speco technologies®

SECUREGUARD®

SecureGuard® Speco Access Setup Guide

v. 2.9.0

4/20/2021

speco technologies®

Contents

1 Overview

The purpose of this manual is to guide you in the configuration of Speco access control devices within the SecureGuard® Configuration Tool. Before starting to add access control devices, please familiarize yourself with the basic usage and setup of SecureGuard® as outlined in the SecureGuard® Technical Manual. This manual assumes you have installed and configured your access control system for your sites and that the devices are in operation.

The instructions here are applicable for the following access controllers:

- A1
- A2E4P
- A2E4

2 Access Control Sites

Within SecureGuard®, an access control device is designated as a non-video site with associated doors.

3 SecureGuard® Access User

In order to use Speco Access with SecureGuard® VMS, a user account needs to be added to the access controller to allow SecureGuard® VMS to communicate with the controller.

4 Access Control Users

Unlike an Operator of the SecureGuard® system, access control users are those managed by the operators and can be staff, employees or visitors; anyone needing access to the monitored premise. An access control user in SecureGuard® consists of a name, access card details, fingerprint record, a photo of the user and the user's access permissions as determined by their role or custom settings.

5 SecureGuard® Configuration Tool

The SecureGuard® system requires configuration information that needs to be initially specified by the Administrator. This includes

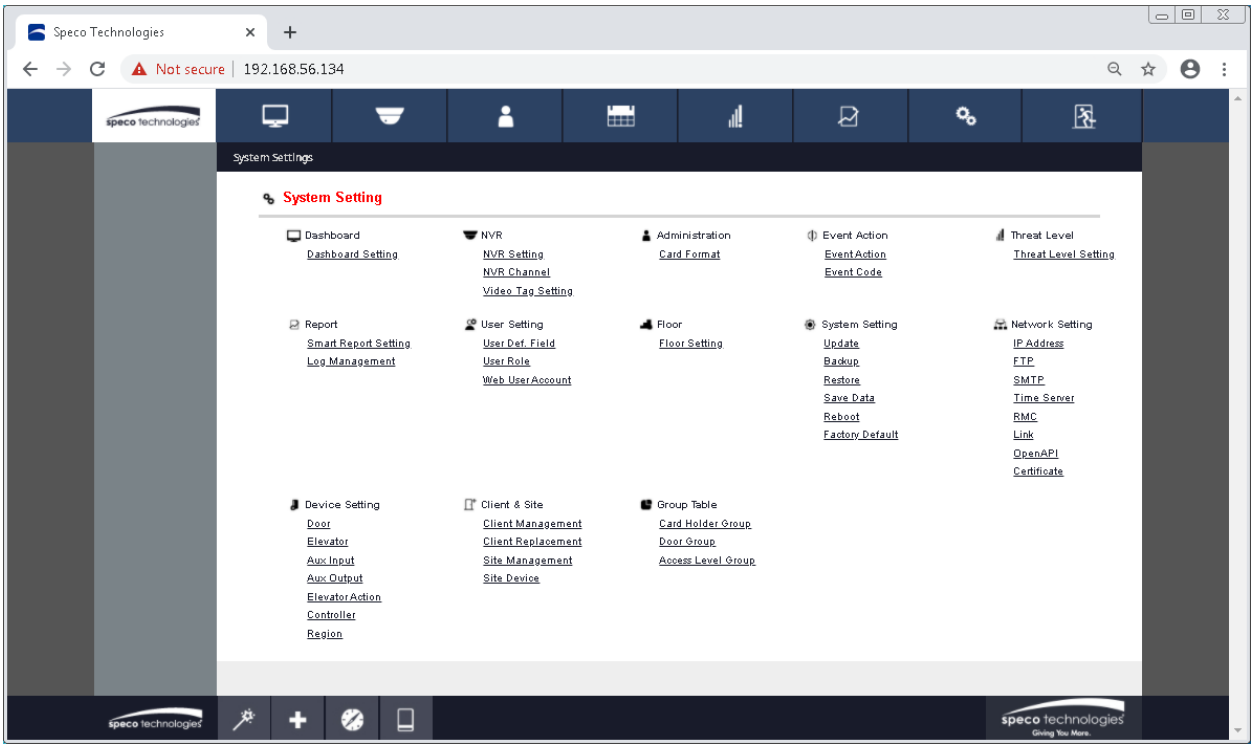
1. Configuration of network settings for communication with access control sites.
2. Individual configuration of Access Control sites
3. User details to add to the access control sites.

