

VuWall2

Video Wall Control Software - 2.10.4

Video Management Systems Integration

Oct 2019

www.vuwall.com

© 2019 VuWall technology, Inc

Simplicity in AV networks & video wall management



Table of Contents

Configure Genetec Security Center for VuWall2 Integration	2
Requirements	2
Create a user account in Security Center	3
Create the RTSP Gateway entity	5
Give your user access to the gateway	7
Create the WEB SDK entity	8
Configure ISS SecurOS for VuWall2 Integration	10
Requirements	10
Create the Integration and Automation Entities	11
Assign User Credentials for the Integration Entities	13
Configure Milestone XProtect for VuWall2 Integration	14
Requirements	14
Install the Milestone ONVIF Bridge	15
Activate access to the ONVIF Bridge Server	
Configure VuWall2 for VMS Integration	18
Register VMS Server and Network Settings	
Display Retrieved VMS Cameras	20
Preferred Renderer (Matrox IPX / Datapath SQX Only)	21

VuMall

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

	41 🧶 👔 Tue 1138 AM 📃 🖬 🛇
✿ Config Tool 🖉 System 🔰 🌡 User manag ×	
Sector • Vidi • P. Antoler uses • P. Antoler uses • C. Particle • Sort by • Sort by • Sort by • Sort by • C. Particle • User group Show all •	
🕈 Add an entity	

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".

	Creating a user			
	User information	Username:	vuwall	
▲ Config Tool System	Creation summary	Password:	•••••	
A	Entity creation outcome	Confirm password:		
Tasks			(mar. 1)	(i
Private tasks		First name:	VuWall	
Public tasks		Last name:	Technology	
Tools			Unseriment	
		User group:	Unassigned	0
Options		Privilege template:	None 🔻]
About			A This user will have no privileges and	d will not be able to access the
			system.	
	Cancel			Next >
				<u></u>
		Favorites and	recent items	



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"**.

							📢 🌀 👖 Tue 1:38 PM 📃 🛄 🔜
🏠 Config Tool	System	. × 1	1 User manag				
🜻 General settings	🎽 Roles	🔝 Sche	edules 🛛 🛛 Scheduled tasks	🖇 Macros	🔛 Output behaviors	> I	er
Search		Ŷ					
Access Manager		—					
Archiver							
Health Monitor							
🗑 LPR Manager							
Map Manager							
Media Router							
Report Manager							
👯 Webbasesdk							
🔋 Zone Manager							
🕂 Add ar	entity	• •	Access Manager				
		Ē	Active Directory				
Refrest	n FS	5 i i i i i i i i i i i i i i i i i i i	Active Directory Federation Se	ervices			
		8	Archiver				
		6	Global Cardholder Synchroniz	er			
			LPR Manager				
		\mathbb{P}	Media Gateway				
		6	Omnicast Federation				
		*	Plugin				
		6	Security Center Federation				
		80	Web-based SDK				
		- R	Zone Manager				
		_	Show all	,			
				_			
🕂 Add an entity							

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 **1 "Properties"**, and take note of the **2 "Listening Port"**

				📢 🥥 👖 Tue 105 PM 📃 🗔 😒
🔒 Config Tool	System × 👔 User manag			
🔮 General settings 🧖 R	oles 📓 Schedules 🛷 Schedu	ed tasks 💲 Macros 📴 Output behaviors 🛛 🖌 🛸 🚏	V⊔Wall	
	•	_		
Search		ldentity	Properties Resources	
Archiver				
b Health Monitor			↑	
👼 LPR Manager	Start multicast ac	dress: 224 . 116 . 117 . 1 : 51914 \$		
🚦 Map Manager	Detector			
T Media Router	Ustenin			
Report Manager	User authenti	ation: 💽	(1)	
👯 Webbasesdk	Accessi	e to: 🎝 Admin		
関 Zone Manager				
🕂 Add an entity 🛛 🗙 De	lete 🚸 Maintenance 🕶			



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"**.

			📢 🎯 👔 Weel TE35.AM 📃 🗖 🔤 🚳
👌 Config Tool 🛛 🔮 System 🚿			
🔮 General settings 🥌 Roles 📾 Sch	nedules 👼 Scheduled tasks 🚿 Macros	🖥 Output behaviors 🖌 > 📫 🏲 YuWall	
Ceneral settings in false in Sch Centrol Access Munager Centrol	edules 🖝 Scheduled tasts 🚿 Macros RTSP Start multicast address: 224 - 116 - 1 Listering port: 554 - 2 User authenticator: Accessible to: Accessible t	Comput behaviors C Comput behaviors C C C C C C C C C C C C C C C C C C C	
🕂 Add an entity 🗙 Delete 🚸 M	faintenance 🔻		



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 **① "Properties"**, **②** take note of the **"Port"**, **"Streaming Ports"** numbers and **"Base URI"** name.

			📢 🥥 👖 Tue 254 PM 📃 🔲 💌
Config Tool	🖲 System 🛛 👋	T User manag	
Seneral settings	s 🚔 Roles 🕅 Scl	hedules 🛷 Scheduled tasks 🍯 Macros 🔀 Output behaviors < 🖇 🛤 🎰 WuWallWebSDK	
Search Access Manager Archiver Health Monitor C LPR Manager Map Manager Map Manager Map Manager Map Manager	٩	Part: (590 C) Streaming port: (591 C) Break Weddat: Uno 50 common	
VuWall			
🕂 Add an entity	🗙 Delete 🛛 🚸 N	Maintenance 🕶	

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

Vu</mark>Mall

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 rightcorner. 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.

