BlueView Access Control Software

Product Detail

October 2023

Intellectual property

Contact

BlueWave LLC
24 21st Street
San Diego, CA 92102

Phone: (760) 929-9596

Technical Support
Online: www.support.bluewavesecurity.com

Sales Offices
Email: Sales@bluewavesecurity.com

Disclaimer

All information contained herein is provided “AS IS.” BlueWave undertakes no obligation to update the information in this publication. BlueWave does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. BlueWave shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Table of Contents

SITES AND AREAS

Overview

Sites - Sites are simply names used to organize and identify physical locations for the BlueWave system. Sites are typically used to identify a particular facility such as "San Diego Sales Office" or "Store 78290" or "Chemistry Building." There can be multiple Sites within a BlueWave system associated with the Company Name. Permissions can be granted on a Site basis. The system comes configured with a default Site named "My Site."

Areas - Sites are subdivided into Areas. Areas are simply names used to organize specific groups of doors. Areas can be physical names such as "1st floor" or logical names such as "Chemistry Department." There can be multiple Areas within each site. Permissions can be granted on an Area basis. The system comes configured with a default Area named "My Area."

Configuring Sites and Areas

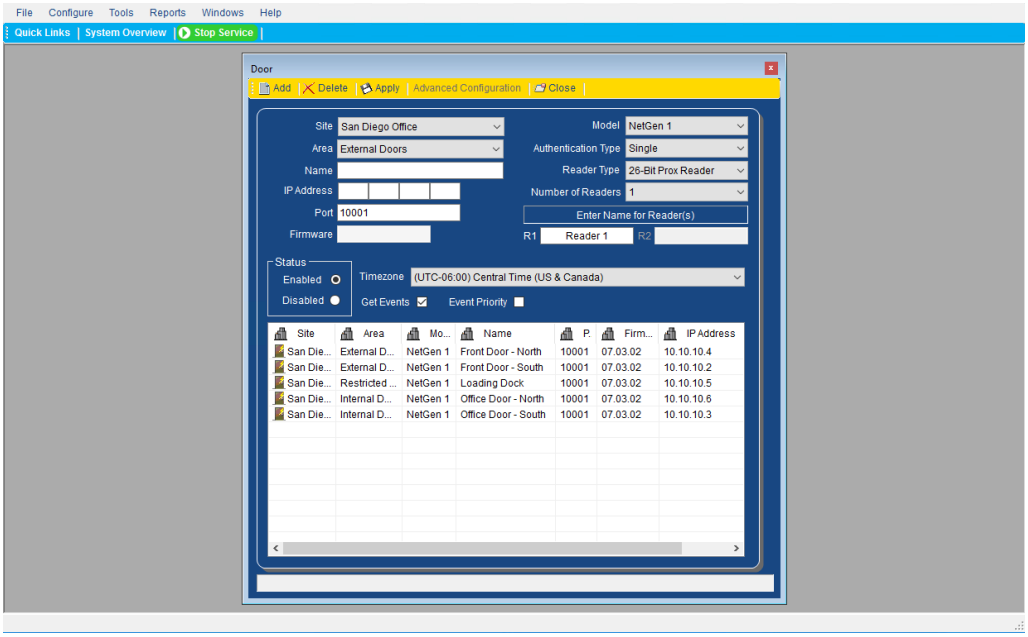
Sites - To change the name of the default site name, click on the Configure menu and select Site. Click on the "My Site" default entry in the Display Site column. In the Site text box on the menu bar, enter the desired name for the Site. Click the "Apply" button to save the new Site name. Enter as many Sites as needed. Click the "Close"button to exit the dialog.

To add a new site, enter the name into the Site box at the top and click Add.
To delete a site click on its name then click Delete at the top. Click Yes to confirm.
To update a site click on its name, edit the name in the Site box and click Save at the top.

Areas - To change the name of the default Area, click on the Configure menu and select Area. Click on the "MyArea" default entry in the Display Area column. In the Area text box on the menu bar, enter the desired name for the Area. Click the "Apply" button to save the new Area name. Enter as many Areas as needed. Click the "Close" button to exit the dialog.

To add a new Area, enter the name into the Area box at the top and click Add.
To delete an Area click on its name then click Delete at the top. Click Yes to confirm.
To update an Area click on its name, edit the name in the Area box and click Save at the top.

DOORS



Screenshot 1: The Door menu for the BlueWave office

Overview

From the Door menu, an administrator can add, edit, delete, and monitor any given door within the system.

Adding a Door to the System

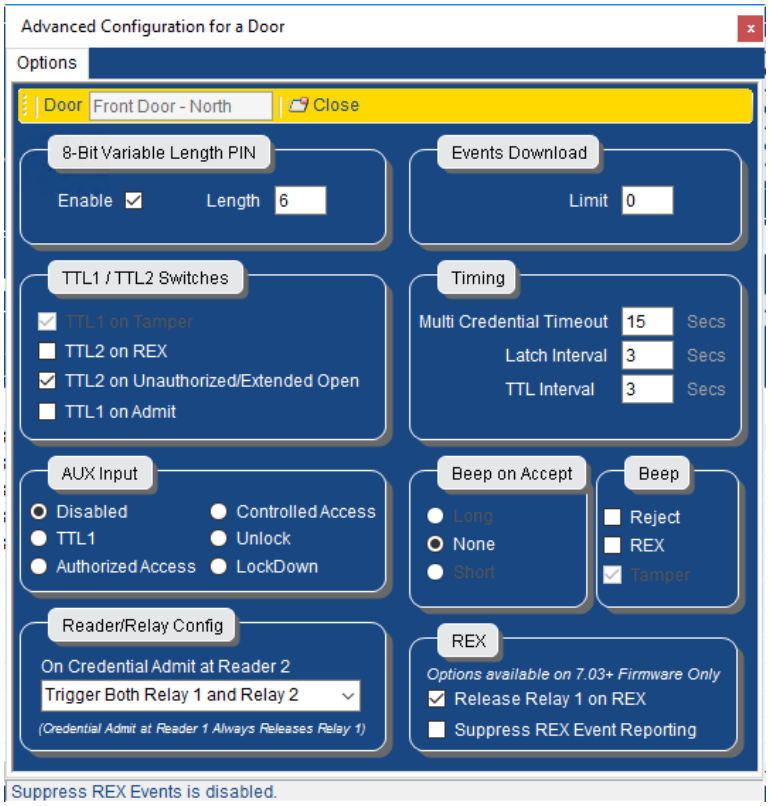
To add a door, enter its Name and IP Address. You can change the port from 10001, if needed. The port should only be changed if you have already changed the port in the Lantronix module on the controller. Select the appropriate Site, Area, Model, Authentication Type, Reader Type, Number of Readers, and Timezone from the drop-down boxes, then click Add.

