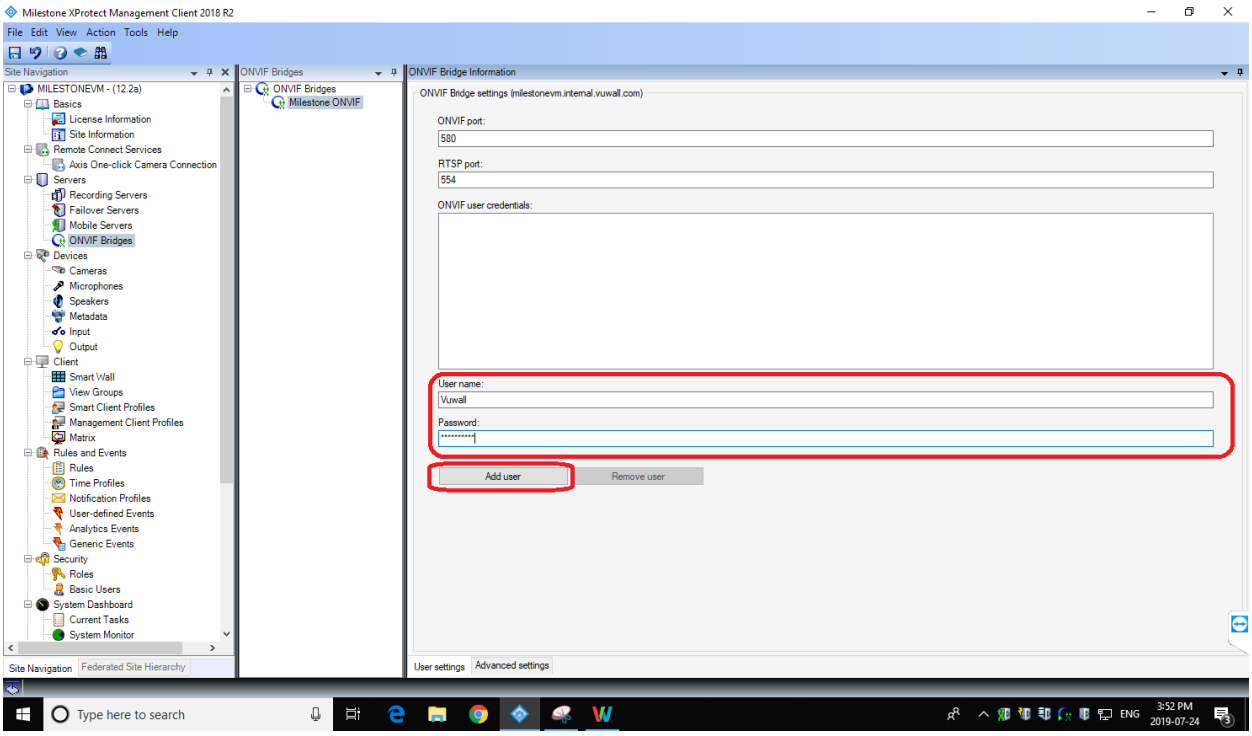
In the Milestone Management Client under the "**Security**" Tab Create a Basic user for accessing the cameras through the ONVIF Bridge.



Go to the "Server" Tab and select ONVIF Bridges. Add New Bridge



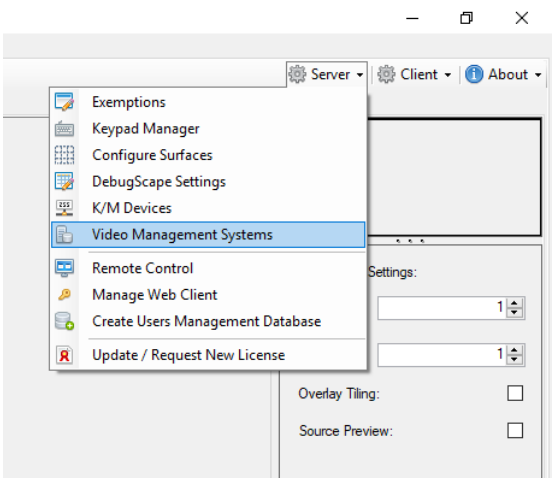
Add recently created user and the password to the ONVIF Bridge. This will allow the video wall controller to retrieve the camera streams from the "**RTSP port**" with these credentials.

