

# Aimetis Symphony™

Version 6.12

Administration Guide

October 9, 2013



---

## Disclaimers and Legal Information

Copyright © 2013 Aimetis Corp. All rights reserved.

This guide 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 Corp. , 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.

Portions Copyright © 1993-2013 ARH Inc.

Portions of this software are based in part on the work of the Independent JPEG Group.

# Document History

**Table 1. Changes to this manual**

Date	Description
August 15, 2013	<p><b>Release 6.12.1</b></p> <ul style="list-style-type: none"> <li>Automatic upgrade feature for Symphony Client now includes Symphony Client upgrades in addition to Device Packs. <a href="#">“ Manage Servers - Client Update” on page 70</a></li> </ul> <p><b>Added:</b></p> <ul style="list-style-type: none"> <li><a href="#">Table 9, "Default Ports," on page 120</a> - Added note: For a complete list of ports, see the Knowledge Base Article: <a href="#">Ports used in Aimetis Symphony</a>.</li> </ul> <p><b>Revised:</b></p> <ul style="list-style-type: none"> <li><a href="#">“Figure 30. View Detailed Events - Usernames joined by underscore indicates two users logged on at same time to same machine” on page 52</a> - Not documented in 6.11.0.1 release: <b>View Detailed Events</b> dialog box now shows Key=<b>users</b> for Supervisor Logon with two users</li> </ul>
June 19, 2013	<p><b>Added:</b></p> <ul style="list-style-type: none"> <li>Footnote regarding grey digital I/O map icons - <a href="#">“Adding Digital Input and Output to Maps” on page 60</a>.</li> <li>Added “Edge Storage” and “SD card storage” terms to <a href="#">“ On-Camera Storage (Edge Storage)” on page 77</a> for PDF searches.</li> </ul> <p><b>Removed:</b></p> <ul style="list-style-type: none"> <li>Video capture cards information for analog camera procedures. Capture cards no longer supported. <a href="#">“Device - Analog Cameras” on page 25</a> must use video encoders.</li> </ul>

Table 1. Changes to this manual (Continued)

Date	Description
June 12, 2013	<p><b>Release 6.12</b></p> <ul style="list-style-type: none"> <li>• Table 1, "Storage Options," on page 66 - new <b>Availability</b> section.</li> <li>• New Backup and Restore options "Back up and Restore" on page 124</li> <li>• Set <b>SNMP Retries =2</b> for SNMP using UDP - "Task 3: Test SNMP" on page 111.</li> </ul> <p><b>Revised:</b></p> <ul style="list-style-type: none"> <li>• Added step "4. Enter 127.0.0.1 as the address and edit advanced options to point the program to your read community (for example "public=" community with "READ ONLY" rights):" on page 112 and "Figure 36. Example using iReasoning MIB Browser with Address field and Advanced options dialog box" on page 112 in "Task 3: Test SNMP" on page 111</li> <li>• Added important note about Overload Protection: "Important: CPU overload protection works if you are using a file storage device (for example, NAS) instead of block storage (such as SAN or a local disk) because the pool of storage does not follow the camera when it is moved. If you have central storage (with a NAS), the storage is always accessible from any server." on page 69</li> <li>• Added important note about Failover: "Important: Failover works if you are using a file storage device (for example, NAS) instead of block storage (such as SAN or a local disk) because the pool of storage does not follow the camera when it is moved. If you have central storage (with a NAS), the storage is always accessible from any server." on page 76</li> <li>• <b>Frame Rate Variance</b> term correctly displayed in <b>General Settings</b>: "Figure 11. General Settings dialog box" on page 81. See also KB article: <a href="https://www.aimetis.com/Xnet/KB/KBArticleView.aspx?ID=10219">https://www.aimetis.com/Xnet/KB/KBArticleView.aspx?ID=10219</a></li> <li>• <b>Device Tree Synchronization</b> section removed from <b>General Settings</b> in <b>Server Configuration</b> - "Figure 11. General Settings dialog box" on page 81, "Table 3. General Settings dialog box options" on page 82</li> </ul>
May 2013	<p><b>Release 6.11.1</b></p> <ul style="list-style-type: none"> <li>• SMTP server - User can define which port to use for the SMTP server Table 3, "General Settings dialog box options," on page 82, "Figure 11. General Settings dialog box" on page 81</li> <li>• Table 3, "General Settings dialog box options," on page 82 - Option in <b>User Connections</b> section renamed to <b>Do not allow more than one concurrent connection per user</b></li> <li>• Windows 8 and Windows Server 2012 operating systems supported: "Table 1. SERVER Operating Systems - Windows" on page 7, "Table 2. CLIENT Operating Systems - Windows" on page 8</li> </ul> <p><b>Revised:</b></p> <ul style="list-style-type: none"> <li>• "Small Deployments" on page 3</li> </ul>

Table 1. Changes to this manual (Continued)

Date	Description
March 2013	<p><b>Release 6.11</b></p> <ul style="list-style-type: none"> <li>• Clarified Task - <a href="#">“Adjust the Video Wall layout and control”</a> on page 96</li> <li>• Load/Save Video VideoWall layout <a href="#">“Save Current Video Wall Layout/Load Current Video Layout”</a> on page 102</li> <li>• Security Configuration - Symphony Users Devices tab - mentioned new Talk through camera and Listen to camera options (default allow) <a href="#">“Modifying Access Rights for a Group”</a> on page 40</li> <li>• Symphony supports two-way audio - <a href="#">“Figure 2. Server Configuration for a network camera”</a> on page 16 and <a href="#">“Table 1. Network tab - Field/button description”</a> on page 17</li> <li>• Limit user login to once per server farm - <a href="#">“Figure 11. General Settings dialog box”</a> on page 81 and <a href="#">“Table 3. General Settings dialog box options”</a> on page 82</li> <li>• Video recording schedule in per minute range - <a href="#">“Figure 4. Recording schedule”</a> on page 21, <a href="#">“Table 2. Conditions under which video is recorded”</a> on page 21</li> <li>• Administrator can view which users are using a camera - <a href="#">“Displaying a List of Users Viewing a Camera”</a> on page 105</li> <li>• <a href="#">“Overload Protection”</a> on page 69 <a href="#">“Figure 2. Server Farm”</a> on page 68</li> <li>• <a href="#">“Manage Servers - Client Update”</a> on page 70, <a href="#">“Figure 3. Device Pack Update Installations Managed by Server - Example”</a> on page 70, <a href="#">“Figure 4. Device Pack Installation Update Message to Client User - Example”</a> on page 70</li> <li>• Select narrower time frame for View Detailed Events - <a href="#">“Figure 31. View Detailed Events”</a> on page 106</li> <li>• Email notification option in Notifications dialog changed for clarity to <b>Video or Search deleted</b> from <b>Footage/video deleted</b> - <a href="#">“Figure 14. Notifications”</a> on page 87, <a href="#">“Table 5. Event Descriptions”</a> on page 88</li> </ul> <p>Other</p> <ul style="list-style-type: none"> <li>• Clarified - <a href="#">“Enabling Control Buttons”</a> on page 28 - now EnablePTZButtons parameter</li> <li>• Clarified- <a href="#">“Table 2. Conditions under which video is recorded”</a> on page 21, <a href="#">“Figure 3. Video tab”</a> on page 20</li> <li>• Clarified - <a href="#">“Panoramic Settings group box:”</a> on page 22</li> <li>• Clarified- <a href="#">“Task 2: Configure SNMP Service Security”</a> on page 109</li> <li>• Removed - Saving/Emailing Images from Scheduled versus Manual Reports</li> <li>• First important note in <a href="#">“Single Sign-On (SSO)”</a> on page 32</li> </ul>
December 6, 2012	<p><b>Updated license information:</b> <a href="#">“Symphony Server Licensing”</a> on page 6</p>
November 15, 2012	<p><b>New features in Symphony Release 6.10.1</b></p> <p><b>Video decorations options</b> - <a href="#">“Table 3. General Settings dialog box options”</a> on page 82</p> <p><b>Video Wall</b> - In video wall manager, you can double-click on a panel to display the image in full screen mode. Double-clicking again restores the view to the previous state. <a href="#">“Full Screen Mode”</a> on page 102</p> <p><b>Added:</b></p> <p>More guidelines around NAS and SAN storage. See <a href="#">“Storage”</a> on page 76</p>

Table 1. Changes to this manual (Continued)

Date	Description
September 13, 2012	<p><b>Revised:</b> “ Adding Digital Input and Output to Maps” on page 60. Supported DIO devices now listed in KB article: <a href="http://www.aimetis.com/Support/kbarticle.aspx?ID=10141">http://www.aimetis.com/Support/kbarticle.aspx?ID=10141</a></p> <p><b>Revised:</b> Table 5, "Event Descriptions," on page 88</p> <p><b>Footage/Video deleted</b></p> <p>A user has deleted one of the following:</p> <ul style="list-style-type: none"> <li>• video from the system</li> <li>• a recurring search definition: no footage will have actually been deleted as a result, the recurring search simply will not continue to recur</li> <li>• a search result: the metadata about the result will be removed as well as the .aira and .mpg files saved explicitly for that result (the original footage is untouched)</li> </ul>
August 2012	<p><del>Added:</del></p> <p><del>“Tracking Color” on page 10</del></p>
August 2012	<p>Release 6.10</p> <ul style="list-style-type: none"> <li>• “Prerequisites” on page 7</li> <li>• “ Supervisor Logon” on page 47</li> <li>• “Table 1. Network tab - Field/button description” on page 17 - New option “Support Direct Connect” on page 18</li> <li>• Added “If there are <b>multiple servers in a farm</b>, all the servers must have the same directory tree structure for the path being used to save reports.” in “Reports” on page 137</li> <li>• Updated - “ Saving/Emailing Images from Scheduled versus Manual Reports” on page 125</li> </ul>
May 2012	<p><b>Added:</b></p> <ul style="list-style-type: none"> <li>• Table 1, "Network tab - Field/button description," on page 17 with extensive information on “FPS” on page 18</li> <li>• Link to Knowledge Base article on Access Devices in “Device - I/O” on page 25</li> <li>• Link to Documentation for Cardax and Axiom RBH integration guides in “Device - I/O” on page 25</li> </ul> <p><b>Removed:</b> PTZ Calibration Beta</p>
March 5, 2012	<p><b>Added:</b></p> <ul style="list-style-type: none"> <li>• “Rules in Symphony for Cameras with Digital I/O” on page 24 - Reference to Aimetis Symphony Analytics and Rules Guide</li> <li>• “Rules in Symphony for I/O Devices” on page 27 - Reference to Aimetis Symphony Analytics and Rules Guide</li> </ul> <p><b>Corrigendum:</b></p> <ul style="list-style-type: none"> <li>• “Ban Live Video” on page 44 - removed quotation marks around <b>Value=UserBanGroup</b></li> </ul>

Table 1. Changes to this manual (Continued)

Date	Description
February 28, 2012	Release 6.9.1 New: “Figure 11. General Settings dialog box” on page 81 - now includes SMTP email server authentication “Figure 14. Notifications” on page 87 - SMTP option moved from Notifications to General Settings, and description for new email server authentication option in Table 3, “General Settings dialog box options,” on page 82 “Saving/Emailing Images from Scheduled versus Manual Reports” on page 125 - Images from scheduled Heat Map reports can be saved/emailed. Revised: <ul style="list-style-type: none"> <li>• “Figure 2. Server Configuration for a network camera” on page 16</li> <li>• “Analytics Engines and Analytics Configuration Tabs - Add Video Engines” on page 24 - reference to new Analytics guide</li> <li>• “ To acknowledge an alarm (rule on map):” on page 60</li> </ul>
February 1, 2012	Update to SNMP mib file table based on Symphony 6.9 “Enabling SNMP” on page 108 - See Table 7, “Mib file details,” on page 113 <b>alarm Monitor Category</b> and added <b>Trap</b> column.
January 31, 2012	This is a new guide. Analytics content now in a separate guide.  <b>Release 6.9</b> <b>Added:</b> <ul style="list-style-type: none"> <li>• “Ban Live Video” on page 44 - Setting up user groups</li> <li>• “On-Camera Storage (Edge Storage)” on page 77 - For AXIS cameras</li> <li>• “Managing General Settings” on page 81 - Footage size polling rate</li> <li>• “Reports” on page 137 - File permissions for scheduled and manually run reports</li> </ul> <b>Revised:</b> <ul style="list-style-type: none"> <li>• “Software Overview” on page 2</li> <li>• “Symphony Web Access” on page 136 - More than 100 cameras in <b>Camera Tree</b>, Web Client shows video from cameras as separate pages, navigated by forward and back buttons.</li> </ul>

Table 1. Changes to this manual (Continued)

Date	Description
November 28, 2011	<p><b>Release 6.8</b></p> <p><b>Revised:</b></p> <ul style="list-style-type: none"> <li>• <del>“Figure 31. Camera Tree—How camera IDs are organized—I/O Devices with status displayed” on page 55</del></li> <li>• <del>“Figure 32. Device Tree Configuration dialog box with Options” on page 56</del></li> <li>• <del>“Figure 33. Digital I/O displayed after Show Digital I/O option selected” on page 57</del></li> <li>• “Adding a Map” on page 53</li> <li>• “Placing Cameras on Maps” on page 54</li> <li>• <del>“(Optional) Creating Map Hot Links” on page 55</del></li> <li>• <del>“Deleting a Map, Removing a Camera Icon or a Hot Link” on page 58</del></li> <li>• “Adding Digital Input and Output to Maps” on page 60</li> <li>• “Customizing Digital Input and Output Names” on page 62</li> <li>• “Activating an Output Device Using the Map Context Menu” on page 64</li> </ul> <p><b>Added:</b></p> <ul style="list-style-type: none"> <li>• “Digital I/O Tab” on page 23</li> <li>• “Figure 5. Adding an Axis Camera with Digital I/O invokes a Digital I/O tab in the Server Configuration dialog box” on page 23</li> <li>• “Figure 6. Digital I/O tab for Axis Cameras in Server Configuration dialog box” on page 23</li> <li>• “Figure 7. Axis Camera I/O” on page 24</li> <li>• “Figure 9. HardwareDevice tab - I/O for Phoenix Devices” on page 26</li> <li>• “Figure 10. Phoenix I/O displayed in Camera Tree dialog box” on page 27</li> <li>• <del>“PTZ Camera Calibration—Beta” on page 25</del></li> <li>• “Single Sign-On (SSO)” on page 32</li> </ul> <p><del>Show Digital I/O option in Device Tree Configuration dialog box</del></p> <ul style="list-style-type: none"> <li>• <del>“Figure 31. Camera Tree—How camera IDs are organized—I/O Devices with status displayed” on page 55</del></li> <li>• <del>“Figure 33. Digital I/O displayed after Show Digital I/O option selected” on page 57</del></li> </ul>
Sym 6.7-P-203	
September 7, 2011	<p><b>Added:</b></p> <p>Video and logs should be stored in separate folders... in “Customizing Storage Settings” on page 65.</p>
September 6, 2011	<p><b>Release 6.7.1</b></p> <p><b>Added:</b></p> <ul style="list-style-type: none"> <li>• Table 3, “Conditions under which audio is recorded,” on page 22- <b>Rule Broken</b> option</li> <li>• “Figure 39. Manage Services dialog box” on page 119- <b>Log on as Local System account</b> option</li> </ul>

Table 1. Changes to this manual (Continued)

Date	Description
August 18, 2011	<p><b>Corrigendum</b> Not in release 6.7 <del>“How To Calibrate Your PTZ Camera” on page 23</del></p> <p><b>Clarification</b> ADAM devices only for Digital I/O on maps, see <a href="#">“ Adding Digital Input and Output to Maps” on page 60</a></p>
August 2011	<p><b>Release 6.7</b></p> <p><b>Added:</b> <del>“How To Calibrate Your PTZ Camera” on page 23</del> <a href="#">“Control PTZ Camera Auxiliary Outputs” on page 28</a> <a href="#">“Using Maps” on page 56</a></p> <ul style="list-style-type: none"> <li>• <a href="#">“Icons on Map” on page 56</a></li> <li>• <a href="#">“Adding Rules to Maps” on page 58</a></li> <li>• <a href="#">“ Adding Digital Input and Output to Maps” on page 60</a></li> </ul>
Sym-6.6-P-200.5	
June 14, 2011	<p><b>Added:.</b></p> <ul style="list-style-type: none"> <li>• Link to external reference <a href="#">“HTTPS for AXIS” on page 121.</a></li> </ul> <p><b>Revised:</b> Icon change for Notes and Examples. <a href="#">“Conventions” on page xi.</a> Font change - highly readable for both online and print documents.</p>
Sym-6.5-P-200.7	
December 16, 2010	<p><b>Revised:</b> <a href="#">“Enabling SNMP” on page 108.</a></p>

Table 1. Changes to this manual (Continued)

Date	Description
November 10, 2010	<p><b>Revised:</b></p> <ul style="list-style-type: none"> <li>• Note in “Device - Analog Cameras” on page 25</li> <li>• “Configuring and Managing a Video Wall” on page 90</li> </ul> <p><b>Removed:</b></p> <ul style="list-style-type: none"> <li>• <b>Server Sets</b> information</li> </ul> <p><b>Added:</b></p> <ul style="list-style-type: none"> <li>• “User Authentication” on page 31</li> <li>• “Symphony Security Authentication Mode” on page 31</li> <li>• “Active Directory Authentication Mode” on page 31</li> <li>• “Associating Groups with Active Directory” on page 43</li> <li>• “Advanced Information - Active Directory Associations” on page 53”</li> <li>• “Authentication Mode Set to Active Directory (in Installation Setup Wizard)” on page 53</li> <li>• “Synchronizing with Active Directory” on page 53</li> <li>• “Periodic Synchronization” on page 54</li> <li>• “Logging on to Symphony if your user does not exist in Symphony” on page 53</li> <li>• “Groups Associated with Active Directory” on page 53</li> <li>• “When a user joins another Active Directory group:” on page 55</li> <li>• “Farm Setup” on page 71</li> <li>• “Creating a Farm from Multiple Existing Farms” on page 71</li> <li>• “Buddy System” on page 75</li> <li>• “Redundancy Configuration Settings” on page 75</li> </ul>
October 6, 2010	First version of this document. Symphony v6.5.3

# Preface

## Conventions

Table 1. Symbols and formatting used in this manual

Icon	Caption/Format	Description
	Note	Additional information.
	Example	Example scenario.
	Important	Vital additional instructions or links.
	Caution	You could lose recording footage or you must pay close attention to setting changes.
	<b>Bold, Arial Font</b>	Graphic User Interface term (button, menu, window, option) or keyboard item.
	<i>Italic, Arial</i>	Emphasis, new term, or an external reference.

# Document Suite

**Table 2. Aimetis documents and videos**

Document Name	Links
Symphony Release Notes	<a href="https://www.aimetis.com/Xnet/downloads/documentation.aspx">https://www.aimetis.com/Xnet/downloads/documentation.aspx</a>
Symphony Installation Guide	<a href="https://www.aimetis.com/Xnet/downloads/documentation.aspx">https://www.aimetis.com/Xnet/downloads/documentation.aspx</a>
Symphony Administration Guide	<a href="https://www.aimetis.com/Xnet/downloads/documentation.aspx">https://www.aimetis.com/Xnet/downloads/documentation.aspx</a>
Symphony Analytics Guide	<a href="https://www.aimetis.com/Xnet/downloads/documentation.aspx">https://www.aimetis.com/Xnet/downloads/documentation.aspx</a>
Symphony Client User Guide	<a href="https://www.aimetis.com/Xnet/downloads/documentation.aspx">https://www.aimetis.com/Xnet/downloads/documentation.aspx</a>
Knowledge Base Articles	<a href="http://www.aimetis.com/Support/knowledgebase.aspx">http://www.aimetis.com/Support/knowledgebase.aspx</a>
Case Studies	<a href="http://www.aimetis.com/Solutions/customers-case-studies.aspx">http://www.aimetis.com/Solutions/customers-case-studies.aspx</a>
White Papers	<a href="http://www.aimetis.com/Solutions/whitepapers.aspx">http://www.aimetis.com/Solutions/whitepapers.aspx</a>
Application Video Samples	<a href="https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx">https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx</a>
Recorded Webinars	<a href="http://www.aimetis.com/Events/webinars.aspx">http://www.aimetis.com/Events/webinars.aspx</a>
Product Tour	<a href="https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx">https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx</a>
Supported Video Devices List	<a href="http://www.aimetis.com/Support/supported-video-devices.aspx">http://www.aimetis.com/Support/supported-video-devices.aspx</a>
Licensing	<a href="http://www.aimetis.com/Symphony/default--licensing.aspx">http://www.aimetis.com/Symphony/default--licensing.aspx</a>
FAQ	<a href="https://www.aimetis.com/Xnet/Support/faqs.aspx">https://www.aimetis.com/Xnet/Support/faqs.aspx</a>

# Aimetis Xnet Portal

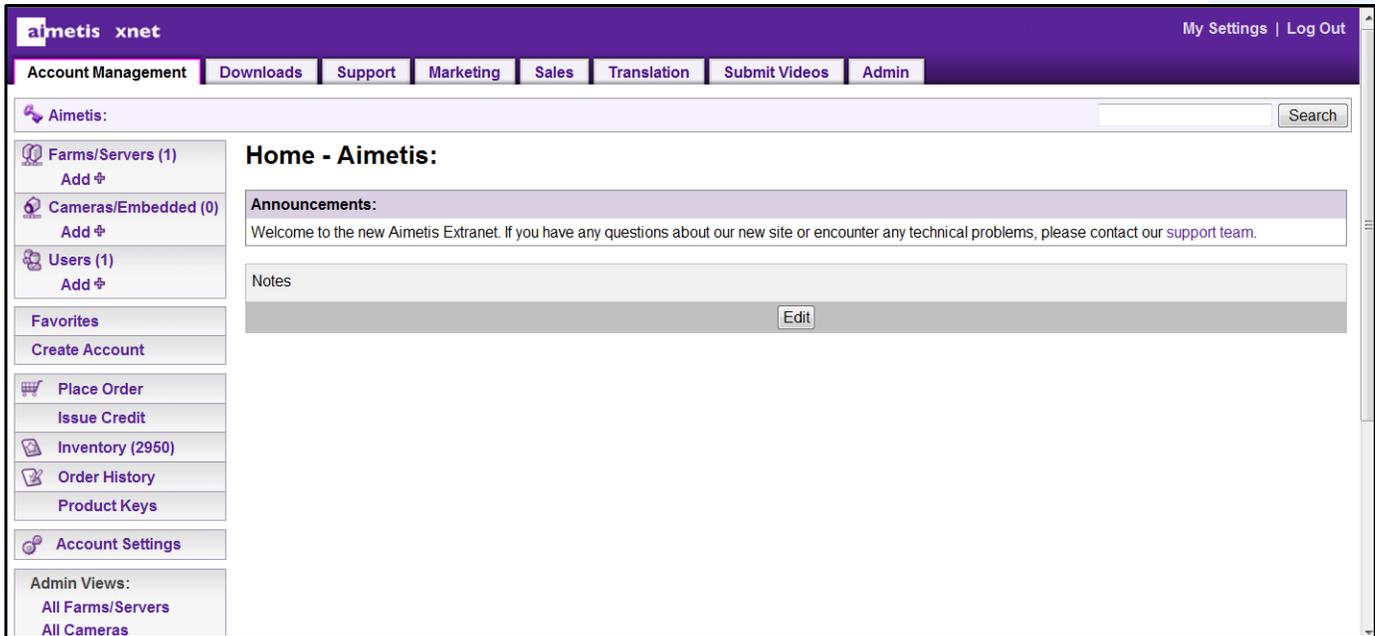


Figure 1. Aimetis Xnet home page

Xnet is the Aimetis Online Portal: [www.aimetis.com/Xnet](http://www.aimetis.com/Xnet)

You can :

- Order Licenses
- Manage Sub-Partner Accounts
- Access Technical Support & Downloads
- Access Sales & Marketing Tools
- Access Aimetis Software Translation



**Note:** Access to tools depends on account type, for example, Distributor, Certified Partner, Authorized Partner, End-User. For instructions, see [Table 3 on page xiii](#).

Table 3. Instructions for using the Xnet

Xnet Instructions	Links
Xnet Training Manual - Resellers	<a href="https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx">https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx</a>
Recorded Webinar - Xnet Training - Distributors	<a href="https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx">https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx</a>

**Table 3. Instructions for using the Xnet**

<b>Xnet Instructions</b>	<b>Links</b>
Recorded Webinar - Xnet Training - Channel Partners	<a href="https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx">https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx</a>
Xnet Training Manual - Distributors	<a href="https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx">https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx</a>
Aimetis Symphony Architectural and Engineering Specification	<a href="https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx">https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx</a>
Hardware Benchmarks guidelines for 10, 20, 40 and 200 camera systems.	<a href="https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx">https://www.aimetis.com/Xnet/Marketing/collateral-library.aspx</a>

# Contact Us

**Table 4. Contact links, addresses, phone numbers**

Contact Type	Description
About Aimetis	<a href="http://www.aimetis.com/Company/default.aspx">http://www.aimetis.com/Company/default.aspx</a>
Contact link	<a href="http://www.aimetis.com/Company/contact.aspx">http://www.aimetis.com/Company/contact.aspx</a>
Support link	<a href="http://www.aimetis.com/Support/default.aspx">http://www.aimetis.com/Support/default.aspx</a>
Americas	Aimetis Headquarters 500 Weber Street North Waterloo, Ontario, Canada N2L 4E9 Phone: +1866-544-2804 or +1 519-746-8888 Fax: +1 519-746-6444
EMEA	Aimetis GmbH Am Prime Parc 7 65479 Raunheim Germany Telefon: +49 (0) 6142 207 98 60 Fax: +49 (0) 6142 207 98 89 <a href="http://www.aimetis.de">www.aimetis.de</a>
Asia - Pacific	Aimetis China Rm. 1328 Yunsun Tower 2025 Zhongshan West Road Xuhui, Shanghai China 200235 Phone: 86-21-6182-6916 Fax: 86-21-6182-6777

---

# Table of Contents

- Overview and Prerequisites ..... 1**
  
- Software Overview ..... 2**
  - Server Computer ..... 2
  - Server and Client Computers ..... 2
  - Client Software Interface ..... 4
  - Server Software Interface ..... 5
  
- Symphony Server Licensing ..... 6**
  
- Prerequisites ..... 7**
  - Server ..... 7
  - Client ..... 7
  - Operating Systems, Database, and Browsers ..... 7
  - Client Prerequisites Installed Automatically ..... 10
  - Server Prerequisites Installed Automatically ..... 10
  
- Symphony Installation and Data Folders ..... 12**
  - Symphony Server ..... 12
  - Symphony Client ..... 14
  
- Chapter 1: ..... 15**
  
- Setting Up Devices ..... 15**
  
- Device - Network (IP) Cameras or Video Servers ..... 16**
  
- Device - Analog Cameras ..... 25**
  
- Device - I/O ..... 25**
  - Rules in Symphony for I/O Devices ..... 27
  
- Control PTZ Camera Auxiliary Outputs ..... 28**
  - Enabling Control Buttons ..... 28
  - Reconfiguring Control Buttons ..... 28

---

<b>Managing Security Profiles .....</b>	<b>29</b>
Adding and Activating Security Profiles .....	30
<b>User Authentication .....</b>	<b>31</b>
Symphony Security Authentication Mode .....	31
Active Directory Authentication Mode .....	31
Single Sign-On (SSO) .....	32
<b>Configuring User Access .....</b>	<b>37</b>
Understanding User Groups .....	38
Adding a New User to a Group .....	39
Making a Group a Member of Another Group .....	40
Modifying Access Rights for a Group .....	40
Managing Users .....	45
<b>Supervisor Logon .....</b>	<b>47</b>
Setting up Supervisor Logon on Your System .....	47
Using Supervisor Logon .....	47
Logging on with Supervisor Privileges .....	51
<b>Advanced Information - Active Directory Associations .....</b>	<b>53</b>
Authentication Mode Set to Active Directory (in Installation Setup Wizard) .....	53
Synchronizing with Active Directory .....	53
Periodic Synchronization .....	54
<b>Using Maps .....</b>	<b>56</b>
Icons on Map .....	56
Adding Rules to Maps .....	58
Acknowledging Rules on Maps .....	60
Adding Digital Input and Output to Maps .....	60
Customizing Digital Input and Output Names .....	62
Activating an Output Device Using the Map Context Menu .....	64

---

<b>Chapter 2:</b> .....	<b>65</b>
<b>Customizing Storage Settings</b> .....	<b>65</b>
<b>Managing Server Farms</b> .....	<b>68</b>
Overload Protection .....	69
Manage Servers - Client Update .....	70
Farm Setup .....	71
Master Server .....	72
Redundant Server .....	72
Failover .....	76
Storage .....	76
Database Configuration .....	77
Symphony Client .....	77
<b>Configuring a Camera Tour</b> .....	<b>78</b>
<b>Managing General Settings</b> .....	<b>81</b>
<b>Specifying Licenses</b> .....	<b>84</b>
Modifying License Settings for a Specific Server .....	85
<b>Using the Manual Configuration Editor</b> .....	<b>86</b>
<b>Setting Up Notifications</b> .....	<b>87</b>
Adding Subscribers to Individual Events .....	88
<b>Integrating 3rd Party Systems with Symphony</b> .....	<b>89</b>
<b>Configuring and Managing a Video Wall</b> .....	<b>90</b>
<b>Viewing Detailed Logs</b> .....	<b>103</b>
<b>Viewing Logins</b> .....	<b>104</b>
Exporting Data from the User Logins Dialog Box .....	104
<b>Displaying a List of Users Viewing a Camera</b> .....	<b>105</b>
<b>Viewing Detailed Events</b> .....	<b>106</b>
<b>Health Monitoring</b> .....	<b>107</b>
Enabling SNMP .....	108
<b>Using the DOS killall Utility with Symphony Services</b> .....	<b>116</b>

---

<b>Receiving Full Diagnostic Information .....</b>	<b>117</b>
<b>Managing Symphony Services .....</b>	<b>118</b>
Starting and Stopping Symphony Services .....	119
<b>Virus Scanning .....</b>	<b>120</b>
<b>Firewalling Symphony .....</b>	<b>120</b>
Publishing Symphony on a Non-Standard Port .....	121
HTTPS for AXIS .....	121
<b>Configuring your Mail Server on Windows 2008 Server R2 .....</b>	<b>122</b>
Using Internal SMTP Server .....	122
Using External SMTP Server .....	123
Windows 7 and Vista - SMTP not included .....	123
<b>Back up and Restore .....</b>	<b>124</b>
Multi-farms only .....	125
Automatic Back up .....	127
Local backup path .....	127
Online back up .....	130
<b>Restore Configuration .....</b>	<b>131</b>
Restore local backup .....	131
Restore from file .....	132
Restore online backup .....	134
<b>Symphony Web Access .....</b>	<b>136</b>
<b>Reports .....</b>	<b>137</b>
File Distribution Permissions for Scheduled versus Manual Reports .....	138

# Overview and Prerequisites

Learn about...
<a href="#">"Software Overview" on page 2</a>
<a href="#">"Symphony Server Licensing" on page 6</a>
<a href="#">"Prerequisites" on page 7</a>
<a href="#">"Server" on page 7</a>
<a href="#">"Client" on page 7</a>
<a href="#">"Operating Systems, Database, and Browsers" on page 7</a>
<a href="#">"Client Prerequisites Installed Automatically" on page 10</a>
<a href="#">"Server Prerequisites Installed Automatically" on page 10</a>
<a href="#">"Symphony Installation and Data Folders" on page 12</a>

## Software Overview

An installation of Aimetis Symphony™ has two components: server software and client software.

### Server Computer

The server computer functions as the intelligence management system that computes the most complicated and intricate tasks.



Figure 1. Server computer

At larger surveillance sites, the server computer may actually be multiple computers linked together to form a Server Farm



Figure 2. Server Farm

### Server and Client Computers

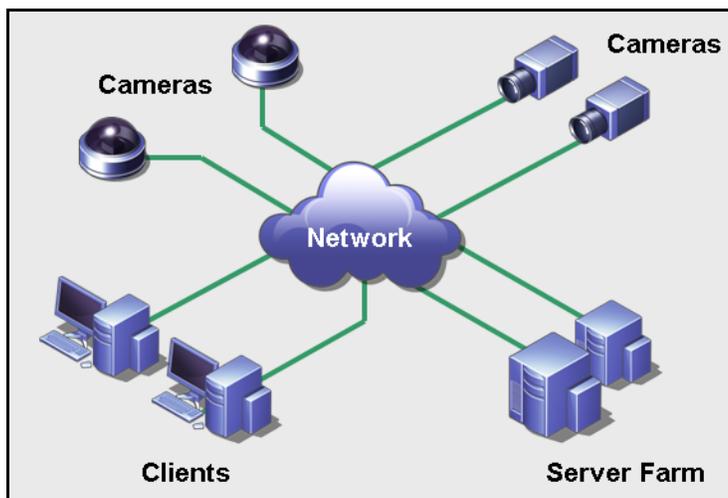


Figure 3. Server Farm with many clients

You can set up clients on many computers or workstations. A typical site would have many client computers connecting to a dedicated server computer. At larger sites, the server computer may actually be multiple computers linked together to form a Server Farm.

## Small Deployments

For small deployments, the server and client computer can be one computer. However, you must consider the following:

- You cannot use multi-views
- The server must be able to handle the additional load, that is, there server has enough CPU and a good video card

Ideally, we do NOT recommend installing the server on client on one computer.

- Regular users should not have access to the server machine because someone might turn off the machine, change the software or configuration on the machine, or even inadvertently crash it.
- Also, using the machine for other tasks may take up a lot of CPU/RAM/network/disk bandwidth and prevent the Symphony server components from working efficiently.

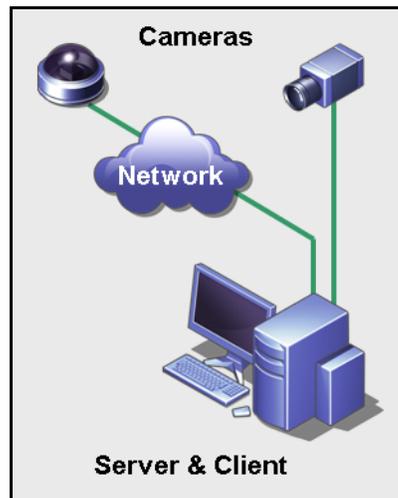


Figure 4. Server and Client on one computer

## Client Software Interface

The client software provides the user interface for all tasks including monitoring, searching, reporting and configuration.

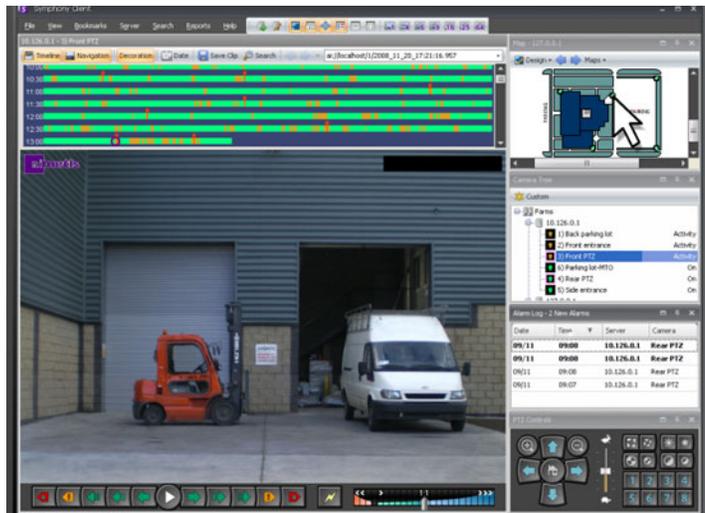


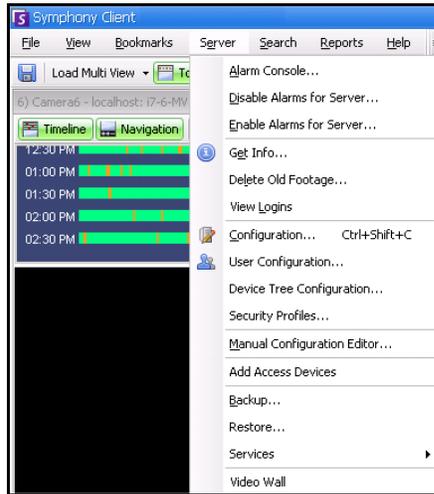
Figure 5. Symphony Client interface

The interface can be arranged over two monitors, and you can even use a Video Wall (a collection of monitors could be on a single wall in a room or in different physical locations).

## Server Software Interface

The server computer is usually and ideally separate from client computers. This is not the case for Aimetis software.

In [Figure 6](#), “Symphony Client” appears in the blue title bar. This is the client interface. You access the server computer through the **Server** menu option in this interface.



**Figure 6. Server menu item in Symphony Client interface**

The interface for both server and client are integrated so that you can connect (configure server tasks) from any client computer in a site. Personnel will often be at client workstations. They must be able to connect to the server (to set up features, for example) from their workstations.

The server software handles all video recording and analytics. It is the intelligence management system that computes the most complicated and intricate tasks.

## Symphony Server Licensing

If you are upgrading an existing installation, ensure that your licenses are eligible for the software version you are installing. If not, contact your Aimetis distributor for an upgrade.

Aimetis Symphony is licensed on a per camera basis. Each physical computer can have multiple Symphony software licenses. The license types are: Standard, Professional and Enterprise. No server or client license fees apply.

License Type	Description
Symphony Server Standard License	Contains all core video management features. For details, see Aimetis <a href="#">Technical Specifications</a> on the Aimetis Web site.
Symphony Server Professional License	Contains all core features of the Standard License plus advanced functionality. This license type is used in large deployments. For details, see Aimetis <a href="#">Technical Specifications</a> on the Aimetis Web site.
Symphony Server Enterprise License	Building on the functionality found in Professional, video analytics can be added on a per camera basis which augments the accuracy of alarm monitoring and includes business intelligence reporting such as people counting. For details, see Aimetis <a href="#">Technical Specifications</a> on the Aimetis Web site.

Licenses can be mixed per physical server, allowing Standard, Pro, and Enterprise to be used per single server. However, there is no advantage of having Standard and Professional licenses mixed on the same server since advanced VMS features will be available only if all licenses are Professional or higher.

## Prerequisites

### Server

- Any Intel CPU or any AMD CPU that supports SSE2 (for example, Opteron)
- 500 Megabytes of free disk space
- At least 1 Gigabyte of RAM

### Client

- 200 Megabytes of free disk space
- 2 GHz or faster processor is recommended
- At least 1 Gigabyte of RAM

## Operating Systems, Database, and Browsers

- **S** = Supported
- **R** = Recommended
- **G** = Recommended for a deployment of greater than 20 cameras
- **N** = Not supported
- **K** = See Knowledge Base on Aimetis Xnet

Table 1. SERVER Operating Systems - Windows

Symphony Product Version	Windows XP SP3 <sup>a</sup>	Windows Server 2003	Windows Vista <sup>a</sup>	Windows Server 2008 R2 <sup>b</sup>	Windows 7	Windows Server 2012	Windows 8
6.5	S	S	S	S,R,G	S,R	N	N
6.6	S	S	S	S,R,G	S,R	N	N
6.7	S	S	S	S,R,G	S,R	N	N
6.8	S	S	S	S,R,G	S,R	N	N
6.9	S	S	S	S,R,G	S,R	N	N
6.10	S	S	S	S,R,G	S,R	N	N
6.11	S	S	S	S,R,G	S,R	S	S
6.12	S	S	S	S,R,G	S,R	S	S

a. See Windows Vista and XP Microsoft End of Support Solution Center

<http://windows.microsoft.com/en-us/windows/help/end-support-windows-xp-sp2-windows-vista-without-service-packs?os=other>

b. Windows 2008 R2 does not install sound components by default. You must install the Desktop Experience Windows component.

Table 2. CLIENT Operating Systems - Windows

Symphony Product Version	Windows XP SP3 <sup>a</sup>	Windows Server 2003	Windows Vista <sup>a</sup>	Windows Server 2008 R2 <sup>b</sup>	Windows 7	Windows Server 2012	Windows 8
6.5	S	S	S	S	S,R,G	N	N
6.6	S	S	S	S	S,R,G	N	N
6.7	S	S	S	S	S,R,G	N	N
6.8	S	S	S	S	S,R,G	N	N
6.9	S	S	S	S	S,R,G	N	N
6.10	S	S	S	S	S,R,G	N	N
6.11	S	S	S	S	S,R,G	S	S
6.12	S	S	S	S	S,R,G	S	S

a. See Windows Vista and XP Microsoft End of Support Solution Center

<http://windows.microsoft.com/en-us/windows/help/end-support-windows-xp-sp2-windows-vista-without-service-packs?os=other>

b. Windows 2008 R2 does not install sound components by default. You must install the Desktop Experience Windows component.

Table 3. Database (SQL Server)

Symphony Product Version	SQL Server 2000	SQL Server 2005	SQL Server 2008	SQL Server 2012
6.5		S	S/R	N
6.6		S	S/R	N
6.7		S	S/R	N
6.8		S	S/R	N
6.9		S	S/R	N
6.10		S	S/R	N
6.11		S	S/R	N
6.12		S	S/R	N

Ensure that the SQL Server database is on a local network (100 Mbps or greater) connected to the servers in the farm.

**Table 4. Browsers**

Symphony Product Version	IE6 <sup>a</sup>	IE7 <sup>a</sup>	IE8 <sup>a</sup>	Firefox 3.x	Safari 5	Chrome 5
6.5			R	*	*	*
6.6			R	*	*	*
6.7			R	*	*	*
6.8			R	*	*	*
6.9			R	*	*	*
6.10			R	*	*	*
6.11			R	*	*	*
6.12			R	*	*	*

a. Limited support for 64-bit version of IE.

\*Limited support (reports, alarms, timeline, JPGs). No live or historical video.

**Table 5. Virtualization Platforms**

Symphony Product Version	Microsoft Virtual PC	VMware Server
6.5	S	R
6.6	S	R
6.7	S	R
6.8	S	R
6.9	S	R
6.10	S	R
6.11	S	R
6.12	S	R

## Client Prerequisites Installed Automatically

The following prerequisites are required by Symphony and (if necessary) will be installed automatically.

**Table 6. Client Prerequisites**

Item	Version	commandline install
XML 6.0 SP1 (x86)	6.10.1129.0	msxml6_x86.msi /qn
XML 6.0 SP1 (x64)	6.10.1129.0	msxml6_x64.msi /qn
Visual C++ 2008 Redistributable Package (x86)	9.0	(components installed by merge modules in installer)
Microsoft .Net 3.5 SP1	3.5 SP1	dotnetfx35 /q /norestart
Visual C++ 8.0 Redistributable (exe install)	8.0 (Service Pack 1 with ATL Security Update, 8.0.50727.4053)	Vcredist_x86_ATLUpdate.exe /q
Microsoft Data Access Components (MDAC) 2.8	2.80.1022.3	Setup.exe
Aimetis Core	6.12.0.0	Msiexec /i Aimetis CoreInstall.msi /q
Microsoft WSE 3.0 Runtime	3.0	msiexec /i "Microsoft WSE 3.0 Runtime.msi" /q
Microsoft VC++ 10.0 CRT (x86)	10.0.40219.1	(components installed by merge modules in installer)
Symphony DevicePack	1.0.6.0	msiexec /i DevicePackLiteClient.msi /q SYMPHONY_PATH="<>install directory">

## Server Prerequisites Installed Automatically

The following prerequisites are required by Symphony and (if necessary) will be installed automatically.