Editing/Deleting a Door

To change a door you can click on it in the grid, edit the fields as appropriate then click Apply.
To delete a door, click on its name, then Delete then Yes to confirm. For Advanced Configuration, see our Configuration Guide.

Advanced Configuration

The screen below lets you configure the advanced settings of a door controller. The table below outlines the definition of all of the advanced options. Available options may vary based on door controller hardware and firmware versions.



8-Bit Variable Length PIN - If an 8-bit burst PIN pad is installed at the door, this setting defines how many PIN digits the controller will look for. Example: For a 7-digit PIN, check Enable and set Length to 7.

Events Download Limit - How many audit events from the controller to download at a time. "0" means continue downloading events until there are no more events left.

Timing - These options configure the timing for certain events at the door.

Latch Interval - This is the default latch interval for the controller. This is how long the controller will remain unlocked when a valid card is presented.

Multi Credential Timeout - Defines how long to wait for the second credential when the first of a multi authentication credential set is presented.

TTL Interval - How long to hold TTL when it is triggered. (Available in FW 7.03 or higher.)

TTL1/TTL2 Switches
The controllers have two output signals, TTL1 and TTL2. These are normally held high at 5 volts when they are not activated. When they are activated, they drop to zero volts. They are frequently tied into alarm systems.

TTL2 on REX - The TTL2 on REX setting will cause the TTL2 signal to be activated if a REX signal is detected.

TTL2 on Unauthorized Open - Active TTL2 signal if an Unauthorized Open Alarm is activated.

TL1 on Admit - Activate TTL1 if a card read results in an Admit.

Beep

- *Beep on Reject* - The controller will beep when a card without permissions is presented.
- *Beep on REX* - The controller will beep when a REX device, such as a button, is pressed.

Beep on Accept

- *None* - the board will remain silent upon accepting a credential.
- *Long* - the board will let out a single, long beep upon accepting a credential.
- Short - the board will let out a single, short beep upon accepting a credential.

AUX Input

- *Disable* - AUX input signal is ignored.
- *TTL1* - Activate the TTL1 signal when AUX input is detected.
- *Authorized Access* - The controller will unlock for the latch interval.
- *Controlled Access* - The controller will unlock for the latch interval if the AUX card number is assigned to a currently valid shift.
- *Unlock* - The controller will toggle between Normal (Locked) mode and Unlock mode when an AUX input is detected.
- *LockDown* - The controller will toggle between Normal (Locked) mode and LockDown mode when an AUX input is detected.

Reader/Relay Config - This option configures what happens when a Credential Admit event occurs at Reader 2.

- *Trigger Both Relay 1 and Relay 2* (DEFAULT)
- *Trigger Relay 1* - will release hardware wired to relay 1.
- *Trigger Relay 2* - will release hardware wired to relay 2.
- *Trigger Neither Relay* - will do nothing.

REX Options - This option configures what happens when a REX device is triggered.

- *Release Relay on REX* - Uncheck to prevent Relay 1 from releasing on a REX event.
- *Suppress REX Event Reporting* - Check to prevent the door controller from sending back REX events to the software.

CARD HOLDER

Overview

This is where you define a person and their assigned credentials.

How to Add/Delete/Edit a Card Holder

To define a Card Holder, enter their first name, last name, optionally enter Employee ID, Email, Cell Phone and select an image, then click Add.

To delete a Card Holder click on their name then Delete, click Yes to confirm.

To update a Card Holder click on their name, edit the fields as appropriate and click Save. By selecting a Card Holder you can see all of the cards assigned to them.

How to Add a Credential to a Card Holder

To add a credential to a person's profile, search for and select their name in the table. Once the person's name is highlighted, click on 'Add/Search Credentials' at the top of the menu. Our system is designed to allow for many credential types with a flexible set of permission types. Enter the card number and facility code, or PIN.

Status - Only Active credentials belonging to Active cardholders will work at a door. All other credential types (Inactive, Lost, Stolen, Suspended, Expired) are for descriptive purposes only.

Effective Start Date - When the BlueView software detects that the Effective Start Date for a credential has passed, the credential's status will be automatically changed to Active, and the affected doors will be automatically updated. If the Immediate box is checked, the software will not automatically change the credential status. If this is checked, or the status is manually set to Active, then the credential will be effective at the door after the next door update.

Expiration Date - When the BlueView software detects that the Expiration Date has passed, the credential's status will be automatically changed to Expired, and the affected doors will be automatically updated. If the Never box is checked, the software will not automatically change the credential status. If the status is manually set to Active, then the credential will continue to work at the door until the credential status, cardholder status, or permissions change such that the credential is no longer valid.

Note: The Effective Start Date and Expiration Date functionality for credentials relies on the Bluelink Network Service (BNS) running on the server and reliable network communication between the server and the door controllers. The start and end times are not exact - there may be a delay of up to several minutes from the specified start or end time to when the change is effective at the door controller. The size of the delay will depend on how many controllers are being managed by the software and other configuration-specific factors. For this reason, the software will only let you set start and end times to the nearest hour.

Dual Authentication

If you wish to use dual authentication you can check the Dual Authentication box and enter the second credential. Both credentials must be of the same Credential Type. One exception to this is that 26 Bit Prox Card and 26 Bit PIN can be used together, because they have the same underlying bit format.

When a cardholder has Dual Authentication enabled for their credential, at Doors that have their Authentication Type set to Dual, the cardholder must present both credentials in order (Credential 1, followed by Credential 2) within the Dual Authentication Timeout period (see Advanced Door Configuration), which is 15 seconds by default. At Doors that have their Authentication Type set to Single, the cardholder will only need to present Credential 1.

Credential Types and Modes

Our accepted credential types include: 22 bit PIN, 26 bit PIN, 26 bit prox card, 34 bit prox card, 4 digit Indala keypad, 8-bit variable length PIN, iClass 35 bit prox card.

Our system allows for flexible permission types on a credential. These are the credential modes:

Normal - A normal credential will allow passage through a door, if the cardholder is configured for access to that door at that time.

