Product Name	Document Number	Document Description
CA Cabinet Series	CA2012-0100	Common Access Cabinet User's Manual

Manual Revision	Revision Date	Revision Description
11	05/02/2022	Configuration Control to enable/disable the HID, CAC, Memory, or Keyboard inputs.

CAC Manager Application Version
Release 5.3.4, Build Date: May 2, 2022

Common Access Cabinet Graphical Users Interface and CAC-Manager

User's Manual

Plug-In Storage Systems Inc.
70 Industry Drive
West Haven, CT 06516

Contents

Acronyms

Acronym	Description
BRICKED	When the user is attempting to authenticate a Memory card or a DoD-CAC card, and the authentication fails the maximum number of times allowed by that card, the card will then stop responding and will no longer be useable. The term BRICK is unofficially used to refer to the card as being as useful as a brick. Typically for the DoD-CAC card it is 3, for SLE4442 card is 3, and for the SLE4428 it is typically 8 failed attempts.
CA	Common Access
CAC	Common Access Card
CAC PIN	PIN number associated with a Common Access Card
CAC-GUI	CA-Cabinet Network Graphical Users Interface application running on an administrator's workstation
CACmanager	Software application running only on each cabinet computer which handles the tasks of the cabinet, including the network communications.
CHUID	Cardholder Unique Identifier
DNS	Domain Name System or Domain Name Service. A network name resolver converting network names or hostnames into IP addresses transparently to the user. (The DNS is like a computer name phonebook to IP address look-up)

Fan-Power-Board	This is the circuit card assembly that filters and down converts the input 12 VDC power for the 8 on-board fan-controllers as well as for the Relay-Board. This board contains the embedded fan-controllers and serves as the distribution board for monitoring up to 24 temperature sensors and driving up to 8 fans. This board also has an alarm driver circuit to operate a piezoelectric buzzer.
HUB or USB HUB	Universal Serial Bus HUB
IP	Internet Protocol (The address used to uniquely identify a computer on a LAN, supported are the IP version 4 and IP version 6.)
IP v4, or Ipv4	Old IP standard. Format of the form: `xxx.xxx.xxx.xxx` Old format example: 192.168.1.11
IP v6, or Ipv6	New IP standard. Format of the form: `HHHH:HHHH:HHHH:HHHH:hhhh:hhhh:hhhh:hhhh` New format example: `2001:0:9d38:5ab8:2ce3:2c70:cda7:1ce8`
KEYPAD-ONLY PIN	PIN number for cabinet entry using only the Keypad. This PIN is created by the user and is NOT the same as the CAC or Memory-Card PIN.
LAN	Local Area Network

Acronym	Description
MEM PIN	PIN number associated with a Memory-Card
NIPRnet	Unclassified but Sensitive Internet Protocol (IP) Router Network
OS	Operating System (Windows 10)
PIN	Personal Identification Number (Associated with either the Keypad-Only, CAC Card or Memory-Card)
Relay-Board	This refers to the circuit card assembly that serves as the distribution board for monitoring and controlling up to 24 drawer latches/solenoids. This board also has an alarm driver circuit to operate a piezoelectric buzzer.
RF	Radio-Frequency (The only intentional system RF transmitters are the RFID readers)
SBC	Single Board Computer
TLS / SSL	Transport Layer Security/Secure Sockets Layer, used for secure, encrypted communications over the local area network (LAN)
USB	Universal Serial Bus
Windows 10	Microsoft® Windows 10 Operating System

SQL Server	A relational database management system developed by Microsoft to store and retrieve data as requested by other software applications
Cabinet Cluster	Several cabinets are grouped together with one set of access equipment
Cloud-based	A service based on internet to share the storage and computing ability to enhance the capacity of individual systems
Toast Notification	A desktop notification popped up to communicate certain events and disappear automatically after a short amount of time
Malware	Software intentionally designed to cause damage to computers or other IT assets. It includes virus, worms, Trojan, ransomware, spyware, etc.
GravityZone	One technology of BitDefender company to manage the security functions of the computer devices.

1 REVISIONS

Revision Number	Description
-	Initial document release
1	Updated to include the new software features for Release 3-2-0: 1. When a user opens the drawer, it is now considered a "check-out." The drawer checkout will not allow anyone else to use that drawer until it is checked in by the same user. 2. The system administrator can open the "checked-out" drawer, and when that happens, it is the same as checking in for that drawer, and then a new user can open it (do a new check-out). 3. The system administrator can do a SYSTEM LOCK or SYSTEM UNLOCK. If the system is LOCKED, it allows any user that has checked something out to check it back in, but no one can do a check out from any drawer. 4. A single user can now have multiple drawer assignments. If all drawers are desired, they will all have to be entered in.
2	Revised to include the new software features for Release 4-1-4 1. Created two modes of operation, FIRST-AVAILABLE, and MULTIPLE-ACCESS. FIRST-AVAILABLE is for cabinets that all have identical Tools / eTools / etc. in each drawer, and MULTIPLE-ACCESS is for cabinets that have unique Tools / eTools /etc. in each drawer. 2. Modified the way a new user gets registered into the system; no administrator is required to add users, as it is a self-registration process utilizing the CAC card. 3. Modified the log file format. System identifies exact drawer number that was opened and for what reason, and by whom. 4. If system identifies a drawer or drawers that are malfunctioning, the system continues to operate but flags the system administrator to try and reconfigure the system to resolve the issue.
3	1. Report to log file on the last 4 digits of Personal ID Number. 2. Added menu options for cabinet Mode and enabling/disabling adding new users. 3. Fixed CAC PIN number handling for PINS less than 8 digits 4. Fixed bugs when going between FIRST-AVAILABLE and MULTIPLE-ACCESS modes.
4	1. Added and modified menu and operational features. Added support for the newly updated Relay and Fan boards. Expanded explanations. 2. Added section for Stand-Alone-GUI, 'CA Config GUI 1.0'.
5	Release to incorporate Network-Enabled CAC-GUI and new CACmanager operations.
6	Updated to reflect changes before submission for DoD Certification Network approval.

7	Configuration Control to enable/disable the HID, CAC, Memory, or Keyboard inputs. Also allows cabinet to boot up and run with and without the CAC card-reader.
8	1. Upgrade to Windows 10 Pro as Operational System 2. Use SQL Server as database 3. Added Cabinet Cluster structure and Cabinet Network structure 4. Added functions of email, statistics, diagnostics, temp user, live sync etc.
9	Add security feature to the cabinet program suite.
10	1. Add MAC address-based management functions 2. Add the usage of control board with 48 ports 3. Add On-premises version of BitDefender 4. Add Syslog server configuration and the related functions
11	1. Add Access configuration of “CAC-Card RFID” 2. Add configuration of RFID reader
12	Add platform of Pool Database

2 FUNCTION INTRODUCTIONS

The Common Access Cabinet provides several means for the user to check-in/checkout the devices, and it is also a management platform to organize and trace the equipment. The cabinet system includes the following functions:

Structure and Principle:

- Single Board Computer
- Fans
- Workstation-based Card Reader
- In-cabinet Card Reader
- LAN
- Stand-alone
- Database with SQL Server

Basic functions:

- Fundamental Function
- Cabinet Startup Process
- Access Management

Cabinet Configuration

- Basic Configuration
- Accessory Setup
- Administrator Activity
- Database Parameter Setup
- Report Function Setup
- Email Configuration
- Firewall Setup

User and Equipment

- User Information Management
- Group Management
- Device Management
- Temporary User PIN Setup
- Management of Broken Device
- Management of Overdue Equipment

Display and Log

- Display the Status of the Cabinet in Real Time
- Cabinet Overview
- Statistics Report with Chart for Various Cabinet Activities
- Detailed Log for Each Action and Status Change of the Cabinet
- Receipt Generation

- Toast Notification of Checkout and Check-in

Remote Control
- Remote Control of the Cabinet with Commands

Cabinet Cluster and Cabinet Network
- Cabinet Cluster Sharing One Control System
- Cloud-based Cabinet Network and Live-sync

Support
- System Diagnostics
- Help from Cabinet Keypad
- Live-support Setup

Security Function
- Security Parameter Setup
- Security Server Setup
- Security Package Installation
- Security Status Display
- Email Alert and Daily (weekly) Report
- Archive Security Source Files
- Manually Scan Device
- Manually Remove Pending Report
- Syslog Server Setup

Management based on Device MAC Address
- MAC Address Function Setup
- MAC Address Scan
- MAC Address Display
- Related log and others

The following is a brief description for each function modules:

1) *Fundamental Functions*

The cabinet provides a drawer for each device and the drawer is normally locked. When the user scans the card or type the PIN, the drawer will open for the user to checkout or check-in the device.

2) *Cabinet Startup Process*

When the computer is powering up, the cabinet starts automatically as a Windows Service. During the first-time startup, CACManager program will set up the default configuration parameters in the database.

3) *Access Management*

The cabinet can be accessed with several methods, such as *keypad PIN*, *CACCard*, *RFID card*, CAC-card RFID, and *Barcode*. The user needs to be registered into the database system before access or during access to the cabinet based on the configuration.

4) *Basic Configuration*

Based on different customer requirement and different hardware setup, some configuring parameters need to be changed accordingly. Normally these parameters are maintained with *CAC-GUI*. Some parameters can also be modified through cabinet keypad panel.

5) *Accessory Setup*

A special drawer can be allocated to store the accessories of the device, such as battery. When the accessory drawer is setup, it will open automatically after the device drawer is open.

6) *Administrator Activity*

From the keypad panel, the administrator can access the cabinet admin menu for configuration and do some maintenance work. More sophisticated tasks can be fulfilled with *CAC-GUI*.

7) *Database Parameter Setup*

The server's name, database name, username and password can be set up when logging into *CAC-GUI*; for running *CACManager*, it only needs server name and database name.

