



Secure365 v1.0.8

User Guide

DECEMBER 7, 2019

REVISION 1.1

Accuracy Statement

While reasonable efforts have been made to assure the accuracy of this document, Siroonian Technologies, Inc. (STI) assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information contained within. STI reserves the right to make changes to any products described and reserves the right to revise this document. STI may make changes from time to time in the content of this document with no obligation to notify any person of revisions or changes. STI assumes no liability arising from application nor does it convey license under its patent rights or the rights of others.

Copyrights

This document, STI products, and 3rd Party software products described in this document may include or describe STI copyrighted and other 3rd Party supplied computer. Laws in the United States preserve for STI, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of STI, its licensors, or 3rd parties contained in STI products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without prior, express written permission from STI. The purchase of STI products shall not be construed to grant either directly or by implication, any license under the copyrights, patents or patent applications of STI or other 3rd Party supplied software, except for the normal license to use that arises in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of STI.

Licensing

The software described in this document is the property of Siroonian Technologies and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement

High Risk Activities

STI and its supplier(s) specifically disclaim any express or implied warranty of fitness of this product for any high-risk activities ("High Risk Use"). Any High-Risk Use is made at your own risk and you shall be responsible for any and all losses, damage or claims arising from said use.

Revision History

Document Version	Updates	Date
v1.0	Initial version	2019-12-05
V1.1	Updated Figures	2019-12-7

Contents

List of Figures	5
About This User Guide	6
Purpose	6
Contacting Siroonian Technologies.....	6
Training	6
System Overview	6
System Components	6
Normal Operation	6
Accessing Secure365.....	7
System Functions	8
Login.....	8
Alert Acknowledgement	8
Alert Hold	9
Alert Resolution	9
Relay Controls Panel	9
Relay Controls Window.....	10
Door Controls.....	11
SAS Log.....	12
Logout	13
System Configuration.....	14
Troubleshooting Guide	14
Login Issues	14
Missing Cause or Responder.....	14
Slow or Unresponsive Application	14
Related Documents & References	15

List of Figures

Figure 1 - Secure365 Dashboard	7
Figure 2 - Secure365 Authentication Window.....	7
Figure 3 – Alerts	8
Figure 4 - Alert Selected	9
Figure 5 - Relay Control Panel.....	10
Figure 6 – Axis Relay Controls, Module List	10
Figure 7 – Axis Relay Controls, Module I/O & Relay Monitoring.....	11
Figure 8 - Door Controls.....	11
Figure 9 - Door Controls Authentication.....	12
Figure 10 - SAS Log.....	13

About This User Guide

Purpose

This user guide provides an overview of Secure365 features and functions for the alarm station operator. This guide focuses on the functions and user flows supporting normal station operation.

Contacting Siroonian Technologies

For sales and product information, please contact Siroonian Technologies at -

info@siroonian.com

(781) 350-3596

For product support and feedback on this document, please contact Siroonian Technologies at -

support@siroonian.com

(781) 350-3596 x10

Training

Users of Secure365 should be familiar with this document prior to use and may require installation specific training. Use of the product without sufficient prior knowledge may result in misuse, loss of data, loss of functionality, and potentially loss of service.

System Overview

Secure365 is a Microsoft Windows application that utilizes .NET to interoperate with Milestone Systems XProtect® video management system (VMS) as a component-based integration. Secure365 provides a simple, integrated interface for an alarm station operator. The system is designed to meet the need of mid-tier Milestone implementations with alarm monitoring requirements.

System Components

Secure365 interface consists of two primary subsystems the alert console and the station log. The alert console includes an active alert list, a 2x2 **Video Callup** panel, and an alert update pane.

The system backend integrates with Milestone Event Server through the MIP SDK for alert notifications and updates as well as the Axis Communications APIXI® API for A1001 for door control and A9188 I/O status and relay reset. Alarm station data and events are stored in a Microsoft SQL Server database.

Normal Operation

In the vast majority of deployments Secure365 will run as a full-screen foreground application 24x7 (Figure 1). An alarm station operator will normally use the File, Switch User menu option to authenticate at shift change (Figure 2).

