

Aimetis Symphony™

Cardax Integration Guide

October 20, 2011



Document History

Sym-6.5-D-501

Table 1. Changes to this manual

Date	Description
October 20, 2011	Added: Table 1, "Supported Versions," on page 1
August 2011	Changed cover page to Cardax Integration Guide Added: <ul style="list-style-type: none"> • "Figure 3. Rules Wizard - Events" on page 5 • "Figure 4. All Cardax events filtered by the rule appear in the Timeline of the selected tracker and in the Alarm Log" on page 6 • "Figure 5. Alarm details will include cardholder images saved in Cardax database" on page 7 • "Figure 6. Cardax device is door icon on map" on page 8
January 27, 2011	First version of this document.

Table of Contents

Overview 1

Work Flow 2

Install Cardax Server software on a computer..... 3

Create a read-only Cardax database server 3

Install required packages in Symphony Server 3

Configure DCOM Access Permissions in Symphony Master Server 3

Create CardaxListener Windows Service in Symphony Server 4

Add device in Symphony 4

For Windows XP Users 9

Configuring Cardax Integration

Overview

Supported in Aimetis Symphony Release 6.5.6.29182 and above.

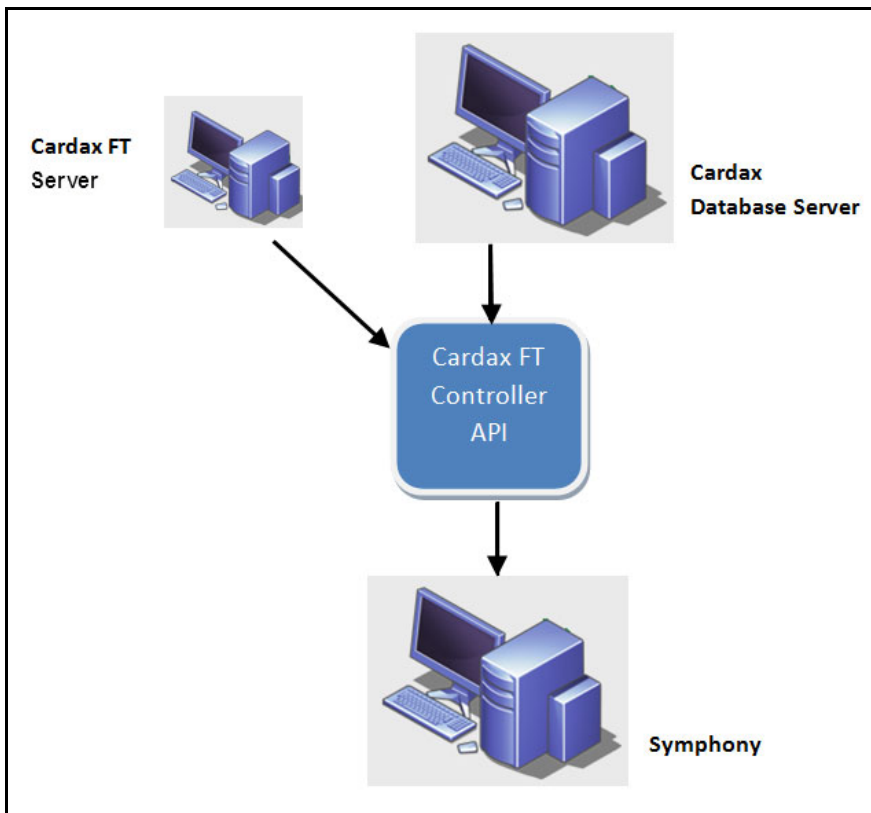


Figure 1. Servers

Table 1. Supported Versions

Symphony Product Version	Cardax Version
6.5.6.29182	vEL6.10.593
6.6	vEL6.10.593
6.7	vEL6.10.593

Work Flow

- [“Task 1: Install Cardax Server software on a computer” on page 3](#)
- [“Task 2: Create a read-only Cardax database server” on page 3](#)
- [“Task 3: Install required packages in Symphony Server” on page 3](#)
- [“Task 4: Configure DCOM Access Permissions in Symphony Master Server” on page 3](#)
- [“Task 5: Create CardaxListener Windows Service in Symphony Server” on page 4](#)
- [“Task 6: Add device in Symphony” on page 4](#)
- [“For Windows XP Users” on page 9](#)

Procedure

Task 1: Install Cardax Server software on a computer

Task 2: Create a read-only Cardax database server

This database can be installed on the same computer running the Cardax Server software.