**Table 7. Server Prerequisite**

Item	Version	commandline install
XML 6.0 SP1 (x86)	6.10.1129.0	msxml6_x86.msi /qn
XML 6.0 SP1 (x64)	6.10.1129.0	msxml6_x64.msi /qn
Visual C++ 2008 Redistributable Package (x86)	9.0	(components installed by merge modules in installer)
Microsoft .Net 3.5 SP1	3.5 SP1	dotnetfx35 /q /norestart

Table 7. Server Prerequisite (Continued)

Item	Version	commandline install
Visual C++ 8.0 Redistributable (exe install)	8.0 (Service Pack 1 with ATL Security Update, 8.0.50727.4053)	Vcredist_x86_ATLUpdate.exe /q
Microsoft Data Access Components (MDAC) 2.8	2.80.1022.3	Setup.exe
Aimetis Core	6.12.0.0	Msiexec /i Aimetis CoreInstall.msi /q
Aimetis SNMP	6.11.1.0	SNMPInstallLauncher.exe "INSTALLDIR=[INSTALLDIR]" (Required files, SNMPInstallLauncher.exe, SNMPSetup.exe, SNMPSetup64.exe)
Microsoft SQL Server Express 2008 R2 SP1	10.50.2500.0	SQLEXPR_x86_ENU /Q /HIDECONSOLE /ACTION=Install /INSTANCENAME=AIMETIS /FEATURES=SQLENGINE /SECURITYMODE=SQL /SAPWD=[SQL_SA_PASSWORD] /IACCEPTSQLSERVERLICENSETERMS /SQLSVCACCOUNT="NT AUTHORITY\SYSTEM" /SQLSYSADMINACCOUNTS="Builtin\Administrators"
Windows Installer 4.5	4.5	[program] /quiet /norestart
OPC Core Components 2.00 Redistributable	2.00.2.20	N/A
Microsoft WSE 3.0 Runtime	3.0	msiexec /i "Microsoft WSE 3.0 Runtime.msi" /q
Microsoft VC++ 10.0 CRT (x86)	10.0.40219.1	(components installed by merge modules in installer)
Symphony DevicePack	1.0.6.0	msiexec /i DevicePackLiteServer.msi /q SYMPHONY_PATH="<symphony install directory>"

# Symphony Installation and Data Folders

## Symphony Server

Symphony server stores three kinds of data to your hard disk.

- Binary application files
- Video data
- Configuration information stored in a SQL Server Database.

Symphony is installed by default in

`C:\Program Files\Aimetis\Symphony\`

or on 64 bit OS

`C:\Program Files (x86)\Aimetis\Symphony`

The default path for all data (log files, video, etc.) is

`C:\Program Files\Aimetis\Symphony\data\`

You can change the:

- default installation path during installation of Symphony.
- default data path during the Setup Wizard.

Table 8 provides a summary of key folders

- <AppRoot> denotes installation path
- <DataRoot> denotes data path)

**Table 8. Key Folders**

Path	Description
<AppRoot>\_bin	Binaries for all Aimetis Symphony executables and DLLs
<AppRoot>\_docs	Small .txt files storing alarm instructions and Aimetis.com's IP address
<AppRoot>\_tools	Tools and utilities that Aimetis Support Specialists use to diagnose system problems
<AppRoot>\_Scripts	Scripts for configuring Symphony. For example, a database schema creation script for manually creating the Symphony database
<AppRoot>\WebRoot	Web files & binaries
<DataRoot>\_footagearchive	Video data recorded from all cameras
<DataRoot>\_images	A cache of JPEG images generated from the footage
<DataRoot>\_logs2	All server log files useful for debugging and diagnosing problems.
<DataRoot>\_searches	Stored searches. These files will not be automatically cleaned and searches must be manually deleted by user
<DataRoot>\_signals	Timeline data (green, yellow, red)

**Table 8. Key Folders (Continued)**

Path	Description
<DataRoot>\_signals2	XML metadata for searches and reports
<DataRoot>\Reports	Location for generated reports. Depending on write-permissions, a generated report will be stored in the \Data\Reports folder on the master server machine. The folder is generated ONLY after a report has been run and saved.
\windows\temp\config_backup\	Location for automatic backups of server configuration

In addition to the folders listed in [Table 8](#), Symphony Server adds the following registry keys:

HKLM\Software\Aimetis

Some configuration data for the server is stored here, such as the database connection string.



**Caution:** It is highly recommended that the <DataRoot> folders are not on the same physical Hard Disk as Windows and <AppRoot>. This is to limit the amount of disk read and writes to the OS disk to prevent catastrophic failure.

---

## Symphony Client

Symphony Client is installed by default in

`C:\Program Files\Aimetis\Symphony Client\`

**Table 9. Key Folders for Client**

Folder	Description
<code>C:\Documents and Settings\%WINUSER%\Application Data\Aimetis\</code>	All client configuration, such as window layouts, general configuration, logs
<code>C:\Documents and Settings\All Users\Application Data\Aimetis\</code>	This folder contains <code>RegisteredFarms.xml</code> and <code>FarmList.xml</code>



**Note:** These paths may be slightly different on different operating system versions.

These files define the farms that have been registered. The default is whatever the client configuration path is set to but you can override this. The paths in [Table 9](#) can be configured via the Aimetis Symphony **Client Settings** dialog box.

- From the **View** menu, select **Settings**.

Two (optional) variables can be used in the path names:

- **%WINUSER%** represents the Windows username of the current user. This is used in the default path so Symphony can store the configuration in the current user's application data folder.
- **%SYMPHONY USER%** represents the Symphony username. This is valid only if credentials are required for login to Symphony.

If a customer prefers to keep these settings global, do not use either of these variables when specifying the paths.

In addition to the folders in [Table 9](#), Aimetis Symphony Client adds the following registry keys:

`HKLM\Software\Aimetis\AiraExplorer`

# Chapter 1

## Setting Up Devices

Three kinds of device types can be added to Symphony Server.

- “Device - Network (IP) Cameras or Video Servers” on page 16
- “Device - Analog Cameras” on page 25
- “Device - I/O” on page 25



**Important:** For a list of supported devices, see <http://aimetis.com/Support/supported-video-devices.aspx>.

If you select a multi-lens camera, multiple licenses will be required. You must contact Sales to be given the difference in licenses.

## Procedure

### To view devices:

- From the **Server** menu, select **Configuration**. The **Configuration** dialog box appears with **Devices** displayed in the right pane.

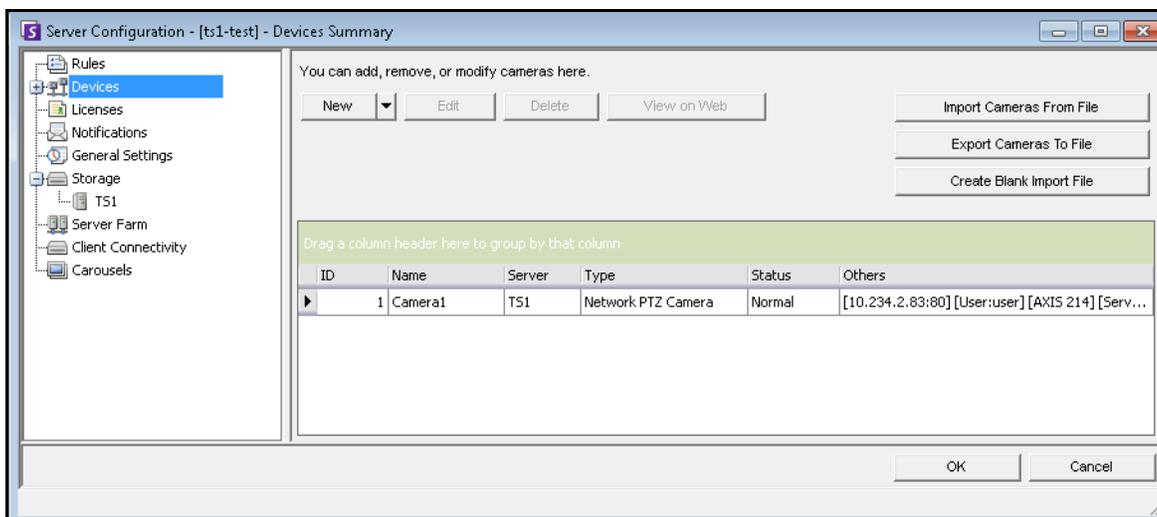


Figure 1. Server Configuration dialog box showing Devices

## Device - Network (IP) Cameras or Video Servers

For network cameras or video servers, you can:

- Add a network camera
- Configure advanced features, for example, recording schedule
- Configure analytics engines (Enterprise license only)

### Procedure

#### To add a new network camera or video server:

1. From the **Server** menu, select **Configuration**. The **Configuration** dialog box appears with **Devices** displayed in the right pane.
2. In the right pane, click **New**. The **Network** tab appears.

The screenshot shows a 'Server Configuration' dialog box with the 'Network' tab selected. The 'Name' field contains 'Camera2'. The 'URL' field has example text: 'e.g. 10.1.2.3 (port 80)', '10.1.2.3:120', 'rtsp://10.1.2.3/mpeg4/1/media.amp (port 554)', and 'rtsp://user:password@10.1.2.3:1666/capture'. The 'Manufacturer' dropdown is set to 'Axis M1031-W'. The 'Camera Type' section has 'Fixed' selected. The 'Resolution' is '640 x 480', 'FPS' is '5', 'Video Format' is 'MPG4', and 'Failover Movability' is 'Movable'. There are checkboxes for 'Support Direct Connect', 'Enable Audio Input', and 'Enable Audio Output'. Buttons for 'Discover Devices', 'View on Web', 'Supported Features', 'Connect to Camera', 'OK', and 'Cancel' are visible.

Figure 2. Server Configuration for a network camera

**Table 1. Network tab - Field/button description**

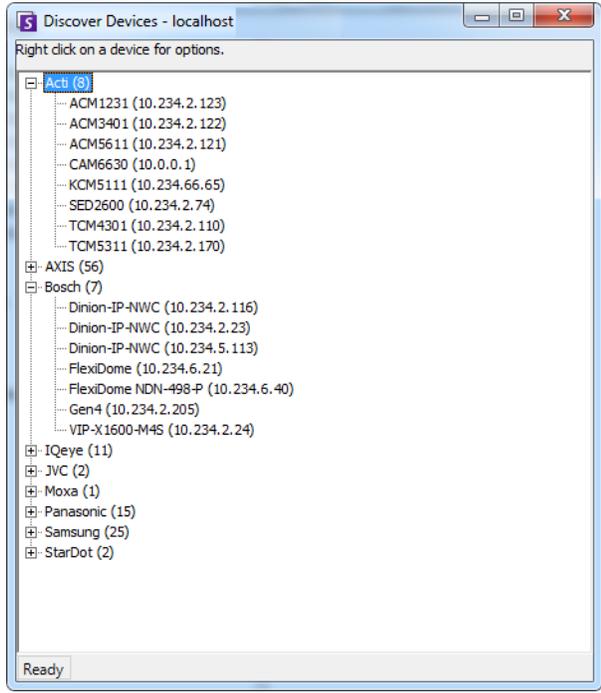
Field/button	Description
<b>Discover Device</b>	<p>Opens the <b>Discover Device</b> dialog box displaying a device tree. Expand the brand name to see a list of devices.</p> 
<b>View on Web Browser</b>	Opens a Web browser to the camera URL (IP address).
<b>Supported Features</b>	Opens the Web browser to the Aimetis Xnet list of supported devices.
<b>Server</b>	The name of the server managing cameras.
<b>Name</b>	Enter an appropriate and easily identifiable name for the camera.
<b>Description</b>	Enter an easily identifiable description. For example, "Camera near front door."
<b>ID/Code</b>	Enter the code or identification you are using to classify and easily identify your cameras.
<b>URL</b>	IP address of the device
<b>Manufacturer</b>	Identify a camera in your system by selecting it by brand name.
<b>Username</b>	Enter a username to access the camera. This may be pre-established based on your company protocol.
<b>Password</b>	Enter a password to access the camera. This may be pre-established based on your company protocol.
<b>Connect to Camera</b>	The Symphony server connects with the camera and automatically detects the <b>Resolution, FPS, and Video Format</b> .

Table 1. Network tab - Field/button description

Field/button	Description
<b>Camera Type</b>	Select one of the options: <b>Fixed</b> , <b>PTZ</b> , or <b>Video Server</b>
<b>Fixed</b>	Fixed camera type.
<b>PTZ</b>	A <b>Pan-Tilt-Zoom</b> type camera.
<b>Video Server</b>	For a device that uses COAX input (from an analog camera), has a compressor, and network port as output.
<b>Resolution</b>	Various resolutions, for example, 160x120, 176x144, 240x180, 320x240, 480x360, 640x480
<b>FPS</b>	<p>Frames Per Second</p> <p><b>Example Scenario:</b></p> <ul style="list-style-type: none"> <li>On-camera <b>FPS = 5</b></li> <li>User selects a video analytic with a default FPS (or chooses an FPS) that is different from the on-camera setting, for example <b>FPS = 8</b></li> </ul> <p><b>Results:</b></p> <ul style="list-style-type: none"> <li>If camera synchronizes with Symphony settings, then <b>FPS=8</b> will be used for streaming from cameras, decompression, video analysis, writing to disk, live video, historical recording, and searches. <ul style="list-style-type: none"> <li>If <b>Video Format = MJPG</b> <ul style="list-style-type: none"> <li><b>FPS=8</b> will be used for streaming from camera, decompression, and video analytics.</li> <li><b>FPS=5</b> will be used for writing to disk, live video, historical recording, and searches.</li> </ul> </li> </ul> </li> <li>If camera does NOT synchronize with Symphony settings, then the on-camera FPS dictates, regardless of the setting in Symphony. As such, in our example, <b>FPS=5</b> will be used for streaming from cameras, decompression, video analysis, writing to disk, live video, historical recording, and searches.</li> </ul>
<b>Video Format</b>	Various formats based on camera type: MJPG, H264, H264 Unicast, H264 Multicast, H264 Over TCP, H264 Over HTTP, H264 over HTTPS
<b>Failover Movability</b>	<p>If set to <b>Movable</b>, then this device can move to another server in the farm during failover.</p> <p>If set to <b>Unmovable</b>, then the device cannot be moved. Any device that requires access to resources available only on a single server (for example, COM port, special SDK or drivers) is unmovable. All others are typically movable.</p>
<b>Enable audio streaming</b>	Depending on camera, allows live audio.
<b>Support Direct Connect</b>	Depending on camera, allows direct connection to camera versus via server when <b>View&gt;Settings&gt;Video</b> tab, <b>Direct connect to camera</b> check box also selected.
<b>Enable Audio Input</b>	Depending on camera design, allows user to speak through the camera.
<b>Enable Audio Output</b>	Depending on camera design, streams live audio from the camera.

## Procedure

---

### Network Tab - Identify a New Network Camera

#### Task 1: Name a new network camera:

1. In the **Name** field, enter an appropriate and easily identifiable name for the camera.
2. In the **Description** field, enter an easily identifiable description. For example, "Camera near front door."
3. (Optional) In the **ID/Code** field, enter the code or identification you are using to classify and easily identify your cameras.

#### Task 2: Locate the camera on the network

1. Enter an IP address in the **URL** field or click **Discover Devices** to locate devices (the IP address) on the network. The **Discover Devices** dialog box opens displaying a device tree.
2. Expand the brand name to see a list of devices.
3. Right-click on a device and select **Connect to Symphony**. The IP address of the device is now displayed in the **URL** field.
4. Enter a **Username** and **Password** for the device. (This may be automatically displayed.)

#### Task 3: Automatically or Manually determine the device specifications:

##### Automatically:

1. Click **Connect to Camera**. The **Camera Type** and values for **Resolution**, **FPS** and **Video Format** are automatically detected and displayed.

##### Manually:

1. From the **Manufacturer** list, select the brand or manufacturer of the camera.
2. Select the **Camera Type**, and set the **Resolution**, **FPS** and **Video Format** appropriately.

#### Task 4: Specify Failover Movability

1. From the **Failover Movability** drop-down list, specify whether the device will automatically move to a redundant server under a failover condition.
  - If set to **Movable**, then this device can move to another server in the farm during failover.
  - If set to **Unmovable**, then the device cannot be moved. Any device that requires access to resources available only on a single server (for example, COM port, special SDK or drivers) is unmovable. All others are typically movable.

## Procedure

### Video Tab - Configure Advanced Features

#### To configure advanced features:

1. Click the **Video** tab. From the **Record Video** and **Record Audio** lists, select a condition or schedule when Symphony should record video and audio on a specific camera. For options, see [Table 2, "Conditions under which video is recorded," on page 21](#) and [Table 3, "Conditions under which audio is recorded," on page 22](#). The options are available only if Symphony has detected that a recording feature is supported by your camera.
2. By default, video is recorded 15 seconds before and after an event. You can adjust this amount by entering a value in seconds in the **Pre Event** and **Post Event** fields.
3. The **Change Frame Rate On Alarm** option is available only if Symphony has detected this feature is supported by your camera.

The screenshot displays the 'Video' configuration tab within a software interface. At the top, there are four tabs: 'Network', 'Video', 'Analytics Engines', and 'Analytics Configuration'. The 'Video' tab is active. Below the tabs, the 'Recording' section contains a 'Record Video' dropdown menu set to 'Schedule & Motion Detected By', a 'Set Schedule' button, and input fields for 'Pre Event' (15 seconds) and 'Post Event' (15 seconds). There is an unchecked checkbox for 'Change frame rate on alarm to' followed by an empty input field and 'FPS'. Below this, a box contains 'Video Quality kilobits/sec' (300) and 'Key frame interval' (25). The 'Misc' section features an 'Add A New Stream' button, a checked checkbox for 'Colour camera', a 'Rotate Degrees' dropdown set to '0', and a 'Maximum Locked Minutes' dropdown set to '5'. The 'Panoramic Settings' section has an unchecked checkbox for 'Enable panoramic technology'.

Figure 3. Video tab

**Table 2. Conditions under which video is recorded**

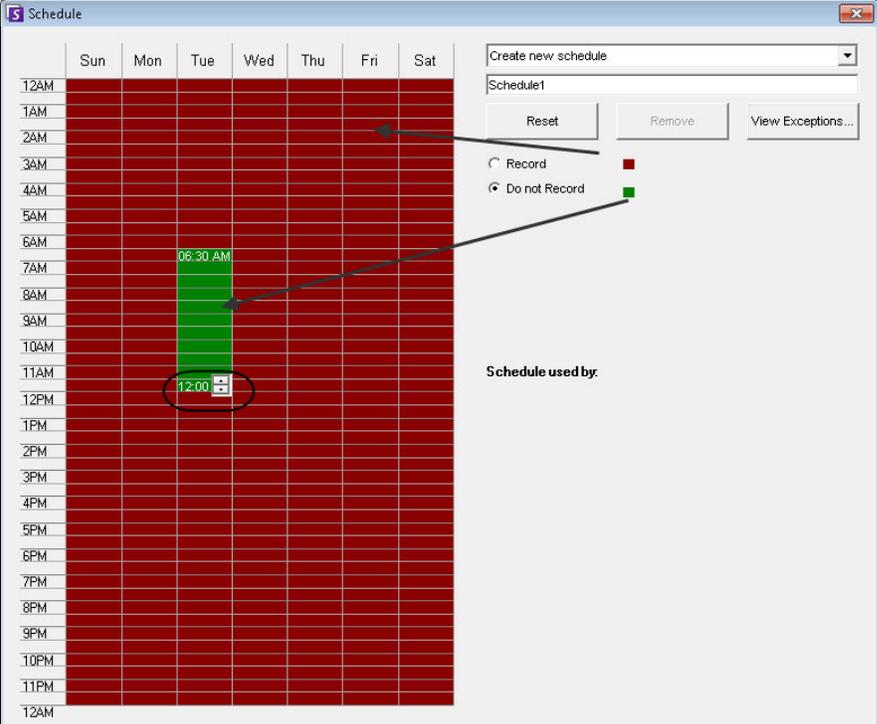
Option	Available for	Symphony records video...
Always	All video cameras	For this specific camera
Schedule	All video cameras	<p>On the schedule you specify.</p> <ol style="list-style-type: none"> <li>1. Click <b>Set Schedule</b>. The <b>Schedule</b> dialog box opens.</li> <li>2. By default, the <b>Do not record</b> option is selected. Using your mouse, click on the date and time intervals you do NOT want video recorded (green) and click <b>OK</b>.</li> </ol> <ul style="list-style-type: none"> <li>• You can set recording schedules to per minute ranges. Click on at least two squares in one column. Hover your mouse over the first square or the last square in the column (earliest or latest hour interval). Arrow range buttons appear. Click the arrows to change times to per minute ranges.</li> </ul>  <p style="text-align: center;"><b>Figure 4. Recording schedule</b></p>
Schedule and Motion Detected by PC	When motion detection video engine also selected	On motion but only during the time period you specify.
Tracked Motion Detected by PC	When motion detection video engine also selected	If objects are tracked through the scene (for example, a person or vehicle moving through the scene is tracked as motion, but moving tree branches should not be tracked and therefore video would not be recorded)
Pixel Changes Detected by PC	When motion detection video engine also selected	Whenever pixel changes are detected. <b>Note:</b> A tree moving in a heavy wind could cause pixel changes and therefore cause Symphony to record video

Table 2. Conditions under which video is recorded (Continued)

Option	Available for	Symphony records video...
Motion Detected by Camera	Cameras which support Motion Detection	Using motion detection capabilities inside the network camera itself, and not using a video analytic engine from Symphony (quality of motion detection similar to <b>Pixel Changes</b> )
Schedule & Motion Detected by Camera	Cameras which support Motion Detection	Records if motion detected during a specific time interval as defined by user. Using motion detection capabilities inside the network camera itself, and not using a video analytic engine from Symphony
Never	All video cameras	Never records video unless specified to be recorded in a <b>Rule</b>

Table 3. Conditions under which audio is recorded

Option	Symphony records audio...
Never	Never records audio unless specified to be recorded in a <b>Rule</b>
Same as video	Records audio based on the video record settings in <a href="#">Table 2</a>
Rule Broken	Records audio only when an alarm is triggered

### Misc group box:

- To add another video stream for the current network device, click **Add a new Stream**.
  - If the network device allows additional network video streams, the streams can be added from the same physical device. Useful when one video is defined for recording and another for live video.

The video recording options available are the same as defined by the default stream (Table 2 on page 21). Video resolution can also be defined independently for the additional stream(s).

- To rotate the picture, select a value from the **Rotate Degrees** field.
- If you are using a PTZ camera, select a value in the **Maximum Locked Minutes** field to specify how long a PTZ camera should remain in its current position before it returns to its preset (Home Position).

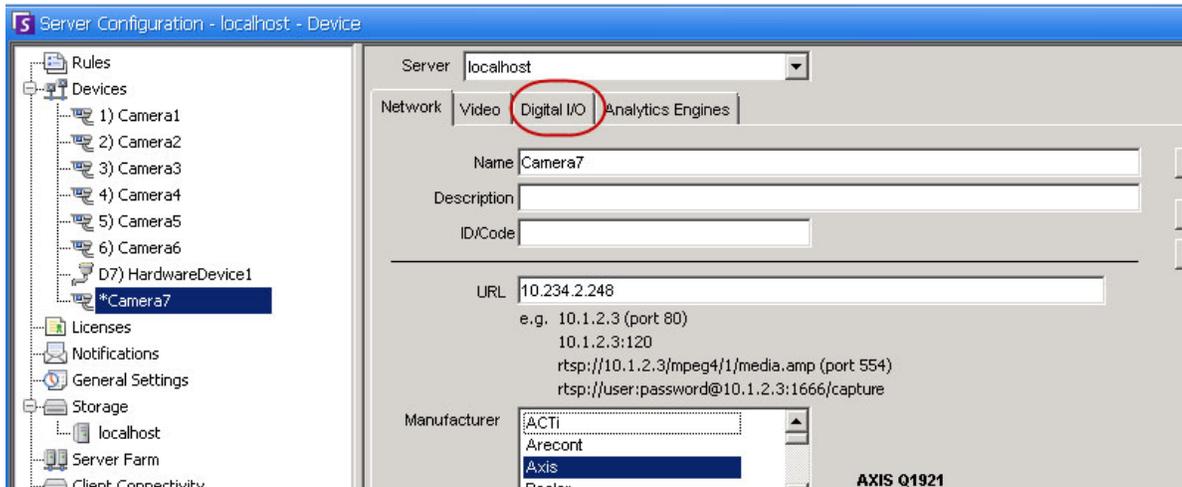
### Panoramic Settings group box:

- Only for 360-degree camera lenses. To de-warp 360-degree video, select the **Enable panoramic technology** check box. From the drop-down lists, select the camera brand and a **Position** (wall, ceiling, ground) for how the camera is mounted.
- Click **Apply** to save your settings and move onto the **Analytics Configuration** tab, or click **OK** to save settings and close the dialog without configuring the selected video analytics engines (default configuration settings will be used).

## Procedure

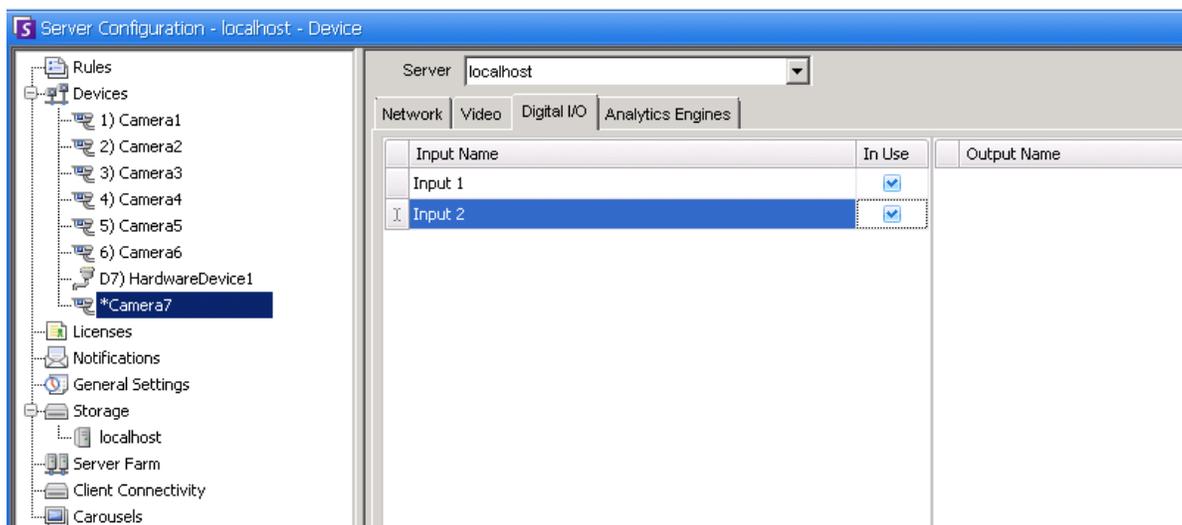
### Digital I/O Tab

For Axis cameras with digital I/O, the **Digital I/O** tab appears.



**Figure 5. Adding an Axis Camera with Digital I/O invokes a Digital I/O tab in the Server Configuration dialog box**

1. Click the **Digital I/O** tab.
2. (Optional) You can change the input and output names by clicking on each row and typing new text.
3. Select the **In Use** check boxes for each I/O as necessary.



**Figure 6. Digital I/O tab for Axis Cameras in Server Configuration dialog box**

4. Activate (or deactivate) each Output for the Axis camera as necessary in the **Camera Tree** dialog box.

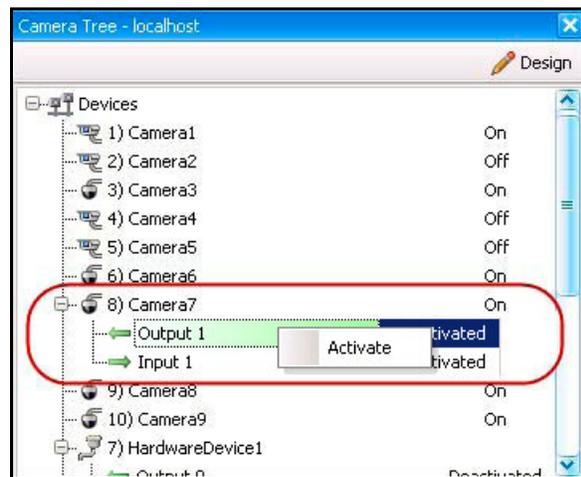


Figure 7. Axis Camera I/O

## Rules in Symphony for Cameras with Digital I/O

Rules in Symphony define what **Event** constitutes an alarm in the real world (for example, a perimeter breach or even suspicious behavior around a car) and what **Action** to take after an alarm is raised (for example, whether to send a security guard to the location in question).

Alarm inputs include Video Motion Detection from network cameras and external I/O devices. To set up rules for I/O devices, see the **Rules** section in the Aimetis Symphony Analytics and Rules Guide.

## Procedure:

### Analytics Engines and Analytics Configuration Tabs - Add Video Engines

By selecting the **Analytics Engines** tab, individual video analytics engines can be added to each camera. An **Enterprise license** is required to enable video engines in the **Analytics Engines** tab. This step is necessary only if video analytics are to be configured on this camera.

- For information on how to configure and select the video analytic engines, see the Aimetis Symphony Analytics and Rules Guide
- For information on licensing, see [“Symphony Server Licensing” on page 6](#)

## Device - Analog Cameras

Use a video encoder (a network device that converts analog video to digital video).

Symphony connects to the video encoder the same way it connects to a network camera; therefore, follow the steps in “[Network Tab - Identify a New Network Camera](#)” on page 19.

## Device - I/O

Input/output, or I/O, refers to the communication between an information processing system (such as a computer running Symphony), and the outside world (possibly a human, or another information processing system such as an access control system).

Inputs are the signals or data received by Symphony, and outputs are the signals or data sent from it.

- Symphony supports ADAM, Phoenix, Axis Camera I/O, and PSA devices. For a complete list of support I/O devices, visit <http://aimetis.com/Support/supported-video-devices.aspx>
- For ADAM devices, see the Knowledge Base article: <https://www.aimetis.com/Xnet/KB/KBArticleDetails.aspx?ID=10072>
- For Gallagher and Axiom RBH, see the integration guides: <https://www.aimetis.com/xnet/Support/documentation.aspx>

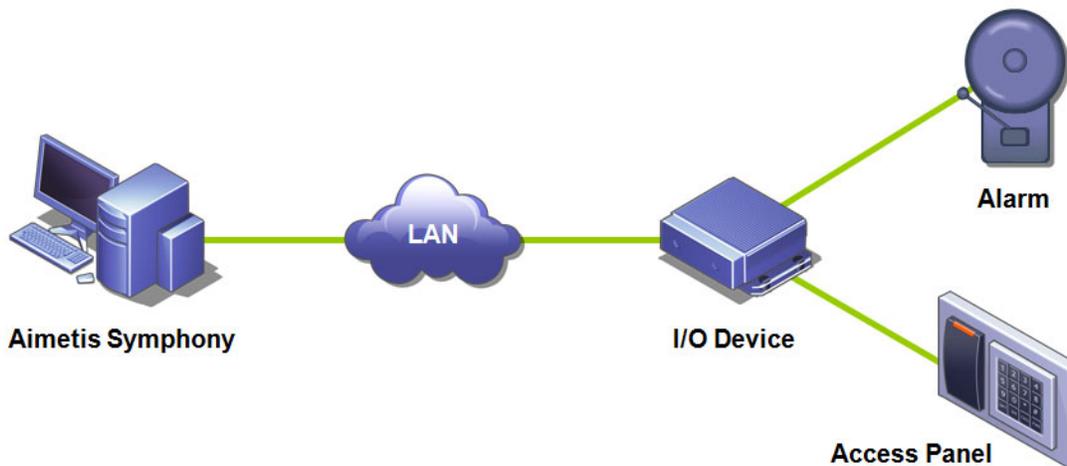


Figure 8. PC sends a signal through the LAN. The I/O device on the LAN receives the signal and then is wired to an alarm in one input or an alarm panel in another input.

## Procedure

### To add and configure an I/O device:

1. From the **Server** menu, select **Configuration**. The **Configuration** dialog box appears with **Devices** displayed in the right pane by default.
2. In the right pane, click the arrow beside the **New** button. Select **Add a Hardware Device** and then one a device. (The recommended device is the **Advantech (Adam) 6060**.)The **HardwareDevice** tab appears for the device type selected.

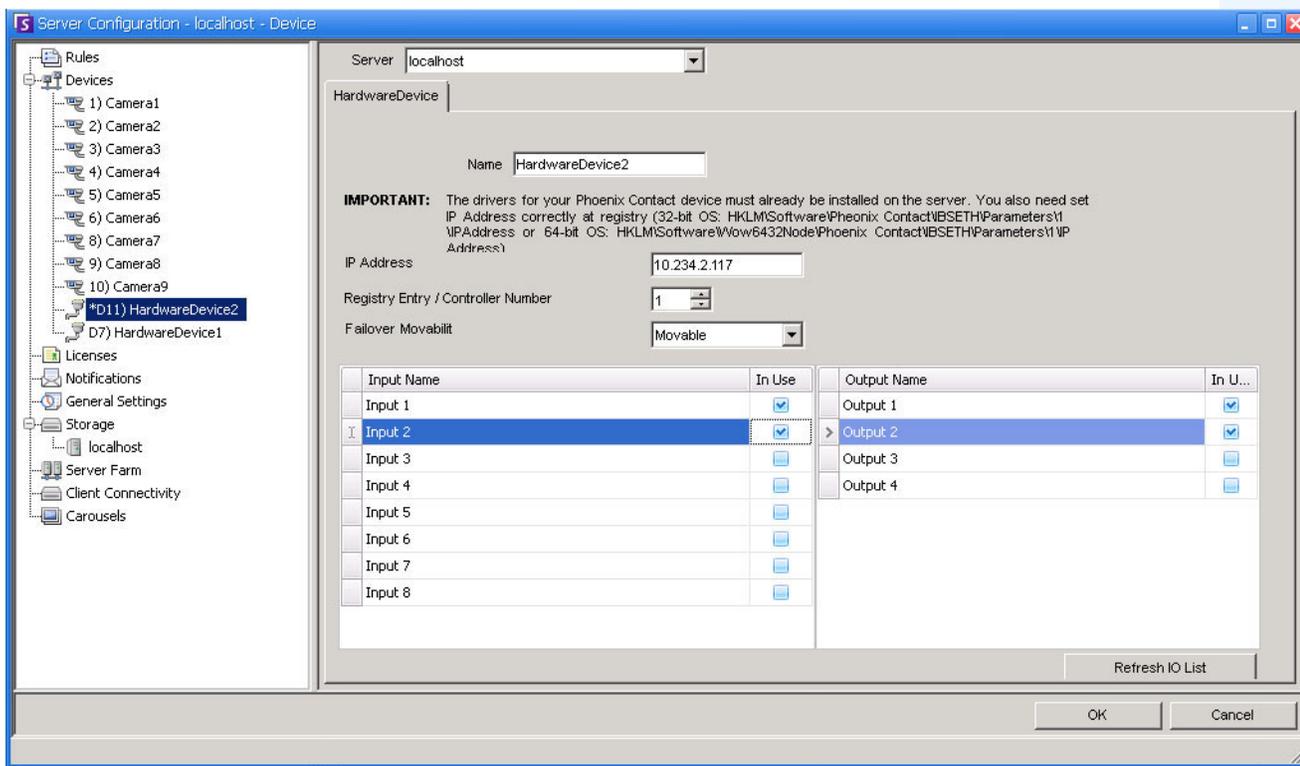


Figure 9. HardwareDevice tab - I/O for Phoenix Devices

3. In the **Name** field, enter a name you want to use for this device.
4. Depending on the I/O device type selected, various fields are displayed:
  - **IP address** - If an IP-based I/O device is configured, enter the **IP Address** of the device.
  - **Module** - Select an Advantech model (6050, 6060, 6066) from the drop-down list.
  - **Registry Entry/Control Number** - For Phoenix. Field populated by default.
  - **COM Port** and **Baud Rate** - If an I/O device is connected to the serial connection of the server, you must configure the **COM Port** address and **Baud Rate** properly.
5. From the **Movability** drop-down list, specify whether the device will automatically move to a redundant server under a failover condition.
  - If set to **Movable** then this device can move to another server in the farm during failover.
  - If set to **Unmovable** then the device cannot be moved. Any device that requires access to resources available only on a single server (for example, COM port, special SDK or drivers) is unmovable. All others are typically movable. For more information, see Server Farm.

6. Activate (or deactivate) each Output as necessary in the **Camera Tree** dialog box.

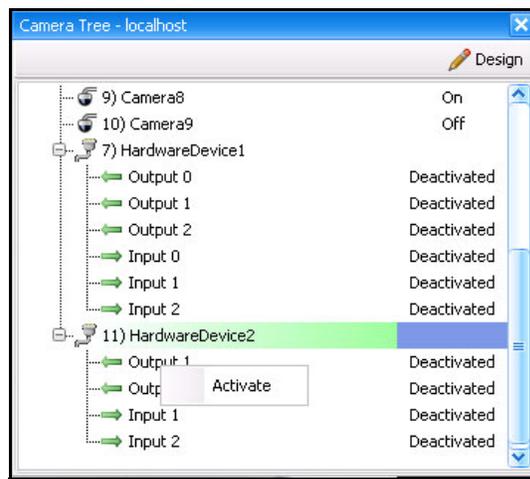


Figure 10. Phoenix I/O displayed in Camera Tree dialog box

## Rules in Symphony for I/O Devices

Rules in Symphony define what **Event** constitutes an alarm in the real world (for example, a perimeter breach or even suspicious behavior around a car) and what **Action** to take after an alarm is raised (for example, whether to send a security guard to the location in question).

Alarm inputs include Video Motion Detection from network cameras and external I/O devices. To set up rules for I/O devices, see the **Rules** section in the Aimetis Symphony Analytics and Rules Guide.

## Control PTZ Camera Auxiliary Outputs

Symphony Client includes two buttons (**Aux on**) and (**Aux off**) on the **PTZ Controls** interface. You can use these buttons to activate and deactivate auxiliary functions on the device, such as a wiper. The first button (**Aux on**) can start the wiper. The second button (**Aux off**) can stop the wiper.

### Enabling Control Buttons

By default, the control buttons are hidden in the **PTZ Control** interface.

### Procedure

---

#### To enable **Aux on** and **Aux off** buttons in the **PTZ Controls** interface:

1. Edit the %appdata%\Aimetis\acc.ini
2. Add the following parameter under [Main]:  
`EnablePTZButtons=True`
3. Save the acc.ini file and restart Symphony Client for the changes to take effect.

### Reconfiguring Control Buttons

The commands for the buttons can be reconfigured using the **Manual Configuration Editor**.

### Procedure

---

#### How to reconfigure the **Aux on** and **Aux off** buttons:

1. Start Symphony Client.
2. From the **Server** menu, select **Manual Configuration Editor**.
3. Click **Add a new setting...** in the first row to activate the cells.
4. For the **Aux on** button, enter the following in the first row: **Type**=Camera, **Section**=PTZ, **ID**=<your camera id>, **Key**=StartWiper, **Value**= ff01000900010b (example value).
5. For **Aux off** button, enter the following in the another row: **Type**=Camera, **Section**=PTZ, **ID**=<your camera id>, **Key**=StopWiper, **Value**= ff01000b00010d (example value).
6. To confirm your entry, click the **Action** cell.
7. Click **OK**.

You can modify these settings any time. Simply find the Camera **ID** and look for the StartWiper or StopWiper values under the **Key** column.

## Managing Security Profiles

All user-access rights are defined in **Groups** in **User Configuration**.

- Each **Group** can have more than one **Security Profile**. Security profiles allow administrators to change security privileges quickly depending on the situation.
- By default, only one **Security Profile** (called **Default**) is used. In most cases this will be sufficient.
- In some cases it may be useful to define additional security profiles and modify access rights of the **Group** per profile. This allows you to quickly change permissions to resources (such as cameras) in cases of an emergency. For example, under normal conditions a group of users may have access to all cameras, but in an emergency situation access may be temporarily suspended with one security group but given to another.



When the **Security Profiles** for a **Farm** is changed, all servers in the farm are notified, as well as all clients connected to those servers. The farm will remain in that security profile until the active security profile is changed again.

## Procedure

### To view Security Profiles:

- From the **Server** menu, select **Security Profiles**. The **Security Profiles** dialog box appears.

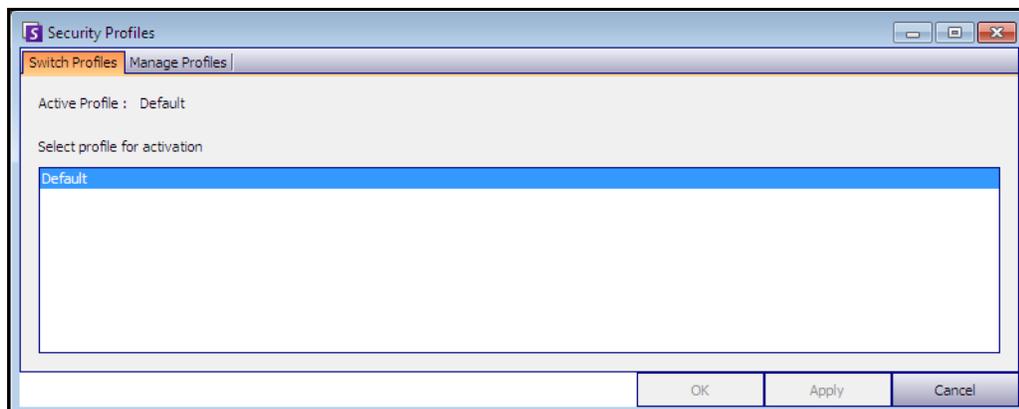


Figure 11. Security Profiles dialog box

## Adding and Activating Security Profiles

### Procedure

---

#### To add a Security Profile:

1. From the **Server** menu, select **Security Profiles**. The **Security Profiles** dialog box appears
2. Click the **Manage Profiles** tab.
3. In the right pane, click **Add**.
4. Click the new field under the **Name** column and enter a name for the new profile.
5. Click the new field under the **Description** column and enter a description of the new profile.
6. Click **Apply** to save changes and then **Close**.

#### To activate a Security Profile:

This will immediately affect user access rights.

1. From the **Server** menu, select **Security Profiles**. The **Security Profiles** dialog box appears
2. In the **Switch Profiles** tab, select the profile for activation.
3. Click **Apply** to save changes. A message appears indicating that the profile is active. Click **Close**.



**Caution:** Access rights are not defined in the **Security Profiles** dialog box. To modify user permissions per Security Profile, configure the appropriate **Group** in **User Configuration**.

---



**Note:** If the Security Profile is changed, remember to change the Profile back in order to restore users to their default permissions.

---

## User Authentication

To connect to a server farm from Symphony Client, a user must be authenticated. Symphony supports two modes of authentication:

- Symphony Security (which is the stand-alone method)
- Active Directory integrated method

Although the authentication mode can be changed, it is generally configured during the initial setup of the farm.