8) *Report Setup*

A report is a summary of certain log information tailored with different requirement of filter, content and time; it can also be some real-time alert. The report can be configured to send to the administrator by email.

9) *Email Configuration*

Email function is used to send the report to the administrator. The parameters of the email accounts include email server, port, username and password.

10) *Firewall Setup*

System Firewall needs to be turned on. The rules for running *CacManager* and *SQL server* are configured.

11) User Information Management

The users who access the cabinets need to set their detailed information; each has a unique GUID number related to the profile.

12) Device Management

The device information needs to be added into the database, and each drawer needs to assign a device before it is ready to be used to the user.

13) Temporary PIN

A temporary user can be given a PIN to access the cabinet for a certain period of time. The PIN is normally sent to the user by email.

14) Broken Device Management

Broken device can be reported from the cabinet and the data will be saved into the database; the administrator can use CAC-GUI to manage the report of broken device.

15) Management of Overdue Equipment

This module is also called *Missing Equipment Management*. It has two layers of alert: warning and alarm. The alert can be sent to administrator by email in real-time.

16) Cloud-based Cabinet Network

All the cabinets in the organization can connect each other to form a network to share the resource and sync their activities. The pool database is used to coordinate all the cabinets and it can be installed anywhere on the Internet.

17) Cabinet Cluster

One set of control system can manage several cabinets in real time. These cabinets need to be physically close; they share one set of access and display system (LCD).

18) Display the Real-time Status of the Cabinet

The dynamic status of the cabinet is displayed in the *Snapshot* tab of *CAC-GUI*. The open/close of the drawer and the checkout/check-in of the device are shown in the screen. *Drawer Overview* tab has similar information with different displaying style.

19) Cabinet Overview

Display a matrix of drawer logos to indicate the real-time cabinet status; it is a demonstration of the cabinet status in a different style of the *snapshot* view.

20) System Diagnostics

The cabinet software system can investigate the major components to see if they are working properly. The entrance of the function is in tab *System Config* of *CAC-GUI*.

21) Remote Command

The administrator can control the cabinet remotely from *CAC-GUI*. The commands include open drawer, restart CACManager, reboot & shutdown the cabinet computer.

22) Statistics

This function module provides the statistics of the usage to the cabinet based on the user, drawer or device. There is diagrammatic chart accompany with each result.

23) Detailed Log

Detailed log for the cabinet activity is available in the database and can be browsed in a *.html* file

24) Receipt Generation

A receipt can be generated when the user checks out a device. The receipt has the detailed information of the operation and the related device.

25) Toast Notification

This function module is about a real-time notification displayed on *CAC-GUI* when there is a device checkout or check-in.

26) Help on Keypad

From the cabinet keypad, the user can find the name and phone number of the administrator.

27) Live support

The administrator can talk with the support center by video, audio or message using *Skype*. The *Skype name* of the support center is required in the process of setup of this module.

28) Security Parameter Setup

The Security feature is using BitDefender technology, monitor and scan the computer, generate the reports of malware and the attempted attack. Some parameters are required to connect to the BitDefender server in order to use APIs.

29) Security Server Setup

For On-premises version of BitDefender, a server needs to be set up in local computer network to fulfil all the security tasks. Currently we are using Linux Ubuntu Server.

30) Security Package Installation

The software package needs to be installed to the computer to scan and monitor the malware. The software is downloaded from the BitDefender server. A BitDefender account needs to be created, and the license needs to be purchased.

31) Security Status Display

The security status of the devices is displayed on CAC-GUI, and the user can check it in real-time. The source file and statistics data can also be viewed.

32) Security Email Alert and email Report

When malware is found in a device, an email will be sent to the administrator, and the related drawer will be locked. A daily or weekly report about the security issues can also be created to be sent to the administrator

33) Archive security source files

The report files of the security checking can be archived to a separate folder after some time.

34) Manually scan devices

Normally a device is scan as soon as it is checked in to the cabinet, but the user can also scan the device manually from CAC-GUI.

35) Manually remove pending report

When there is some issue in scanning a device, the report generation may be stuck forever. The user can remove the generating process manually from CAC-GUI.

36) Syslog server setup

Syslog server can be set up to receive all the notifications sent from GravityZone, the notification can be parsed and saved into the SQL server database.

37) MAC Address Function Setup

The MAC address related functions need to be configured before use. The availability of the functions is based on the cabinet hardware. The function setup located at System Config tab of CAC-GUI.

38) MAC Address Scan

The MAC address can be manually typed in, but normally it is scanned automatically by the program for the convenience.

39) MAC Address Display

MAC address is displayed in Equipment List tab of CAC-GUI, and there is a separate tab for the live update about equipment check-in/checkout.

40) MAC Address Related Log and others

When MAC address is enabled, the log can record the device MAC address of the check-in /checkout and other activities. Some statistics can be viewed based on the MAC address. Issues related to MAC address can be diagnosed by running Diagnostics function.

The above is the brief description of each module, the detailed discussion will be in the following chapters.

3 STRUCTURE AND PRINCIPLE

Plug-In Storage Systems Common Access Cabinets (CA Cabinet) can be operated in a stand-alone or a networked configuration. This manual addresses both aspects. Figure 1 illustrates a typical 20-drawer configuration depicting the top-level functional block diagram of the internal design.

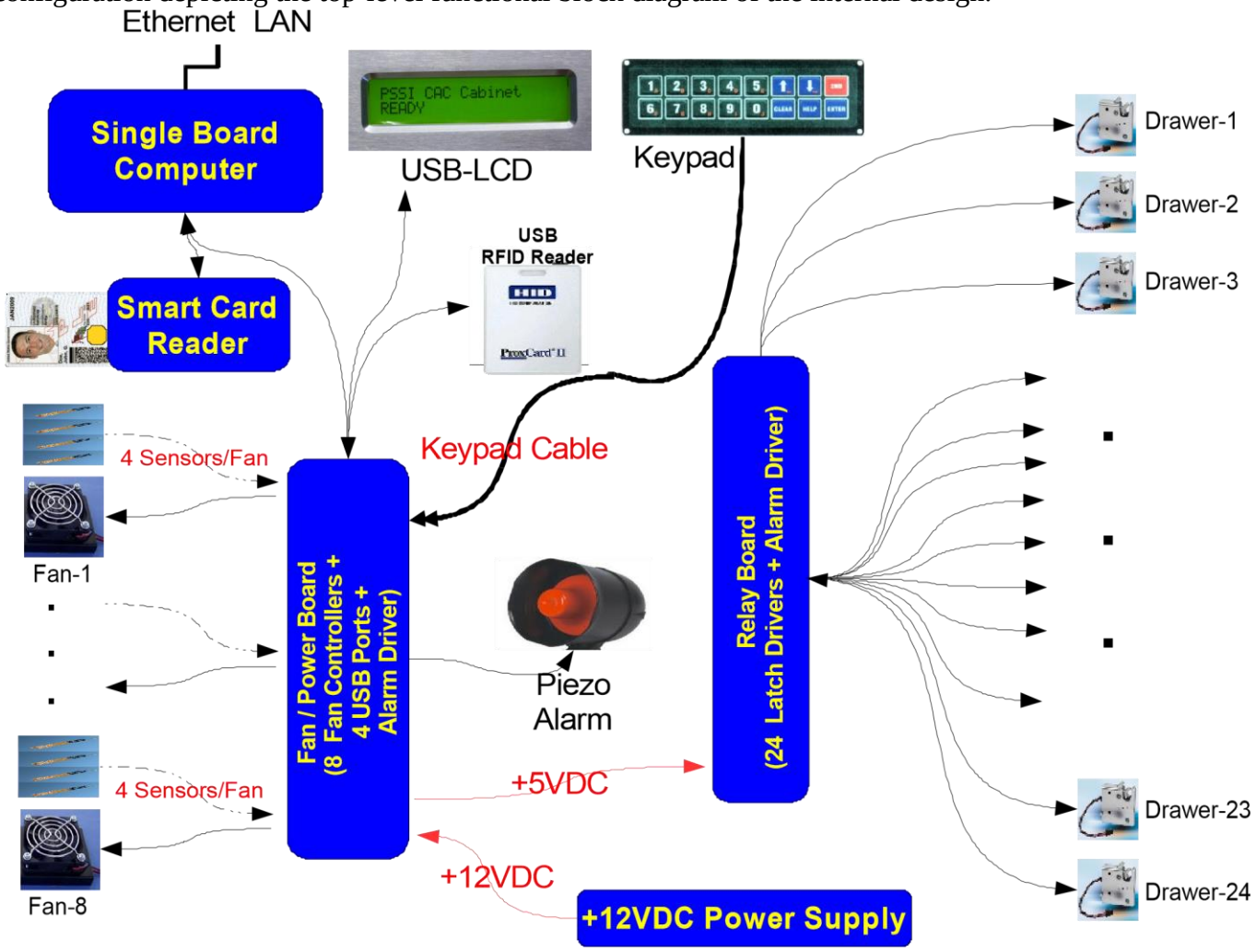


Figure 1. CA Cabinet System Block Diagram for 20-Drawer Unit

3.1 Single Board Computer

At the heart of the system resides a Single Board Computer (SBC). This SBC has all of the software applications and drivers necessary to operate in a secure networking or stand-alone environment. The standalone configuration simply means that the CA Cabinet operates without an external LAN connected. All interfaces to and from the SBC are wired connections, except for the optional HID RFID and Parallax RFID card readers. These RFID readers are optional subsystems and if installed they would be the only intentional RF transmitter used in this system. One, none, or both RFID Card Readers may be incorporated into a single system without any additional software additions or firmware upgrades.

