



**Securus Web**

*SecurusWeb*  
Users Manual



# Table of Contents

Foreword .....	0
<b>Part I SecurusWeb .....</b>	<b>5</b>
<b>1 Release Notes .....</b>	<b>5</b>
<b>2 Installing SecurusWeb .....</b>	<b>9</b>
PC Requirements .....	9
Network Requirements .....	10
User Permissions .....	11
Starting the Install .....	12
Post Install Checklist .....	20
<b>3 Using SecurusWeb .....</b>	<b>20</b>
<b>Rich Client .....</b>	<b>21</b>
Menu Bar .....	22
Explorer .....	24
Discovering VertX/Edge Hardw are.....	26
Commanding Hardw are.....	28
System Grid.....	29
Users .....	30
Security .....	30
Users .....	32
Roles .....	33
Settings .....	33
Events .....	35
Configuring an Event.....	36
Configuring an Alarm.....	36
Reports .....	40
Setup Tab .....	41
Criteria Tab.....	42
Sort/Group Tab.....	43
Columns Tab.....	43
Layout Tab.....	44
Partitions .....	44
<b>Web Client .....</b>	<b>48</b>
Monitor/Command.....	49
Events .....	50
Status .....	52
Reader Configuration.....	53
Scheduled Commands.....	54
Access Control.....	55
Cards .....	56
Card Sets .....	58
Access Levels.....	59
Door Groups.....	60
Areas .....	62
Contact Schedules.....	63
Schedules.....	65
Holiday Groups.....	67
Holidays .....	69
People .....	70

CardHolder Directory.....	70
Reporting .....	72
Reports .....	73
Utilities .....	75
Change User Passw ord.....	75
Upload Card Format.....	76
Customize Screen.....	76
<b>Utilities .....</b>	<b>76</b>
Data Archive.....	77
Database Maintenance.....	79
Database Brow ser.....	81
License Editor.....	82
<b>4 Troubleshooting SecurusWeb .....</b>	<b>82</b>
Error Log .....	82
Diagnostic Reports .....	82
VertX Communication Log .....	83
<b>Index .....</b>	<b>0</b>

# 1 SecurusWeb

Welcome to the SecurusWeb 4.3.0 Users Guide.

This guide provides procedural and reference information for the SecurusWeb application. To get the most out of this documentation, you should be familiar with:

- Normal application usage (Outlook, Word, etc...)
- The Microsoft Windows 2003 Server (and greater) environments
- General Programming and SQL concepts and usage
- The concepts of access control and building automation
- Working knowledge of HID's VertX and Assa Abloy's AHG420 hardware

Before you begin programming and administering the SecurusWeb system, please read this guide completely in order to avoid clerical and system configuration errors. If you are unsure of a programming procedure, please contact your installing dealer.

## 1.1 Release Notes

### **SecurusWeb 4.3.0:**

#### **Major Features/Enhancements**

- Support for HID EVO product line.
- Updated VertX/EVO Performance Counters
- Made HID data encryption call thread safe
- Mapped cards sets (removed previous ceiling of 254 total card sets)
- Set AHG420 anti-tailgating feature to OFF (default)
- Magnetic strip format modifications
- Firmware of AHG20 locksets is now stored in the database (more secure)
- AHG420 "callback" functionality enabled

#### **Bug Fixes**

- Numerous bug fixes and cosmetic changes.
- Fixed service Start/Stop windows event messages
- Stopped logging service interrogation windows event messages
- Updated DST rules during start up
- Card refresh performance optimizations
- Fixed minor memory leak and data synchronization holes

### **SecurusWeb 4.1.0:**

#### **Major Features/Enhancements**

- Added AES Encryption between AHG420 hardware and software.
- Improved network scalability related to the total number of AHG420 controllers.
- Added feature and licensing for Visual Verification.

- Implemented AHG420 support for iClass CSN, Felica, MiFare and DESFire cards.
- Added System Notification to the Home page.
- Support for more than 250 Access Levels.
- Compatible with IE7, IE8, Safari, FireFox and Chrome.
- Added ability to bulk add cards.

### **Bug Fixes**

- Numerous bug fixes and cosmetic changes.
- Fixed issue when renaming reader in Web Client.

## **SecurusWeb 4.0.0:**

### **Major Features/Enhancements**

- Added Encryption between VertX hardware and software.
- Improved network scalability related to the total number of VertX controllers per hardware server.
- Added licensing for ADImporter feature.
- New database schema (from 4 databases to 1).
- Compatibility with 32bit and 64bit versions of Windows Vista, 7 and Server 2008.
- Support for SQL Server 2008
- AVHS Support (AXIS video)

### **Bug Fixes**

- Added indexes to improve event history reporting.
- Partitions listbox in WebClient is now sorted.
- Numerous bug fixes and cosmetic changes.
- Install modified to handle both Default or Named Instance of SQL database.

## **SecurusWeb 3.3.0**

### **Major Features/Enhancements**

- Use of disconnected recordsets to improve speed (reporting).
- Added "Card and Pin" and "Pin Only" reader types.

### **Bug Fixes**

- Numerous cosmetic adjustments.

## **SecurusWeb 3.2.0:**

### **Major Features/Enhancements**

- Added ability to change hardware names via Web Client.
- Added ability to define users and assign roles via the Web Client.
- Changed the available Commands on the Status screen.
- Added simple alarm definition to the Web Client.
- Added the display of Tamper, Battery and AC Fail in the Web Client.

- Added ability to configure local inputs on a controller.
- Added the 37bit No Facility code card format.
- Added compatibility for VertX firmware version 2.2.7.49

## **Bug Fixes**

- Fixed a delayed Web Client UI issue introduced in 3.1
- Removed a 250 item limit in Web Client UI.
- Changed the default Keypad type from Essex to HID.
- Replaced archived reports
- Fixed bug with NO Facility code card sets.
- Addressed Event Report time outs.

## **SecurusWeb 3.1.0:**

### **Major Features/Enhancements**

- Installation Privatization
- Partition Privatization
- Custom card format definition in the WebClient
- Partition Administrator Utility (assign multiple Administrators of a single partition)
- Native SQL 2005 support

### **Bug Fixes**

- Numerous cosmetic and scalability fixes.

## **SecurusWeb 3.0.0:**

### **Major Features/Enhancements**

- Added support for HID VertX firmware versions 2.2.7.33, 2.2.7.38 and 2.2.7.39
- AHG420 Lockset support
- ONSSI Video support
- Full system auditing
- Additional Web-Browsers supported (Chrome, FireFox, IE and Opera)
- Additional WebClient functions (change password, view/modify alarm details, card set configuration)

### **Bug Fixes**

- Numerous cosmetic fixes

## **SecurusWeb 2.8.0:**

### **Major Features/Enhancements**

- Added support for HID VertX firmware version 2.2.7.20
- Updated VertX driver
  - Handles incoming events while waiting for CMD response

- Shorten timeout for card modifications
- Immediate disconnect on a timeout
- Added 2 new connection related events
- Added 3 counters for better diagnostics
- Correction of synchronization (UI/database/hardware)
- Addition of diagnostic reports
- Added the # of readers per partition on the “Home” page of the web client.
- Added a uninstall utility. (Start > Programs > WeBrix)
- Added PDF and links for Edge reader documentation.
- Added event/alarm comments and details to the web client.
- Addition of partition filtering in web client
- Added additional registry entries for better troubleshooting (gateway cache)
- Added connection timeout setting in registry
- Added additional support for users in a “workgroup” for setup.exe

## Bug Fixes

- Removed unneeded event bindings and added new “connection” related ones.
- Made the default SA password strong
- Fixed “Scheduled Commands” cross link bug.
- Modified UDL script to be more defensive
- Deleted cards are now shown in the rich client (once a “Refresh Cards” has been administered from the rich client.)
- Corrected visible events and hardware depending on partition rights
- Corrected the ability to save a cardset without a name.
- Modified Alarms Reports to show “Removed” alarms and user comments.
- Corrected the ability to assign access levels as an administrator of a second partition
- Updated HID VertX pdf's with the most current documents.
- Numerous cosmetic fixes

## **SecurusWeb 2.6.0:**

### Major Features/Enhancements

- Added support for HID VertX firmware version 2.2.7.18
- Added support for HID Edge Reader

### Bug Fixes

- Validation added to card number input field.
- Added support for EEPROM values formerly provided by Program Data
- Fixed Scheduled Commands edit error
- Validating Encoded ID is unique per cardset vs. globally
- Modified Card Detail page
  - When editing an existing card and the card has been assigned to a cardholder, AND the total number of cardholders available in the partition is under the limit for maximum number of items to display in a dropdown list, then the cardholder dropdown list should be populated with all available cardholders and the currently assigned cardholder selected. (Note: If the total number of cardholders available in the partition is OVER the limit for maximum number of items to display in a dropdown list, keep the current behavior—the cardholder dropdown list should be populated with ONLY the currently assigned cardholder.)



- Eliminated the possibility of duplicate Encoded IDs with leading zeroes
- Removed the automatic addition of firmware versions to the software.
- VertX firmware that's supported by SecurusWeb 2.6.0
  - 2.2.7.18
  - 2.2.5.7
  - 2.2.3.2
  - 2.2.3
  - 2.2.2
  - 2.2.1
  - 2.2.0
  - 2.1.1
  - 2.0.1
  - 2.0.0

## 1.2 Installing SecurusWeb

SecurusWeb is a modular software, meaning it can be installed on one server or spread across multiple servers on a network. Every SecurusWeb system must include the following features.

- Client Application: Also called the Rich Client. It's acceptable to have more than one server running the client application feature.
- Field Hardware Server: Also called the DCS (Device Communication Server). It's acceptable to have more than one server acting as a Field Hardware Server.
- Database Server: Only one Database Server is allowed per SecurusWeb system.
- Web Server: Multiple Web Servers are allowed per SecurusWeb system, but typically only one is present.

### Quick Links:

- [PC Requirements](#)
- [Network Requirements](#)
- [User Permissions](#)
- [Starting the Install](#)
- [Post Install Checklist](#)

### 1.2.1 PC Requirements

A typical SecurusWeb Server has the following requirements:

Item	Required	Recommended
Memory	2 GB	4GB+
Storage	5 GB of free space	25 GB for every 150 devices (v1000, v2000, Edge or AHG420 Lockset)
Processor	Pentium III Compatible - 1Ghz Clock Speed	3+Ghz
Screen	1024 x 768 Recommended	

**Required hardware:** Network Card

**Supported Operating System:**

- Windows XP (32bit)
- Windows Server 2003 (32bit)
- Windows Vista (32bit)
- Windows Vista (64bit)
- Windows 7 (32bit)
- Windows 7 (64bit)
- Windows Server 2008 (32bit)
- Windows Server 2008 (64bit)
- Windows Server 2008 R2 (64bit)

**Additional requirements:** Internet Explorer 7.0 or later (Chrome and Firefox are also supported), IIS (Internet Information Services).

**NOTE:** Additionally, the following will be installed or upgraded by setup:

- Windows Installer 4.5
- .NET Framework 3.5



***If installed on a XP machine, IIS limits the connection to 10. If the system is intended for more than 2 web-based users at any given time, use a Windows Server class operating system.***



***If installed on a server class machine, make sure the server has the Web Server and Application Server roles applied. In addition, the ASP.NET feature of the Web Server role must be enabled.***

## 1.2.2 Network Requirements

It very important to verify that the network is configured to accept and work with SecurusWeb.

In summary, verify the following:

- TCP port 4050 (from PC to VertX) and port 4070 (from VertX to PC) are available and not being blocked by a firewall or router.
- TCP port 2571 (AHG420 Lockset) is available and not being blocked by a firewall or router.
- Port 80 (for HTTP communication) is available and not being blocked by a firewall or router.
- Ports 23 (for Telnet) and Port 20 & 21 (for FTP) are available and not being blocked by a firewall or router.
- IPMulticasting using port 4555 is allowed on the network and not being blocker by a firewall or router.

**Average VertX/Edge/EVO Packet Sizes:**

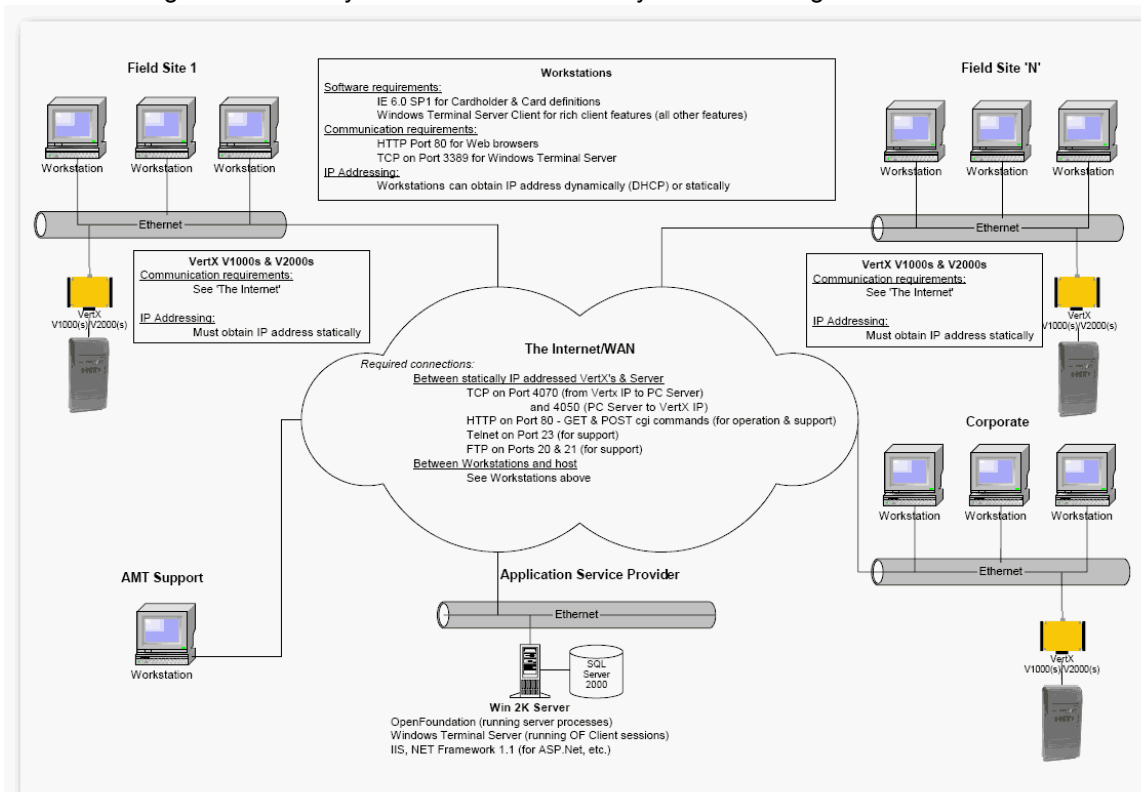
The following explains the average packet size for common network communications between a VertX/EDGE/EVO controller and SecurusWeb.

**Packet Sizes**

Traffic Causes	Total Traffic	Controller Send	Host Send (estimates)
Card Add/Modify/Delete	326 bytes	76 bytes	250 bytes
Discovery Process *	34 Kbytes	7 Kbytes	27 Kbytes
HereIAm Exchange	300 bytes	221 bytes	76 bytes
Single Event/Alarm	326 bytes	250 bytes	76 bytes
Command (open door)	326 bytes	76 bytes	250 bytes
Average Traffic Total	1 Kbytes per second		
*			

\* Determined by as average V1000 installation that includes a controller, two V100 panels, four Wiegand readers, four schedules, and 100 cards.

Below is a diagram the visually outlines some of the key network configurations:



### 1.2.3 User Permissions

When installing SecurusWeb, log into the server as a local Administrator. In other words, a user that is a member of the local Administrators group. **This user must have a password (not blank) as it's required when using DCOM.**

During the installation of SecurusWeb you'll be prompted to enter the username and password for the user who's authority the needed services will run under. This user also needs to be a local administrator. The machine you're installing SecurusWeb on can fall into one of two categories. The server can either be part of domain or part of a workgroup. There are some "best practice" rules

that apply to both scenarios.

- ✓ Workgroup: When installing SecurusWeb across multiple machines in a workgroup environment you should create a user that's part of the Administrators group on every server involved. This user must have the same username and password on each server. This user should be the one who's authority the needed services will run under.
- ✓ Domain: When installing SecurusWeb across multiple machines in a domain environment you should create a domain user and had this user to the Administrators group on every server involved. This user should be the one who's authority the needed services will run under.



***When installing the database feature on a machine that has a default instance of SQL already installed, the install will require the input of the sa password. If the sa password is incorrect or not known, the install will not complete successfully.***

## 1.2.4 Starting the Install

To install SecurusWeb, run the setup.exe from the CD (or resource location). The install will ask some basic questions that will vary on the PC state. The install will also install needed components if necessary (MDAC, .NET, etc.).

Continue through the basic setup screens until reaching the “Features” screen (see figure Features).

If you're doing a “all in one” install, all features should be checked. SecurusWeb is a modular software, meaning these features can be spread across multiple machines, but each SecurusWeb system must have ALL features (including the database) installed and communicating on the network in order to function properly. When installing a modular system (a system spread across multiple PC's), it's recommended to install the SecurusWeb database first and then continue on with the other features. If you have questions regarding setup, please contact support.

The features screen also asks to install a SecurusWeb database or attach to an existing one.

**WebBrix Setup**

**Select Features**  
Please select the function(s) which this machine will perform.

☒ Client Application  
☒ Field Hardware Server  
☒ Web Server

This feature installs the web application on the web server. This enables browser based access to the application.

**Database**

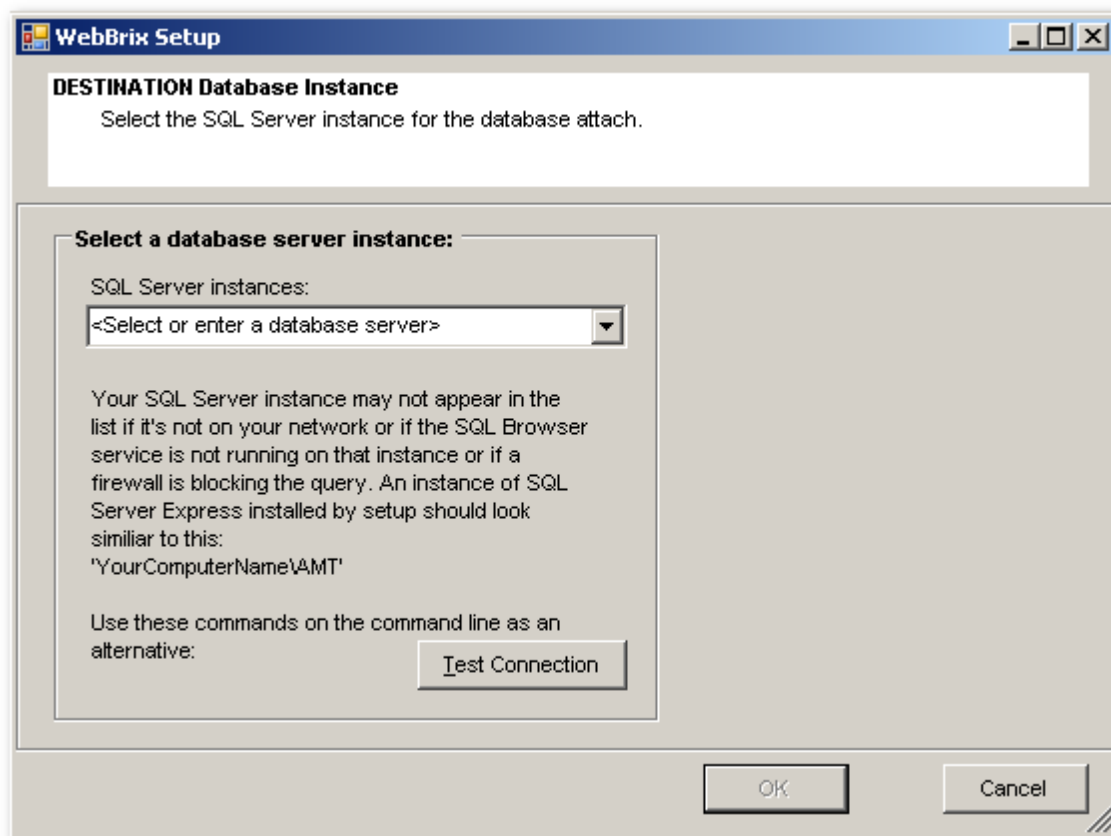
☒ Install the WebBrix database.  
☐ Attach to an existing WebBrix database.

The WebBrix database will be installed.  
By default, the SQL Server Express database engine will installed locally and the WebBrix database will be installed on it.