Figure 12. Defining Security Mode during Setup Wizard



To review the Security Mode in the Setup Wizard, from the **Start Menu**, select **Aimetis**, and then **Setup Wizard**. For details, see the **Installation Guide**.

## Symphony Security Authentication Mode

When the authentication mode is set to Symphony **Security**, the credentials (user name and password) are stored in the Symphony database. The password is encrypted for security. When a user attempts to log in, the credentials are compared to the credentials in the Symphony database, and a successful match allows the user to log in. This is the default method and requires no additional configuration.

## Active Directory Authentication Mode

Active Directory integrated mode uses Windows user passwords and as a result, users are not required to remember and maintain different passwords, even if the Windows password changes. Additionally, IT managers do not carry the additional burden of managing users in different applications. If a Windows user account is disabled, that user will not be allowed to log on to Symphony.

When the authentication mode is set to **Active Directory**, the user name is stored in the Symphony database, but not the password. Additionally, a mapping to the Active Directory user is stored (the Security Identifier, or SID). When a user attempts to log on, the credentials are checked against Active Directory. If Active Directory accepts the credentials, the user is allowed to log on.



For Active Directory integrated mode to be used, Professional & Enterprise licenses must be used. A Standard license will restrict access to this feature.

## Single Sign-On (SSO)

Single Sign-On is designed to restrict users from using different PCs with the same user name. It is transparent to the user; there are no specific messages associated with it. When registering to a new farm or editing an existing farm having **Windows Authentication** selected, the following message is displayed in case of failure: **Windows Authentication Failed. You must enter the user and the password.**

SSO works alongside the current/existing Symphony authentication process. Windows authentication is more secure than Symphony authentication; it makes use of the built-in Windows security system. Communication between client and server is made through a WSE 3.0 SOAP Web Service.



**Important:** If users need their registered farms available on any machine on the domain, they must enable roaming user profile (Windows).

Symphony does **not** support cross-domain authentication for SSO.

SSO is designed to restrict users from using different PCs with the same user name; however, a user may *inadvertently* log on multiple times on the same PC.

### Process Flow

1. When Symphony Client connects to a farm, it creates a security token, based on the identity of the currently logged-in Windows user; the user **MUST** have logged-in on the domain account.
2. The security token is sent to the farm/server for authentication.
3. Farm/server verifies that the token is valid and determines the domain account associated with it.
4. Upon success, farm/server sends a session ID back to the client.
5. On failure, the client's farm state changes to **Unauthorized**.
6. In case of failure, the user can login using Symphony credentials:
  - a. In Symphony Client, right-click your farm in **Server List**.
  - b. Select **Edit**. The **Server Login Information** dialog box opens.
  - c. Disable single sign-on: clear the **Windows Authentication** check box.
  - d. Click **OK**.
  - e. Enter user name and password.



**Important:** Multiple Symphony Clients on a single Windows login (each registered with a different user) are needed to run **Live Ban**. As such, **Single Sign On** will not be available for **Video Walls** when also running **Live Ban**.

### Prerequisites

The Single Sign On feature uses the client's domain identity to authenticate to the server; therefore, the client and the server must be in the same security realm. As such, the Single Sign On feature is available only when:

- Client and server machines are logged on to the same domain, and
- The user logs on to the client machine as a *domain user* by using the domain credentials. (A user can log on to a machine *locally* in which case the Single Sign On feature is not available.)

On domains controlled by Windows Server 2008 (or later) and clients running Vista/Windows 7:

- AES256\_HMAC\_SHA1 encryption must be disabled because it cannot be handled by the WSE 3.0 used by Single Sign On. This policy must be enforced by the domain controller and must be set by the IT personnel in charge of the domain.

## Enabling Single Sign-On (SSO)

- “Task 1: In Symphony Client (or manually) enable single-sign on”
- “Task 2: In Symphony Client, change the storage path for the farm registration to a network server” on page 35

### Task 1: In Symphony Client (or manually) enable single-sign on

#### Procedure

##### To enable or disable single sign-on in Symphony Client:

1. In Symphony Client, right-click your farm in the **Server List**.
2. Select **Edit**. The **Server Login Information** dialog box opens.
  - To enable single sign-on, select the **Windows Authentication** check box.
  - To disable single sign-on, clear the **Windows Authentication** check box.
3. Click **OK**.

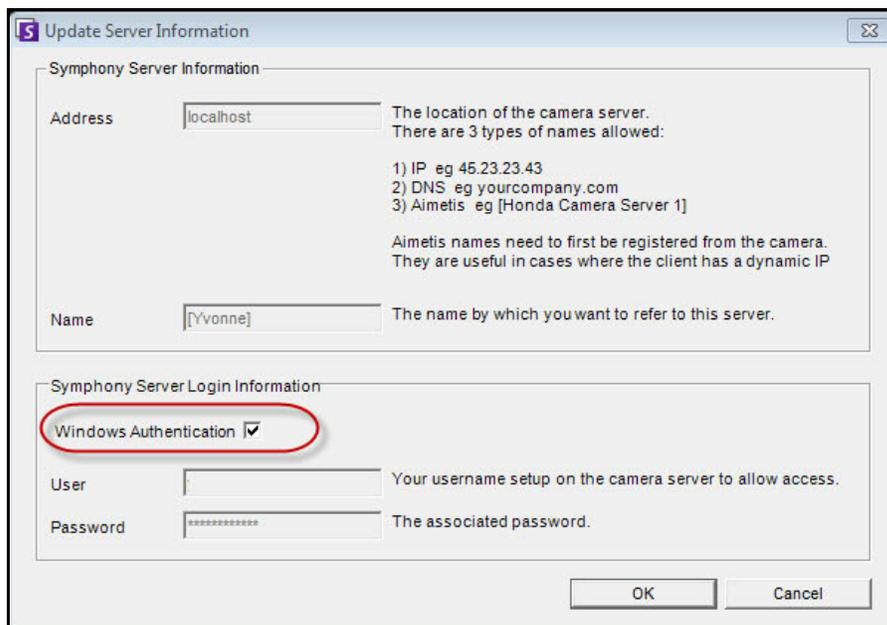


Figure 13. Windows Authentication check box

## Procedure

---

### To enable single sign-on manually:

1. Edit %APPDATA%\Aimetis\RegisteredFarms.xml.

#### Example:

```
<RegisteredFarms>
  <Farm ID="74083">
    <Encryption>6.2</Encryption>
    <Alias>10.234.10.76</Alias>
    <SpecifiedAddress>10.234.10.76</SpecifiedAddress>
    <UserName>MVYITEIRRUhQ</UserName>
    <Password>kjdfldskjflakj</Password>
    <UseWindowsAuthentication>false </UseWindowsAuthentication>
    <Addresses>
      <Address>
        <SpecifiedAddress>10.222.10.73</SpecifiedAddress>
        <IP>10.222.10.73</IP>
        <Port>50001</Port>
      </Address>
    </Addresses>
  </Farm>
</RegisteredFarms>
```

2. Under **<Farm ID = "number">**,
  - To enable single sign-on set **<UseWindowsAuthentication>true </UseWindowsAuthentication>**
  - To disable single sign-on set **<UseWindowsAuthentication>false </UseWindowsAuthentication>**

## Task 2: In Symphony Client, change the storage path for the farm registration to a network server

### Procedure

#### To ensure that farm registration information is stored on a network server:

1. From the **View** menu, select **Settings**. The **Symphony Client Settings** dialog box opens.
2. Click the **Global** tab.

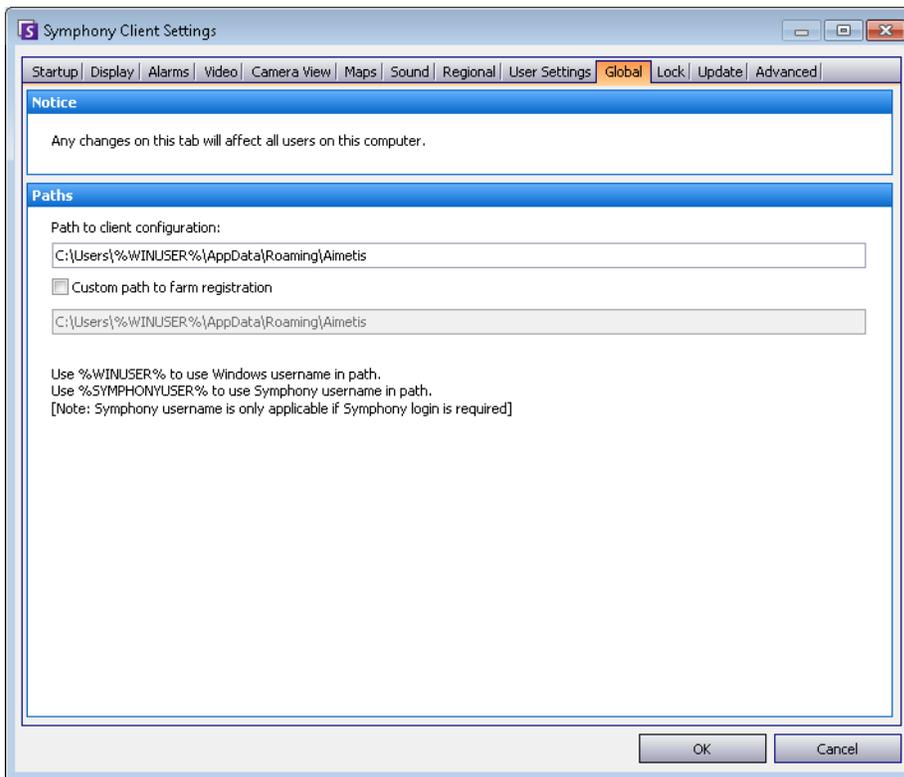


Figure 14. Global tab in the Symphony Client Settings dialog box

3. Select the **Custom path to farm registration** check box.
4. In the next field enter the path on the network where the registration information will be stored for all roaming users.
  - The network server storing all the farm registrations must be accessible from all Clients.

- This is a global setting. All users that login to this Client will use this setting. Use the %WINUSER% variable when configuring this path so that each user has a unique path where the farm registration is stored. The user must have Windows “modify” rights to this folder. This is set only once on each Client machine.



**Important:** It is a security risk to have multiple users share a farm registration.

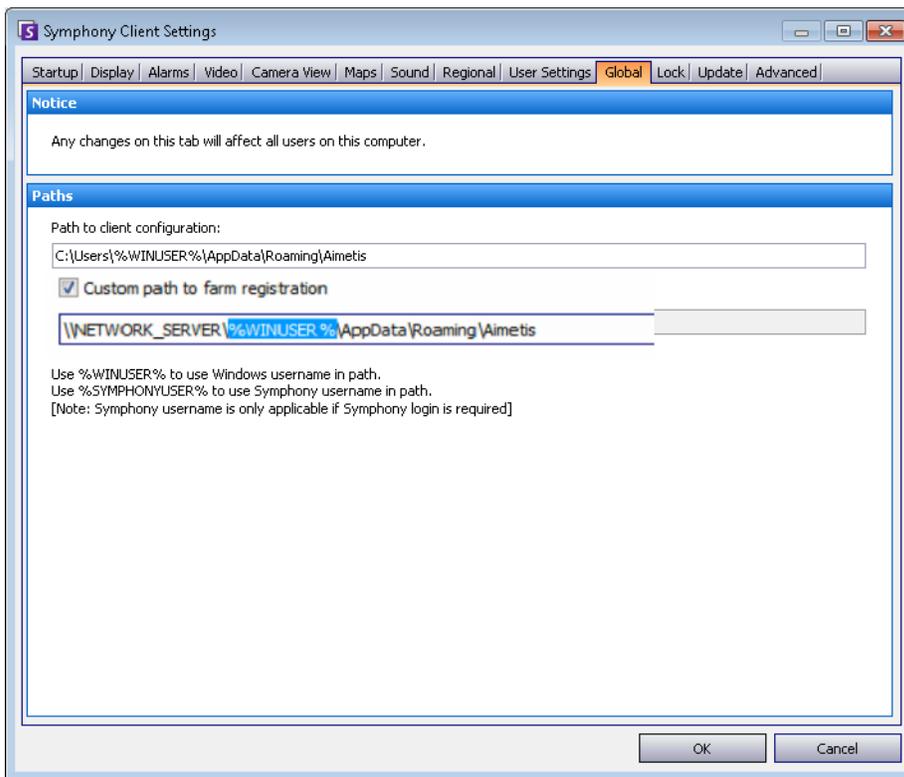


Figure 15. Changing where farm registration information is stored

# Configuring User Access

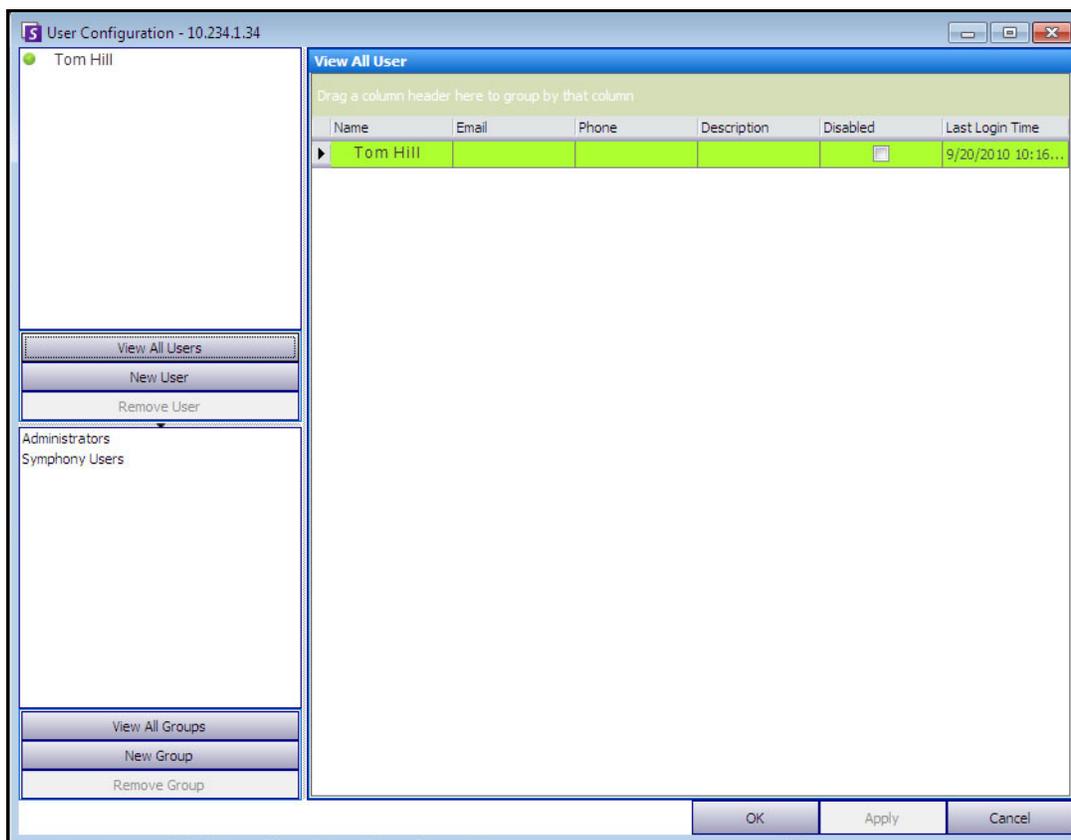
**Groups** and **Users** are managed in the **User Configuration** dialog box.

Users can be created, modified, and deleted from the **User Configuration** dialog box in Symphony Client. Several properties for a user that can be changed, including user name, password, and description.

## Procedure

### To view User Configuration:

- From the **Server** menu, select **User Configuration**. The **User Configuration** dialog box opens.



**Figure 16. User Configuration dialog box**

The **Users** section in the left pane summarizes a list of users on the system. The color of the button beside each user indicates the status of the user:

- green for logged on
- red for disabled
- grey for logged off

The **Groups** section in the lower left pane summarizes all security groups in Symphony.

## Understanding User Groups

The user management system in Symphony employs user groups. This allows administrators to organize the security privileges of users as part of **Groups**. The administrator establishes group security privileges and then assigns users to groups.

- An administrator can create, rename, and delete groups, as well as modify group membership.
- A group may contain users or even other groups.
- Both a user and a group may be in multiple groups.  
(Not allowed: Group A is part of Group B, which is part of Group A.)

By default, there are two User Groups.

- The **Administrators** user group allows users who are a member of this group full access to the system.
- The Symphony **Users** group allows users limited access.

**Group** membership makes the security management of many users easier than managing privileges on a per user basis.

- If a security restriction is applied to a group, this restriction is implicitly applied to all members of that group.
- If users are added to the group at a later date, the same security restrictions automatically apply.
- If users are removed, the security restrictions no longer apply.

## Procedure

### To view an existing User Group:

- From the **Groups** section, select the name of the group. The **Group Information** is displayed in the right pane.

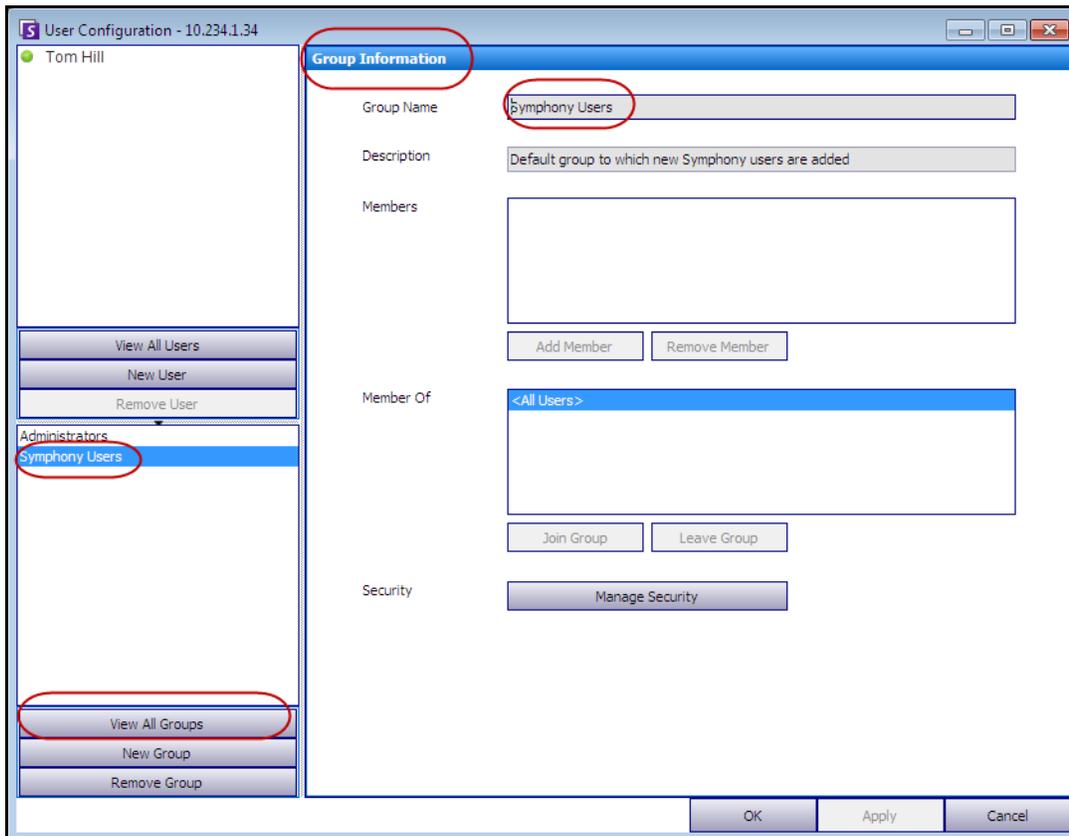


Figure 17. Group Information

## Adding a New User to a Group

### Procedure

#### To add a new User to a Group:

- From the **Groups** section, select the name of the group. The **Group Information** is displayed in the right pane.
- Click **Add Member**. The **User/Group Selection** dialog box opens.
- Select a user name and click **OK**.
- Click **Apply**.

## Making a Group a Member of Another Group

### Procedure

#### To make a Group a member of another Group:

1. From the **Groups** section, select the name of the group. The **Group Information** is displayed in the right pane.
2. Click **Join Group**. The **User/Group Selection** dialog box opens.
3. Select a group name and click **OK**.
4. Click **Apply**.

### Modifying Access Rights for a Group

Security rights will be defined at a resource (for example, camera) level within the group. Rights may include the ability to view a camera, to use the PTZ, or to change camera settings. Permissions to access these rights can be associated with users and/or user groups by an administrator.

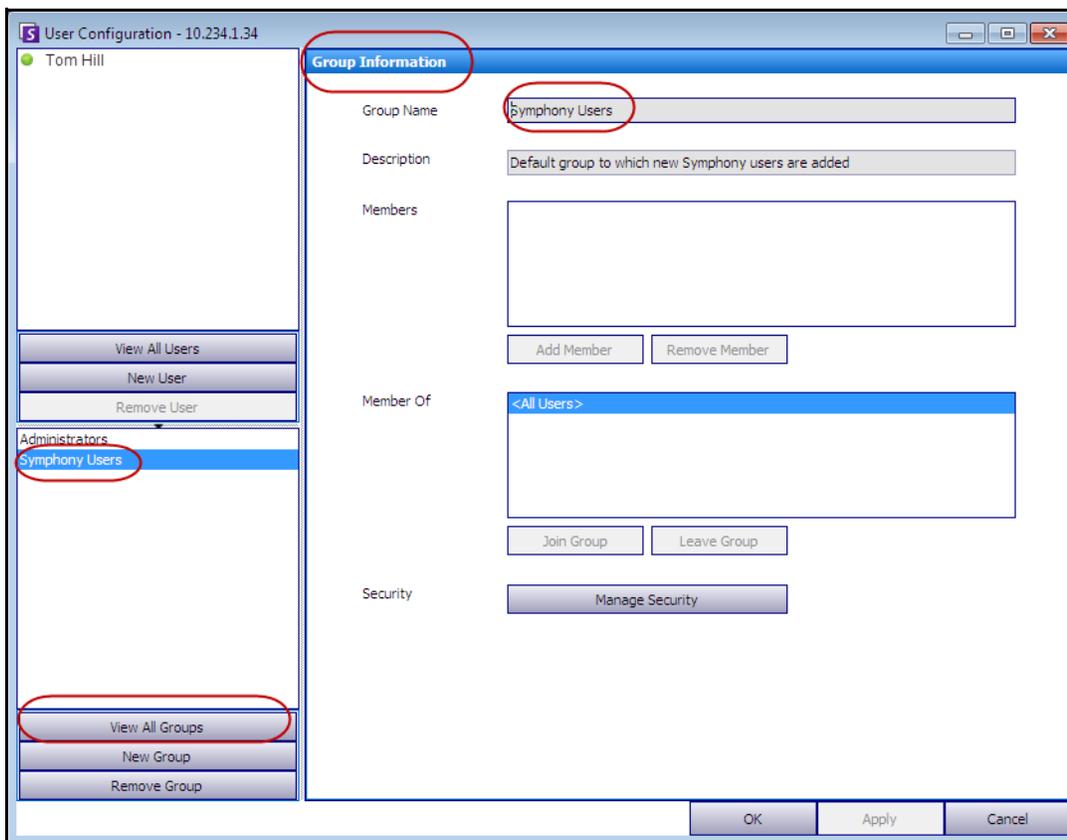


Figure 18. Manage Security

## Procedure

### To modify access rights for a Group:

1. From the **Groups** section, select the name of the group. The **Group Information** is displayed in the right pane.
2. Click **Manage Security**. The **Security Configuration** dialog box opens.
3. From the **Security Profiles** drop-down box, select the profile for which you want to modify privileges. (For background information, see [“Managing Security Profiles”](#) on page 29.)

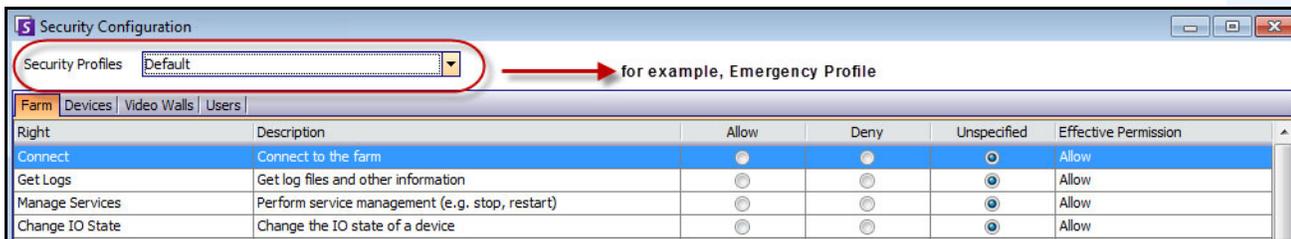


Figure 19. Selecting a Security Profile

4. Select the **Allow**, **Deny**, or **Unspecified** option for each **Right** (see [Figure 20](#) on page 42).
  - **Farm** tab defines access rights for core functionality that is not specific to a camera or other resource; for example, whether a user can connect to the farm, or export video.
  - **Devices** tab defines user permissions that can be defined for device; for example, whether a user can view the live feed or change the configuration for a specified camera, or listen to a camera or talk through a camera
  - **Video Walls** tab defines user permissions that can be defined for video walls; for example, whether a user can move a window in the video wall, or edit a video wall layout.
  - **Users** tab defines user permissions that can be defined for other users; for example, whether a user can view or edit the properties of another user or group.
  - The **Effective Permission** column calculates the access granted this group for the current functionality. Symphony checks if this group is a member of another group that may restrict access to the resource. For example if the current group allows access but another group of which it is a member restricts access, the effective permission will be **Deny**.
5. Click **Apply** to save changes and then **Close**.

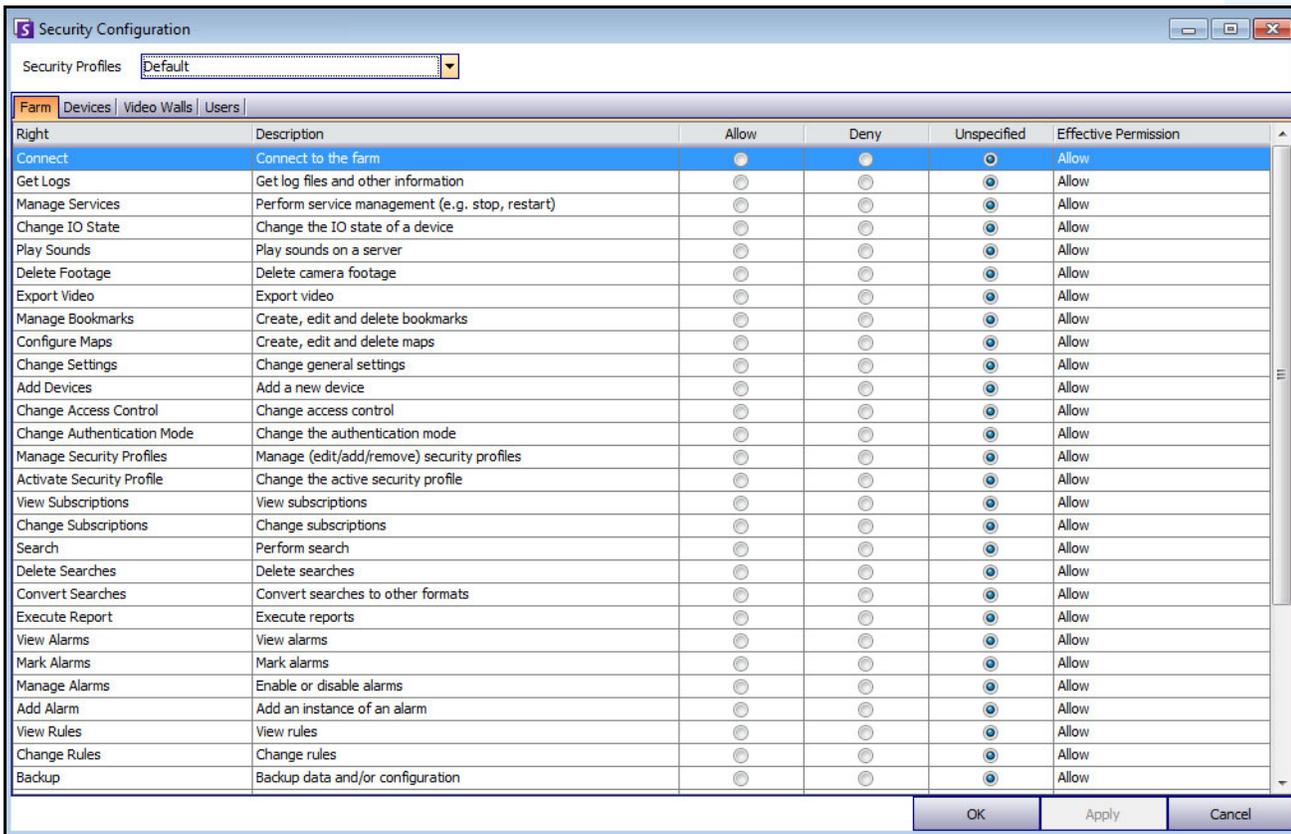


Figure 20. Security Permissions

You can click on the effective permission entry for a given right to display a list of inherited permissions. This helps you determine which group membership is causing the current effective permission.

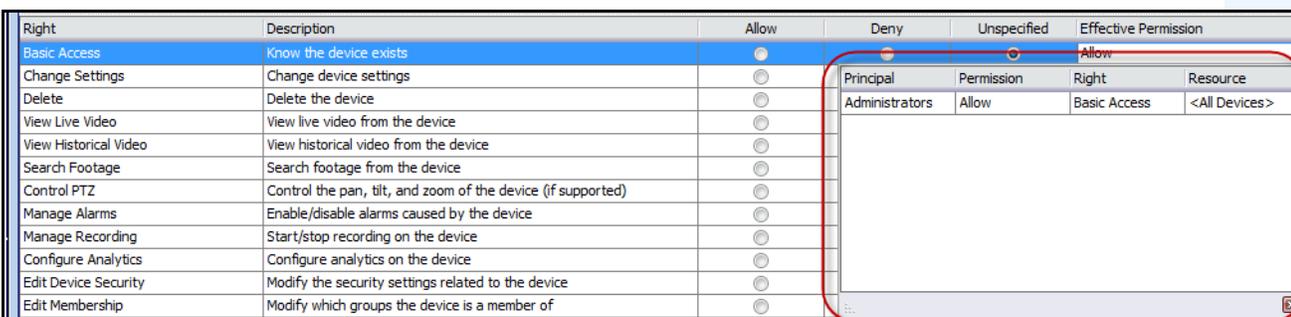


Figure 21. View inherited permissions

## Users within Groups and Effective Permissions

Users can be assigned individual security privileges if necessary.

The **Deny** option for any individual user or group overrides **Allow**.

- If at any point there is an explicit **Deny** permission defined between a user/group and the resource/group, permission will be denied.
- If there are no explicit **Allow** or **Deny** permissions, permission will be denied.
- If no explicit **Deny** permissions exist, but there is at least one **Allow** permission, permission will be allowed.

Example 1	
	<p>User A has individual right of <b>Allow</b>, belongs to Group 1 which also has <b>Allow</b>, but is a sub group of Group 2, which has <b>Deny</b>. User A will be <b>Denied</b> the right.</p> <p>User B has individual right of <b>Deny</b>, belongs to Group 1 which has <b>Allow</b> and is a subgroup of Group 2, which has <b>Allow</b>. User B will be <b>Denied</b> the right, irrespective of the group designations (of Allow). <b>Deny</b> is always the effective overriding permission.</p>

## Associating Groups with Active Directory

When the Active Directory authentication is enabled, groups can be optionally associated with Active Directory groups. Associating groups with Active Directory may be beneficial in large organizations with an existing Active Directory hierarchy. Once the associations have been defined, Symphony is periodically synchronized with Active Directory to ensure that the group relationships are equivalent.

### Procedure

#### To associate a group with Active Directory groups:

1. In the **Group Information** dialog box, click the **Associate** button. The **Active Directory Search** dialog box opens.



**Figure 22. Active Directory options**

2. Use the search feature to find and select the Active Directory group to associate. If groups are associated with Active Directory, group membership is automatically synchronized.

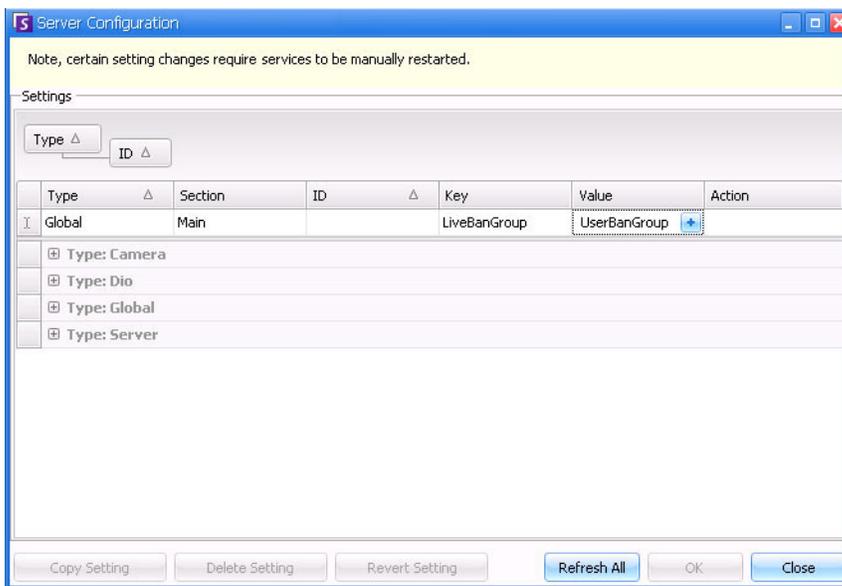
## Ban Live Video

Allows you to ban video from cameras and camera groups. Only users and groups with specified permissions can use this feature. You must set up all server machines for this feature.

### Procedure

#### To create a User Ban Group:

1. Create a group named *UserBanGroup*. To this new group, add the following users:
  - All non-admin users that should be banned from selected devices during a video ban.
  - Users who log into video wall clients. This is so that video wall clients are properly banned.
2. Add this group to database settings table:
  - a. From the **Server** menu, select **Manual Configuration Editor**.
  - b. Click **Add a new setting** in the first row to activate the cells.
  - c. Enter the following in cells under each column:
    - Type**=Global
    - Section**=Main
    - ID**=<empty>
    - Key**=LiveBanGroup,
    - Value**= UserBanGroup



3. To confirm your entry, click the **Action** cell.
4. Click **OK**.

## Managing Users

Users are managed from the **User Configuration** dialog box. The following information is stored about a user:

- Name, password, email, phone, description
- Priority (higher priority has control of PTZ camera) PTZ priority and rule management is configured on a per-user basis, not through Groups.
- Type of User
  - Symphony (basic user with customized restrictions)
  - Administrator (advanced user with customized restrictions)
- Membership in Group (must be a member of at least one group). The security permissions for each user are defined through its Group membership.

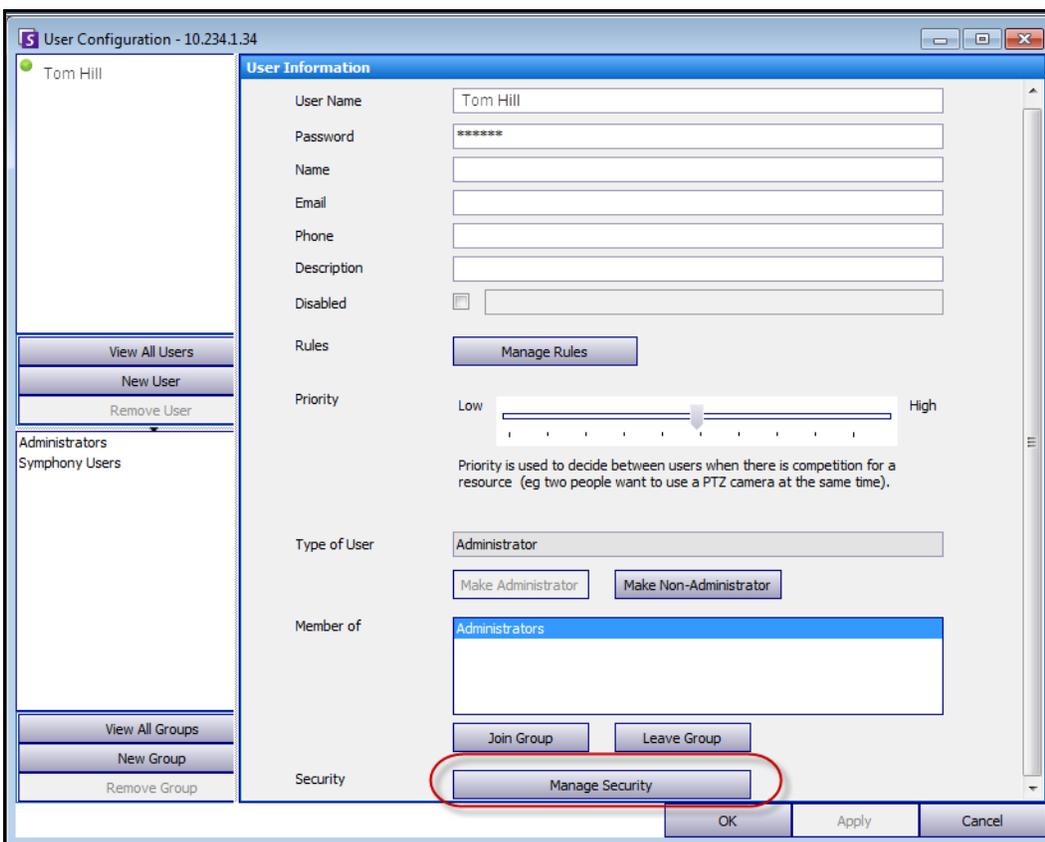


Figure 23. User Configuration dialog box

## Procedure

---

### To set up a new user:

1. From the **Server** menu, select **User Configuration**. The **User Configuration** dialog box opens.
2. In the left pane, click **New User**. The **User Information** dialog box opens. By default, the new user is a member of Symphony **Users** and is designated as a Symphony User **Type**.
3. Enter information about the user such as **User Name** and **Password**.
4. Click **Apply**.



**Note:** If Active Directory mode was defined during setup, no password is stored in Symphony as the Windows domain password will be used.

---

5. Define the rules for which the user will receive alarms:

By default, the user receives all alarm notifications configured for that user. In some cases, however, users may not want to receive alarms for particular rules, despite having access to the camera.

  - a. Click **Manage Rules**. The **Rule Configuration** dialog box opens.
  - b. Select or clear the rule check boxes as necessary and click **Ok**.
6. Using the **Priority** slider in the middle of the dialog box, assign **High** or **Low** priority access for your user. For example, a user with higher priority gets control of PTZ camera when two users want to access the camera.
7. To define access rights for this user, select the appropriate group in the **Member Of** section.
8. Click **Apply** to save changes and then **Close**.



If you upgraded from Symphony v6.2 to v6.7, note that the **Priority** slider settings for PTZ control is now very simple. Users with a high priority should be set to **High**. Users with a low priority should be set to **Low**.

---

## Active Directory Authentication

When Active Directory authentication is enabled, each user in Symphony must have a corresponding Active Directory user. The **Check Active Directory** button is enabled only when Active Directory authentication was enabled in the **Setup Wizard** (see **Installation Guide**). When the **Check Active Directory** button is clicked, Symphony attempts to find the closest match to the text currently typed into the **User Name** field.

- If there is only one match, the **User Name**, **Name**, and **Description** fields will be populated from the corresponding fields in Active Directory.
- If there are no matches, or multiple matches, the **Active Directory Search** dialog box will be displayed. This allows you to find the appropriate Active Directory user to associate with the Symphony user.

## Supervisor Logon

Depending on your installation, Symphony can be configured to allow Supervisor Logons. This feature allows two users to log on simultaneously in Symphony on the same PC, granting them higher user privileges than they normally have on an individual basis. For example, users who are members of the Symphony Users Group may have insufficient privileges to export video. But if they log on concurrently together in Supervisor mode they have sufficient privileges to do so.

You must create a new virtual Supervisor User and a new User Group (for example, Power Users) which this user will be a member of. The new User Group should have greater privileges than the Symphony User Group.

You cannot modify an existing user to have these supervisor privileges. Essentially, this virtual Supervisor User name will work like a key to open (allow) certain privileges for two users logging on at the same time.

## Setting up Supervisor Logon on Your System

- [“Task 1: Edit the acc.ini file for Supervisor Privileges and Reason field”](#)
- [“Task 2: Set up a “Power Users” group for a virtual user for supervisor privileges:” on page 48](#)
- [“Task 3: Set up a virtual user for supervisor privileges” on page 49](#)
- [“Task 4: Define who can log on as the virtual supervisor user” on page 50](#)

## Using Supervisor Logon

- [“Logging on with Supervisor Privileges” on page 51](#)
- [“Understanding User Logins in View Detailed Events” on page 52](#)
- [“User Logins Report - Notes Column Indicates Supervisor Login Reason” on page 52](#)

### Task 1: Edit the acc.ini file for Supervisor Privileges and Reason field

1. Close Symphony Client.
2. Edit %appdata%\Aimetis\acc.ini file.
3. To display the Supervisor Logon feature:
  - Under **[Main]**, add **ShowTwoManRule=True**
4. (Optional) By default, the **Reason** field is displayed when the Supervisor Logon feature is activated and the user must include a reason for logging on.  
To suppress the **Reason** field requirement:
  - Under **[Main]**, add **TwoManRuleReasonIsMandatory=False**

## Task 2: Set up a “Power Users” group for a virtual user for supervisor privileges:

1. From the **Server** menu, select **User Configuration**. The **User Configuration** dialog box opens.
2. In the left pane, click **New Group**. The **Group Information** dialog box opens. Create a group that the virtual supervisor user will belong to, for example, a “Power Users” group containing high privileges.
3. Ensure that this group has higher privileges than the regular Symphony Users group.
4. Click **Apply** to save changes.

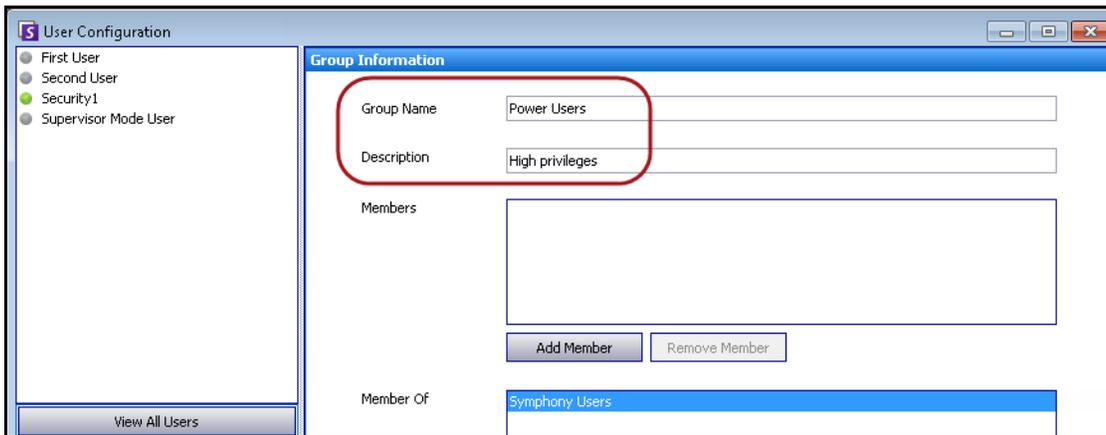


Figure 24. New “Power Users” group

For added security, ensure that the **Change Settings** permission for the “Power Users” group is set to **Deny**. As such, when two users log on together, they will NOT be able to change their account permissions and make themselves Admin users. (Click the **Manage Security** button in the **User Configuration/Group Information** dialog box.)