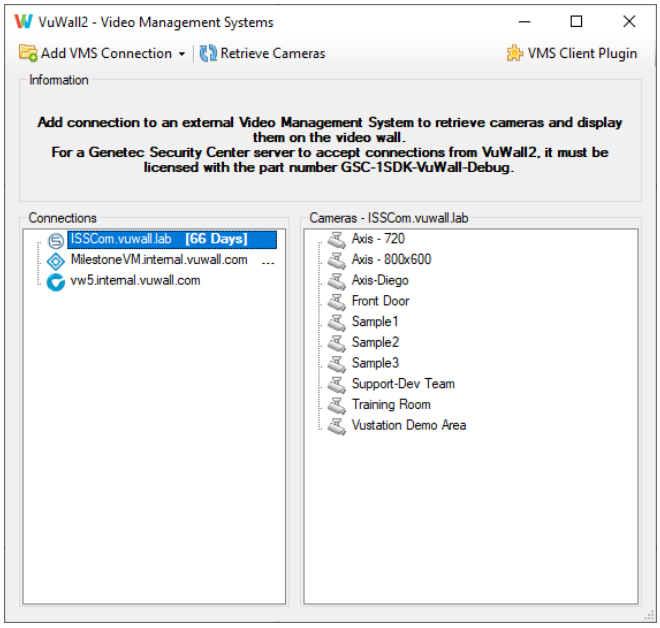


Configure VuWall2 for VMS Integration

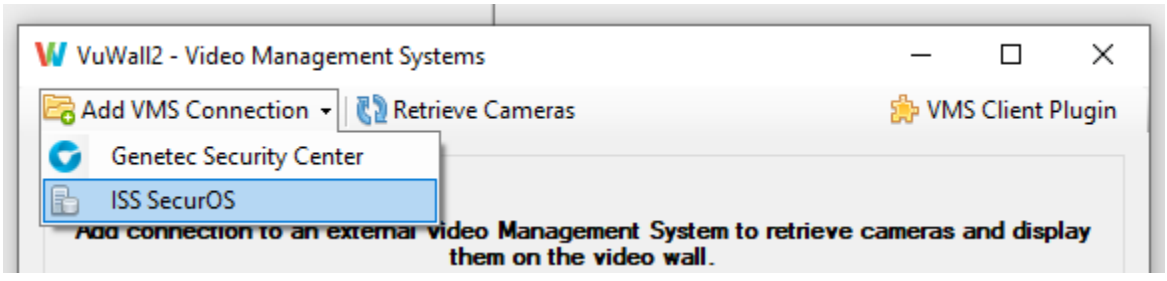
Register VMS Server and Network Settings

Launch a VuWall2 Client connected to the VuWall2 Server. Click on the Server **"Gear"** button, toward the top right corner, to display its pull-down menu. Then select **"Video Management Systems"**.

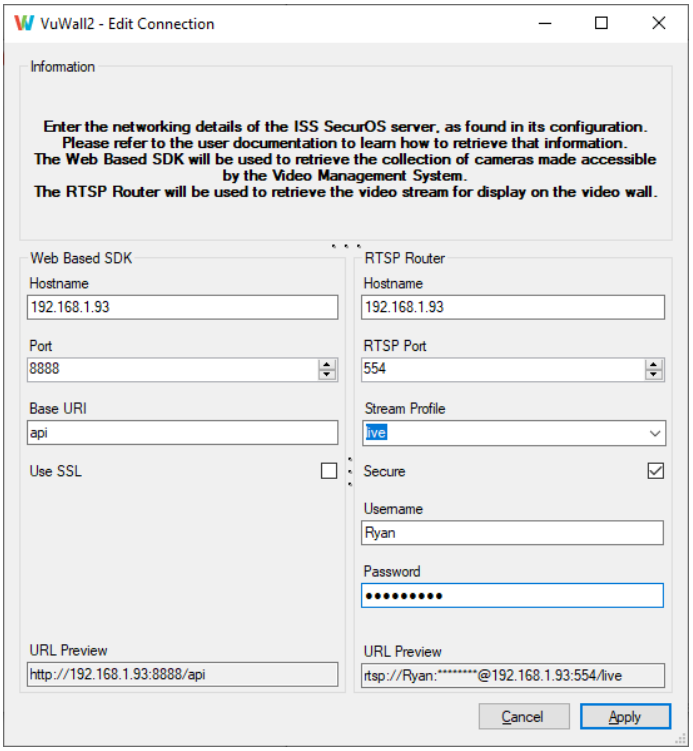




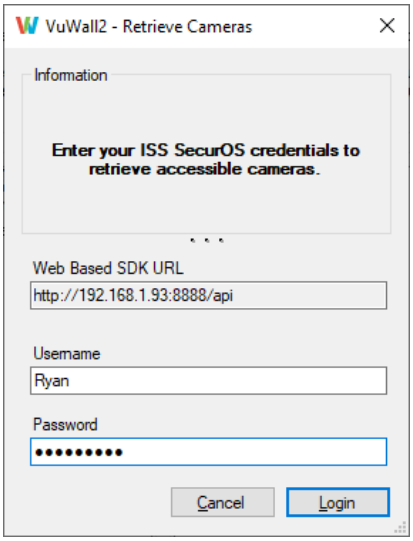
On the next window, click on **"Add VMS Connection"** and select one of the compatible Video Management System from which to retrieve cameras. The VMS Server must have been previously configured according to the relevant instructions in this document.