All of the command and control throughout the cabinet, for the stand-alone configuration, occurs over the USB bus through multiport hubs embedded in each of the Relay and Fan boards. The system is configured such that the USB hubs serve primarily as the bidirectional communications link to each subsystem, including the CAC card-reader, RFID-readers, LCD display, keypad, drawer-controllers and fan-controllers. The bidirectional communication over this bus is used for command, control and status feedback of all of these sub-system devices. The system is designed such that all of the power to the SBC and the subsystems come up together. This is important, as the SBC initiates a service task that requires all of the subsystems to be powered and operating in a standby state waiting for the SBC to enumerate and communicate with them. If the subsystems are powered up or plugged in after the CACmanager starts running, incorrect and indeterminate results can be expected.

The electronics for each of the drawers have independently controlled relay drivers. These relay drivers are combined on a single board which monitors each of the drawer's statuses. The sensor to the drawers will indicate if the drawer is open, closed, whether a sensor wire is broken or even shorted. The relay driver provides the drive capability for opening each of the drawers by driving the drawer's latch or solenoid.

3.2 Fans

The USB bus is always utilized for monitoring and setup, or programming of the operating temperatures for the cabinet's fan cooling system. Typically, the cabinet's cooling system is configured with two to four temperature sensors paired with a single fan and fan-controller. For each controller, when any one of the sensors exceed the programmed turn-on temperature, then the controller turns that fan on. Likewise, below the turn-off temperature programmed set-point, when all of the temperature sensors have dropped below this set-point, the fan control board turns the associated fan off. During fan operations the control electronics will drive the fan speed at a reduced rate if the temperature is only slightly above the upper temperature set-point and will increase the speed as the temperature rises. This allows the fans to operate quietly for moderate temperatures. These on and off temperature set-points are configurable via the USB bus for various environmental scenarios through the system's front-panel control and via the CAC-GUI. The piezoelectric buzzer is enunciated for temperatures 18 degrees F over the turn-on-temperature, and for over-current conditions of each fan.

3.3 Workstation-based Card Reader

The Smart-Card readers supported on the CAC-GUI workstation should have PC/SC capability so the CACGUI can utilize the standard Windows-10 Smart-Card drivers.

3.4 In-cabinet Card Reader

Only one Smart-Card reader is allowed to be attached to the cabinet computer due to the special software drivers loaded for Memory-Card operations. The USB Smart-Card reader integrated into the cabinet is a SCM Microsystems Inc., model SCR333. This card reader and associated software drivers are all ISO 7816, PIV II FIPS 201 Compliant. Please see the following link for the “FIPS 201 Evaluation Program Approved Products List”: http://fips201ep.cio.gov/apl.php

3.5 LAN

The SBC's on-board Local Area Network (LAN) Ethernet interface is the interface utilized by the CAC-GUI application to manage the cabinet computer for configuration, control, status and activity log queries. The CAC-

GUI application running on an administrator's workstation communicates to the SBC over the LAN. On the SBC, the CACmanager program is acting as the cabinet server and handles all of the Transport Layer Security / Secure Sockets Layer (TLS/SSL) messages to and from the CAC-GUI. The encrypted communications are designed to operate over Unclassified but Sensitive Internet Protocol (IP) Router Network (NIPRnet) military networks and uses the SSL protocol version SSLv23. FIPS-140-2 hashing is utilized for matching-ids and/or passwords. The network communication pathway allows the administrator to manage the control, update user accounts and system configuration, check status, and upload from each cabinet activity logs to view and print. Activity reports can be filtered and sorted by many attributes such as: by user name, ID, drawer number, time-range, access method, etc.

Figure 2, below shows an example network diagram with four cabinets attached to the LAN. The administrator's workstation on the left of the diagram is running the CAC-GUI and as indicated is communicating with one of the cabinets. The architecture is set up so that the workstation operates as a client to the cabinet, and the cabinet operates as its own cabinet-server. When the administrator communicates with a second or third cabinet, that cabinet in turn will operate as its own server. This eliminates a centralized server architecture, thus enhancing reliability (no single-point failure for a multi-cabinet network). This design keeps all the database files including user accounts and activity records on each of the cabinets as well as on the administrator's workstation. This cabinet server only allows a limited set of operations which are solely based upon operations of the cabinet. The current version of this cabinet's server will only allow a single secure connection at a time for the cabinet network operations. Therefore, if an administrator wants to gain access from a secondary workstation, they must first log-off / disconnect from the first workstation. If needed, this software can be enhanced to allow multiple connections simultaneously, however from a database management standpoint, allowances would need to be made.

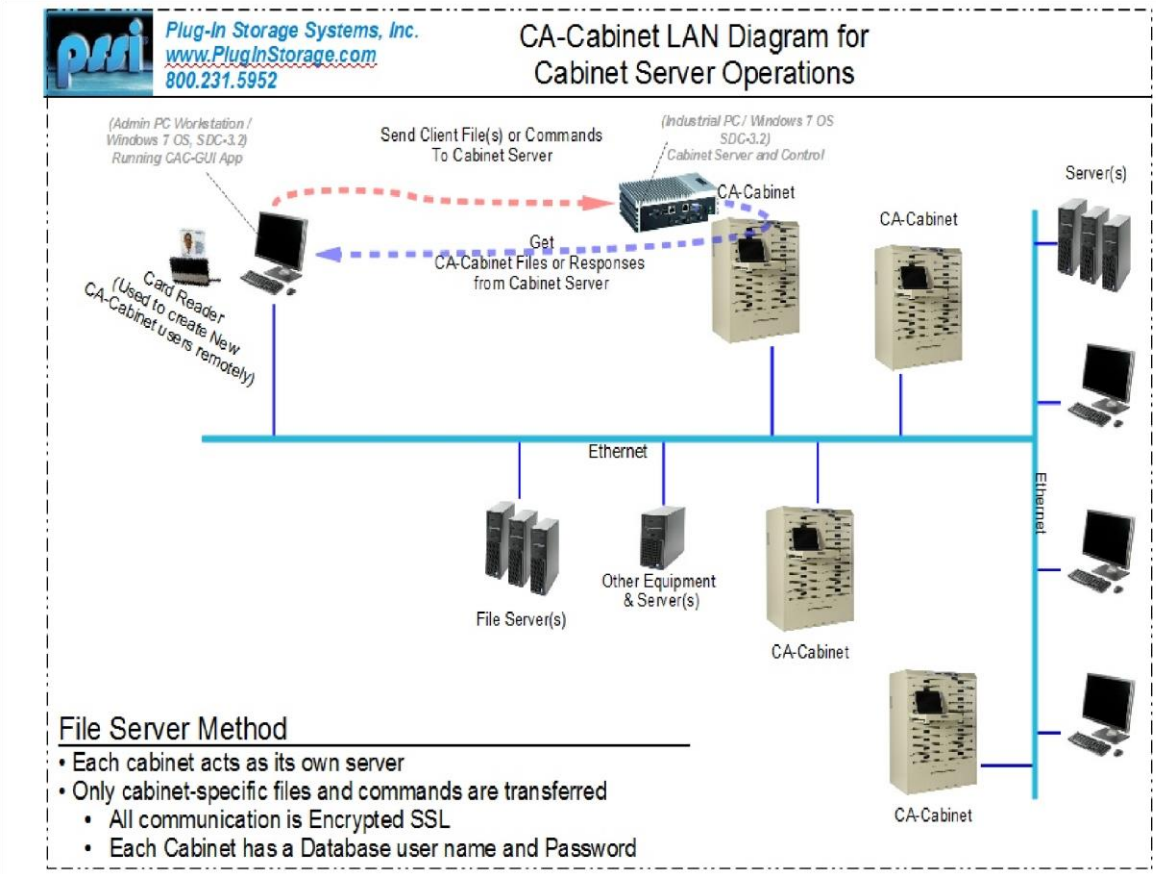


Figure 2: ***LAN Network Data-Flow for Communication to each Cabinet from a Workstation.***

Note also that the diagram in Figure 2 indicates other "File Server(s)", "Server(s)" and "Other Equipment & Server(s)". This is included on the diagram simply to emphasize that the CAC-GUI and CACmanager do not need a separate set of equipment or servers to operate smoothly over a complex network which may include a myriad of other systems.

A complete process of using the CAC-GUI in setting up and communicating with a cabinet is covered in the "CAC-GUI Operations" section.

3.6 Stand Alone

For operations as a stand-alone system, the CAC-GUI can be loaded on the cabinet computer and allow the same operations as if connected via the network. This allows the administrator all of the same aspects for changing the cabinet's operating modes & configuration, to add / modify users, etc. Refer to the "CAC-GUI Operations" sections.

3.6.1 Access Methods

The various drawer-access methods supported by this CA Cabinet system are listed as follows:

- DoD CAC card (PIN required),

- Memory-Card (PIN required),
- HID-RFID card (no PIN required) (optional),
- RFID card (no PIN required) (optional), and
- Keypad-only (PIN required).
- Temporary PIN

From the front-panel Keypad, only the cabinet administrators can administrate the operations of the cabinet. The administrator can delete or modify the authority of a user from normal user to administrator privileges. If the user has not been added into the system by the CAC-GUI, then the access method for new users is based upon how that user initially interacts with the cabinet. For example for a user that comes up to the system and starts typing in a new keypad code, and assuming that the system successfully authenticates the user with their CAC card, this new user is created as a Keypad-only user and saved in the database. Likewise, for a new HID-RFID and RFID user, their initial interface starts once they swipe an unused RFID card over the appropriate RFIDreader; for a CAC card user an account is created once the users CAC card is authenticated by the user. For uninitialized memory-Cards however, the CAC-GUI must be utilized to set-up a temporary memory-Card PIN, thereafter the uninitialized card can be inserted and enrolled. Temporary PIN is a temporary method for the user to check in; it has more detail in section 2.9.

