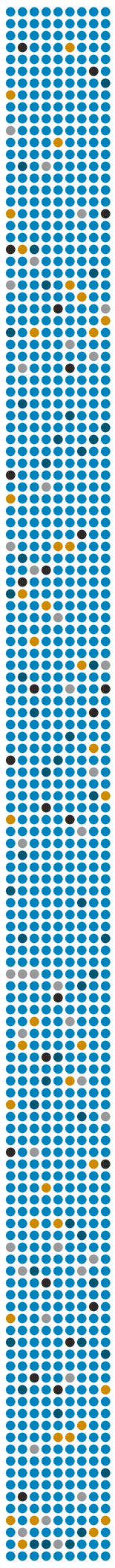




Senstar Symphony

Lenel OnGuard Integration Guide



Contents

Introduction.....	3
Lenel OnGuard.....	3
Integration.....	4
Authorize a Windows user account.....	4
Install Lenel OnGuard.....	4
Configure Windows Management Instrumentation.....	4
Allow Windows Management Instrumentation traffic through the firewall (OnGuard).....	4
Configure DCOM (OnGuard).....	4
Start the LS Linkage Server service.....	5
Configure the DataConduIT platform.....	5
Configure the Symphony services.....	5
Allow traffic through the firewall (Symphony).....	5
Configure DCOM (Symphony).....	5
Add an OnGuard device to Symphony.....	6
Add the Lenel Listener.....	6
Rules.....	6
Create a rule.....	7
Create an event.....	7
Create an action set.....	7
Create a schedule.....	8
Legal information.....	9

Introduction

Senstar Symphony is an award-winning, intelligent video surveillance software that offers a single, innovative, and open IP video platform for video management, video analytics, system integration, and alarm management.

Symphony installs on standard IT hardware, supports both analog and IP cameras from hundreds of manufacturers, provides a feature-rich, easy-to-use interface, and incorporates IT friendly features to make administration simple. The Symphony Server can reside on a single computer or multiple computers in a server farm.

Symphony comprises two main components: the Symphony Server and the Symphony Client. You can use the server configuration interface to configure the Symphony Server and the client interface to interact with the cameras connected to Symphony.

Symphony also includes the Symphony Web Client and the Symphony Player. The Web Client provides functionality similar to the Client, but in a Web browser and without requiring installed software. The Player allows you to play video files that you export from Symphony.

Lenel OnGuard

Lenel OnGuard[®] is a security management solution that offers access control and alarm monitoring for multiple sites.

Integration

You can integrate Lenel OnGuard with Symphony to allow Symphony to use events from OnGuard to trigger alarms.

To integrate OnGuard, complete the following workflow:

1. On the computer that hosts the Lenel OnGuard, perform the following tasks:
 - a. Authorize a Windows user account.
 - b. Install Lenel OnGuard.
 - c. Configure Windows Management Instrumentation.
 - d. Allow Windows Management Instrumentation traffic through the firewall.
 - e. Configure DCOM.
 - f. Start the LS Linkage Server service.
 - g. Configure the DataConduIT platform.
2. On the computer that hosts the Symphony Server, perform the following tasks:
 - a. Add the Lenel Listener service.
 - b. Configure the OnGuard connection.
 - c. Add OnGuard devices to Symphony.
 - d. Create an alarm in the Symphony server configuration interface.

Authorize a Windows user account

1. On the computer that will host the OnGuard server, create a Windows user account or select a Windows user account from Active Directory.
2. Grant the Windows user account administrator permissions.

Install Lenel OnGuard

Install the Lenel OnGuard software. For instructions, see the Lenel OnGuard Installation Guide at www.lenel.com or on the installation media.

Configure Windows Management Instrumentation

On the computer that will host the OnGuard server, grant permissions for all actions to the authenticated Windows user account for both the CIMV2 and OnGuard namespaces. For more information, see the [Authorize WMI users and set permissions](#) page at [Microsoft TechNet](#).

