

RS2 Milestone Access Control Plugin

User Guide

Version 1.0.0.14

Last Updated: July 22 2020

Changes from v1.0.0.13 to 1.0.0.14

1. Support added for alarms generated by inputs.

Changes from version 1.0.0.12 to 1.0.0.13

1. Added support for independent polling periods for events and badge updates.

Changes from version 1.0.0.10 to 1.0.0.12

1. Added logging.

Changes from version 1.0.0.9 to version 1.0.0.10

1. Removed “Web API Public Key” configuration setting. This is no longer required.
2. Only import readers from RS2 that are flagged as being installed.

Changes from version 1.0.0.1 to version 1.0.0.9

1. Ability to not do strict SSL certificate checking. In order for this to be enabled the “Use strict SSL certificate check” option must be enabled in the XProtect Management client.
2. “Access Control Administration” dropdown buttons in the Smart Client will open a browser and take the user to cardholders or reporting sections of the web client. In order for this to work, the “RS2 Access It! Universal.NET Web Client URL” text field must be filled in in the XProtect Management client.
3. Additional door commands have been added, including “Grant Access” and ability to set the reader mode to “Card Only”, “PIN Only”, etc.
4. Ability to log into the RS2 access control system as a particular user. The user will be prompted for their RS2 credentials after they login to the Smart Client. In order for this to work, The “Operator login required” checkbox must be checked in the XProtect Management client. When this feature is enabled, users will only see doors (readers) that they have privileges for. Also, users will only be allowed to execute reader commands that they have permissions for.
5. Version 1.0.0.8 was build using Release 2020 R1 of the MIP SDK. Version 1.0.0.1 was built using Release 2018 R1.

Changes from version 1.0.0.0 to version 1.0.0.1

1. Support has been added for the Access It! Universal.NET web service PublicKey header.

Introduction

The RS2 Milestone Access Control Plugin can be used to integrate with the RS2 Access It! Universal.Net system in order to add basic access control functionality to the Milestone XProtect Smart Client. This will allow the Smart Client user to:

- View current RS2 credential holders (including photos).
- Associate cameras with doors.
- View the current state of doors (locked/unlocked/open/closed).
- Unlock and lock doors with a button press.
- View access control events as they happen (e.g. door opened/closed/forced open).
- Have alarms raised in the XProtect Smart Client as a result of access control events.

Pre-Installation

Access It! Universal.NET must be licensed and configured to use its native API and a dedicated MIPS login with password with full permissions (Administrators group) must exist within the Users section. More information on configuring the API can be found within the RS2 Technologies knowledge base.

When using the native API with Access It! Universal.NET Version 7, HTTPS is required. The API port will need to be an encrypted connection and SSL certificate bound to the port.

(See KB article for reference on Binding SSL Certificate to Port:
<https://helpdesk.rs2tech.com/kb/article/701-bind-ssl-certificate-to-port>)

During the installation the Milestone MIPS will require a Public API key to be entered. This information should be provided during the Access It! Universal.NET licensing setup. Should the API keys not be delivered, please contact APIKeyRequest@rs2tech.com providing the dongle serial number.

Installation

The plugin should be installed on the machine that runs the XProtect Event Server. A new folder should be created at the following location:

C:\Program Files\Milestone\MIPPlugins\RS2MIPPlugin

The following files should be copied there:
acplugin.def IO.Swagger.dll

Newtonsoft.Json.dll
RestSharp.dll
RS2MIPPlugin.dll

On certain Windows 10 installations the DLL's may be blocked. To resolve this, right-click on each DLL and select Properties. Within the properties screen check the Unblock option.