In each of these cases when creating new users, the user must have a valid CAC card and must know the PIN code associated with that particular CAC card for authenticating. This is necessary to track and keep each user accountable for the items removed from one or more drawers. Once a user has been added into the system, the administrator can modify the users' usage authority to be an administrator or can even delete the user from the system.

3.6.2 Role of Administrator

An administrator has the authority to prohibit new users from being added into the system, locking out particular drawers, changing the operational modes of the system (Single-Drawer assignment, First-Available, Multiple Access, Check-In-Only, and Check-Out-Only), reconfiguring the fan controllers to modify the on and off setpoint temperatures of the cabinet, or even to reconfigure the drawer number assignments as to how the drawers are numbered, i.e. which drawer is numbered 1, 2, 3, etc.

Also note that a single CAC card holder can create as many keypad-only, HID/RFID-card, and Memory-Card user accounts as needed, and likewise via the CAC-GUI any number of new users can be created without the use of a CAC card. In each case where the CAC card is used to create new users at the cabinet, the CAC card allows a limited trail for tracking the non-CAC card user, since each time a new account is created the CAC card used is associated with this new account so that the administrator will know who each of the accounts belong to. This is accomplished by creating a User ID that can be associated with a CAC card. For CAC card-only accounts, only one entry per CAC card can be created.

3.6.3 PIN number & Serial Number

Care must be taken so that the user does not confuse or mix the PIN numbers associated with their CAC card, the keypad-Only PINs, Memory-card PINs and Memory-card Temporary PINs. This is facilitated by the system prompting the user to use the appropriate type of PIN depending upon what is needed, such as prompting for entry of: “CAC PIN”, “KEYPAD-ONLY PIN”, “TEMPORARY PIN”, or “MEM PIN”.

As inferred above, each CAC card is unique and has unique identifiers saved on it, and as such the CAC card is used as the access gateway for any new user account creation. This is true in STAND-ALONE mode if the CAC-GUI is not used for creating the account, as the CAC-GUI gives more flexibility in creating accounts that would not necessarily be tied to the CAC card. Once a user has been created, the person's name and a newly created personal ID number will be associated with each CAC card. This is what tracks that user and it is recorded in the activity log each time a drawer is opened. The CAC-GUI allows the administrator to modify this information for each user except for the matching-id as described below.

Each CAC card has unique serial numbers and identifiers that are guaranteed to be different from all other CAC cards. Accordingly, information is read from the CAC card and used to build a unique signature which is stored in the local database for the user, and is referred to as the database matching key, matching-id, or signature-id. This matching-id is a 64-byte FIPS-140-2 compliant SHA-256 hash string. When the user attempts to gain access at a later time, this unique matching key / signature-id is used to track the user. This unique matching key is saved in a local database along with other information such as access privileges.

3.6.4 Cabinet Mode

The drawer-access check-in / check-out operation allows a user to open a drawer and the system will then mark that drawer as used and tag the drawer or drawers as “Checked-out” by that particular user. No other user can then access that drawer until the user that first opened it for check-out opens it back up to return the item(s) as checked-in. This is true for all the cabinet modes except for the Check-Out-Only and Check-In-Only modes, which are discussed later. Once a drawer is opened back up for “check-in,” the check-out / check-in process cycle is then complete. When the cabinet is setup to run in FIRST-AVAILABLE mode, checking out a drawer checks out the first drawer that is available which has been checked in the longest. This is designed so that a maximum charge time is given to battery-powered tools before they are checked-out again. This FIRST-AVAILABLE mode assumes that all of the items in the cabinet are identical, such as updated lap-tops, or GPS's, and it is unimportant which of the units is actually checked out except for the battery charge levels.

When the cabinet is setup to run in MULTIPLE-ACCESS mode, the user is prompted as to which drawers they want to open for check-out. If a drawer selected is already checked out, the system will notify the user and the user can select a different drawer. This allows the cabinet to be filled with unique tools for each drawer and a single user is allowed to check out as many drawers as they need. Upon check-in, depending upon how the system has been configured, either all of the drawers will be opened and the user must check in all of these items at the same time, or the LCD will prompt and query the user for if whether or not they want to return each of the items that were checked-out. This one-by-one query for returning each item can be turned on if the system is configured with the CHECK-IN-QUERY enabled.

When the cabinet is setup to run in FIXED-ACCESS mode, the first time the user accesses the cabinet, the system asks the user which drawer they want to use. If it is available that drawer is logged into the system database and will be the only drawer permitted to be used by that user. The next time and any subsequent access by this user, the system will remember this drawer assignment and force the user to use only that drawer. Note that more than one user can be assigned the same drawer, but when that drawer is checked-out then no other user can open that drawer until that drawer has been checked back in.

In the case that the system administrator logs in and opens a drawer that has been left in a checked-out state, the administrator is prompted with the option of forcing the check-in for the selected drawer or keeping that drawer

checked out but still opening the drawer for some other reason. In either case, the drawer opening is recorded to the activity log file.

The modes Check-Out-Only and Check-In-Only are set up to be complementary of one another. These modes are configured to handle situations where users can check out equipment-items and give the equipment-items to another user to subsequently return them. The best way to utilize these two modes would be to have one cabinet configured as Check-Out-Only, and a second cabinet configured as Check-In-Only. The first set of users would then use the Check-Out-Only cabinet to check out the needed equipment-items, and then, out in the field would give the equipment-items to a new user. Once this new user comes back to the facility, they would go to the Check-In-Only cabinet and check the equipment-items back in.

3.6.5 Cabinet Lock-out

The system administrator also has the ability to lockout any number of selected drawers or to force a cabinet wide system lock-out. When a drawer is locked out, no user can check-out that drawer, however the user that had previously done a check-out of that drawer can check-in the item to that drawer. This operates regardless of whether that individual drawer or the system as a whole had been locked out.

The system-administrator can also lock-out users from using the system. This requires the CAC-GUI and is a simple checkbox to enable and/or disable each users access mode.

3.7 Database Connection with SQL Server

The cabinet is using SQL Server as the database to store the information of configuration, users, equipment, and the activity log. The login parameters are stored in file *DatabaseParameter.txt* located at *C:\Users\PlugInStorage\AppData*. When cabinet is started, CacManager code will read the above file to get the parameter and connect to the database automatically. When the database name or username is changed, the parameter file needs to be changed accordingly.

Although the data in the database can be modified manually, it is not the preferable way to do it. The data can be modified and queried from *CAC-GUI* in order to maintain the integrity of the database.

4. BASIC FUNCTIONS

4.1 Fundamental function

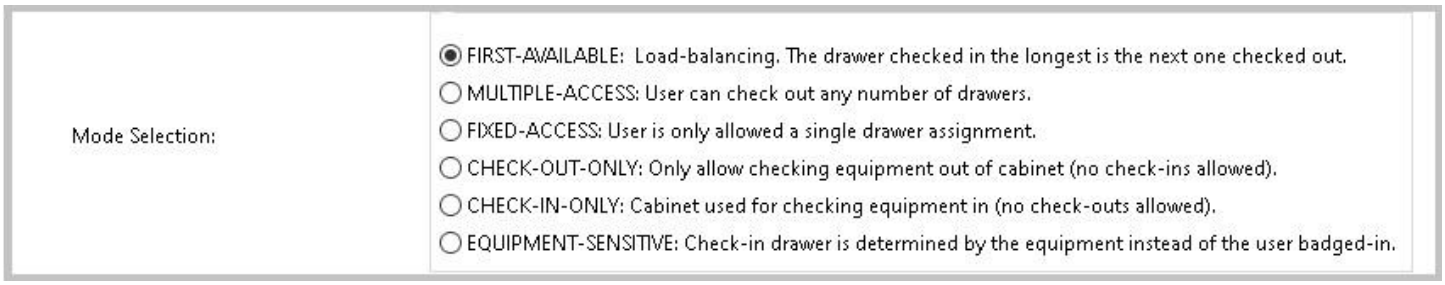
The CA Cabinets system is a computer storage cabinet solution that physically protects laptops and notebooks for organizations wishing to employ a high level of security while updating and recharging mobile assets. The CA Cabinets solution features the CAC Manager software, a Graphical User Interface application which manages the cabinet computer configuration, control, status, and activity log queries. The basic actions include check-out a device and check-in a device.

For a check-out process, the user accesses the cabinet by applying different means (more details in section 3.2), one drawer of the cabinet with device will open, the user can take away the device and close the drawer; all the actions are recorded in the database. For a check-in process, after the user has badged in or typed the correct PIN, an empty drawer will open, and the user can place the device into the drawer and close the drawer.

Based on the device selection and type of the checkout/check-in process, the cabinet has the following modes:

- First-available mode: Load-balancing. The drawer (device) with longest waiting time is the one to be checked out. This is the most popular mode, and it is the default one
- Multiple-access mode: the user can check out several devices; he/she can check out another device without returning the one(s) he/she already has
- Fixed-access mode: the user is assigned to a fixed drawer (device). He/she can only checkout/check-in the drawer assigned. The assignation of the drawer to the user can be done in *User Accounts* tab of *CAC-GUI*. Column *Drawer #* is the drawer for the user.
- Check-out-only mode: only allow checking equipment out of the cabinet; no check-in is available
- Check-in-only mode: only allow checking in equipment to the cabinet; no checkout is available
- Equipment-sensitive mode: the check-in drawer is determined by the equipment instead of the user who are accessing the cabinet.

For a certain time, only one mode can be selected. The setup of the mode is located in *System Config* tab of *CAC-GUI*. The following graph is the section of the mode selection:



4.2 Cabinet Start-up

When the power is on, CAC manager program will start automatically as a Windows service. The following sections are some discussion about the startup process

4.2.1 Stand-alone

When starting up a cabinet for the first time, the cabinet is configured to have only a single administrative user in the database. The individual that is going to be the system administrator can immediately gain access to the cabinet via the default Keypad PIN password, thereby logging into the system as the system administrator.