1. Contact Cardax Technical Support. Request the **ReadOnlyDatabaseUserCreator** utility for your licensed Cardax installation.
2. Create one read-only database user with the **ReadOnlyDatabaseUserCreator** utility from Cardax.
3. In the Cardax server, run **svrnetcn.exe**.
4. Add **TCP/IP** to enable remote access to the database.
5. Create one Cardax operator (cardholder) with logon name "opc" and password "" (blank). Ensure that the operator group to which this operator belongs has the privileges **View Events and Alarms** and **View Site**.

Task 3: Install required packages in Symphony Server

1. Install the following components:
 - OPC Core Components 3.00 Redistributable (x86) from <http://opcfoundation.org>
 - Cardax OPC Bridge Configuration Version 6 from Cardax.

Task 4: Configure DCOM Access Permissions in Symphony Master Server

Note: To determine which is the Symphony Master Server.



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

1. In Windows, launch **Component Services**.
2. Expand the folders **Component Services>Computers>My Computer**.
3. Right-click **My Computer** and select **Properties**. The **My Computer Properties** dialog box opens.
4. Select the **COM Security** tab. In the **Access Permissions** section, click **Edit Limits**. The **Access Permission** dialog box opens.
 - Select the **Allow Local Access** and **Allow Remote Access** check boxes for **ANONYMOUS LOGON**, and click **OK**.
5. Click **OK** to close **Component Services**.

Task 5: Create CardaxListener Windows Service in Symphony Server

- From Windows command prompt, enter the following:


```
sc create "AI CardaxListener" binPath = "c:\program
files\aimetis\symphony\_bin\CardaxListener.exe 30" // 30 seconds
or
sc create "AI CardaxListener" binPath = "c:\program
files\aimetis\symphony\_bin\CardaxListener.exe" // default 1 minute
where service name must be AI CardaxListener exactly.
```
- Restart Server Services. (This will run the CardaxListener service.)

Task 6: Add device in Symphony

- From the **Server** menu, select **Add Access Device**. The **Add Access Device** dialog box opens.

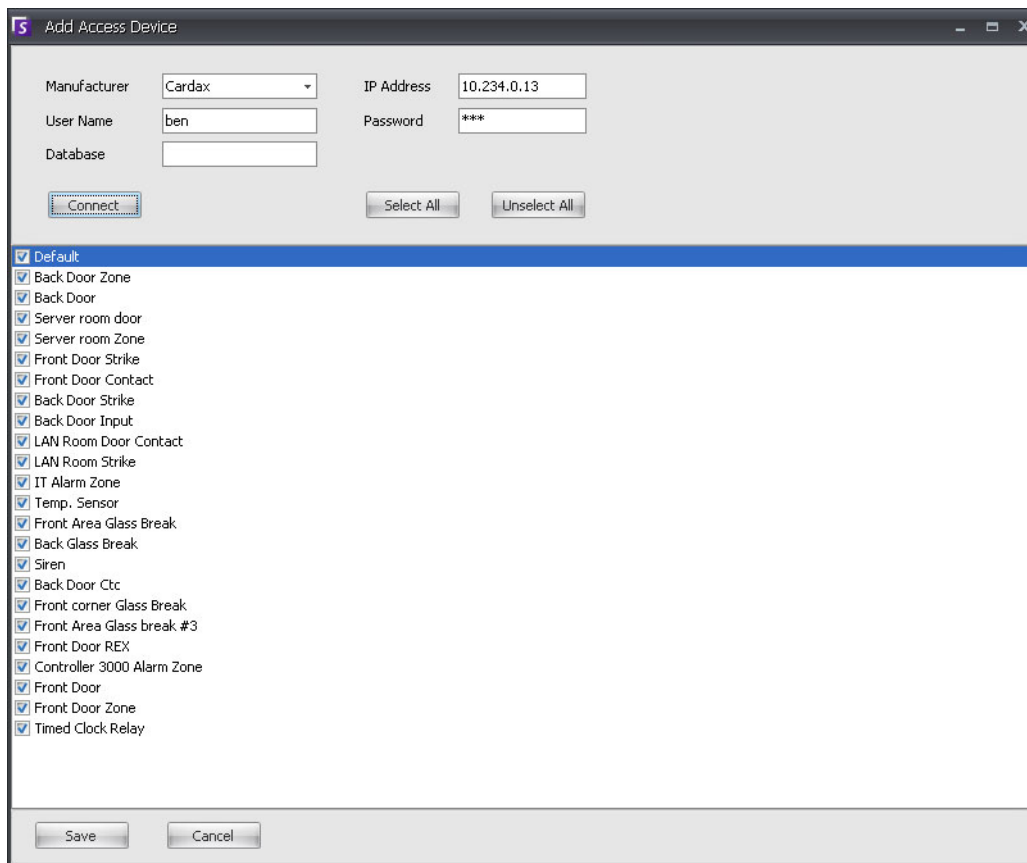


Figure 2. Add Access Device dialog box in Symphony

- From the **Manufacturer** field, select **Cardax**.
- In the **IP** field, enter an IP address of the Cardax server.
- Enter a **Username** and **Password** you created using the database utility in [“Task 2: Create a read-only Cardax database server” on page 3.](#)