**Destination folder to install application to:**  
C:\Program Files\WebBrix Browse...

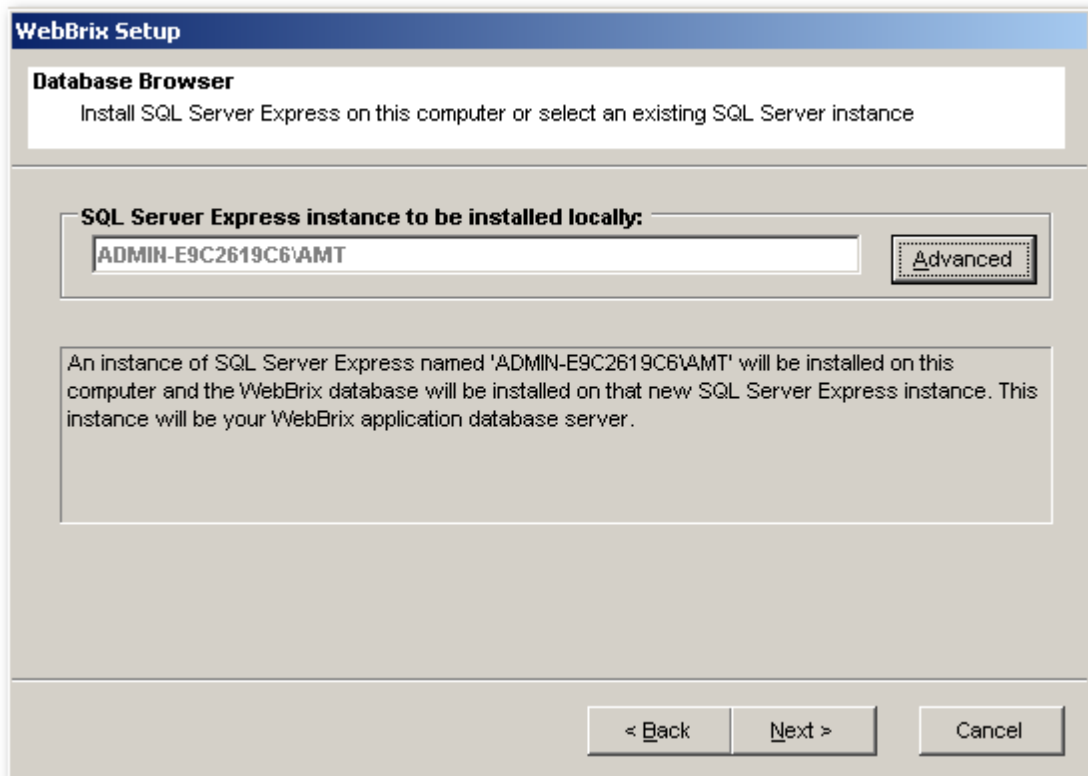
< Back   Next >   Cancel

If attaching to an existing database (see figure Existing), select the database server from the list and click the "Test Connection" button to verify.



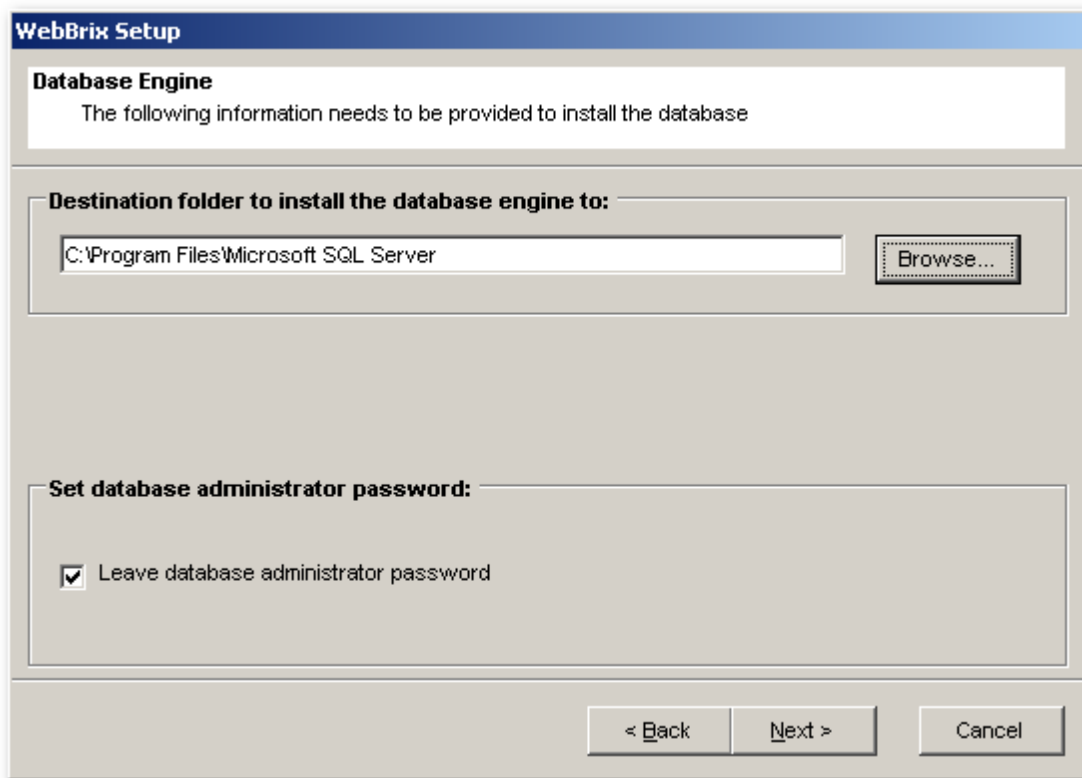
Existing

If installing the database (see figure Install), either click "Next" to install the database locally (on current machine) or click "Advanced" to select another SQL machine.



**Install**

Again, if installing the database, select the location and set the Administrator (sa) password and click "Next"



The screenshot shows a Windows-style setup window titled "WebBrix Setup". It has a blue header bar. Below the header, there's a section titled "Database Engine" with a subtitle "The following information needs to be provided to install the database". The main area contains two sections. The first is "Destination folder to install the database engine to:" followed by a text box containing "C:\Program Files\Microsoft SQL Server" and a "Browse..." button. The second is "Set database administrator password:" followed by a large text box. Inside this box, there is a checked checkbox labeled "Leave database administrator password". At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

Destination

The SecurusWeb install might need to reboot the PC depending on what was installed. This screen prompts for the password for the current user in order to automatically log back into the PC if a reboot is necessary.



**Password for User Account**  
Enter the password for the currently logged on user.

**Windows Operating System User Account Password**

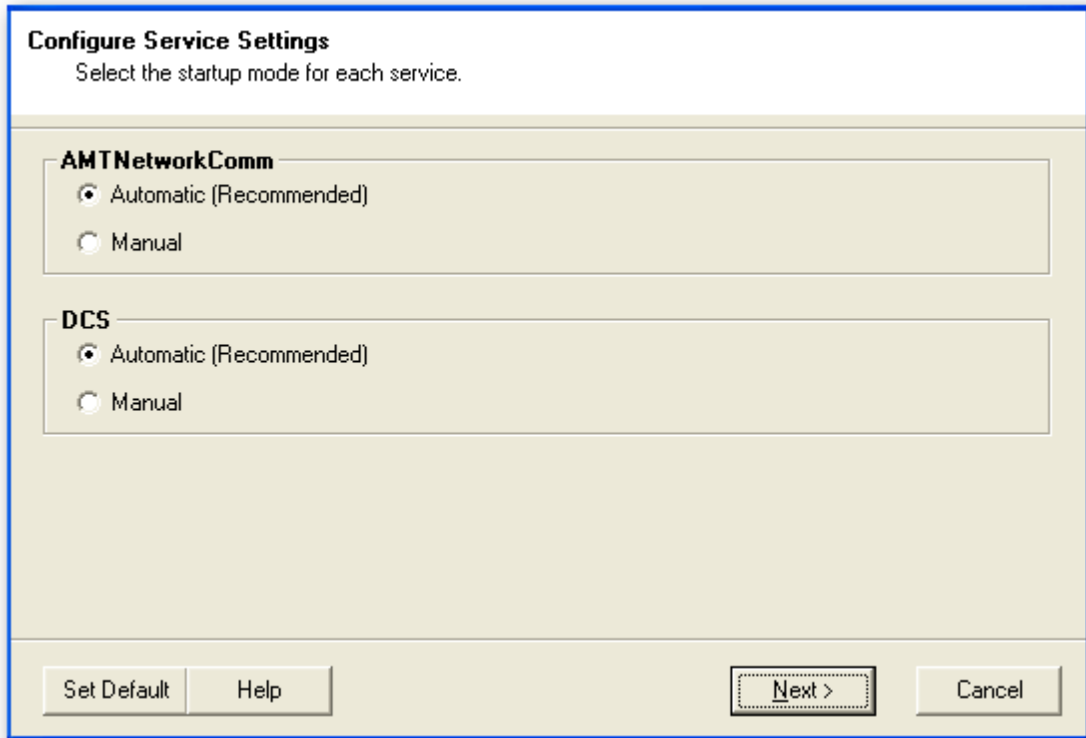
The installation wizard may need to reboot the machine one or more times during setup. If you want the installation wizard to automatically logon and continue the setup process after a reboot, please enter the password for the currently logged on user.

Password:

Confirm Password:

< Back   Next >   Cancel

The next screen is the “Configuration Editor”. This allows you to specify a user that the needed SecurusWeb services will run under. It’s recommended you keep the default “Automatic” setting. Click Next to continue.



**Configure Service Settings**  
Select the startup mode for each service.

**AMTNetworkComm**

☒ Automatic (Recommended)  
☐ Manual

**DCS**

☒ Automatic (Recommended)  
☐ Manual

Set Default    Help    **Next >**    Cancel

Enter the user who's authority the services will run under. This user needs to be an Administrator on the local machine. If your SecurusWeb system is spread across multiple machines, it's recommended this user be a domain user that's part of the Administrators group on all SecurusWeb machines. You'll then use the same user to run the services on all PC's.

**Configure Run As Settings**  
Select user under whose authority DCOM components and services will run.

**User Account for Run As**

User Account:  (Format: 'DOMAIN\Username')

Password:

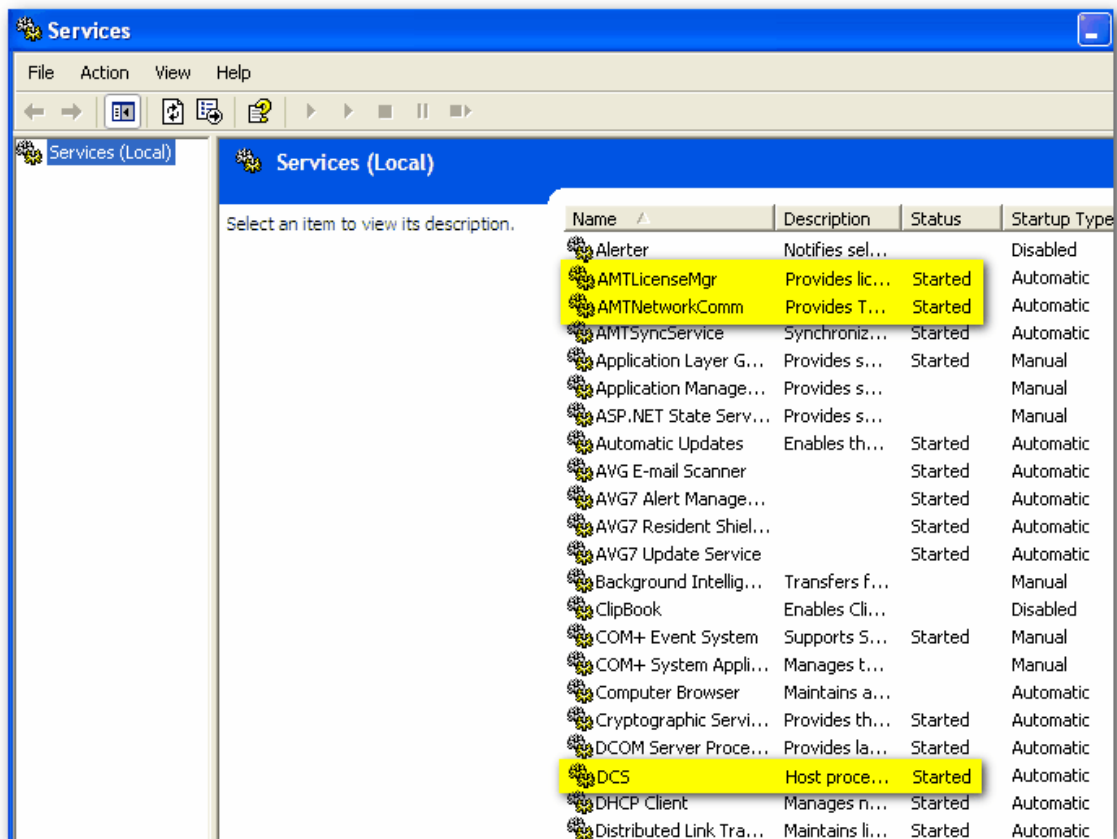
Re-enter Password:

NOTE: The account MUST have administrative authority on THIS machine (the account must be a member of the local administrators group).

The install will complete and will prompt you to reboot the computer. Congratulations, once rebooted, you're now ready to start working with SecurusWeb.

### 1.2.5 Post Install Checklist

After the SecurusWeb installation is completed and the PC has been rebooted, there should be 3 services running. To check this go to *Start>Settings>Control Panel>Administrative Tools>Services*.



Services

The Services window should show the AMTLicenseMgr, AMTNetworkComm and DCS services having the "Started" status (see figure Services). If your PC **isn't** a Hardware Server, the DCS service isn't necessary.

In addition to checking the services, checking the contents of the AMTErrorlog.txt file is recommended. Every time the PC is rebooted (or the AMTNetworkComm service is restarted), SecurusWeb will create a new error log. The default location of this log file is *C:\Documents and Settings\All Users\Application Data\SecurusWeb*.

## 1.3 Using SecurusWeb

The SecurusWeb application is made up of two separate sets of screens, or user interfaces.

- [Rich Client](#)
- [Web Client](#)

The functionality of the SecurusWeb system is similarly divided with the system setup provided via the Rich Client and the day-to-day operations of the SecurusWeb system provided through the Web

Client. This design allows all the complexity of the system set up and database management to be segregated from the screens that are most commonly used. It should be noted that certain functions such as reporting are available from both the Rich and Web client screens.

In addition to the Rich Client and the Web Client, there are numerous [Utilities](#) that add functionality to your SecurusWeb system.

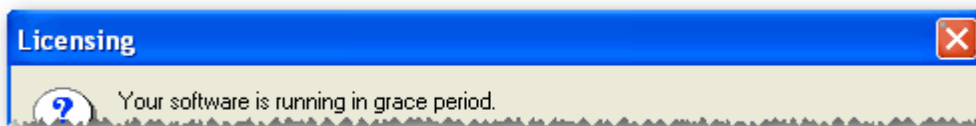
### 1.3.1 Rich Client

Start the SecurusWeb rich client by double clicking the desktop icon or browsing to *Start > Program Files > SecurusWeb*. The default login for SecurusWeb is Admin for the username and nothing for the password.(see figure Login) It's recommended this be changed to something more secure during system configuration.



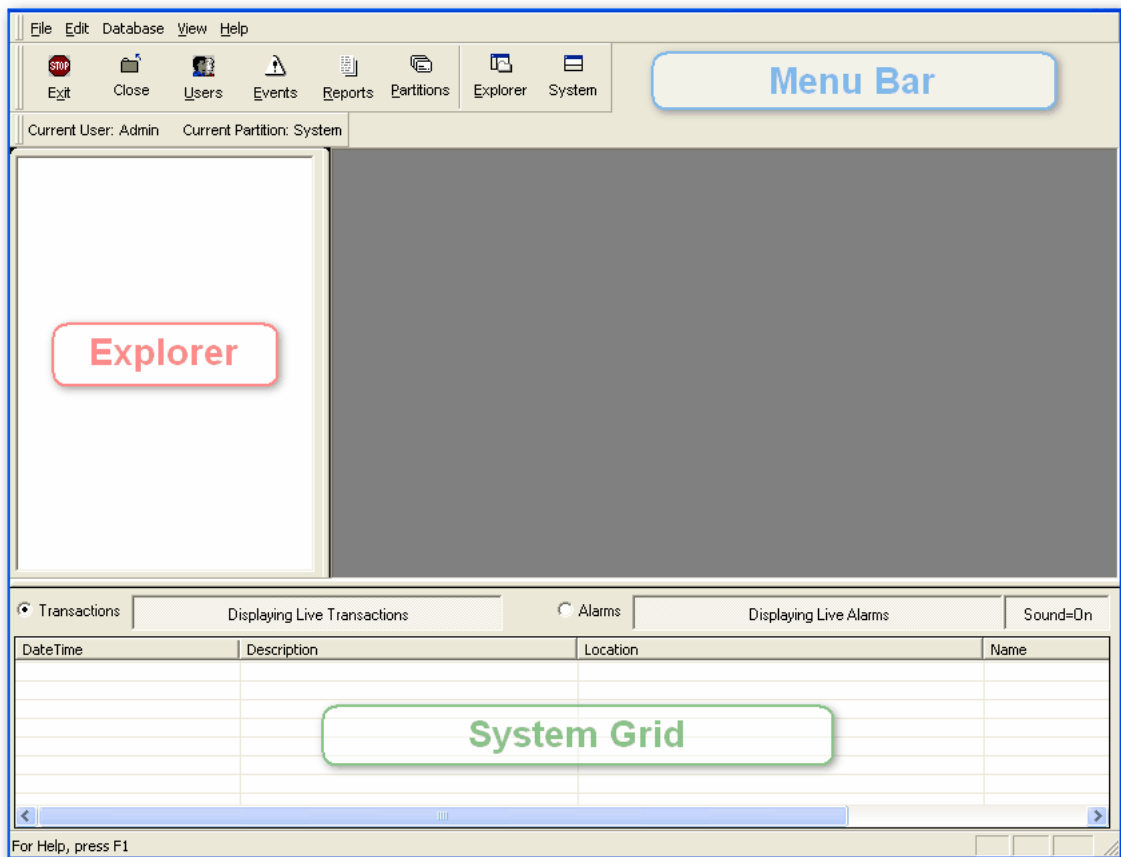
Login

If this is the first time logging in or SecurusWeb isn't yet licensed, you will see the Licensing screen. (see figure Licensing) SecurusWeb has a 14 grace period before it's required to be licensed. To learn more about licensing, see the [License Editor](#) section of this help. Click OK to continue.



Licensing

Once logged in, there are three main areas of the Rich Client user interface. These areas are the [Menu Bar](#), [Explorer](#) and [System Grid](#). (see figure Rich Client)



**Rich Client**

It's important to be familiar with the functions of each of these areas:

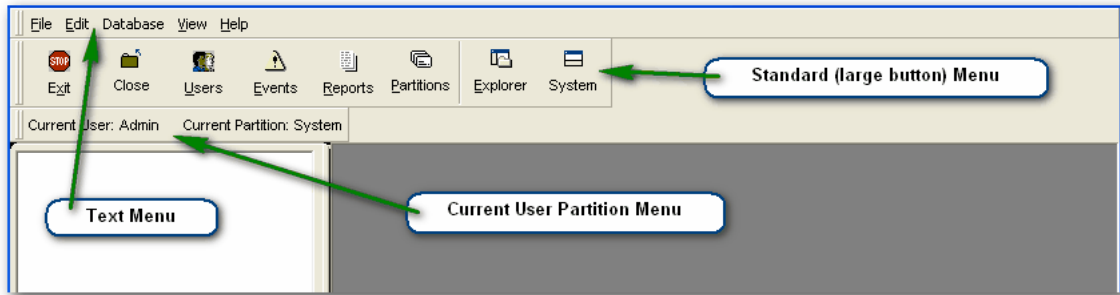
- Menu Bar - To start and close SecurusWeb utilities and navigate the Rich Client UI.
- Explorer - To view and command system hardware.
- System Grid - To view transactions and alarms.

### 1.3.1.1 Menu Bar

The Menu Bar has two main functions.

- To open/close Rich Client documents or SecurusWeb utilities.
- Navigate the Rich Client user interface.

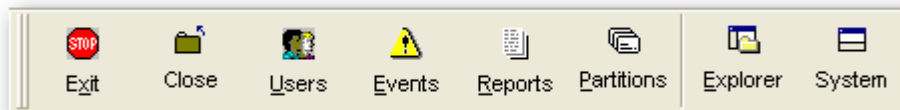
By default the Menu Bar will show 3 individual ribbons. (see figure Ribbons)



Ribbons

### Standard Menu

The Standard Menu is the most used menu. (see figure Standard Menu)



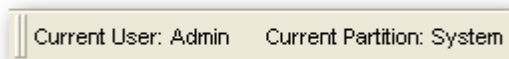
Standard Menu

Here's a list of the default icons and their function.

