

Lenel OnGuard 8.3/8.4 - Senstar Symphony Integration Guide

Version 8.12

Table of Contents

Overview 3

 Requirements 3

Integration 4

 Authorize a Windows User Account 4

 Compatibility Matrix 4

 Configure the DataConduIT Platform 4

 Configure the Symphony Services 4

 Allow Traffic Through the Firewall (Symphony) 4

 Configure DCOM (Symphony) 5

 Add an OnGuard Access Control to Senstar Symphony 5

 Troubleshooting 6

 Rules 7

Legal information 8

Overview

OnGuard® Access Control is a security management solution that offers access control and alarm monitoring for multiple sites.

This guide describes how to integrate OnGuard 8.3/8.4 Access Control with Senstar Symphony™ Server so that Symphony receives hardware events from OnGuard for alarm generation and device or panel status updates. It covers the requirements for both systems, the Windows, DataConduIT, firewall, and DCOM configuration required on the Symphony host, the steps to add an OnGuard Access Control device in Symphony, and troubleshooting guidance for common issues.

Requirements

Requirement	Description
Senstar Symphony™	Senstar Symphony 8.12 or higher with minimum requirement
OnGuard®	OnGuard 8.3/8.4

Integration

In an OnGuard® 8.3/8.4 Symphony integration, Senstar Symphony™ receives and processes hardware events (hardwareevent) from OnGuard for alarm generation and for device or panel status updates.

The certified integration is fully event-driven. Symphony does not rely on periodic polling for status information; instead, all status and alarm changes are driven by the hardware event stream received from OnGuard.

To integrate OnGuard 8.3/8.4 Access Control, complete the following workflows.



Ensure that the required OnGuard integration permit is enabled and that Symphony is licensed to connect to OnGuard 8.3 before beginning configuration.

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.

Compatibility Matrix

Senstar Symphony™ version	OnGuard® version	Note
8.12	OnGuard 8.3.x	Tested version: OnGuard 8.3.670.0

Configure the DataConduIT Platform

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

1. Link the directory that contains the authorized Windows user account to the OnGuard® system.
2. Create an OnGuard user account with System Admin permission and link it to the authorized user account.
3. Configure Single Sign-On for the OnGuard user.

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 window, 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 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:
 - a. Select the user account.
 - b. Enable **all** permissions in the Permissions pane.
 - c. Click OK.
9. In the Access Permissions pane, click Edit Limits and repeat the previous step.
10. Click OK to close all dialog boxes.

Add an OnGuard Access Control to Senstar Symphony

1. In the Symphony Server interface, click Devices.
2. Click Integrations.
3. Click Add Hardware.
4. In the Device Type drop-down list, select OnGuard Access Control.
5. On the General tab, type the following:
 - a. Name: a descriptive name (for example, OnGuard Site A).
 - b. IP Address: the IP of the computer that hosts the OnGuard® server.
 - c. Port: `8080` (default for OpenAccess).
 - d. Username and Password: the credentials of the authenticated Windows user account (SSO-enabled).

- e. Alarm Logical Sources ID: Add Alarm Logical Sources with comma delimited sources such as "Symphony".
6. Click Connect to Device to verify connectivity.
7. On the Groups tab, select the group in which the device should appear in the Device Tree.
8. Click Save.

Troubleshooting

This section lists common issues and provides resolution information.

Panel-Status Cache Interval

OnGuard® refreshes the panel-status cache every 60 seconds by default. To shorten the status-update delay in Symphony:

1. Create or edit C:\ProgramData\Ln1\openaccess.ini.
2. Add the lines:

```
[cache]
panel_status_refresh_interval=5
```

Restart the LS Linkage Server, LS Message Broker, and OpenAccess services (or reboot the OnGuard server) to apply the change.

Service Status

Verify these services are running on the OnGuard server: License Server, LS Linkage Server, LS Message Broker, and OpenAccess.

Log Files

Check C:\ProgramData\Ln1\logs\Ln1Error.log and rabbit.log for errors.

RabbitMQ User Missing

If the LenelRabbitLD user is missing, follow the steps in OnGuard KB article "RabbitMQ and NGINX uninstall / installation".

Run Setup Assistant

After installing or upgrading OnGuard, run the Setup Assistant and complete every step. The wizard validates database connectivity, Windows services, and security settings. Rerun it after Windows Updates or Lenel patches.

Authentication Failures

Connection failures related to authentication (incorrect or expired password, invalid license, invalid authentication token) will not automatically be retried. In these cases, the Authentication Status node will show as Unauthenticated, and a manual Reauthenticate command from the same node is required to attempt reconnection.

Rules

Senstar Symphony™ can generate alarms using rules. A rule consists of events, action sets, and schedules. For detailed instructions, see the Senstar Symphony 8 User Guide.

Legal information

Copyright © 2026 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.

Senstar and the Senstar logo are registered trademarks of Senstar Corporation.

All other trademarks are the property of their respective owners.