Configuration

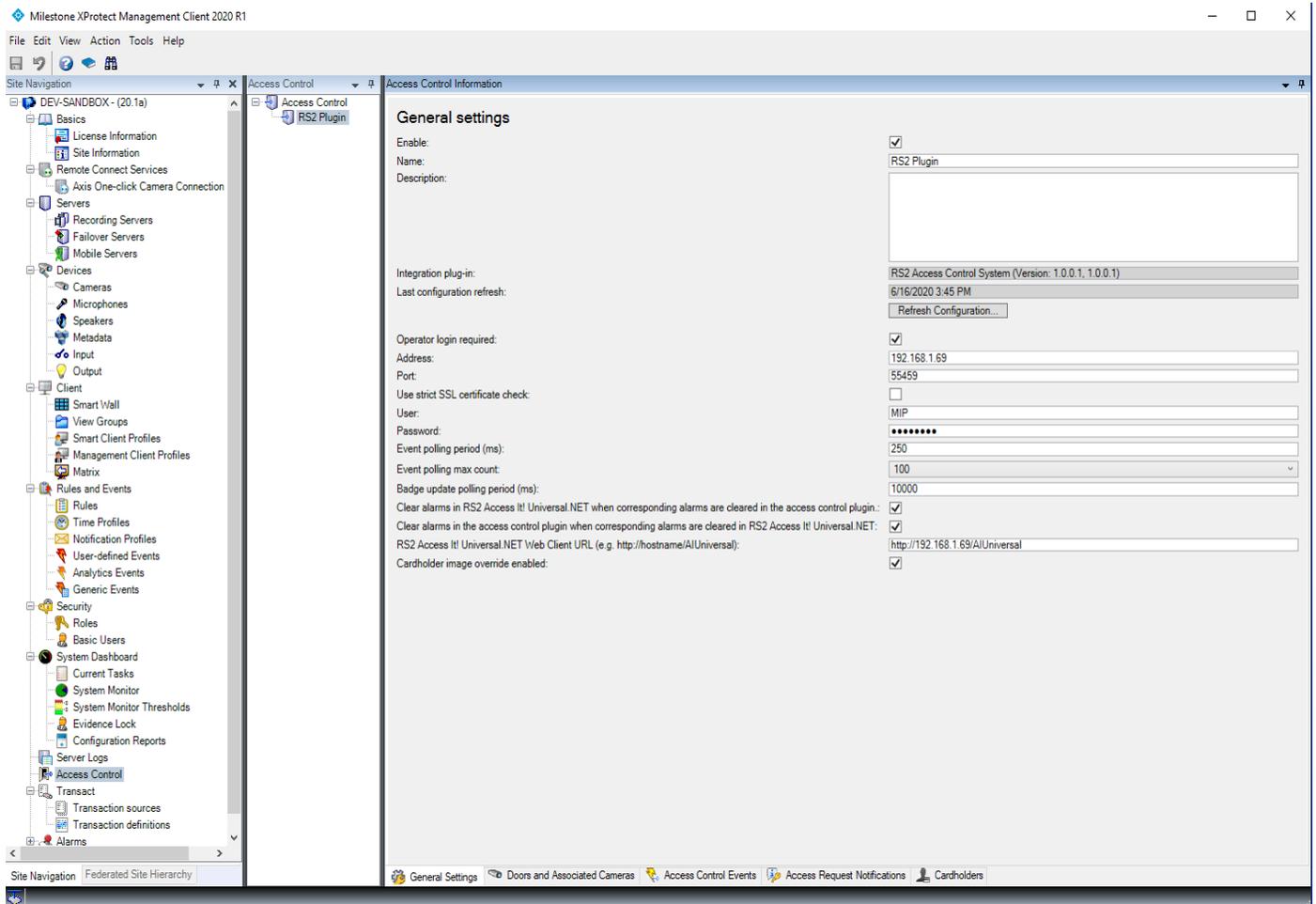
XProtect Management Client

Once the plugin has been installed it can be configured using the XProtect Management Client using the Access Control section (see screenshot). To start, right click on "Access Control" and select "Create New..." select "RS2 Access Control System" in the dropdown and enter a name for the plugin. Modify the settings as desired and save.

Note that the "Web API Public Key" is required. Strict SSL certificate checking can be disabled if desired using a checkbox.

When prompted for Port, enter the Access It! Universal.NET API Port.

When prompted for Username and Password enter the dedicated (Administrator) login created in the preinstallation section.