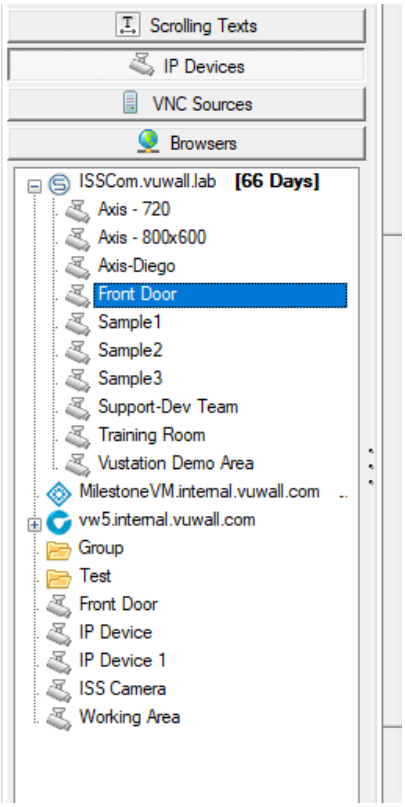
Type in the missing information as previously entered in the VMS Server's own configuration. Default networking configuration values particular to each VMS are filled in automatically; you may edit them to match the VMS Server. Then click "**Apply"**, give a name to your connection, and click on **"Save Connection"**.



The process will now attempt to contact the VMS Server over the network to retrieve the list of available cameras. A new window titled **"Retrieve Cameras"** will be displayed, asking for credentials to continue. Click on **"Login"**.

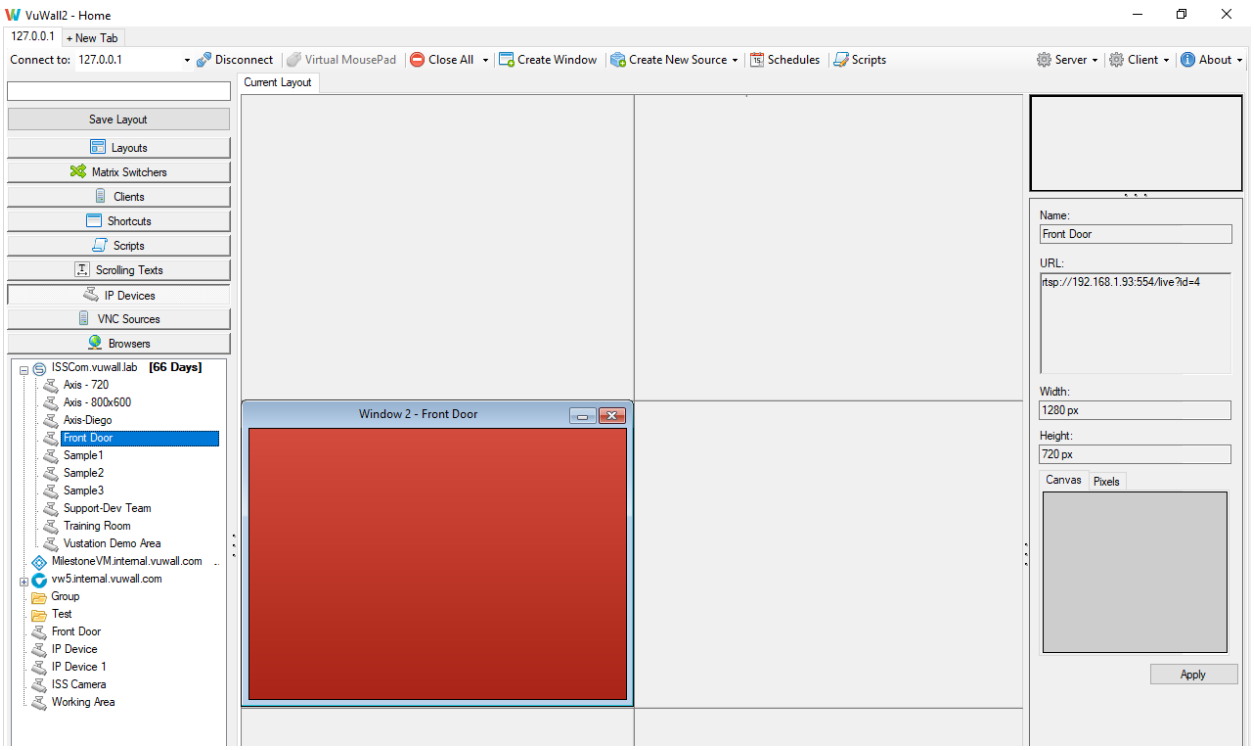


Display Retrieved VMS Cameras



After a successful login, you will see cameras appear in the "**Cameras**" section on the right of the "**Video Management Systems**" form.

Back in the main VuWall2 Client form, a registered VMS is reflected as a new folder in the **"IP Devices"** source section, allowing you to drag and drop those cameras onto the video wall layout.



Preferred Renderer (Matrox IPX / Datapath SQX Only)

It is possible to set the Preferred Renderer of a given VMS camera to leverage the hardware decoding capability of the video wall processor and improve performance. To do so, right-click on the camera you'd like to modify and set its Preferred Renderer.