Allow Windows Management Instrumentation traffic through the firewall (OnGuard)

On the computer that hosts the OnGuard server, allow Windows Management Instrumentation traffic through the firewall. For more information, see the [Setting up a Remote WMI Connection](#) page on the [Microsoft Developer Network](#).

1. On the computer that hosts the OnGuard server, run the command prompt as an administrator.
2. Type `netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes` and press **Enter**.

Configure DCOM (OnGuard)

1. On the computer that hosts the OnGuard server, click **Start > Run**.
2. Type `DCOMCNFG` and click **OK**.

3. In the Component Services box, click **Component Services > Computers > .**
4. Right-click **My Computer** and click **Properties**.
5. Click the **COM Security** tab.
6. In the **Launch and Activation** permissions, click **Edit Limits**.
7. If the ANONYMOUS LOGON user account is not in the list, perform the following tasks:
 - a) Click **Add**.
 - b) Type ANONYMOUS LOGON and click **Check Names**.
 - c) Click **OK**.
8. For both the ANONYMOUS LOGON and authenticated Windows user accounts, perform the following tasks:
 - a) Click the user account.
 - b) In the **Permissions for Distributed COM Users** pane, allow all of the permissions.
9. Click **OK**.

Start the LS Linkage Server service

1. On the **Administration > System Options** page, configure the Linkage Server Host to be the local machine.
2. In the System Management Console, perform the following tasks:
 - a) Start the LS Linkage Server service.
 - b) Start the LS Communication Server service.
 - c) Set the LS Application Server service to log on as the authorized Windows user account and start the service.

Configure the DataConduIT platform

For more information, see the [DataConduIT User Guide](http://www.lenel.com) at <http://www.lenel.com>.

1. Link the directory that contains the authorized user account to OnGuard.
2. Create an OnGuard user account with System Admin permission and link it to the authorized user account.
3. Configure the OnGuard user for single sign-on.

Configure the Symphony services

1. Set all of the Symphony services to log on as the authenticated Windows user account.
2. Restart the Symphony services.

Allow traffic through the firewall (Symphony)

On the computer that hosts the Symphony Server, allow Windows Management Instrumentation traffic through the firewall. For more information, see the [Setting up a Remote WMI Connection](#) page on the [Microsoft Developer Network](#).

1. On the computer that hosts the Symphony Server, run the command prompt as an administrator.
2. Type `netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes` and press **Enter**.

Configure DCOM (Symphony)

1. On the computer that hosts the Symphony Server, click **Start > Run**.
2. Type `DCOMCNFG` and click **OK**.


3. In the Component Services box, click **Component Services > Computers**.
4. Right-click **My Computer** and click **Properties**.
5. Click the **COM Security** tab.
6. In the **Launch and Activation Permissions** pane, click **Edit Limits**.
7. If the ANONYMOUS LOGON user account is not in the list, perform the following tasks:
 - a) Click **Add**.
 - b) Type ANONYMOUS LOGON and click **Check Names**.
 - c) Click **OK**.
8. For both the ANONYMOUS LOGON and Distributed COM User accounts, perform the following tasks:
 - a) Click the user account.
 - b) In the **Permissions** pane, allow all of the permissions.
 - c) Click **OK**.
9. In the **Access Permissions** pane, click **Edit Limits**.
10. For both the ANONYMOUS LOGON and Distributed COM User accounts, perform the following tasks:
 - a) Click the user account.
 - b) In the **Permissions** pane, allow all of the permissions.
 - c) Click **OK**.
11. Click **OK**.

Add an OnGuard device to Symphony

1. In the Symphony server configuration interface, click **Devices**.
2. Click **Access Devices**.
3. In the **Manufacturer** field, select `Lenel`.
4. In the **Database** field, type IP address of the computer that hosts the OnGuard server and database.
5. In the **Server** field, select the computer that hosts the Symphony Server to which to add the OnGuard device.
6. In the **Username** field, type the username for the authenticated Windows user account.
7. In the **Password** field, type the password for the authenticated Windows user account.
8. In the **Sources** list, select the input sources from the OnGuard device for Symphony to monitor.
9. Click **Save**.