One of the first things that should be done is to do a "RECONFIGURE SYSTEM" so that all of the drawers in the cabinet are known and assigned. They would typically then change the system's configuration to allow automatic log-in, so as to allow their own CAC card to create a new user.

Attention: In cabinet CACmanager 5.3.x series, the operation of RECONFIGURE SYSTEM is not necessary anymore.

Once they have successfully become a new CAC-card user, they would then log back in as the default Keypad administrator and edit or change the CAC card user (now in the database) and change their authority to be an administrator. The old, default Keypad PIN administrator account can then be changed to a normal user, and then deleted if desired.

Note that for FIRST-AVAILABLE mode, the very first time the system is used, the cabinet will not have anything in the drawers for the users to use, so the system administrator is expected to open each of the drawers one at a time with the administrator account option under "OPEN DRAWER," and put a tool/laptop in each of the drawers. Once this is done the first time, then the system can keep track of which tool/laptop has charged the longest after it has been checked in. If the system administrator fails to put something in all of the drawers for the first time where one or more of the drawers have not been opened at least once, the system will not treat these unopened drawers as having battery-charge-times and so the next available drawer that a user will automatically get is from the set of drawers that have been used and checked-in.

4.2.2 CAC_GUI Access

When logging into a new cabinet, the default database password is nonexistent; there is no password on the system. In this case, any username and password typed into the GUI fields will allow the administrator to log on to the cabinet database. It is highly recommended that the administrator changes the cabinet database user name and password immediately. This is covered in the "*CAC-GUI Operations*" section.

Attention: In CACmanager 5.3.x series, the login parameters are the login information for SQL Server.

4.2.3 Start-up for the first time

When starting the system for the first time, the cabinet is configured for several default settings from the factory as follows:

Configuration Item	Default Setting
Drawer numbering	The drawer numbers are set in a default configuration with drawer number 1 starting as the top-most drawer, and then incrementing by one going down towards the bottom of the cabinet. For cabinets with more than one column of drawers, such as a 20-drawer system, the drawer number 11 starts at the top of the second column. This may be changed by the administrator when reconfiguring the system.
Administrator User Password	On new cabinets, there is only a single entry for one user. The single entry is for the system administrator. This default password is the Keypad-only PIN entry, with PIN number 0000000000, i.e., ten zero's as the PIN number.
Database Username and Password	For new cabinets, the CAG-GUI default User Name and Password on the cabinet are nonexistent, therefore any User Name and Password will allow the administrator to gain access to the cabinet and database. However, once the User Name and Password are changed, this condition will not be allowed again. Attention: For CACManager 5.2.x series, the login parameters are the one for SQL Server
Fan temperature set-points	The fan on/off temperature-control set-points are setup by default for the fan(s) to come on when the drawer temperature is above 90 Degrees F, and to turn off when the temperature drops below 85 Degrees F.
Alarm activation	The piezoelectric alarm is wired from the Fan/Power board and is set to sound when one of the following occurs: 1. When the temperature on any of the sensors exceeds the ON temperature set-point by more than approximately 10 degrees C (~18 degrees Fahrenheit) 2. If a fan is running but is drawing more current than is normal, such as when a fan has an obstruction or the bearings are failing. The alarm will stop when the temperature falls below that mentioned above for over-temperature. For an over-current condition the alarm will stop when the current comes within the normal operating range.
SBC Operating System Configuration	The SBC shipped with each cabinet has Microsoft's Windows 7 Professional operating system loaded on it, with the workgroup network domain as 'WORKGOUP'. The SBC is set up so that two Windows Service task are automatically started on boot-up. One is for the operations of the cabinet, named “PSSI_CACmanager_Service”, and the second is for automatically printing equipment receipts, named “PSSI_Receipt_Printing_Service”.

System Lock-out	The default is that the entire cabinet system is configured as UNLOCKED. To modify this to LOCKED, a system administrator must log on and change specific drawers to locked or the entire system, or change it through the CACGUI. Any locked drawers prohibits all users except the administrator from checking out that drawer or that set of drawers which are locked. Check-in is always allowed for LOCKED drawers.
Query Check-In	The default is ON. With this feature enabled, any time a user attempts to check in a drawer, the system will query the user as to their desire to do a Check-In or keep it Checked-Out. This is setup such that if the user wants to keep the drawer checked-out but reopen the drawer to get out a cable or other misc. item the system will allow it without checking the item back in. This parameter (QUERY_CHECKIN either ON or OFF,) is modified from the front-panel or by using the CAC-GUI in the System Config tabbed window.
Cabinet Name	The default name given to the cabinet is the Microsoft Windows computer name. If the cabinet is setup as a Windows WORKGROUP, then the CACGUI can use the “Microsoft Computer Name” instead of the IP address to connect the cabinet. The cabinet name, can be modified by using the CACGUI in the System Config tabbed window. Note that even if this cabinet name is changed, the WORKGROUP name will not be change and WORGROUP access will still respond the Microsoft Computer Name, not the new cabinet
	name.
Cabinet Mode of Operation	Default is set to “FIRST-AVAILABLE.” This mode can be changed to “FIXED-ACCESS”, “MULTIPLE-ACCESS”, “CHECK-IN-ONLY” or “CHECK-OUT-ONLY”. To modify the MODE: the system admin either utilizes the GUI, or by logging in as the administrator and selecting the “CHANGE CABINET MODE.”
Auto-Enrollment feature	The default is set to “OFF”. If set to ON, then any user with a valid CAC card and associated PIN can become a normal user on the system without the need of the system-administrator. To change this mode, either log in as the administrator and change this setting by selecting the “CHANGE AUTO ADD-USER” feature, or utilize the CAC-GUI and check or uncheck the “AUTO-ENROLLMENT” checkbox.
Auto-User-Name feature	The default is set to “ON”. To help protect any personal data on a user's CACcard, this feature when enabled tells the CACmanager to not use the person's name on the CAC card, but to substitute “John Doe” for the user name. In the CAC-GUI, this name can be modified later if desired.
Missing-Equipment-Time-Out	Default is set to 12 hours. This setting is only used by the Activity Report Generator on the CAC-GUI. Refer to the CAC-GUI Operations section.

Unusable Drawers	A typical cabinet has electronics support for more drawers than is physically outfitted. This allows easy expansion for new drawers. Unusable drawers show up when the electronics which are not attached to a physical drawer detect that there is no drawer available to control. These drawers, which include broken or shorted wires, are detected and marked as "Unusable".
Enabled Access Methods	For a virgin cabinet, when the cabinet boots up, it tries to enable all of the subsystems for cabinet access, namely, 1) The CAC card, 2) Memory card, 3) HID / RFID cards, and 4) the Keypad-only access. These are only disabled when the GUI selection un-checks those access methods or the system can not find that equipment in the cabinet.

4.2.4 Normal Startup

When starting the system up normally, the system should be coming up from a power off condition. Upon applying power to the system, normally within 1 to 2 minutes, the CA cabinet should be ready for user access. The normal display will appear with the cabinet-name on the first line of the LCD, and the 24-hour time and date displayed on the second line. The cabinet name default is the SBC's computer name, but can easily be changed to any 20-character text string. This is easily modified using the CAC-GUI. In the following Illustration, the name has been modified to "PSS Inc CAC Cabinet". In the second line of the LCD display, the seconds should be incrementing every second. The following image illustrates a normal start-up display.

Illustration 1: Normal Display Indicating Cabinet is Ready for Access. Note Time Incrementing Every Second.

To validate the CACmanager software version operating on the cabinet, press the "**2nd**" key while in this "Idle" mode. Once pressed, system information will be displayed briefly, scrolling through various information pertaining to the cabinet. This includes the cabinet's IP number if operating in IPv4, the cabinet's maximum temperature sensed, the ON and OFF set-point temperatures of the fans, the access methods that are enabled, the number of available drawers, locked drawers, unusable drawers, the operating mode of the cabinet, the auto-add setting, the run-time (in hours) and the software release version. The following is an example LCD display sequence what would display on a cabinet that is configured for 20 drawers with one broken drawer sensor number 4, four "phantom" drawers that are not there (drawer numbers 21 through 24), but where the electronics are there to support future additions, and with drawers 8, 9 and 11 being used (checked-out):

Sequence	LCD Display
1	IpV4 192.168.1.11 Release 5.2.0
2	Max DR Temp 75.3 F ON: 90 OFF: 85
3	Avail: 14 Locked: 0 Unusable: 5
4	Access Enabled: CAC HID Keypad MEM
5	USED DRAWER #'s: 8-9 11
6	AVAILABLE DRAWERS #'s 1-3 5-7 10 12-20
7	UNUSABLE DRAWERS #'s 4 21-24
8	AUTO ADD-USER: ON Mode: MULTIPLE-ACCESS
9	RUN-TIME: 43.0 hrs Release: 5.2.0

Note that if say the Keypad was disabled via the GUI, the sequence showing the Access Enabled screen would not have 'Keypad' displayed. Also, the last display, as shown above indicates how long the CACmanager application has been running since the CACmanager was last commanded to reconfigure the drawer arrangement or since the last time the CACmanager was last started. For the maximum temperature displayed, if the system has just booted up, the temperatures of the fan-controller probes may not have been read so a display of -40 degrees would show up indicating an invalid temperature reading.

A normal system start-up is where the system power is switched on, the system boots up, and after approximately 2 to 3 minutes, it is ready for cabinet drawer and/or administrator access from the front panel.

The power-up sequence of the system should be setup such that the Single Board Computer (SBC) and the +12VDC power supply for the Relay and Fan boards come on at the same time. This is important.

This is important because these boards must be enumerated, i.e., identified by the system before the CACmanager task starts up automatically. If these boards are not enumerated, and all the ports on them before hand, then the CA system will not operate properly. This may or may not result in the detection that the cabinet should be reconfigured and a message displayed as a result. In the situation where the system needs reconfiguration, the front-panel LCD display will indicate this with a message displayed in the following illustration.