Lockdown/Unlock - These credentials are known as Mode Cards, which will cause the controller to change its mode upon presentation of the credential. If the credential is presented a second time the controller returns to its previous mode. When the door is in Unlock Mode, the door is unlatched and anyone may enter without presenting a credential. When the door is in Lockdown Mode, the door will ignore all credentials except another Lockdown credential or a Master credential, even if the credential would otherwise be authorized for the door at this time.

Manager/Managed - Manager and Managed credentials are used with a special Manager shift type. When this type of shift is in effect, a cardholder assigned a Managed credential will be denied passage through the door until a cardholder with a Manager credential has arrived and presented their credential to the reader.

Master - A master credential works at ALL doors configured in the system, regardless of permission or shift. This is the only credential that will work when a door is in Lockdown Mode.

GROUPS

From the *Configure* menu, select *Group*. This is where you define a group of *People* that should have the same *Permissions*. Enter the name for your group in the *Group* text entry field. Click *Add* to add the new group. Add more Groups if needed. To delete a group, click on its name then *Delete* and confirm. To update a group, click on its name, edit the name in the Group box and click *Apply*. Click the *Close* button to return to the *System Overview* dialog.

GROUP MEMBERS

From the *Configure* menu, select *Group Member*. Group Member is where you assign *People* to a *Group*. Select the group you wish to assign members to from the drop down box. To assign a member to a group, click their name, then click *Add*. To remove a member from a group click their name then click *Remove*. Use *Shift* or *Ctrl* to select multiple cardholders. Click the *Close* button to return to the *System Overview* dialog.

SHIFTS

The *Shift* screen is where you define the begin, end and applicable days for a shift. From the *Configure* menu, select *Shift*. The process is simple once you know the definitions of the shift types and exceptions.

1. Type a name for the shift into the Name text entry field.
2. Click the desired days of the week for this shift.
3. Set a Start and End time for the shift.
4. Click the Add button.

Add as many Shifts as needed. Click the Close button to return to the System Overview dialog.

Shift Types

Normal - Door will be released on a valid card read. Door will relock after the latch interval (3 seconds by default, configurable from the Doors screen under Advanced Configuration)

Unlock - Door will unlock at the shift start time and stay unlocked until the shift end time.

Unlock with a Card - The door will remain locked at the start of this shift until a person assigned to this shift presents their credential. Upon presentation of a valid credential, after the shift start time, the door will unlock and stay unlocked until the shift end time.

Toggle with a Card - The door will remain locked at the start of this shift until a person assigned to this shift presents their credential. Upon presentation of a valid credential, after the shift start time, the door will unlock and stay unlocked until the card is presented again. Each time the card is presented the door will toggle between locked and unlocked. At the shift end time, if the door is unlocked, it will return to locked mode.

Manager - This shift works with 2 credential modes (Manager and Managed). During the specified shift hours, the Managed credentials will not work until a Manager credential is first presented. Manager and Managed credential modes are configured from the Cardholders screen, via the Add/Search Credentials button.

Applies To: Definitions

Normal - This shift will be valid on Normal days ONLY. A Normal day is any day that is NOT defined as an Exception day by defining an Exception on the Exceptions tab of the Shift screen, and associating it with the door on the Cardholder Permissions screen, Exceptions tab.

Exception - This shift will be valid on Exception days ONLY. An Exception day (also known as a Holiday) is defined by creating an Exception on the Exceptions tab of the Shift screen, and associating it with the door on the Cardholder Permissions screen, Exceptions tab.

Both - This shift will be valid on Both Normal days AND Exception days.

Exceptions/Holidays

Please note that only unlock schedules can be adjusted from the web application. If you need to make permanent changes to your door's standard unlock or temporary changes to other types of schedules, follow the Configuring Cardholder Permissions Guide to adjust from the software. For current door status and to make any immediate changes to your door's schedule, go to the *Doors* screen. To set schedules for days in the future, go to the *Holidays* screen. Holidays or 'Exceptions' can be scheduled up to one week in advance.

In BlueView, the term "Exception" is used to describe a day where the controller operates differently than normal. The most common example of an exception day is a holiday (4th of July, Thanksgiving, Christmas), although it's also useful for sale days, inclement weather days, etc.

This article assumes that your BlueView system has already been configured for Normal operation, meaning the way it should operate on any non-exception day. Before proceeding, you will need to have the following information available:

The date and weekday of the exception day
The hours and type of shift(s) that you want to happen on that day, if any
The set of doors that will need to behave differently on the exception day

Note: If there are certain Normal (non-exception) shifts that you want to occur regardless of whether or not a given day is an exception day, make sure that those shifts are marked as "Applies To: Both" in the Shifts screen. For example: A door's normal operation is to allow employees with valid credentials to access the door from 7 AM to 7 PM. The door also unlocks during business hours, from 8 AM to 5 PM. On holidays, the administrator wants the door to remain locked all day, but still allow credentialed employees to have access within the usual window. In this case, the 7 AM to 7 PM shift will need to be marked as "Applies To: Both" and the 8 AM to 5 PM Unlock shift will need to be marked as "Applies To: Normal." Then, proceed with the rest of the exception day setup.

Exception Day - This is the date that you want your doors to do something different than normal.

Exception Shift (Optional) - This shift defines what you want your door to do on the Exception Day. If no exception shift is defined, the door will simply NOT do whatever it normally does. (Typically, the result is that admission is denied to everyone.)

Exception Day Permission - This tells the system which doors you want to be affected by the Exception Day.

Exception Shift Permission (Optional) - This permission tells the system which doors you want to use the Exception Shift on the Exception Day. If you have not defined an Exception Shift, this permission is unnecessary.

The first question that needs to be addressed is what do you want the door to do on the given exception day. If you simply want it to NOT do what it normally does, then no Exception Shift or Exception Shift Permission is required. A door that has an Exception Day defined but no associated Exception Shift will ignore any shifts marked as "Applies To: Normal" and execute any shifts marked as "Applies To: Both." If you want the door to do something DIFFERENTLY than normal, you will need to additionally define the Exception Shift and Exception Shift Permission.
Configure Exception Shifts (Holiday Shifts)

In Exceptions you define special calendar dates that require different shift programming than normal.
To define an exception, enter its name and the date, then click Add. To delete an exception click on its name then Delete , click Yes to confirm. To update an exception click on its name, edit the name and/or other fields as appropriate and click Save.