5. If the Cardax database is not the default on the server, enter the database name in the **Database** field.
6. Click **Connect** . Select the devices and click **Save**.
7. Create a new rule by selecting desired devices corresponding triggers and the tracker you want to forward the Cardax events.

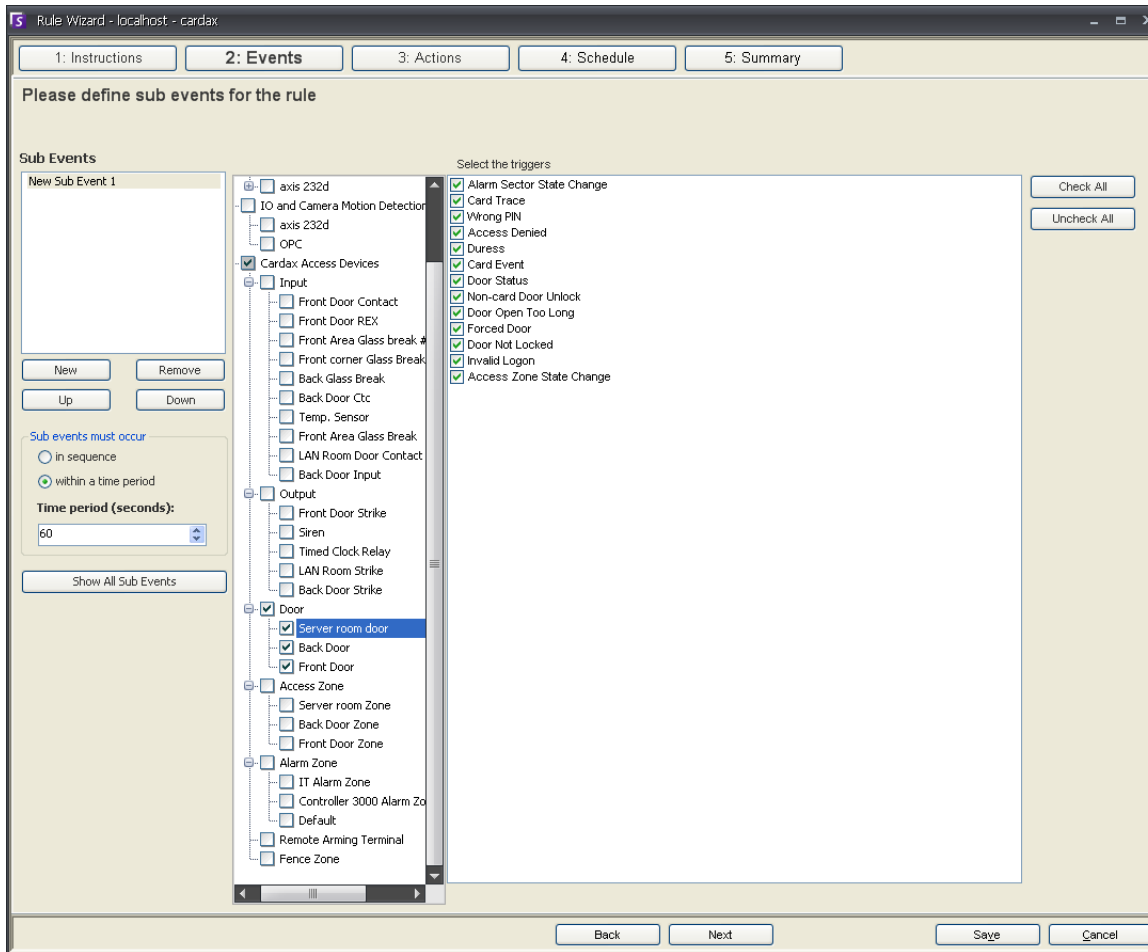


Figure 3. Rules Wizard - Events

8. For instructions in using the **Rule Wizard**, see *Symphony 6.5 Administration and Analytics Guide* <https://www.aimetis.com/Xnet/downloads/documentation.aspx>.