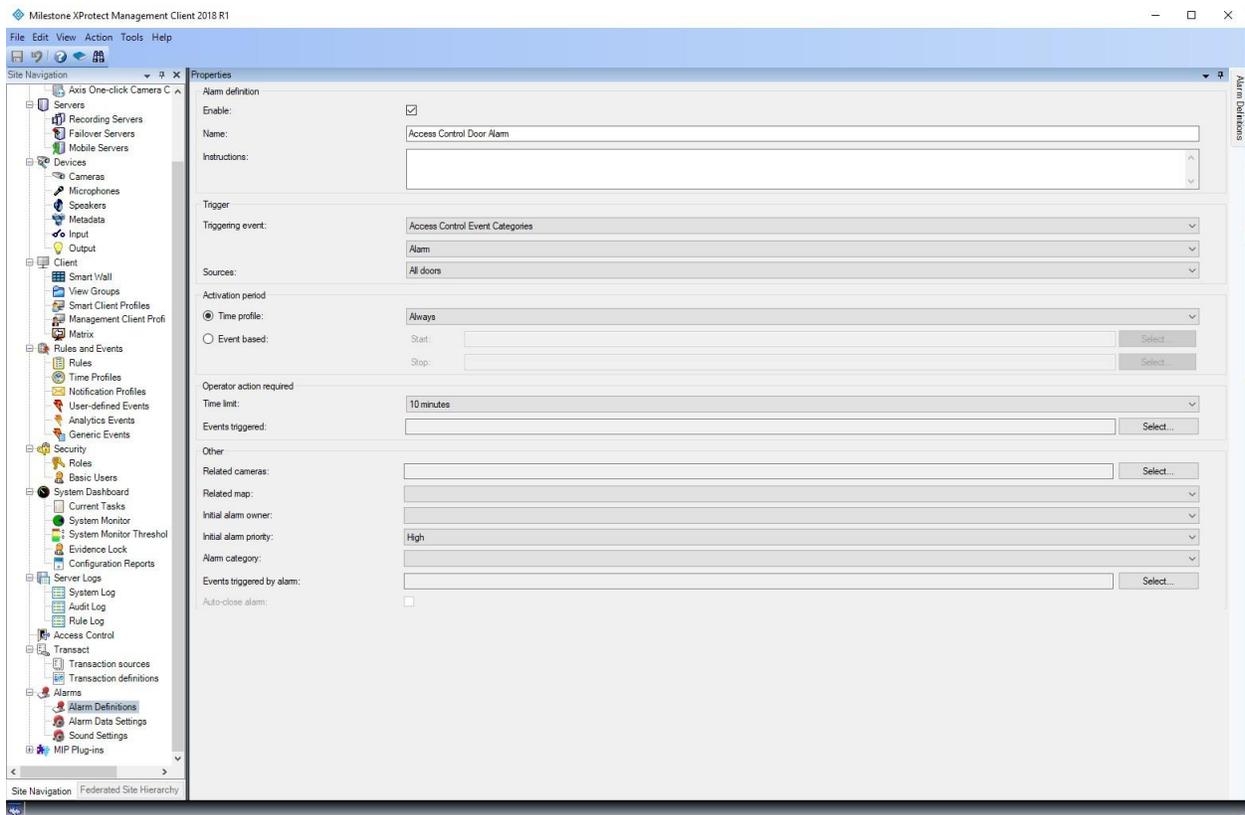


If the access control hardware configuration changes (e.g. a new reader was added) the “Refresh Configuration...” button should be pressed to sync those changes to the RS2 Access It! Universal.NET software.

Event/Alarm Categories

A list of all events and event categories can be viewed in the “Access Control Events” tab of the XProtect Management Client. One way to have an event trigger an alarm is as follows:

1. Add the alarm category to the event
2. In the “Alarms” section of the Management Client (selected using the tree view), add an Alarm Definition with a triggering event of “Access Control Event Categories” and select the “Alarm” category. See screenshot below.



Alarm Syncing

It is possible to sync the clearing of alarms between the Milestone XProtect system and RS2 Access It! Universal.Net. There are two options to enable syncing:

- Clear alarms in RS2 Access It! Universal.NET when corresponding alarms are cleared using the access control plugin.
- Clear alarms in the access control plugin when corresponding alarms are cleared in RS2 Access It! Universal.NET.