Exception Shifts are shifts that are scheduled for special days when a customer does not want a given portal to have normal behavior. So for example if a user has defined an unlock shift that operates from Monday thru Friday 8am-5pm for a given set of doors and they have programmed a shift exception to occur on Friday July 4th. The resulting behavior for the doors on the exception day will be whatever the shift exception that has been defined for that day.

Users can configure up to 64 shift exception dates and define a single exception shift that will dictate how the controller is to operate on the configured exception dates.
Configuring multiple types of shifts can only be accomplished by programming the shifts for the first holiday and then going back and updating the exception shift after the first exception date. So for example if a user wants the doors that are normally unlocked from 8-5 M-F to be locked on July 4th and they want them to unlock on a shorter shift from 8-12 on Labor Day. They would configure the first exception shift to be a normal exception shift for 8-5. Then after the July 4th exception date passes and before the next exception date they will change the exception shift time and type and type parameters.

CARD HOLDER PERMISSIONS

Configuration

From the Configure menu, select Card Holder Permissions. When setting up a simple system, the 24x7 shift, the All group and the Company target may be sufficient to allow all card holders to have access through all doors at all times. However, if access needs to be restricted to ANY door in the system, the permission 24x7/All/Company should not be used, as it will override any other permissions. When creating permissions, be sure that your sites, areas, and doors are all organized in a way that allows easy separation of access.

Creating permissions on this table is telling the system WHO (Group) has access to WHERE (Company/Site/Area/Door) and WHEN (Shift). Using the drop-down menus at the top of the dialog, select a Shift, Group, and Target. Click the Add button to add to the List of Permissions. Once you have entered all of the permissions, you can update the door controllers by clicking the Activation tab. If you have programmed exceptions to the normal shift patterns you must choose which doors to apply them to using the Exceptions tab.

Note: If you select a Shift that is of type Unlock then you will not be able to select a Group as cards are not relevant for this type of shift. The dropdown box will be disabled when creating the permission.

Exceptions

To define an exception permission, select an exception and a target set of controllers, then click Add. To delete an exception permission click on its name then Delete and confirm. To update an exception permission click on it then select different values as appropriate and click Save. Once you have entered all of the exception permissions, you can update the door controllers by clicking the Activation tab.

Activation

From here you can update your door controllers with the latest permissions you have added. Before you activate your permissions please ensure you have configured all the required permissions for a controller.

To activate the card holder permissions for a door, click the checkbox next to a door, and then click on Activate Now. You can select multiple doors or use the Select All checkbox to update the full list. The rows for each selected door controller will change to orange with a Door Status of Queued. The programming of the controllers is complete when the rows of all selected doors turn green, with a status of Successful. This can take anywhere from a few seconds to several minutes, depending on the number of credentials in your system and the speed of your network. In our most recent version of BlueView, your system will be able to update multiple controllers at once, speeding up this process.

To view the credentials that have been sent to each door, select the appropriate row on the left side of the screen, and the credentials sent to that door will appear in the middle Permissions Sent pane on the right.
Cardholder permissions activations are handled in the background by Bluelink Network Services, so you do not need to leave the Permissions Activation screen open while they are being processed.

DISCOVER DOOR CONTROLLERS

In BlueView, navigate to Tools > Discover Door Controllers, a window will appear.

Use the dropdown to select your local network, then click on “Discover Door Controllers”. A list of devices will show up, which will be identified by controller type and MAC address.

For controllers on the list that do not have a static IP address, you will need to note their current IP address and enter that into any web browser. This should cause a login window to appear as seen below.

BATCHLOAD CARDS

This feature allows you to add a set of credentials with users quickly and easily. The credentials must be in numerical order and have the same Facility/Site Code.

Model -The model of the door controller that these credentials will be used for. Most users will leave the default NetGen 1

Credential Type - The type of credential that will be imported.

Group - If checked, the new cardholders will be assigned to the selected Group, in addition to the All group. (All cardholders in BlueView are assigned to the All group, regardless of whether the box is checked.)

Name - The cardholders created by this tool will have a blank first name and a last name that consists of the text input in this box plus the card or pin number assigned to that cardholder.

Facility Code - This is the Facility or Site Code for the cards assigned to this batch. (Credential types that do not need this will have this box grayed out.)

Start/End Card Number and Start/End Pin Number - Which of these options are enabled depends on the Credential Type selection. The Start Card number will be the first credential loaded in the batch. After that, credentials will be loaded sequentially until the credential selected as the End Card or Pin Number is reached.

After all parameters have been input, click OK to load the batch of credentials. A box will pop up with a success message when the load is complete. Open the Cardholders screen to verify the new cardholders and their credentials.

IMPORT

Groups / People / Cards

This feature allows you to import a set of people and their credentials from a file quickly and easily. The file must have a txt or csv extension and contain comma separated values. There is a easy sample file at the end of this page. In BlueView, go to the Tools menu. Choose Import, then Groups/People/Cards.

1. Click Generate to create a spreadsheet template. BlueView will ask where you would like to save the template file. Once the template file has been saved, BlueView will attempt to open the template file for editing using a spreadsheet editor on your computer, such as Microsoft Excel or Apache OpenOffice. (Spreadsheet editors are not provided with BlueView.) Alternatively, the template file can be edited in text format using Notepad or a similar program.

Note: Alternate Option: ***Another option is to export your existing BlueView groups/people/cards to use as a template. Choose Reports from the BlueView main menu. Select "System Export" as the Report Type, then "Groups/People/Credentials" as the Export Type, and click Get Report. To save the output, click on File, then Export and choose a name for the csv file.***

2. Edit the file to remove the example data and add your data for import into BlueView. Be sure to leave the first row populated with the column headings:

Column A: *GroupName*
Column B: *FirstName*
Column C: *LastName*
Column D: *EmployeeID*
Column E: *CardNumberPIN*
Column F: *FacilityCode*
Column G: *CredentialType*
Column H: *CredentialMode*
Column I: *CredentialStatus*
Column J: *CredentialStartDate*
Column K: *CredentialExpirationDate*

Data Descriptions

GroupName - The group name (or comma-separated list of group names) that the person should be added to in BlueView. Group names that do not match an existing group in BlueView will be used to create new BlueView groups. If left blank, the person will be added to the built-in All group only. Each group name must be 50 characters or less.

FirstName - First name of the cardholder. Must be 50 characters or less.

LastName - Last name of the cardholder. Must be 50 characters or less. Required Field.

EmployeeID - Must be 20 characters or less.