The screenshot shows the 'Security Configuration - Power Users' dialog box. It features a dropdown for 'Security Profiles' set to 'Default' and a tabbed interface with 'Farm', 'Devices', 'Video Walls', and 'Users' tabs. Below is a table of permissions:

Right	Description	Allow	Deny	Unspecified	Effective Permission
Activate Security Profile	Change the active security profile	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Add Alarm	Add an instance of an alarm	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Add Devices	Add a new device	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Add or Edit License Plate Metadata	Edit the description and additional details about a license plate or...	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Add Users	Add new users and groups	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Backup	Backup data and/or configuration	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Change Access Control	Change access control	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Change Authentication Mode	Change the authentication mode	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Change Carousels	Change carousels	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Allow
Change IO State	Change the IO state of a device	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Change Rules	Change rules	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
<b>Change Settings</b>	<b>Change general settings</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<b>Deny</b>
Change Subscriptions	Change subscriptions	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny
Change Video Wall Client	Register/Unregister current Symphony Client as Video Wall Client	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	Deny

Figure 25. Recommended: Change Settings permission set to Deny for “Power Users” group

### Task 3: Set up a virtual user for supervisor privileges

1. In the left pane, click **New User**. The **User Information** dialog box opens.
2. Enter a **User Name** and **Password** for the virtual user for Supervisor Logon. By default, this new virtual user is a member of **Symphony Users**.
3. Join this user to the new “Power Users” group you created in [“Task 2: Set up a “Power Users” group for a virtual user for supervisor privileges:”](#).
  - a. Click **Join Group**. The **User/Group Selection** dialog opens.
  - b. Select the “Power Users” group and click **OK**.
4. Click **Apply** to save changes.

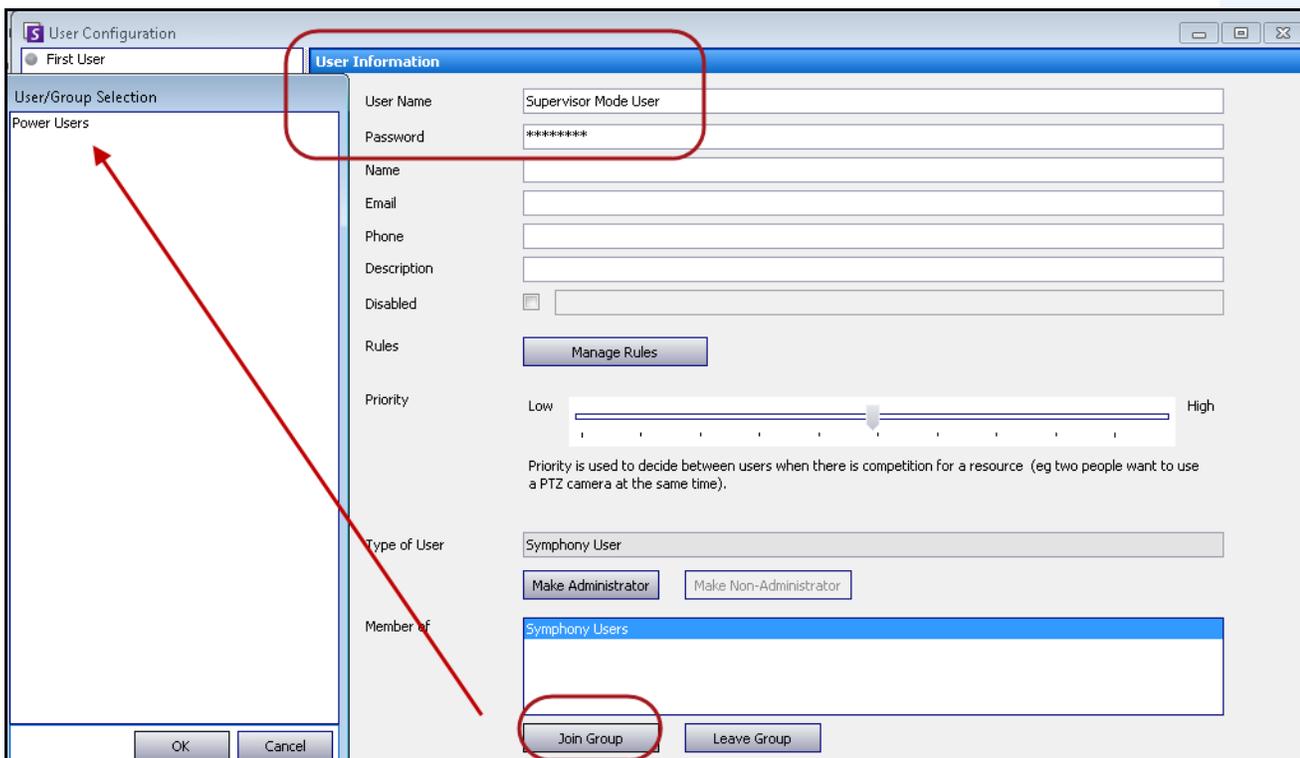


Figure 26. New virtual user must join “Power Users” group

## Task 4: Define who can log on as the virtual supervisor user

1. With the virtual new user dialog box still open, select the **Supervisor** check box.
2. From the drop-down list, select Symphony **Users** group (or any group that you want two members to log in with Supervisor Mode). This allows two members of a Low Priority/Privileges Group to log on as a virtual user, who is a member of a Higher Priority/Privileges Group.
3. Click **Apply** to save changes and then **OK**.

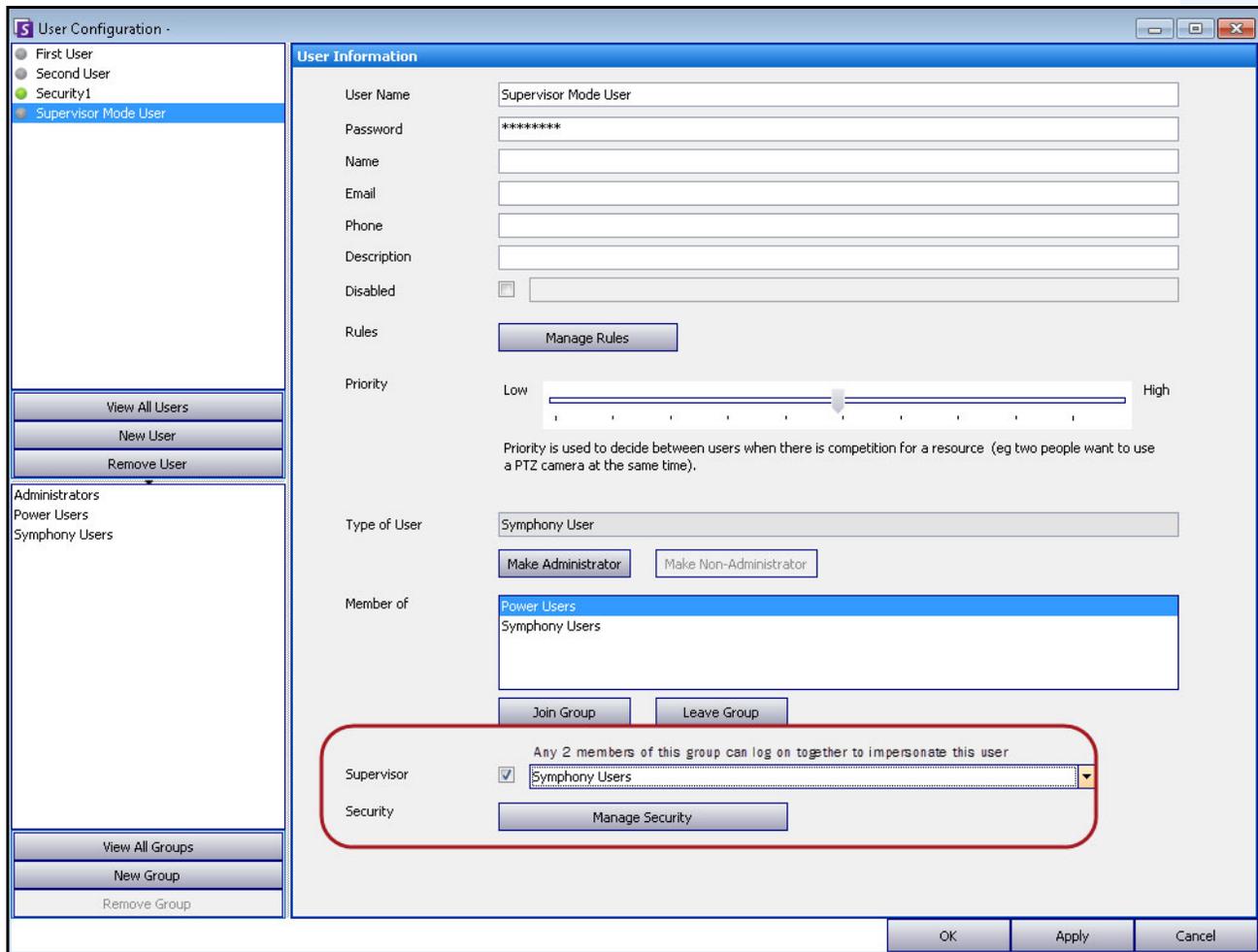


Figure 27. Supervisor check box

## Logging on with Supervisor Privileges

### Procedure

#### To log on with supervisor privileges:

1. In Symphony Client, from the **File** menu, select **Log On/Switch User**. The **Logon** dialog box opens.
2. Select the **Server** to log on to with supervisor privileges. The **Supervisor Logon** check box appears.



Figure 28. Logon

3. Enter the **User** and **Password** of one of the two users.
4. Select the **Supervisor Logon** check box. More fields appear.
5. Enter the **User** and **Password** of the second user wanting to log on at the same time.
6. Enter the **Supervisor User** name. It is the same name of the virtual user you created in the **User Configuration** dialog box. (See ["Task 3: Set up a virtual user for supervisor privileges" on page 49.](#)) Essentially, this **Supervisor User** name works like a key to open (allow) certain privileges for the two users logging on at the same time.

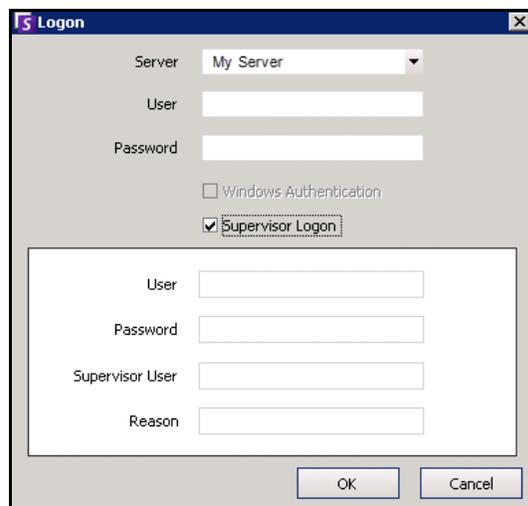


Figure 29. Supervisor Logon fields displayed

7. If the **Reason** text box is displayed, enter information that describes why you are logging in with supervisor privileges. (An **acc.ini** file controls whether the **Reason** field is mandatory.)
8. Click **OK**. You can now use the system.

## Understanding User Logins in View Detailed Events

In the **Help>View Detailed Events** dialog box, two users logged in with supervisor mode will have their usernames joined by the underscore character.

Time	Name	Event ID	Group ID	Key	Value
07/19/2012 03:30:48 PM	ConfigurationChange		4016	username	Security1
07/19/2012 03:30:48 PM	ConfigurationChange		4016	Edited	User
07/19/2012 03:30:48 PM	ConfigurationChange		4016	Id	0
07/19/2012 03:30:48 PM	ConfigurationChange		4016		
07/19/2012 03:31:25 PM	SessionEnded		4017	b77fca7a-9124-44f6-9a79-3... sessionId	b77fca7a-9124-44f6-9a79-3...
07/19/2012 03:31:25 PM	SessionEnded				
07/19/2012 03:31:26 PM	SessionCreated			users	First User_Second User
07/19/2012 03:31:26 PM	SessionCreated			notes	Testing
07/19/2012 03:31:26 PM	SessionCreated				

**Figure 30. View Detailed Events - Usernames joined by underscore indicates two users logged on at same time to same machine**

## User Logins Report - Notes Column Indicates Supervisor Login Reason

In the **Server>View Logins, User Logins** dialog box, the **Notes** column contains the reason two users had to log in at the same time.

Date	Time	Username	IP	Notes
07/19/2012	02:47:03 PM	Security1	10.234.5.31	
07/19/2012	02:51:07 PM	First User_Second User		testing
07/19/2012	02:53:55 PM	Security1		
07/19/2012	03:00:11 PM	Security1		
07/19/2012	03:23:42 PM	Security1		
07/19/2012	03:31:26 PM	First User_Second User		Testing
07/19/2012	03:32:33 PM	Security1		

**Figure 31. User Logins showing Notes column**

## Advanced Information - Active Directory Associations

Before reading this advanced level information, ensure that you have reviewed the information in the following sections:

- [“User Authentication” on page 31](#)
- [“Configuring User Access” on page 37](#)
- [“Understanding User Groups” on page 38](#)

### Authentication Mode Set to Active Directory (in Installation Setup Wizard)

When the authentication mode is set to Active Directory, Symphony users are tightly bound to their Active Directory information.

- When creating a new user in Symphony, the user must have a corresponding Active Directory user designation. (See [“Active Directory Authentication” on page 46](#)).
- Users with no Active Directory association cannot be authenticated. The user properties of unassociated users, however, are still modifiable.

### Synchronizing with Active Directory

On a periodic basis, certain user attributes are synchronized with Active Directory, and thus these properties cannot be modified manually.

The following properties are synchronized with Active Directory:

- User Name, Full Name, and Description.
- Group membership except for Administrators. Users in the **Administrator Group** are only in the Administrator group.



**Important:** Passwords are never stored in this mode, so they cannot be modified.

---

### Logging on to Symphony if your user does not exist in Symphony

- If authentication mode is Symphony, logon will fail because the credentials cannot be authenticated.
- If authentication mode is **Active Directory** - after the credentials have been successfully authenticated against Active Directory - a new Symphony user is created and associated with the specified Active Directory user. This user is added to the Symphony Users group, and thus inherits all security permissions from that group.

### Groups Associated with Active Directory

When the authentication mode is set to Active Directory, groups can optionally be associated with Active Directory groups. Groups with Active Directory associations have their group membership periodically synchronized with Active Directory.

<b>Example 2</b>	
	<p>Symphony Group A is associated with Active Directory group 1 Symphony Group B is associated with Active Directory group 2</p> <p>If group 1 is a member of group 2, then Symphony Group A will become a member of Symphony Group B when group membership is synchronized.</p>

**Table 4. Restrictions on Symphony Groups**

<b>Membership</b>	<b>Symphony Group</b>	<b>Symphony Group with Active Directory Association</b>
Member of another Symphony group	Allowed	Allowed
Member of another Active Directory group	Not-allowed	Allowed
Explicitly <b>leave</b> an Active Directory group		Not-allowed
Explicitly <b>join</b> an Active Directory group		Not-allowed

## Periodic Synchronization

Periodically (daily, at 11:59 pm), Symphony is synchronized with Active Directory. The process is as follows:

1. User associations are verified and updated
  - a. For every Symphony user **without** an Active Directory association, we determine if there is a matching Active Directory member (by comparing user name to Active Directory account name).
    - If there is a match we create an association between the two.
  - b. For every Symphony user **with** an Active Directory association, we verify that the Active Directory member still exists.
    - If not, we remove the association.
    - If the association exists, we ensure that the user name, full name, and description in Symphony match the same values in Active Directory.
2. Group membership is updated
  - a. For every Symphony user and group with an Active Directory association, we determine the Active Directory group membership.
    - If group membership has changed in Active Directory, then those changes are applied to the Symphony Group membership. Any non-Active Directory relationships are maintained.

For a visual representation of this process, see [Figure 32 on page 55](#).

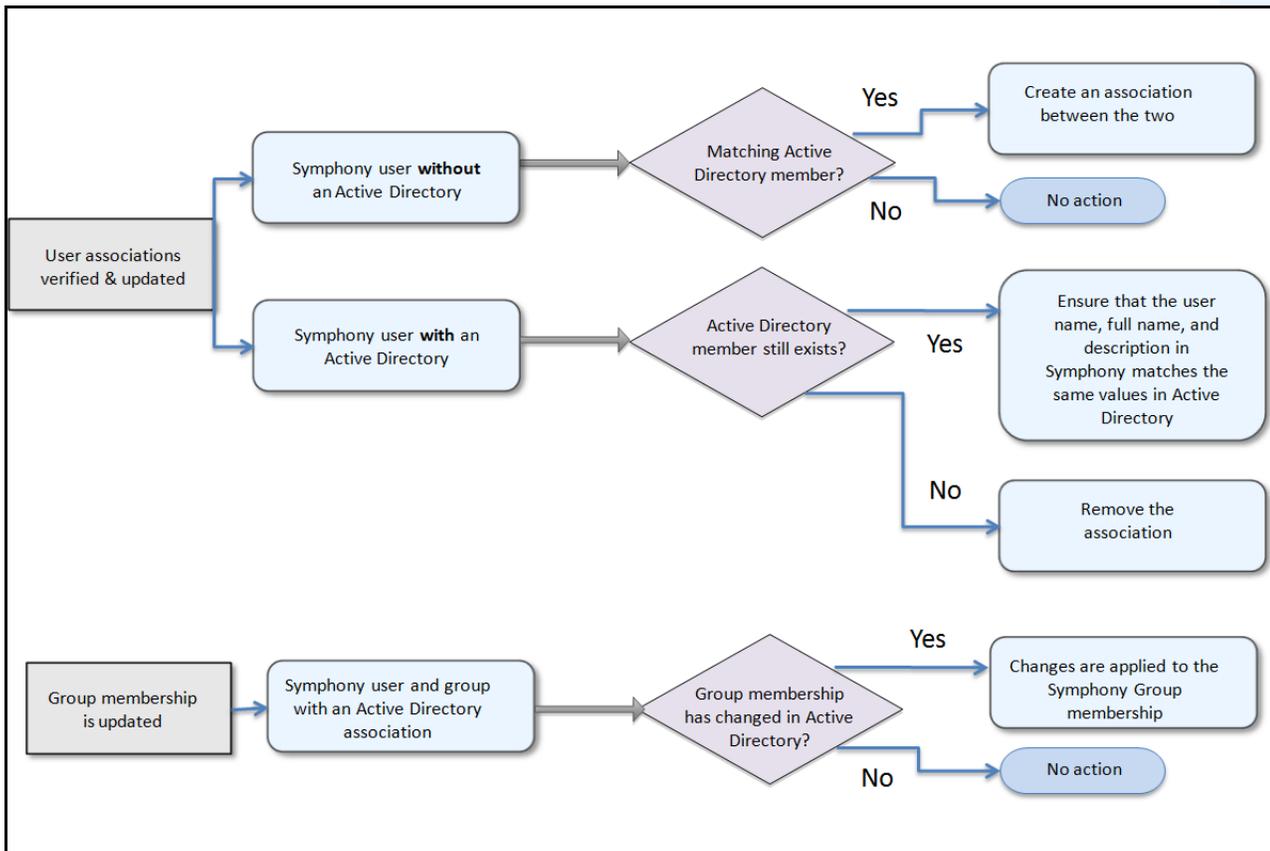


Figure 32. Synchronization Process

### When a user joins another Active Directory group:

1. Any changes to Active Directory will not be detected immediately by Symphony.
2. When the daily synchronization occurs, Symphony will detect that the user has joined a new Active Directory group.
3. The server will then attempt to find a matching Symphony group.
  - If a matching Symphony group exists, the user will be added to that group.
  - If not, the server proceeds to recursively check all the parents of the Active Directory group, trying to find a match with Symphony groups. The operation continues up each parental line until either:
    - a. an associated Symphony group is found, or
    - b. there is no parent to check.

This operation ensures that the Symphony group membership matches the Active Directory group membership as closely as possible.

## Using Maps

Symphony allows you to upload an image (jpg, gif or bmp file) to be used as a map (visual representation) of your camera configuration. For basic usage, see the Aimetis Symphony **Client User Guide**. This section provides instructions on more advanced features of **Maps**.

- [“Icons on Map”](#)
- [“Adding Rules to Maps” on page 58](#)
- [“Adding Digital Input and Output to Maps” on page 60](#)
- [“Customizing Digital Input and Output Names” on page 62](#)
- [“Activating an Output Device Using the Map Context Menu” on page 64](#)

## Icons on Map

Use the following legend to understand the icons placed on maps.

**Table 5. Map Icon Legend**

Icon	Icon Description	Represents	Colors Indicate
	Filled in circle	Rule on a camera	You can set colors to indicate various states as necessary
	Triangle pointing up in circle	Digital Input (e.g., person presses a button, which causes an appropriate action in the system)	Green arrow, white background - not activated Green arrow, yellow background - activated
	Triangle pointing down in circle	Digital Output (e.g., motion sensor detects motion and closes a gate)	Green arrow, white background - not activated Green arrow, yellow background - activated
	Circle containing an arrow	Camera	Green arrow - recording Orange arrow - activity Red arrow - alarm  Orange circle - camera currently selected
	Box around a circle containing an arrow	PTZ Camera	Green arrow - recording Orange arrow - activity Red arrow - alarm  Orange circle - camera currently selected
	Door	Access control device (e.g., key card or key fob)	Green - access granted Red - access denied

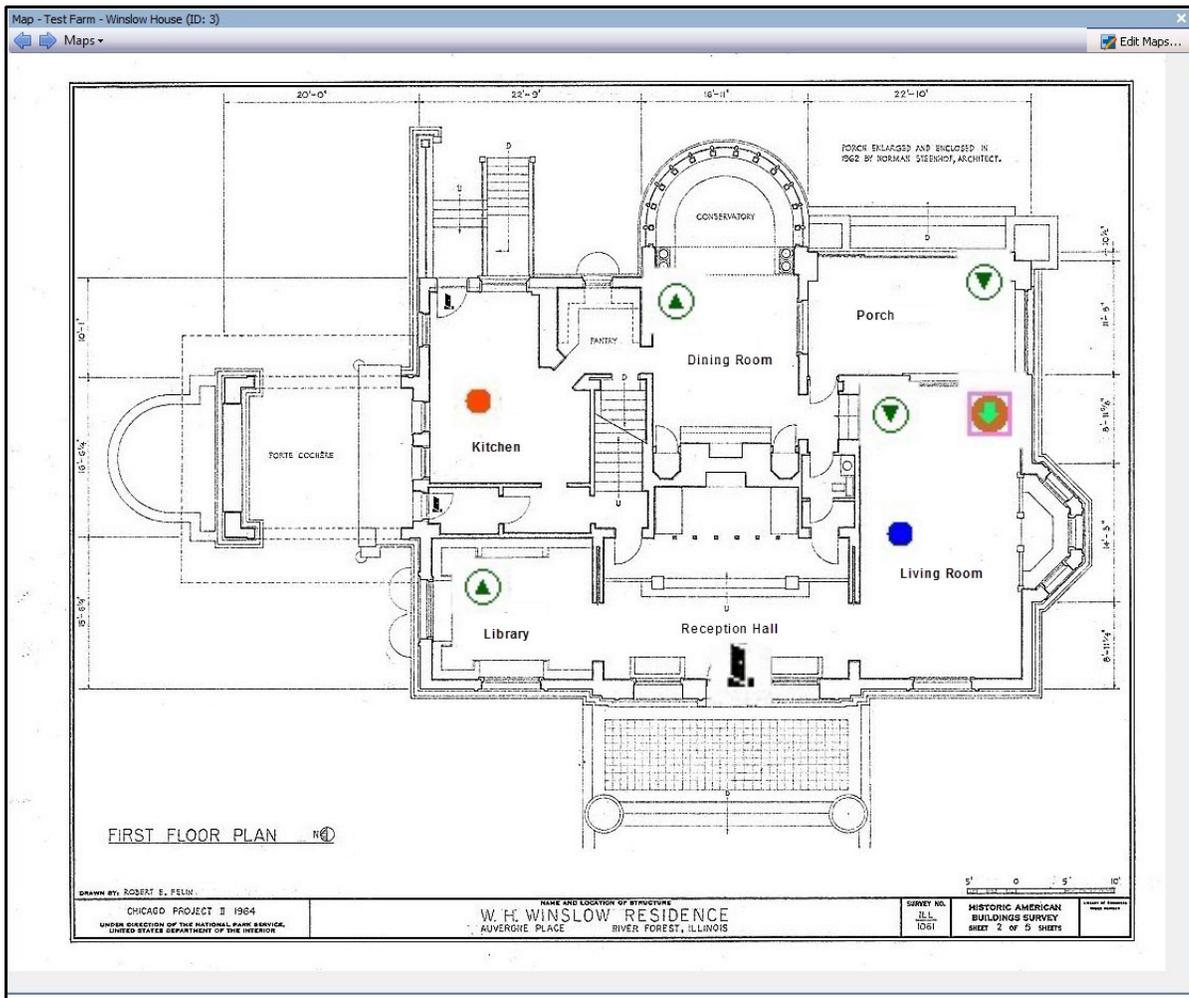


Figure 33. Example of a typical map with camera, PTZ camera, digital I/O, and control access device icons, and rules

## Adding Rules to Maps

Every Rule on Map must be associated with a camera or a device. The Rule on Map icon helps emphasize alarm notification by either flashing for 10 seconds at every new alarm, or by flashing until security personnel mark the alarms as real/false/actionable.

Because you can always create more than one rule for the same camera, with Rules on Maps, you can see exactly which rule is triggered. The name of the rule is displayed when hovering over a map.

Any rule created for a server in the active server farm in the **Rules Wizard** will be listed in the **Rules** tab of the **Map Configuration** dialog box. For more information on the creating rules, see the Aimetis Symphony Analytics Guide.

A Rule can be used in the following ways:

- Added to multiple maps.
- Added to the same map more than once.
- Moved to another location on the same map.
- Removed from a map.

Alarms function as follows:

- Only alarms that appear in the **Alarm Log** will appear on the map. (If you start the Symphony Client and there are pre-existing unacknowledged alarms loaded, the map will display flashing alarm icons (if this has been configured).
- When you left-click on the rule icon, the Symphony Client will display the last unacknowledged alarm JPEG for the associated camera (the first camera if there are multiple cameras).

A Rule on map reflects the current state, configurable by user:

- Option 1: Flashes if any alarms are unacknowledged; otherwise, remains invisible. Once you have acknowledged all alarms (related to that rule), the rule disappears from the map.
- Option 2: Flashes for 10 seconds when a new alarm occurs; otherwise, remains invisible
- These options are available in the **Maps** tab of the **Client Settings** dialog box.
  - From the **View** menu, select **Settings**. The **Client Settings** dialog box opens. Click the **Maps** tab.

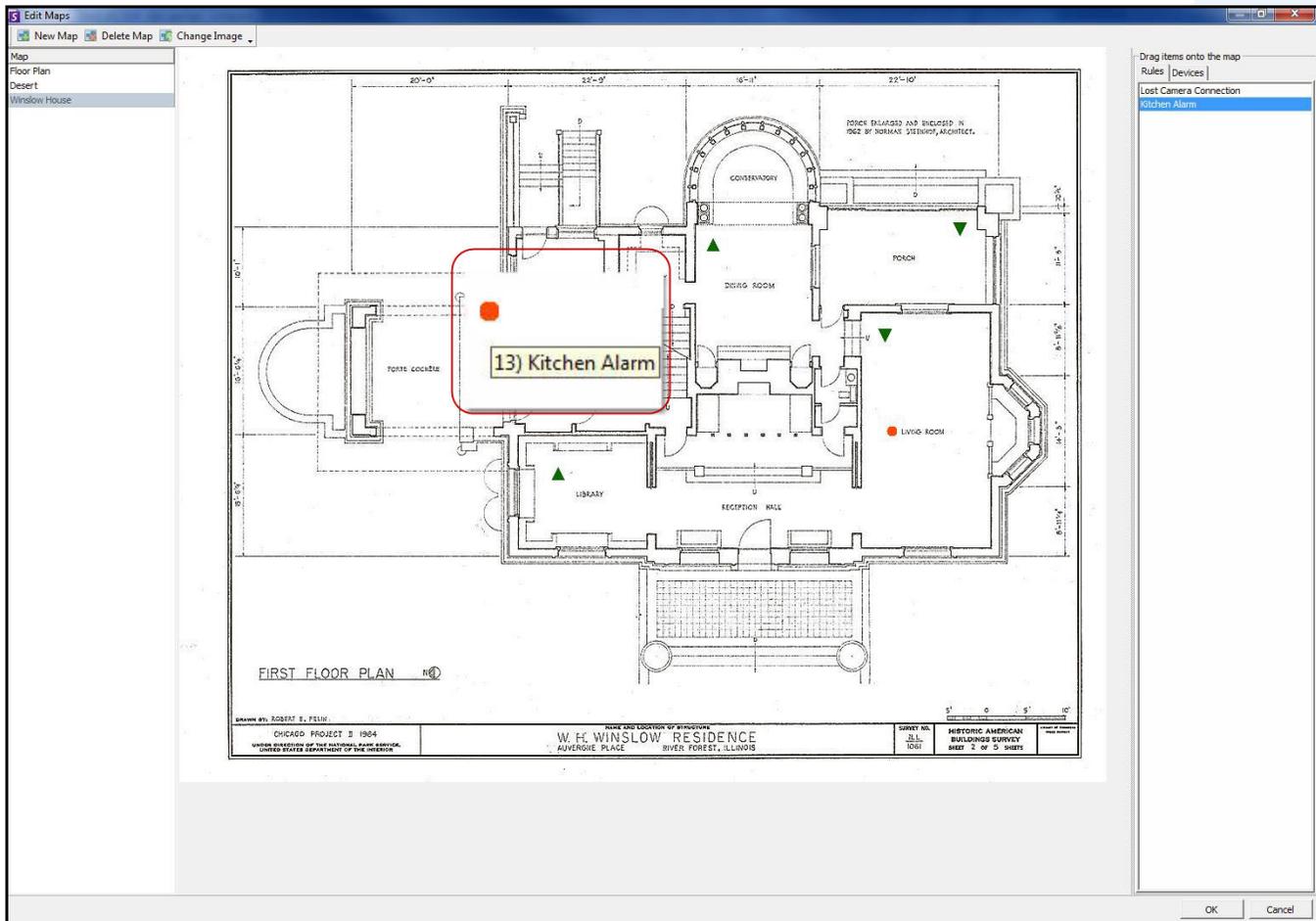


Figure 34. Rule on Map example

## Procedure

### To place rules on a map:

1. From the **View** menu, select **Map Navigation**.
2. Scroll through the maps to select the one which will have rules.
3. In the upper right corner of the **Map** dialog box, click **Edit Maps**. The **Edit Maps** dialog box opens.
4. Click the **Rules** tab. From the right pane listing the rules, drag and drop your rules to the map with your mouse.
5. Click **OK** to save settings.

## Acknowledging Rules on Maps

### Procedure

#### To acknowledge an alarm (rule on map):

1. From the **View** menu, select **Alarm Log** OR click the **Alarm Log** icon on the Menu Toolbar.
2. Right-click on the alarm you want to acknowledge.
3. Select an action to perform:
  - **Mark As Alarm** - To mark as a real alarm.
  - **Mark as False Alarm** - To mark as a false alarm.
  - **Mark as Real Actionable** - To mark as real alarm that requires action, for example, security staff should investigate the alarm.

### Adding Digital Input and Output to Maps

Not on all devices. See list in Knowledge Base article: <http://www.aimetis.com/Support/kbarticle.aspx?ID=10141>

The **Map Configuration** dialog box contains a **Devices** tab, listing all cameras and digital input and output devices. You can customize digital input and output names to help identify them.



**Important:** The **Show Digital I/O** option must be enabled in **Device Tree Configuration** dialog box for the digital I/O to be displayed, regardless of which specific inputs/outputs are selected.

Icon	Icon Description	Represents	Colours <sup>a</sup> Indicate
	Triangle pointing up in circle	Digital Input (e.g., person presses a button, which causes an appropriate action in the system)	Green arrow up, white background = not activated
			Green arrow up, yellow background = activated
	Triangle pointing down in circle	Digital Output (e.g., motion sensor detects motion and closes a gate)	Green arrow down, white background = not activated
			Green arrow down, yellow background = activated

a. If a device is in an Unknown state (map icon is grey), right-click to display the context menu and to activate or deactivate the device

## Procedure

### To place digital inputs/outputs on the Map:

1. From the **View** menu, select **Map Navigation**.
2. Scroll through the maps to select the one which will have rules.
3. In the upper right corner of the **Map** dialog box, click **Edit Maps**. The **Edit Maps** dialog box opens.
4. Click the **Devices** tab. From the right pane listing the devices, drag and drop the digital devices to the map with your mouse.
5. Click **OK** to save settings.

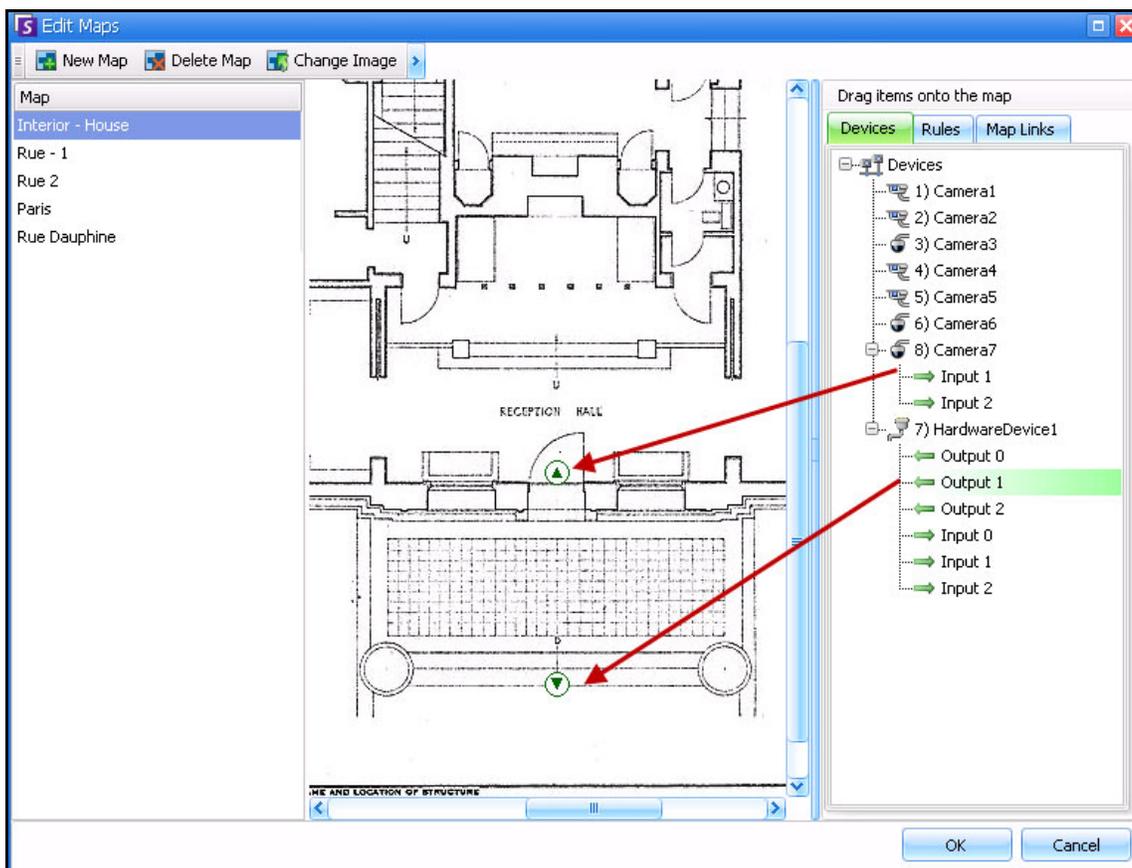


Figure 35. Digital I/O on map displayed with arrow icons

# Customizing Digital Input and Output Names

## Procedure

To customize digital input and output names:

1. For Hardware Device:
  - a. Right-click on a device in the **Camera Tree**, and select **Setup**. The **HardwareDevice** panel opens in the **Server Configuration** dialog box.

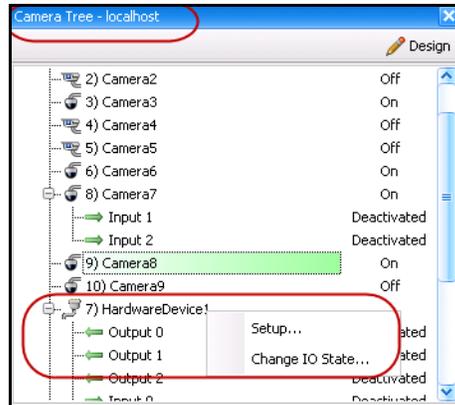


Figure 36. Camera Tree dialog box - Right-click on Hardware Device

- b. Click on each **Input** or **Output** you want to change and enter a new name.

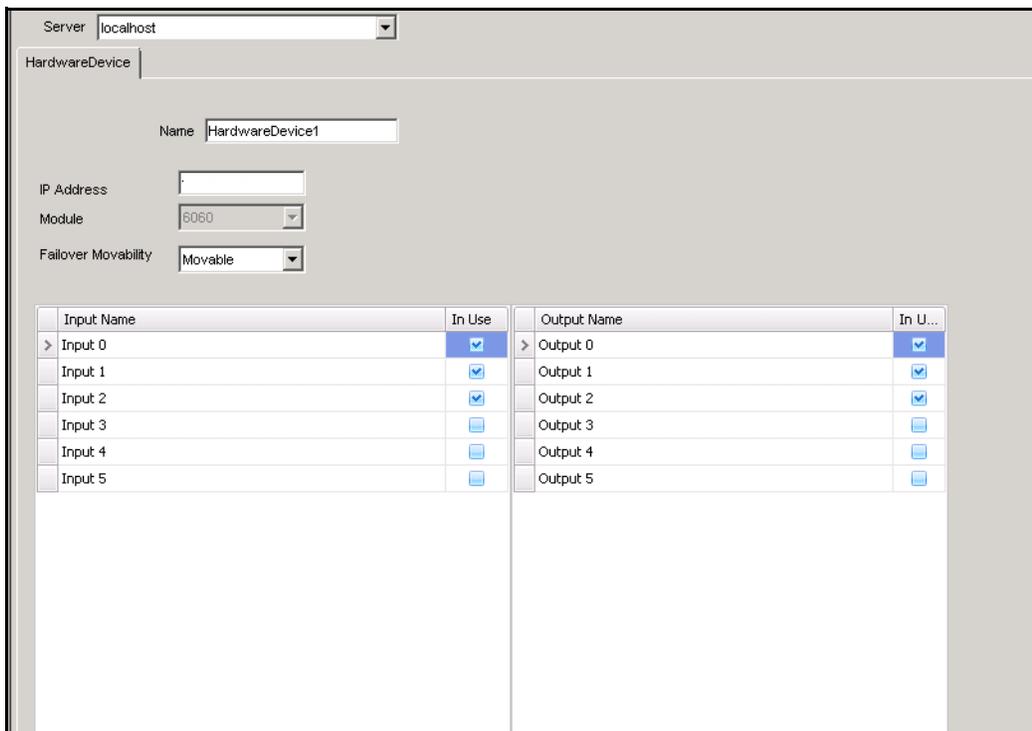


Figure 37. HardwareDevice tab in Server Configuration dialog box

2. For camera with digital I/O:
  - a. Right-click on a camera in the **Camera Tree**, and select **Camera Setup**. The **Server Configuration** dialog box opens.

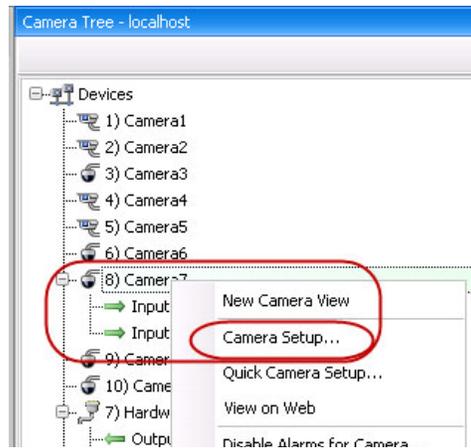


Figure 38. Camera Tree dialog box

- b. Click the **Digital I/O** tab.
  - c. Click on each **Input** or **Output** you want to change and enter a new name.