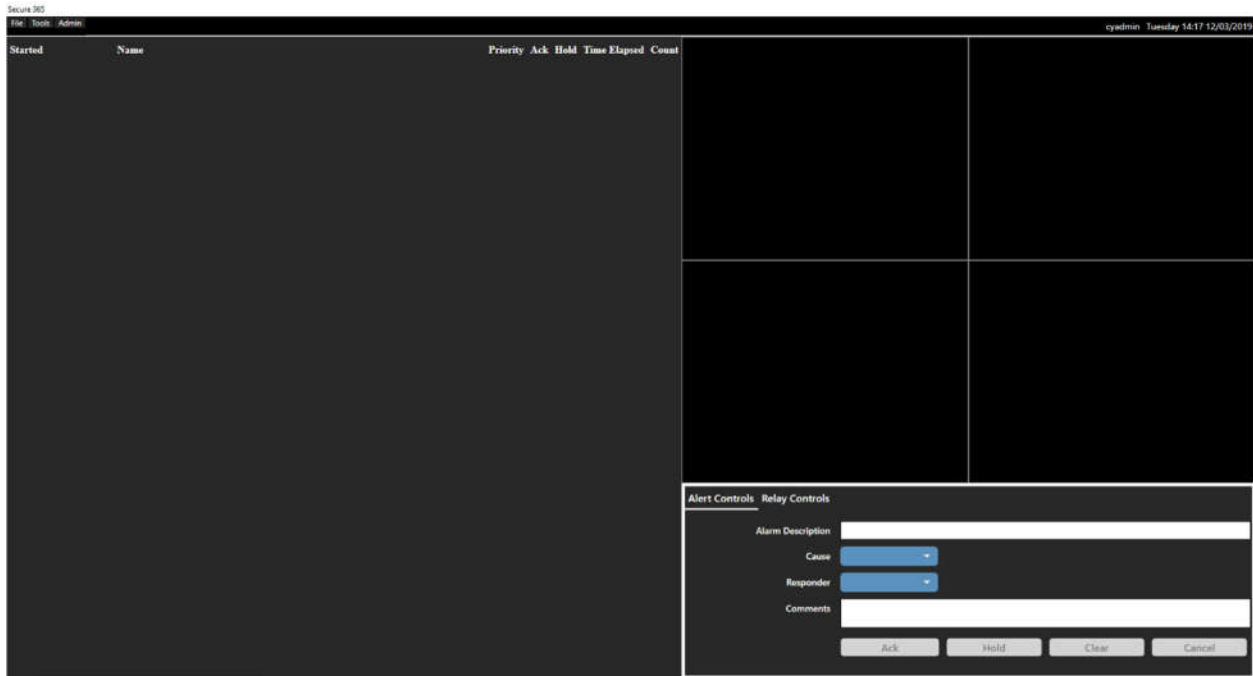


Figure 1 - Secure365 Dashboard

Accessing Secure365

Secure365 can be launched from its Windows desktop shortcut or taskbar icon. Launching the application brings up the **Authentication** window (Figure 2).