Note: If populated, it must be unique across all cardholders, including both those in the import spreadsheet and in the existing BlueView database UNLESS the checkbox to "Allow duplicate Employee IDs" is checked. In that case, any rows that have a duplicate Employee ID, either in the spreadsheet or in the existing BlueView database, will be interpreted as updates to the original record with that Employee ID. Updates will only ADD credentials and/or group memberships, not remove or replace any previously assigned groups or credentials.

CardNumberPIN - Should be completed with either the card number or the pin number credential to be assigned to the person. Numbers only - limits are subject to the credential type specified. Combined with the Facility Code, it must be unique across all people records, including both those in the import spreadsheet and in the existing BlueView database. Only one credential per person can be imported.

FacilityCode - Card number credentials require a corresponding Facility Code. This number may be determined from the documentation that came with the cards, or by swiping the card at a BlueWave door and checking the reports for the resulting Card Number and Facility Code.

CredentialType - Choose from the following values for the credential type field, which describes the type of credential that will be assigned to the person: 26-BIT, 34-BIT, 35-BIT, 8-BIT PIN.

CredentialMode - Choose from the following values for the credential mode field, which describes the behavior of the credential that will be assigned to the person: Normal, Lockdown, Unlock, Managed, Manager, Master. If left blank, this field will default to Normal.

CredentialStatus - Choose from the following values for the credential status field: Active, Inactive, Expired, Suspended, Lost, Stolen. If left blank, this field will default to Active.
CredentialStartDate - This field indicates when the credential status should become Active. If left blank, the credential will become Active immediately.

CredentialExpirationDate - This field indicates when the credential should expire. If left blank, the credential will never expire.

Note for Dates: The recommended format is "mm/dd/yyyy hh:mm xm" to the nearest hour. For example, "11/27/2017 05:00 PM".

Duplicates - This tool is designed primarily for use in system commissioning and initial data entry. BlueView assumes each row in the spreadsheet is a new person to be inserted in the database. It does not try to match people by first and last name for either validation or input, because a person's first and last name cannot generally be relied upon to be a unique identifier for that person. Therefore, attempting to import "John Smith" into BlueView when a "John Smith" already exists in BlueView will result in duplicate cardholders being created.

To use the import tool to update existing cardholder records with new groups and/or credentials, there MUST be an Employee ID used in both the spreadsheet and in the existing BlueView database so that the software can match the records. In the event that a record is matched for update rather than insert, note that new groups and

credentials found in the spreadsheet will be added to the person's record, but existing groups and credentials will NOT be removed automatically.

From the spreadsheet software, save the newly populated spreadsheet as a .csv (comma-separated values) file. If opened in Notepad or another text editor, the contents of the resulting file should look similar in format to the text below:

GroupName,FirstName,LastName,EmployeeID,CardNumberPIN,FacilityCode,CredentialType,CredentialMode,Credentialstatus,CredentialStartDate,CredentialExpirationDate
,Joe,Brown,1,14557,120,26-BIT,Normal,Active,,
Management,Mary,Brown,2,1234567,,8-BIT-PIN,Master,,07/20/2017 05:00 PM,07/20/2018 05:00 PM
"Management, Overnight",Bob,Brown,3,14559,120,26-BIT,Normal,Active,,

<u>Notes on Legacy Format:</u> Files exported from BlueView 16 will only contain the first 7 columns described above. The import utility will allow import of these legacy files. The software will warn that the incorrect number of columns was detected, but it will proceed to import the records, setting the additional fields to their default values.

3. Select the file you just edited by clicking the Browse button in the Import screen in BlueView, then click Validate to validate your file for import.

Troubleshooting Steps:

A. You may need to close the spreadsheet editor, if it still has the file open.

B. If the validation reports errors, go back to the spreadsheet editor to make corrections and then try again.

C. If the validation reports an incorrect number of columns, make sure that the first row of your spreadsheet contains the column names to match the spreadsheet template.

D. If the validation reports duplicate Employee IDs, and the intent was for the import to update the matching records, check the checkbox next to "Allow duplicate Employee IDs" and try the validation again.

E. If you're having trouble and do not need to specify CredentialMode, CredentialStatus, and Credential Start/Expiring Dates, these columns can be left off completely, and their values will be set to defaults as described above.

4. Once the import file has been validated, click Import to import the data into BlueView. Progress will display in the status box at the bottom of the screen. When the import is complete, you can verify the import by checking for the new records in BlueView under Configure->Cardholders.
Please be aware that if you are importing a large number of records (> 10,000), the import may take a long time. Please be patient, or else break up the data into several smaller .csv files.

Doors

This feature allows you to import a list of doors from a file quickly and easily. The file must have a txt or csv extension and contain comma separated values.

In BlueView, go to the Tools menu. Choose Import, then Doors.

1. Click Generate to create a spreadsheet template. BlueView will ask where you would like to save the template file. Once the template file has been saved, BlueView will attempt to open the template file for editing using a spreadsheet editor on your computer, such as Microsoft Excel or Apache OpenOffice. (Spreadsheet editors are not provided with BlueView.) Alternatively, the template file can be edited in text format using Notepad or similar.

***Note: Alternate Option:** Another option is to export your existing BlueView doors to use as a template. Choose Reports from the BlueView main menu. Select "System Export" as the Report Type, then "Doors" as the Export Type, and click Get Report. To save the output, click on File, then Export and choose a name for the csv file.*

2. Edit the file to remove the example data and add your data for import into BlueView.

Column A: *Site*
Column B: *Area*
Column C: *DoorName*
Column D: *IPAddress*

Data Descriptions:

Site - Site name under which the Door will be stored in BlueView. Must be 50 characters or less.

Area - Area name under which the Door will be stored in BlueView. Must be 50 characters or less.

DoorName - Name to use for the Door in the BlueView software. For larger systems, it is useful to prepend door names with abbreviations for the Site and Area under which it falls, in order to more easily identify the door in all screens. Must be 50 characters or less.

IP Address - The IP address that will be used to communicate with the controller at this Door.

***Note** The process to assign IP Addresses to NetGen controllers is separate from the process of importing the IP addresses into the software using this tool. Please refer to the document for more information about setting controller IP addresses.*

All columns must be populated. From the spreadsheet software, save the newly populated spreadsheet as a .csv (comma-separated values) file. If opened in Notepad or another text editor, the contents of the resulting file should look similar in format to the text below:

Site,Area,DoorName,IPAddress
Example Site,Example Area 1,Front Door,192.168.0.10
Example Site,Example Area 2,Back Door,192.168.0.11
Example Site,Example Area 2,Side Door,192.168.0.12

3. Select the file you just edited by clicking the Browse button in the Import Doors screen in BlueView, then click Validate to validate your file for import.