6 SecureGuard® Access User Setup

Prior to adding the controller to the SecureGuard® VMS, add a SecureGuard® user via the Speco Access web interface.

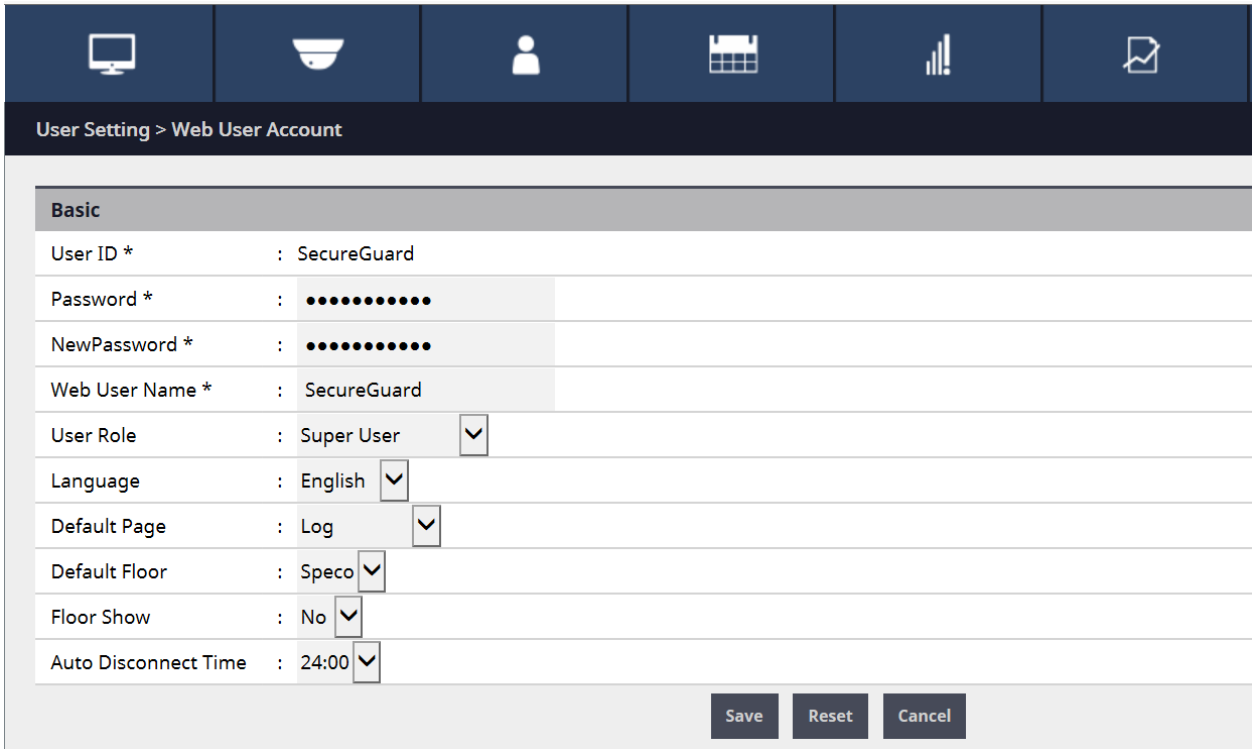
1. Log into the Speco Access web interface with your super admin account.