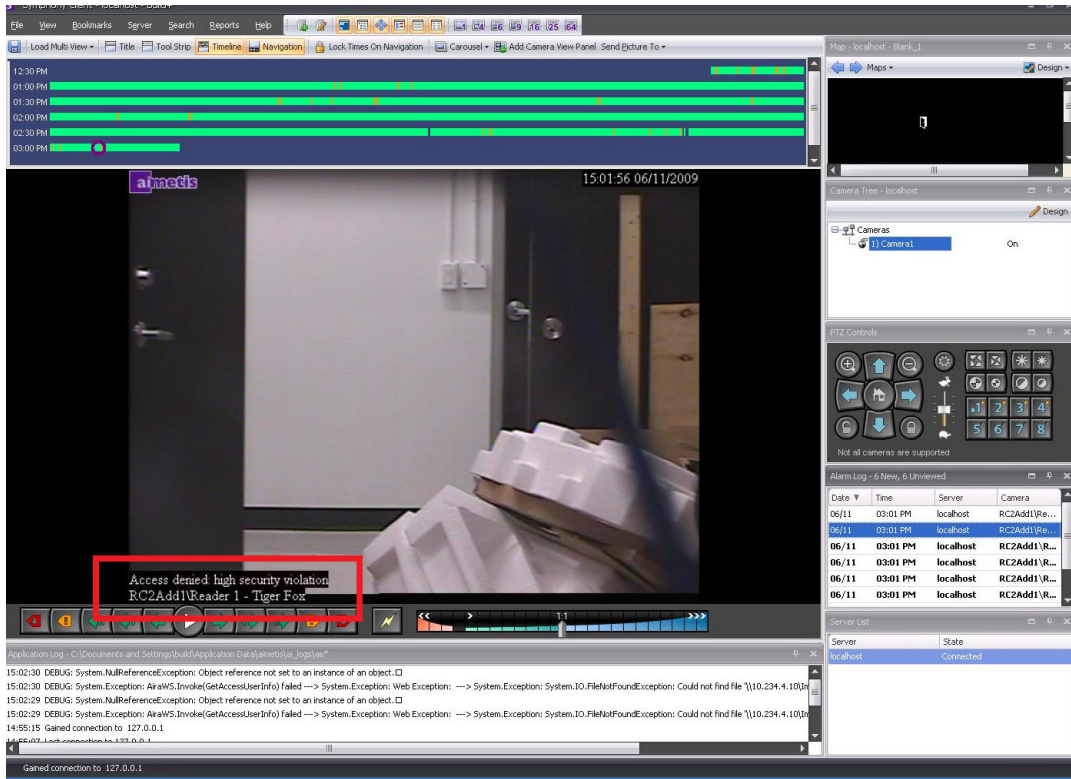


Figure 4. All Cardax events filtered by the rule appear in the Timeline of the selected tracker and in the Alarm Log