Troubleshooting Steps:

A. You may need to close the spreadsheet editor, if it still has the file open.

B. If the validation reports errors, go back to the spreadsheet editor to make corrections and then try again.

4. Once the import file has been validated, click Import to import the data into BlueView. Progress will display in the status box at the bottom of the screen. When the import is complete, you can verify the import by checking for the new records in BlueView under Configure->Door.

Shifts

This feature allows you to import a list of shifts from a file quickly and easily. The file must have a txt or csv extension and contain comma separated values.

In BlueView, go to the Tools menu. Choose Import, then Shifts.

1. Click Generate to create a spreadsheet template. BlueView will ask where you would like to save the template file. Once the template file has been saved, BlueView will attempt to open the template file for editing using a spreadsheet editor on your computer, such as Microsoft Excel or Apache OpenOffice. (Spreadsheet editors are not provided with BlueView.) Alternatively, the template file can be edited in text format using Notepad or similar.

***Note: Alternate Option:** Another option is to export your existing BlueWave doors to use as a template. Choose Reports from the BlueView main menu. Select "System Export" as the report type, then "Shifts" as the Export Type, and click Get Report. To save the output, click on File, then Export and choose a name for the csv file. 2. Edit the file to remove the example data and add your data for import into BlueView.*

Column A: *ShiftName*
Column B: *ShiftType*
Column C: *ShiftAppliesTo*
Column D: *SU*
Column E: *M*
Column F: *TU*
Column G: *W*
Column H: *TH*
Column I: *F*
Column J: *SA*
Column K: *StartTime*
Column L: *EndTime*

Definitions:

ShiftName - The name of the Shift. Each ShiftName specified must be unique across both the spreadsheet for import and any existing shifts in the BlueView system. Must be 50 characters or less.

ShiftType - The shift type defines how the shift will operate. Options are Normal, Unlock, Unlock with a Card, Toggle with a Card, Manager.

ShiftAppliesTo - Defines whether this is a holiday or regular shift. Options are Normal, Exception, or Both.

ShiftDays(SU, M, TU, W, TH, F, SA) - These columns indicate on which days of the week this shift will be valid. Place an 'x' or an 'X' in the appropriate column if the shift will be active on that day of the week, and leave the column blank if the shift will NOT be active that day.

StartTime/EndTime - These columns specify the start and end time for the shift. The recommended time format is HH:mm:ss AM/PM (ie, 12:00:00 AM).

***Note:* Shifts cannot cross the midnight boundary - if such a shift is required, it should be split into two separate shifts. For example, a 10 PM to 4 AM shift should be specified as two shifts, one from 10:00:00 PM to 11:59:59 PM, and another from 12:00:00 AM to 4:00:00 AM.**

From the spreadsheet software, save the newly populated spreadsheet as a .csv (comma-separated values) file. If opened in Notepad or another text editor, the contents of the resulting file should look similar in format to the text below:

ShiftName,ShiftType,ShiftAppliesTo,SU,M,TU,W,TH,F,SA,StartTime,EndTime

M-F 8-5,Unlock,Normal,,x,x,x,x,x,,08:00:00 AM,05:00:00 PM
24x7,Normal,Normal,x,x,x,x,x,x,x,12:00:00 AM,11:59:59 PM
M-F 8-5 M,Manager,Both,,x,x,x,x,x,,08:00:00 AM,05:00:00 PM
M-F 8-5 UwC,Unlock With a Card,Both,,x,x,x,x,x,,08:00:00 AM,05:00:00 PM
M-F 8-5 TwC,Toggle With a Card,Both,,x,x,x,x,x,,08:00:00 AM,05:00:00 PM

3. Select the file you just edited by clicking the Browse button in the Import Doors screen in BlueView, then click Validate to validate your file for import.

Troubleshooting Steps:

A. You may need to close the spreadsheet editor, if it still has the file open.

B. If the validation reports errors, go back to the spreadsheet editor to make corrections and then try again.

4. Once the import file has been validated, click Import to import the data into BlueView. Progress will display in the status box at the bottom of the screen. When the import is complete, you can verify the import by checking for the new records in BlueView under Configure->Door.

LOGIN ADMINISTRATION

Overview

This form allows you to add, update and delete Logins for the BlueView software. These same logins are also used in the BlueWave web interface.

Login

To add a new BlueView user/login:

1. Type a User Name
2. Type a Password, then confirm the Password in the Confirm box.
3. Choose the associated BlueView Card Holder. If the new User is not already a BlueView cardholder, click the Add a User button to open the Cardholders screen.
4. Select a Login Role (see Role below for more information).
5. Click Add to add the new login.

To update an existing user/login:

1. Select the login from the table
2. Make any necessary changes to the User Name, Password (you will be asked to re-type the password in the Confirm box, if changed), Card Holder or Role
3. Click Apply to save your changes

To delete a login:

1. Select the login from the table
2. Click Delete to delete the login

Role

Login Roles define what a user is able to do within BlueView. Built-in Login Roles are as follows (these roles cannot be modified or deleted):

Administrator

A. Full access to all doors, groups, and shifts in BlueView, and the ability to perform any task in BlueView.
Monitor

B. Read-only access for all doors, groups, and shifts in BlueView (the user can view but not make changes), and the ability to run reports.

Operations

A. Read-only access for all doors, groups, and shifts in BlueView (the user can view but not make changes), and the ability to run reports, activate permissions, and send door override commands.
B.

To add a new login role (available in Professional and Enterprise editions only):

1. Type a Name for the Login Role

2. Click Add to add the login role with default role permissions

3. Click Set Role Permissions to choose which role permissions to assign to the role. Use the arrows to move selected role permissions between the Available Role Permissions and Current Role Permissions column.

4. Close the Role Permissions window when done

To update a login role:

1. Select an existing Role from the list

2. Click Set Role Permissions to choose which role permissions to assign to the role. Use the arrows to move selected role permissions between the Available Role Permissions and Current Role Permissions column.
3. Close the Role Permissions window when done (changes are saved as you go)

To delete a login role:

1. Select an existing Role from the list

2. Click Delete to delete the login role

Login Role Permissions

Read - Read-Only access. This login cannot make any changes to the system (this will OVERRIDE other role permissions you may choose)

Read/Write - Full access to view and make changes to the system (this will OVERRIDE other role permissions you may choose)

To provide more granular login role permission selection, leave BOTH Read and Read/Write OFF of the "Current Role Permissions" list.