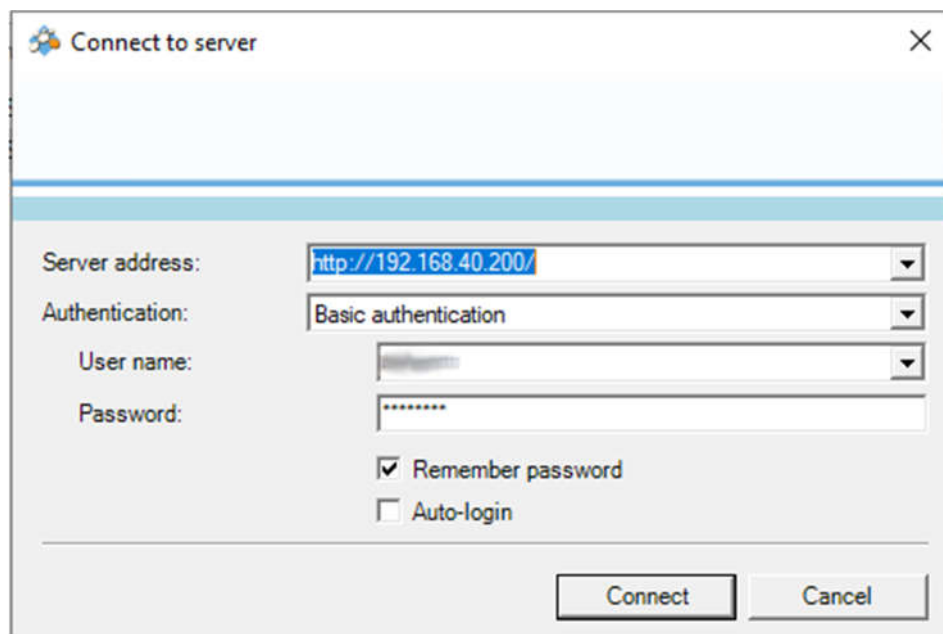


Figure 2 - Secure365 Authentication Window

In this window, the Server Address will be prefilled by the system installer, as will the Authentication method.

System Functions

Login

To login to the system, the alarm station operator will provide their Milestone XProtect Smart Client username and password in the **Authentication** window (Figure 2). The **Connect** button at the bottom of the **Authentication** window validates the user credentials and, when successful, launches the **Dashboard** window.

In a shared console deployment, operators would not normally specify Remember password or Auto-login. These functions are intended for single operator consoles.

Alert Acknowledgement

When a new alert event occurs, Secure365 will play the designated alert sound and insert a new row at the top of the active alert list (Figure 3). If configured by the Secure365 Administrator, the cameras associated with the alert will appear in the **video callups** panel at the top right of the **dashboard** window.

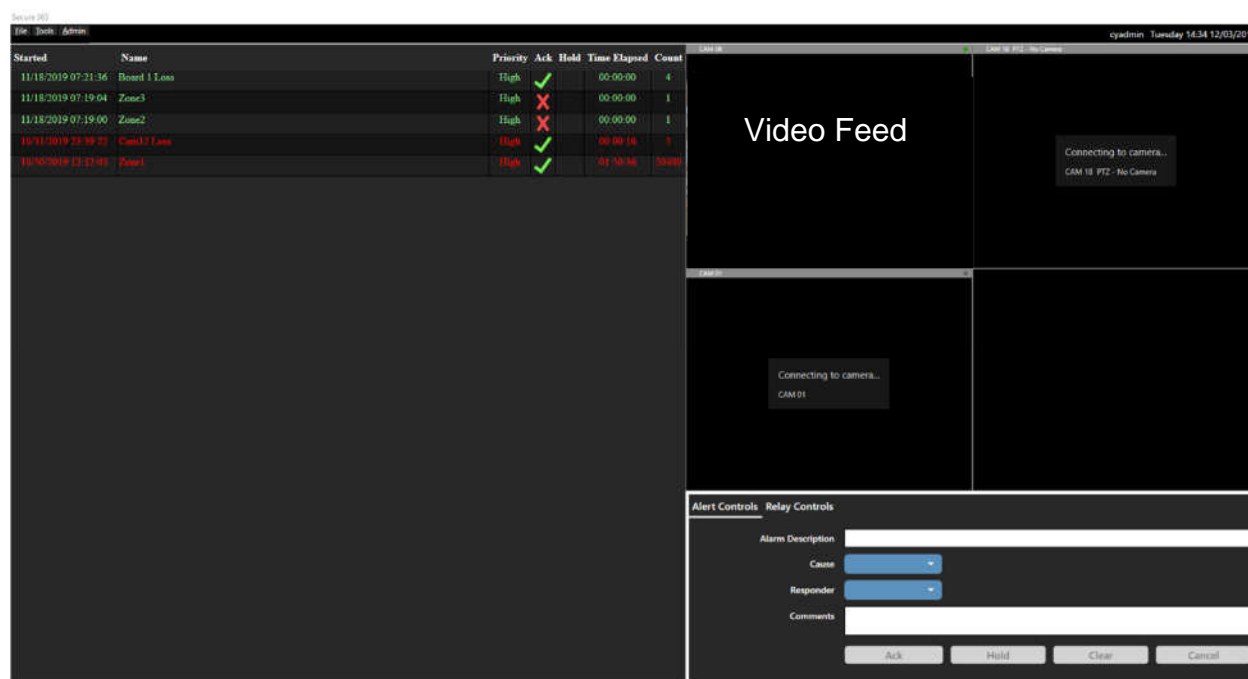


Figure 3 – Alerts

To acknowledge an alert, the operator must click on the appropriate row in the active alert table, causing the row to become highlighted (Figure 4). The **Ack** button (Acknowledge) is found in the **Alert Controls** panel at lower right of the **Dashboard** window or by right clicking on the Alert. Clicking Ack, silences the alert tone, and places a green check mark in the Ack column of the selected alert row.

