# Aimetis<sup>™</sup> Symphony VE510 Metadata Analytic

Setup

## **Disclaimers and Legal Information**

Copyright<sup>©</sup> 2015 Aimetis Inc. All rights reserved.

This material is for informational purposes only. AIMETIS MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Aimetis Corp.

Aimetis may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Aimetis, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Aimetis and Aimetis Symphony are either registered trademarks or trademarks of Aimetis Corp. in the United States and/or other countries.

#### **Document History**

February 12, 2015

# Setup

#### Display the VE510 analytic in Symphony

- 1. In the \_bin\algos folder of your Symphony install, find Intel\_VE510.xml and using an editor change the <Display> tag to true.
- 2. Save the file.
- 3. In Symphony, restart Symphony Services. Server>Services>Restart Symphony Services.

S <u>e</u> r	ver	<u>S</u> earch	LPR	<u>R</u> eports	Ŀ	
	<u>A</u> ları	m Console				
	<u>D</u> isa	ble Alarms	for Serv	er		
	<u>E</u> nab	ole Alarms f	or Serve	er		
١	G <u>e</u> t I	nfo				
	De <u>l</u> e	te Old Foot	age			
	View	Logins			×	
2	<u>C</u> ont	figuration	Ct	rl+Shift+C		
2	User	Configurat	ion			
	Devi	ce Tree Cor	nfigurat	ion		
	Secu	rity Profiles	5			
	<u>M</u> an	ual Configu	uration	Editor		
	Add	Access Dev	vices			
	<u>B</u> ack	up				
	Rest	ore				
	Serv	ices			•	Stop Symphony Services
	Vide	o Wall				Start Symphony Services
						Restart Symphony Services
						Manage Symphony Services

#### Configure a camera to use VE510

- 1. In Symphony, select Server>Configuration.
- 2. In left pane, click **Devices**.
- 3. Select the camera you want to configure and click Edit.
- 4. Select the Analytics Engines tab and select VE510- Metadata.
- 5. Select the **Analytics Configuration** tab. The **Intel\_VE510 engine** is displayed. No configuration is required. Click **OK**.



Server Configuration - localhost - Device					
Rules	Server	Screenshots	•	_	
The second secon	Network	Video Digital VO Analytics Engines	Analytics Configuration		
AXIS Q74361					
		Analytics Engines Intel_VE510	•	Restore Defaults	
				Show XML View	
				SHOW ANL VIEW	
- (5) General Settings	The VE51	0 does not require any configuratio	n.		
Maintenance Settings					

#### Create a rule to alarm on metadata

- 1. In Symphony, select **Server>Configuration**.
- 2. In left pane, click **Rules**.
- 3. Click New. The Rule Wizard opens. Click Next.
- 4. Select the check box next the camera using the VE510 analytic.
- 5. Select the **Alarm Type** Alarm on any metadata (e.g. serial numbers, barcode numbers) OR enter a specific item (e.g. serial number/barcode number) to alarm on.
- 6. Click Action.
- 7. In the Alarm tab, select the camera and the Raise Alarm check box.
- 8. Select the **FTP** tab and configure as necessary. You can include the metadata in the filename using the **%md** option.
- 9. Proceed with **Schedule** and **Summary** and click **OK**. Remember to save the rule with an appropriate name.

S Rule Wizard - localhost - New Rule	2				
1: Instructions	2: Event	3: Action	4: Schedule	5: Summary	
Please define sub events	for the rule				
Sub Events		Select VE51	video engine from those running ) - Metadata	on camera	
New Sub Event 2           New         Remove           Up         Down	Cameras     AXIS Q	74361_1 a 1 a 2 a 3 ra Motion Detection 74361_1 a 1 a 2 a 3 are Device1	n type larm on any metadata larm on metadata that contains:		

1: Instructions	2: Event	3: Action	4: Schodulo	5: Summary
	2. Livent	3. Action	4. Scheddle	5. Summary
Choose which action	ns you want this	rule to take when an alar	moccurs	
Create new action	-	Edit Domouro Dooo	+ 1	
Cleate new action	<u> </u>	Luit Nellove Nese	L	
Action name Actio	n2			
Alarm Record Relays	FTP Email TO	P Run Program Sounds Zo	oom Instructions Rule	e OPC SMS
FTP camera images or	n alarm	☑ Transfer a picture of the alar	m to an FTP server	Â
- ₽ Devices		Serve	r name	Port 21
	1_1	Use	mame	
- Camera 1 - Camera 2		Pas	ssword	
- 😴 5) Camera3		Remote di	rectory	Example: public_html/
ن السي (3) HardwareDe	evice1		,	
		🔽 Transfer Multiple pictures		Rename the transferred file according to this pattern
		Pre-alarm pi	ctures 6	E
		Post-alarm pi	ctures 6	Use UTC date and time
		Interval between pi	ctures 200 millisecon	conds *YYYY - Year
				*MM - Month *DD - Day
		Show all Decorations		%HH - Hour in 24-hour format %hh - Hour in 12-hour format
		M Boxes		<pre>%mm - Minute %ss - Seconds</pre>
		M lext Ime		<pre>%tt - An or PA %fff - Milliseconds %n - Dula Vara</pre>
		☑ Path		*1 Andre Name *b - Abbreviated Rule Name *o - Rule Mumber
		Resize the transferred file		te - Caneta Mane tn - Caneta Munber tnd - Hetadata +

## Set up OPC for Symphony

**Important:** This procedure assumes that you already have an Aimetis Symphony server running with the appropriate OPC Server license (SYM-OPC-SL) on it.