2. Go to the Settings (gears) tab.



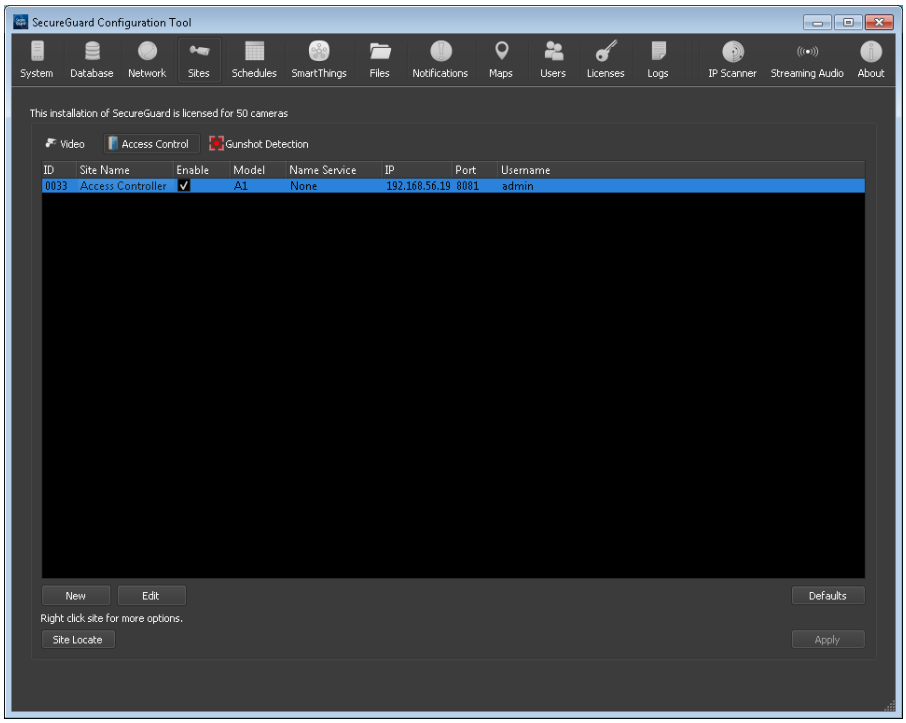
3. Under User Setting, select Web User Account and click "New" to create a new user.

4. For "User Role", select "Super User". For "Language", select "English". For "Auto Disconnect Time", select "24:00". Fill in the remaining fields as desired (remember the password). When you are done your screen should look similar to the image below. Click "Save" to save the SecureGuard® user.



7 Access Control Site Setup

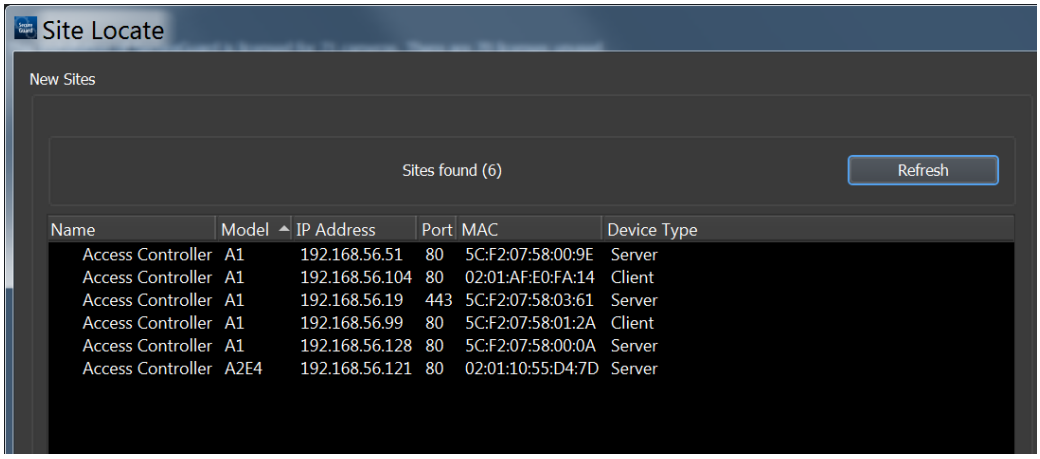
A *site* refers to a DVR, NVR, IP camera or access control devices. Use the Sites dialog to configure connections to these devices. Click the Access Control button (sub-tab) to view access control devices.



The following site operations are available:

7.1 Site Locate

An easy way to locate and add sites for access control devices on your local network is to use the *Site Locate* button. This function helps automate the creation of site objects for local devices. When the Access Control button/sub-tab is selected, pressing Site Locate brings up a dialog as shown below listing only access control devices.