- **Exit** - Will exit the SecurusWeb Rich Client application.
- **Close** - Will close the top most Rich Client document.
- **Users** - Will open the Users (Admin Tools) document.
- **Events** - Will open the Events document.
- **Reports** - Will open the Report Generator document.
- **Partitions** - Will open the Partitions document.
- **Explorer** - Will show/hide the Explorer.
- **System** - Will show/hide the System Grid.

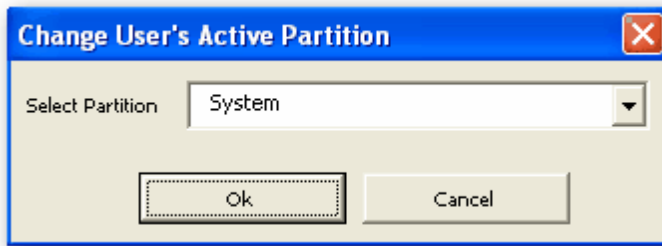
### Current User Partition Menu

The Current User Partition Menu will show general information about the logged in user and the current partition. (see figure Partition Menu)



Partition Menu

Current User is the user that's currently logged into SecurusWeb. Current Partition is the partition the Current User is working in. Clicking anywhere on the Current User Partition Menu will open the Change User's Active Partition screen. (see figure Active Partition)



Active Partition

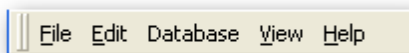
Use this screen to select which partition you'd like to administer.



*Only partitions the user has access to will appear in the list.*

### Text Menu

The Text Menu is the only menu ribbon that cannot be removed. (see figure Text Menu) That said, this ribbon can still be configured by adding or removing options.



Text Menu

Here are the default menu items and sub-items:

<u>F</u> ile	<u>E</u> dit	<u>D</u> atabase	<u>V</u> iew	<u>H</u> elp
<ul style="list-style-type: none"> <li>• New</li> <li>• Open</li> <li>• Close</li> <li>• Save</li> <li>• Save As</li> <li>• Database Maintenance</li> <li>• Data Archiving</li> <li>• Exit</li> </ul>	<ul style="list-style-type: none"> <li>• Design</li> </ul>	<ul style="list-style-type: none"> <li>• Change active Partition</li> <li>• Users</li> <li>• Events</li> <li>• Reports</li> <li>• Partitions</li> </ul>	<ul style="list-style-type: none"> <li>• Explorer</li> <li>• System Bar</li> <li>• Status Bar</li> <li>• Show IDE</li> </ul>	<ul style="list-style-type: none"> <li>• About</li> </ul>












### 1.3.1.2 Explorer

The Explorer has three main functions:

- Allows the adding or deleting of system hardware.
- Allows the ability to command system hardware.
- Graphically represents the state of system hardware.

Here's a list of all possible hardware. (see figure Hardware Icons)

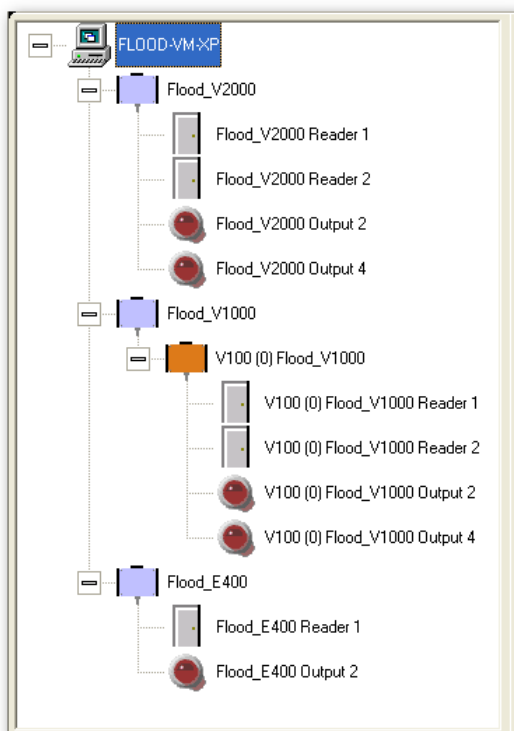


Hardware Type	Default Icon (normal state)	Description
Computer		The Computer object is the parent to all other object in the Explorer. You must first add a computer (Hardware Server) before any additional hardware can be discovered.
E400		The E400 or Edge controller is a child of the Computer. The E400 is a 1 Reader/1 Output controller.
V2000		The V2000 controller is a child of the Computer. The V2000 is a 2 Reader/2 Output controller.
V1000		The V1000 controller is a child of the Computer. This controller has no readers or outputs, but will have downstream devices attached to it (V100, V200 and V300).
V100		The V100 is a child of the V1000 and is a 2 Reader/2 Output panel.
V200		The V200 is a child of the V1000 and is a 16 input panel.
V300		The V300 is a child of the V1000 and is a 12 output.
Reader		The Reader is a child of the V2000, E400 or V100.
Output		The Output is a child of the V2000, E400, V100 and V300
Input		The Input is child of the V200 panel.
AHG420		The AHG420 lockset is a child of the Computer. The AHG420 lockset doesn't have any children.

#### Hardware Icons

The icons shown (see Hardware Icons) indicate the default or normal states of the hardware types. To modify the icons for the different hardware types and their states, right click on the object in the Explorer and select Properties and then select the Profiles tab.

This is a Explorer that is populated with a Computer, V2000, V1000 and E400. (see figure Explorer)



Explorer

### 1.3.1.2.1 Discovering VertX/Edge Hardware

In order to add hardware to the SecurusWeb system, the hardware server(s) must be added to the Explorer. To do this, right click in the Explorer and select New and then Computer. This will open the Computer Definition window. (see figure Computer Definition)

The 'Computer Definition' dialog box has a title bar with a close button. It contains three text input fields: 'Computer:' with 'FLOOD-VM-XP' and a 'Select...' button to its right; 'Remote Name:' with '\\FLOOD-VM-XP'; and 'Name:' with 'FLOOD-VM-XP'. At the bottom are 'OK' and 'Cancel' buttons.

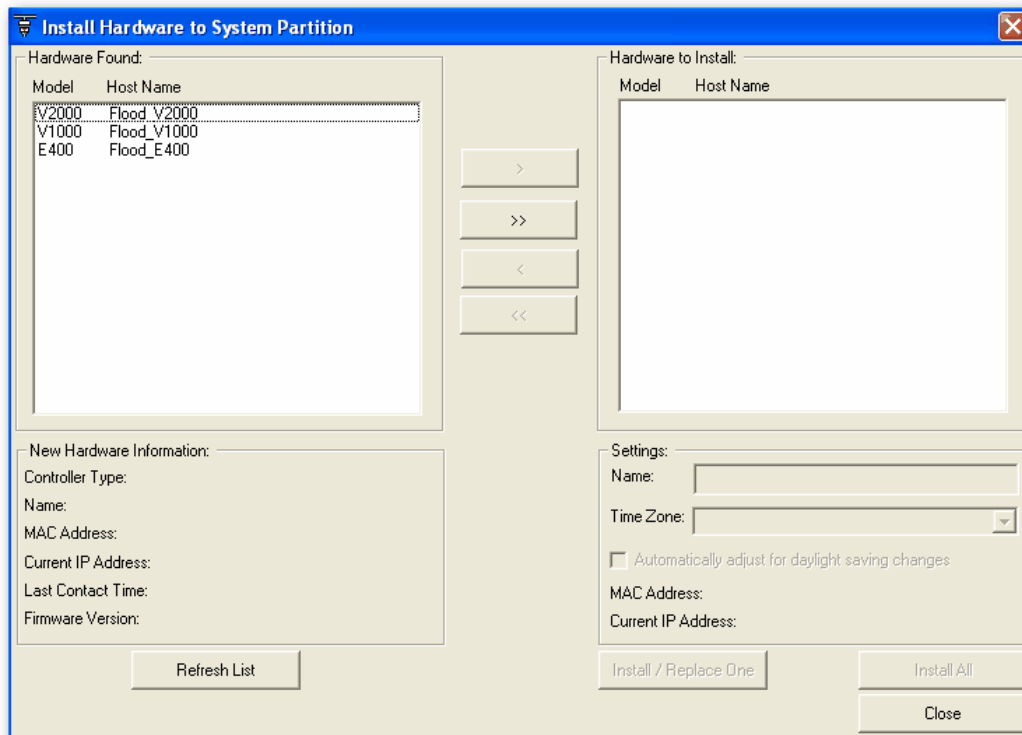
Computer Definition

When the Computer Definition window first opens, the defaults are for the local computer. If the local machine isn't the hardware server, click the Select button to select the hardware server to be added. Click OK to add the selected computer to the Explorer.



**The Name field is the text that will show in the Explorer as the Name of the computer.**

Once the hardware server computer has been added to the Explorer, hardware can be discovered or attached to it. To do this, right click the computer and select Discover New VertX Controllers. This will open the Install Hardware window. This window will show all VertX hardware that's available for discovery. (see figure Install Hardware)



**Install Hardware**

This window can be broke down into two sections; Hardware Found and Hardware to Install.

### Hardware Found

This section will lists all VertX controllers that the SecurusWeb system has found. In order for the SecurusWeb software to see the controller(s), the controller must be configure to point to the hardware server and the HereIAm value must be set to something other the zero. Clicking on the controllers in this list will show details below in the New Hardware Information section.

### Hardware to Install

This section list all VertX controllers ready to be installed. To place controllers in this section select them from the Hardware Found section and click the > button. Clicking the >> button will move all controllers from the Hardware Found section to the Hardware to Install section. Once the controller (s) are in the Hardware to Install section, clicking on them individually will allow changes to the controllers Name and Time Zone.



***The Time Zone of a controller cannot be changed after discovery without going directly to the database.***

Clicking the Install All button will start the discovery process for all controllers in the Hardware to Install section. Highlighting a specific controller and clicking the Install/Replace One button will

open a list of existing controllers. Use this option to replace a faulty controller without having to modify door groups and access privileges.

### 1.3.1.2.2 Commanding Hardware

Commands can be sent to most hardware objects in the Explorer. To issue commands, right click the hardware object in the Explorer and select the desired command. Here is a list of hardware object types and their available commands.

Object Type	Commands
<b>Computer</b>	No available commands.
<b>Controllers</b> (E400, V1000 or V2000)	<ul style="list-style-type: none"> <li>• <b>Refresh Cards Only</b> - Issues a Database Changeover which updates all the cards for the selected controller.</li> <li>• <b>Refresh Configuration and Reboot</b> - Issues a Database Changeover and resends all controller configuration data.</li> <li>• <b>Reboot</b> - Sends a reboot command to the controller</li> <li>• <b>Set Time</b> - Sends the current time to the controller based on the hardware server time and the GMT offset value.</li> <li>• <b>Query Status</b> - Queries the status of the controller and all attached devices.</li> <li>• <b>APB Forgive</b> - Resets ALL APB status's for this controller.</li> <li>• <b>Discover Downstream Devices</b> - Queries the controller for missing or newly added hardware.</li> </ul>
<b>Panels</b> (V100, V200 or V300)	<ul style="list-style-type: none"> <li>• <b>Reboot</b> - Sends a reboot command to the controller.</li> <li>• <b>Query Status</b> - Queries the status of the controller and all attached devices.</li> </ul>
<b>Readers</b>	<ul style="list-style-type: none"> <li>• <b>Grant Access</b> - Unlocks the door for the defined "Normal Access Time" value. (default is 6 seconds)</li> <li>• <b>Lock</b> - Locks the door indefinitely.</li> <li>• <b>Unlock</b> - Unlocks the door indefinitely.</li> </ul>
<b>Outputs</b>	<ul style="list-style-type: none"> <li>• <b>Activate</b> - Activate the output.</li> <li>• <b>Deactivate</b> - Deactivate the output.</li> </ul>
<b>Inputs</b>	No available commands.
<b>AHG420 Lockset</b>	<ul style="list-style-type: none"> <li>• Lock</li> <li>• Unlock</li> </ul>

In addition to the object specific commands, every Explorer object has the following commands available.

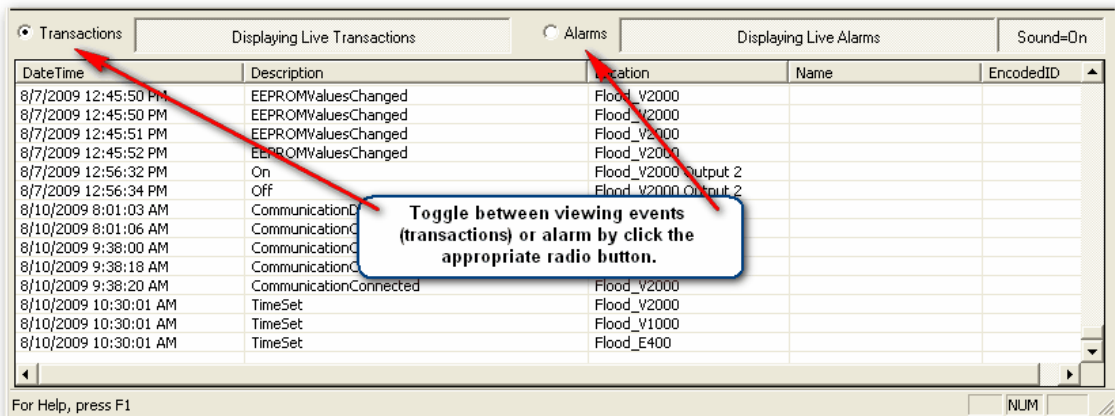
- **Cut** - This will copy the object to memory (clipboard) and remove it from the Explorer. You can then paste it to another location in the Explorer.
- **Copy** - This will copy the object to memory (clipboard) and leave it in the Explorer. You can the paste it to another location in the Explorer.
- **Paste** - This will paste a copied or cut object to a specific location in the Explorer.
- **Rename** - This will rename the selected object.
- **Delete** - This will delete the selected object. **USE WITH CAUTION**
- **Properties** - Will open the selected objects Properties window.



**If a hardware object is deleted by mistake or new hardware was added to a controller, issue a Discover Downstream Devices from the target controller to bring these hardware objects into the Explorer.**

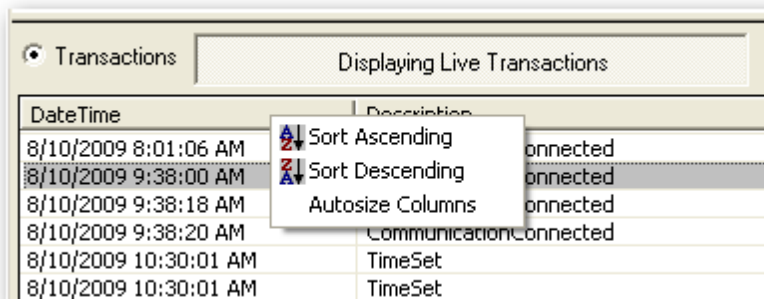
### 1.3.1.3 System Grid

The System Grid shows all defined transactions and alarms. To toggle between viewing transactions or alarms, click the appropriate radio button (see figure System Grid). To pause viewing live event/alarm, toggle the "Display Live Transactions" or "Display Live Alarms" buttons. The Sound button (upper right corner) will toggle the playing of a sound when a new alarm is logged.



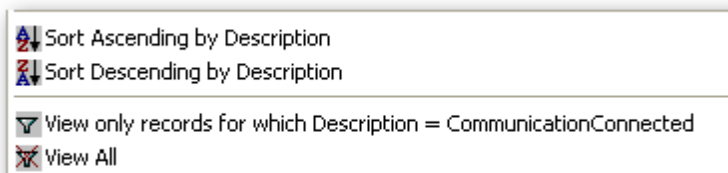
System Grid

When viewing transactions or alarms, right click any column header to view the sorting options for that column (see figure Sorting Options).



Sorting Options

Both transactions and alarms have 4 filtering options that can be viewed by right clicking a cell in the grid (see figure Filtering Options).



Filtering Options

When right clicking Alarms these addition options are available:

- **Acknowledge & Remove:** Will indicate the alarm has been acknowledged and will remove it from the grid.
- **Acknowledge Only:** Will indicate the alarm has been acknowledged and leave it in the grid.
- **Unacknowledge:** Will change an acknowledged alarm to unacknowledged.
- **Add Comment:** Will open of the User Comments window, allowing the user to add a comment to the selected alarm.
- **View Comment History:** Will show the comment history for the selected alarm.



*Acknowledged alarms will appear in **GREEN** and Unacknowledged alarms will appear in **RED**.*

### 1.3.1.4 Users

The Users document (also referred to as Admin Tools) is used to add, modify, delete or set permissions for SecurusWeb users and roles. The main SecurusWeb security settings are also configured using this document.

The Users document can be broke down into four separate areas:

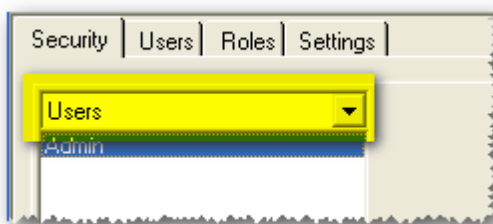
- [Security](#)
- [Users](#)
- [Roles](#)
- [Settings](#)



*When reviewing this section, the term "user" is referring to a user of the SecurusWeb application, NOT a card holder.*

#### 1.3.1.4.1 Security

The Security tab of the Users document (Admin Tools) is used to set the security permissions for users and roles. Selecting either Users or Roles from the drop down list (see figure Dropdown List) will populate the list below with all the available users or roles.



**Dropdown List**

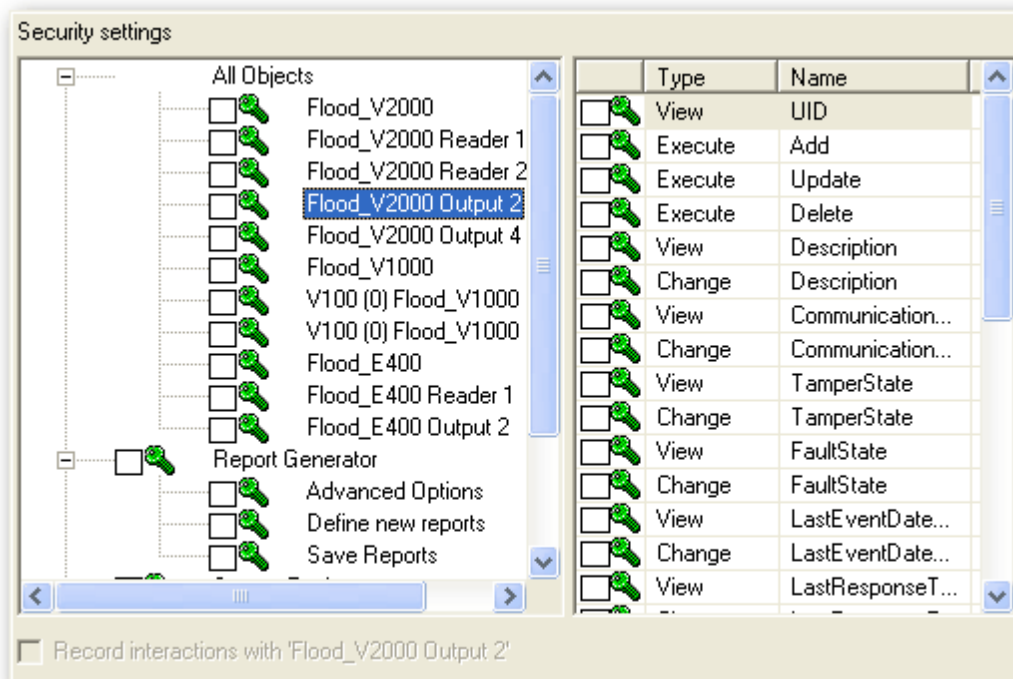
WebBrix installs with only one user, Admin. This default user belongs to the Administrators role. WebBrix also installs with five roles. These roles are Administrator, Data Entry, Guard, Headquarters Administrator and View Only. The only required role is Administrator. The other

default roles are placeholders for what a WebBrix system might have.



**Security cannot be modified for the Administrator role or any users that belong to the Administrator role. There must be at least one user that's a member of the Administrator role at all times.**

Selecting either User or Roles (see figure Dropdown List) and selecting a User that isn't part of the Administrator role or a role other than Administrator will expose the Security Setting for that entity. (see figure Security Settings)



**Security Settings**

The Security Setting section will show all the securable entities and the current security setting based on the selected user or role. Highlighting an entity in the tree view (left side) will populate the property list (right side) with all securable properties for that entity. The icons by each entity and property indicate what permissions the selected user or role has for that object. A icon outside of the box indicates the security for this object has been inherited. A icon inside the box indicates the security for this object as been set individually or not inherited. The order of security inheritance, starting at the top, is the security default, roles and finally users. In other words, all roles inherit the security default and all users inherit their security from there role. If a user hasn't been assigned a role they inherit the security default.



**The WebBrix security default can be found in the settings tab of the User (Admin Tools) document.**

Unchecking the "Advanced" checkbox will hide the selected entities properties. This is often times desired when security is only needed at high level.