Activate Permissions - Ability to activate permissions (from BlueView software)

Import Cards - Ability to use Import Cards tool (BlueView software)

Load Batch of Cards - Ability to use Batch Load tool (BlueView software)

Login Administration - Ability to access Login Administration screen (BlueView software) to make changes to system logins

Remote Configuration - Ability to access Database Configuration/Client Setup screen (BlueView software)

Reset Database - Ability to access Reset Database tool (under Tools --> Import in BlueView software) that can delete all people/groups/shifts from the software. Intended to be used ONLY when a spreadsheet import on a new system doesn't produce the correct results and the administrator needs to start over.

Run Report - Ability to access Reports screen in BlueView or Reports tab in BlueWeb

Send Command - Grants ability to send any command (Ops Admit, Unlock, Lockdown, Normal) from BlueView or BlueWeb

Send Command Lockdown - Grants ability to send Lockdown command from BlueView or BlueWeb (lock the door so that ONLY Master cards will work at the door)

Send Command Normal - Grants ability to send Normal command from BlueView or BlueWeb (take door out of Lockdown or Unlock override modes)

Send Command Unlock - Grants ability to send Unlock command from BlueView or BlueWeb (put the door in an Unlock override mode)

Send Command Ops Admit - Grants ability to send Ops Admit command from BlueView or BlueWeb (momentarily unlock the door for its latch interval, default is 3 seconds)
Update Firmware - Ability to access the Firmware Updater screen (BlueView software)

Web Add Cardholder - Grants ability to add a new Person/Cardholder to the system from BlueWeb

Web Advanced Door Operations - Grants ability to access the Advanced Troubleshooting

Features from the Door page on the web interface - these include the ability to enable/disable communication with a door and initiate a full or incremental permissions update

Web Change Cardholder Status - Grants ability to Activate or Deactivate a Person/Cardholder record on the People screen in BlueWeb

Web Change Credential - Grants ability to add/edit/delete a credential (card or PIN) record on the People screen in BlueWeb

Web Change Door Status - Grants ability to change a door's status using Door Operations on the Doors screen in BlueWeb (Lock door for the rest of the day, change today's hours for this door, etc.)

Web Change Group - Grants ability to add a person to a group or remove a person from a group on the People screen in BlueWeb

Web Delete Cardholder - Grants ability to delete a Person/Cardholder from the system on the People screen in BlueWeb

Web Edit Cardholder - Grants ability to edit Person/Cardholder information (name, employee ID, picture, etc.) on the People screen in BlueWeb

Web Holidays - Grants ability to input holiday unlock hours for doors from the Holidays page in BlueWeb

The following Credential Mode settings can restrict which Credential Modes show up in the Credential Mode dropdown on the People screen in BlueWeb. (The Credential Mode drop-down may be turned off (invisible) in BlueWeb via BlueWeb configuration settings. These settings would only apply if this dropdown is configured to be visible.)

Web Permit Cred Mode Lockdown - Grants ability to set a credential mode for a credential to Lockdown (when a card is presented, it puts the door into Lockdown override mode)

Web Permit Cred Mode Manager - Grants ability to set a credential mode for a credential to Manager (to be used with Manager/Managed shifts)

Web Permit Cred Mode Master - Grants ability to set a credential mode for a credential to Master (ability to access any door in the system, including doors in Lockdown override mode)

Web Permit Cred Mode Unlock - Grants ability to set a credential mode for a credential to Unlock (when a card is presented, it puts the door into an Unlock override mode)

Access List

This tab allows the user to define exactly which locations (doors), groups (cardholders) and shifts can be accessed by this login role within BlueView.

To change the locations, groups, or shifts visible to a login role, first choose the Role from the drop-down list. Then use the arrows to move selected Locations, Groups, and Shifts between the Available and Visible to these Role columns (changes are saved as you go).

DATABASE CONFIGURATION

Overview

This screen is where you specify how BlueView software will connect to the SQL Server database. It is shown when you first install the software and can be found under Tools, in Database Configuration.

Guide Me

This is a wizard that will help you set up your connection to SQL Server. It has information relating to installing SQL Server, different configurations for BlueView servers and clients, SQL Server installed on a remote machine, etc. This is the best place to start when configuring BlueView for the first time.

BlueView Server or Client

The BlueView Server is the primary installation of BlueView on the network. There can only be one BlueView Server on the network, because this is the software that handles communication between the door controllers and the software. Despite the term "server," a BlueView server can run on any type of computer (laptop, workstation, server) that meets the minimum hardware requirements.

A BlueView Client allows the BlueView system to be managed from other computers on the same network. BlueView Clients are identical to BlueView Servers in terms of management capabilities, except that BlueView Clients do not have the ability to start or stop Bluelink Network Services (which runs ONLY on the BlueView Server). BlueView Client installations are subject to BlueView software licensing. Clients cannot be configured until the BlueView server has been installed and configured. For more information on setting up a client, see our Guide for Client Setup.

Database Management and Administration

Database Location:

Server Name or IP Address: This is the server name or IP address of the machine hosting the BlueWave SQL Server database.

If SQL Server is running on the same machine as this installation of BlueView, the server name can be set to "." which means local machine.

If SQL Server is on a different machine than BlueView, this field should contain either the name or the IP address of the computer where SQL Server is running. Note that when SQL Server is on a different machine than BlueView, there are additional steps needed to configure SQL Server so that it can be accessed remotely.

Instance Name: This is the name of the SQL Server Instance where the BlueWave database is/will be installed. This would have been set when SQL Server was installed. The default instance name is usually MSSQLSERVER but is sometimes SQLEXPRESS, left blank or set to a custom name by the person who installed SQL Server. Use the Browse button or go through Guide Me to search for available SQL Server instances on your machine and/or network.
Connection Timeout (in seconds): This specifies how long BlueView will wait for a response SQL Server when trying to connect. It can be adjusted at your discretion, based on your computer and network latencies.

Database Login: This section specifies the credentials that BlueView software will use to connect to the database. There are two options:

Integrated Security: This option means that BlueView will try to access SQL Server using the credentials of the Windows account that is currently logged into the machine. By default, ONLY the Windows account that installed SQL Server will have access using this method. If you are using SQL Server 2012 or higher, this option is available ONLY for expert SQL Server users. This is because Bluelink Network Services will not have access to the database without the Windows service being given explicit access to the BlueWave SQL database. We recommend using SQL Server Authentication instead. If additional Windows accounts need to be able to use BlueView, these accounts will also need to be given access to the SQL Server database. If you do not know how to do this, we recommend using SQL Server Authentication

Test Connection: Use the Test Connection button to test the connection information.