If a remote monitoring station (RMS) trigger has been configured acknowledging and an alert will stop the RMS timer. Additional occurrences of an acknowledged alert increment the counter in the count column of that alert row. The Secure365 Administrator can designate an alert to be a remote monitoring station triggers.

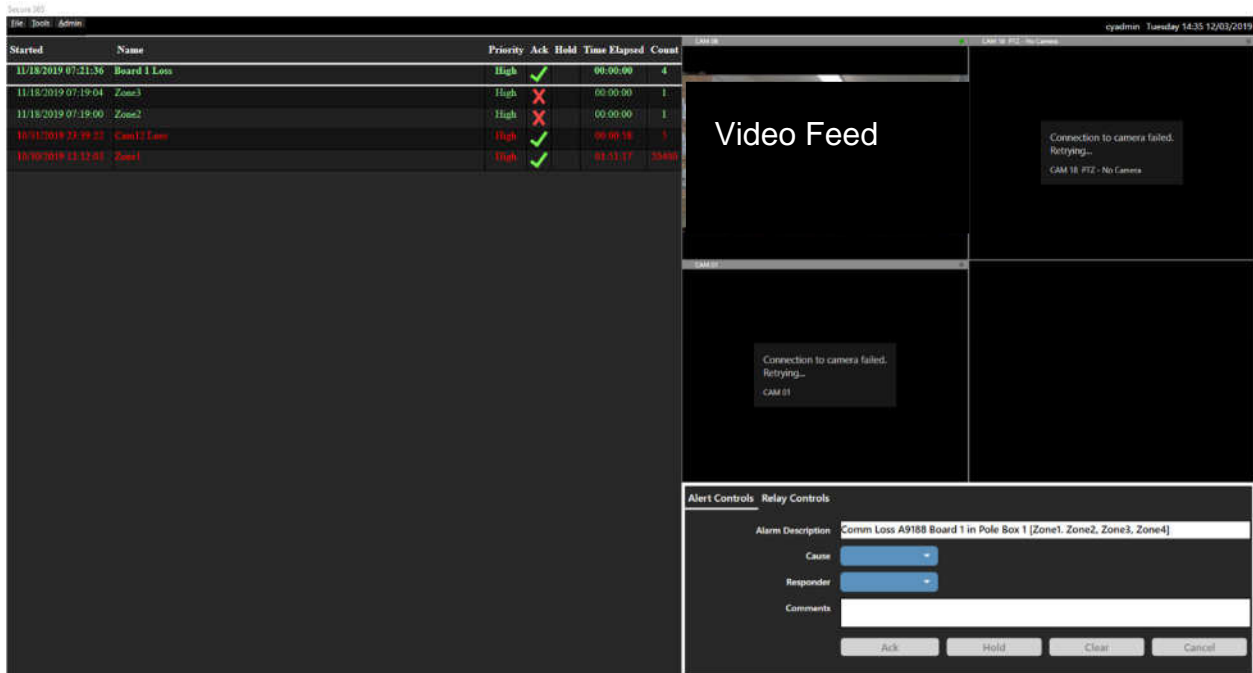


Figure 4 - Alert Selected

Alert Hold

The alarm station operator may provide a Cause, Responder, or Comments on an active alert without clearing the alert from the active alert table. After selecting or entering the desired information into the **Alert Controls** panel, the operator can click the **Hold** button in the lower right of the screen to save the input(s) with the active alert.

Alert Resolution

To clear or resolve a selected alert, the operator specifies a cause and a responder from the pre-configured dropdown lists in the **Alert Controls** panel at the lower right of the **Dashboard** window. With this information in place, the operator can click the **Clear** button which removes the alert from the active alert list.

Relay Controls Panel

The alarm station operator can view a list of the known Axis A9188 modules by selecting the **Relay Controls** tab in the lower right panel of the **Dashboard** window (Figure 5). The Secure365 Administrator configures the modules displayed in this panel.