There are a few things to keep in mind:

1. Alarm syncing is done between source and target systems for events having the same source device (e.g. the same door reader) and the same event type (e.g. door forced open) in both systems. In other words, if all door forced alarms for the building entrance reader are cleared in the plugin, those alarms will also be cleared in the RS2 system (assuming that the feature is enabled via the configuration option). No other alarms will be cleared in the RS2 system.
2. Alarm syncing is all or nothing - only when ALL alarms of a particular source and event type are cleared in the source system will ALL corresponding alarms be cleared in the target system.
3. There are conditions that can prevent an alarm being acknowledged and cleared in RS2 Access It! Universal.NET. These include:

- a. An option can be set in Access It! Universal.NET to require that an operator comment be entered before an alarm is acknowledged. If this option is set, the alarm won't be automatically acknowledged and cleared.
- b. An option can be set in Access It! Universal.NET to prevent alarms from being cleared if the device that generated the alarm is in an unsecure state. If this option is set then the alarm won't be automatically be cleared in Access It! Universal.NET.

Setting up Alarms triggered by Inputs

To trigger an alarm, events must be assigned to one or more event categories. There are predefined event categories for inputs. These can be seen in the “Access Control Events” tab in the Management Client, see below circled in red. It is also possible to create a user-defined event category (see button at bottom of screenshot).

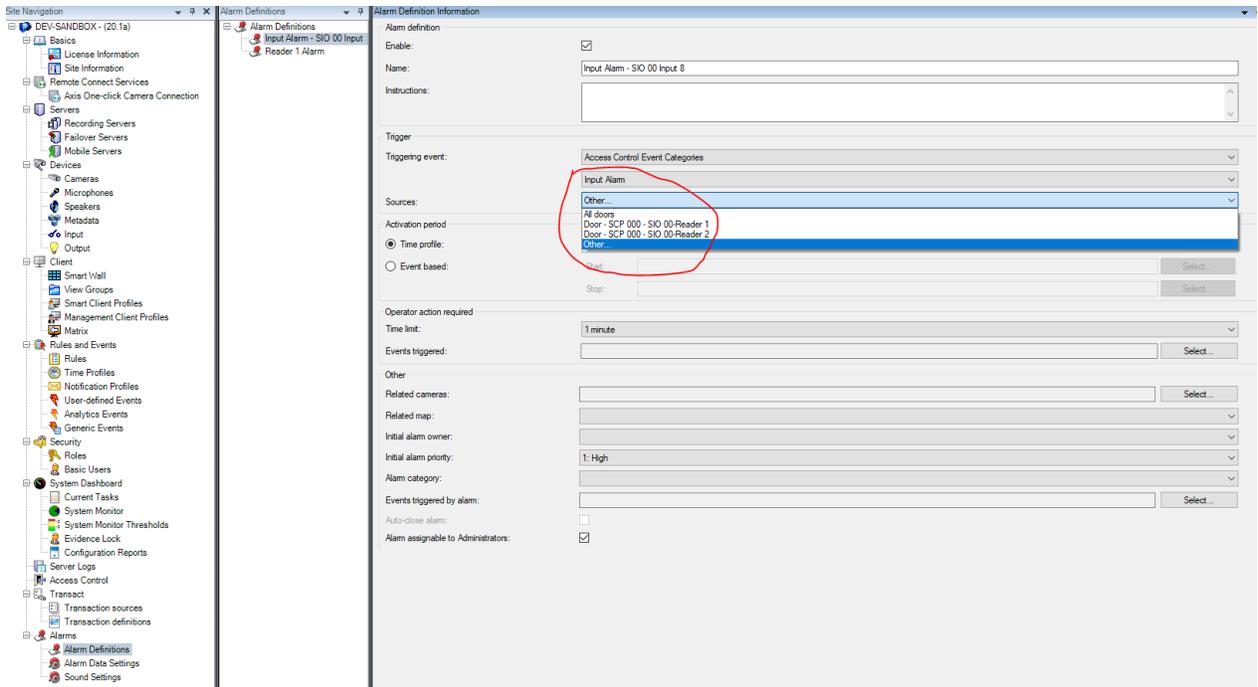
The screenshot shows the 'Access Control Information' window with the 'Access control events' tab selected. The window contains a table of events and a dropdown menu for the 'Event Category' column. The 'Input Alarm' category is circled in red.