The function scans the local network for access control devices and displays information about these devices in table format. The information includes the name, model, IP address, web port number, MAC address and device type.

Note: if no devices are found, check that the Client and Video Interfaces selected on the Network tab are set to the local area network.

Sites with a "Device Type" of "Server" can be added to SecureGuard by double-clicking the entry. This opens the Site Settings dialog (below) with many of the required entries prefilled. Change the site Name if desired, enter the Username and Password created in the previous section and click "Check Site". If all is correct, you will get a pop-up window with the message "Connection successful". Click "OK".

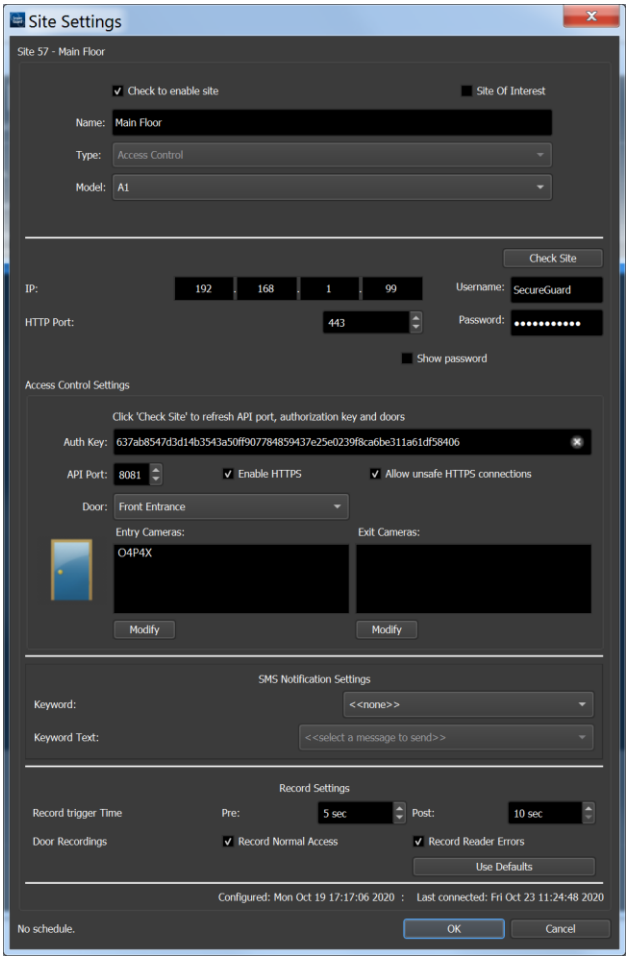
If the site is using HTTPS and you get the error message "Connection refused", you will either need to install the site's SSL certificate on your PC or check the option "Allow unsafe HTTPS connections".

If "Check Site" was successful, the "Authorization Key" and "API Port" fields should now be filled in and the "Door" combo box should contain a list of the names of the doors associated with the site. Click the "Modify" button below the "Entry Cameras" and "Exit Cameras" lists to associate entry and/or exit cameras with the site. Once the site is fully defined, click OK to add the device.

7.2 Site Settings

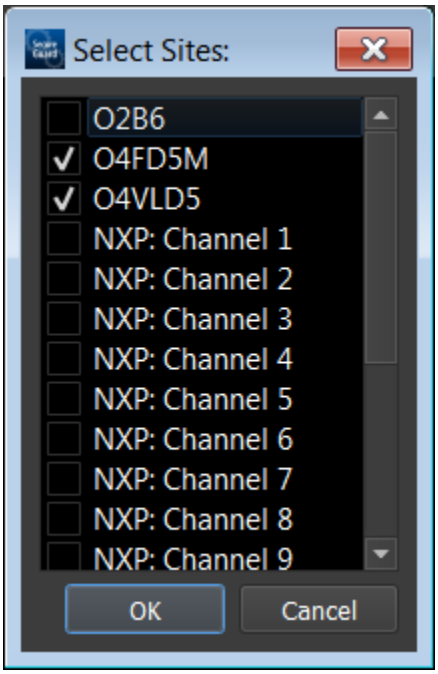
To add a new site or edit a site prefilled using Site Locate, do the following:

1. Click the *New* button (if needed). This opens a Site Settings dialog. Examples of this are shown below. Note: Sites that are chosen to be edited cannot have their *Type* or *Model* changed.