Here's a list of possible icons:

- **Green Key** - Admin
- **Red X** - Denied
- **Green Check** - Granted

### 1.3.1.4.2 Users

The Users tab of the Users document (Admin Tools) is used to add, modify or delete users. The Users tab has three core sections. (see figure Users Tab).

The screenshot displays the 'Users Tab' interface. On the left, a list titled '2 Users Listed' contains 'Admin' and 'rflood', with 'rflood' selected. The main area is divided into three tabs: 'Details' (active), 'Roles', and 'Projects'. The 'Details' tab shows fields for 'First Name' (Rick), 'Middle', 'Last' (Flood), 'Description' (Sys. Admin), 'Activation Date' (8/13/2009), 'Expiration Date' (8/13/2009), 'Password', 'Confirm', 'Last Modified' (8/13/2009 8:36:28 AM), and 'Modified By' (Admin). There are also checkboxes for 'Account Locked Out', 'Disable Account', 'User Must Change password at next login', 'Password Never Expires', and 'Never Lockout Account'. At the bottom left are 'Add User' and 'Delete User' buttons. At the bottom right are 'Save' and 'Close' buttons.

**Users Tab**

#### Details Tab

The Details tab contains basic user information.

#### Roles Tab

The Roles tab contains two lists of roles, Available Roles (right side) and Assigned Roles (left side). To assign a role to the selected user, highlight the role in the All Available Roles list and move it to the Assigned Roles list.

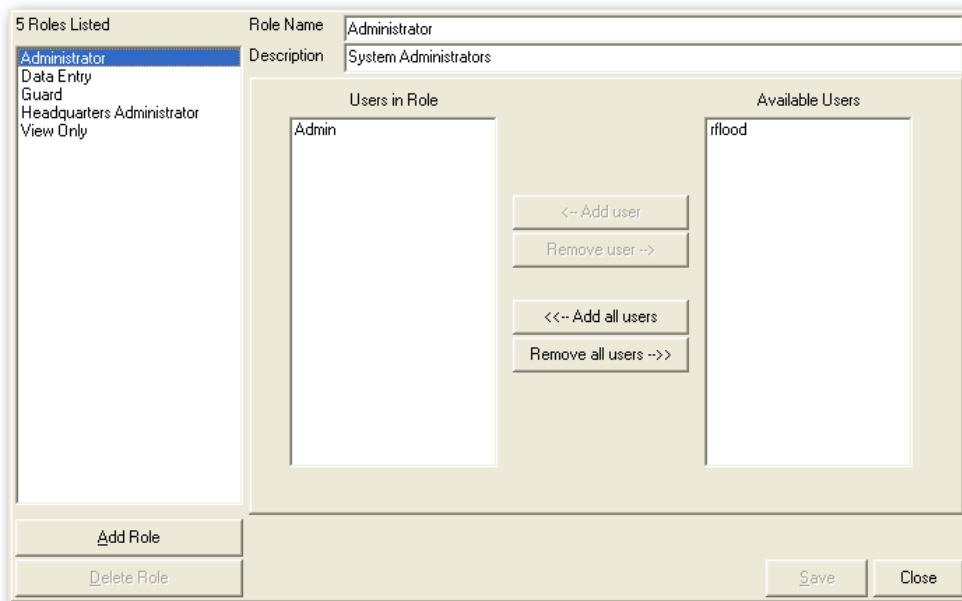
#### Projects Tab

The Projects tab contains three drop down lists that assign certain project to the selected user.



### 1.3.1.4.3 Roles

The Roles tab of the Users document (Admin Tools) is used to assign users to roles. Users can be assigned multiple roles. Use the Add and Remove buttons to assign users to the selected role. (see figure Roles Tab)



Roles Tab

Use the Add Role and Delete Role buttons to add or delete roles from the SecurusWeb system.



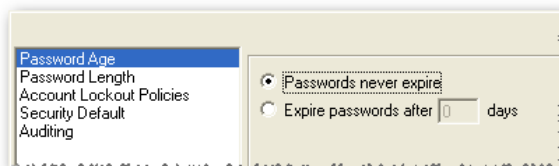
**When assigned a user to multiple roles, the most secure setting will apply. In other words, if John was assigned the Data Entry role and the Guard role and the Data Entry role denied the view of all hardware and the Guard role granted viewing of all hardware, John would not be able to view hardware because that's the most secure option.**

### 1.3.1.4.4 Settings

The Setting tab of the Users document (Admin Tools) is used to set overall SecurusWeb security and policies.

#### Password Age

The Password Age setting can either be set to never expire or expire after X amount of days. (see figure Password Age)

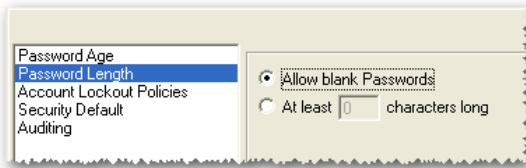


Password Age

#### Password Length

The Password Length setting can allow blank passwords or require a password be X characters in

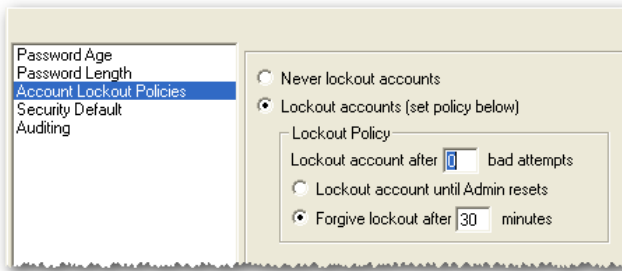
length. (see figure Password Length)



**Password Length**

### Account Lockout Policies

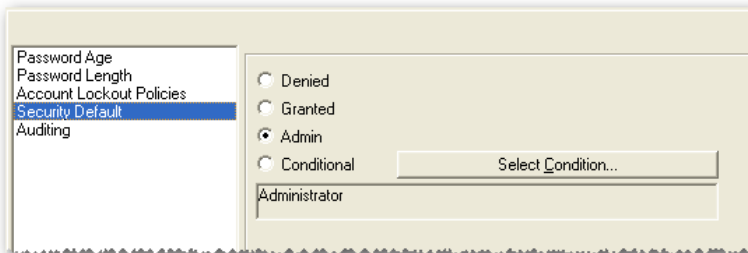
The Account Lockout Policies setting can be set to never lockout accounts or lockout accounts based on the defined policy. (see figure Account Lockout)



**Account Lockout**

### Security Defaults

The Security Defaults setting will configure the overall SecurusWeb security default. (see figure Security Defaults)



**Security Defaults**



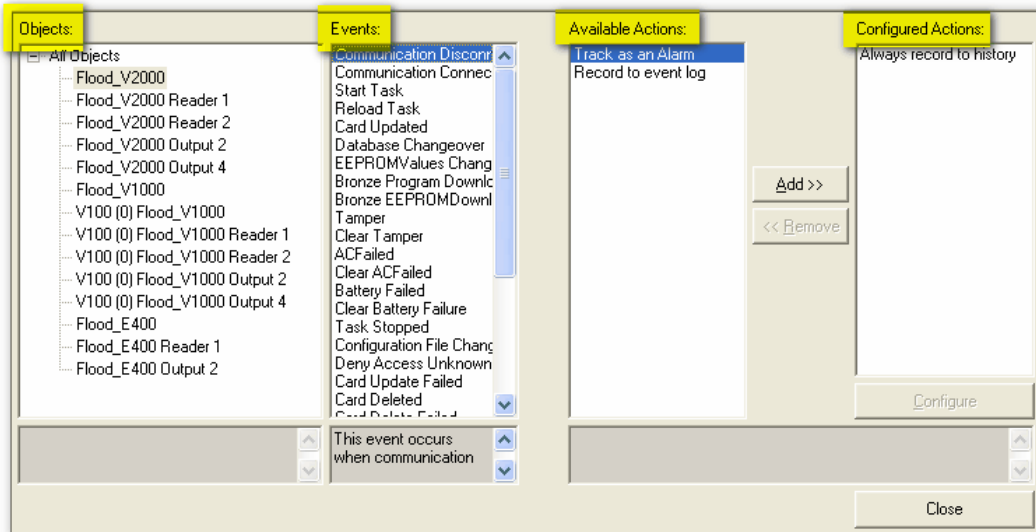
*If there are users or roles that inherit from the security default, changing this setting will effect those entities.*

### Auditing

The Auditing setting can enable or disable System Auditing. Auditing is enabled by default.

### 1.3.1.5 Events

The Events document is used to create, modify or delete either events (transactions) or alarms. This document contains four lists. (see figure Event Configuration)



Event Configuration

#### Objects

The Objects list contains all the objects in the Explorer that can produce events.

#### Events

The Events list contains all the events for the selected object in the Object list.

#### Available Actions

The Available Actions list contains all actions that can be applied to an event. The two actions that come with SecurusWeb are "Track as an Alarm" and "Record to event Log". To assign an action to the selected event, highlight the desired action and click the Add button.



**By default, all events for all objects are set to use the "Record to event log" action. In other words, all events will be recorded to history.**

#### Configured Actions

The Configured Actions list contains all the configured actions for the selected object and event. It is possible to have multiple configured actions, but not of the same type. To configure a configured action, select the desired configured action and click the Configure button. To remove an action, highlight the action and click the Remove button.

### 1.3.1.5.1 Configuring an Event

When configuring an event, there are 3 options. (see figure Event Logging)

**Event Logging**

- Always (default): Will always track this event to history.
- Never (disable): Will never track this event to history.
- Only when the following condition is TRUE: **Not implemented in this version of SecurusWeb**

### 1.3.1.5.2 Configuring an Alarm

When configuring alarms, there are three main areas. (see figure Configuring an Alarm) These areas are Alarm Info, Routing and Actions.

**Configuring an Alarm**

#### Alarm Info

- **When** - Specifies when the event should be an alarm. The choices are always, never or when a condition is true. Remember, conditions aren't used in this version of SecurusWeb so the only 2 valid choices here are always or never.
- **Settings** - Specifies if a user comment is requested, required or both. This will occur when the user acknowledges the alarm.
- **Priority** - Specifies the priority of the alarm. The range is from 1 to 99.

- **Multiple Occurrences** - Specifies if the alarm will update the existing alarm by incrementing the count field or log a completely separate alarm.

**Routing** (see figure Alarm Routing)

This tab configures which user, roles or PC's the alarm will be routed to.

Alarm Info | Routing | Actions

☒ Route to all Users on all Computers

☐ Route to all Users in Role:

☐ Route as follows:

Route destinations:

Add Delete

When:

☐ Always

☐ Never (disable)

☐ After   if not acknowledged.

☐ When this condition is TRUE:  Select...

Save Close

**Alarm Routing**

There are three routing options.

- **Route to all Users on all Computers** - Will route the alarm to all users on every SecurusWeb computer.
- **Route to all Users in a Role** - Will route the alarm to all users in the selected role.
- **Route as follows** - Enables the Route Destination and When sections. (see figure Routing Destination)

Alarm Info | Routing | Actions

☐ Route to all Users on all Computers

☐ Route to all Users in Role:

☒ Route as follows:

Route destinations:

- Admin (User)
- FLOOD-VM-XP (Computer)

When

☐ Always

☐ Never (disable)

☒ After 5 Minutes if not acknowledged.

☐ When this condition is TRUE:  Select...

Add Delete

Save Close

### Routing Destination

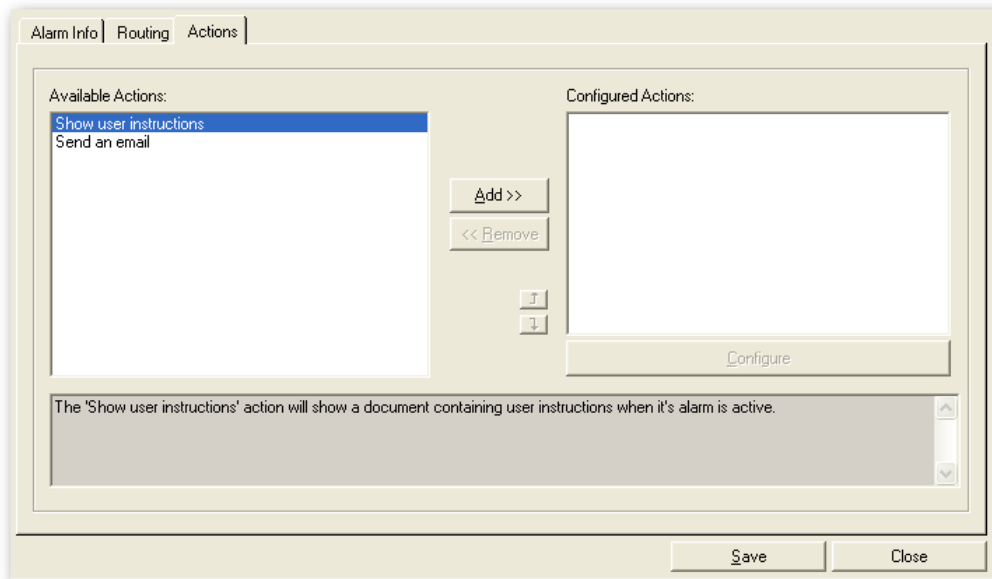
The Route Destination list can contain any combination of Users and/or Computers. To add or delete users or computers to this list use the Add or Delete buttons.

The "When" section specifies when the alarm will be routed. Each entry in the Route Destination list has its own "When" settings. The available settings are always, never or after X minutes/hours/days if not acknowledged. The option "When this condition is TRUE" isn't enabled in this version of SecurusWeb.

In this example (see figure Routing Destination), the alarm will be routed to the Admin user if the alarm isn't acknowledged within 5 minutes.

### Actions (see figure Alarm Actions)

The Action tab allows will allow the assignment of actions to an alarm.



**Alarm Action**

The two available actions are:

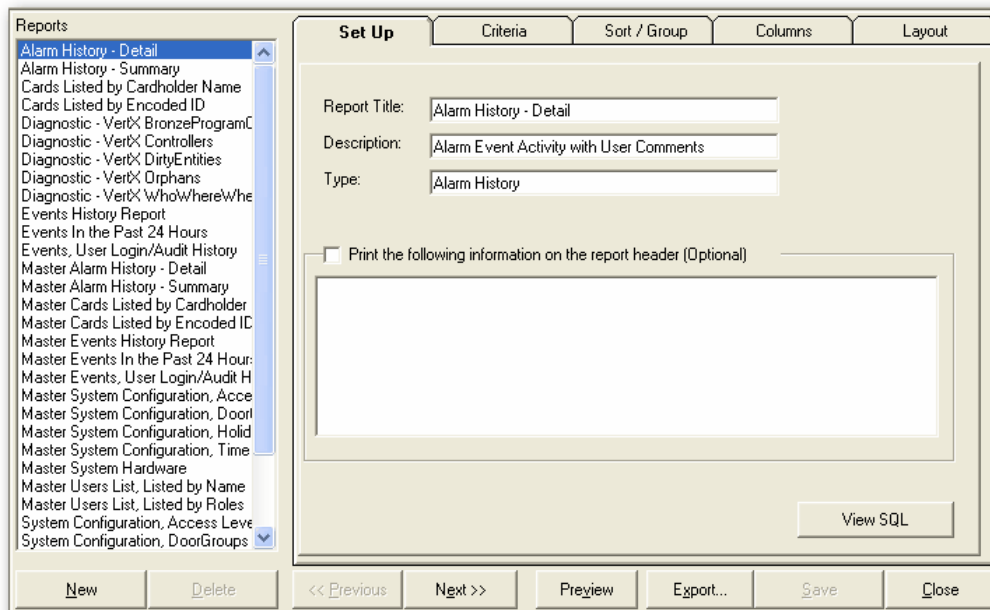
- **Show User Instructions** - Will show text instructions when an alarm occurs.
- **Send an Email** - Will send an email when an alarm occurs.



**Using the "Send an Email" action requires the setup of an SMTP server. Use the Email Action Configuration utility to set this up prior to adding an email action to an alarm.**

### 1.3.1.6 Reports

The Reports document is used to create, modify or delete reports. This document will list all the default reports and separate the selected report properties into five, tabbed categories. (see figure Reports)



**Reports**

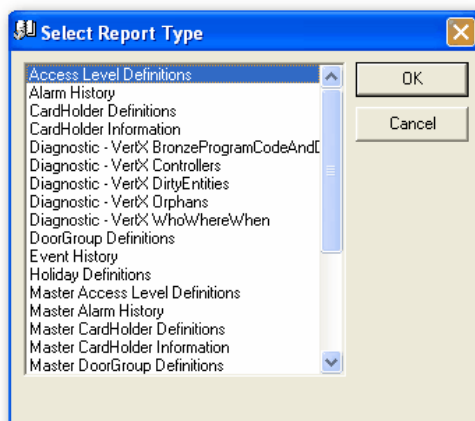
Use the New and Delete buttons to add or remove reports from the SecurusWeb system. Use the Preview button to preview the selected report in PDF format. Use the Export button to save the selected report to a specific format. The available formats are PDF, RFT, TXT, XLS and HTML.



**None of the default reports can be deleted.**

#### Creating a new report

Clicking the New button will open the Select Report Type window. (see figure New Report)



**New Report**



Select the report type the new report will be based on and click the OK button. Use the tabs to configure the properties of the newly created report and click the Save button when done.

### 1.3.1.6.1 Setup Tab

The Setup tab allows configuration of the reports title and description. The type property is a read only value that represents the report type this report was derived from. (see figure Setup Tab)

The screenshot shows a window titled "Setup Tab" with five tabs: "Set Up", "Criteria", "Sort / Group", "Columns", and "Layout". The "Set Up" tab is active. It contains three text input fields: "Report Title:" with the value "Alarm History - Detail", "Description:" with the value "Alarm Event Activity with User Comments", and "Type:" with the value "Alarm History". Below these fields is a checkbox labeled "Print the following information on the report header (Optional)" which is checked. Under the checkbox is a large empty text box. At the bottom right of the window is a button labeled "View SQL".

**Setup Tab**

If the "Print the following information on the report header" checkbox is checked, the text in the below text box will be placed in the header of the report.

To view the SQL statement used to generate the selected report, click the View SQL button.

### 1.3.1.6.2 Criteria Tab

The Criteria tab is used to filter the selected report. Reports can be filtered by dates and/or objects. (see figure Criteria Tab)

**Criteria Tab**

The available date options are as follows:

- **All Dates** - This will NOT apply any date filtering to the selected report.
- **Select Date Range** - This will apply a configurable start and end date to the report.
- **Previous Period** - This will apply a predefined date range to the selected report. The available periods are previous hour, day, week, month, quarter or year.

Reports can also be filtered on up to three of any of the visible columns. Visible columns are configured using the Columns tab of this screen. When filtering on specific report data, select the data to be reported on. Anything that isn't checked will NOT show in the report. If nothing is checked for a specific column, the report will include all the data for that criteria.

### 1.3.1.6.3 Sort/Group Tab

The Sort/Group tab is used to sort and/or group the selected report. You can group and/or sort on up to three of any of the visible columns in the selected report. (see figure Sort/Group)

The screenshot shows the 'Sort / Group' tab selected in a window with tabs: Set Up, Criteria, Sort / Group, Columns, and Layout. The 'Group By:' section has three columns. The first column has a dropdown set to 'EncodedID', with radio buttons for 'Ascending Order' (selected) and 'Descending Order', and checkboxes for 'Lines', 'Totals', 'Indent', 'Large', 'Bold', and 'Italic'. The second and third columns have dropdowns set to '<None>' and no other options. The 'Sort Report By:' section also has three columns. The first column has a dropdown set to 'DateTime', with radio buttons for 'Ascending Order' (selected) and 'Descending Order'. The second and third columns have dropdowns set to '<None>' and no other options.

**Sort/Group**

### 1.3.1.6.4 Columns Tab

The Columns tab is used to set which of the available columns are visible in the selected report. (see figure Columns Tab)

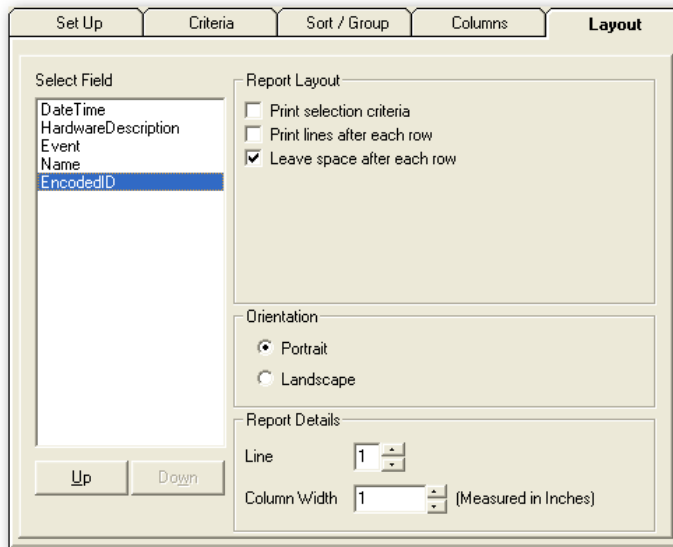
The screenshot shows the 'Columns' tab selected in a window with tabs: Set Up, Criteria, Sort / Group, Columns, and Layout. The 'Available Columns' list on the left contains 'PartitionID'. The 'Columns on Report' list on the right contains 'DateTime', 'HardwareDescription', 'Event', 'Name', and 'EncodedID'. Between the two lists are two buttons: 'Add >>' and '<< Remove'.