In a multiple server farm environment, you must install OPC on each server in the farm, including redundancy servers, to ensure that alarms are received across all servers in the farm from all active, moved, or failed over devices. Installing the OPC Server on a virtual machine running Symphony Server is also supported.

- As a Windows Administrative user, open a command prompt and navigate to: (which is typically C:\Program Files (x86)\Aimetis\Symphony\\_bin\)
- 2. Run the command: airaopcserver.exe -regserver
- Launch Component Services. (From the Start > Run menu enter dcomcnfg to launch Component Services.)
- 4. Navigate through the tree to: **Component Services > Computers > My Computer > DCOM Config > AiraOPCServer**. Right-click on **AiraOPCServer** and select **Properties**.



5. On the General tab set the Authentication Level to None and click OK.

General	Location Securi	ty Endpoints Identity		
Gene	ral properties of thi	s DCOM application		
Ap	plication Name:	AiraOPCServer		
Ap	plication ID:	(630A9661-659A-4D36-A4C9-8F6991FA	F78E}	
Ap	plication Type:	Local Service		
Au	thentication Level	None		•
Se	rvice Name:	Al AiraOPCServer		_

6. In Windows Services restart the AI Scheduler service. (To access Windows Services, select Windows Start > Run menu and enter Services.msc.)

**Note:** Every time a camera device or rule is modified in Aimetis Symphony, you must restart BOTH the **AI Scheduler** and the **AiraOPCServer** via Microsoft<sup>®</sup> Windows<sup>®</sup> Services (Services.msc).

#### Enable Remote Access to Symphony OPC Server

- 1. From the **Start > Run** menu enter **dcomcnfg** to launch **Component Services.**
- 2. Navigate through the tree to: **Component Services > Computers > My Computer**.
- 3. Right-click on My Computer and select Properties.
- 4. On the **COM Security** tab click **Edit Limits...** for both sections (Access Permissions and Launch and Activation Permissions). Add the user group **Everyone** and make sure this new Everyone group has all **Remote** permissions enabled (as available). Click **OK**.

	Access Pe	ermissions		
My Computer Properties		Access Permission		2 ×
General         Options         Default Properties         Default Protocols         COM S           Access Permissions         You may edit who is allowed default access to applications also set limits on applications that determine their own permissions         Caution: Modifying access permissions can affect applications to start, connect, function and/or run side	ecurity MSDTC You may issions the ability of ecurely.	Security Limits Group or user names:		-
Edit Limits. Edit Launch and Activation Permissions You may edit who is allowed by default to launch application objects. You may also set limits on applications that determine permissions. Caution: Modifying launch and activation permission securely. Edit Limits. Edit	Default. Is or activate ne their own ms can affect and/or run Default.	Permissions for Everyone Local Access Remote Access	AddAllow	Remove Deny
Learn more about setting these properties		Learn about access control and p	ermissions OK	Cancel

Computer Properties	
General Options Default Properties Default Protocols COM Security MSDTC	Launch and Activation Permission
Access Permissions You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions. Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely. EditLimits. Edit Default	Group or user names:
Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions. Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect function and/or run securely. Edit Limits. Edit Default.	Add Bernove Permissions for Everyone Allow Deny Local Launch Remote Launch Local Activation Remote Activation Rem
Learn more about setting these properties.	Learn about access control and permissions

- 5. Click **OK** again to close the My Computer Properties dialog.
- 6. In Component services, navigate to Component Services > Computers > My Computer > DCOM Config. Right-click on AiraOPCServer and select Properties.



7. On the Security tab select the Customize option for all three sections (Launch and Activation Permissions, Access Permissions, and Configuration Permissions). For each section, click Edit... and add the Everyone user group. Make sure this new Everyone group has all Remote and Full Control permissions enabled (as available) and click OK.

C	Use Default				
C	Customize		 2	Edit	
Ac	cess Permissions				
0	Customize			Edit	)
Co	nfiguration Permiss	ions			
C	Customize			Edit	)

Security	Access Permission	2 ×		
Group or user names:	Security Group or user names:	Change Configuration Permission Security Group or user names:	)	2
Permissions for Everyone	S& SYSTEM	線 CREATOR OWNER 線 SYSTEM 線 Administrators 線 Everyone 線 Users		
Local Launch Remote Launch Local Activation Remote Activation	Permissions for Everyone Local Access Remote Access	Permissions for Everyone Full Control Read Special permissions	AddAllow	Deny
Learn about access control and per	Learn about access control and perm	For special permissions or advanclick Advanced.	ced settings.	Advanced

- 8. When finished, click **OK** to close the AiraOPCServer Properties dialog.
- Launch Windows Administrative Tools. Depending on your version of Windows there are different ways to access this. In Windows 7/Server 2008 enter Admin in the Windows > Start menu and choose Administrative Tools.