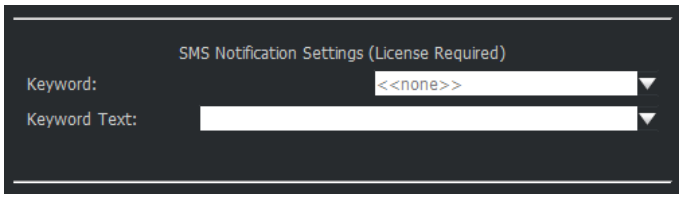


2. In the Site Settings dialog, enter a new name for the site if desired. All site names in the Sites list **must be unique.**
3. All sites are *enabled* by default, initiating communication with SecureGuard®. Deselect this checkbox to prevent SecureGuard® from using this site. Note a disabled access controller will operate as a stand-alone device such that the doors will continue to operate as last configured.
4. Sites may be designated as a *Site of Interest*. This action will prepend a special character to the site name everywhere it is used within the application, making special locations stand out among other sites being monitored.
5. Select the *Model* for the site, if not prefilled. If you do not see the correct model in the list shown, scroll up or down to see additional choices.
6. Enter the site IP address and port
7. Enter the SecureGuard® User login credentials (username and password) that you created from the Speco Access web interface.
8. Enter the Authorization Key (Auth Key) for the controller you are adding. This Auth Key can be found on the controller's web interface under information.
9. If device is connected to multiple doors, select the door number to assign a name and associate entry and exit cameras.
10. Check Disable if the door is not in use.
11. Check Swap In/Out Signals to reverse the direction of the read event signals. This is used if an exit reader is physically wired to the entry junction terminals on the controller (or visa-versa). For example, a bi-directional door can be configured using connections to door 1 and 2 and checking this box for door 2. The signal is used for real-time event logging and recording triggers.

12. Click the ‘Modify’ button below Entry Cameras and Exit Cameras to associate video sites to the access control device. Multiple video sites may be associated to the entry and exit function of the access control device.
13. Click the Check Site button to validate the connection and credentials.



14. When a valid SMS Mass Notification license is installed, the following SMS Notification Settings section will be enabled. SMS notification may be defined on a per site basis. Keyword and Keyword Text information will accompany license. Alarm inputs on the controller can be used to trigger the SMS notification. Note that access events do not currently support SMS notifications.