**Columns Tab**

To add or remove report columns, use the Add>> and <<Remove buttons.

### 1.3.1.6.5 Layout Tab

The Layout tab is used to configure the layout and appearance of the selected report. (see figure Layout Tab)



**Layout Tab**

The Select Field box will list all of the columns in the report and the order they will appear. To change the order, use the Up or Down buttons.

The Report Layout and Orientation sections contain general configuration options. The Report Details section defines what line and width the selected field will be placed on in the report.

### 1.3.1.7 Partitions

The Partition document is used to create, edit or delete partitions (see figure Partitions Document). Partitions are ultimately a set of rules that define visibility. In other words, partitions define which users can see what information. This is accomplished by following a two step process; first sharing, then consuming.

The screenshot shows a window titled "Partitions Document". On the left is a list box labeled "Partitions:" containing the items "System", "two", "three", and "four". "System" is selected. To the right of the list box are three tabs: "Name & Description" (active), "Items available to other Partitions", and "Items shared from other Partitions". Under the "Name & Description" tab, there are two text input fields: "Partition Name:" with the value "System" and "Partition Description:" with the value "System Partition". At the bottom of the window are five buttons: "New", "Delete", "Edit Administrators", "Save", and "Cancel".

**Partitions Document**

The Partitions box will contain all the partitions that are available to the logged in user.

To add or delete a partition, use the New and Delete buttons located underneath the partitions box. When creating a new partition, the Partition Name field is required. When saving a new partition, the Partition Administrator screen will appear (see figure Partition Administrator). An administrator is needed for every partition in the SecurusWeb system.

The screenshot shows a window titled "Creating an Administrator for the new partition". It contains a message: "A new partition needs at least one user. This user is needed to add other users and to modify partition settings. Please fill in the fields below for this new user." Below the message is a section titled "Partition Administrator" containing several text input fields: "Login Name", "First Name", "Middle Initial", "Last Name", "Description", "Password", and "Confirm". At the bottom of this section is a checkbox labeled "User must change password at next login". At the bottom right of the window are "OK" and "Cancel" buttons.

**Partition Administrator**

The only required field for a new partition administrator is the Login Name. To require the partition administrator to change their password the next time they log in, check the box at the bottom of the screen (see figure Partition Administrator).



*The login name must be unique system wide. In other words, no two partitions can have a username that is the same.*

Clicking on the Edit Administrators button will open the Partition Administrators window. This window will show all Administrator users that are not owned by the System partition and which partitions that user has Administrative access to. To add or remove partitions the selected user can administer, use the Make Admin and Remove Admin buttons (see figure Administrator Configuration).

**Partition Administrators**

This form shows how Users who are Administrators can access specific Partitions. Users who are not Administrators or who are owned by the System Partition are not listed below. Administrators who are owned by the System Partition always have access to all partitions and cannot be restricted.

Users

- dlarson
- glarson
- rflood**

Partitions Administered by User rflood

- two

Partitions User does not Administer

- four
- three

Make Admin >>

<< Remove Admin

Save Close

**Administrator Configuration**

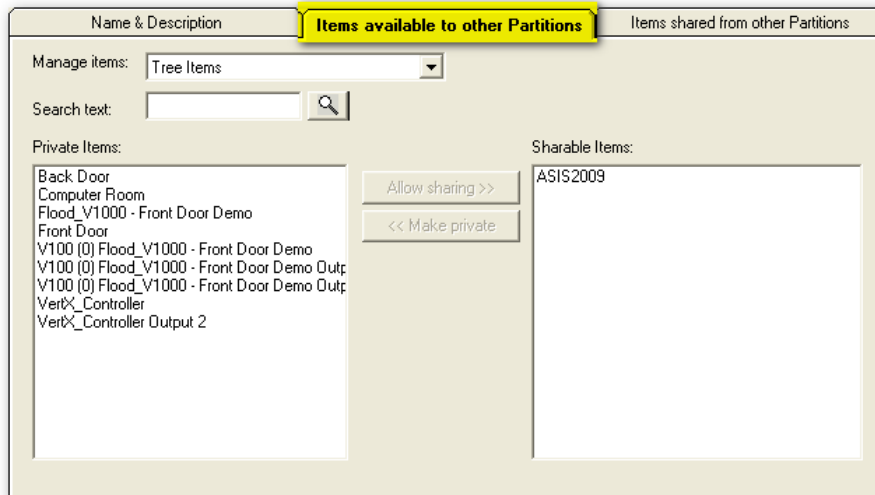
Again, partitioning can be broke down into two processes.

- **Sharing** - The owning partition of an object must share or expose that object before any other partition can consume it.
- **Consume** - A partition must consume a shared object before it can become functional within that

partition.

### Sharing

To share an object from the owning partition (the partition that object was created in), use the "Items available to the other Partitions" tab (see figure Partition Sharing).



Partition Sharing

Select the object type from the Manage Items dropdown list. If the object type contains a large number of objects, use the Search Text field to find a specific object by name.

To share an object, highlight the object in the Private Items list and click the Allow Sharing button to move it to the Shareable Items list. To make a shared object private, highlight the object in Shareable Items list and click the Make Private button to move it to the Private Items list.



**Tree Item objects are dependant on their parent. In other words, sharing an Edge controller without sharing the Computer it's attached to will not allow Edge controller to be seen in the consuming partition. You must share and consume the Parent object to view a Child Tree Item object.**

### Consuming

To consume an shared object, use the "Items Shared from other Partitions" tab (see figure Partition Consuming).

**Partition Consuming**

Select the object type from the Manage Items dropdown list. If the object type contains a large number of objects, use the Search Text field to find a specific object by name. To only see shared objects from a specific partition, use the Share Items From dropdown to choose a specific partition.

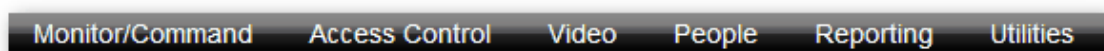
To consume an object, highlight the object in the Shareable Items list and click the Share button to move it to the Shared Items list. To remove a consumed object, highlight the object in the Shared Items list and click the Don't Share button to move it to the Shareable Items list.

Click the Save button to save any changes to the partition.

### 1.3.2 Web Client

To open the Web Client double click the desktop icon or navigate to *Start > Program Files > SecurusWeb*. The default username is Admin and the password is nothing (blank). It's recommended this be changed to something more secure during system configuration.

The web client menu bar can be divided into 6 main sections or tabs (See Figure 1).

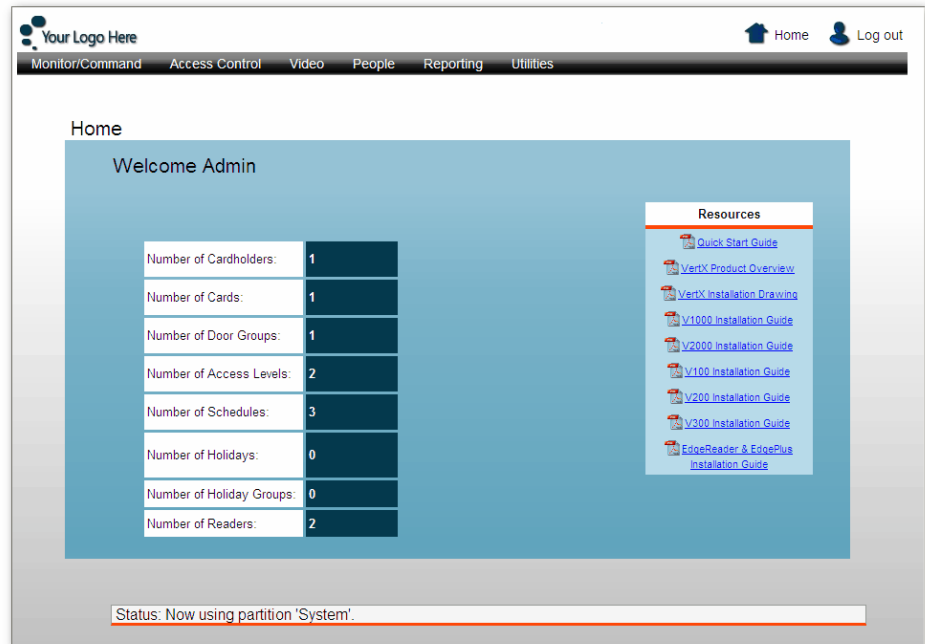


**Figure 1**

Each of these tabs contains sub topics. Here is a list of all the tabs:



- [Monitor/Command](#)
- [Access Control](#)
- [Video](#)
- [People](#)
- [Reporting](#)
- [Utilities](#)



Home Screen

In addition to the tabs and their sub topics, there are also two links in the upper right hand corner, Home and Log Out (See Figure 2).



Figure 2

There is also a status bar on the bottom of the screen.

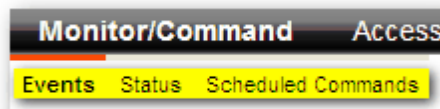


**The SecurusWeb system is licensed for a certain amount of Clients. Once logged into SecurusWeb through a browser, a Client license is being used. If you fail to log out before shutting the browser down, the used Client license will remain in use until the IIS timeout period has expired. The default timeout period in IIS is 20 minutes.**

### 1.3.2.1 Monitor/Command

The Monitor/Command tab contains the following menu items:

- [Events](#)
- [Status](#)
- [Scheduled Commands](#)



### 1.3.2.1.1 Events

The Events screen will show live events or alarms. To toggle between events and alarms, click the "View Event History" or "View Active Alarms" tabs.

Clicking the arrows on the bottom of the screen placed the window in Pause mode and allows the navigation of past events. To return to Live mode, click the "View Event History" or "View Active Alarms" tab.

Events and Alarms: Live View

View Event History View Active Alarms

Date/Time	Description	Location	Name	EncodedID
11/12/2009 2:50:06 PM	ReloadTask Access Task	Flood_V1000		
11/12/2009 2:50:04 PM	StartTask Identification Task	Flood_V1000		
11/12/2009 2:50:04 PM	ReloadTask Identity Task	Flood_V1000		
11/12/2009 2:50:02 PM	DatabaseChangeover	Flood_V1000		
11/12/2009 2:49:51 PM	StartTask RS485 Task	Flood_V1000		
11/12/2009 2:49:54 PM	ReloadTask RS485 chain 1 Task	Flood_V1000		
11/12/2009 2:49:51 PM	StartTask Access Task	Flood_V1000		
11/12/2009 2:49:49 PM	ReloadTask RS485 chain 0 Task	Flood_V1000		
11/12/2009 2:49:46 PM	StartTask RS485 Task	Flood_V1000		
11/12/2009 2:48:15 PM	Off	V100 (0) Flood_V1000 Output 2		
11/12/2009 2:48:10 PM	On	V100 (0) Flood_V1000 Output 2		
11/12/2009 2:30:00 PM	TimeSet	Flood_V1000		
11/12/2009 1:54:55 PM	CommunicationConnected	Flood_V1000		
11/12/2009 1:30:00 PM	TimeSet	Flood_V1000		
11/12/2009 12:30:00 PM	TimeSet	Flood_V1000		

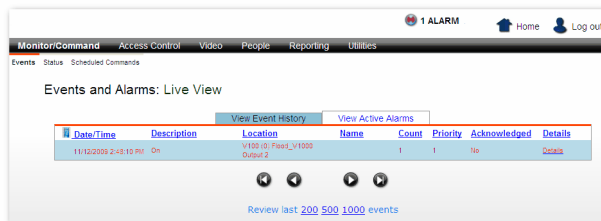
Review last [200](#) [500](#) [1000](#) events

Event History Screen

To review the last 200, 500 or 1000 events, click the appropriate link at the bottom of the screen. This will open a new browser window.

The events/alarms are sorted by Date/Time ascending. To change what column the events are sorted by, or to toggle between ascending and descending, click the column header. Doing this will place the window in pause mode. To return to Live mode, click either of the tabs or the "Resume Live Mode" link. Once back in Live mode, the default sorting of Date/Time ascending will be reapplied.

Entries in the Name and Encoded ID columns show as links and will allow navigation to a card holder or card. This is useful when adding cards.



Active Alarm Screen

The Active Alarms screen shows all active alarms. An alarm icon to the left of the Home icon or a red highlighted event (see Event History Screen) indicate there's an active alarm.

The alarms follow the same pausing, navigation and sorting rules that the events do.

A red alarm indicates the alarm is an Unacknowledged alarm or new. A green alarm indicates the alarm has been Acknowledged.

An alarm will stay in the grid as long as it has not been Acknowledged & Removed.

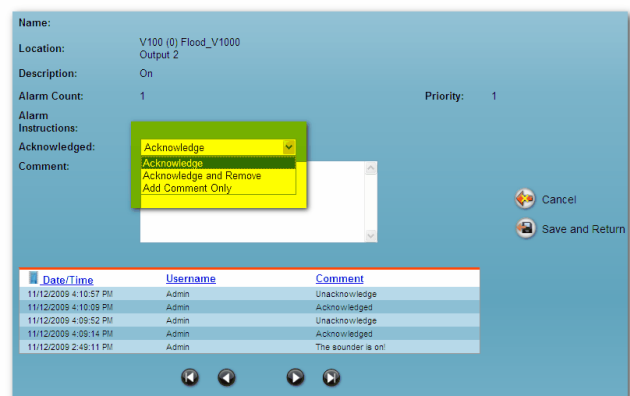
Clicking on "Details" for any alarm will display that alarm's detail page. This screen will contain details about the alarm including user comment history.

There are 4 possible actions for every alarm:

- Unacknowledge - Only possible for previously Acknowledged alarms.
- Acknowledge - Only possible for Unacknowledged alarms.
- Acknowledge and Remove - Will remove the alarm from the active alarm list.
- Add Comment Only - Will only add the text in the comments section to the alarm.

Click the arrows to navigate the user comments.

Click Save and Return to save any changes and return to the Active Alarm Screen.



Alarm Details

### 1.3.2.1.2 Status

The Status screen will list all the hardware objects for the current partition (See Figure Status Screen).

**Status and Command**

Find Name

Name	Status	Command	Command	Command
Flood_V1000 - Front Door Demo	Comm: Connected	Set Time	APB Forgive	
V100 (0) Flood_V1000 - Front Door Demo Output 2	Inactive	Activate	Deactivate	
V100 (0) Flood_V1000 - Front Door Demo Output 4	Inactive	Activate	Deactivate	
V100 (0) Flood_V1000 - Front Door Demo Reader 1	Locked	Grant Access	Lock	Unlock
V100 (0) Flood_V1000 - Front Door Demo Reader 2	Locked	Grant Access	Lock	Unlock
V100 (0) Flood_V1000 - Front Door Demo	AC: Normal - Battery: Normal			

Status:

**Status Screen**

This screen will update or refresh every 5 seconds (default) in order to update the hardware status.



**To change the refresh rate of the Status Screen, modify the registry value at HKLM\Software\AMT\Settings\HWStatusGridRefreshInterval.**

The text in the Status column indicates the current state of the hardware object. It's worth noting that unlike the rich client, the icons will NOT change to represent the hardware state.

The command columns contain the available commands for the hardware objects.

On larger systems or systems with many hardware objects, use the search box, navigation arrows or rolodex tab to locate specific hardware objects.

To configure the properties of hardware objects, click on the object name. For all practical purposes, the reader object is likely the only object you'll need to configure. See [Reader Configuration](#) for more information about how to configure the reader object.

### 1.3.2.1.2.1 Reader Configuration

The Reader Configuration screen is used to set the properties and behavior of the selected reader (See Figure Reader Configuration).

The screenshot shows the 'Reader Configuration' interface. At the top, the 'Status' is 'Locked'. The 'Reader Type' is set to 'Wiegand'. Below this are fields for 'Normal Access Time' (6), 'Extended Access Time' (20), and 'Door Held Time' (38). The 'Door Contact Line Supervision' is set to '<None>'. The 'Door Contact Normal Position' is 'Contact closed when door closed (recommended)'. The 'Door Contact Debounce Time' is 96. The 'REX Action' is 'Shunts alarm and unlocks the door (typical for mag locks)'. The 'REX Shunt/Unlock Time' is 6. The 'REX Line Supervision' is '<None>'. The 'REX Contact Normal Position' is 'Contact closed when REX activated [OR] Nothing wired (recommended)'. The 'REX Contact Debounce Time' is 96. The 'Access Method' is 'Card Only' and the 'APB Type' is '<None>'. Below these settings are two dropdown menus for 'When saving': 'These settings are not the defaults for new readers' and 'Change this object only'. A 'Show Default Values' button is also present. On the right side, there are 'Commands' (Grant Access, Lock, Unlock) and 'Help' (Quick Start Guide). At the bottom, there is a 'Recent History' table with columns 'Date and Time', 'Location', and 'Description'. The table contains five entries. To the right of the table are two buttons: 'Return without Saving' and 'Save & Return'.

Date and Time	Location	Description
11/13/2009 12:42:40 PM	V100 (0) Flood_V1000 - Front Door Demo Reader 1	ClearDoorForcedOpen
11/13/2009 10:44:44 AM	V100 (0) Flood_V1000 - Front Door Demo Reader 1	DoorForcedOpen
11/13/2009 10:42:20 AM	V100 (0) Flood_V1000 - Front Door Demo Reader 1	ClearDoorForcedOpen
11/13/2009 10:42:20 AM	V100 (0) Flood_V1000 - Front Door Demo Reader 1	ClearDoorHeldOpen
11/13/2009 10:42:20 AM	V100 (0) Flood_V1000 - Front Door Demo Reader 1	ClearFaultLineSupervisionREX

Reader Configuration

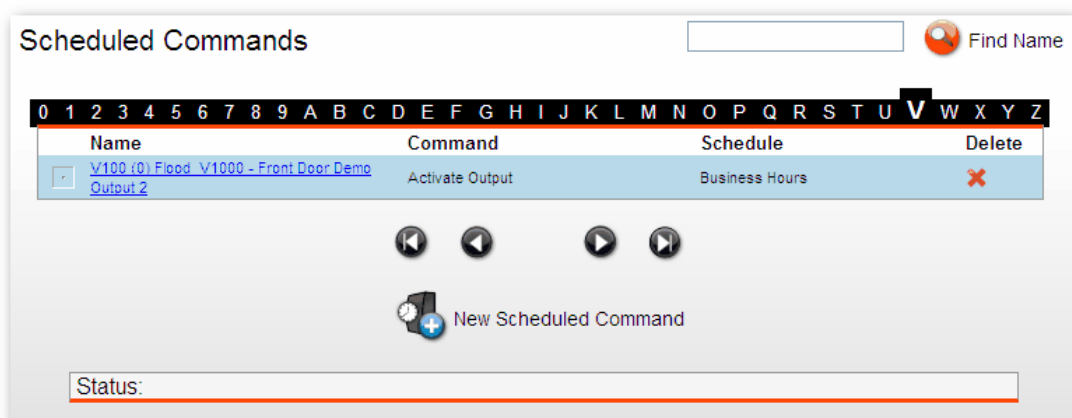
Here's a description of the reader options:

- **Status** - This is a read-only property and represents the state of the reader.
- **Reader Type**
  - **Wiegand** - Typical for most prox and iclass cards.
  - **Clock and Data Mode for HID Prox** -
  - **Clock and Data (ABA 128 bits max)** -
  - **Wiegand (ABA Clock and Data format)** -
- **Normal Access Time** - The time in seconds that the strike is activated on a valid card swipe.
- **Extended Access Time** - The time in seconds that the strike is activated for a valid extended access card swipe.
- **Door Held Time** - The time in seconds that the door contact needs to be open before the Door Held event is sent.
- **Door Contact Line Supervision** - Used to supervise the contact against tampering.
  - None
  - 2K/1K
  - 4K/2K
- **Door Contact Normal Position**
  - Contact closed when door closed (Recommended)

- Contact open when door closed [or] Nothing wired
- **Door Contact Debounce Time** - The amount of time (milliseconds) the controller will disregard repetitive door contact events.
- **Rex Action**
  - Shunts alarm and unlocks the door (Typical for mag locks)
  - Shunts alarm only (Typical for electric strike)
- **Rex Shunt/Unlock Time** - The time in seconds a REX event will unlock the door.
- **Rex Line Supervision** - Used to supervise the contact against tampering.
  - None
  - 2K/1K
  - 4K/2K
- **Rex Contact Normal Position**
  - Contact closed when REX activated [or] Nothing wired (recommended)
  - Contact open when REX activated
- **Rex Contact Debounce Time** - The amount of time (milliseconds) the controller will disregard repetitive REX events.
- **Access Method**
  - Card Only
  - Card and Pin
- **APB Type**
  - None
  - Real
  - Timed
- **When Saving** - Use this section to set defaults for new readers or configure existing readers connected to the controller.
- **Recent History** - Shows the recent activity for the reader.