Enabled	Access Control Event	Source Type	Event Category
<input checked="" type="checkbox"/>	Deadbolt Deactivated		
<input checked="" type="checkbox"/>	Delete Record		
<input checked="" type="checkbox"/>	Device Offline		
<input checked="" type="checkbox"/>	Device Online		
<input checked="" type="checkbox"/>	Diagnostics Failed		
<input checked="" type="checkbox"/>	Diagnostics Passed		
<input checked="" type="checkbox"/>	Door Closed	Access Point, Door	
<input checked="" type="checkbox"/>	Door Forced Open	Access Point, Door	Door Error
<input checked="" type="checkbox"/>	Door Forced Open Disabled	Access Point, Door	Door Error
<input checked="" type="checkbox"/>	Door Forced Open Enabled	Access Point, Door	Door Error
<input checked="" type="checkbox"/>	Door Held Open	Access Point, Door	
<input checked="" type="checkbox"/>	Door Held Open Disabled	Access Point, Door	
<input checked="" type="checkbox"/>	Door Held Open Enabled	Access Point, Door	
<input checked="" type="checkbox"/>	Door Held Open PreAlarm	Access Point, Door	
<input checked="" type="checkbox"/>	Door Open	Access Point, Door	
<input checked="" type="checkbox"/>	Door Supervisory Fault	Access Point, Door	
<input checked="" type="checkbox"/>	Double Card Event	Access Point, Door	
<input checked="" type="checkbox"/>	Double Card Event (door locked/unlocked)	Access Point, Door	
<input checked="" type="checkbox"/>	Elevator DEC Offline		
<input checked="" type="checkbox"/>	Elevator DEC Online		
<input checked="" type="checkbox"/>	Email Send Failed		
<input checked="" type="checkbox"/>	Email Sent		
<input checked="" type="checkbox"/>	Enrollment-Existing Card		
<input checked="" type="checkbox"/>	Enrollment-New Card		
<input checked="" type="checkbox"/>	Entry Delay In Progress	Access Point, Door, Input	
<input checked="" type="checkbox"/>	Execute Command		
<input checked="" type="checkbox"/>	Input Alarm	Access Point, Door, Input	Input Alarm
<input checked="" type="checkbox"/>	Input Disabled	Access Point, Door, Input	
<input checked="" type="checkbox"/>	Input Enabled	Access Point, Door, Input	
<input checked="" type="checkbox"/>	Input Secure	Access Point, Door, Input	
<input checked="" type="checkbox"/>	Input Supervisory Fault	Access Point, Door, Input	
<input checked="" type="checkbox"/>	Insert Record		
<input checked="" type="checkbox"/>	Intercom Call Requested		
<input checked="" type="checkbox"/>	Intercom Door Open Request		
<input checked="" type="checkbox"/>	Intercom Station Connected		
<input checked="" type="checkbox"/>	Intercom Station Disconnected		
<input checked="" type="checkbox"/>	Interior Push Button Activated		
<input checked="" type="checkbox"/>	Interior Push Button Deactivated		