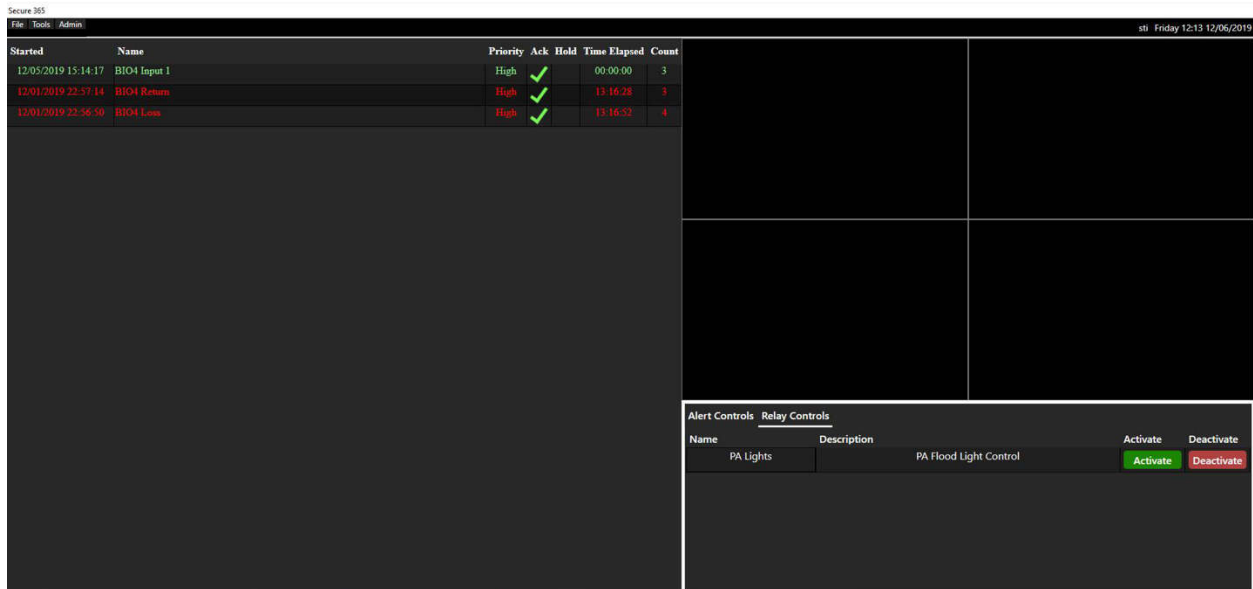


Figure 5 - Relay Control Panel

Relay Controls Window

The Tools, Axis Tool, Relay Controls menu item, give the alarm station operator the ability to inspect the state of known Axis A9188 modules (Figure 6). The operator can gain port level detail by selecting a row from the module list and clicking **Start Monitoring** button.

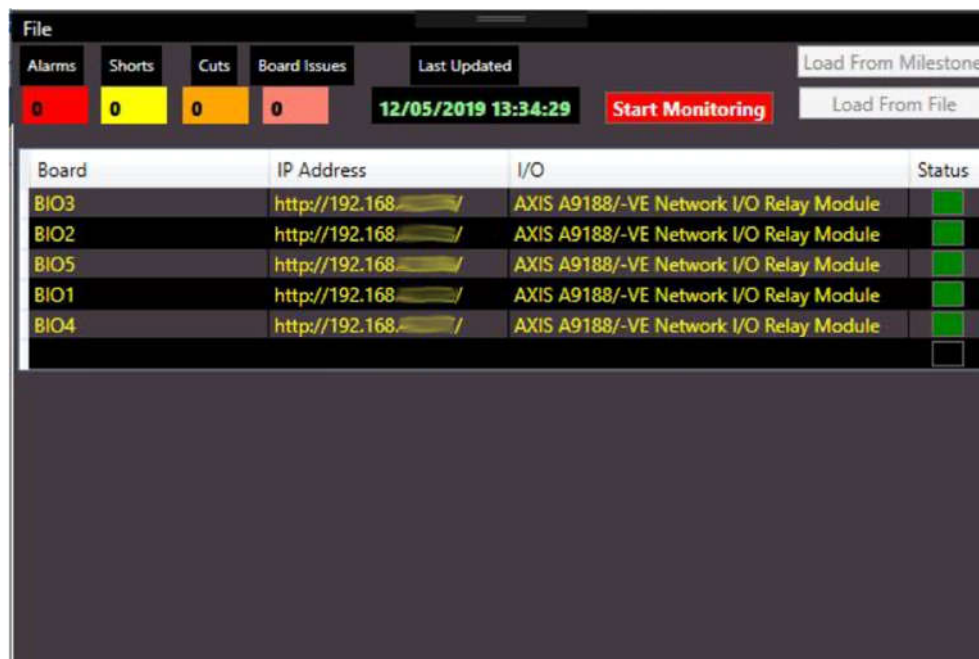


Figure 6 – Axis Relay Controls, Module List

The result is a listing of board ports showing type and status (Figure 7).