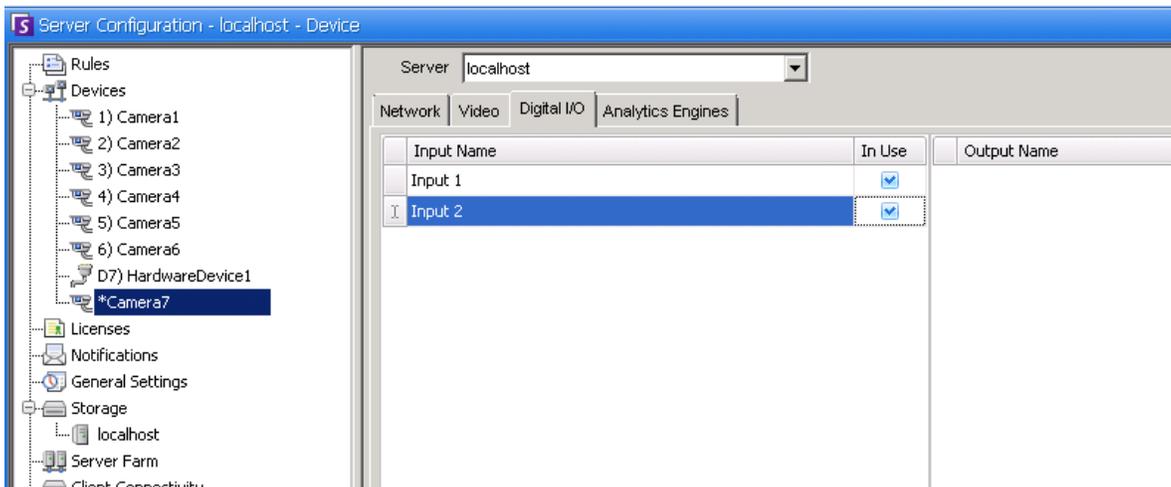


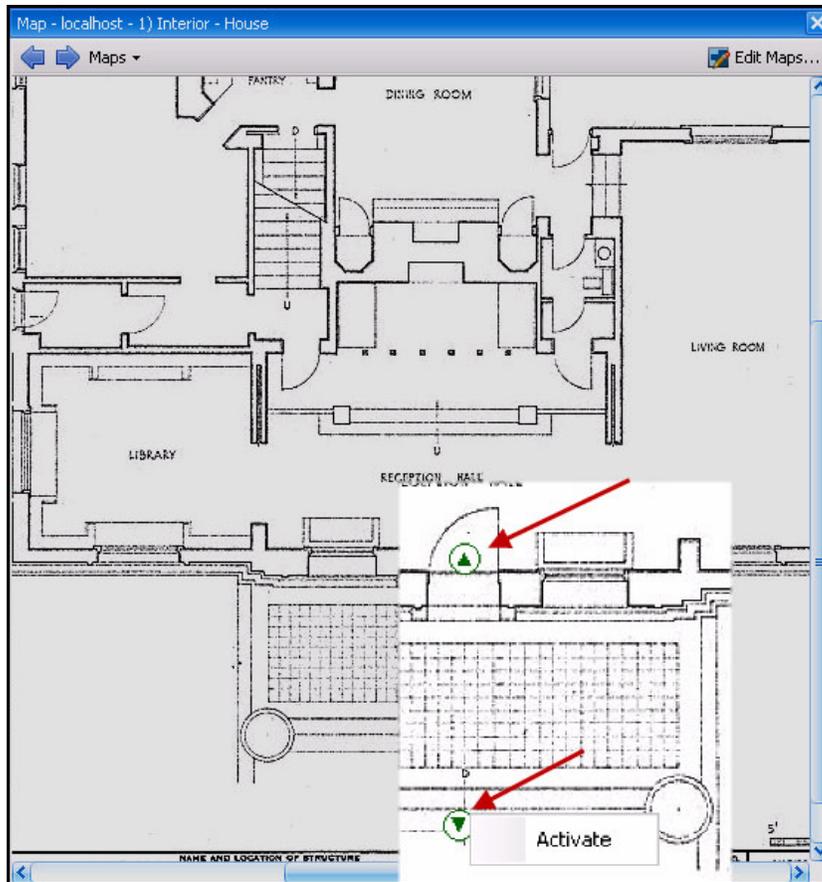
Figure 39. Digital I/O tab for Axis Cameras in Server Configuration dialog box

## Activating an Output Device Using the Map Context Menu

### Procedure

To activate output device using the context menu:

1. Right-click on the device. The context menu opens.
2. Click **Activate**. The icon turns yellow.



**Figure 40. Activating an Output device on a Map  
Only Output device has context menu for Activate**

# Chapter 2

## Customizing Storage Settings

Symphony allows you to customize where video is stored, how much storage to use, and when video should be deleted. Video and logs should be stored in separate folders. Ideally, no more than 5000 files per folder. We recommend that each camera store its video in its own folder. You can group them in a logical way so that you do not have to manage hundreds or thousands of folders.

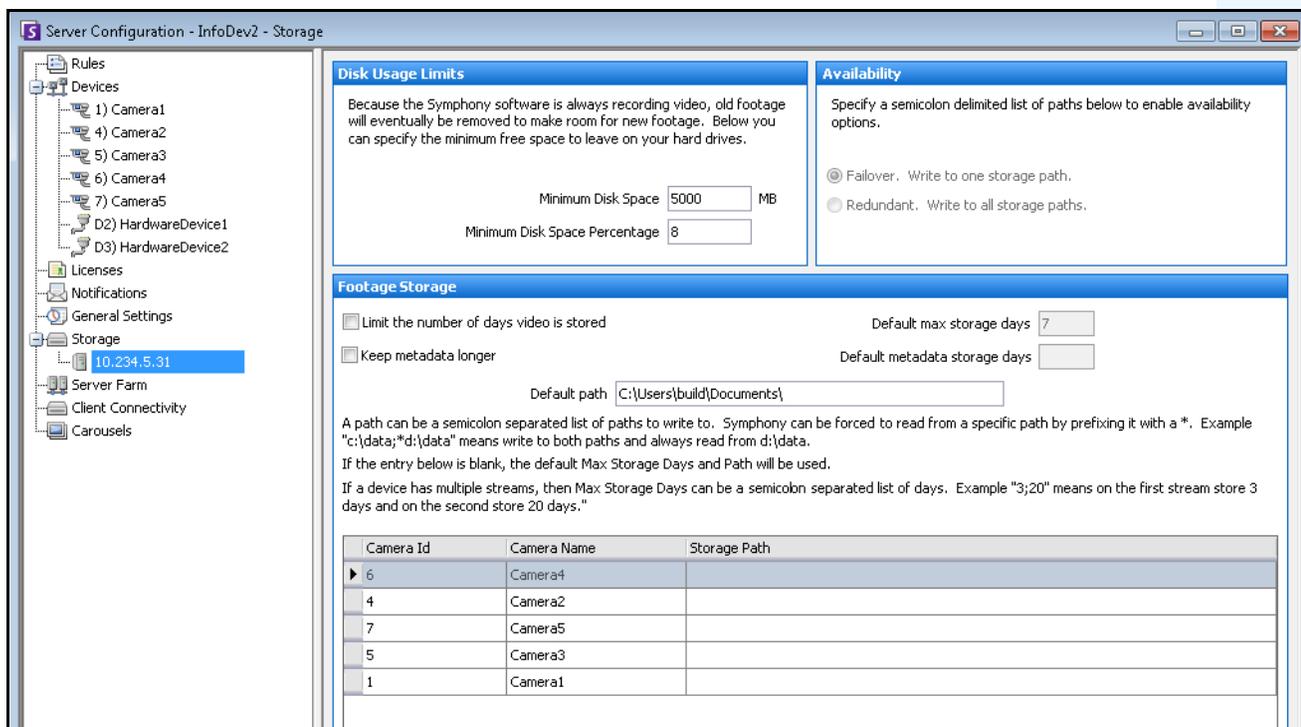


Figure 1. Storage Settings

## Procedure

### To view the storage settings:

1. From the **Server** menu, select **Configuration**.
2. Using the tree view in the left pane, select **Storage**. The **Storage Summary** is displayed in the right pane.
3. Click on one of the storage devices in the tree. **Disk Usage Limits** and **Footage Storage** information are displayed. For details, see [Table 1](#).

Table 1. Storage Options

Storage	Task
<b>Disk Usage Limits</b>	
<b>Minimum Disk Space</b>	Specify the minimum amount of free disk space on the hard disk. Symphony starts deleting video as soon as free disk space is below this setting.
<b>Minimum Disk Percentage</b>	Specify a percentage of free disk space to maintain.
<b>Availability</b>	Allows you to define whether the second storage path is for failover or for redundant mode.
<b>Failover</b>	Write to one storage path. An alternative location if the primary location fails. (For Failover recording, ensure that you are using a NAS if you have multiple servers on the farm.) See <a href="#">“Important: Failover works if you are using a file storage device (for example, NAS) instead of block storage (such as SAN or a local disk) because the pool of storage does not follow the camera when it is moved. If you have central storage (with a NAS), the storage is always accessible from any server.” on page 76.</a>
<b>Redundant</b>	Write to all storage paths. Simultaneously record to two locations.
<b>Footage Storage</b>	
<b>Limit the number of days video is stored</b>	Specify a global setting ( <b>Default max storage days</b> field) or <b>Max Storage Days</b> for each camera in the <b>Footage Storage</b> section. In certain situations, disk space may be available to record more video, but you may want to artificially have the video removed. This may be the case in certain jurisdictions where you are legally required to delete video after a certain time.
<b>Default max storage days (global setting)</b>	If the <b>Limit the number of days video is stored</b> option is enabled, specify the default value in days when video is over written, even if extra hard disk space exists. Alternatively, by adjusting the <b>Max Storage Days</b> value per camera, individual camera settings supersede the global settings.
<b>Keep metadata longer</b>	Specify that metadata can be stored longer than video. This is useful in order to maintain reporting capability.
<b>Default metadata storage days</b>	Specify how long metadata will be stored.

**Table 1. Storage Options (Continued)**

Storage	Task
<b>Default path</b>	The default path location where video will be recorded is displayed (as defined at installation). You can adjust the path for an individual camera under the <b>Storage Path</b> column in the camera table.
<b>Storage Path</b>	<p>A semicolon separated list of paths to write to.                      If the <b>Storage Path</b> per <b>Camera ID/Name</b> is blank, the settings in the <b>Default max storage days</b> and <b>Default path</b> fields will be used.</p> <p>Symphony can be forced to read from a specific path by prefixing the path with an *.                      Example:                      "c:\data;*d:\data" means write to both paths and always read from d:\data.</p> <p>If a device has multiple streams, then <b>Max storage days</b> can be a semicolon separated list of days.                      Example:                      "3;20" means store 3 days for the first stream and store 20 days for the second stream.</p>

# Managing Server Farms

A Server Farm is a collection of computer servers used to accomplish server needs beyond the capability of one machine. Server farms often have backup (redundant) servers, which can take over the function of primary servers in the event of a primary server failure.

## Procedure

### To manage your Server Farm:

1. From the **Server** menu, select **Configuration**. The **Configuration** dialog appears.
2. In the left pane, click **Server Farm**. The **Server Farm Summary** is displayed in the right pane. The server named displayed in bold is the Master server.

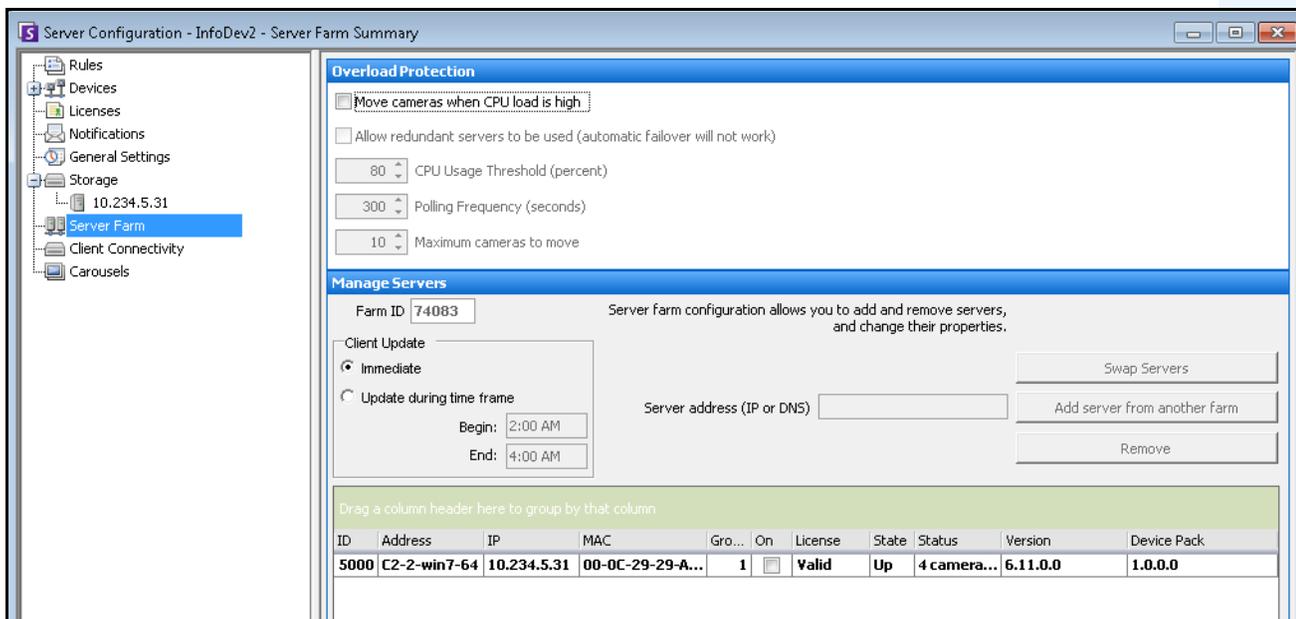


Figure 2. Server Farm

## Overload Protection

Each server monitors its own CPU load every <**Polling Frequency**> seconds. If it detects its CPU load exceeding <**CPU Usage Threshold**>, it finds another server in the same redundancy group with the lowest load. If redundancy is off, or the current server has the lowest load, no swapping occurs.

Once a server is found, cameras are moved starting with the highest camera ID on this server until <**Maximum cameras to move**> are moved, or 25% of the total cameras on this system, whichever comes first. Cameras that are not **Movable** (as per **Failover Movability** setting [Table 1, "Network tab - Field/button description," on page 17](#)) are not moved.



**Important:** CPU overload protection works if you are using a file storage device (for example, NAS) instead of block storage (such as SAN or a local disk) because the pool of storage does not follow the camera when it is moved. If you have central storage (with a NAS), the storage is always accessible from any server.

---

## Procedure

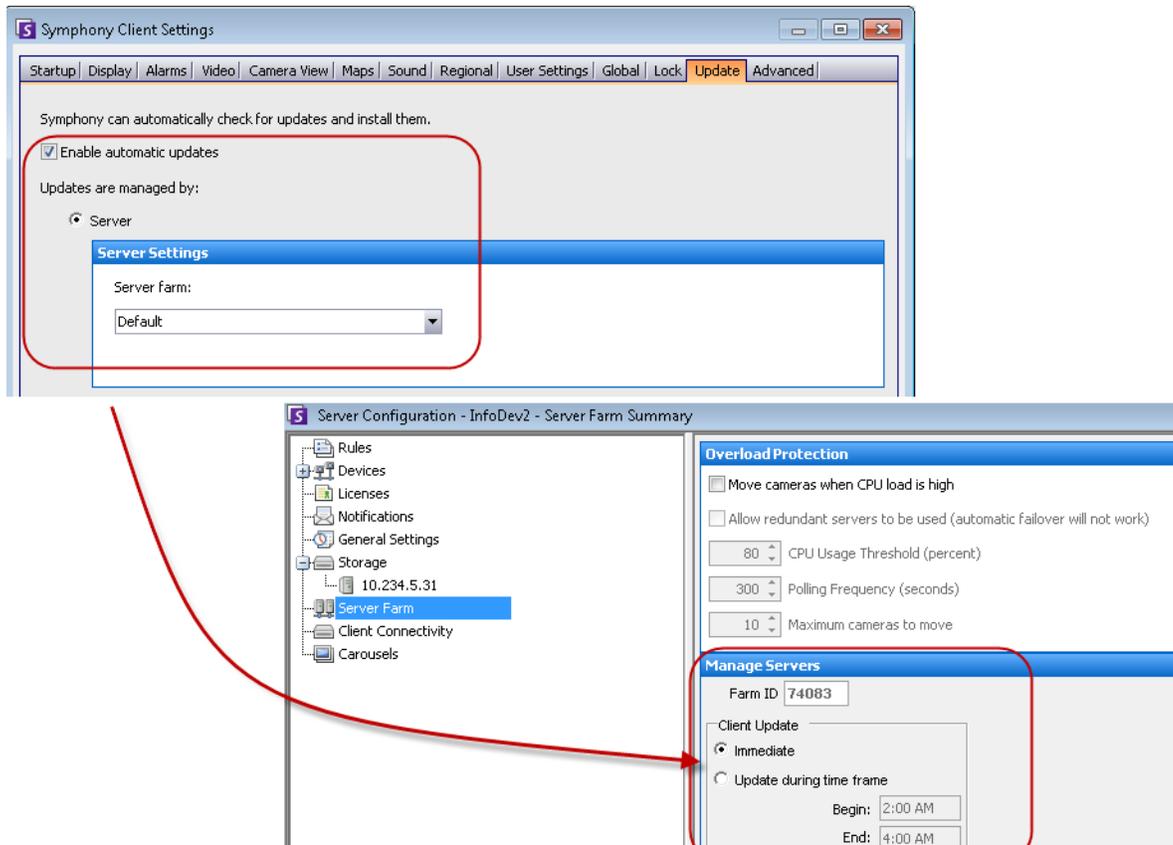
---

### To set up overload protection:

1. Select the **Move cameras when CPU load is high** to enable all other fields.
2. (Optional) Select the Allow redundant servers to be used check box. If you select this option, automatic failover will not work. (See ["Failover" on page 76.](#))
3. Use the default settings or change as necessary for the following:
  - **CPU Usage Threshold (percent)** - The CPU percentage that must be exceeded before cameras are moved.
  - **Polling Frequency (seconds)** - The number of seconds between checks.
  - **Maximum cameras to move** - 25% of the server's current camera count up to this maximum will be moved.
  - Whenever the CPU is high enough that overload protection is required, a message is sent to the Symphony User indicating Redundancy Off, No server available, or Moved x cameras.

## Manage Servers - Client Update

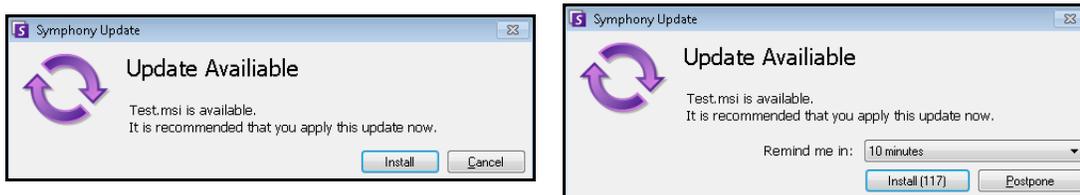
If in the Symphony **Client Settings** for a particular client, you have selected that the server manage Device Pack or Client updates, then you must indicate when Device Pack or Client updates will be installed on the Client machine.



**Figure 3. Device Pack Update Installations Managed by Server - Example**

- **Immediate** - The Device Pack or Client update is installed immediately.
- **Update during time frame** - The Device Pack or Client update will be installed in the time frame selected.

The Client user will be prompted with one of the following messages during an installation:



**Figure 4. Device Pack Installation Update Message to Client User - Example**

- If any issues are encountered during the installation process, consult [Device Pack Installation Errors](#).
- For Device Pack Installation Wizard instructions, consult [How to install a Device Pack](#).
- [How to change download scheduling and speed for Device Pack and Symphony Client updates](#)

## Farm Setup

You can create a server farm two ways:

- One at installation - refer to the Aimetis Symphony Installation Guide.
- By merging existing farms into a single farm - See "[Creating a Farm from Multiple Existing Farms](#)"

### Creating a Farm from Multiple Existing Farms

The following steps will create a multi-server farm from 2 or more existing farms.

#### Procedure

##### To create a multi-server farm from existing farms:

1. Save configuration settings for each server:
  - a. If upgrading servers, save configuration settings for each server.
  - b. When uninstalling, select the **Save Settings** option.
  - c. Ensure all servers are installed as or upgraded to the same version of Symphony (6.2 or later).
2. On all servers enable SQL remote access. For instructions, see, <http://support.microsoft.com/default.aspx?scid=kb;EN-US;914277>
3. Choose one server to be the master, for example, Server A.
  - a. On the Aimetis Xnet web account, select the **Servers** link from the left panel.
  - b. Click on Server A's ID to launch the **Server Settings** page.
  - c. The ID for server A will now be considered the Farm Id. All other servers and their ID's will become void once they are in the Farm.
  - d. Click the **Add Server to Farm** link to add the MAC addresses of all child servers to server A.
  - e. Refresh the **Settings** page for server A to ensure all MACs have been added correctly.
4. Start Symphony Client and register the farm by [farm name] or server A's IP address or DNS name. From the **File** menu, select **New Symphony Server Registration**.

Figure 5. Register Symphony Server

5. Open the **Server Configuration Licenses** page:
  - a. From the **Server** menu, select **Configuration**. The **Server Configuration** dialog box opens.
  - b. In the left pane, select **Licenses**. The **Licenses Summary** is displayed in the right pane.
  - c. Click the **Refresh licenses from Aimetis** button.
6. In the left pane, select **Server Farm**. The **Server Farm** information is displayed in the right pane.
  - If this page is not available it may be because some standard camera licenses exist. Server farms will only work if there are no standard licenses. All camera licenses must be Professional and/or Enterprise.
    - a. In the **Server address** field, enter the IP address or DNS name of a child server to merge into the farm. Do 1 child at a time.
    - b. Click the **Add server from another farm** button. This will add the child to the farm, transfer all cameras and rules from the child server to the farm's database (residing on server A), and change the database connection string on the child to point to server A's database.
7. Restart server A and the child server that was just added.
8. Ensure that all cameras from the child have been added correctly, as well as all rules and masks.
9. Repeat steps **6a** to **8** for remaining servers.

## Master Server

At all times one of the servers is deemed Master. The Master takes on the additional task of controlling the operations of a failover. If the Master happens to be the down server, another master is quickly designated to take over the failed master's duties.

## Redundant Server

A redundant server is a server currently running 0 cameras. Upon detecting a server as being down, a redundant server is used to replace the down server's camera and device processing in its entirety. Meaning, all cameras will be moved and run on the redundant server. Video loss will be a little as 15 seconds.

To enable redundancy:

- you must have at least 1 redundant server available at all times (one with 0 cameras).
- the redundant server must be in the same **Redundancy Group** as the potential down server.
- redundancy must be turned **On** for that **Redundancy Group**

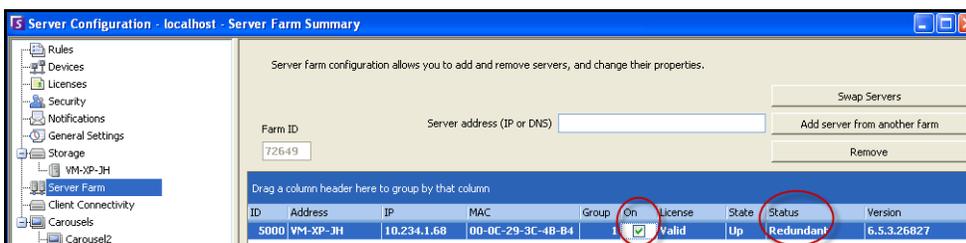


Figure 6. Redundancy for Group is On

**Example 1**



Server Farm configuration:

If either of the first 2 servers fail, their cameras will failover to the 3rd Redundant server.

ID	Address	IP	MAC	Group	On	License	State	Status
<b>5000</b>	<b>DEV15</b>	<b>10.234.1.35</b>	<b>00-19-D1-56-4A-7C</b>	<b>1</b>	<input checked="" type="checkbox"/>	Valid	<b>Up</b>	<b>4 cameras</b>
5001	10.234.1.58	10.234.1.58	00-1B-77-DF-BC-3B	1	<input checked="" type="checkbox"/>	Valid	Up	2 cameras
5002	Juke1.com	125.53.24.72	AB-CD-EF-GH-IJ-01	1	<input checked="" type="checkbox"/>	Valid	Up	Redundant

**Figure 7. Example - All three servers in the same Redundancy Group "1"**

If the first server (Redundancy Group 7) fails, no failover will occur, as there is no Redundant server in Group 7.

ID	Address	IP	MAC	Group	On	License	State	Status
<b>5000</b>	<b>DEV15</b>	<b>10.234.1.35</b>	<b>00-19-D1-56-4A-7C</b>	<b>7</b>	<input type="checkbox"/>	Valid	<b>Up</b>	<b>4 cameras</b>
5001	10.234.1.58	10.234.1.58	00-1B-77-DF-BC-3B	1	<input checked="" type="checkbox"/>	Valid	Up	2 cameras
5002	Juke1.com	125.53.24.72	AB-CD-EF-GH-IJ-01	1	<input checked="" type="checkbox"/>	Valid	Up	Redundant

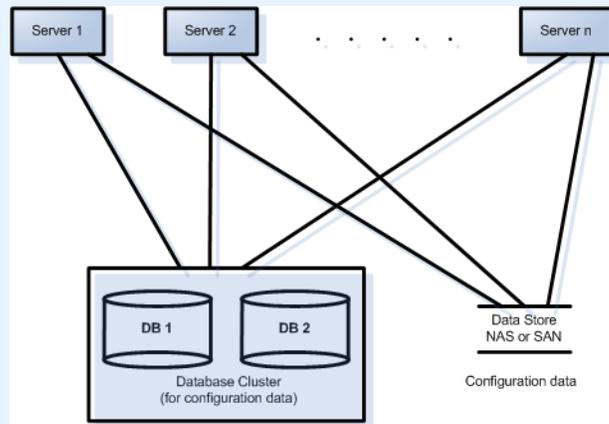
**Different Redundancy Groups "1" and "7"**

**Example 2**

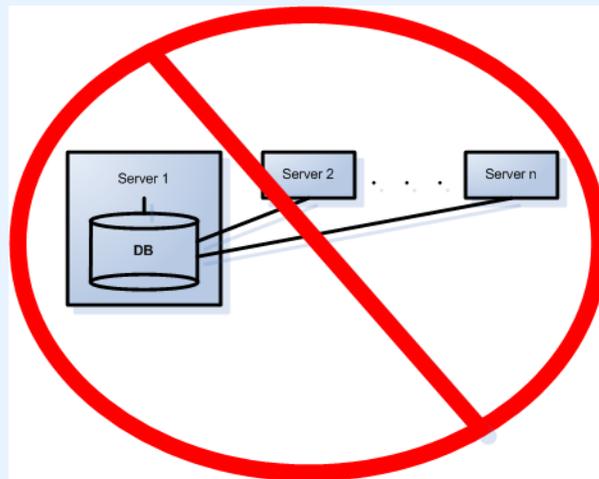


**Typical Symphony Server Farm:**

This configuration depicts use of an external database cluster for configuration data redundancy, and a NAS or SAN for historical footage file access after failover.



**Multi-server Farm with configuration database existing on one of the Symphony Servers:**  
 If server redundancy is a requirement, this is not a recommended setup, since it involves a single point of failure, namely Server 1. If this server fails, configuration is not accessible by the remaining servers.



## Redundancy Groups

Due to geographical constraints for file storage, it may be necessary for certain servers to failover only to specific servers. A redundancy group allows you to group your servers such that failover happens only amongst servers within the same group. Ensure that there is at least 1 redundant server within each server group.

## Buddy System

A **Redundancy Group** uses a buddy neighbor system where each server monitors the health of its neighbors (or buddies). Each server broadcasts an **Alive** status every second to each of its buddy servers, and each server listens for **Alive** messages from other neighbors. It is a connected graph of neighbors such that if more than one server is **down** there will always be someone to detect them.

Each server runs a monitoring thread that receives UDP socket messages from each of its buddies.

- If the detection threshold time expires without receiving an **Alive** message from a particular buddy, then that server may be **down**. A **possible down server** message is sent to the Master server.
- If more than 1/2 of the buddies notify the Master of this **down** server, it is confirmed to be **down**. In this case a failover camera swapping algorithm takes place to transfer all the **down** server's camera processing to a redundant server if one is available.

## Redundancy Configuration Settings

The following are the configurable farm redundancy settings.

**Table 2. Configuration Farm Redundancy Settings**

Setting	Description
FarmHealthStartDelayMs	On server startup, it will delay by this amount before starting to monitor for one of its buddies being down.
FarmHealthSockTimeoutMs	UDP sockets are used to receive <b>Alive</b> messages from all buddies. Each will have this timeout. (You should not have to change this).
FarmHealthMissedUdpMs	The amount of time in milliseconds a server can be down before it is determined <b>down</b> and failover is performed. Some customers may want this to be several minutes to allow a windows update reboot to perform.
FarmHealthUdpPort	Only change this if failover is not working at all and the <b>is*</b> log files indicate there are port conflicts.

These settings are NOT in the database by default. To add them, use the following lines. The last parameter is the default used.

```
dbupdater "insert into Settings (Type,ID,Section,K,V) values ('Global','','Main','FarmHealthStartDelayMs', '5000')"
```

```
dbupdater "insert into Settings (Type,ID,Section,K,V) values ('Global','','Main','FarmHealthSockTimeoutMs', '1500')"
```

```
dbupdater "insert into Settings (Type,ID,Section,K,V) values ('Global','','Main','FarmHealthMissedUdpMs', '30000')"
```

```
dbupdater "insert into Settings (Type,ID,Section,K,V) values ('Global','','Main','FarmHealthUdpPort', '5045')"
```

## Failover

A down server is detected within 30 seconds, but can be configured for any time threshold. Windows operating system updates or other maintenance that cause a reboot may be reason to increase this threshold to several minutes. Failover will transfer all the camera processes from running on the down server to running on a redundant server. It will transfer only cameras that are **Movable** according to the camera configuration as defined in the **Device** settings. Some devices are not movable by nature (USB devices, or analog cameras plugged into a video card on the down server for example). When a down server comes back up, and its cameras have been failed over to another server, it will now be considered a redundant server, since it has no cameras.



**Important:** Failover works if you are using a file storage device (for example, NAS) instead of block storage (such as SAN or a local disk) because the pool of storage does not follow the camera when it is moved. If you have central storage (with a NAS), the storage is always accessible from any server.

---

## Storage

Symphony supports both NAS and SAN storage:

- Some SANs can be configured to be accessible by multiple servers simultaneously; Symphony is agnostic to this process
- Assuming sufficient bus capacity and disk I/O, a SAN can be used for redundant storage in a farm configuration
- For further information consult your SAN documentation and support



**Important:** Aimetis **strongly** recommends a NAS in cases where failover is required.

---

Each server writes its footage and files to one of the following:

1. a data folder on the server itself
2. a logical drive on a SAN
3. a logical drive on a NAS

If method 1 is applied, the footage files for a given camera will exist on the original server up until the failover swap, from which point they will be created on the redundant server.

If method 2 or 3 is applied, the footage files for a given camera will never move. When a failover swap happens, the new server will just point to the data of the down server's logical drive on the SAN or NAS.

## On-Camera Storage (Edge Storage)

On-camera storage for AXIS cameras (also known as Edge Storage or SD card storage) provides video recording redundancy. Symphony automatically detects if an AXIS camera supports this and has been configured for on-camera storage.

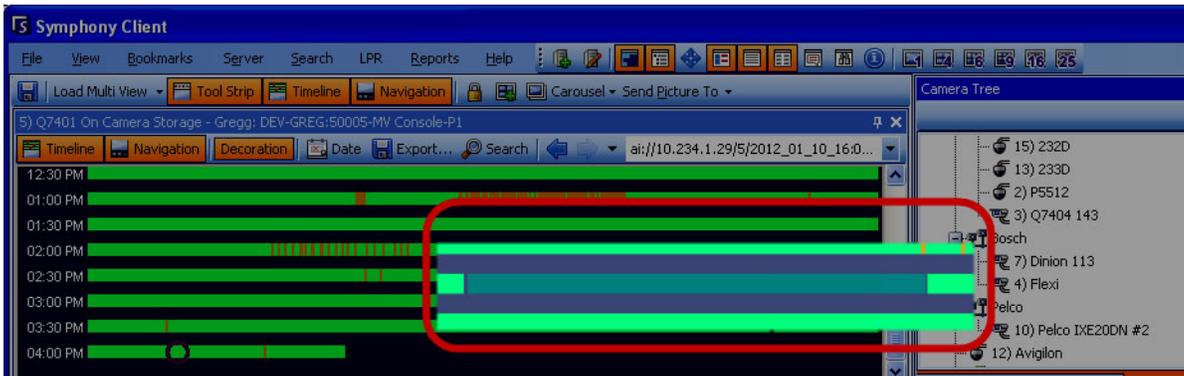


Figure 8. Green bar indicates video recorded on-camera

In the **Timeline**, a contrasting green bar (magnified in the following figure) indicates that video was not recorded locally in the Windows machine, but Symphony is already downloading the video from the AXIS camera. Symphony does not analyze video downloaded from the camera. As such, it does not determine activity type, for example, broken rule or video signal lost.

## Database Configuration

All configuration settings for an entire farm are stored in a single SQL database. For this reason it is recommended that the database reside on a reliable server in the farm, or better yet on a separate dedicated database server set up with its own redundancy system (such as a Microsoft Windows cluster).

Without a reliable server or dedicated database server, the entire farm will no longer be able to make any configuration changes, and stopped trackers will not be able to restart if the Symphony server that contains the database fails.

All Symphony servers in a farm must be granted access to the centralized configuration database. To enable remote access to the SQL server, refer to the Installation guide.

## Symphony Client

The client application can register (connect to) any server in a farm. Upon failover, if the client's registered server is the one that failed, one of the servers will notify the clients that a server is down and the registration will automatically switch to an up server to take future requests.

## Configuring a Camera Tour

By default, each Pan-Tilt-Zoom (PTZ) camera has a Home Position, where it is positioned unless a user manually controls the camera, or if the camera is automatically controlled by Symphony (for more information on auto control, see the Rule element Actions). Using the Camera Tour function, the camera can be configured to have multiple Home Positions. This effectively allows the camera to cover more area.

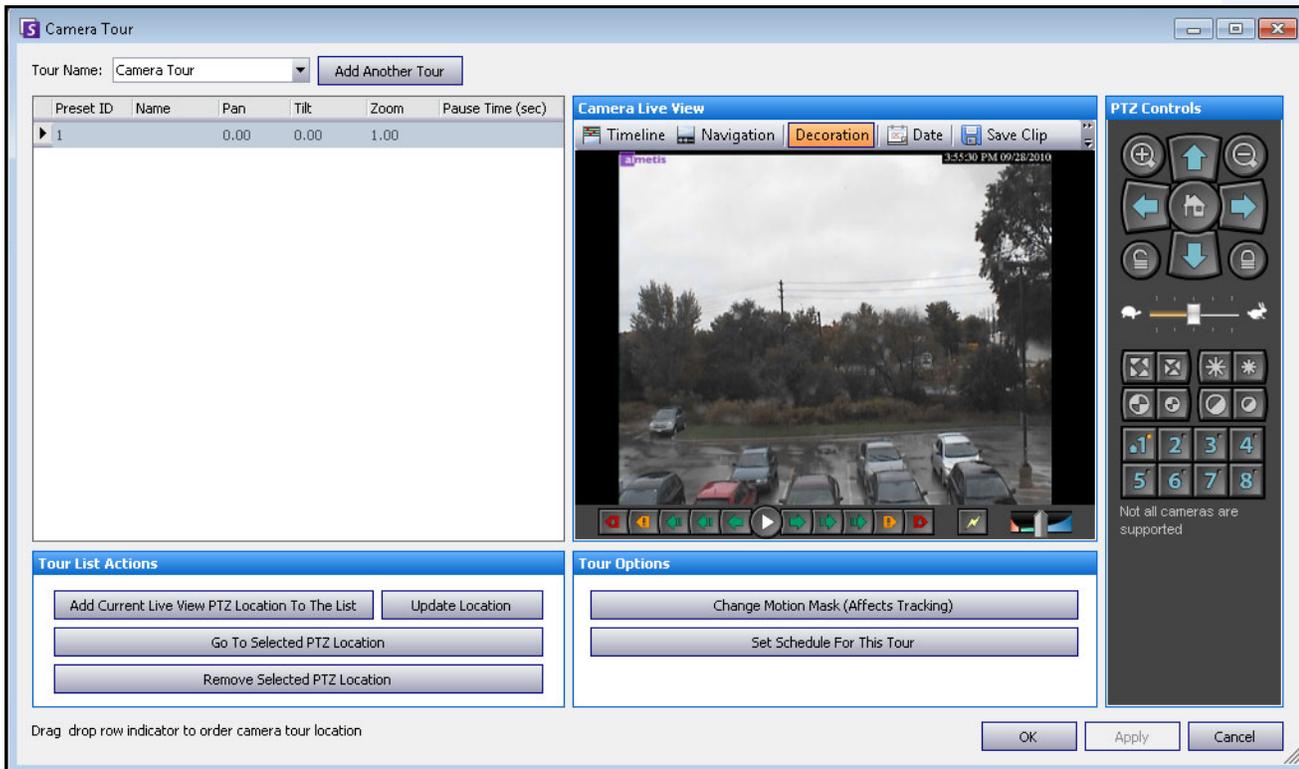


Figure 9. Camera Tour dialog box



**Important:** Analytics running on PTZ cameras in the case where the camera tour is configured but disabled may not function correctly, as the analytic settings will revert to defaults.

## Procedure

### To configure a Camera Tour:

1. Access your PTZ camera. For example, click on the PTZ camera name in the **Camera Tree**.

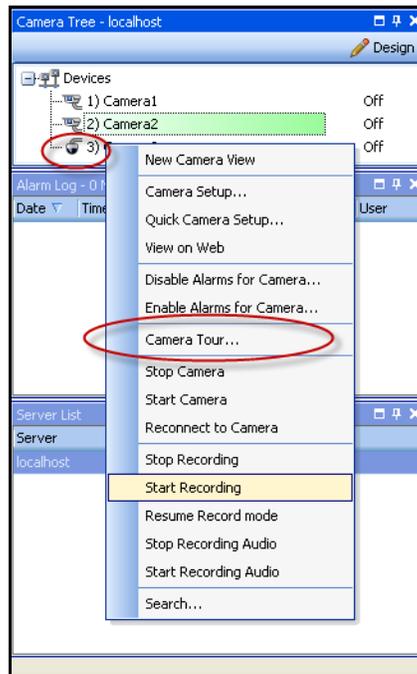


Figure 10. Right-click on the PTZ camera name

2. Right-click on the live view of the camera and select **Camera Tour** and then click **Edit**. from the menu. The **Camera Tour** dialog box opens.
3. From the **Tour Name** drop-down list, select a tour to modify. By default, there is one Camera Tour configuration. You can create multiple Camera Tour configurations with different tour locations and schedules.
4. Using the PTZ controls, move the camera to the desired location by using the arrows, and the **+** and **-** buttons to configure the zoom level.
5. To save location, in the **Tour List Actions** group area, click **Add Current Live View PTZ Location To The List**.
6. By default, Symphony will move the camera between the different locations every 600 seconds. To change this value, modify the value (in seconds) in the **Pause Time** field.
7. To modify the mask an area for the new Camera Tour location, in the **Tour Options** area, click **Change Motion Mask**. The **Server Configuration** dialog box open with the **Devices** listed and the mask tool (eraser icon) tool active.
  - This enables you to define where Symphony should track or not track objects.
  - Each Camera Tour location is much like a separate camera, since it has its own field of view. As a result, must define the **Motion Mask** area for each Camera Tour location. For more information on setting a Motion Mask, see Masks.

8. To modify perspective information for the new Camera Tour location (not all video analytic engines require this), click **Change Perspective Settings**. The Camera Tour location requires its own perspective information (to classify objects properly). For more information, see Perspective configuration.
9. To define when this Camera Tour is active, click **Set Schedule for This Tour**. Since many Camera Tours can be configured, you may decide to have a Camera Tour sequence that is different during the day than at night. The **Set Schedule for this Tour** dialog allows you to configure the schedule for this specific Camera Tour. Each Camera Tour can run on a separate schedule. Make sure that Camera Tour schedules do not overlap in time.
10. Click **Apply** to save changes and **OK** to complete the configuration.

## Managing General Settings

You can configure various system settings in the **General Settings** dialog box.

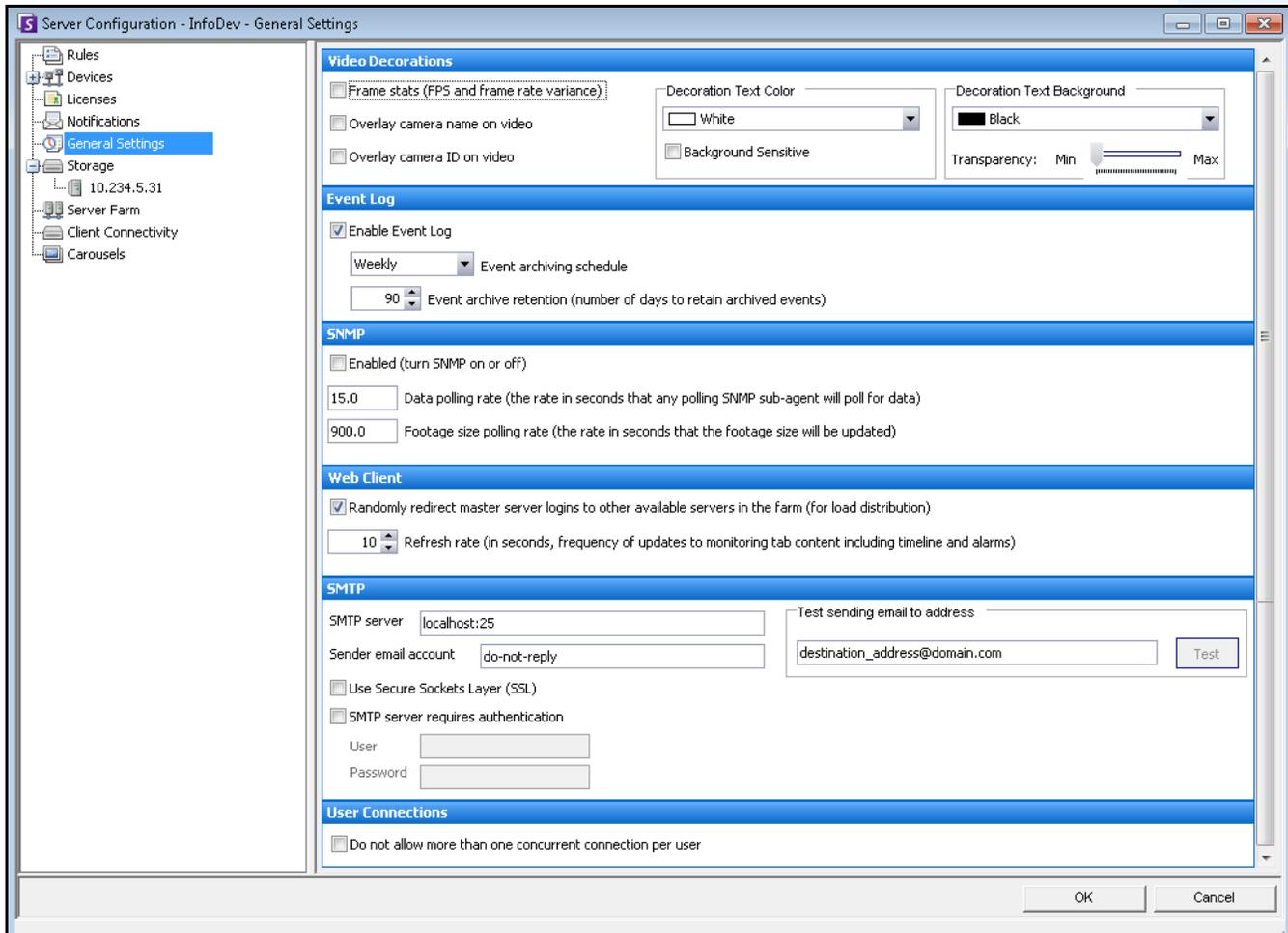


Figure 11. General Settings dialog box

## Procedure

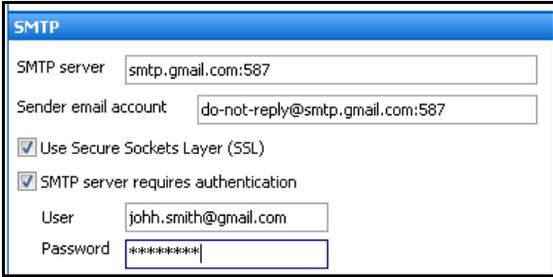
### To access the General Settings dialog box:

1. From the **Server** menu, select **Configuration**. The **Server Configuration** dialog box opens.
2. In the left pane, click **General Settings**. The **General Settings** dialog box opens in the right pane.