Also be aware that shortly after start-up the system may incorrectly determine that a reconfiguration is needed. After a few minutes, if this is the case, this "NEED TO RECONFIGURE" will clear automatically after the next set of drawer sensor queries have been completed and have reported back their states. In the condition that this does not clear, the system should be "Reconfigured" by the administrator, and can only be done via the font panel LCD/Keypad. In certain hardware conditions, the system may not detect there is an issue, but the system administrator may do a manual reconfiguration if they are having problems associated with drawer openings. The following display illustrates this condition:

Illustration 2: System's Built-In Self-Test Determined Reconfiguration Necessary.

When a reconfiguration is needed, the system administrator will need to log-in at the front-panel and do a system reconfiguration to assure all subsystems are configured correctly. In extreme cases, the power to the entire cabinet will need to be cycled off and then back on again, including cycling the UPS that powers the SBC, Relay and Fan boards.

4.2.5 Startup Failure

In the event of a power failure, the system's UPS will hold the power stable to the SBC and control boards (Relay and Fan boards) for approximately 30 minutes up to several hours, where the time-frame depends upon the UPS battery size, the number of drawers and fans in the system and the fan's activities. In extreme cases, an SBC may develop a glitch on power loss, and the system-administrator may need to provide assistance in rebooting by cycling power to the cabinet and electronics. The configuration of the Microsoft Windows 7 OS has been set to ignore any "aggravated" conditions which would require a reboot into "Safe-Mode" or "System Restore", but there are cases when the operating system will do an automatic file-system check and attempted repair without user intervention. In these cases, it may take Window 7 system up to 10 minutes to reboot. If the system does not reboot in this timeframe, then the system administrator needs to physically remove power from the system, shut-down the UPS, wait 15 seconds and then reapply power. Several attempts may be necessary for Windows-7 to recover. If this fails, the system would then need to be reloaded with both the OS and reinstall the CACmanager.

On a Windows 10 system, the startup failure is mostly caused by incorrect login parameters of SQL Server, so need to make sure the parameters in the file are the latest.

4.3 Access Management

There are two functional ways of opening drawers electronically; either with the CAC-GUI or with the front panel operations. The CAC-GUI access is covered in the CAC-GUI Operations section. For front-panel access there are several ways of opening drawers: 1) Keypad-only, 2) DoD-CAC card, 3) Memory card, and optionally, the 4) HID-RFID, 5) Parallax RFID card entry and 6) Temporary PIN. A brief description of each is listed in the following table.

Access Method	Description
KEYPAD ONLY	Access by using only the keypad and entering a 4 to 20 digit PIN code and then typing <ENTER>. Certain common "easy" keypad PIN numbers have been excluded out of the STAND-ALONE operations that the user can not pick, such as "1111", or "2222", "1234", etc. These "easy" password PINS are not excluded if entering them from the CAC-GUI, however in the CAC-GUI they must be at least 5 digits long.
MEMORY CARD	In STAND-ALONE operations, access is started by inserting either a SLE4442 or a SLE4428 memory card into the card reader, and then when prompted the user enters in the the appropriate PIN code for the Memory card. If the card has not been initialized, the holder of the Memory Card can NOT gain access; they must be assigned a TEMPORARY PIN via the CAC-GUI first. Once assigned, when the memory card is inserted in the cabinet, the system will notify the user that the card has not been initialized, and will ask for the old PIN and then a new Memory Card PIN and then for the TEMPORARY PIN assigned during CAC-GUI entry. If all are authenticated, the card is then initialized, and the system will not allow rewrites to this memory card so the memory card's new PIN will not be able to be modified. The SLE4442 cards require exactly 6 digits for the PIN code, and the SLE4428 cards require exactly 4 digits for the PIN code. When entering in the PIN, the keypad can be used to select the numbers 0-9. The 2nd key is used to select hexadecimal numbers A-F, silk-screened in red on the keypad. The <ENTER> key must be used to complete the entry. If the PIN is incorrect, the system will notify the user by displaying "PIN ERROR", and informing the user as to how many more PIN attempts they have left on the memory card to get the PIN correct before the card is
	"BRICKED," or nonfunctional.
DoD-CAC/PIV CARD	In STAND-ALONE operations, presenting a government-issued DoD-CAC card to the card reader and then the typing in users PIN code followed by the <ENTER> key will allow access.

HID RFID and RFID CARD	This these optional entry methods, and depend upon the original installation. If either the HID-RIFD or the Parallax RFID card readers have been installed, then this option is available. The user positions the HID or RFID card near the reader plate, holding it there for approximately one half of a second. The reader will automatically read the card and the system will search the database for the user and if found will automatically open the drawer. If not found, it will ask for the CAC card to add the user. Using the GUI, an HID card can be configured to require a "User ID". The cabinet handles this by first reading the card's ID and looking it up in the database. If it is not found, it will query the user for their "User ID." Once this is entered in, the database is again searched and if found when combined with the Card ID, it will allow access.
TEMPORARLY PIN	This a method a temporary user to access the cabinet to checkout and check in the device. It could be an employee forgetting his/her badge at home, or for a visitor. The administrator creates a temp user from CAC-GUI, and the temporary PIN can be sent with email to the user's account. The valid time length of the PIN can be one hour, one day, one week or other length. The PIN can be renewed by the administrator if needed. The usage of the Temporary PIN is like that of KEYPAD ONLY (see above).

In using the either the CAC card or the Memory-card, the system will alert the user that a bad PIN was entered and inform the user of how many more incorrect PIN entries in a row before that particular card becomes BRICKED, such as the following display:

4.3.1 Receipts

The system will automatically generate a receipt for the equipment checked out of the cabinet. Receipts are generated only for Check-Outs, and not for Check-Ins. Also note that receipts are never generated for the Administrator opening and/or closing drawers, but only for users checking out drawers. If enabled by the CACGUI, and a printer has been set-up on the cabinet computer, including networked or shared printers, receipts will be automatically sent to this printer for each check-out. Note that a maximum of 6 pieces of equipment can fit on this receipt form.

I acknowledge receipt of and responsibility IAW AFI 23-111 for the items described below and will return them upon mission completion.

ISSUED TO: SIGNATURE	DUTY PHONE	ISSUED BY:
Digital signature: A516BD847A0DA5FC41F90DCA6EDB4D61	407.293.4505	Cabinet OSS/OSK-0123
ISSUED TO: LAST, FIRST, RANK	**SQUADRON**	**DATE ISSUED**
KARPEL, MARC, Civilian	373 Training	10/23/2012 22:41:07

IDENTIFYING NUMBER	DESCRIPTION OF ITEM	U/I	QNTY
#CF19-037	Panasonic CF-19 Laptop S/N 037	Ea	1
#CF19-038	Panasonic CF-19 Laptop S/N 038	Ea	1
#CF19-039	Panasonic CF-19 Laptop S/N 039	Ea	1
#CF29-123	Panasonic CF-29 Laptop S/N 123	Ea	1

Legibly fill in all yellow areas and return to the 60 OSS/OSK HILL AFB DSN 777-7221/5775

AF FORM 1297 , JUL 87 (EF-V2) (PerFORM Pro) PREVIOUS EDITION WILL BE USED TEMPORARY ISSUE RECEIPT

Setup and automatic printouts of these Check-Out receipts are covered in the "*CAC-GUI Operations*" section.

4.3.2 Keypad-only Access

To gain access to the system through the keypad-only entry method, the user types in their PIN code. If the Keypad has been disabled via the GUI control, a temporary access can be enabled by pressing the "HELP" key. After "HELP" is pressed, then for about 1 minute the Keypad-Only access will be enabled.

When gaining access via the Keypad-Only, the user just starts typing their PIN-code on the keypad. The PIN code would most likely have been first entered in using the GUI. Shown below is the Keypad.

Illustration 4: Keypad. Used for PIN Entry and System Admin Functions.

As soon as the first digit is entered, the LCD display will change, displaying the asterisk (*) as each digit is entered. A minimum of 4 PIN digits and maximum of 20 PIN digits are accepted. For a 10-digit PIN, and before typing the ENTER key, the display will look like the following.

Illustration 5: LCD Display for PIN Keypad Entry after 10-digits

Once the digits are complete, the user must type the “ENTER” key on the keypad for the system to check the database for allowing or denying access.

Any time that the system cannot match a user entry to the database, it will display “ADDING NEW USER” and “INSERT CAC CARD” on the LCD as follows:

Illustration 6: Adding New Users Not in the Database

In MULTIPLE-ACCESS mode, when the database matches the user's credentials, the system will display the user's name and prompt the user for which drawer number that the user needs access to for check-out. It then will open the drawer and log the user as checking out that drawer, and then ask for the next drawer. The user either presses the CANCEL button on the keypad or waits for the system to automatically time out. If any of the requested drawers are in use, then the system notifies the user that that drawer is “IN USE” and prompts for a different drawer number.

In FIXED-ACCESS mode, after a database match of the user's credentials, the system will display the user's name and drawer number assigned to them. The system will then open the drawer and log the user as checking out this drawer. If that drawer is in use, then the system notifies the user that that drawer is “IN USE” and then the system goes back into an idle state.

In FIRST-AVAILABLE mode, when the database matches a user's credentials already in the database, the system will display the user's name and automatically open the next available drawer which has been checked-in the longest. This is to maximize the check-in time for tools that have batteries needing charging. When checking in a drawer in this mode, when the user's credentials are matched, the particular drawer that was checked out previously will open automatically and the system then logs the time the user had it checked out. In all cases, the system logs the check-in's and check-outs into log files. The CAC-GUI transfers one of them over to the workstation to process for specific activity reports, and the other log file, which is an html formatted file, remains on the cabinet computer as a legacy logfile for an admin at the cabinet if needed to be viewed.