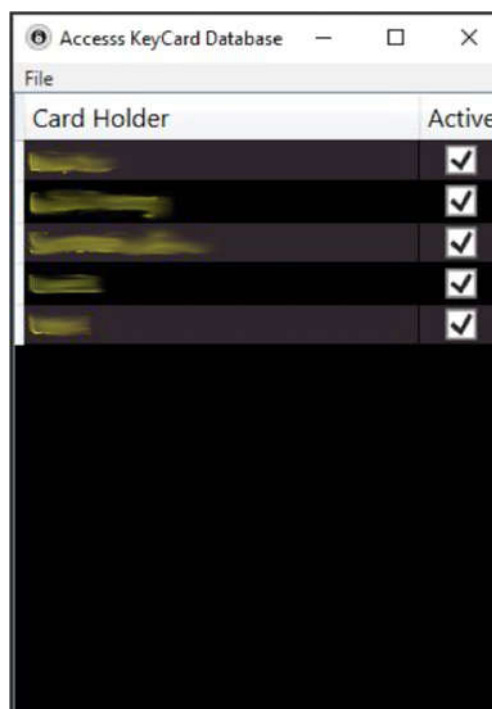


Board	IP Address	I/O	Status
BIO3	192.168.1.1	I/O 1	Green
BIO3	192.168.1.1	I/O 2	Green
BIO3	192.168.1.1	I/O 3	Red
BIO3	192.168.1.1	I/O 4	Red
BIO3	192.168.1.1	I/O 5	Green
BIO3	192.168.1.1	I/O 6	Green
BIO3	192.168.1.1	I/O 7	Green
BIO3	192.168.1.1	I/O 8	Green
BIO3	192.168.1.1	Relay 1	Green
BIO3	192.168.1.1	Relay 2	Green
BIO3	192.168.1.1	Relay 3	Green
BIO3	192.168.1.1	Relay 4	Green
BIO3	192.168.1.1	Relay 5	Green
BIO3	192.168.1.1	Relay 6	Green
BIO3	192.168.1.1	Relay 7	Green
BIO3	192.168.1.1	Relay 8	Green

Figure 7 – Axis Relay Controls, Module I/O & Relay Monitoring

Door Controls

The alarm station operator can deactivate or activate a Card Holder's access to an Axis A1001 access controller door through the Tools, Door Controls menu item.



Card Holder	Active
[Redacted]	✓
[Redacted]	✓
[Redacted]	✓
[Redacted]	✓
[Redacted]	✓

Figure 8 - Door Controls

The operator can specify the specific access controller and controller credential through the File menu in the **Access KeyCard Database** window (Figure 9 - Door Controls AuthenticationFigure 9). After specifying the **IP Address**, **Username**, and **Password**, clicking the **Save** button in the **Options_Windows** (Figure 9) launches the **Access KeyCard Database** window for the new access controller.

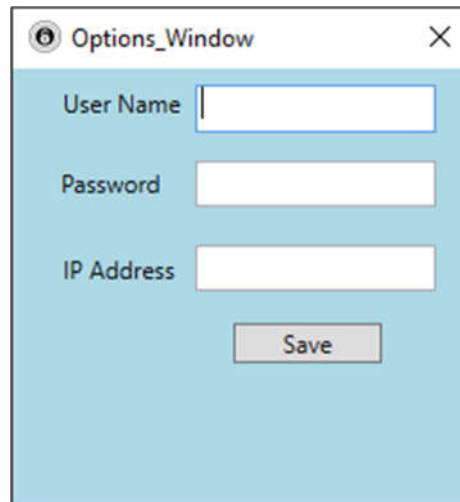
A screenshot of a software window titled "Options_Window" with a close button (X) in the top right corner. The window has a light blue background. It contains three text input fields: "User Name", "Password", and "IP Address", each with a corresponding label to its left. Below these fields is a "Save" button.