**Table 3. General Settings dialog box options**

Option	Task
<b>Video Decorations</b>	
Frame stats (FPS and frame time deviation)	Select this check box to display frame information on live video
Overlay camera name on video	Select this check box to display camera name on actual live video in addition to video title bar
Overlay camera ID on video	Select this check box to display camera ID on actual live video in addition to video title bar
Decoration Text Color	Select from a palette of colors for text (information) that is displayed over the video image
Background Sensitive check box	Text color automatically adjusts so as to contrast with background color of video image. For example, when the background in the video image is light, the text becomes black, and when the background in the video image is dark, the text becomes white.
Decoration Text Background	Select from a palette of colors as background contrast to the text that is displayed over the video image. Using the slider, you can adjust the transparency of the box to show more or less of the video image behind the text box.
<b>Event Log</b>	
	Schedule archiving
	Define how long events are saved before being over written
<b>SNMP</b>	
	Enable or disable SNMP. For more information visit SNMP section.
	Indicate data polling rate in seconds.
	Footage size polling rate timer (in seconds) specifies how often footage information is updated. Default value is 60 seconds.
<b>Web Client</b>	
	Randomly redirect master server logins to other available servers in the farm.
<b>SMTP</b>	

**Table 3. General Settings dialog box options (Continued)**

Option	Task
	<p>You must have a SMTP server configured on the Symphony PC. Includes username/password for the email server authentication.</p> <p>SMTP server field configurable. For Google Gmail, you must also select the Use Secure Sockets Layer (SSL) check box.</p> 
<b>User Connections</b>	
	Restrict user from logging in more than once per server farm.

# Specifying Licenses

The **Licenses** dialog box allows you to specify which license to run on which camera.

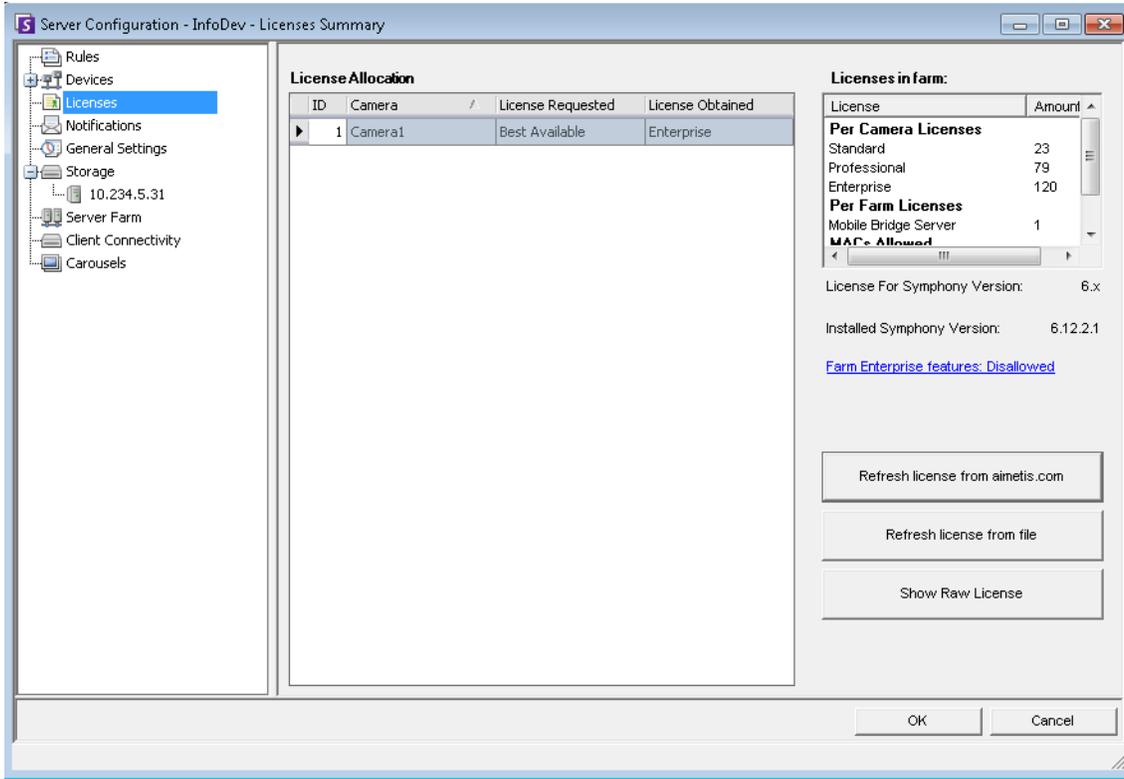


Figure 12. Licenses dialog box

## Procedure

### To view the License dialog box:

1. From the **Server** menu, select **Configuration**. The **Server Configuration** dialog box opens.
2. In the left pane, select **Licenses**. The **Licenses Summary** is displayed in the right pane. The **Licenses Summary** indicates counts of each license type per server.

## Modifying License Settings for a Specific Server

### Procedure

**To modify license settings for a specific server:**

1. From the **Server** menu, select **Configuration**. The **Server Configuration** dialog box opens.
2. In the left pane, select **Licenses**. The **Licenses Summary** is displayed in the right pane.
3. Click on the server in the **Licenses** tree in the left pane. The **Licenses Allocation** for that server appears. It displays how many licenses are available and what type of license is applied per camera.
4. To change License types between cameras, select a licence type from the **License Requested** drop-down field adjacent to each camera. If the **Licensed Requested** field does not equal the **License Obtained** field, this indicates that this license was not available.
5. Click **OK** to save changes.

**Table 4. Additional License Tasks**

Button	Action
<b>Refresh license from Aimetis</b>	If a newer license is available for your server, clicking this button will force Symphony to download the latest license file. (You must have internet connectivity for this option.)
<b>Refresh license from file</b>	If you have a Symphony server without internet access, or are otherwise unable to automatically download a new license, this option allows you to download the license and then manually apply it to the server.
<b>Show Raw License</b>	Displays the raw license in XML.



**Note:** In a Server Farm, the entire farm shares one license file. All cameras and licenses will be summarized as if it were one physical server.

## Using the Manual Configuration Editor

Symphony settings can be changed by modifying the configuration settings directly, which are stored in the SQL database. The configuration can be accessed directly through Symphony Client. This may be required for less common features that do not have a graphical user interface and must be configured through the configuration files directly.



**Caution:** Modifying configuration incorrectly can cause serious problems that may require you to reinstall Symphony. Aimetis cannot guarantee that problems resulting from incorrectly modifying the configuration files can be solved. Do this at your own risk.

## Procedure

### To manually edit the configuration files:

1. From the **Server** menu, select **Manual Configuration Editor**.
2. Modify the portion of the configuration by navigating to the value under the **Value** column  
or  
Add a new setting. Click the **Add a new setting...** field. Enter values under each column ([Figure 13 on page 86](#)).
3. Click **OK** to save changes.
4. Restart the Symphony services in order for the changes to take effect.

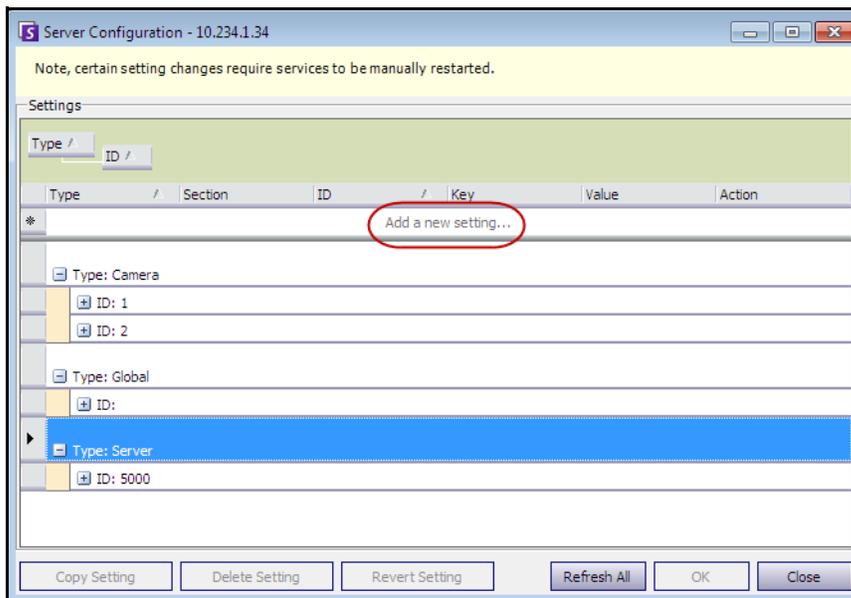


Figure 13. Manual Configuration Editor with the Add a new setting button featured

## Setting Up Notifications

Use Notifications to automatically email information to users when an event occurs on the Symphony server, for example, when some configuration has changed.

- The Notifications are NOT used for Alarms. To be notified via email whenever an alarm occurs, you must first set up **Rule Actions** in the **Email** tab of the **Rules Wizard**. This allows different users to be notified only for specific Rules triggers (for example, user A wishes to be notified in a vehicle parks, user B wishes to be notified if people are loitering).
- Each email includes the username, IP, date/time, and event-specific content.

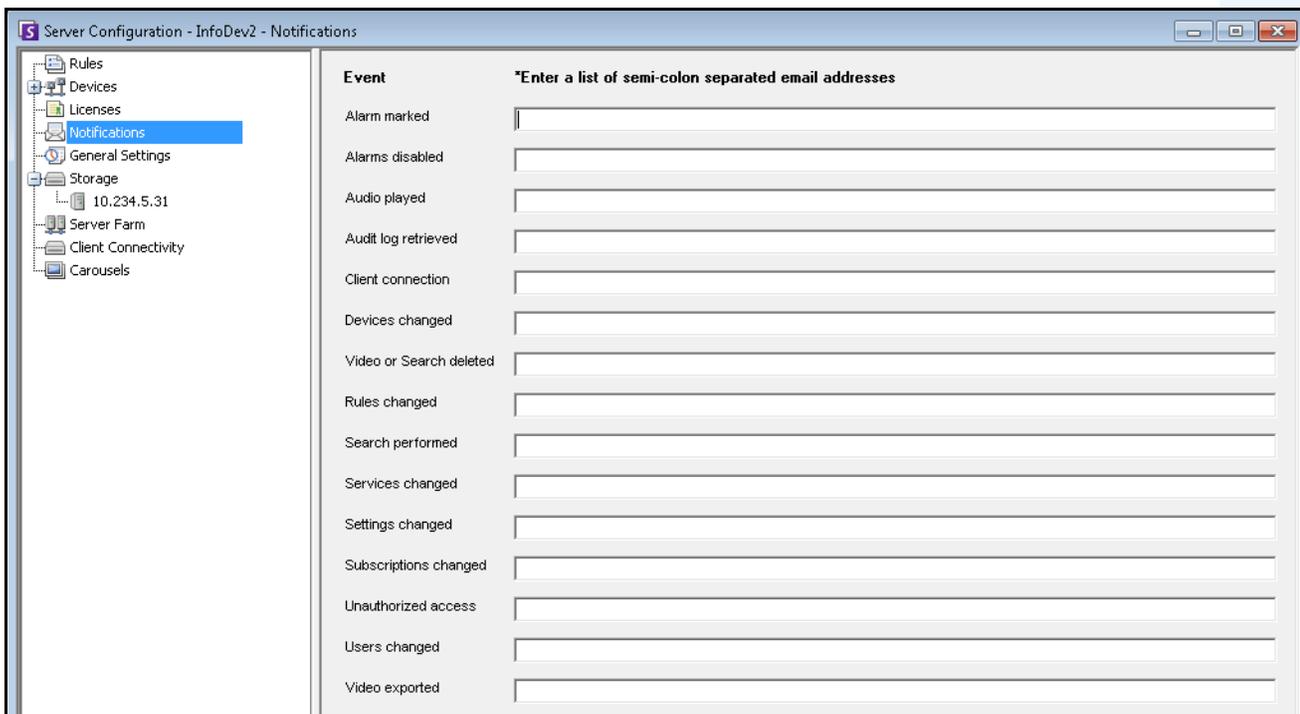


Figure 14. Notifications

## Procedure

### To view the Notifications dialog box:

1. From the **Server** menu, select **Configuration**. The **Server Configuration** dialog box opens.
2. In the left pane, click **Notifications**. The **Notifications** list is displayed in the right pane.

## Adding Subscribers to Individual Events

### Procedure

#### To add subscribers to individual events:

1. From the **Server** menu, select **Configuration**. The **Server Configuration** dialog box opens.
2. In the left pane, click **Notifications**. The **Notifications** list is displayed in the right pane.
3. Next to each event listed under the **Event** column, enter an email address in the corresponding text box. To add multiple recipients of an event, separate the email addresses with a **semicolon**. For a description of notifications, see [Table 5](#).
4. Click **OK** to save changes.

**Table 5. Event Descriptions**

Event	Description
<b>Alarm marked</b>	An alarm was marked as false or real or comments were added via the alarm log panel.
<b>Audio played</b>	A user played a sound file or spoke over the speaker using the Alarm console.
<b>Audit log retrieved</b>	The audit logs detailing everything that occurs on the Symphony server were retrieved
<b>Client connection</b>	A user connected from Symphony Client.
<b>Devices changed</b>	A user has added, deleted, or modified a Device.
<b>Exported video</b>	A user has exported video from the system.
<b>Video or Search deleted</b>	A user has deleted one of the following: <ul style="list-style-type: none"> <li>• video from the system</li> <li>• a recurring search definition: no footage will have actually been deleted as a result, the recurring search simply will not continue to recur</li> <li>• a search result: the metadata about the result will be removed as well as the .aira and .mpg files saved explicitly for that result (the original footage is untouched)</li> </ul>
<b>Rules changed</b>	A user added, deleted, or changed a Rule.
<b>PTZ Control</b>	A user has taken control over a PTZ camera.
<b>Search performed</b>	A user performed a video search.
<b>Server updated</b>	The Symphony server code was updated to a new version from Aimetis.
<b>Services changed</b>	A user changed which Services are running.
<b>Settings changed</b>	A user changed camera, video, or other miscellaneous setting.
<b>Subscriptions changed</b>	A user changed settings on this form.
<b>Unauthorized access</b>	A user tried to access something he or she was not allowed to access.
<b>Users changed</b>	Users were added, deleted, or changed

## Integrating 3rd Party Systems with Symphony

Symphony can interface with 3rd party systems (such as alarm panels or access control products) using any of following ways:

- Using I/O Device
- TCP tab in Actions
- SDK
- Packaged Integrations

### Using I/O Device

Symphony can communicate with external systems by interfacing with dry contact (or Input/Output) devices. This is the simplest form of access control support.

- To receive alarms via I/O device, configure a Rule where the input is the dry contact of a network camera or external IO device.
- Symphony can also close relay's on I/O devices by configuring the **Actions** tab in the **Rule Wizard**.

### TCP tab in Actions

Another way of sending alarms to external systems is by using the **TCP** tab in the **Actions** menu. On alarm, the Rule Action will be to send a plain text message to a designated IP/Port on the network.

### SDK

Symphony can communicate more richly with 3rd party systems via the Aimetis SDK. The SDK includes numerous sample applications with source code, which demonstrate communicating over a TCP/IP network.

### Packaged Integrations

Symphony has pre-packaged integrations with Access Control Manufacturers. For more information, refer to the Technical Paper on Access Control Support.

## Configuring and Managing a Video Wall

With Aimetis Symphony, you can create video walls by using numerous PCs and controlling them remotely through the network.

The video wall is not a physical wall but a **software representation of a collection of real monitors** displaying video.

- The collection of monitors could be on a single wall in a room or in different physical locations.
- Multiple video walls can be associated with a farm, each with different sets and layouts of monitors.

Any Symphony Client can become a Video Wall Client.

- When a Symphony Client is designated as a Video Wall Client, all monitors associated with that client can be included in a video wall.
- Any client on the network can control the monitors remotely.

For video wall functionality, Professional or Enterprise licenses must be used. No Standard licenses can be used.

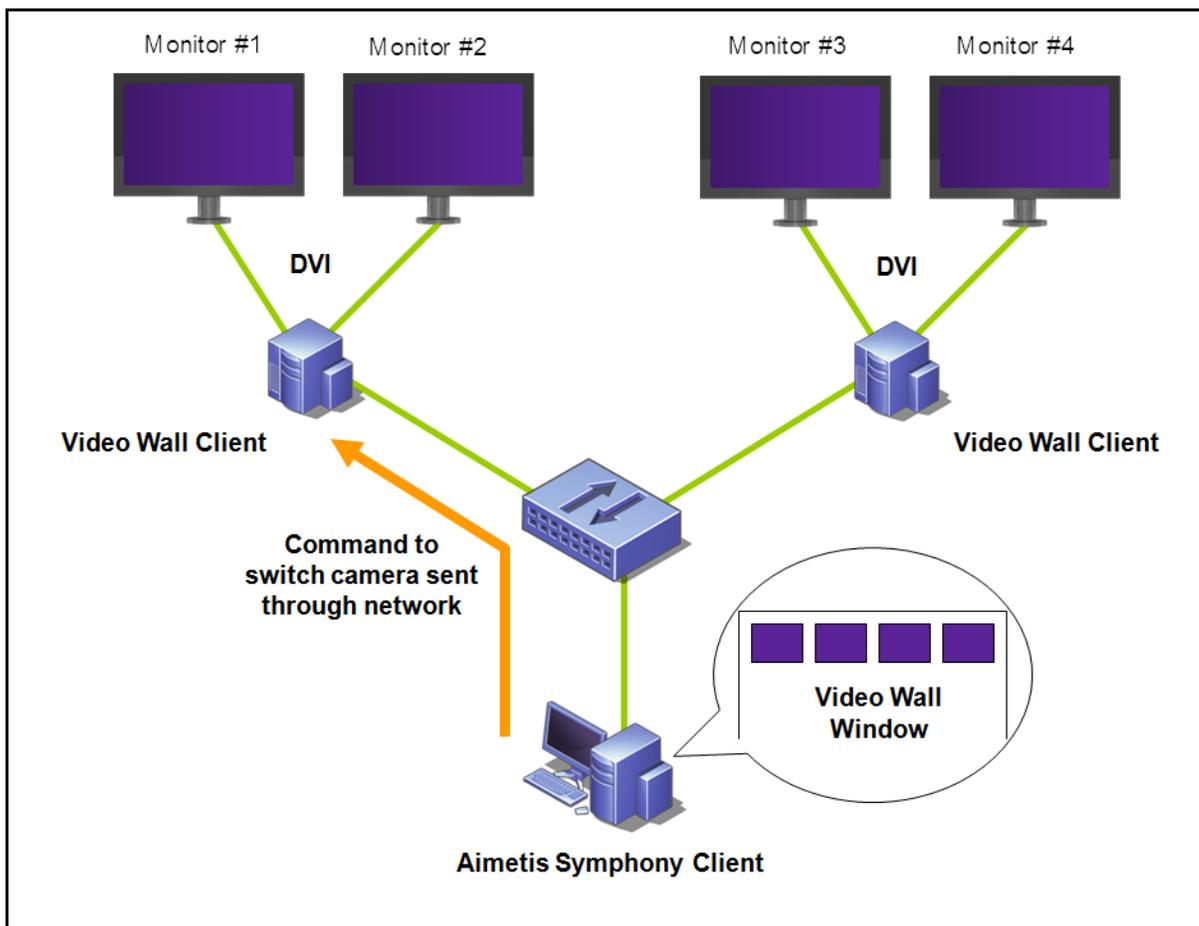


Figure 15. Video Wall

## Procedure

### To configure and manage Video Walls from SymphonyClient:

#### Task 1: Register the PCs (clients) whose monitors will be used in the Video Wall

1. Login to every computer (client) that is physically connected to the monitors which will be used in the Video Wall. Using the following diagram as an example, you would login to computer (client) **B** or **C** or both.
2. Launch the Symphony Client software.

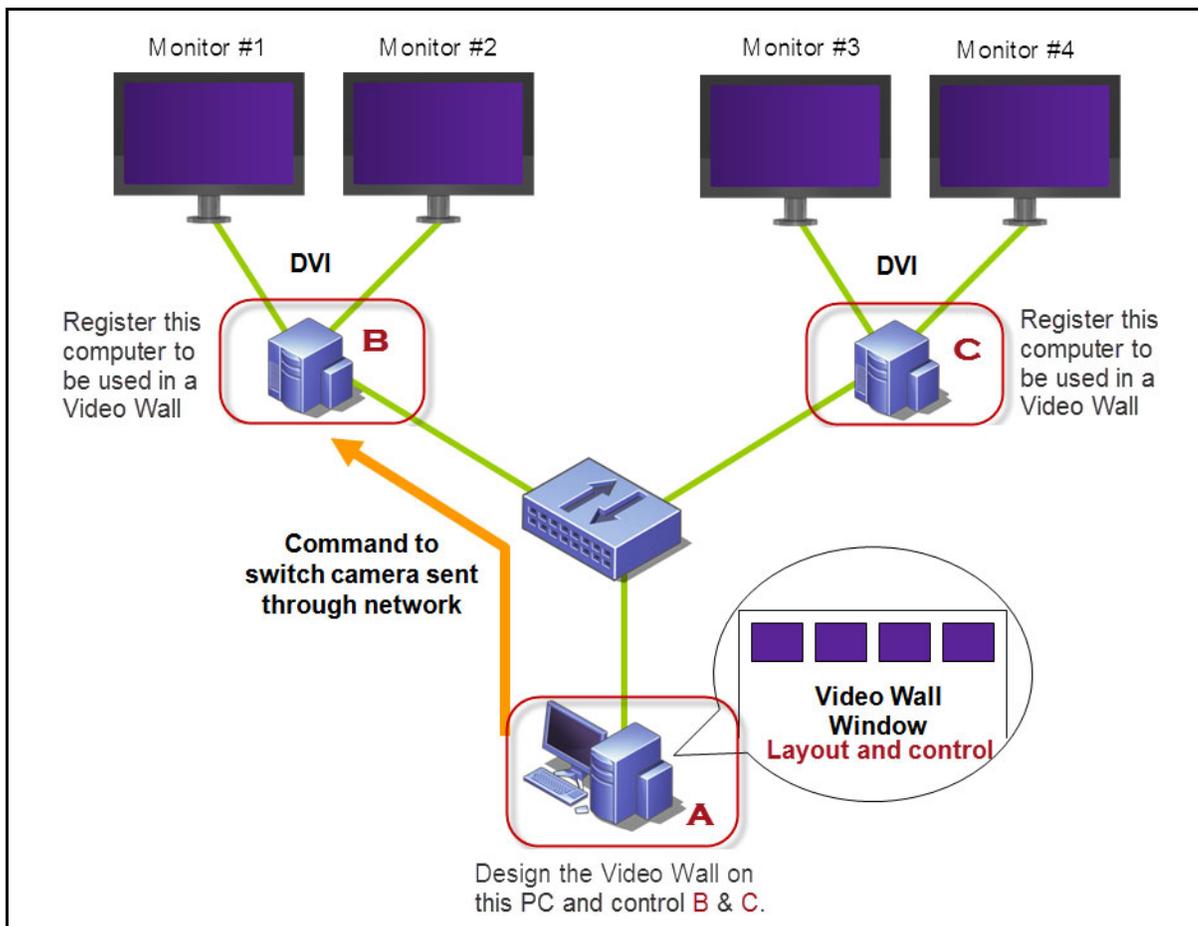


Figure 16. Video Wall setup diagram

- From the **Server** menu, select **Video Wall**.

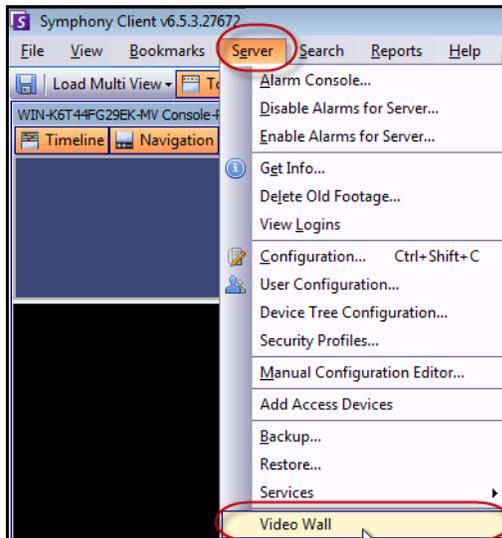


Figure 17. Server menu > Video Wall

- The **Video Wall** dialog box opens. Click the **Video Wall Client Configuration** tab.
- Click **Register current Symphony Client**. This allows you to remotely control that registered client from a video wall window you will create in **Task 2**. (You will be able to remotely control video, switch cameras, create/change/close a **Multi View** and more of that registered client.) Aimetis provides an SDK for this feature. For more details, see <https://www.aimetis.com/Xnet/Downloads/Files.aspx?P=development%2fSDK>.

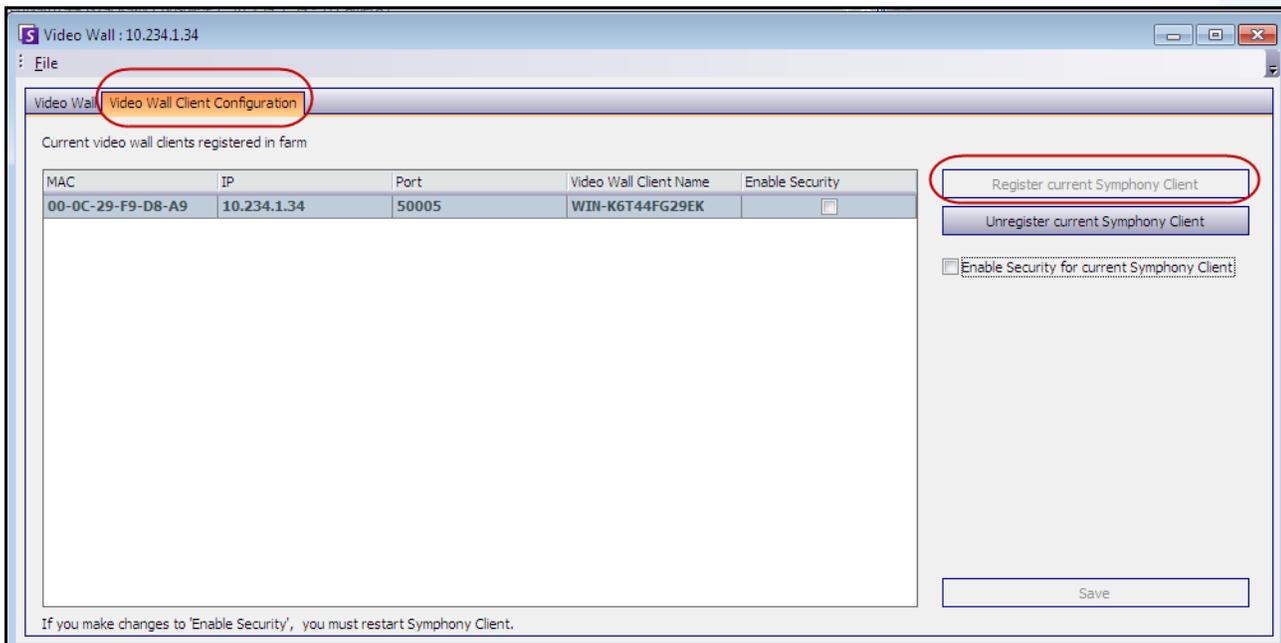
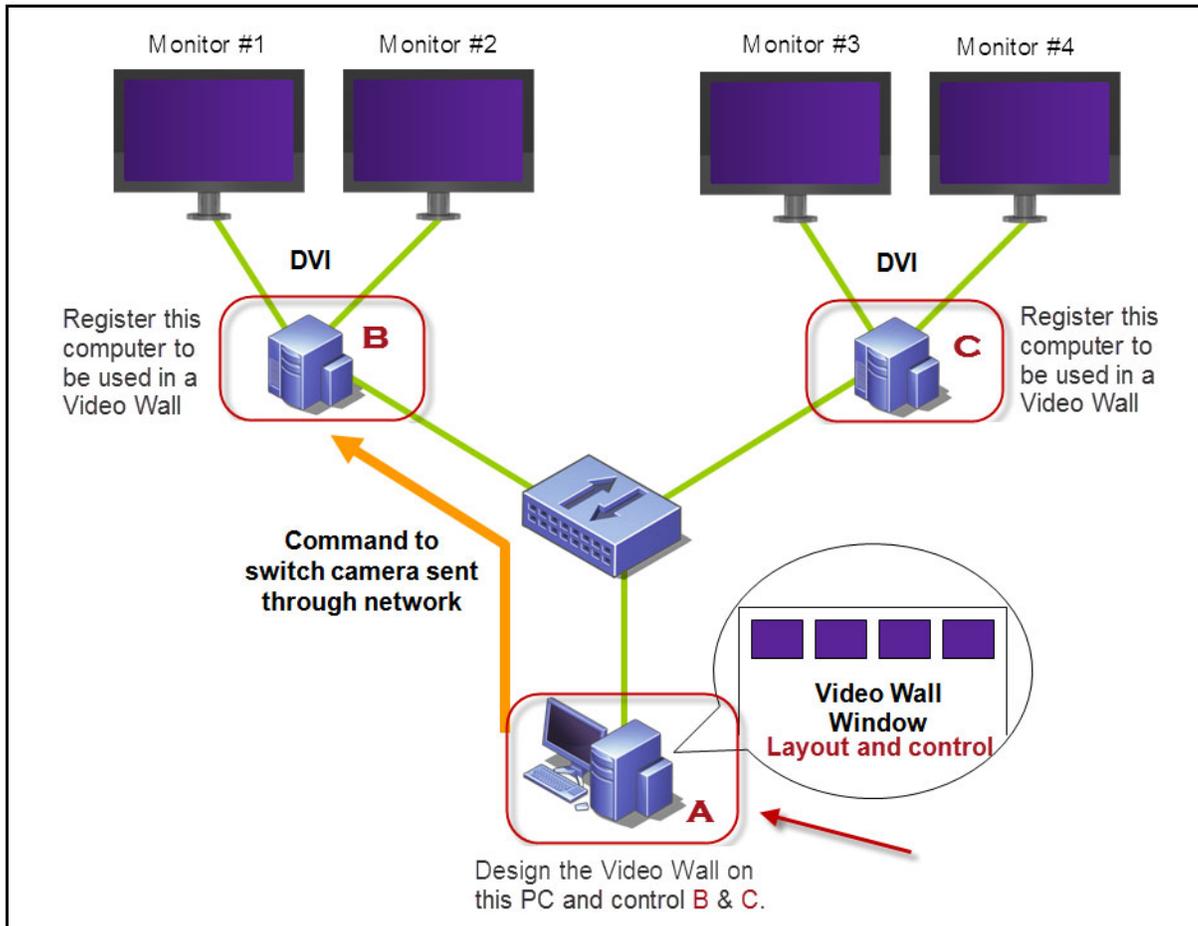


Figure 18. Video Wall dialog box

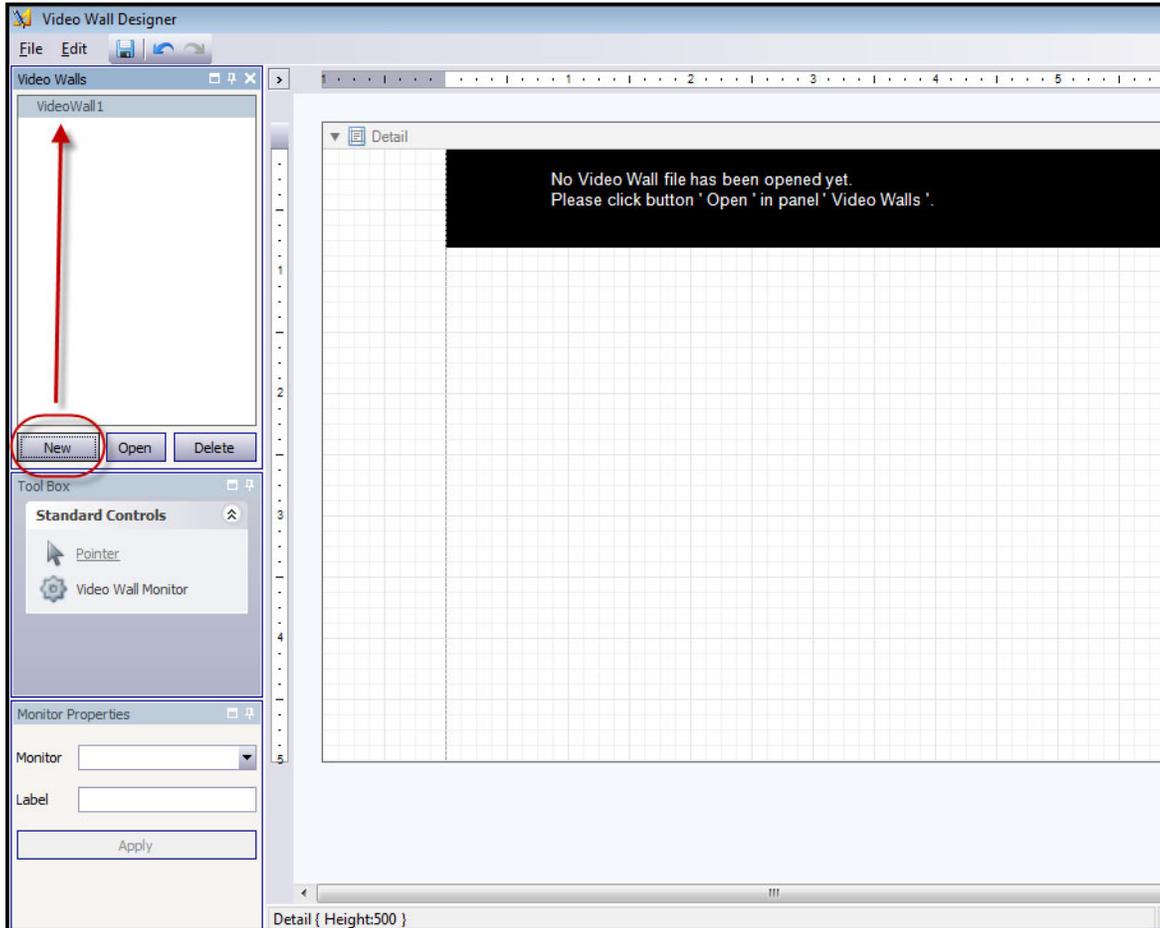
## Task 2: Design the Video Wall

1. Login to a computer (client) that you want to use to design the video wall layout and control the computers you registered in **Task 1**. Using the following diagram as an example, you would login to computer (client) **A**.



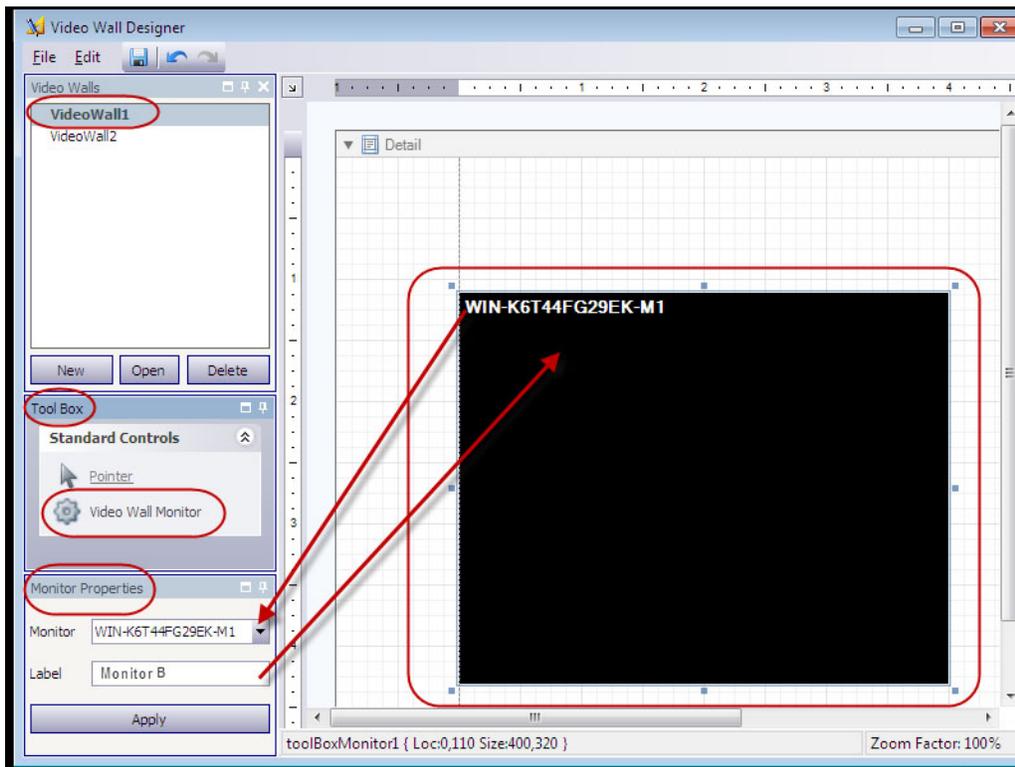
**Figure 19. Use computer A to design the video wall**

2. Launch Symphony Client.
3. From the **Server** menu, select **Video Wall**. The **Video Wall** dialog box opens.
4. From the **File** menu, select **Design Video Wall**. The **Video Wall Designer** opens (Figure 20).
5. Click **New** to create a new layout. By default, the layout is named **VideoWall1**. You can rename the layout by clicking on the name to edit/type a new name.



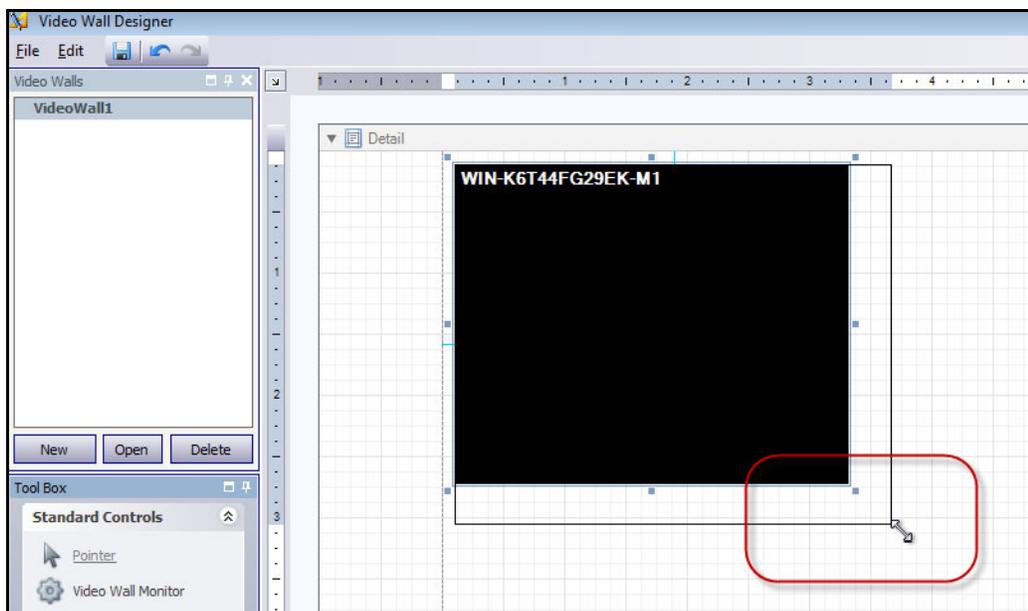
**Figure 20. Video Wall Designer**

6. Select the name of the video wall and click **Open**. A message in the layout field appears, indicating that you must now select the monitors be used in the video wall you plan to design. Using the example diagram (Figure 19 on page 93), you would select B-Monitor 1 or 2 or C.-Monitor 3 or 4.
7. In the left pane, under **Tool Box**, select the **Video Wall Monitor** icon link and drag it to the grid. If more than one monitor is connected drag it to the grid as well.
8. A black box including the name of the monitor is displayed in the grid. Click the box to activate it. The name of the monitor is displayed in **Monitor Properties** in the left pane in the **Monitor** and **Label** fields (Figure 21 on page 95).
9. (Optional) You can label the monitor with a short, easily identifiable name, for example Monitor B. Edit the **Label** field to enter the name. Click **Apply**.



**Figure 21. Changing the Label of the monitor**

10. You can resize the monitors represented in the grid. Click on the monitor and drag the sizing boxes as necessary. To move the monitor in the grid, click on the center of the black box and drag the entire box.



**Figure 22. Resizing Monitor**

11. When are you satisfied with the layout, you must save it. From the **File** menu, select **Save** and then **Exit**.

### Task 3: Adjust the Video Wall layout and control

1. Launch Symphony Client on the computer where you designed the Video Wall layout. (For example, in [Figure 19 on page 93](#), that would be computer A.)
2. From the **Server** menu, select **Video Wall**. The **Video Wall** dialog box opens.
3. Click the **Video Wall** tab.
4. From the **Current Video Wall** drop-down field, select a layout. (This is the layout you saved in **Task 2**.)



**Important:** At this point, you are now in control of the display on other monitors. (Using the example diagram in [Figure 19 on page 93](#), you would be in control of the layout on Client B or C.)

---

5. You have several options to control layout on the registered monitors.
  - [“Camera Tree” on page 97](#)
  - [“Add Camera View” on page 98](#)
  - [“Change Camera View or Close Camera View” on page 99](#)
  - [“Camera View Context Menu” on page 100](#)
  - [“Camera View Context Menu” on page 101](#)
  - [“Save Current Video Wall Layout/Load Current Video Layout” on page 102](#)

## Camera Tree

To change cameras, from the main menu of the **Video Wall** dialog box, click **Camera Tree**. The **Camera Tree** panel is displayed. Drag a camera from the **Camera Tree** into the layout,

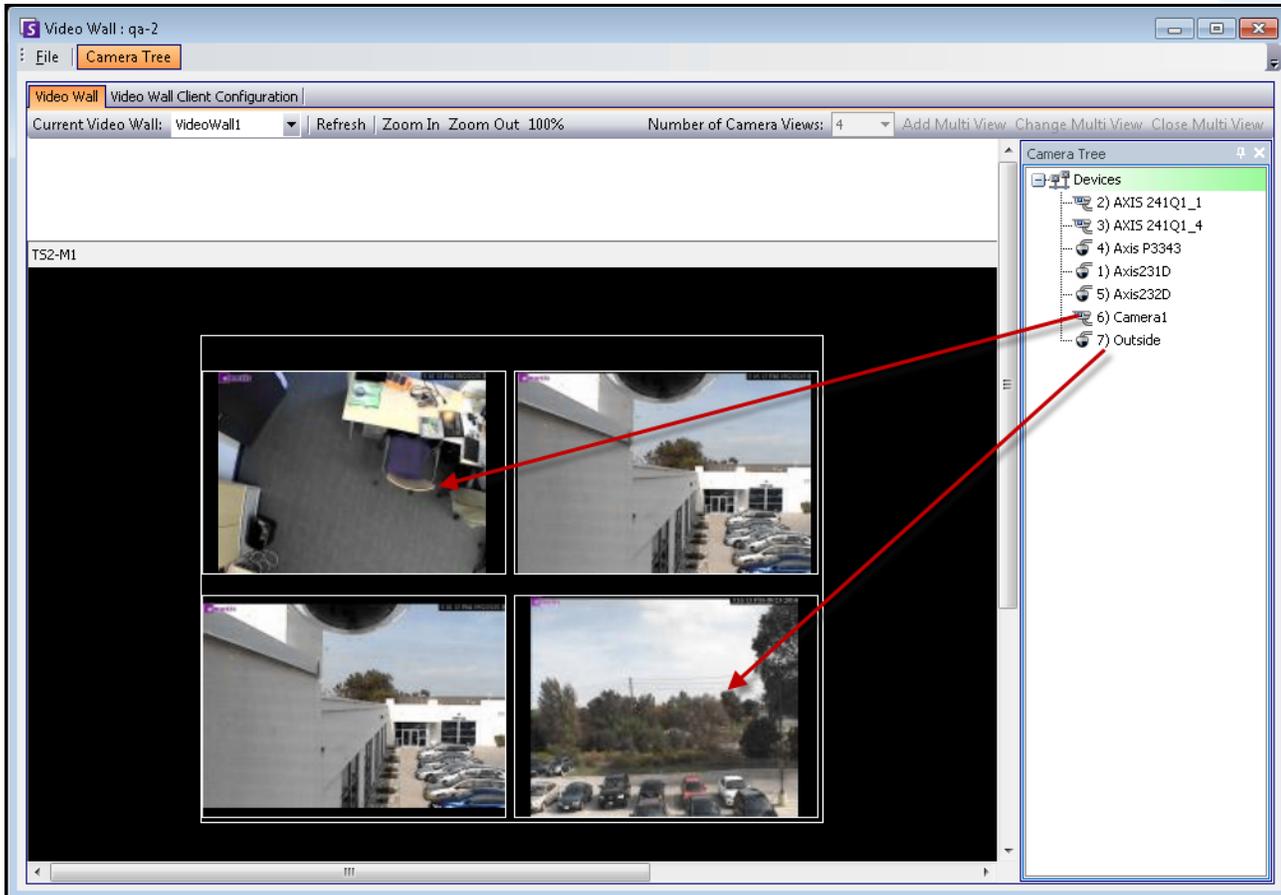


Figure 23. Drag cameras to video wall

## Add Camera View

Allows you to change the layout of the registered clients to Camera View.