Create SQL Login: This button can be used to create a SQL Login that can be used for BlueView to access the database. This will ONLY work if a valid connection to the database has already been confirmed using *Test Connection*. It also relies on Mixed Mode Authentication being turned on in SQL Server. If Mixed Mode Authentication is not enabled in SQL Server, a message on the Create SQL User screen will direct you to the appropriate documentation to resolve the problem.

Restore Defaults: This button will restore the Database Location information to the default settings that ship with BlueView.

Be sure to hit Apply before leaving this screen to save the new settings. BlueView will re-test the connection before saving and will only allow valid settings to be saved.

Troubleshooting Notes

BlueView needs to be run as an Administrator (Windows setting), especially when setting up the initial database. This should happen automatically, but in case it doesn't, use Windows Explorer to navigate BlueView's installation directory (typically C:\Program Files\BlueView). Right-click on BlueView.exe and select Properties. Click on the Compatibility tab. Under Privilege Level, check "Run as Administrator." Then OK to close. Now, try running BlueView again.

If changes you make in the Database Configuration screen do not "stick" after Apply and Close, the problem may be that the file where these settings are stored may be marked as Read-Only by Windows. Using Windows Explorer, go to BlueView's installation directory (typically C:\Program Files\BlueView). Right-click on the file DAL.config folder and select Properties. Next to Attributes near the bottom, click on the check box next to Read Only to clear the box. Then click OK. It will then tell you you need to provide administrator permission to change these attributes. Click Continue.

FIRMWARE UPDATER

Overview

The 'Firmware Updater' tool is used when a controller is not behaving as expected or is needing to be updated in its base programming. Once started, the system will wipe all data on the board and begin to write lines to build the firmware. This means a door will be locked to all credentialed profiles while updating firmware. This process usually takes a few minutes. While updating, the LED on the board will turn off. Once complete, the controller will initialize, causing the LED to light up yellow for around seventy seconds as the controller reboots and initializes.

How to Update a Door

Select the 'Firmware Updater' under 'Tools' from the utility bar. Before you begin, ensure that you are *only selecting a single door*, along with the correct firmware version. Though the tool allows you to select by area, site, or company, DO NOT apply firmware updates in bulk. This can be unstable, and due to the nature of the tool, interruptions and breaks can cause damage to the functionality of the board.

Under 'Choose Doors for Update', use the first dropdown menu to select 'Door' (it will be set to 'Company' by default). In the dropdown menu to the right, select the desired door. You may also update the door by IP address as opposed to name.

Ensure a proper network connection by using the 'Ping' button a few times sequentially.
Upon successfully pinging the door, commence the update with the 'Start Firmware Update' button. The speed of the update will depend on the network, but generally these updates will take no longer than 5 minutes. After the initialization process finishes, the system will report a successful update. The door will automatically be scheduled with a full programming update and will upload the configuration settings along with credentials. Test the door to confirm functionality has returned.

If the process fails at the start command for any reason, you can do the following:
Check off the box for "Disable current firmware check". The tool checks the compatibility of the firmware you are pushing as well as checking the current firmware of the board. This will bypass the check, which can often fail due to the missing or corrupted data.

You can also power cycle the board and system, along with a network reset, in order to possibly bring the door back to a state in which it can be updated. It is always recommended to directly connect a laptop to the controller's network port to ensure the most stable connection and rule out any outside factors.

Firmware Versions

There are three active firmware versions in the most recent release of BlueView. *Version 3.0+* is used in legacy boards of the previous hardware iteration, while newer versions accept *5.0+* and *7.0+*. When just trying to clear corrupted data or programming, simply pushing the same version that is on the board is sufficient to refresh the firmware.

Sync Service

Overview

BlueView’s Active Directory Module enhances access control efficiency by synchronizing user and group data between Active Directory and BlueView cardholders. This module operates in two modes: 'Users Only' and 'Users and their Groups'. In both modes, it imports users from Active Directory, creating corresponding BlueView cardholder records with details like names and employee IDs, and aligns the Active/Inactive status of cardholders with Active Directory records. The 'Users and their Groups' mode further manages group synchronization, assigning users to matching BlueView access control groups and updating group names and memberships based on Active Directory changes. Integration requires specific Active Directory access credentials and settings, and it operates on a user-defined sync interval. BlueView's system updates door controllers accordingly during each sync, maintaining secure and accurate access control. This module is compatible exclusively with Microsoft Active Directory.

Notifications

Overview

The notifications feature allows users to set up email alerts for a group of people in response to specific events related to door access control. This feature is essential for monitoring emergency lockdown modes, unauthorized door openings without valid credentials, or doors staying open longer than a set duration (e.g., 60 seconds). It requires door contacts to function effectively. Users can be notified of these events if they are grouped appropriately and have an email address registered in the system.

How to Create a Notification

1. Assign email addresses to desired cardholder or person in the system.
2. Assign individuals to specific groups designated for receiving notifications.
3. Navigate to the 'Tools' menu, then select 'Notifications' to enable this feature.
4. Choose how frequently the system checks for events (e.g., every minute, hour, day, week, or month).
5. Specify which events should trigger notifications to the group.
6. Configure Email Server: Access the 'Email Server' settings under 'File' > 'Preferences'. Input the necessary email server settings as provided by your IT personnel.

Log Viewer

Overview

The BareTail Log Viewer, accessible under Tools>Start Log Viewer in the software, provides real-time updates of software communications through a live-updating window displaying reports line-by-line. The BNS log details

communication attempts with controllers, network connections, and credential activities, useful for monitoring direct interactions and identifying interruptions.

Reports

Overview

From this tool, you can generate a history of activity in the system. This report can be exported as either CSV or Excel filetypes using the ‘File’ dropdown at the leftmost side of the toolbar.

Report Types

Audit - System Health

Card Holder
This card holder list shows all card holders within the system in chronological order. You can also select a specific cardholder to audit.

Events
This events list shows activity within the system in chronological order. The dropdown allows you to select by door or even event type.

Groups
This report shows all people and their associated groups.

Permissions
This report shows all the permissions within the system.

Shift
This report shows all the shifts within the system.