Figure 9 - Door Controls Authentication

SAS Log

The SAS Log function within Secure365 provides an integrated digital alarm station log to decrease the workload of the alarm station operator. To generate a new log entry, the operator specifies who is making the entry in the Operator field, and the Log Entry content at the top of the **SAS Log** Window (Figure 10). Log Entry content can be entered or selected from the dropdown list. Clicking the **Submit** button saves the entry with an auto-incrementing Log Id and automated timestamp in the Date/Time field. Entries are write-only and cannot be edited or deleted once submitted.

Log Id	Date/Time	Operator	Log Entry
10309	11/25/19 11:07:24	Operator	one two three
10308	11/25/19 11:07:08	Operator	live long and prosper
10307	11/25/19 11:07:06	Operator	live long and prosper
10306	11/25/19 11:06:53	Operator	test2
10305	11/25/19 11:06:50	Operator	test2
10304	11/12/19 09:29:19	Operator	test2
10303	11/12/19 09:24:31	Operator	test2

Figure 10 - SAS Log

Logout

To logout of the system, the operator selects File, Switch User from the menu bar to bring up the **Authentication** window for another operator (Figure 2).

If it becomes necessary to exit Secure365, the operator selects File, Exit from the menu bar.

System Configuration

System configuration functions are reserved for Secure365 administrators and support personnel. Users of Secure365 should not, under normal use, alter the configuration of the system, user accounts, or alerts.

Troubleshooting Guide

Login Issues

If an operator's login credentials produce an invalid login message, first check the Server Name and Authentication method in the **Authentication** window against the site-specific configuration. If these parameters are correct, contact your Secure365 Administrator to validate the username and potentially reset the password.

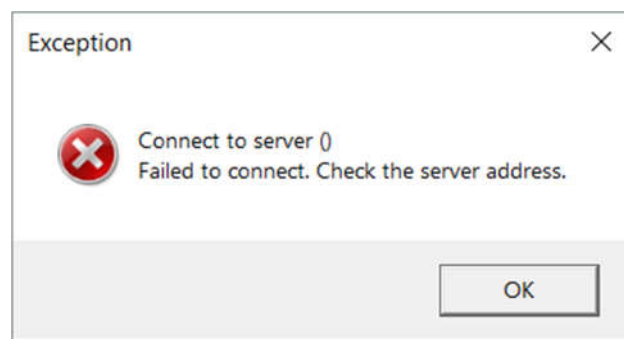




Figure 11 - Failed Login

Missing Cause or Responder

If the content of the Cause or Responder dropdown lists differ from the expected values, contact your Secure365 Administrator to validate the contents of the list(s) and to request updates.

Slow or Unresponsive Application

If the Secure365 Application become slow or unresponsive for more than a few seconds (due to high alert arrival rates or other activities), first attempt to exit the application by selecting File, Exit from the menu bar. If this is not possible, terminate the application using the Windows Task Manager. The Task Manager can be launched through *Type here to search* in the taskbar or by pressing Ctrl+Alt+Delete and selecting task manager from the list that appears on the screen. Once Secure365 has exited, it can be relaunched after a brief delay.

If restarting the application fails to clear the response issue, restart the Windows workstation through the Start menu () at the lower left of the display. Restart is in Power sub-menu (). After restarting the workstation, relaunch Secure365.

If restarting the workstation fails to clear the response issue, contact you Secure365 Administrator.

Related Documents & References

Secure365 Administrator Guide

Secure365 Installation Guide

XProtect VMS Products - Administrator getting started guide -

<https://www.milestonesys.com/support/self-service-and-support/manuals-and-guides/?prod=3&type=13&lang=27>

Bringing open IP benefits to physical access control. AXIS A1001 Network Door Controller -

https://www.axis.com/files/brochure/bc_pacs_a1001_57901_210x280_en_1405_lo.pdf

AXIS A1001 Network Door Controller Installation Guide -

https://www.axis.com/files/manuals/iq_a1001_1972057_en_1903.pdf

AXIS A9188 Network I/O Relay Module Installation Guide - Full Reference -

https://www.axis.com/files/manuals/iq_a9188_1742335_en_1705.pdf