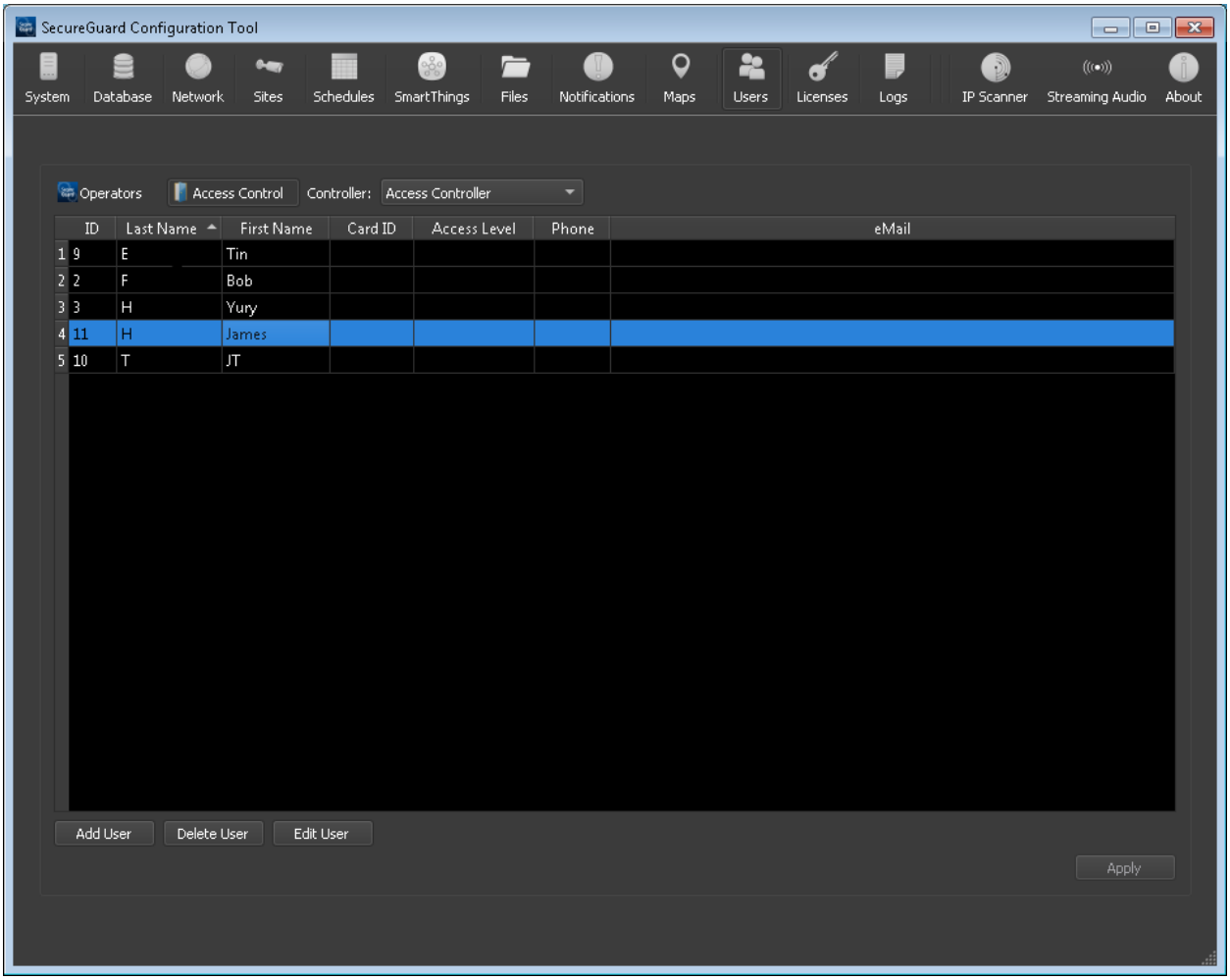
15. *Record Trigger Time* may be set to add a specified number of seconds to both the beginning and end of a system recording.
16. *Door Recordings* are enabled for both normal access (access granted) and reader errors (access denied). Uncheck either checkbox to disable the recording for the corresponding access events.

The following additional functions are available by selecting an access controller site in the Sites tab and clicking the right mouse button:

- *New* - Manually add a controller.
- *Edit* - Update an existing site. Select a site from the sites list and press the Edit button, or double-click on the site to open the Site Settings dialog and make changes to the information.
  Note: *Type* and *Model* cannot be changed when editing.
- *Delete* - A pop-up is displayed to confirm this action.
- *Duplicate* - Within an environment, there may be multiple site entries for the same type of site with slight differences such as Username and password. This function creates a new site item with the same parameters as the original. *Edit* the site to modify any parameters.
- *Rename* - Enter a new name in the location provided. Sites may also be renamed using the *Edit* button.
- *Enable* - Enable/disable site.

8 User & User Access Setup

The list of SecureGuard® access control users and their access permissions in the system is maintained using the Configuration Application on the Users Tab and *Access Control* button/sub-tab.



9 User Management Window

The user window displays the list of access control users, including a unique Identification number assigned to the user, last name, first names, Card ID (credentials), access level, phone number and email address.

10 Adding a new user

To add an access control user to the SecureGuard® system, use the *Add User* button. This will open a dialog as shown below. Enter information in the fields provided then click *OK*. All fields will correspond to user fields configured in your access controller. Please keep in mind modifying the fields in SecureGuard® will update your controller with the new information.