Add the Lenel Listener

1. On the computer that hosts the Symphony Server, run the command prompt as an administrator.
2. Type `sc create "AI Lenel Listener" binPath= "C:\Program Files (x86)\Aimetis\Symphony Server v7_bin\LenelListener.exe"` and press **Enter**.

 **Important:** Type the text (including spaces) exactly as it appears above.
3. Start the service.

Rules

Symphony can generate alarms from rules. Rules include events, action sets, and schedules.

You create rules in the server configuration interface. When you create a rule, you either associate existing events, action sets, and a schedule with the rule, or you create new events, action sets, and a schedule for the rule.

An event triggers a rule. Examples include events from video analytics, camera inputs, and access devices.

An action set defines the actions that Symphony takes when an event triggers a rule. Examples include displaying or recording footage from a camera, sending an email, and switching a relay.

A schedule defines when a rule is active. An event must occur during an active time in the schedule to trigger a rule.

When a rule is enabled, the occurrence of an event associated with the rule during an active period in the rule's schedule causes Symphony to perform the actions defined in the rule's action set.

Create a rule

You can create a rule to trigger actions in Symphony.

1. In the Symphony server configuration interface, click **Rules > Rules**.
2. Click **Add**.
3. Type a name for the rule.
4. Enable or disable the rule.
5. Add an existing event to the rule or create a new event to add to the rule.
6. If you add multiple events to the rule, select how the events must occur to trigger the rule.
 - Select **in sequence** to trigger a rule when the events occur in the order in which the server configuration interface lists the events.
 - Select **within a time period of** and specify the number of seconds to trigger an rule when all of the events occur in the specified time period.
7. Add an existing action set to the rule or create a new action set to add to the rule.
8. Add an existing schedule to the rule or create a new schedule to add to the rule.
9. Click **Save**.

Create an event

You can create an event that triggers the Face Recognition rule.

1. In the Symphony server configuration interface, click **Rules > Events**.
2. Click **New Event**.
3. Type a name for the event.
4. To add a device, perform the following tasks:
 - a) Click **Add Devices**.
 - b) Select the device.
 - c) Click **OK**.
5. Perform one of the follow tasks:
 - If you add a camera, select the video engine and configure how it triggers a rule.
 - If you add a metadata device, select the input and configure how it triggers a rule.
 - If you add an access control device, select the readers and inputs, and configure how they trigger a rule.
6. Click **Save**.

Create an action set

You can create an action set to determine what actions Symphony takes when rule is triggered.

1. In the Symphony server configuration interface, click **Rules > Action Sets**.
2. Click **New Action Set**.

3. Type a name for the action set.
4. In the **Alarm** list, select the cameras to view when an alarm occurs.
5. In the **Choose a Camera** list, select the device that displays the alarm in its timeline.
6. To select where the alarm appears, perform one of the following tasks:
 - To associate the alarm with a camera and display the alarm in a camera timeline, select the camera in the **Choose a Camera** list.
 - To associate the alarm with a map and display the alarm on the map, select the map in the **Choose a Map** list.
7. In the **Record** list, select the cameras that record footage when an alarm occurs.
8. To add other actions, perform the following tasks:
 - a) In the **Pick an item** list, select an action.
 - b) Click **Add**.
 - c) Configure the settings for the action.
9. Click **Save**.

Create a schedule

You can create a schedule to determine when a rule is active.

1. In the server configuration interface, click **Rules > Schedules**.
2. Click **Add Schedule**.
3. Type a name for the schedule.
4. Define the active and inactive times for the schedule.
5. If required, add exceptions to the schedule.
 - a) Select a date.
 - b) Select whether to repeat the exception every year on that date.
 - c) Click **Add Exception**.
 - d) Define the active and inactive times for the exception.
6. Click **Save**.

Legal information

Copyright © 2019 Senstar Corporation and/or its Licensor(s). All rights reserved.

This material is for informational purposes only. Senstar 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 Senstar Corporation

Senstar 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 Senstar, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

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

All other trademarks are the property of their respective owners.