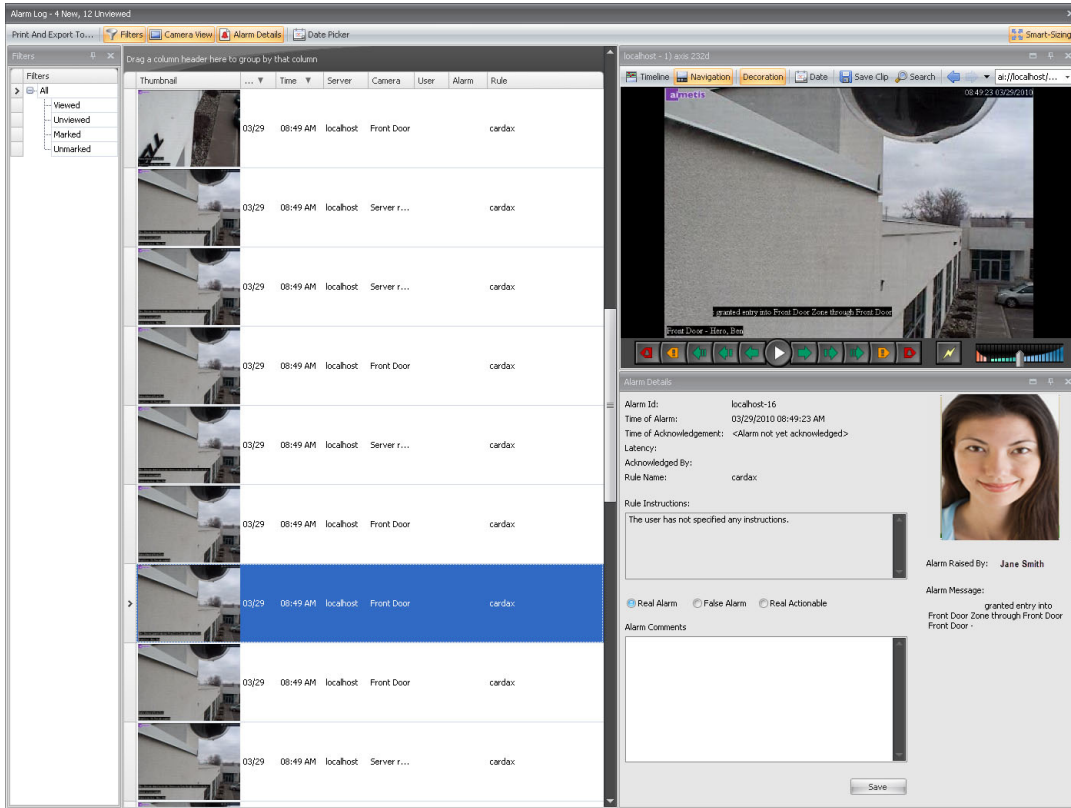


Figure 5. Alarm details will include cardholder images saved in Cardax database

9. Place the cameras on the **Map**.

- Alarms and events from Remote Arming Terminal and Elevators are not supported.
- All Cardax devices are shown as a door icon on the map.

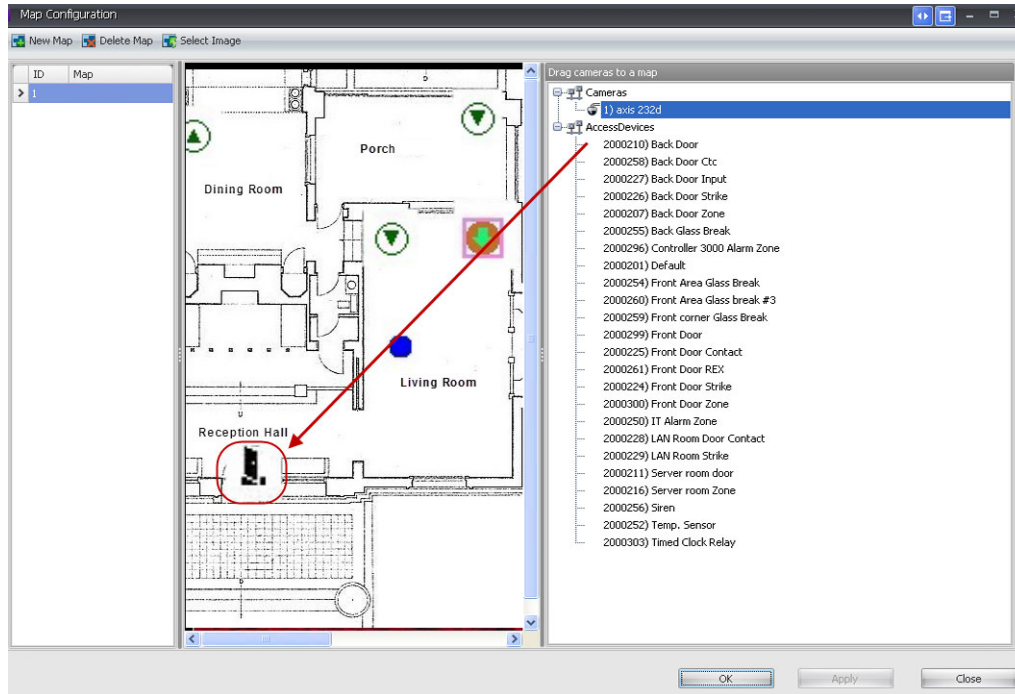


Figure 6. Cardax device is door icon on map

10. For instructions, see *Configuring a Map* in *Symphony 6.5 Administration and Analytics Guide*
<https://www.aimetis.com/Xnet/downloads/documentation.aspx>



Important: In any installation of Symphony, you are allowed only one type of Access Control. If you are using RBH, you cannot use Cardax at the same time.

For Windows XP Users

You must set up security policies.

Procedure

To set up security policies in Windows XP:

1. From the Windows **Control Panel**, click **Administrative Tools** and then **Local Security Policy**. The **Local Security Policy** dialog box opens.
2. Expand the **Local Policies** folder and click on **Security Options**.
 - In **Network Access: Sharing any security model for local account**, ensure that the security setting is set to **Classic – local users authenticate as themselves**.
 - In **System Objects: Default owner for objects created by members of the administrator group**, ensure that the security setting is set to **Administrators Group**.

Copyright © 2011 Aimetis Inc. 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, 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.