### 1.3.2.1.3 Scheduled Commands

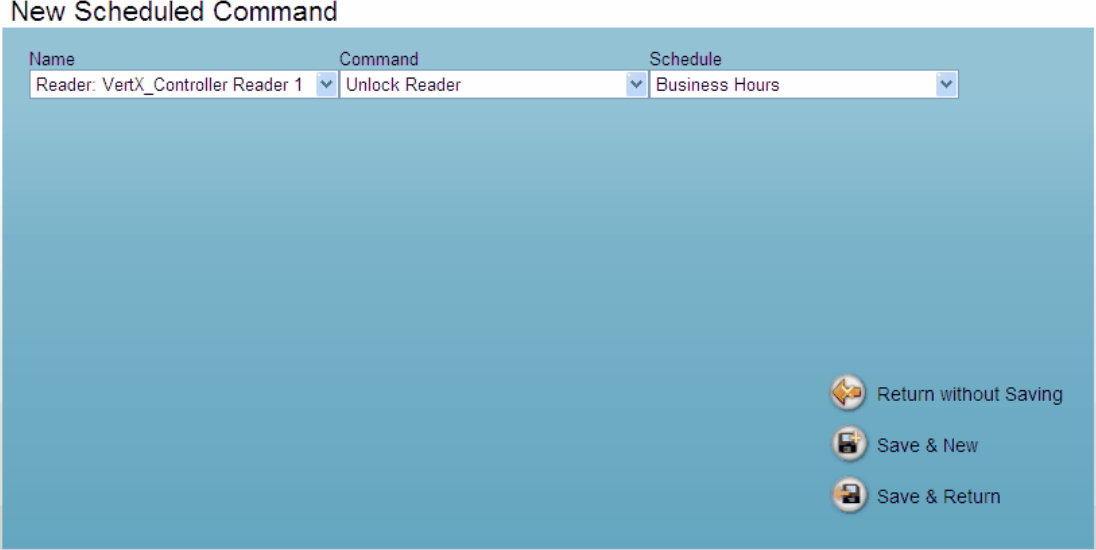
The Scheduled Commands screen will show all created scheduled commands (See figure Scheduled Commands). An example of a scheduled command would be assigning your Front Door to be open during the "Business Hours" schedule.



**Scheduled Commands**

On larger systems or systems with many scheduled commands, use the search box, navigation arrows or rolodex tab to locate specific scheduled commands.

To add a new scheduled command, click the New Scheduled Command link at the bottom of the page. This will open the New Scheduled Command screen (See figure New Scheduled Command).



**New Scheduled Command**

To create a new scheduled command, select the object to be commanded in the Name field, the command to be issued in the Command field and the schedule this command will follow in the Schedule field. Click Save & Return to save and return to the previous screen or Save & New to save and create another scheduled command.

### 1.3.2.2 Access Control

The Access Control tab (see figure Access Control) contains the following menu items:



**Access Control**

- [Cards](#)
- [Cardsets](#)
- [Access Levels](#)
- [Door Groups](#)
- [Areas](#)
- [Contact Schedules](#)
- [Schedules](#)
- [Holiday Groups](#)
- [Holidays](#)



*When setting up a new SecurusWeb system, working through the menu items from right to left will make more sense. Create the Holidays, then Holiday Groups. Create the Schedules and Door Groups and then create Access Levels. Define Card Sets and then Cards.*

### 1.3.2.2.1 Cards

The Card screen will show all the cards in the system (See figure Cards).

**Cards**

On larger systems or systems with many cards, use the search box, navigation arrows or rolodex tab to locate a specific card.

To modify an existing card, click the card number.

To add a new card to the system, click the New Card link at the bottom of the Cards screen. This will open the New Card screen (See figure New Card).

**New Card**

To add a group of cards all at once, click the New Cards link at the bottom of the Cards screen. This will open the New Cards screen, which has the additional field of "Number of Cards" (see figure Bulk Cards)



**New Cards**

Card Number

Card Set

Active On  /  /  At  :

Expires NEVER

Number of Cards

PIN Code

Confirm PIN

#### Bulk Cards

Here is a list of card options:

- **Card Number** - The encoded ID of the actual card.
- **Card Set** - The card set this specific card will use.
- **Active On** - This is the date the card will be activated. The default is the current date and time.
- **Expires** - There are three possible values for this option:
  - **Expires Never** - The card will never expire. (default)
  - **Expire On** - Selecting this option will expose date and time fields. Specify a date and time in the future that this card will expire on.
  - **Expire Now** - The card will expire immediately.
- **Credential Type** - There are two possible values for this option:
  - Card Only/Card Plus PIN
  - Pin Only
- **Number of Cards (New Cards only)** - The number of cards to add, starting with the value in the Card Number field.
- **PIN Code** - The PIN associated with the card.
- **Confirm PIN** - Confirmation of the PIN code.
- **Communication User** - Used for AHG420 Locksets only. This credential will wake the onboard WiFi.
- **Extended Access** - This indicates that this card will use the Extended Access time.
- **Passback Exempt** - This card will be APB exempt.
- **PIN Exempt** - This card will be PIN exempt.
- **Assigned To** - The cardholder this card belongs to.
- **Search cardholder by** - This selects what field the search criteria will be applied to.
- **for matches beginning with** - On systems with a large cardholder population, use this field to find a specific cardholder.
- **Access Levels** - The Access Levels assigned to the card.

### 1.3.2.2.2 Card Sets

The Card Sets screen will show all the card sets that are available in the current partition (see figure Card Sets).

**Card Sets**

On larger systems or systems with many card sets, use the search box, navigation arrows or rolodex tab to locate a specific card set.

To modify an existing card set, click the card set name.

To add a new card set to the system, click the New Card Set link at the bottom of the Card Set screen. This will open the New Card Set screen (see figure New Card Set).

**New Card Set**

Card sets have three properties:

- **Description** - The name of the card set.
- **Facility Code** - The facility code of the card set. (optional)
- **Card Type** - The card format the card set will use. The available formats are:
  - 26 bit
  - 33 bit
  - 34 bit
  - 37 bit

- Corp1000
- 37 bit with Facility Code

Click Save & Return to save and return to the previous screen or Save & New to save and create another card set.

### 1.3.2.2.3 Access Levels

The Access Levels screen will show all the Access Levels in the system (See figure Access Levels).

Name	Description	Delete
<a href="#">All Door - 24x7</a>		✖
<a href="#">No Access</a>	No Access at any place at any time.	✖

Access Levels

On larger systems or systems with many access levels, use the search box, navigation arrows or rolodex tab to locate a access level.

To edit an existing access level, click the name of the access level.

To create a new access level, click the New Access Level link at the bottom of the Access Levels screen. This will open the New Access Levels screen (See figure New Access Level).

New Access Level

Access levels have five properties:

- **Name** - The name of the access level.
- **Description** - The description of the access level.
- **Deadbolt Override** - Cards that are associated with an access level that has this option checked will override the deadbolt.
- **Door Groups** - The name of a specific door group.
- **Schedules** - The name of the schedule assigned to the selected door group.

Access levels can contain multiple door group/schedule associations. For example, a access level named "All doors - 24x7" might contain two sets of door group/schedule associations (See figure Multiple Door Groups).

All Door - 24x7

Name: All Door - 24x7

Description: This access level defines 24x7 access to all doors.

Deadbolt Override: ☐

Door Groups: Interior Doors Schedules: Always Add

Door Group	Schedule	Delete	Undelete
Exterior Doors	Always	X	X
Interior Doors	Always	X	X

Return without Saving  
Save & New  
Save & Return

Multiple Door Groups

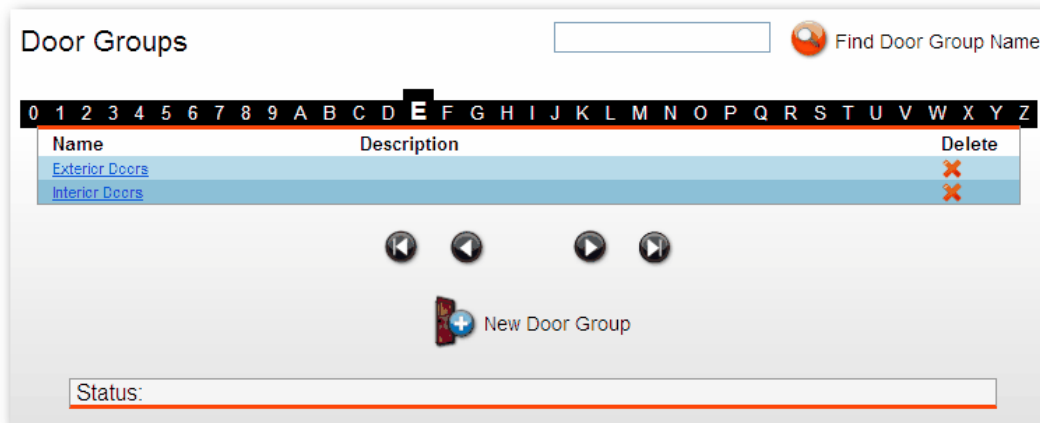


**When adding a door group/schedule association, make sure to click the Add button before saving. If you fail to click the Add button, the access level will be created but will not contain a door group/schedule association. This is a common mistake and will give the appearance that the SecurusWeb system is not working properly.**

Click Save & Return to save and return to the previous screen or Save & New to save and create another access level.

#### 1.3.2.2.4 Door Groups

The Door Groups screen will show all the door groups in the current partition (See figure Door Groups). Door groups are a grouping of doors that will later be associated with a schedule to create access levels.

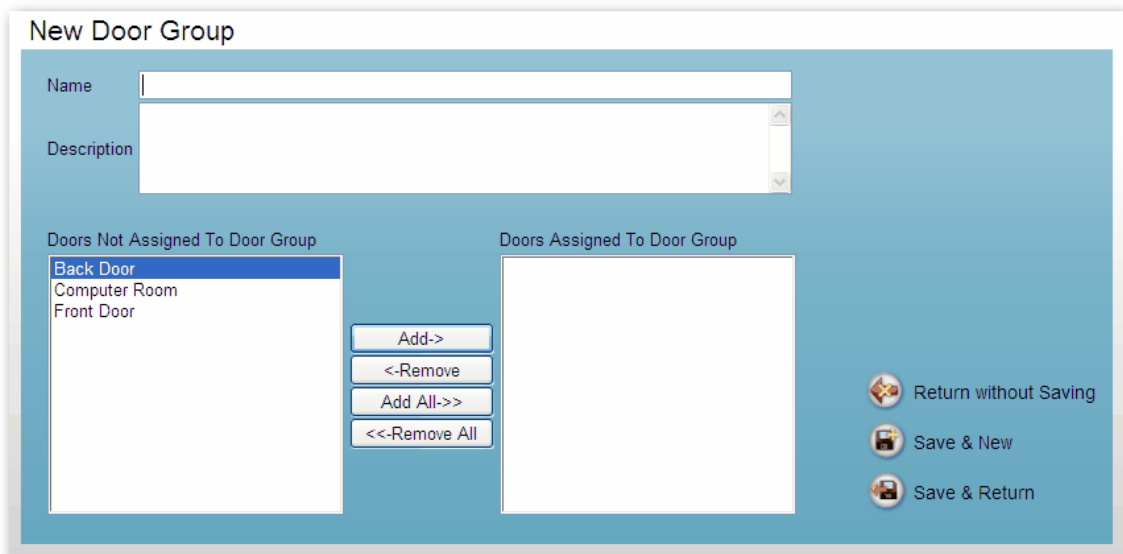


Door Groups

On larger systems or systems with many access levels, use the search box, navigation arrows or rolodex tab to locate a door group.

To edit an existing door group, click the name of the door group.

To create a new door group, click the New Door Group link at the bottom of the Door Groups screen. This will open the New Door Group screen (See figure New Door Group).



New Door Group

Door groups have four properties:

- **Name** - The name of the door group.
  - This is usually something descriptive such as "Exterior Doors"
- **Description** - A description of the door group.
- **Doors Not Assigned to Door Group** - All the doors that are NOT part of the door group.
- **Door Assigned To Door Group** - All the doors that are part of the door group.

Click Save & Return to save and return to the previous screen or Save & New to save and create another door group.

### 1.3.2.2.5 Areas

The Areas screen will show all the Areas in the current partitions (see figure APB Areas). Areas are the definition of entry and exit readers for an APB (anti-passback) area.

APB Areas

Find Area Name

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Name	Description	Delete
------	-------------	--------

New Area

Status:

**APB Areas**

On larger systems or systems with many areas, use the search box, navigation arrows or rolodex tab to locate an area.

To edit an existing area, click the name of the area.

To create a new area, click the New Area link at the bottom of the APB Areas screen. This will open the New Area screen (See figure New Area).

**New Area**

Name

Description

**Entry Readers**

Readers Not Entering Area

- Back Door
- Computer Room
- Front Door

Readers Entering Area

Add-> <-Remove Add All->> <<-Remove All

**Exit Readers**

Readers Not Exiting Area

- Back Door
- Computer Room
- Front Door

Readers Exiting Area

Add-> <-Remove Add All->> <<-Remove All

Return without Saving Save & New Save & Return

#### New Area

New areas have four properties:

- **Name** - The name of the area.
- **Description** - The description of the area. (optional)
- **Entry Readers** - Readers defined as entry readers.
- **Exit Readers** - Readers defined as exit readers.

To add or remove entry or exit readers, use the Add/Remove buttons.

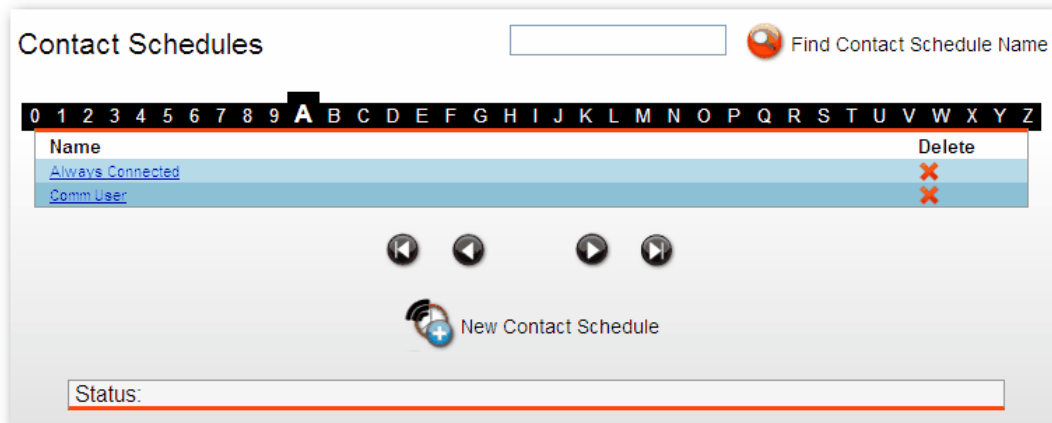


**The entry and exit readers contained within an area must be physically wired to a single controller. An Edge reader CANNOT be part of an area.**

Click Save & Return to save and return to the previous screen or Save & New to save and create another area.

#### 1.3.2.2.6 Contact Schedules

The Contact Schedule screen will show all the contact schedules in the current partition (see figure Contact Schedules). Contact schedules are used by the standalone AHG420 locksets to control the built in Wi-Fi radio.

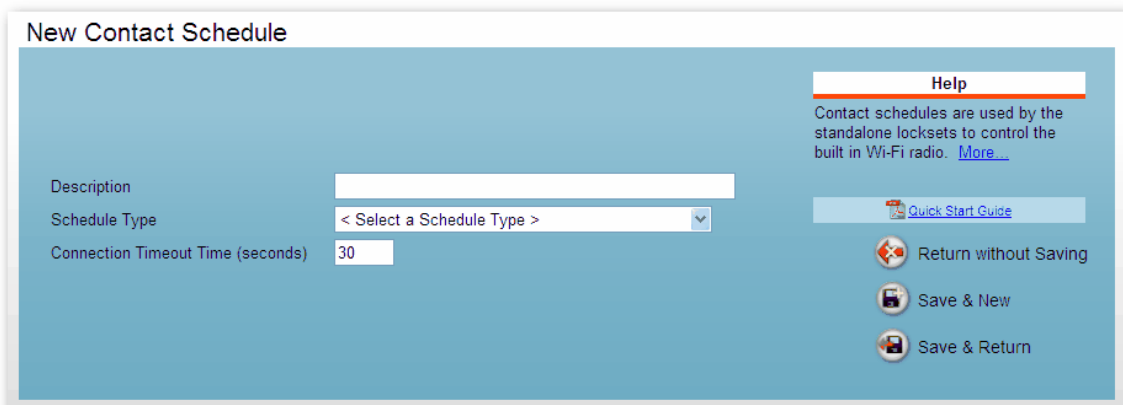


Contact Schedules

On larger systems or systems with many contact schedules, use the search box, navigation arrows or rolodex tab to locate a contact schedule.

To edit an existing contact schedule, click the name of the contact schedule.

To create a new contact schedule, click the New Contact Schedule link at the bottom of the Contact Schedule screen. This will open the New Contact Schedule (See figure New Contact Schedule).



New Contact Schedule

New contact schedules have three properties:

- **Description** - The name of the contact schedule.
- **Schedule Type** - The type of schedule the contact schedule will use. There are five possible options:
  - **Comm User Only** - The lockset does not automatically wake up on any schedule. Only a Communication User can wake the lock up in the field.
  - **Day of Month** - Select certain days of the month for the schedule to operate.
    - **Day(s) of Month** - Select the dates that you wish the lock to activate each month.
    - **Time of Day** - Select from 1 to 4 times per day that you wish the lockset to wake up.
  - **Day of Week** - Select certain days of the week for the schedule to operate.
    - **Day(s) of Week** - Select the days that you wish the lock to activate each week.
    - **Time of Day** - Select from 1 to 4 times per day that you wish the lockset to wake up.

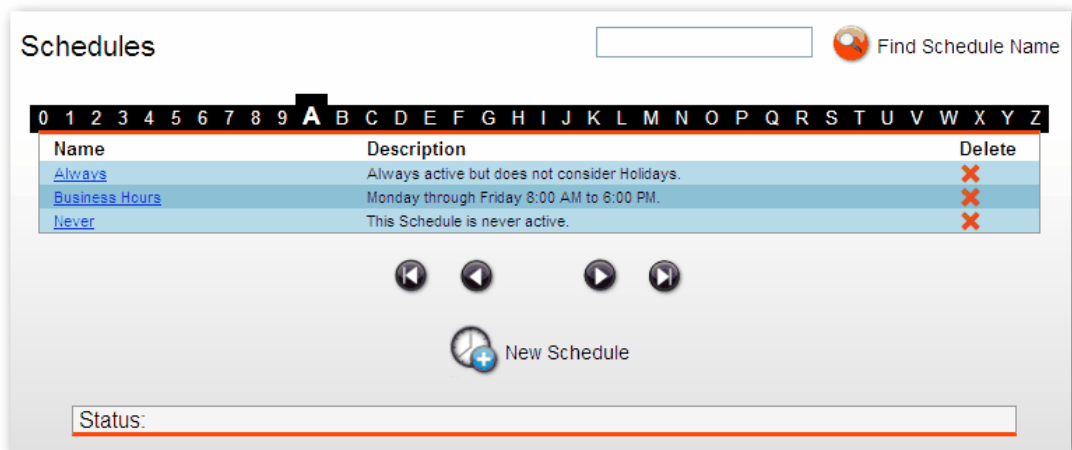


- **Connection Always On** - The lockset radio will never turn off. Recommended for use **ONLY** on hard powered locks, as this setting will greatly reduce battery life.
- **Simple('x' minutes off, 'y' seconds on scheduler)** - The lockset radio will remain off for the sleep period.
  - **Sleep Period (minutes)** - The number of minutes for the radio to remain off until connecting to the server again.
- **Connection Timeout Time (seconds)** - The maximum number of seconds to leave the radio running. We recommend a value of 30 seconds.

Click Save & Return to save and return to the previous screen or Save & New to save and create another contact schedule

### 1.3.2.2.7 Schedules

The Schedules screen will show all the schedules available to the current partition (See figure Schedules).



**Schedules**

On larger systems or systems with many schedules, use the search box, navigation arrows or rolodex tab to locate a schedule.

To edit an existing schedule, click the name of the schedule.

To create a new schedule, click the New Schedule link at the bottom of the Schedules screen. This will open the New Schedule screen (See figure New Schedule).

### New Schedule

Name

Description

Day  Start Time  :  AM Stop Time  :  PM

New Schedule

Schedules have 5 properties:

- **Name** - The name of the schedule.
- **Description** - A description of the schedule (optional)
- **Day/Start Time/Stop Time** - The Day of the week and the associated Start and Stop times.