When a user has administration privileges, the LCD will display an ADMIN ACCESS and the user is allowed to perform administration activities. Note that there can be multiple administrators, but should never be zero.

4.3.3 Memory-Card Access

To gain access to the system using a memory card, the user presents the card to the card reader by inserting the contacts facing up as shown below. Note that if the Card-Reader's LED is on the right-side of the card slot, then the contacts would be oriented with the gold contacts facing-down

Illustration 7: Memory Card Almost Inserted for Presentation to the Card Reader. Note that the Gold Contacts are Right-Side Up.

Once the card has been completely inserted and the system recognizes the card, the system will ask the user for the memory card PIN code as shown below.

Illustration 8: System Prompt for User to Enter the Memory-Card PIN.

The user will then enter the PIN code and complete the PIN sequence by typing the <ENTER> key on the keypad.

Illustration 9: Alert to User that Memory Card is Blank.

If the memory card is uninitialized, the system will alert the user as follows and prompt the user to enter a new PIN for this blank memory card. This new memory card PIN must have the exact number of digits for that particular memory-Card, but is any PIN code that the user chooses.

Illustration 10: System Prompt for User to Enter the Memory-Card PIN.

Next, but not shown, the system will ask the user for a "TEMPORARY PIN" assigned when enrolling a new Memory-card via the CAC-GUI interface. Once the TEMPORARY PIN has been successfully entered, the display will show that the card is now ready be used.

Illustration 11: Memory Card Ready to Use in System..

If the memory card has already been initialized and was not enrolled by the process above, and this memory card is not in the system database, then when the user inputs the correct memory-card PIN, then the system will prompt the user to insert their CAC card. Once the CAC card has been verified with the CAC PIN, this new Memory-Card user will be added to the system database, and depending upon the cabinet mode, a drawer will automatically open if in FIRST-AVAILABLE, or the user will be prompted for the drawer number if the system is in MULTIPLE-ACCESS mode, etc.

Note: The user must know the number of memory card PIN digits and the correct memory card PIN code to gain access. If the card has not yet been initialized, the card still has the default PIN code stored in it, and that

PIN code needs to be known. Once the PIN code is authenticated correctly, the system will notify the user that the card has not been initialized and will automatically initialize the memory card. Note that default memory card PIN codes for the SLE4442 and SLE4428 memory cards are set according to the card manufacturer's policies and procedures.

The system is setup to accept SLE4442 and SLE4428 memory cards. For authentication, the card type has a limited number of failed attempts at trying to gain access to the cards' data, and once the maximum number of consecutive attempts are made, the card will be blocked or BRICKED from further attempts. The remaining number of attempts are displayed on the LCD if the user enters the PIN incorrectly as follows:

Illustration 12: Warning to User for Number of PIN Attempts left before Card is Bricked.

Typically for the SLE4442 card it is 3 failed attempts in a row, and for the SLE4428 it is typically 8 failed attempts in a row to cause the card to be BRICKED. If a successful PIN authentication is performed before the card has become BRICKED, the card's internal failed-attempt-counter is reset to zero, as if there were no failed attempts.

4.3.4 DoD-CAC/PIV-Card Access

To gain access to the system using a DOD-CAC card, the user presents the card to the card reader by inserting the card with the contacts right-side up as show below, and then waiting for the system to display a prompt for CAC PIN entry:

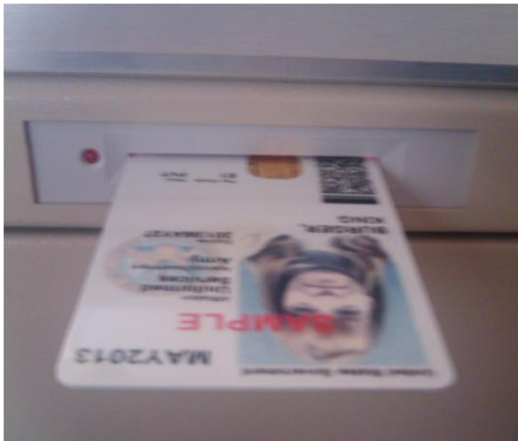


Illustration 13: DoD-CAC Card Almost Inserted for Presentation to the Card Reader. Note that the Gold Contacts are Right-Side Up.

The system will prompt the user for the CAC PIN code by displaying the following on the LCD:

Illustration 14: System Waiting for PIN entry for DoD-CAC Card

Note that the user has approximately 10 seconds to type the first PIN digit and only about 5 seconds per digit for any successive PIN digits. Once the user enters the entire PIN code in, an additional 5 seconds are given to complete the PIN sequence by typing the <ENTER> key on the keypad. For FIRST-AVAILABLE mode, the next available drawer will open automatically, and if in MULTIPLE-ACCESS mode the user will be prompted for the drawer to open.

For the ability to hide all personal data read from a user's CAC Card, the system has an option enabled by default (changeable via CAC-GUI) to not save the user's name or other personal data in the database when read from the CAC-card. This option is named “AUTO-USER-NAME” and will automatically insert “John Doe x” for each successive CAC users that is automatically enrolling themselves at the cabinet's font-panel.

Also keep in mind that the user must know the number of CAC PIN digits and the correct CAC PIN code to their own personal CAC card to gain access. If their CAC card has not been initialized, then the system will not allow the user to create a new cabinet access account. Also note that the system never tries to write any data or CAC PIN codes to the DoD-CAC cards. The only access for CAC cards is reading the CHUID and person-data information from the card.
Concerning authentication, as with the memory-cards, the CAC Cards only have a limited number of failed attempts at trying to authenticate the CAC PIN code, and once the maximum number of consecutive attempts are made, the card will be blocked or BRICKED from further attempts. Typically for the standard DoD-CAC card it is 3 failed attempts in a row. If a successful CAC PIN authentication is performed before the card has become BRICKED, the card's internal failed-attempt-counter is reset to zero, as if there were no failed attempts.

4.3.5 HID RFID Card Access (Optional)

For systems that are equipped with the optional pcProx HID RFID card reader, this will enable the system to read ProxCard® II HID RFID cards manufactured by the HID Corporation. For the user’s that already have an entry in the database, gaining entry is very simple. The registered user in the database gains access by first presenting the RFID card in front of the HID RFID reader. If the user’s HID card has been entered into the database via the GUI without a User ID, no further action by the user is needed. If the User ID was utilized during the registration process, then the User ID will be queried to be entered via the Keypad.

If the system mode is in FIRST-AVAILABLE mode, then the next available drawer is automatically opened once the user’s unique signature from the swiped RFID card (plus User ID if needed) is validated in the database. If the HID RFID ID is not in the database, the system will prompt the user to insert their CAC Card

to register the new HID RFID card so that cabinet access using this HID RFID card can be tracked to the user. Otherwise if there is not CAC card reader, the user must be registered via the GUI.

The HID RFID card-reader utilized in this system is a RFIDeas Inc. OEM Module which is a USB based card reader. The model number is #RDR-60N2AKU, and information about this reader can be found at their website: (http://www.rfideas.com/products/pcprox_readers/pcprox_enroll/OEM.php).

4.3.6 Parallax RFID Card Access (Optional)

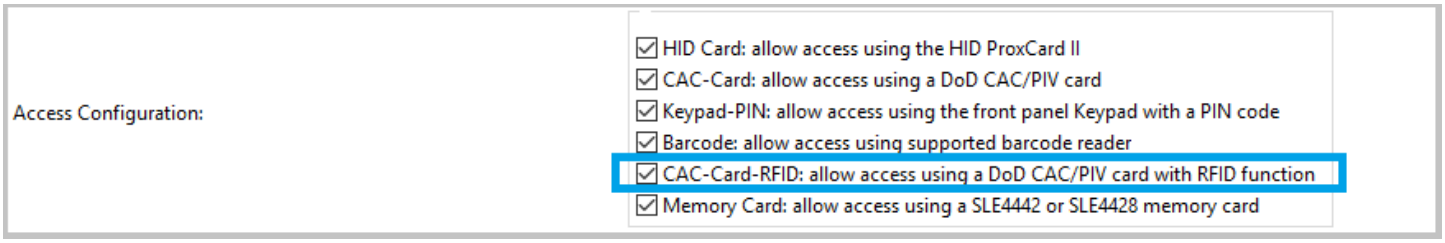
For systems that are equipped with this optional RFID card reader, the user's that already have an entry in the database, gaining entry is very simple. The registered user in the database gains access simply by presenting the RFID card in front of the RFID reader plate. This is typically about 1/4" from the metal control panel cutout for the RFID reader. Unless the serial numbers of the Parallax RFID cards are known, there is no way to register Parallax RFID cards by way of the GUI; these type cards must be registered via a CAC card user/holder.

If the system mode is in FIRST-AVAILABLE mode, then the next available drawer is automatically opened once the user's unique signature from the swiped RFID card is validated in the database. If the RFID ID is not in the database, the system will prompt the user to insert their CAC Card to register the new RFID card so that cabinet access using this RFID card can be tracked to the user.

The RFID card-reader utilized in this system is a Parallax Module #28340, which reports a 12-digit unique ID read from the RFID card or tag. Only 125 KHz RFID cards or tags are supported (EM-4100 family). Additional RFID card-readers can be integrated into the system upon request.

4.3.7 CAC-Card RFID

Some CAC-Cards have built-in RFID function besides the regular CAC function. The RFID function can be taken advantage of for its convenient use. The two functions (CAC and RFID) of the card can be internally linked together for the user. In order to use the RFID function for a CAC card, the related access method should be selected. The following is the screenshot:



After CAC-Card-RFID is selected in Access Configuration, the user can use either CAC (with PIN) or RFID for the device checking in or checking out, and the management system will regard it as the activity of the same person. Basically, the user can use CAC function to check-in and checkout, or use CAC to check out and use

RFID to check in, or use CAC to check in and use RFID to check out, or use RFID for both check-in and checkout.