1. Click title bar of the monitor to activate the button.
2. Click the **Add Camera View** button.
3. From the **Number of Camera Views** drop-down list, select the number of camera views.

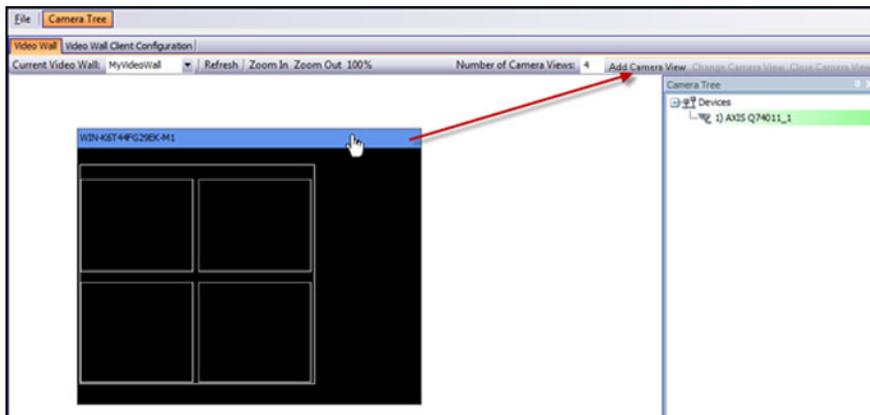


Figure 24. Activate the Add Camera View button

## Change Camera View or Close Camera View

You can change or close the views on the remote clients from here.

1. Click on the **Camera View** bar. The **Change Camera View** and **Close Camera View** buttons become active.
2. If you click **Change Camera View**, select the number of camera views from the **Number of Camera Views** drop-down list.

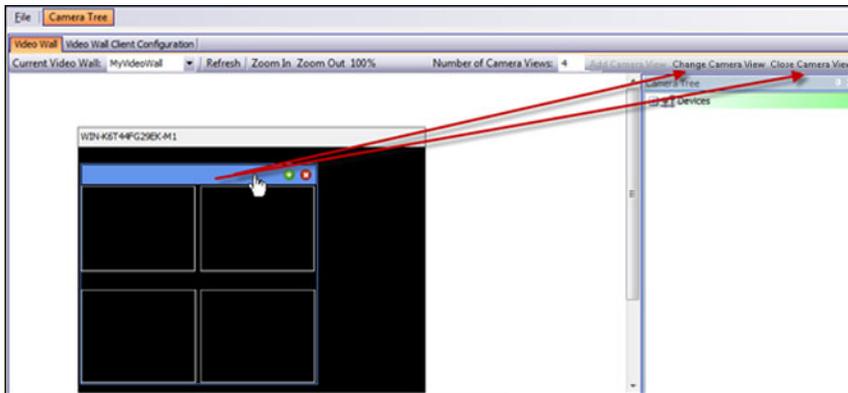


Figure 25. Activate the Change Multi View and Close Camera View buttons

## Camera View Context Menu

If you have a **Camera View** display, right-click on the multi view bar (not the monitor title bar). The context menu appears. You can show/hide the **Tool Strip**, **Timeline**, **Navigation Bar**, or display full screen on the remote clients.

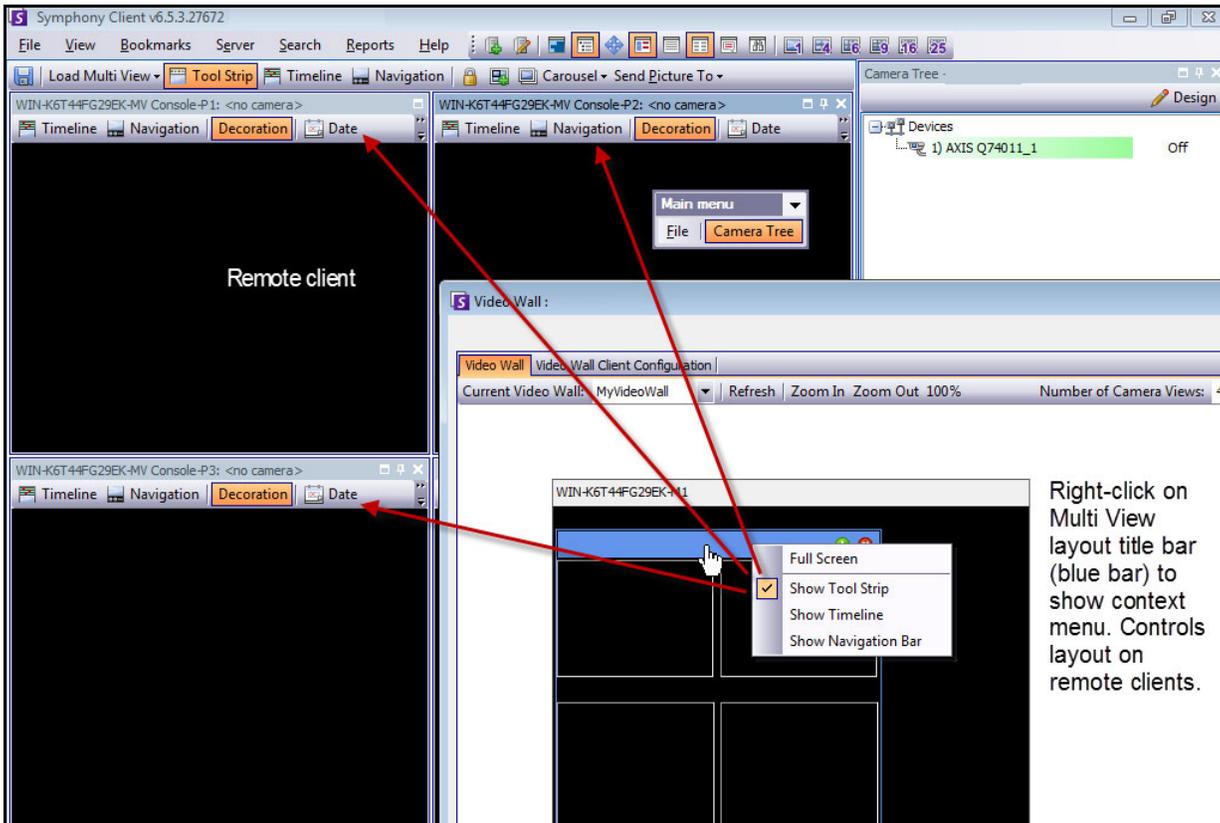


Figure 26. Remotely change the layout of all monitors

## Camera View Context Menu

Right-click on a panel (not the monitor title bar). The context menu appears. You can enable live video, show/hide the **Tool Strip**, **Timeline**, **Navigation Bar**, or change the Camera View **Settings** on the remote client.

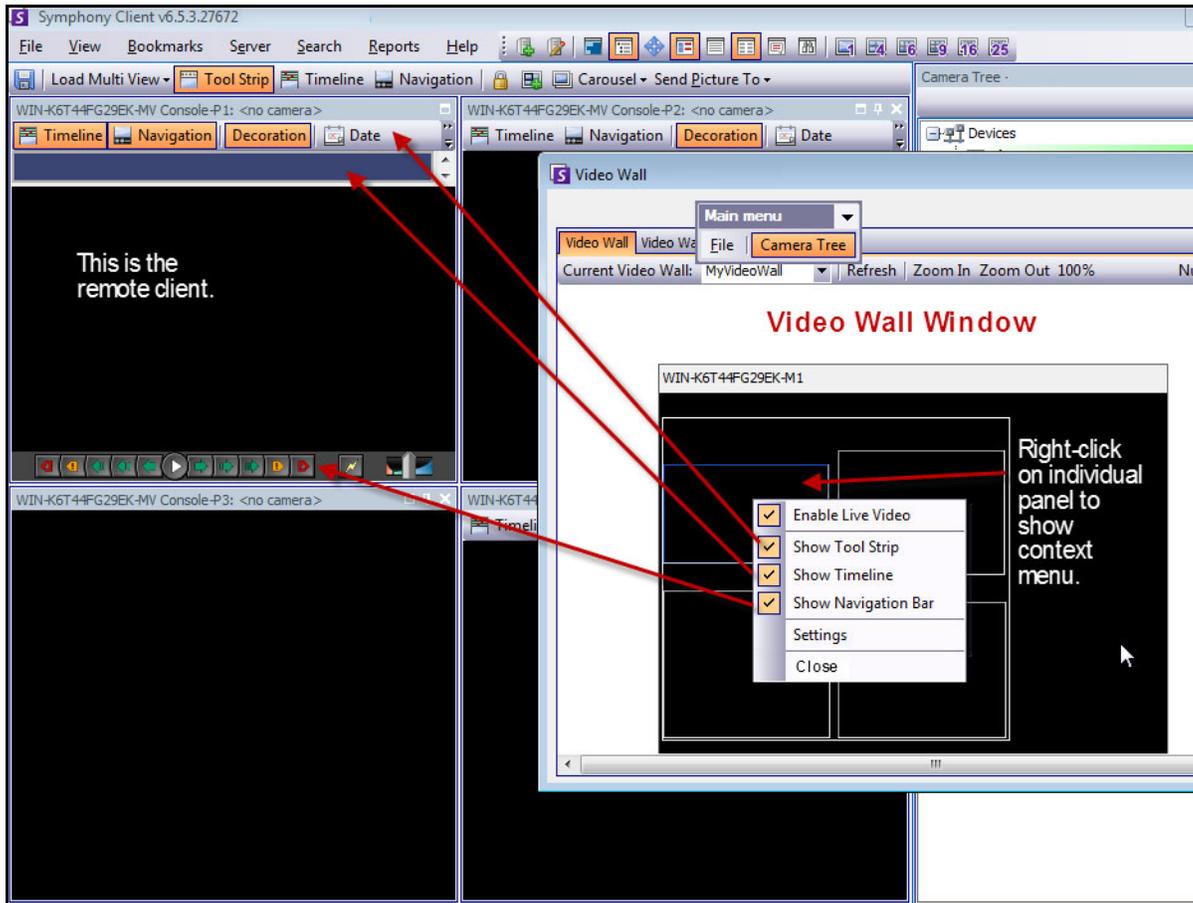


Figure 27. Change the layout in one panel

## Save Current Video Wall Layout/Load Current Video Layout



- This layout is saved on the remote computer (client) and NOT on the controlling computer. Using the example diagram (Figure 19 on page 93), the layout would be saved on computer B or C (if C is online) but not on A. Each connected (registered) video wall client saves (or loads) its client layout on its own machine.
- The layout **name**, however, is also saved in the database.

## Refresh

If you click the **Refresh** button, all screens are updated immediately; otherwise, the Video Wall Window updates each camera view screenshot in round-robin. It takes 30 seconds to update all camera views.

## Zoom In/Zoom Out

Allows you to zoom layout. It does not zoom the images on the remote (registered clients).

## Full Screen Mode

In video wall manager, you can double-click on a panel to display the image in full screen mode. Double-clicking again restores the view to the previous state.

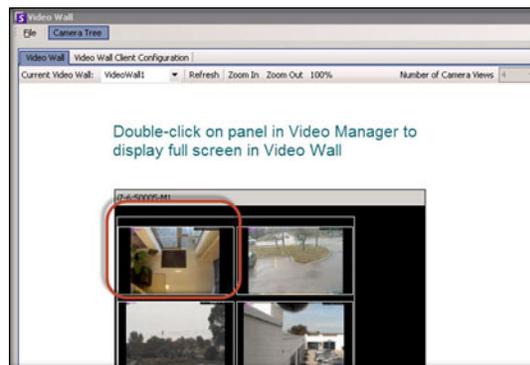


Figure 28. Full screen mode

## Viewing Detailed Logs

The **View Detailed Logs** feature provides a view of all logs recorded on Symphony server and Symphony Client.

### Procedure

#### To view detailed logs:

1. From the **Help** menu, select **View Detailed Logs**. The **View Detailed Logs** dialog box opens for the current date.
2. By default, the client logs are shown. To access the server logs, click a server in the list. The server name is displayed in square brackets.
3. For a description of menu options, see [Table 6](#). You can right-click on the menu bar to **Customize** the menu and tool bar.



**Important:** It could take several minutes to get all log files from with a slow connection.

**Table 6. View Detailed Log dialog box menu options**

Menu option	Description/Action
<b>Date</b>	Shows the logs for the current date. Click the drop-down arrow to activate the calendar interface and select another date.
<b>Copy to Clipboard</b>	Copies Entire text to clipboard.
<b>Download</b>	Zips all log files and places them on your desktop. You can then send them to Aimetis for troubleshooting.
<b>Find Next</b>	Enter text to query the log file.

## Viewing Logins

The **View Logins** feature can be used to see who is accessing a Symphony server.

### Procedure

---

#### To view logins:

1. From the **Server** menu, select **View Logins**. The **User Logins** dialog box opens.
2. From the **Date** drop-down list, select a day to view.
3. (Optional) To copy data to the clipboard, click **Copy to Clipboard**.
4. (Optional) To group by a column header, drag the column header to the top, above the other columns.
5. (Optional) To print, export, or send the log via email, click **Print and Export**. The **Preview** dialog box opens. From the **File** menu, select any of the options.

## Exporting Data from the User Logins Dialog Box

### Procedure

---

#### To export data from the User Logins dialog box:

1. From the **Server** menu, select **View Logins**. The **User Logins** dialog box opens.
2. From the **Date** drop-down list, select a day to view.
3. Click **Print and Export**. The **Preview** dialog box opens.
4. From the **File** menu, select **Export Document**, and then one of the many formats (PDF, HTML MHT, RTF, XLS, XLSX, CSV, Text, Image). Depending on your selection, additional formatting dialog boxes open, allowing you to refine your exported file.

# Displaying a List of Users Viewing a Camera

As an administrator, you can determine which users are using a camera.

## Procedure

### To display a list of users using a camera:

1. Right-click on a camera in the **Camera Tree**.
2. From the context menu, select **Users Viewing Camera**. The **Users View Camera** dialog box opens listing the user name of the user viewing the camera selected.
3. (Optional) Click **Refresh** to display an updated list.

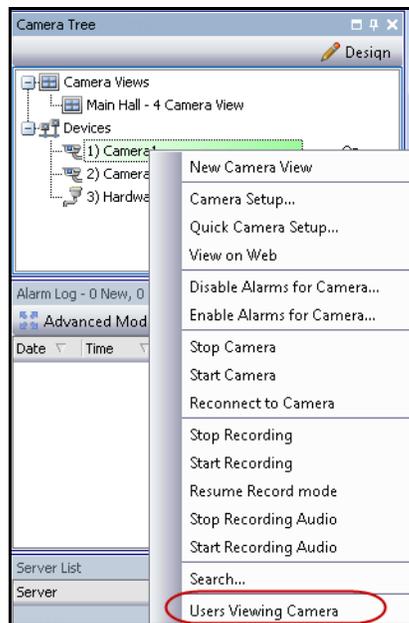


Figure 29. Camera Tree context menu

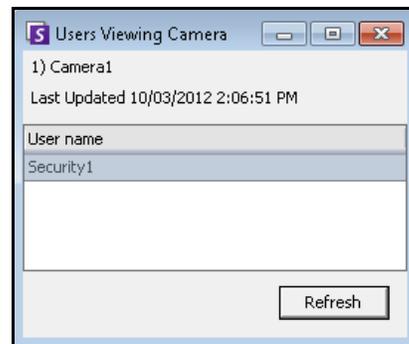


Figure 30. Users Viewing Camera

## Viewing Detailed Events

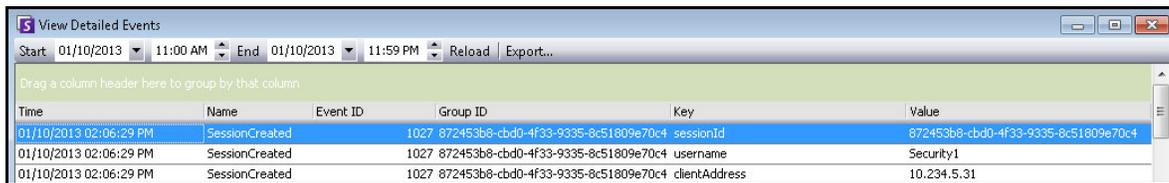
Any event or action caused by a user or the system user is logged in the database. This information may be exported as PDF, HTML, MHT, RTF, Excel, CSV, Text or image file.

Information is sorted by Time, Name, EventID, GroupID, Key and Value.

### Procedure

#### To view detailed events:

1. From the **Help** menu, select **View Detailed Events**. The **View Detailed Events** dialog box opens with events listed based on a **Start** and **End** date.
2. (Optional) You can select a specific date/time frame by selecting a **Start** and **End** date/time and clicking **Reload**.
3. (Optional) You can filter information by right-clicking a column and selecting **Filter Editor**. (The right-click menu offers various sorting options.)



The screenshot shows a window titled "View Detailed Events" with a search bar and a table of event data. The search bar contains "Start: 01/10/2013 11:00 AM" and "End: 01/10/2013 11:59 PM". The table has columns for Time, Name, Event ID, Group ID, Key, and Value. The first row is highlighted in blue.

Time	Name	Event ID	Group ID	Key	Value
01/10/2013 02:06:29 PM	SessionCreated	1027	872453b8-cbd0-4f33-9335-8c51809e70c4	sessionId	872453b8-cbd0-4f33-9335-8c51809e70c4
01/10/2013 02:06:29 PM	SessionCreated	1027	872453b8-cbd0-4f33-9335-8c51809e70c4	username	Security1
01/10/2013 02:06:29 PM	SessionCreated	1027	872453b8-cbd0-4f33-9335-8c51809e70c4	clientAddress	10.234.5.31

Figure 31. View Detailed Events

## Health Monitoring

If the **Health Monitoring** option has been purchased, Symphony Server sends every 15 minutes for each camera a health packet which contains health information about the server.

Aimetis offers a managed service that enables users to login to the Aimetis Xnet (<http://aimetis.com/xnet/>) and see the status on all Symphony Services. Health Packets are sent as UDP packets.

Each Health Packet contains the following information:

- Server name
- Server ID
- Camera ID
- Source IP address
- Version of Aimetis software running on the server
- Amount of CPU the AI Tracker has used
- How long the AI Tracker has been running
- Number of alarms
- Amount of free disk space

The health packet interval can be re-configured in the **Manual Configuration Editor**.



**Caution:** Modifying configuration incorrectly can cause serious problems that may require you to reinstall Symphony. Aimetis cannot guarantee that problems resulting from incorrectly modifying the configuration files can be solved. Do this at your own risk.

---

## Procedure

### To reconfigure the health packet interval:

1. From the **Server** menu, select **Manual Configuration Editor**.
2. Select the **Section = Main** and **Key = StatusInterval** row.
3. In the **Value** field, enter the number of seconds between packets. The default value is **900**.
  - To apply change to a single server only, select the row where **Type = Server**, **Id** = the server's logical ID.
  - To apply to all servers in the farm, select the row where **Type = Global** and **Id** = <empty string>
4. Click **OK** to save changes.
5. Restart the Symphony services in order for the changes to take effect.

## Enabling SNMP

Symphony SNMP support is built upon Microsoft's Extendible SNMP Agent. During Symphony installation, the Symphony SNMP Extension-Agent is registered with Microsoft's SNMP Agent by modifying the Windows registry.



**Important:** The Symphony **Get Info** feature provides more information than “Walking” through mib files using a SNMP query tool. See [“Receiving Full Diagnostic Information”](#) on page 117.

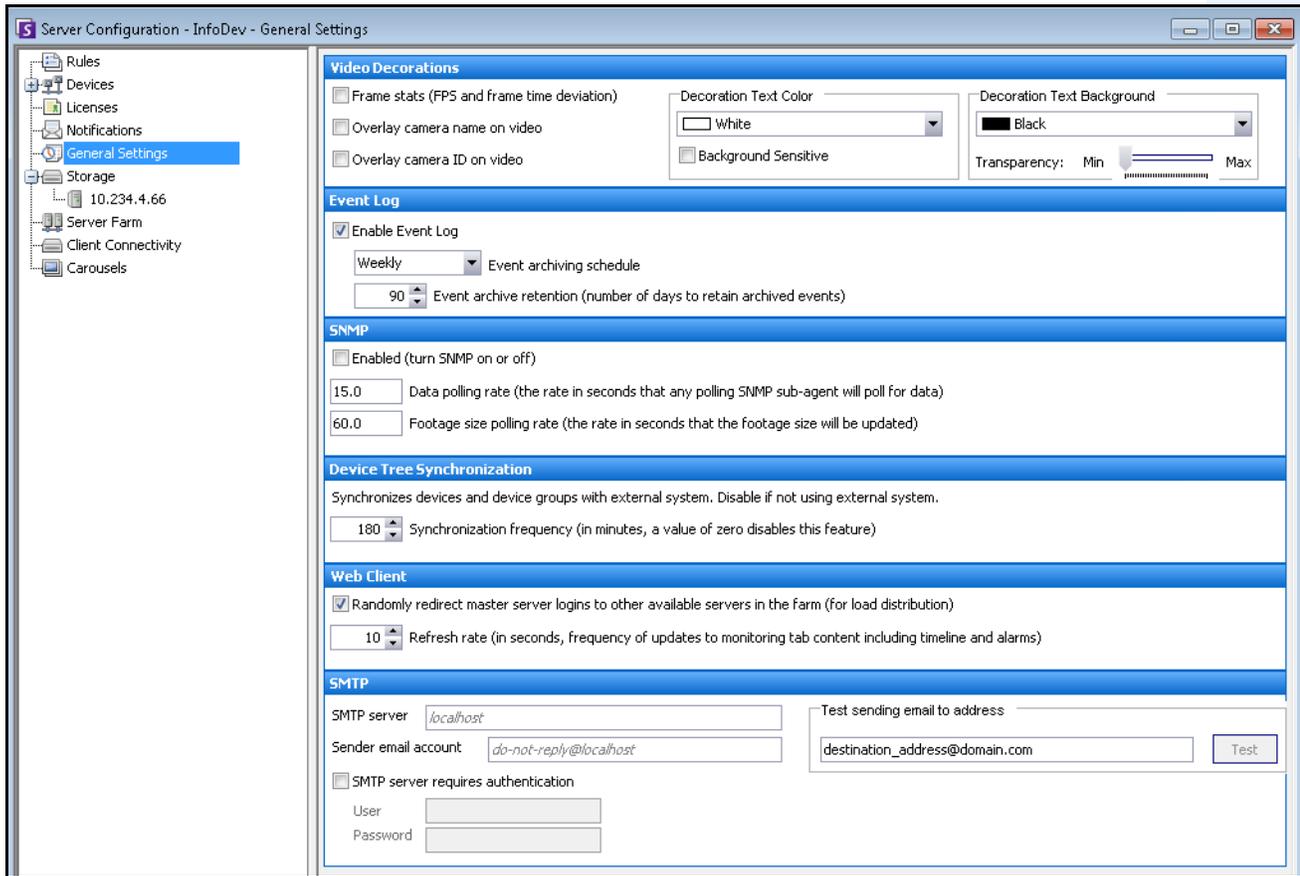


Figure 32. General Settings dialog box featuring SNMP

## Procedure

### To enable SNMP in Symphony:

Ensure that Microsoft's SNMP Windows Component is installed and set to start automatically with Windows.

#### Task 1: Enable SNMP in Symphony

1. From the **Server** menu, select **Configuration**.
2. In the left pane, click **General Settings**. The **General Settings** dialog box opens (Figure 32).
3. In the **SNMP** group area, select the **Enabled** check box and click **OK**.
4. Restart Symphony services: From the **Server** menu, select **Services**, and then **Start Symphony Services**.

#### Task 2: Configure SNMP Service Security

Microsoft's SNMP Agent supports **SNMP v2c**; therefore, the SNMP Agent must be configured with the accepted community names and hosts.

1. Ensure that SNMP service is installed on your machine: **Control Panel>Programs and Features>Windows Features>Simple Network Management Protocol(SNMP)** check box.

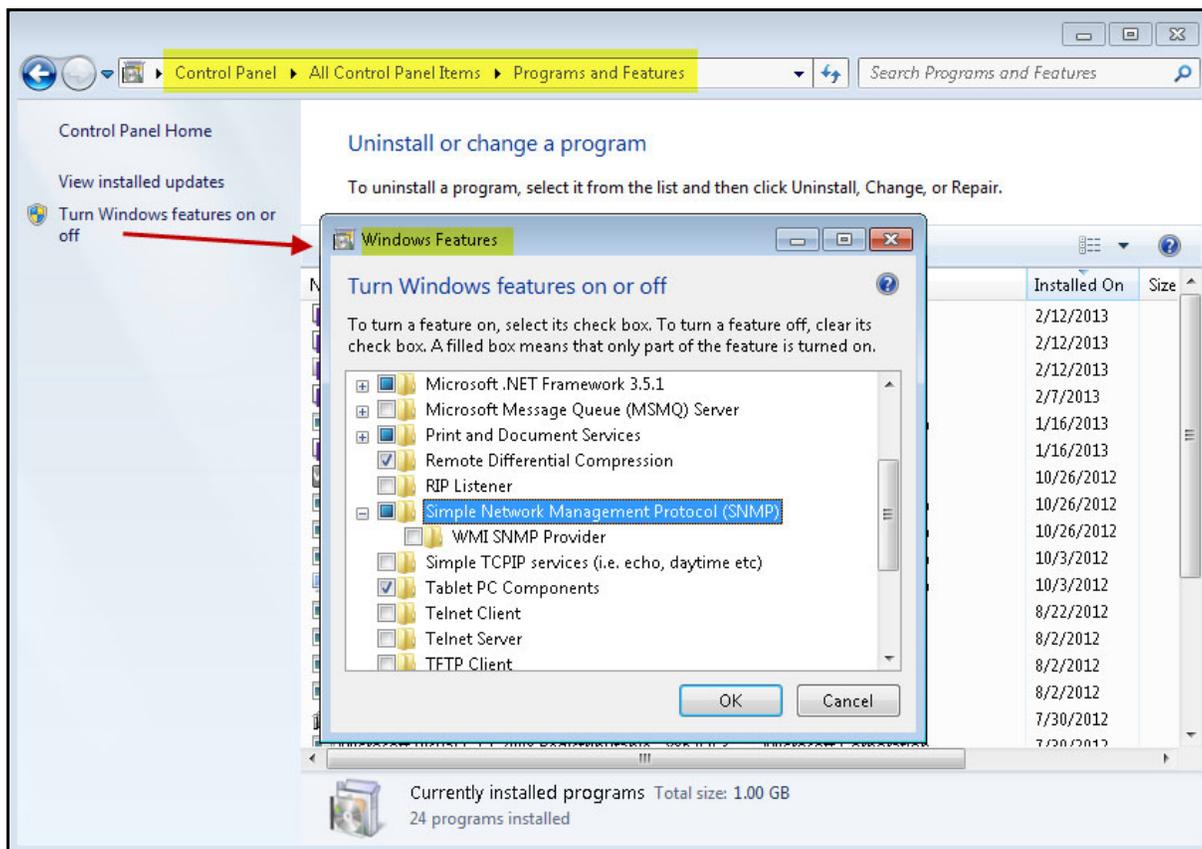


Figure 33. Windows Feature: SNMP

2. Ensure that you are logged on as local administrator; otherwise, depending on your Windows operating system, the **Security** tab in the **SNMP Service Properties** dialog box will not be accessible or visible.
3. Via the Windows **Services** management console, open the properties of the **SNMP Service**.

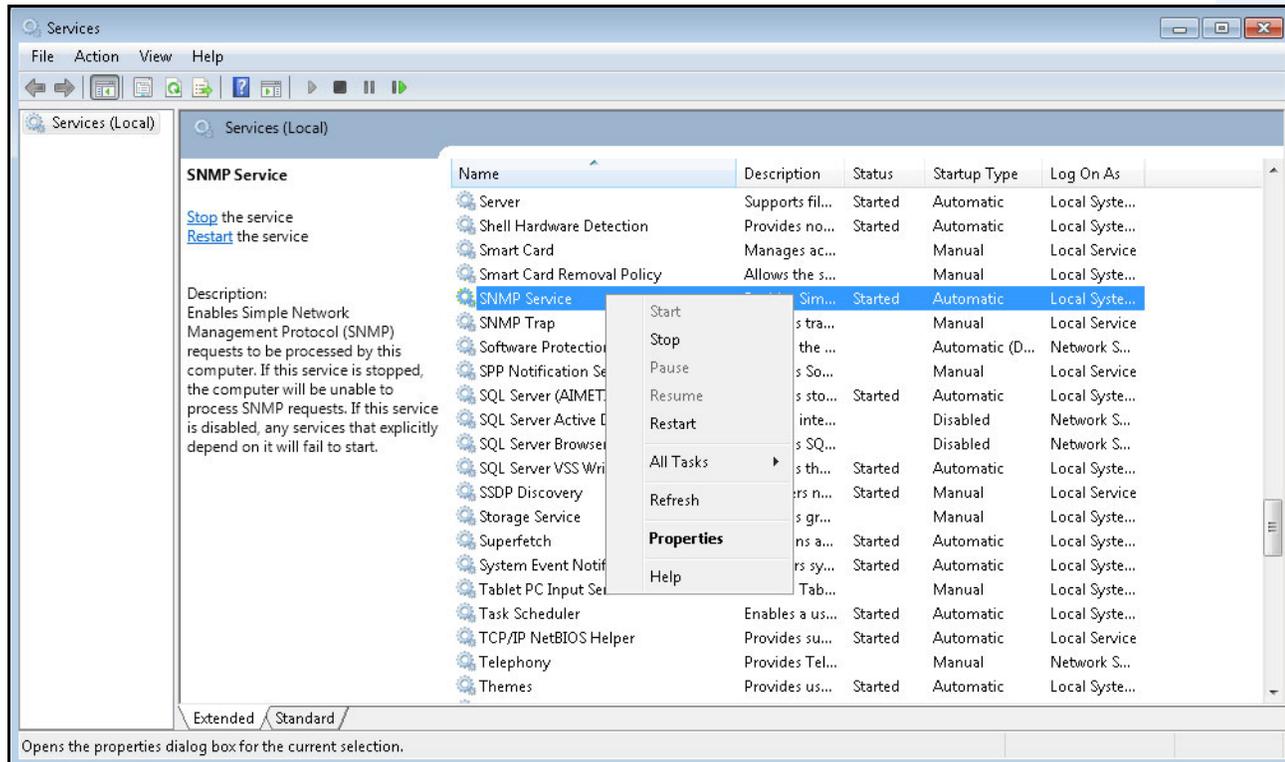
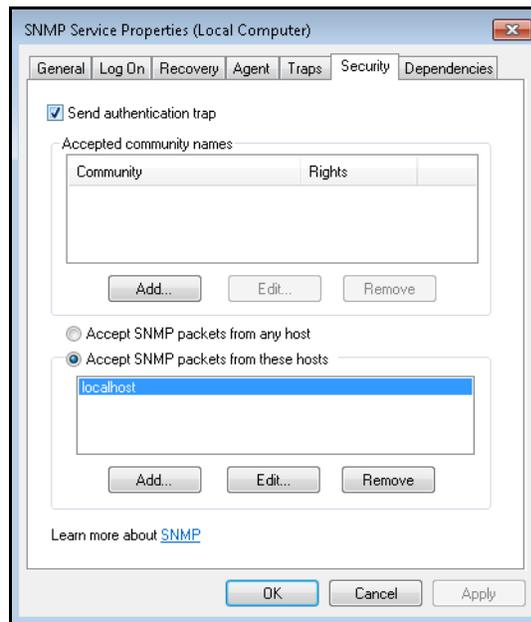


Figure 34. Windows Services dialog box with SNMP Service

4. Click the **Security** tab.



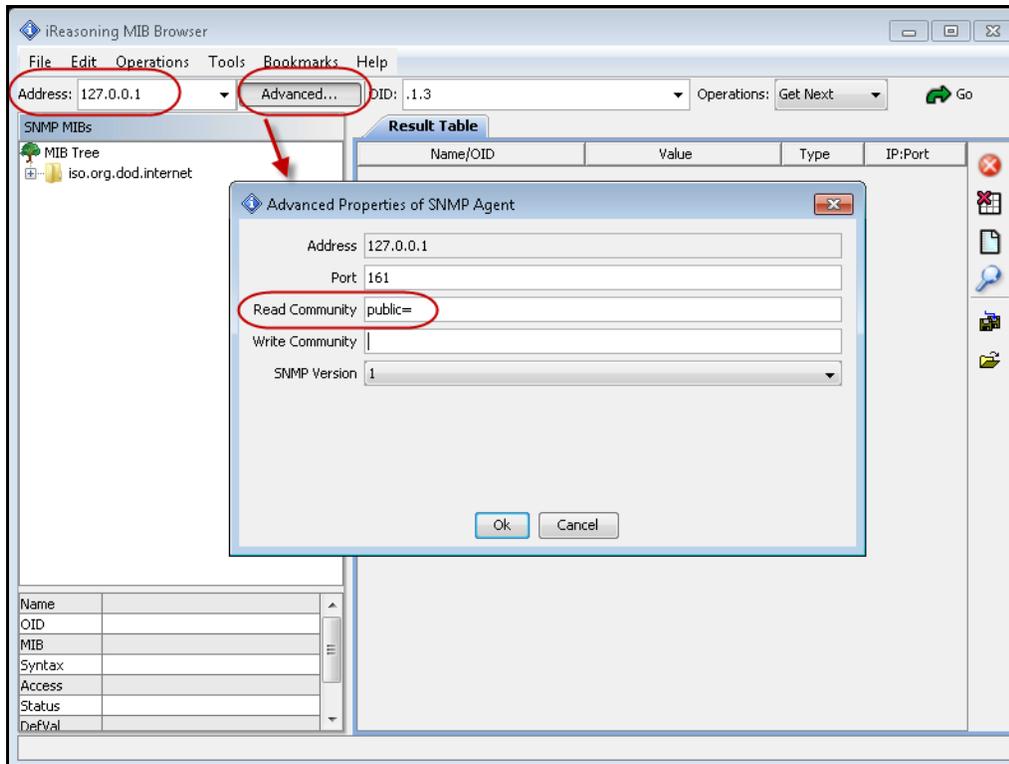
**Figure 35. SNMP Service Properties dialog box**

5. Create the desired communities (for example “public=” community with “READ ONLY” rights)
6. (Optional) Restrict which hosts may issue SNMP requests.
7. Click **OK**.

### Task 3: Test SNMP

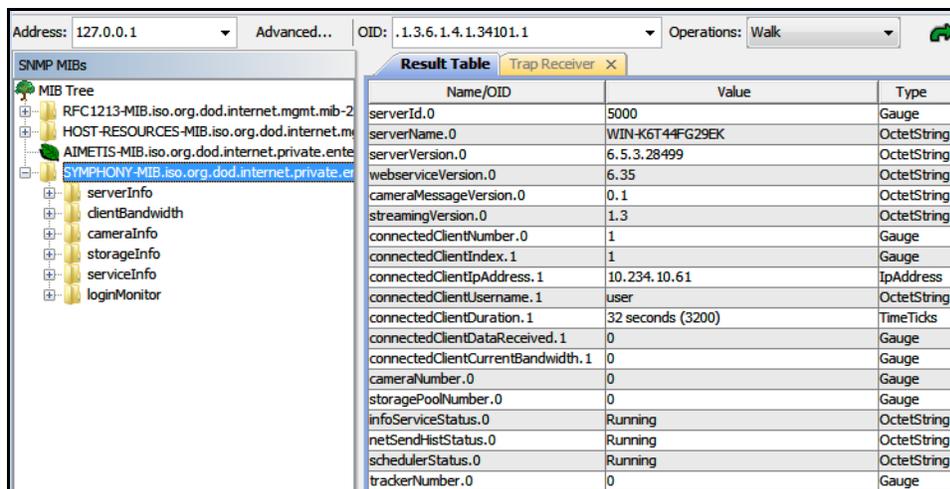
1. Start the Symphony services: From the **Server** menu, select **Services**, and then **Start Symphony Services**.  
At this time, SNMP data is provided by the **AI InfoService** and **AI Watchdog** services.
  - The **AI Watchdog** service is responsible for providing the service status SNMP values, and **AI InfoService** all other values.
  - The **AI SNMP Registry** serves as a registration of all the sub-agents (and is used by our SNMP Extension Agent).
  - The Symphony management values are rooted at object-identifier 1.3.6.1.4.1.34101.1.
2. Use an SNMP software package to query the SNMP Agent. For example, you can use a GUI tool such as the iReasoning MIB Browser: <http://ireasoning.com/mibbrowser.shtml>.
3. Start the MIB Browser and open the Symphony mib files. The Symphony mib files are typically located in the program files: **C:\Program Files\Aimetis\Symphony\mib files**.
  - If you are using the iReasoning MIB Browser, for example, you must load the Symphony mib files into the browser: **File>Load MIBs**. In the file manager that opens, navigate to and select the Symphony mib files (**aimetis.mib** and **Symphony.mib**).
  - Additionally, for **SNMP using UDP**, set **SNMP Retries** to **2**. (**Tools>Options>General tab, SNMP Retries=2** field.)

4. Enter **127.0.0.1** as the address and edit advanced options to point the program to your read community (for example “public=” community with “READ ONLY” rights).



**Figure 36. Example using iReasoning MIB Browser with Address field and Advanced options dialog box**

5. Walk all the management values currently available within the Symphony sub-tree.



**Figure 37. MIB Browser displays Symphony mib files after a “Walk” operation**

6. For individual object-identifier descriptions, consult [Table 7, "Mib file details," on page 113.](#)

Table 7. Mib file details

Category	Details	Description	Trap Yes/No
<b>server Info</b>	Server ID		
	Server Computer Name		
<b>versionInfo</b>	Server version	Assembly version of the Symphony server	
	webserviceVersion	Version for Symphony web-service protocol	
	cameraMessageVersion	Version for Symphony camera message protocol	
	streamingVersion	Version for Symphony streaming protocol	
<b>clientBandwidth</b>	connectedClientNumber	Number of connected clients to this Symphony server	
	connectedClientIndex	Unique value for each connected client	
	connectedClientIpAddress	IP address the client is connected from	
	connectedClientUsername	Username that the client is connected with	
	connectedClientDuration	Duration that the client has been connect to this server	
	connectedClientDataReceived	Data received, in Kbytes, by the client via this connection	
	connectedClientCurrentBandWidth	Current bandwidth, in Kbytes per second, between client and this server	
<b>cameraInfo</b>	cameraNumber	Number of cameras managed by this server	
	cameraID	Unique identifier for the camera	
	cameraName	Name of camera	
	footagePath	Path to camera's footage	
	footageSize	Size of camera's footage in bytes	
<b>storageInfo</b>	storagePoolNumber	Number of storage pools managed by this server	
	storagePath	Path to the storage pool	
	storageCapacity	Capacity of storage pools in Mbytes	

Table 7. Mib file details (Continued)

Category	Details	Description	Trap Yes/No
	storagePercentAvailable	Available capacity in the storage pool, as a percentage of <b>storageCapacity</b>	
	storageFootageSize	Size of footage within the storage pool in Mbytes	
	storageFootageFiles	Number of footage files in the storage pool.	
<b>serviceInfo</b>	infoServiceStatus	Status of <b>AI InfoService</b> service	
	netSendHistStatus	Status of <b>AI NetSendHist</b> service	
	schedulerStatus	Status of <b>AI Scheduler</b> service	
	trackerNumber	Number of tracker services	
	trackerID	The ID of the tracker	
	trackerStatus	Status of the <b>AI Tracker</b> service for the <b>trackerID</b>	
<b>loginMonitor</b>	authorizedLoginNotif	Notification sent when a login is successful	<b>Yes</b>
	unauthorizedLoginNotif	Notification sent when an unauthorized login is attempted	<b>Yes</b>
	loginNotifyIpAddress	IP address that the client is connected from	
	loginNotifyUsername	Username that the client is attempting to login with	
	loginNotificationMessage	Message with additional details about the login attempt	
<b>alarmMonitor</b>	alarmNotif	Notification sent when an alarm occurs or is marked	<b>Yes</b>
	alarmNotifyCameraId	Camera ID of the camera that recorded the alarm	
	alarmNotifyCameraName	Camera name of the camera that recorded the alarm	
	alarmNotifyUserId	User ID of the user that marked the alarm	
	alarmNotifyUserName	User name of the user that marked the alarm	
	alarmNotifyMarkedDelay	Time alarm was marked	
	alarmNotifyFalseAlarm	Is this a false alarm	
	alarmNotifyRuleId	Rule ID of the rule causing the alarm	

Table 7. Mib file details (Continued)

Category	Details	Description	Trap Yes/No
	alarmNotifyRuleName	Rule name of the rule causing the alarm	
	alarmNotifyDBId	ID of the alarm	
	alarmNotifyComment	Comments associated with the alarm	
	alarmNotifyMSSinceChange	Number of milliseconds between when the alarm occurred and when it was detected	



Symphony traps for unauthorized logins and all alarms when they occur or when the user marks them.

## Additional Tools and Information

If you prefer a command line tool instead of a GUI MIB Browser, you can use a free command line tool (Net-SNMP) to walk the mib files. (The **snmpwalk** command will perform a sequence of chained **GETNEXT** requests automatically.)

- For instructions, see Net-SNMP: <http://net-snmp.sourceforge.net/>

The following sites also provide information on SNMP:

- How SNMP Works: [http://technet.microsoft.com/en-us/library/cc783142\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc783142(WS.10).aspx)
- How to effectively use a MIB Browser: <http://www.unleashnetworks.com/resources/articles/88-how-to-effectively-use-a-mib-browser.html>

## Using the DOS killall Utility with Symphony Services

Symphony comes with a dos utility that can be used to automatically start, stop or restart the Symphony Services. This can be faster than individually managing the services from the Services console in Windows (accessed by running **Services.msc** from the **Start > Run** command).