•	🚛 Notifications		
~	🚯 Integration & Automation	Port: 8888	
	• ONVIF Server 1 [1]	WebSocket port: 8080	
	Rest API 1 [1]		
	RTSP RTSP Server 1 [1]	Use Event Filter: Don't use 🔻	
•	Mobile & Web Servers	OK Cancel Apply	

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.

KISP port:	554 🜩	HTTP port	t: 81	÷
Cameras:				
× ∑ S4	Computer ISSCOM Axis - 720 [6] Axis - 800x600 [9 Axis - 800x600 [9 Axis-Diego [10] Front Door [4] Sample1 [1] Sample2 [2] Sample3 [3] Support-Dev Te Training Room	[ISSCOM])] am [5] 7] Area [8]		

Vu<mark>\//</mark>all

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.

Rights
V ③ System
✓ ③ SecurOS Enterprise [1]
> X Objects of type Department
> X Objects of type Liser Rights
Objects of type Computer
Computer ISSCOM [ISSCOM]
> X Objects of type Desktop
Objects of type Video Capture Device
> X Objects of type ONVIF Server
> 🗙 Objects of type Rest API
> X Objects of type RTSP Server
Video Wall Controller 1 [1]
Forbid to hide interface
Allow to configure system
Allow to hold PTZ control
PTZ control priority 1
Providers
SecurOS (local)
Users and Groups
Ryan
OK Cancel Apply

VuMall

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: <u>https://www.milestonesys.com/support/resources/download-software</u>

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.

SOLUTIONS	COMMUNITY	SUPPORT	EVENTS	NEWS	
	Downloa	ad softw	are		
Welcome to the Download section, when sure to choose your do	re you can download Miles ownload location before yo	tone software and ou click "Filter". Th	d device packs in th is will speed up the	e version and langu download process.	age you need. Be
	Download location	North Americ	av		
	Dominadi locadori				
Product		Туре			
Milestone ONVIF Bridge		Software			*
Version		Language			
Milestone ONVIF Bridge 2018 R2 (12.2	a) 🔻	English			Ψ
Free Search					
					Filter
Name	Version			Size	÷
O Milestere ONVE Drider				-	
ONVIF Bridge	2018 R2 (12.2	a)		98.32 MB	
Milestone EULA	20170814			95.39 KB	

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.

Specify the	primary surveillance system server
Enter the address o log in, and the user	f the primary surveillance system to which your ONVIF Bridge server shoul name and password used for this login.
Server URL:	localhost
Log in as:	User account V
User name:	
Password:	



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.

File Edit View Action Tools Help Ste Nampston Ste Nampston P MILESTONEVM - (12 2a) ONVF Bridges ONVF Bridge Information OVVF Bridge Information OVVF Bridge Information OVVF Bridge Information OVVF Bridge Stellings Infectioneym Intend Vuewal Com	→ ‡
Ste Navigation • • •	• ‡
Site Navigation • • • × ONV/F Bridges • • ONV/F Bridge Information • • • • • • ONV/F Bridge Information • • • • • • • ONV/F Bridge Information ONV/F Bridge Strings (nifestonewn.intend.vuwal.com)	↓ ₽
E 📭 MILESTONEVM - (12 2a) A E 😯 ONVIE Bridges ONVIE Bridges ettings (intestoneym intendi vuvval.com)	
With Back With Back Back Sometice Bac	
🕂 🔿 Type here to search 🔱 뷰 含 🔚 🎯 💠 🤐 W 🥵 R 🕫 🕫 🕫 😒	M -24 🖏

Vu<mark>\//</mark>all

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.

\phantom VuWall2 - Video Management Systems	_		×
🔀 Add VMS Connection 👻 🖏 Retrieve Cameras	🍰 VM	S Client P	lugin
Genetec Security Center			
E ISS SecurOS			
Add connection to an external video Management System to re them on the video wall.	etrieve cameras	and disp	lay



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**".

Enter the networking detail Please refer to the user	ls of the ISS Se documentation	ecu to	urOS server, as found learn how to retrieve	in its cor that info	nfiguration.	on.
The Web Based SDK will be b The RTSP Router will be us	used to retriev y the Video Ma ed to retrieve th	ne i na he	the collection of came gement System. video stream for disp	eras made lay on the	e access e video v	sible wal
Web Based SDK		ì	RTSP Router			
Hostname			Hostname			
192.168.1.93			192.168.1.93			
Port			RTSP Port			
8888	-		554			ŀ
Base URI			Stream Profile			
api			live			
Use SSL		••••	Secure			I
			Usemame			
			Ryan			_
			Password			
			•••••			
			URL Preview			

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"**.

VuWall2 - Retri	eve Cameras	>			
Enter your ISS SecurOS credentials to retrieve accessible cameras.					
Web Based SDK I					
http://192.168.1.9	93:8888/api				
Usemame					
-					
Ryan					
Ryan Password					



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.

🚺 VuW	all2 - Genetec	IP Camera		—		\times
URI:						
rtsp://vu	.wall:******@19	92.168.1.27:65	4/			
Pref	erred Decoder					_
Matrox	IPX					\sim
Enable	e OSD					
🗹 Use	Source Name					
Text:						
Font:	Arial, Regular,	24				
				Cho	ose Font.	
Alianmer	nt.					
Text Cold	or:					
Back	ground Color:				1	
		Apply	/			