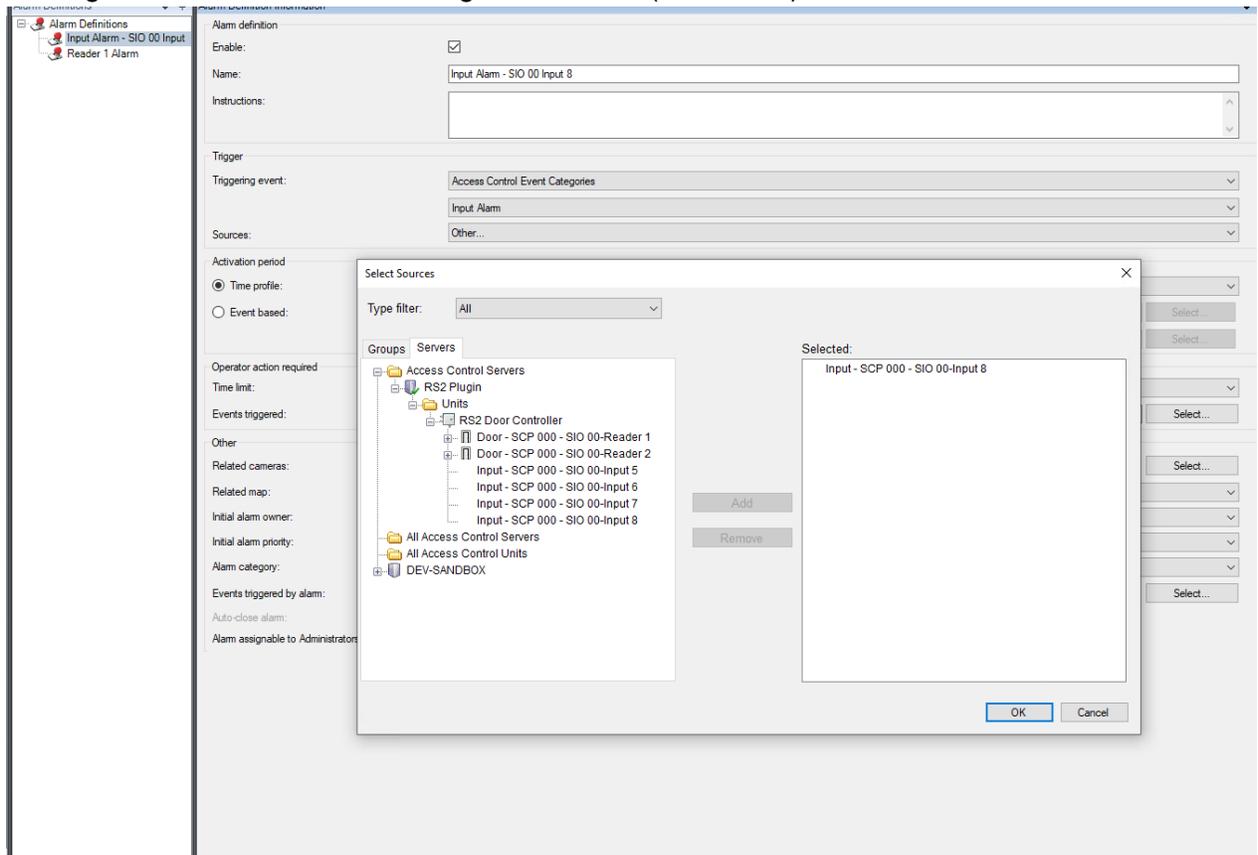
The dropdown menu for 'Event Category' is open, showing the following options:

- All categories
- Access denied
- Access granted
- Access request
- Alarm
- Door Error
- Error
- Input Alarm
- Input Disabled
- Input Enabled
- Input Entry Delay In Progress
- Input Secure

An alarm definition must be defined before input alarms can be triggered in the XProtect smart client. One or more inputs can be selected by picking “Other...” from the Sources dropdown of the Alarm definition screen (see below).



Picking "Other..." will cause a dialog to be shown (see below):



The inputs can be selected by expanding the folders beneath “Access Control Servers” as shown above and scrolling down beneath the list of doors. One or more inputs can be selected, double clicking will move the input to the “Selected” list on the right hand side.

Once this setup has been done the selected inputs will generate alarms for events of the selected categories.

Error logs

For troubleshooting purposes, error logs are available in the following location:

C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs

Typical Usage

The RS2 access control plugin is shown below. There are several views available (cardholders/doors/events). The screenshot shows the Events view in Live Update mode.

8:45:25 AM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 3/28/2019. To fully license the product, please contact your reseller or find one on www.milestoneys.com.

Events Doors Cardholders

Search cardholders Live update

Live update All events All doors

Time	Event	Source	Cardholder
7/25/2018 11:09:30 AM	Door Held Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 11:09:00 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 11:09:00 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 11:08:59 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 11:08:59 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 10:25:30 AM	Door Held Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 10:25:00 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 10:24:59 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 10:24:54 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 10:24:54 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:44 AM	Door Held Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:14 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:13 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:12 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:12 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:12 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:11 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:11 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:11 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:10 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:10 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:09 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:24:09 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:23:06 AM	Door Held Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:36 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:35 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:35 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:32 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:32 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:31 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:31 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:26 AM	Door Forced Open	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:26 AM	Door Closed	SCP 022 - SIO 00-Reader 1	
7/25/2018 9:22:26 AM	Door Closed	SCP 022 - SIO 00-Reader 1	

No related cameras.

Server connected

Time:
7/25/2018 9:02:08 AM

Source:
RS2 Access Control System on localhost