**Note:** Using the **killall** utility will not restart the SQL Database.

<b>killall &lt;command&gt;</b> Where next <b>command</b> is one of:
<b>1</b> - Stop Services gracefully
<b>2</b> - Terminate services
<b>3</b> - Start services gracefully (restart web)
<b>4</b> - Terminate services only if necessary
<b>5</b> - Start services gracefully (leave web alone)
<b>6</b> - <b>&lt;pid&gt;</b> - Kill the specified pid
<b>7</b> - Restart web
<b>8</b> - Get CPU usage from shared memory
<b>9</b> - Same as 4 except will also kill infoservice
<b>r</b> - Restart services (killall 9, killall 5)
<b>s</b> - Restart services in sequence
<b>t &lt;tracker id&gt;</b> - Restart tracker <b>&lt;tracker id&gt;</b>

<b>Example 3</b>	
	<p>To restart all system services:</p> <p style="text-align: center;">From the command prompt, enter: <b>killall r</b></p> <p>Click ENTER on keyboard to run command</p>

## Receiving Full Diagnostic Information

Symphony server provides detailed logs and monitoring functionality.

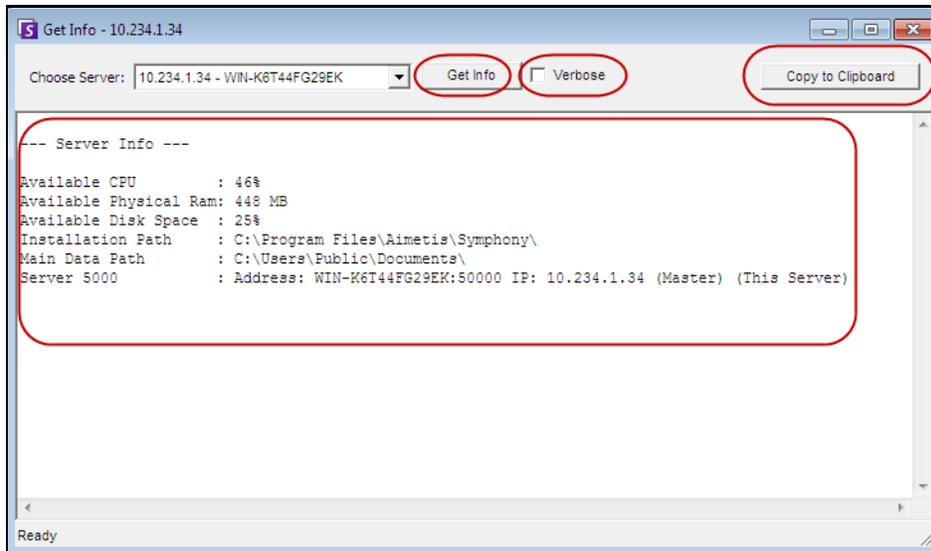


Figure 38. Get Info dialog box

## Procedure

### To receive full diagnostic information on your Symphony server:

1. From the **Server** menu, select **Get Info**. The **Get Info** dialog box opens. By default, CPU, RAM and DISK information is displayed.
2. (Optional) Select the **Verbose** check box and click **Get Info**. More information is displayed.
3. (Optional) Click **Copy to Clipboard**. The text is copied to the clipboard.

## Managing Symphony Services

Symphony server runs the following core Services. All Symphony Services are prefixed with an "AI".

**Table 8. Symphony Services**

Service	Description
<b>AI InfoService</b>	Web Server running Symphony's web service which receives all requests from the client.
<b>AI NetSendHist</b>	Responsible for historical video streaming and historical .JPEG creation.
<b>AI Scheduler</b>	Responsible for polling hardware alarm inputs, cleaning video, running reports and searches, synchronizes CPU and other processes on system.
<b>AI Tracker #</b>	The process that performs video analysis, saves video to disk, live video streaming. Each camera requires its own AI Tracker service.

### Troubleshooting Tips

- Symphony requires the **AI InfoService** to be running properly. Normally connectivity issues between the client and server are caused by a resource conflict between another process using Port 50000, or a firewall preventing Symphony and the **AI InfoService** from communicating properly.
- By default, Symphony installs a Microsoft SQL Server express database during the installation of Symphony Server. Make sure the SQL Server (Aimetis) service is started.

## Starting and Stopping Symphony Services

Symphony services can be stopped and started individually. Services can be individually restarted directly from Symphony Client or from Windows directly by using the Services Console.

If you do not have direct access to the Windows environment on the Symphony server, you can manage services remotely using Symphony Client.

### Procedure: Using Symphony Client

#### To manually stop and start individual services:

1. From the **Server** menu, select **Services** and then **Manage Symphony Services**. The **Manage Services** dialog box opens.
2. Select which server to configure from the drop-down field above the **Refresh** button.
3. Select the services you want start or stop by clicking on the service under the **Servername** column.
4. Click the **Toggle** button and then click the **Refresh** button to see if the state of the server changed. In State column, the service will indicate **Running** or **Stopped**.

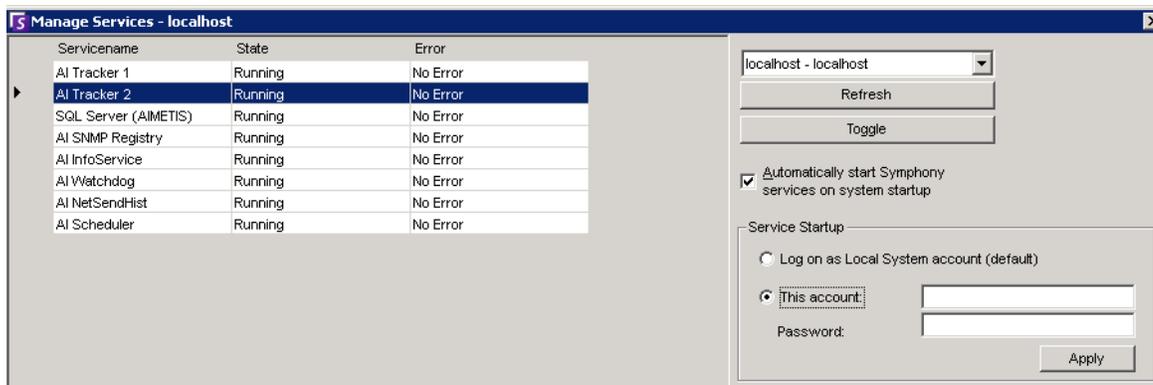


Figure 39. Manage Services dialog box

- By default, the Symphony Services start on startup of the operating system. If you do not want Symphony Services to automatically start on system startup, clear the **Automatically Start Symphony Services on system startup** check box.
- You can change the **Log on as Local System account** for ALL services in the **Service Startup** section.



**Caution:** Changing service states can adversely affect your Symphony installation.

## Procedure: Using Windows directly

---

### To restart the Symphony Services directly from Windows:

1. In your Windows operating system, select **Start** and then **Run**.
2. Enter **Services.msc** and click **OK**. The **Services** dialog box opens.
3. Load the Services Console. Right-click on the service you want to start, stop, or restart.

## Virus Scanning

We recommend that you disable virus scanning software on the Symphony server. Virus scans use a large amount of system resources to scan data. Virus scanning software, in some cases, locks each file it scans. Overall, it can affect performance negatively.

## Firewalling Symphony

Firewalling your server is a good way to reduce the chances of someone hacking in and damaging your system.

### Procedure

---

#### To firewall your system:

1. From Control Panel, double-click on the **Network Connections** icon.
2. Right-click on your internet connection and select **Properties**.
3. Select the **Advanced** tab.
4. Select the **Protect my computer** check box.
5. Click **Settings**.
6. Ensure that none of the check boxes in the **Services** tab are selected.
7. Add a new service entry for every TCP port you want to allow through
8. Click the **Add...** button and fill in the dialog box.
9. Enter the name of your computer in the **Name** field.
10. Leave the **Internal Port Number** field empty. By default, Symphony uses the following ports:

**Table 9. Default Ports**

Port number	Description	Configurable
50000	WS1	Yes
50001	WS2	Yes
50010	camera1 live	Yes
50012	camera1 historical	Yes
50020	camera2 live	Yes
50022	camera2 historical	Yes
50030	camera3 live	Yes

**Table 9. Default Ports (Continued)**

Port number	Description	Configurable
50032	camera3 historical	Yes
5045	health checks	No

The port list in [Table 9 on page 120](#) assumes you are publishing 3 cameras on the Symphony server PC behind the firewall. If you are publishing more cameras on the PC, continue opening ports similar to those in [Table 9](#).



**Important:** If you are using Video Wall functionality, open port 50005 on the client PC.

For a complete list of ports, see the Knowledge Base Article: [Ports used in Aimetis Symphony](#).

## Publishing Symphony on a Non-Standard Port

By default, Symphony servers will use port 50000 as the default web port. However, in some cases the default port may need to be changed. For example, if multiple servers are being published on the same external IP address, the default ports of the subsequent server(s) need to be changed. By changing the BasePort (web port), other ports will automatically change as well.

## Procedure

### To change the default ports:

1. In Symphony Client, from the **Server** menu, select **Manual Configuration Editor**.
2. Click **Add a new setting...** The fields under the column headings are activated.
3. Enter the following information:
  - **Type** = Server
  - **Section** = Main
  - **ID** = (enter your Server ID)
  - **Key** = BasePort
  - **Value** = (enter your new default web port)
4. Restart the Symphony services.

## HTTPS for AXIS

For instructions on setting up HTTPS for AXIS cameras, refer to the **How To Configure HTTPS for AXIS** document on the Xnet: <https://www.aimetis.com/Xnet/Downloads/documentation.aspx>

## Configuring your Mail Server on Windows 2008 Server R2

Configuring your mail server allows your Symphony server to send email notifications when events happen. Symphony may send emails as a result of Rule (Action) configuration or Subscriptions. Symphony will relay email via an email server defined in the Subscriptions page.

- [“Using Internal SMTP Server”](#)
- [“Using External SMTP Server” on page 123](#)
- [“Windows 7 and Vista - SMTP not included” on page 123](#)

### Using Internal SMTP Server

Allow Symphony server to relay email through itself using Microsoft SMTP server.

#### Task 1: Install IIS on the server

- Follow the instructions at <http://digitizor.com/2009/02/20/how-to-install-microsoft-iis-server-on-windows-7/>

#### Task 2: Add SMTP Server:

1. Start the **Server Manager MMC**.
2. In the **Features** section, click **Add Features**.
3. Select **SMTP Server**.

#### Task 3: Configure the mail server

1. From the Windows Control Panel, double-click on the **Administrative Tools** icon.
2. Double-click on the **Internet Information Services** icon.
  - If this is not installed:
    - a. Go to Control Panel, **Add/Remove Programs**, and select **Add/Remove Windows Components**.
    - b. Scroll to **Internet Information Services**, click **Details**, and add SMTP service.
3. Expand the tree. Right-click on **Default SMTP Virtual Server** and select **Start** if it is enabled.
4. Right-click on **Default SMTP Virtual Server** and select **Properties**.
5. Click the **Access** tab and then click **Connection**.
6. Select the **Only the list below** option and click **Add**.
7. Select the **Single computer** option and enter **127.0.0.1** as the IP address.
8. Click **OK** to close the **Computer** dialog box and click **OK** to close the **Connection** dialog box.
9. Click the **Relay...** button.
10. Select the **Only the list below** option and click **Add**.
11. Select the **Single computer** option and enter **127.0.0.1** as the IP address.
12. Click **OK** to close the **Computer** dialog box.
13. Clear the **Allow all computers that successfully authenticate to relay** check box.
14. Click **OK** to close the **Relay Restrictions** dialog box.

## Using External SMTP Server

If an external SMTP server is used for Symphony email relaying, specify this address in the Subscriptions SMTP field. Please note the connection to the SMTP service is not authenticated. Ensure that the SMTP server allows for unauthenticated connections from the Symphony server IP address.

### Windows 7 and Vista - SMTP not included

SMTP is not included in Vista or Windows 7. The IIS 6.0 Manager shipped with Windows 7 is not aimed for IIS 7.5 Management. To manage IIS 7.5/FTP 7.5 shipped with Windows 7, you must use IIS 7 Manager.

You have three options if you want SMTP support, so Symphony can email directly from the server:

- Use a server operating system and you then use the Microsoft supplied SMTP server.
- Use Windows 7 but use an external email gateway. For example, if the Symphony server is on the office LAN with a local email server, Symphony can relay through that server.
- Install a 3rd party SMTP server that works with Windows 7.

## Back up and Restore

If you are upgrading, we recommend that you back up the entire Symphony configuration after installation is complete, and that, in general, you schedule automatic backups. The configuration file contains all server settings (but no recorded video).

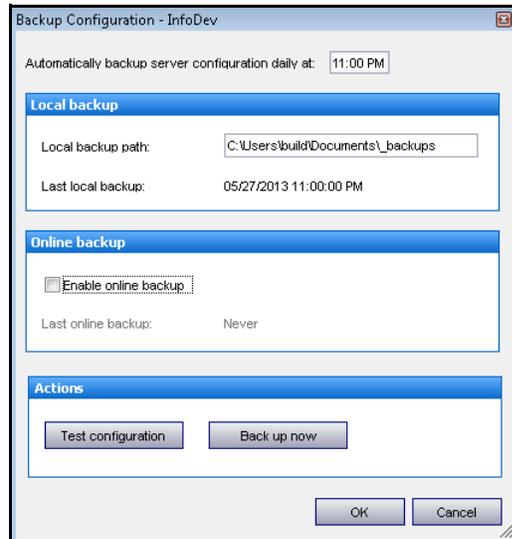


Figure 40. Backup Configuration dialog box

After a new installation, (if no previous Symphony server installation exists that contains the Symphony 6.12 backup/restore functionality) the **Local backup path** field will use the **Data Path** as configured in Symphony **Setup Wizard** (“Figure 41. Data Path in Symphony Setup Wizard”), with “\\_backups” appended .

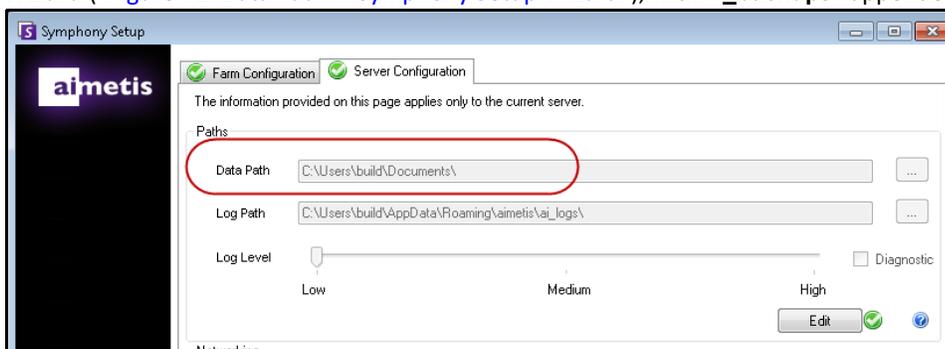


Figure 41. Data Path in Symphony Setup Wizard

If you are using a multi-farm system, follow these instructions first.

- [“Multi-farms only” on page 125](#)

Otherwise, follow the instructions in any of the back up and restore sections:

- [“Automatic Back up” on page 127](#)
- [“Local backup path” on page 127](#)
- [“Online back up” on page 130](#)
- [“Restore local backup” on page 131](#)
- [“Restore from file” on page 132](#)
- [“Restore online backup” on page 134](#)

## Multi-farms only

After a new installation, (if no previous Symphony server installation exists that contains the Symphony 6.12 backup/restore functionality) the **Local backup path** field will use the **Data Path** as configured in Symphony **Setup Wizard**, with “\\_backups” appended.

## Procedure

To ensure that data is backed up correctly in a multi-farm setup, do one of the following:

- “Option A: Customize the backup path during installation in the Setup Wizard”

**OR**

- “Option B: Customize the backup path after installation” on page 126

### Option A: Customize the backup path during installation in the Setup Wizard

1. Set up a writable, shared folder that all server members of the farm will use. The shared folder that is to be designated as backup repository for all servers may be hosted on a PC or other specialized form of network storage. For increased backup data reliability and availability (in case of disaster recovery), it is strongly recommended that the shared storage location is not hosted by any of the servers that are members of the farm,
2. Ensure that the **Data Path** in the **Setup Wizard** is set to be the same for all the member servers, and accessible to all.

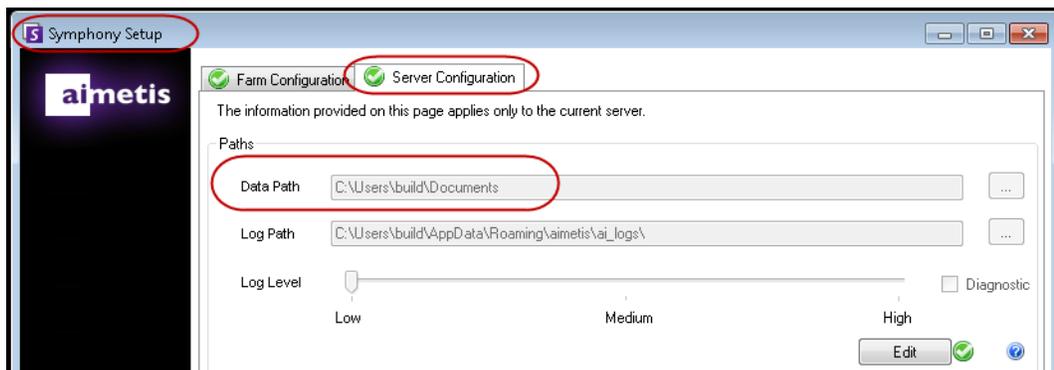


Figure 42. Setup Wizard showing Data Path

## Option B: Customize the backup path after installation

1. Set up a writable, shared folder that all server members of the farm will use. The shared folder that is to be designated as backup repository for all servers may be hosted on a PC or other specialized form of network storage. For increased backup data reliability and availability (in case of disaster recovery), it is strongly recommended that the shared storage location is not hosted by any of the servers that are members of the farm.
2. In the **Backup Configuration** dialog box, **Local backup path** field, enter the path for this shared folder that will be accessible to all servers in the farm.

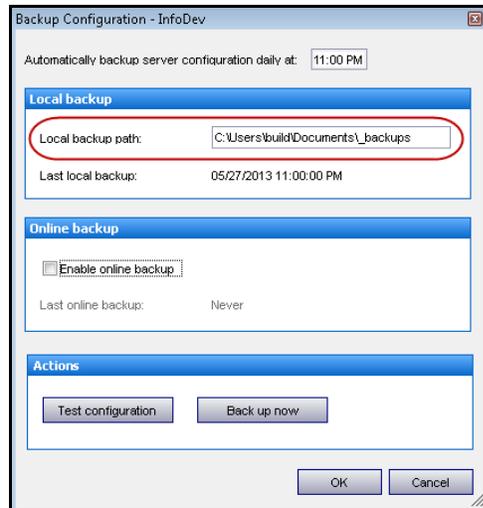


Figure 43. Backup Configuration dialog box

## Automatic Back up

By default, the server configuration is backed up daily at **11:00 PM** to the **Local backup path**. Automatic online back up is optional.

You can change the time by editing the **Automatically backup server configuration daily at:** time field.

## Local backup path

After a new installation, (if no previous Symphony server installation exists that contains the Symphony 6.12 backup/restore functionality) the **Local backup path** field will use the **Data Path** as configured in Symphony **Setup Wizard** (“[Figure 44. Data Path in Symphony Setup Wizard](#)”), with “\\_backups” appended.

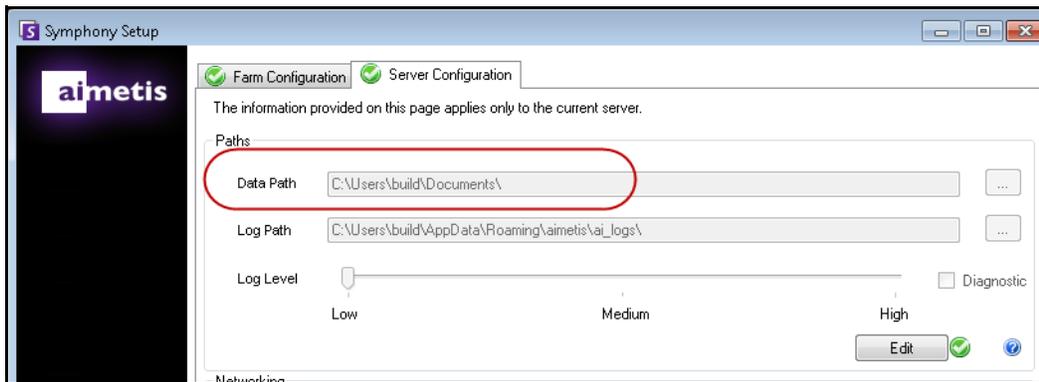


Figure 44. Data Path in Symphony Setup Wizard

## Procedure

### To back up to the local machine:

1. From the **Server** menu, select **Backup**. Symphony retrieves your backup settings from the server. The **Backup Configuration** dialog box opens.

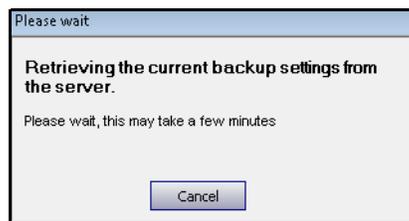


Figure 45. Symphony retrieving backup settings

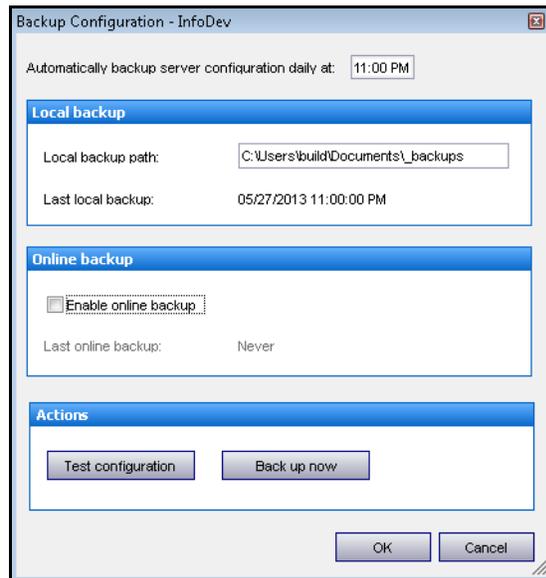


Figure 46. Backup Configuration

2. You can change the **Local backup path** only if:
  - You are sure that the Symphony server (the one currently elected as the master server) can create and access this path locally (or via network shares or via NAS, SAN, etc.).
  - In a **multi-server farm scenario** you accept that the path is a local file system path. The use of such a path is not recommended. Instead, a centralized/network path (accessible to all farm member servers) is recommended. See “[Multi-farms only](#)” on page 125.If you are unsure about the path, click **Test configuration**.
3. Click **Back up now**.

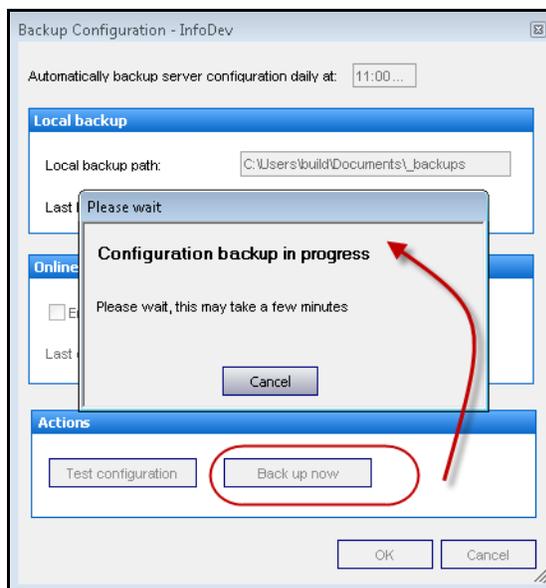
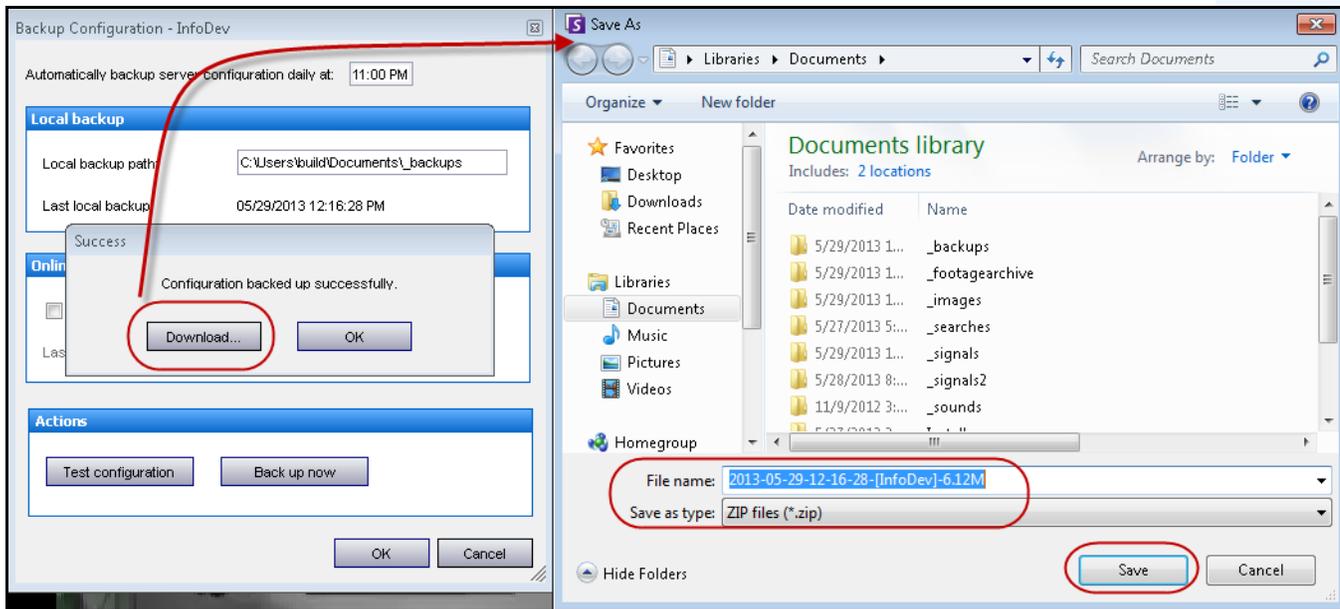


Figure 47. Clicking the Back up now button

4. After the configuration is backed up, you have the option of downloading the configuration in a **.zip** file. Click **Download** to save the file to a location on your machine or **OK** to simply close the **Success (Configuration backed up successfully)** dialog box.



**Figure 48. (Optional) Download the backup configuration**

5. Click **OK** when finished. The **Backup Configuration** dialog box closes.

## Online back up

The Symphony master server for a farm uploads the local backups to an online location.

## Procedure

### To back up to an online location:

1. From the **Server** menu, select **Backup**. Symphony retrieves your backup settings from the server. The **Backup Configuration** dialog box opens.

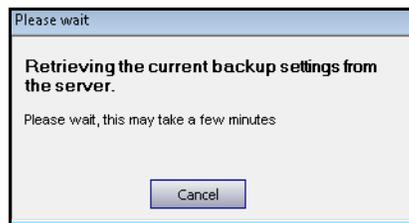


Figure 49. Symphony retrieving backup settings

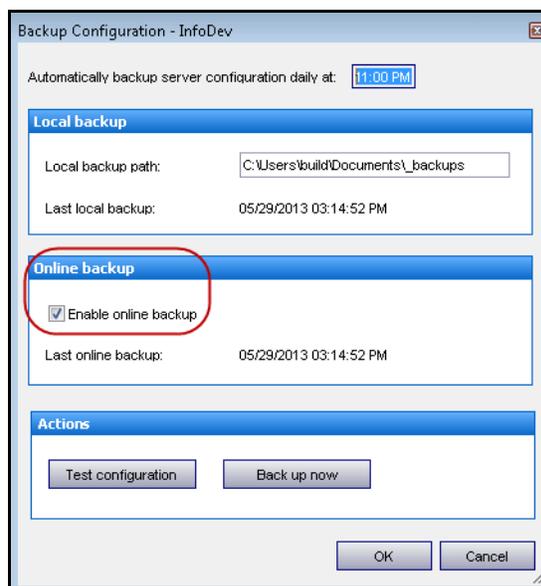


Figure 50. Backup Configuration dialog box with Online backup enabled

2. Select the **Enable online backup** check box. Click **Test configuration**. If successful, click **Back up now**.
3. After the configuration is backed up, you have the option of downloading the configuration in a **.zip** file. Click **Download** to save the file to a location on your machine or **OK** to simply close the **Success** (Configuration backed up successfully) dialog box.
4. Click **OK** when finished. The **Backup Configuration** dialog box closes.

## Restore Configuration

Symphony can restore the entire configuration to a previous state, including, for example, rule information, log files, alarm masks, and site maps in configuration files. Video data is **not** contained in the configuration backup.

### Restore local backup

You can restore server configuration settings from a **.zip** file that was saved locally. See [“Local backup path” on page 127](#).

### Procedure

#### To restore configuration from a local **.zip** file:

1. From the **Server** menu, select **Restore**. The **Restore Configuration** dialog box opens.
2. Select the **Restore local backup** option and select a backup file from the displayed list.

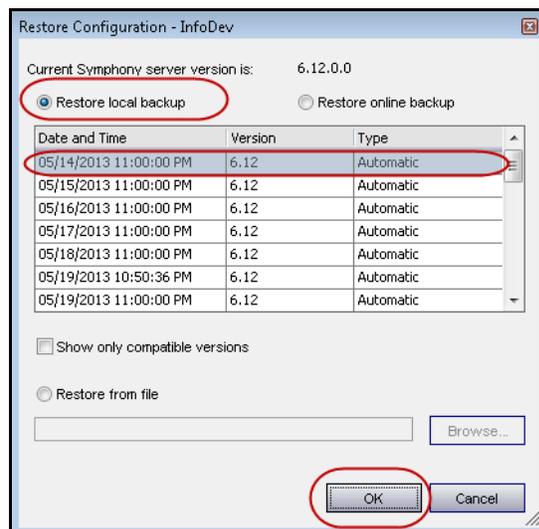
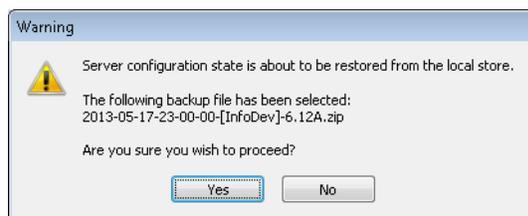


Figure 51. Restore Configuration dialog box - Restore local backup option

3. Click **OK**. Symphony asks you to confirm whether to proceed with the restore process, displaying the full name of the **.zip** file containing the server configuration.



4. If this is the correct **.zip** file, click **Yes**. Symphony starts the restore process. Click **OK** once it has successfully completed. The **Restore Configuration** dialog box closes.

## Restore from file

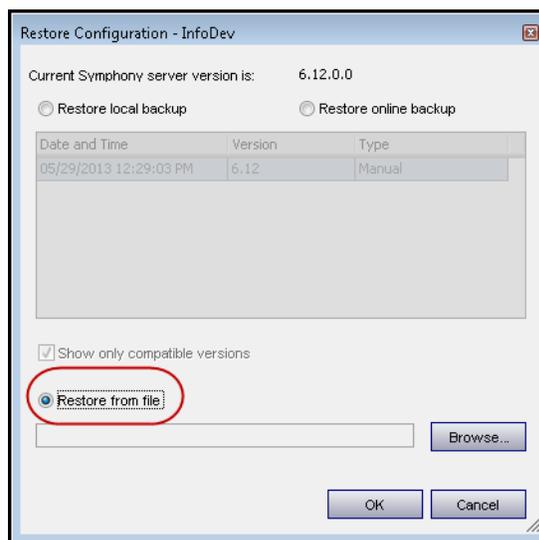
You can manually download a previously uploaded/created backup file (.zip) and use it manually to restore the configuration on a Symphony client PC that is not necessarily the same machine on which the backup policy has been configured (or a manual backup was requested). This is potentially useful for:

- Situations where you do not have internet access
- Data mining
- Centralized configuration for an enterprise-level of support

## Procedure

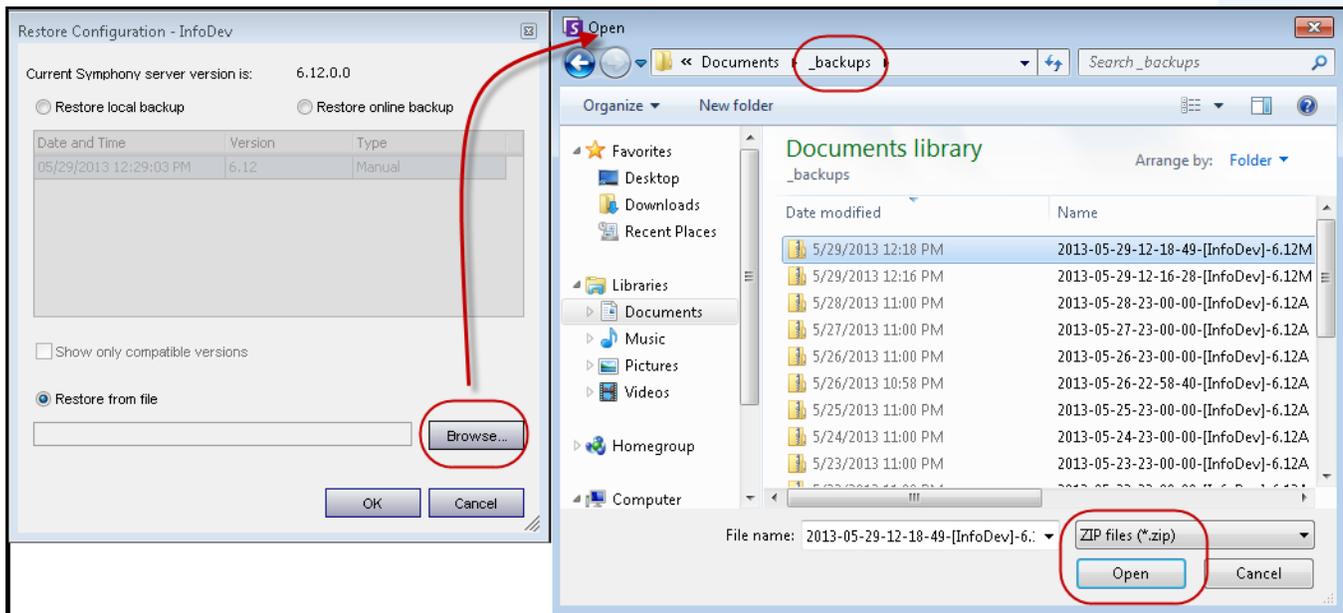
### To restore configuration from a .zip file:

1. From the **Server** menu, select **Restore**. The **Restore Configuration** dialog box opens.
2. Select the **Restore from file** option.



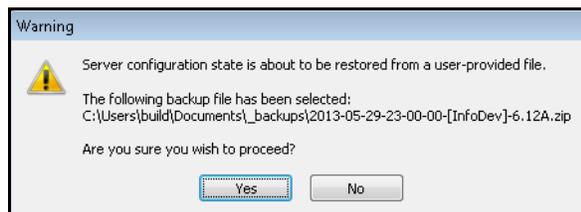
**Figure 52. Restore Configuration dialog box - Restore from file option**

3. Click **Browse** to locate the .zip file. Select and **Open** file with the correct date.



**Figure 53. Browse for .zip file containing backup configuration**

4. The file path and name will appear in the field next to the **Browse** button. Click **OK** to begin the restore process.
5. Symphony asks you to confirm whether to proceed with the restore process, displaying the full name of the **.zip** file containing the server configuration.



6. If this is the correct **.zip** file, click **Yes**. Symphony starts the restore process. Click **OK** once it has successfully completed. The **Restore Configuration** dialog box closes.

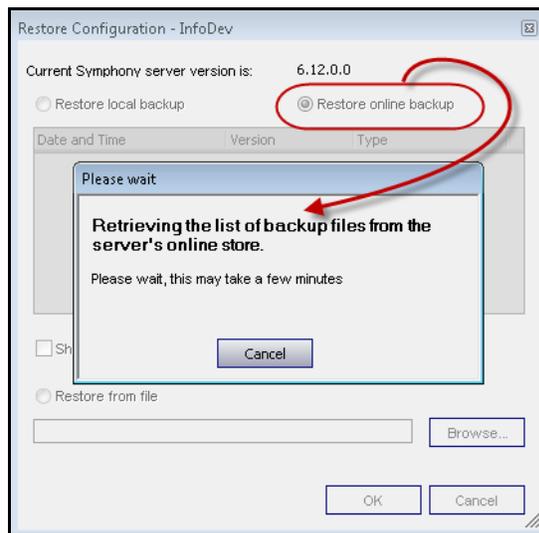
## Restore online backup

You can restore server configuration settings from a **.zip** file that was saved in online storage. See [“Online backup up” on page 130](#).

### Procedure

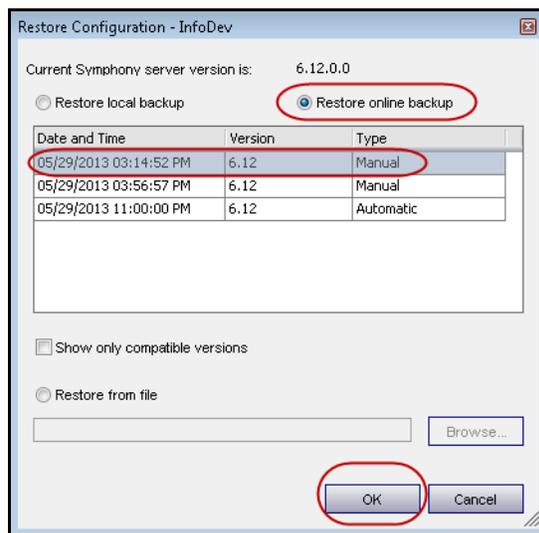
#### To restore configuration from a **.zip** file from online storage:

1. From the **Server** menu, select **Restore**. The **Restore Configuration** dialog box opens.
2. Select the **Restore online backup** option. Symphony retrieves the backup files from the online storage.

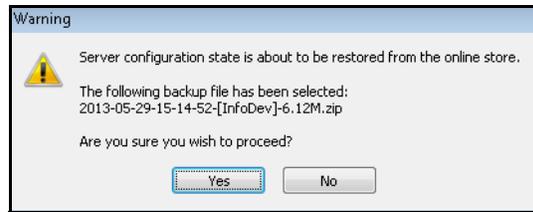


**Figure 54. Restore Configuration dialog box - Restore online backup option**

3. Once the list of backup files is displayed, select a backup file and click **OK**.



4. Symphony asks you to confirm whether to proceed with the restore process, displaying the full name of the **.zip** file containing the server configuration.



5. If this is the correct **.zip** file, click **Yes**. Symphony starts the restore process. Click **OK** once it has successfully completed. The **Restore Configuration** dialog box closes.

## Symphony Web Access

Aimetis Symphony also includes a web interface. Each server has its own web interface.

The web interface is designed to mimic the windows rich client (Symphony Client) as much as possible. All core features such as Alarm Log, Timeline, Reporting and live video streaming are included.

If the **Camera Tree** contains more than 100 devices, the Web Client shows video from cameras as separate pages, navigated by forward and back buttons.

### Procedure

---

#### To access the web interface:

1. Navigate to **http://SERVERNAME:50000** (where SERVERNAME can be your windows hostname or the IP address of the server).
2. Log in.
3. Select a camera from the camera tree to view video.

### Procedure

---

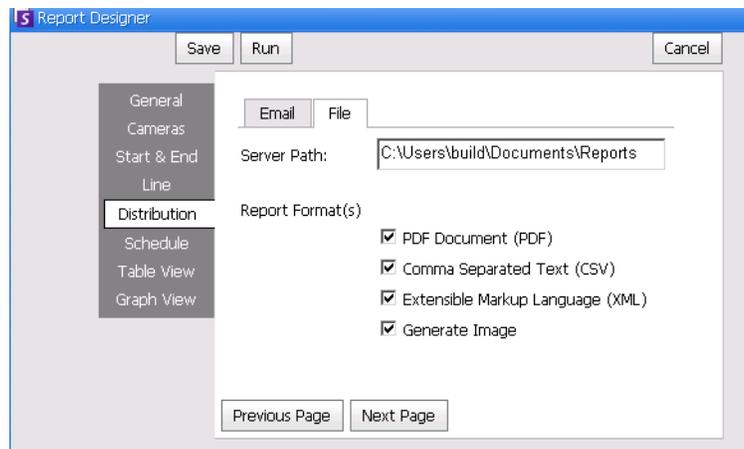
#### To access web based reporting:

- Click the **Reports** link. Visit Reports section for help on using reports.

## Reports

Depending on write-permissions, the generated report will be stored in the \Data\Reports folder on the master server machine. (This default folder is designated during the initial Symphony installation and setup or can be changed in the **Server Path** field.

If there are **multiple servers in a farm**, all the servers must have the same directory tree structure for the path being used to save reports. The path specified in [Figure 55](#), for example, must exist on all servers in the farm.

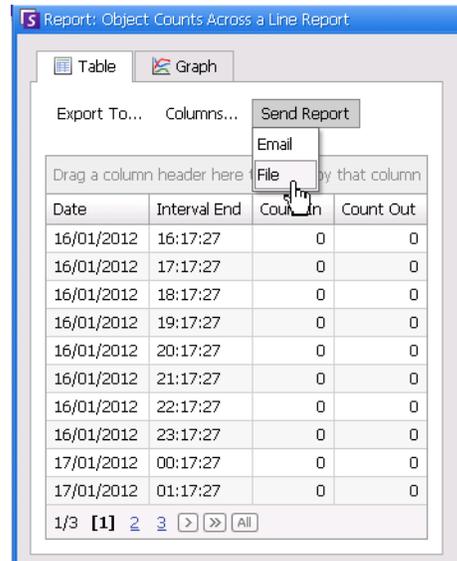


**Figure 55. Server Path field for saving a generated report**

**Recommended:** Set up a writable, shared folder on a machine and designate it as the reports repository using the **Server Path** field.

## File Distribution Permissions for Scheduled versus Manual Reports

When designating a folder on the system to save a generated report (**Send Report>File**), you must be aware of the following.



**Figure 56. Send Report > File saves a generated report**

- For scheduled reports, the files will be saved using the account (identity) of the user running the services (in particular InfoService). So that account must have permission to write to the default \Reports folder. If a user changes the default path (**Server Path** in **File** subtab of **Distribution** tab in **Reports Designer**), then the user must ensure that the Windows account the InfoService is running as can write to that new folder.
- For manual reports, the files will be saved using the account of the user logged in running the report. If restricted user does not have access to write to say c:\windows, and changes the default path (**Server Path** in **File** subtab of **Distribution** tab in **Reports Designer**), the report will NOT be saved.

---

Copyright © 2013 Aimetis Corp. All rights reserved.

This guide 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 Corp. , 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.

Portions Copyright © 1993-2013 ARH Inc.

Portions of this software are based in part on the work of the Independent JPEG Group.