It's common to have a schedule contain many Day/Start & Stop Time associations. For example, SecurusWeb comes with a default "Business Hours" schedule. This schedule contains five Day/Time associations (see figure Business Hours). Notice that the Start Times are at 8:00AM and the Stop Times are at 5:59PM. This is because Start Times start at the beginning of the minute (8:00:01AM) and Stop Times end at the end of the minute (5:59:59PM).

### Business Hours

Name

Description

Day  Start Time  :  AM Stop Time  :  PM

Day	Start Time	Stop Time	Delete Undelete
Monday	8:00 AM	5:59 PM	<input type="button" value="X"/>
Tuesday	8:00 AM	5:59 PM	<input type="button" value="X"/>
Wednesday	8:00 AM	5:59 PM	<input type="button" value="X"/>
Thursday	8:00 AM	5:59 PM	<input type="button" value="X"/>
Friday	8:00 AM	5:59 PM	<input type="button" value="X"/>

Business Hours

The Day field also contains Holiday Groups. This feature is used to assign specific time intervals to Holidays contained within a Holiday Group. For example, let's say there's a Holiday Group named "Half Day Holidays" that contains all the weekday Holidays the company will only works half days on. Add a Holiday Group/Start & Stop Time association (see figure Half Day Holiday).

Day	Start Time	Stop Time	Delete Undelete
Monday	8:00 AM	5:59 PM	
Tuesday	8:00 AM	5:59 PM	
Wednesday	8:00 AM	5:59 PM	
Thursday	8:00 AM	5:59 PM	
Friday	8:00 AM	5:59 PM	
Half Day Holidays	8:00 AM	11:59 AM	

Half Day Holiday



**Holiday Group/Time associations will always trump Day/Time associations. In other words, if a holiday group contains a holiday that falls on a Wednesday and the normal Wednesday time interval is 8:00am to 5:59pm, but the holiday time interval is 8:00am to 11:59am, the holiday interval will be applied.**

It's also common to have multiple Start and Stop times for a single day. For example, a night crew might work from 7:00pm until 4:00am the following day (see figure Night Shift).

**New Schedule**

Name:

Description:

Day:  Start Time:  :  AM Stop Time:  :  AM

Day	Start Time	Stop Time	Delete Undelete
Monday	7:00 PM	11:59 PM	
Tuesday	12:00 AM	3:59 AM	
Tuesday	7:00 PM	11:59 PM	
Wednesday	12:00 AM	3:59 AM	
Wednesday	7:00 PM	11:59 PM	
Thursday	12:00 AM	3:59 AM	
Thursday	7:00 PM	11:59 PM	
Friday	12:00 AM	3:59 AM	

Night Shift

Finally, it's also common to create a "Never" time interval. This is typically used when creating a a Holiday Group/Time association. The correct Start Time and Stop Time for a NEVER schedule are 12:00am to 12:00am.

### 1.3.2.2.8 Holiday Groups

The Holiday Groups screen will show all the Holiday Groups that are available in the current partition (see figure Holiday Groups). Holiday Groups are a group of similar holidays and are used when creating schedules.

**Holiday Groups**

Find Holiday Group Name

0 1 2 3 4 5 6 7 8 9 A B C D E F G **H** I J K L M N O P Q R S T U V W X Y Z

Name	Description	Delete
Half Day Holidays		X

Navigation arrows: Previous, Next, First, Last

New Holiday Group

Status:

**Holiday Groups**

On larger systems or systems with many holidays groups, use the search box, navigation arrows or rolodex tab to locate a holiday group.

To edit an existing holiday group, click the name of the holiday group.

To create a new holiday group, click the New Holiday Group link at the bottom of the Holiday Groups screen. This will open the New Holiday Group screen (See figure New Holiday Group).

**New Holiday Group**

Name:

Description:

**Holidays Not Assigned To Holiday Group**

- Company Picnic
- New Year Day
- New Year Eve

**Holidays Assigned To Holiday Group**

Buttons between lists: Add->, <-Remove, Add All->>, <<-Remove All

Buttons on right: Return without Saving, Save & New, Save & Return

**New Holiday Group**

There are four properties for a new holiday group:

- **Name** - The name of the holiday group.
- **Description** - The description of the holiday group. (optional)
- **Holidays Not Assigned To Holiday Group** - All holidays not assigned to the holiday group.
- **Holidays Assigned To Holiday Group** - Holidays assigned to the holiday group.

To assign a holiday to the holiday group, highlight the holiday in the Holidays Not Assigned To Holiday Group box and click the Add button. This will place the selected holiday in the Holidays Assigned To Holiday Group box.

Click **Save & Return** to save and return to the previous screen or **Save & New** to save and create another holiday group.

### 1.3.2.2.9 Holidays

The Holidays screen will show all the holidays that are available in the current partition (see figure Holidays). Similar holidays will be grouped in Holiday Groups for use in creating schedules.

Holidays

Find Holiday Name

0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Name	Date	Description	Delete
------	------	-------------	--------

Navigation arrows: Previous, First, Last, Next

New Holiday

Status:

**Holidays**

On larger systems or systems with many holidays, use the search box, navigation arrows or rolodex tab to locate a holiday.

To edit an existing holiday, click the name of the holiday.

To create a new holiday, click the **New Holiday** link at the bottom of the Holidays screen. This will open the New Holiday screen (See figure New Holiday).

New Holiday

Name

Description

Date: 11 / 18 / 2009

November 2009

Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

Return without Saving

Save & New

Save & Return

**New Holiday**

There are three properties for a new holiday:

- **Name** - The name of the holiday.
- **Description** - The description of the holiday. (optional)
- **Date** - The data of the holiday
  - To set the date either use the month/day/year dropdown boxes or the interactive calendar.

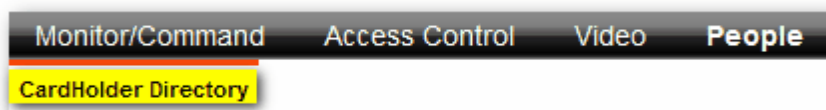
Click Save & Return to save and return to the previous screen or Save & New to save and create another holiday.



**Holidays are set on a yearly basis. In other words, even though some holidays are on the same date every year, they still need to have year attribute modified to be active for the next year.**

### 1.3.2.3 People

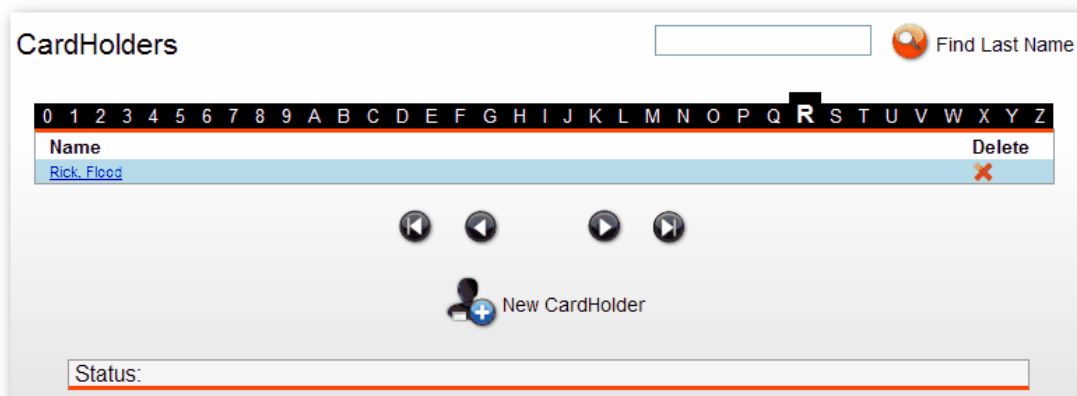
The People tab contains one menu item (see figure People). This menu item is [CardHolder Directory](#).



People

#### 1.3.2.3.1 CardHolder Directory

The Cardholder Directory screen will show all the available cardholders in the current partition (see CardHolders). SecurusWeb separates cards and cardholders. In this section only cardholders will be defined, not cards. Use the cards section of SecurusWeb to assign cards to cardholders.



CardHolders

On larger systems or systems with many cardholders, use the search box, navigation arrows or rolodex tab to locate a specific cardholder.

To modify an existing cardholder, click the cardholder name.

To add a new cardholder to the system, click the New CardHolder link at the bottom of the CardHolder screen. This will open the New CardHolder screen (See figure New CardHolder).

**New CardHolder**

CardholderID  Synchronize from directory server ☐

Last Name  First  MI

Street

City  State  Zip Code

Phone  Fax

Cell Phone  Email

Department  Supervisor

Emergency

[Show Additional Fields...](#)

Notes

Recent History

**Photo**

No Photo Found  
(Aspect Ratio 2x3)

[Use This Photo](#)

**Assigned Cards**

[Save CardHolder and create a new card](#)

**New CardHolder**

There are many New CardHolder properties, but only two of them are required; Last Name and First.

The "Synchronize from directory server" check box is related to the IDHolderDataImporter utility. When a cardholder is imported from an Active Directory server, this check box is checked. This indicates that this cardholder should sync with the matching user in Active Directory. In other words, if the matching user in Active Directory is removed, the related cardholder in SecurusWeb will also be removed. When manually creating a new cardholder using SecurusWeb, this check box will NOT be checked.



***Deleting a cardholder in SecurusWeb will not delete the matching user in the associated Active Directory.***

The "Show Additional Fields" link will expose a set of additional fields (see figure Additional Fields).



<a href="#">Hide Additional Fields</a>			
Vehicle Model	<input type="text"/>	Vehicle Year	<input type="text"/>
Vehicle Color	<input type="text"/>	Vehicle Plate	<input type="text"/>
CustomA	<input type="text"/>	CustomB	<input type="text"/>
CustomC	<input type="text"/>	CustomD	<input type="text"/>
CustomE	<input type="text"/>	CustomF	<input type="text"/>

#### Additional Fields

To assign a picture to the cardholder, click the Browse button in the Photo section to locate the desired picture. Once a picture is selected, click the Use This Photo to complete the association. A picture with an aspect ratio of 2x3 will look the best.

To save the current cardholder and create a new card, click the link under Assigned Cards section.

Click Save & Return to save and return to the previous screen or Save & New to save and create another cardholder.

### 1.3.2.4 Reporting

The Reporting tab contains one menu item (see figure Reporting). The menu item is Reports

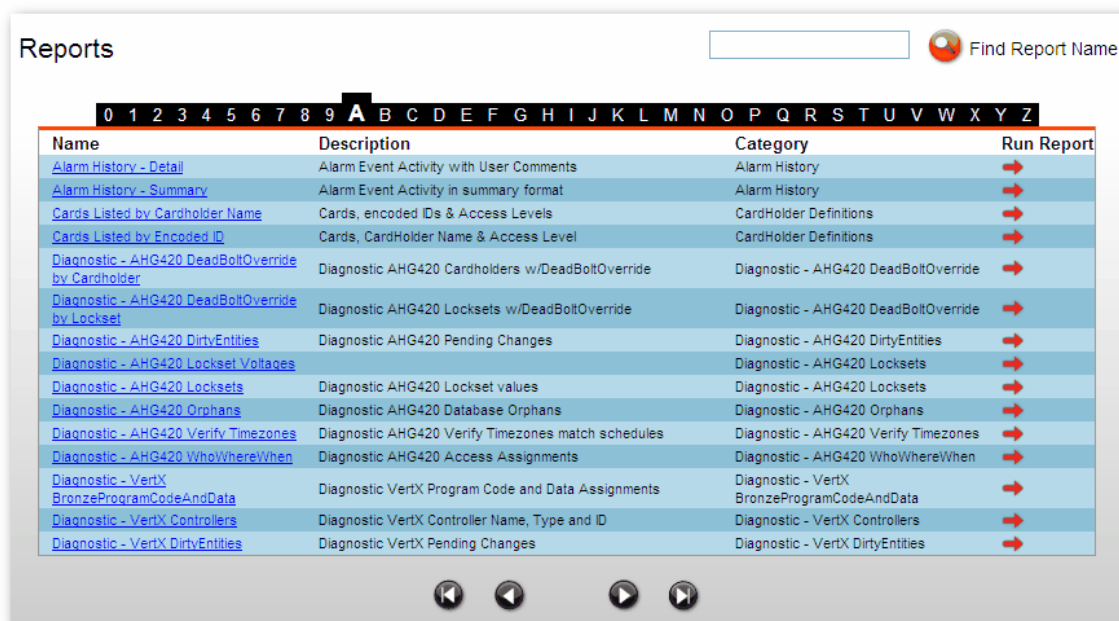


#### Reporting



### 1.3.2.4.1 Reports

The Reports screen will show all the available reports for the current partition (see figure Reports).



Reports

On larger systems or systems with many reports, use the search box, navigation arrows or rolodex tab to locate a specific report.

To run a default report, click the appropriate red arrow. This will start the generation of the report (see figure Generating Report).

#### Cards Listed by Encoded ID

The report is currently being created. There are 1 report(s) in the queue.


While the report is in the queue and during the creation of the report, you can continue to use all other functions in the application. You can then return to this page at any time to check on the status of the report.

Generating Report

As this screen indicates, you may continue to use SecurusWeb while this process is taking place and return to the reports screen to check the status of the report. Typically the report generation will take 5 to 15 seconds, but on larger systems or when running reports that contain large amounts of data, this may take longer. When generation is complete click the View Report link (see figure View Report).

### Cards Listed by Encoded ID

The report is complete.

 Return to Report List

 View Report

**View Report**

Clicking the View Report link will open the PDF report in the default browser window (see figure PDF Report).

### Cards Listed by Encoded ID

#### Cards, CardHolder Name & Access Level

EncodedID	LastName	FirstName	AccessLevelName
1001	Rick	Flood	All Door - 24x7
Rows Listed 1			

**PDF Report**

Use the reports section of the rich client to modify the columns, grouping/sorting and appearance of reports.

To apply filtering to a report, click the report name (see figure Reports). This will show the report limitation screen (see figure Report Limitation).

### Events History Report

The report has the following limitations applied:

Limitation:

Matches:

The resulting report has 48 rows.

**Report Limitation**

Click the Add Limitation button to add filtering. Click the Run Report icon to run the report after all filters have been applied.

### 1.3.2.5 Utilities

The Utilities tab contains 2 menu items (see figure Utilities).

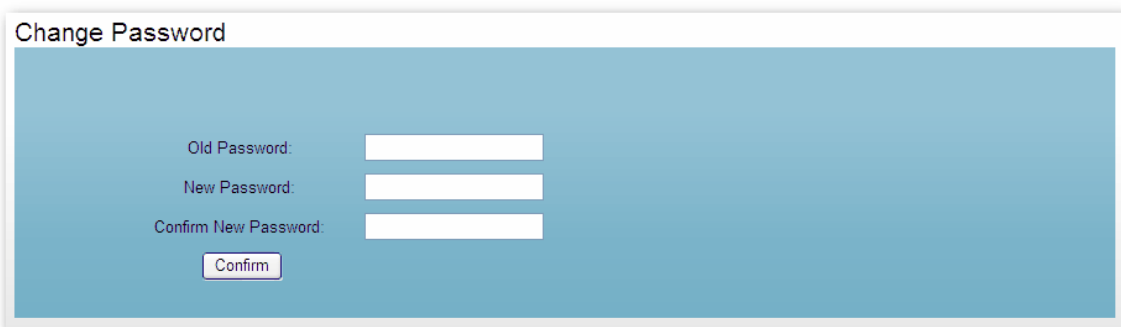


Utilities

- [Change User Password](#)
- [Upload Card Format](#)
- [Customize Screen](#)

#### 1.3.2.5.1 Change User Password

The Change User Password screen will allow the logged in user to change their password (see figure Change Password).

A screenshot of a web form titled 'Change Password'. The form has a light blue background. It contains three text input fields: 'Old Password:', 'New Password:', and 'Confirm New Password:'. Below the 'Confirm New Password' field is a 'Confirm' button.

Change Password

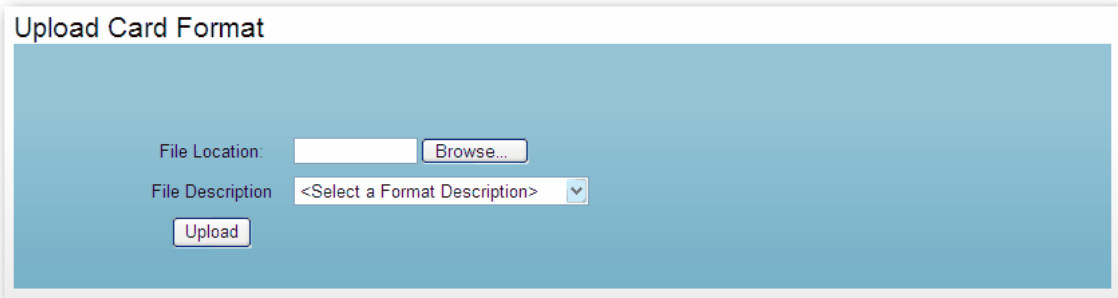
The Change Password screen has three fields:

- **Old Password** - The logged in users current password.
- **New Password** - The password the logged in user would like to use.
- **Confirm New Password** - The new password again for confirmation.

Click the Confirm button to change the password.

### 1.3.2.5.2 Upload Card Format

The Upload Card Format screen allows the adding or changing of Card Formats to the SecurusWeb system (see figure Upload Card Format).



**Upload Card Format**

The Upload Card Format screen has two fields:

- File Location - Click the Browse button to select the card format file.
- File Description - Select one of the six possible formats:
  - 26 bit Wiegand
  - 33 bit Wiegand
  - 34 bit Wiegand
  - 37 bit Wiegand
  - Corp1000
  - 37 bit Wiegand with Facility Code

Click the Upload button to save the selected card format to the database.



***The SecurusWeb system only allows one of each format type. Custom formats are NOT allowed in SecurusWeb 4.3.0.***

### 1.3.2.5.3 Customize Screen

Enter topic text here.

## 1.3.3 Utilities

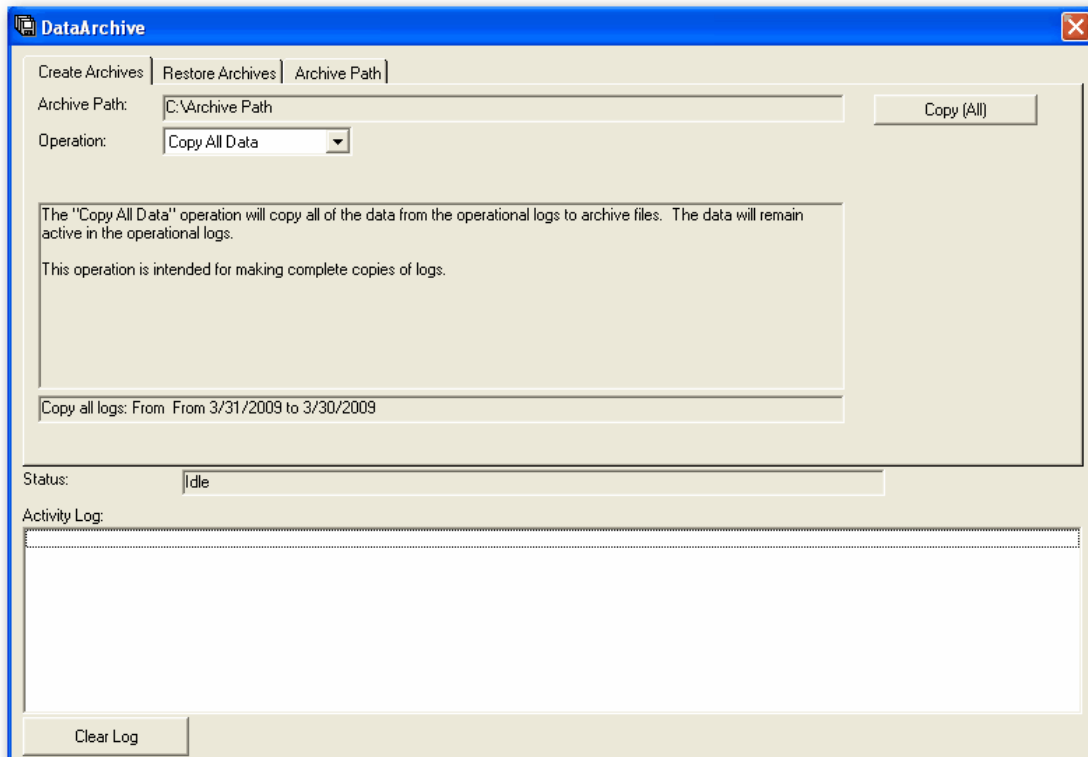
The SecurusWeb system has the following utilities:

- [Data Archive](#)
- [Data Maintenance](#)
- [Database Browser](#)

The SecurusWeb utilities can be found at Start > Program Files > SecurusWeb.

