

S2 NetBox™ Access Control

APPLICATION INFORMATION
for Version 2.5 and later

Feature Summary

- Built-in ODBC-compliant database for personnel data
- Integrated photo ID capability with video verification
- System-wide anti-passback function
- Dual reader and keypad support by time and threat level
- “First-in-unlock” rule enforcement
- Network-secure API for external application integration
- Multiple access cards per person
- Simultaneous support for multiple access card formats
- One-click playback of access-related video
- Elevator control
- Access levels variable by threat level
- Personnel report shows date and time of last card use
- Schedule portal unlock by time and threat level
- Central station alarm panel integration for disarm on access
- Card format decoder quickly decodes unknown card formats
- Card enrollment by reader or keyboard
- Freeform query specification for access history reports
- Daily history export for time and attendance applications
- Activation and expiration date and time to the minute
- User-defined data fields in personnel records

Overview

The S2 NetBox™ access control system offers a full-featured, credential-based access control program running on a solid state network appliance. Its architecture is fully distributed, with a complete database maintained on the S2 Network Controller (S2NC) and relevant data distributed to the S2 Network Nodes (S2NNs), assuring that the access control capability survives network outages. The ODBC-compliant database permits multiple cards per person and multiple card formats per system. The system is controlled from a standard web browser requiring no software installation and no client licenses.

The access control facility integrates fully with the optional Identity Management Solution for ID photo capture and badge

generation as well as with the Video Management System for access transaction recording and replay. Integration with common alarm panels includes such features as system disarm on valid access by selected people and access privileges that are enabled when a building alarm system is disarmed.

Security policies and business rules can be changed based on the day of the week, time of day, holiday schedule, or instantly using the system’s threat level capability. The access privilege mechanism supports general portal and elevator access control regimes, and is integrated with threat levels and alarm panels.

Access history is stored in the database which is automatically backed up nightly to on-board compact flash (CF card) and optionally exported to network attached storage (NAS or FTP). Historical queries are run from the system’s user interface and the data is available online through ODBC to such applications as Crystal Reports® and Microsoft Excel® or offline through the automatically exported CSV file. Reports automatically retrieve historical data from offline storage if required.

When interfacing or control through external applications is desired, the access control database can be populated using the system’s XML-based API. Both routine communication between the S2NC and S2NN and the API utilize encryption and authentication for data security.



All personnel data, including ID badge production, is managed from a tabbed display in your web browser



Access Control in detail...

Main : Administration : Reports : History : Access History

Date	Time	Local Date/Time	Name	Reader	Type	Location
2006-02-22	13:24:54	2006-02-22 13:24:46	Welles, Michael	Back Door	Access granted	Back Door
2006-02-22	11:49:03	2006-02-22 11:49:01	Welles, Michael	Front Door	Access granted	Front Door
2006-02-22	11:11:09	2006-02-22 11:11:04	Welles, Michael	Back Door	Access granted	Back Door
2006-02-22	11:08:25	2006-02-22 11:08:21	Welles, Michael	Dev (S1P1)	Access granted	S2Dev Front D
2006-02-22	11:07:17	2006-02-22 11:07:14	Welles, Michael	Back Dnrr	Access granted	Back Dnrr

"TRACE MICHAEL WELLES FROM JANUARY TO MARCH" natural language query results. Highlighted links let you navigate to the data right from the report. Knowledge of SQL is not needed to get useful information.

Queries on person data fields can be used to locate matching records for

The built-in card format decoder simplifies determination of unknown card formats facilitating retrofits of legacy security systems.

The S2 NetBox event scheduler lets users plan in advance by scheduling extended portal unlocks or temporarily suspending automatic unlocks as required.

Scheduled Action - Windows Internet Explorer

http://192.168.0.250/manualoverride.asp?_sessionId=1148617282&typecode=P8&id=1

Action	Start Date/Time	End Date/Time	Comment	Person	Delete?
Unlock	11/08/2006 18:28:17	11/08/2006 20:28:17	Late staff meeting	Moss, John	Yes
Lock	11/09/2006 14:00:00	11/09/2006 18:00:00	Closing early for inventory	Moss, John	Yes
Unlock	11/10/2006 18:00:00	11/10/2006 21:00:00	Board meeting	Moss, John	Yes

add new

Lock 11/08/2006 17:30:16

Now At In (HH:MM) After (HH:MM)

Save Cancel

Specifications

Card readers per S2 Network Node	14	Controlled floors per elevator	52
Card readers per S2 Network Controller	224	Access levels per person	16
Card records per S2 Network Node	20,000	Card formats per Network Node	15
Online history transactions	up to 7,000,000	Cards per person	6
Card readers per Access Control Module	2	Access levels per Network Controller	512
Alarm points per Access Control Module	4	Certified web browsers	MS-IE 6.0+ Firefox 1.0+ Safari (Mac)
Relays per Access Control Module	4		

S2 Security Corporation

World Headquarters
6 Abbott Road
Wellesley, MA 02418 USA
Tel: +1 781 237 0800
Fax: +1 781 237 4141

S2 Security EMEA

PO Box 292
West Byfleet
Surrey KT147NZ
United Kingdom
Tel: +44 (0) 1483 852181

S2 Security ASIA

808, #04-151 French Road
Kitchener Complex
Singapore 200808
Singapore
Tel: +65 65658916



www.s2sys.com