**Note:** If you are using Windows Embedded, Windows 8 or Windows 8.1, you can omit the following steps. (These Windows versions do not have Local Security Policy (secpol.msc) settings. Aimetis OPC works on PSA with these versions.)

 Launch the Local Security Policy. Navigate through the tree to: Local Policies > Security Options > DCOM:Machine Launch Restrictions in Security Descriptor... Right-click and select Properties.

File Action View Help					
Security Settings  Account Policies  Local Policies  Audit Policy  Guese Rights Assignment	Policy Audit: Force audit pol Audit: Shut down syst DCOM: Machine Acce	icy subcategory set em immediately if ss.Restrictions in Se	ttings (Windows Vi unable to log secu ecurity Descriptor	Security Setting Not Defined Disabled Not Defined	
Security Options	DCOM: Machine Laun	ch Restrictions in S	ecurity Descriptor	Not Defined	
Windows Firewall with Advance     Network List Manager Policies     Public Key Policies     Software Restriction Policies     Application Control Policies     FIP Security Policies on Local Co     Advanced Audit Policy Config	Devices: Allowed to Devices: Prevent users Devices: Restrict CD-F Devices: Restrict flopp Domain controller: Al Domain controller: LD Domain controller: Re Domain member: Dig Domain member: Dig Domain member: Dig Domain member: Dig Domain member: Dig Domain member: Dig Domain member: Dig	Help from installing pri IOM access to locally low server operato DAP server signing r fuse machine acco itally encrypt or sig itally encrypt secur itally sign secure cl able machine acco ximum machine acco	able media nter drivers Ily logged-on user logged-on user on rs to schedule tasks requirements unt password chan gn secure channel d re channel data (when unt password chan count password chan count password age	Not Defined Disabled Not Defined Not Defined Not Defined Not Defined Enabled Enabled Disabled 30 days	

11. On the Template Security Policy Setting choose Edit Security...

emplate	Security Policy Setting Explain
i	DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax
If the se templat	curity descriptor is left blank after defining the policy setting in the e, the policy setting will not be enforced.
Security	/ descriptor.
	Lancount.

12. Make sure the **Everyone** user group has all **Remote** permissions enabled and click **OK**.

Reveryone	
Everyone     Administrators     Performance Log Users     Distributed COM Users     Add	
Administrators     Performance Log Users     Distributed COM Users     Add	
Performance Log Users     Distributed COM Users     Add	
Distributed COM Users     Add	
Add Rer	
Add Rer	
Add Ren	
	move
	100
Immissions for Everyone Allow De	eny
Local Launch	
Remote Launch	
Local Activation	
Remote Activation	3

13. Click OK to close the DCOM: Machine Launch Restrictions in Security Descriptor dialog.

#### **Push Metadata to OPC Client**

1. In the OPC client, go to the **DA Browse** tab and add the ToAira.Camera\_x.Metadata (where x is the camera ID).



2. On the **DA Items** tab, select ToAira.Camera\_x.Metadata (where x is the camera ID). In the top-right corner of the OPC client screen, enter the metadata in the **Write** field and then click **Write**.

Softing OPC Toolbox Demo Client										
File Edit	Session Vi	ew								
New	🖻 Open	<b>R</b> Save	Properties	Delete	🗙 Stop	<u>/</u> Connect	C Start			MetadataHere Write
⊡	a Access OPC Server Oroup	for BIS usin ra.Cameraj	ng Aira2005 _1.Metadata	Item	uira. Camera	_1.Metadata	I	Value	Quality GOOD	TimeStamp Re 09:48:29.706

Important! Ensure that firewall settings allow/disallow connections to port.

## How to Search for Alarms

1. In Symphony, click the **Search** icon.

<u>Fi</u> le	<u>V</u> iew	<u>B</u> ookmarks	Server	<u>S</u> earch	<u>R</u> eports	Help	1	<b>4</b>	
8	Load Multi	i View 👻 🧮 T	ool Strip	Timeline	Havig-	ation	8		Carousel → Send Picture To →
1) Cameral - localhost: i7-6-MV Console-P1									
🔚 Timeline 🔚 Navigation Decoration 🖾 Date 🔚 Export 🖉 Search ) 🦏 📦 🔻 ai://10.234.10.67/1/2011_11_30_16:36:07.123									
02:0	0 PM 📃		1				5		
02:3	0 PM								

- 2. The VE510 Metadata analytic appears in the **Search** dialog box.
- 3. For a specific time/date range, you may search:

On an alarm for any metadata (e.g. serial numbers, barcode numbers)

OR

For metadata containing a specific item (e.g. serial number/barcode number).

Search - Camera 1 - localhost	
Alarm type Alarm on any metadata Alarm on metadata that contains:	Search Type           From         02/05/2015 12:54 PM           To         02/06/2015 12:54 PM
	Analytics Engines
	✓ VES10 - Metadata