### 1.3.3.1 Data Archive

The Data Archive utility creates and/or restores transaction and alarm archives. Access this utility by clicking on Start > Programs > SecurusWeb > Data Archive. (see figure Data Archive)



Data Archive

When creating an archive there are three "Operation" options:

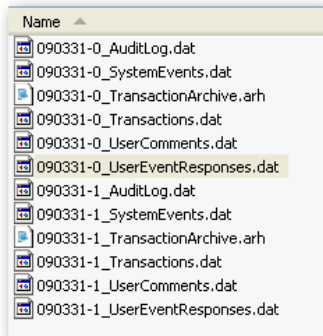
- **Copy All Data:** This operation will copy all of the data from the operational logs to the archive files. The data will remain active in the database. This operation is intended for making complete copies of logs.
- **Copy Data:** This operation will copy the specified data from the operational logs to the archive files. The data will remain active in the database. This operation is intended for making copies of specific data.
- **Archive (Move) Data:** This operation will move the specified data from the operational logs to the archive files. This operation is intended for long-term storage of data this is not likely to be needed again. To run reports against this data, restore the data first. Specify the amount of data to keep in the active log.

After verifying the Archive Path and Operation, click the Copy/Archive button in the upper right hand section of the window. The Status box will show a realtime account of what the archive utility is doing and a log will be generated in the Activity Log window. When completed, the Status box will read "Idle".

The archived files will be placed in the location specified in Archive Path. These files are SQL .dat files and have the following naming convention.

*YYMMDD-X\_ArchiveName.dat*

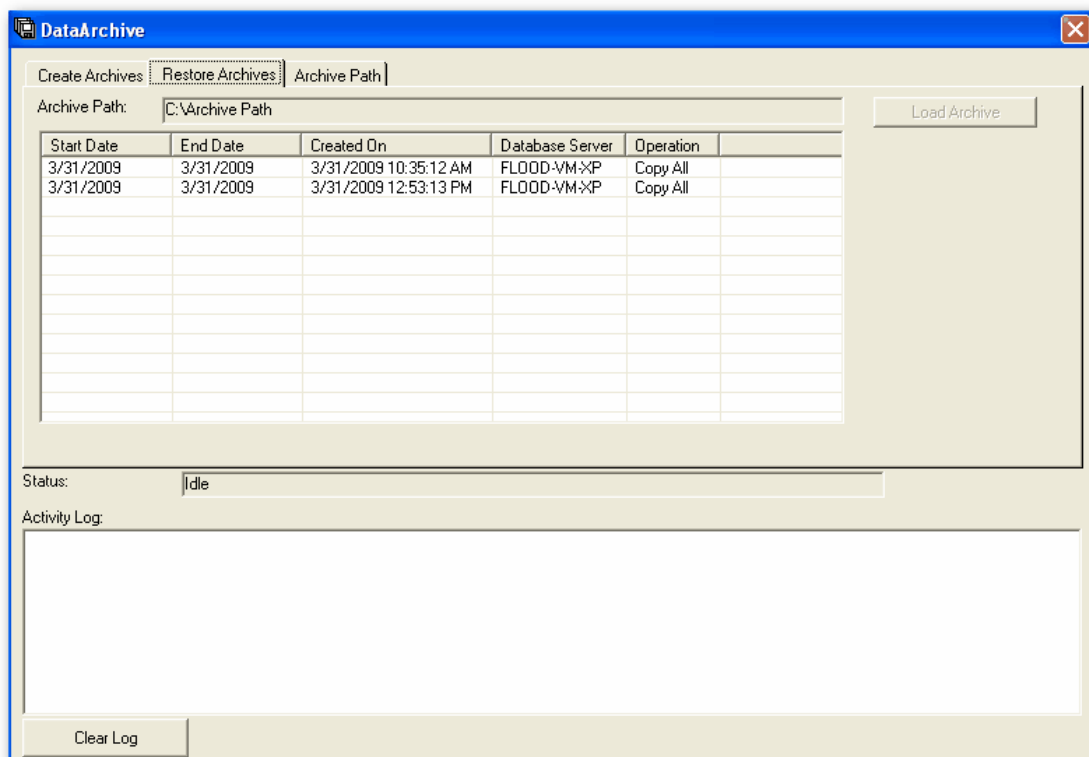
**YY** is the 2 digit year, **MM** is the 2 digit month, **DD** is the 2 digit day and **X** is a zero based counter that increments for every archive done for a specific day. (see figure Archives)



**Archives**

In addition to the .dat files there are .arh files that are used by the Data Archive utilities restore feature. **It's important to place all these files in a safe place.**

To restore an archive, click on the Restore Archives tab (see figure Restore Archive). Select a archive from the grid and click Load Archive. The Status box will show a realtime account of what the archive utility is doing and a log will be generated in the Activity Log window. When completed, the Status box will read "Idle".



**Restore Archive**

To change the "create" or "restore" locations, use the Archive Path tab.

### 1.3.3.2 Database Maintenance

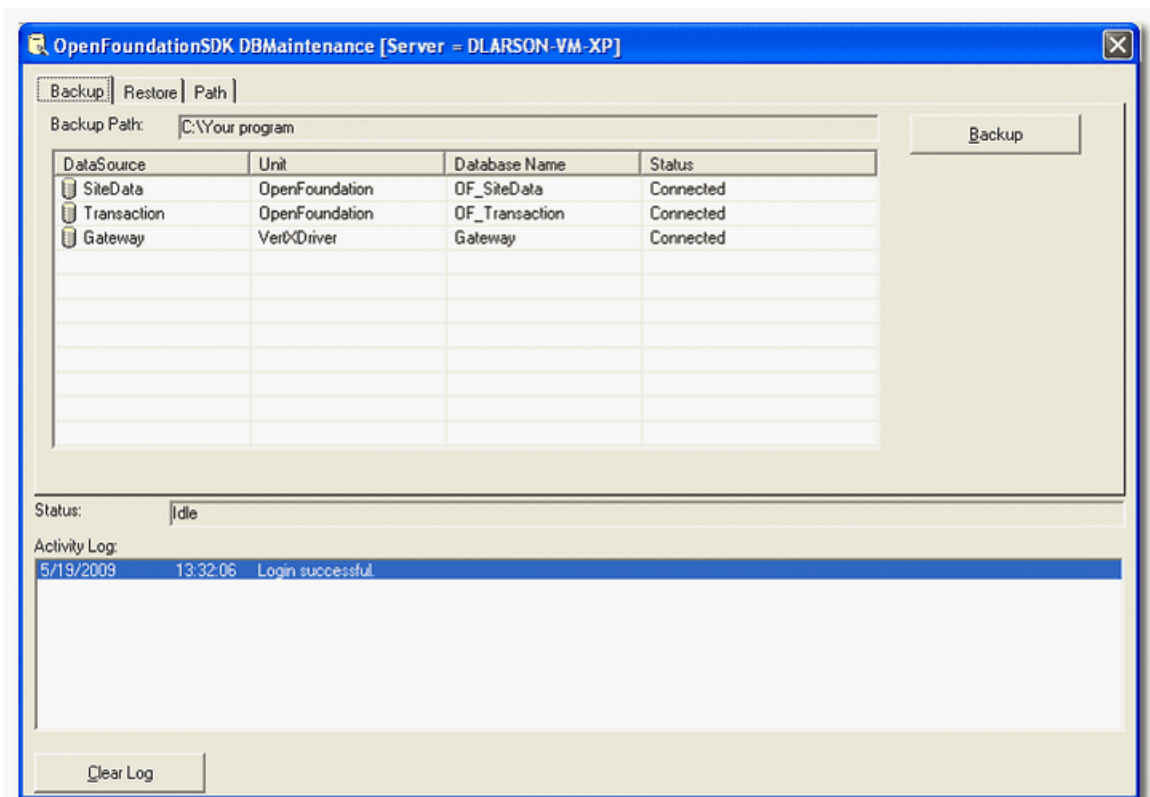
The Database Maintenance Utility is used to do routine database backups. Regular database backups are useful when attempting to restore a system to a known good state.

The Database Maintenance Utility is located under *Start>Programs>SecurusWeb>Database Maintenance*.

The Database Maintenance window contains 3 tabs. Backup, Restore and Path

#### **Backup Tab**

This tab contains the Backup Path and Data Sources (databases) that will be backed up (see figure Backup Tab). Clicking the Backup button will begin the backup. The progress will shown in the Activity Log window. To clear the activity log, click Clear Log.



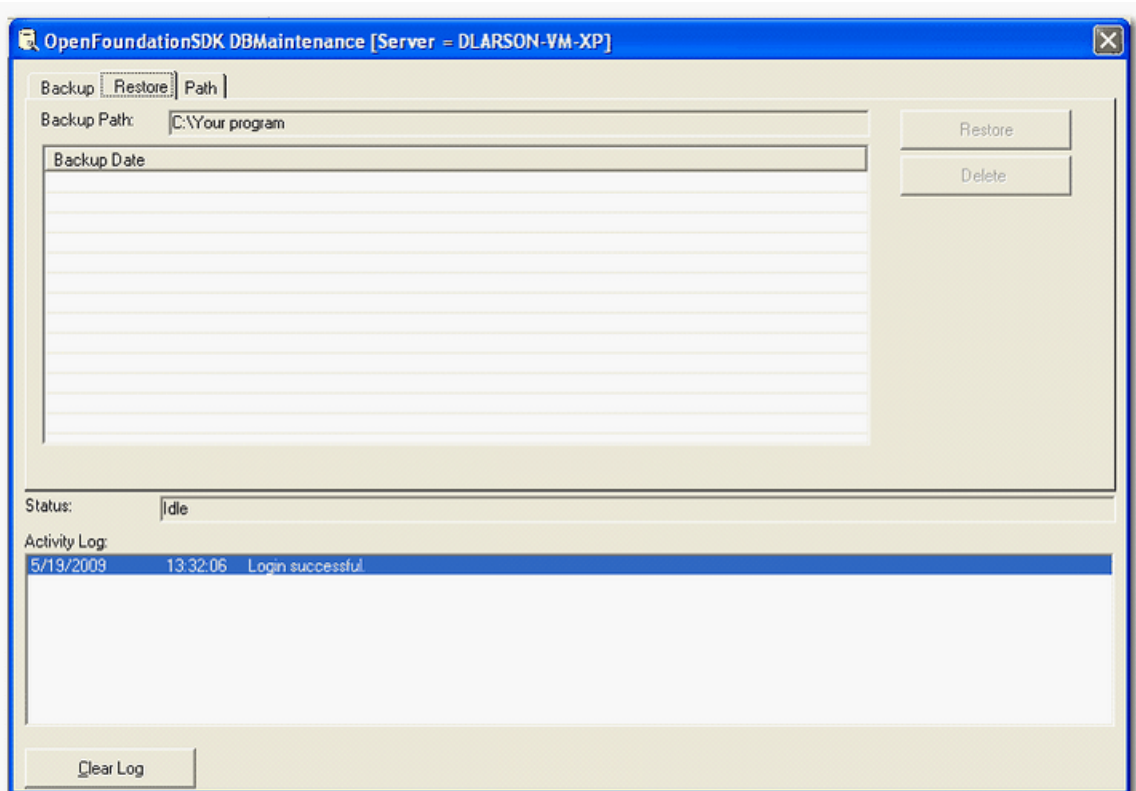
Backup Tab



**Only one backup per day will be saved. In other words, if you attempt to backup your system more than once in a day, the previous backup will be overwritten.**

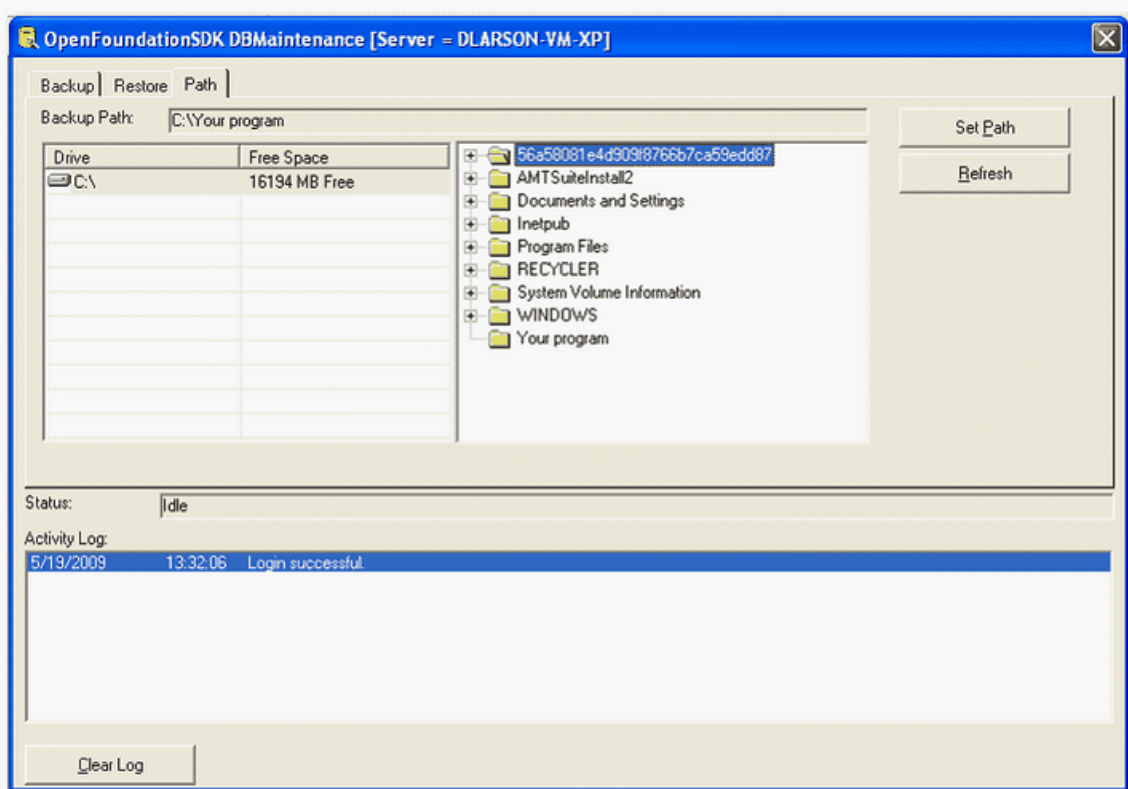
#### **Restore Tab**

This restore tab allows you to select a backup to restore (see figure Restore Tab). Simply highlight the desired backup and click Restore. The Activity Log window will show the progress.

**Restore Tab****Path Tab**

This path tab allows you to select the location to backup to or restore from (see figure Path Tab). When the desired location is highlighted, click Set Path.

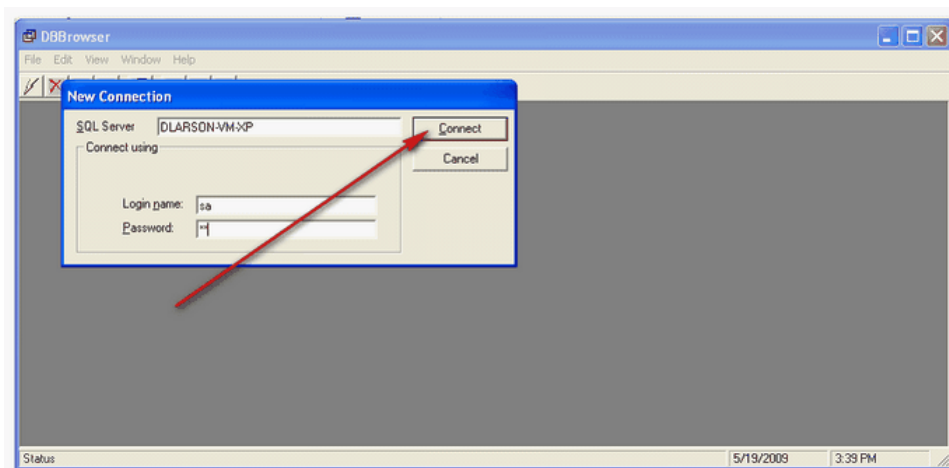




Path Tab

### 1.3.3.3 Database Browser

The Database Browser Utility is used to view SQL databases and is located under *Start>Programs>SecurusWeb>Database Browser*. Log in using the SA username and password. (see figure Database Browser)



Database Browser

This utility is helpful for developers or database administrators. Its purpose is to give the user the ability to view the databases without the need of SQL client tools.



**Please use caution when using the Database Browser utility. Changing the SecurusWeb data directly could result in unexpected behavior.**

### 1.3.3.4 License Editor

## 1.4 Troubleshooting SecurusWeb

This section goes over some of the more common troubleshooting areas and techniques.

For additional support please contact SecuriCo support at [or](#) .

### 1.4.1 Error Log

The AMErrorlog.txt is the place where SecurusWeb will log all errors. It's typically located at *C:\Documents and Settings\All Users\Application Data\SecurusWeb*.

Folders	Name	Size	Type	Date Modified
Desktop	GatewayCache		File Folder	3/12/2009 2:52 PM
My Documents	AMErrorLog.txt	1 KB	Text Document	3/30/2009 8:59 PM
My Computer	AMTsyncService.log	8 KB	Text Document	3/30/2009 9:00 PM
3 1/2 Floppy (A:)				
Local Disk (C:)				

The error log will typically give a brief description of each error, along with some detailed information.

This additional information will be more useful to a software engineer and will often help give a general idea of what is causing the error.



**When contacting support, the AMErrorlog.txt is something that should be readily available. The most current error log will be named AMErrorLog.txt. The other AMErrorLogXXXXXXXXXX.txt files are older error logs kept for historic troubleshooting if necessary.**

### 1.4.2 Diagnostic Reports

SecurusWeb has 13 diagnostic reports to aid in the troubleshooting.

#### HID

- Diagnostic - VertX BronzeProgramCodeAndData
- Diagnostic - VertX Controllers
- Diagnostic - VertX DirtyEntities
- Diagnostic - VertX Orphans
- Diagnostic - VertX WhoWhereWhen

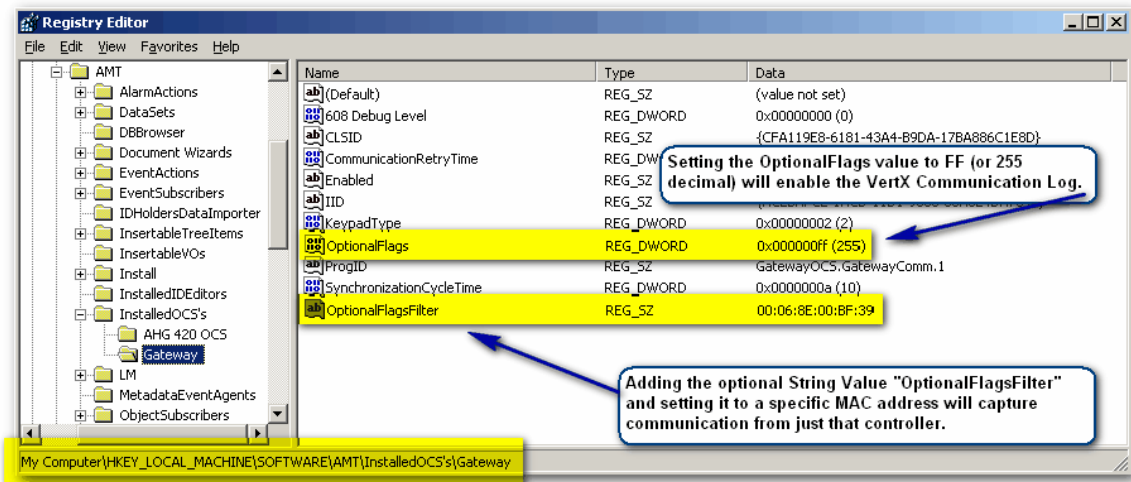
#### Sargent

- Diagnostic - AHG420 DeadBoltOverride by Cardholder
- Diagnostic - AHG420 DeadBoltOverride by Lockset
- Diagnostic - AHG420 DirtyEntities
- Diagnostic - AHG420 Lockset Voltages
- Diagnostic - AHG420 Locksets

- Diagnostic - AHG420 Orphans
- Diagnostic - AHG420 Verify Timezones
- Diagnostic - AHG420 WhoWhereWhen

### 1.4.3 VertX Communication Log

SecurusWeb has the ability to log all communication to and from the VertX controllers. To enable these logs, open the registry to HKLM/Software/AMT/InstalledOCSs/Gateway. Setting the OptionalFlags key to 255 (decimal) will enable the log. (see figure Optional Flags)



Optional Flags

The generated log file will be located at C:\Documents and Settings\All Users\Application Data\WebBrix\GatewayCache\VertXCommunication.log. AMT engineers will use this log to determine exactly what communication is happening between the software and the hardware.

Optionally, you can add the key "OptionalFlagsFilter". This string value can contain one or more (separated by a semicolon) MAC addresses of controllers. When this key is populated, the log file will filter out any communication that ISN'T from one of the entered MAC addresses. This is useful for larger systems.



**Remember to set the OptionalFlags value to 0 when done troubleshooting. If this isn't done, the log file will eventually grow to a size that may effect your PC performance.**