The CAC-card user needs to do an initial setup in order to use the RFID function in the card. The setup is relatively easy, after the user successfully access the system by using CAC-card function, the screen will give direction to scan the card on the RFID reader. After the user have scanned the card, the RFID information will be added to the user, and the setup is done.

By the way, if the cabinet requires a PIN for the RFID usage, the user also needs to setup and use a PIN number, this can be done by following the standard RFID procedure.

5 CABINET CONFIGURATIONS

This chapter is about the major configurations of the cabinet. There are also some configurations illustrated in other chapters based on the topic.

5.1 Basic Configuration

Most configuration needs to be done with *CAC-GUI*, some setups are only available with the cabinet keypad.

The *CAC-GUI* has the following basic configuration items; they are mostly located in *System Config* tab:

Remote Cabinet IP: This is the computer IP address of the cabinet. When *CAC-GUI* is running on the cabinet computer locally, the IP is *localhost* or *127.0.0.1*. This is automatically generated, does not need to be changed, and the field is read-only. A screenshot is as following:

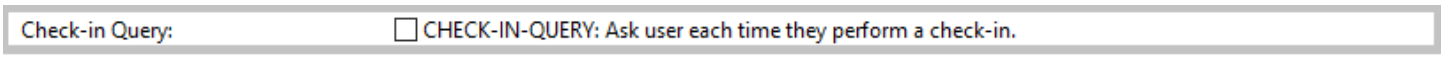
Cabinet Name: The name of the cabinet. It appears in all the display, log, report and email. This is not the computer name of the cabinet.

Total Drawer Number: The number of total drawers of the cabinet. For a system with multiple cabinets, it is the add-up of all the drawers of master cabinet and the slave cabinets (more details in section *Cabinet Cluster*)

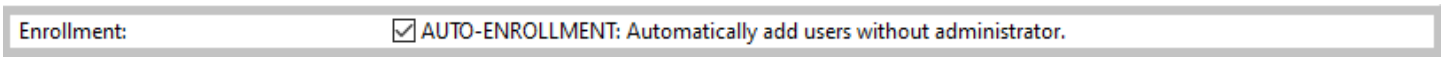
Control Board IP: The IP address of the control board. The cabinet computer communicates with the control board with ethernet. The IP address is fixed for the cabinet. Normally user does not need to change this value.

Control Board Port: The port number of the control board. The value is fixed with the cabinet.

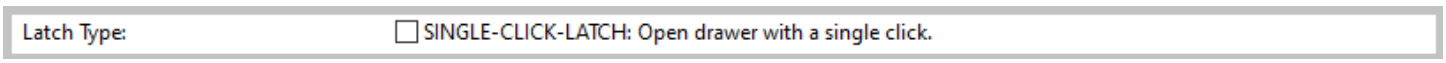
Check-in Query: Need confirmation when the user check-in a device. The default setup is OFF.



Auto Enrollment: Automatically enroll new users without the help of administrator. The new user is added into the database when he/she is accessing the cabinet.

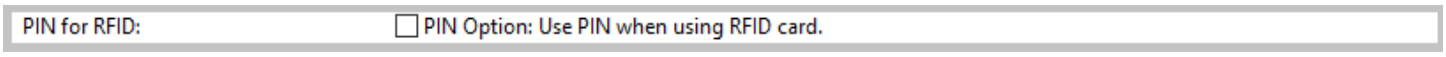


Latch Type: When selected, the cabinet is using Single-click-latch; otherwise the cabinet is using Double-click-latch. This setup is hardware related, normally the user does not need to change it.

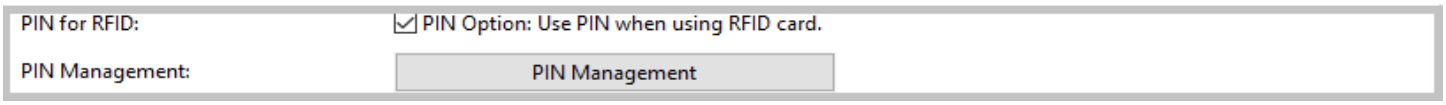


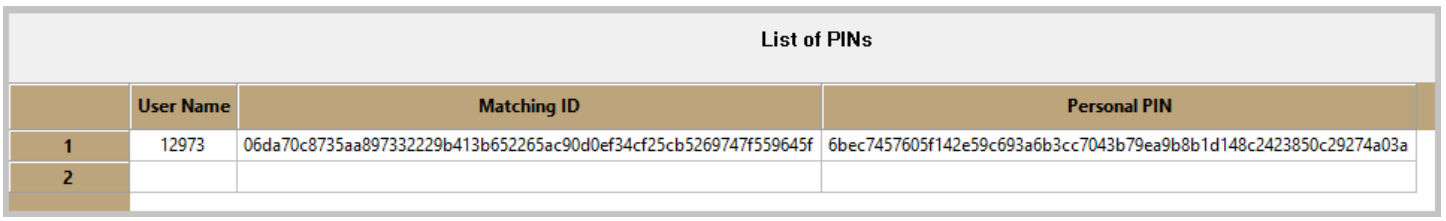
PIN for RFID: When chosen, the RFID card users need a PIN number on top of the RFID badge to access the cabinet. The default setup is OFF.

The PIN can be created with the cabinet keypad when the user accesses the cabinet at the first time.



PIN Management: The setup is valid only when *PIN for RFID* is ON. When the button is pressed, a window will popup; it shows the list of the users with PIN number. The user can be removed from the database for the user to setup a new PIN number.





List of PINs

	User Name	Matching ID	Personal PIN
1	12973	06da70c8735aa897332229b413b652265ac90d0ef34cf25cb5269747f559645f	6bec7457605f142e59c693a6b3cc7043b79ea9b8b1d148c2423850c29274a03a
2			

Fan on Temperature: The temperature when the fan is turned on automatically. This is legacy setup; user does not need to change.

Fan off Temperature: The temperature when the fan is turned off automatically. This is legacy setup; user does not need to change.

Barcode User Trim: For the users using barcode reader to access the cabinet, the barcode has leading zeroes in some situations. When this setup is chosen, the leading zeroes will be removed in the barcode.

Number of Control Boards: The total number of the control boards used in the cabinet, or cabinets in master-slave structure. The maximum number of control boards is 10.

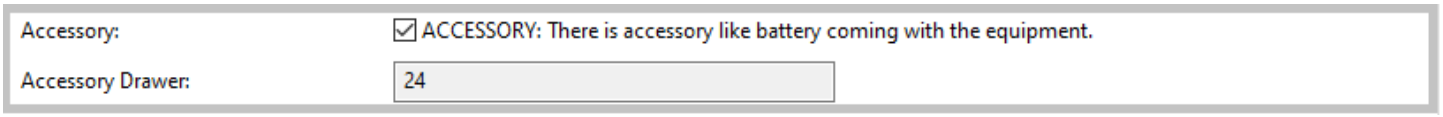
Port Number of Control Boards: The port number for each control boards. It can be set up as 16 ports or 48 ports.

For the configuration from cabinet panel, the details will be introduced in section *5.3 Administrator Activity*

5.2 Accessory Setup

The user has an option to store an accessory in the cabinet accompanying with the device; the number of the drawer can be set up from *CAC-GUI*. When this option is selected, the drawer with the accessory will open after the device drawer has opened. For a checkout process, the accessory drawer is opened for the user to get the accessory; and for a check-in process, the drawer is opened for the user to return the accessory.

A screenshot for setting accessory is as following:



5.3 Administrator Activities

To log on to the administrator, either use the factory-default Keypad-Only PIN if it has not been deleted or, if a user has been added and assigned administrator privileges, use that account. Once logged in, the administrator can manage many of the aspects of the system. In most of the administrator activities, the CLEAR button will cancel the current operation and log the administrator out if currently at the top menu. Otherwise the system administrator will have the option to do multiple tasks before logging out of the administrator account. The HELP button suggests that the user refer to this user's manual. The following is displayed when an administrator has logged in:

Illustration 15: Administrator Access Activity Prompt Display

When in this administrator mode, the system will time-out if there are no key presses for approximately 20 to 30 seconds. Upon timeout the administrator will then be logged out, and the system will again be ready for normal access.

When an administrator logs in, the system will query the administrator for what type of activity is requested. As indicated above, the administrator uses the up and down arrows on the keypad to scroll up or down to select the desired activity.

The following table lists the activities that the administrator can select by pressing the up and down arrows on the keypad. To select the desired activity, scroll to that activity and then press the ENTER key.

Activity Selection (Displayed on bottom line of LCD)	Description

OPEN DRAWER	Opens any drawer in the cabinet. If a drawer is selected that is not detected in the system, the system will indicated that it can not find that drawer. If the drawer selected is a drawer currently checked out, the administrator is prompted for checking that drawer in. If the administrator chooses to check this drawer in, then that drawer is marked as checked-in and the checkin/check-out cycle is reset, otherwise the drawer remains in the checked-out state.
CHANGE CABINET MODE	Switch the cabinet's operating mode between FIXED-ACCESS, FIRST-AVAILABLE and MULTIPLE-ACCESS, CHECK-IN-ONLY, and CHECKOUT-ONLY. In FIXED-ACCESS, a user account is assigned a single drawer and can not access any other drawer. For the FIRST-AVAILABLE mode, the system finds the drawer that has been checked-in the longest and opens it automatically for the user. In MULTIPLE-ACCESS mode, the system prompts the user for which drawer the user wants to open. The display will display:

	"MODES: 1=1st 2=Fixed" "3=Mult 4=Cout 4=Cin" This allows the administrator to select which default mode to run the cabinet in. This default setting will then be saved in the CACconfig.cfg file as one of the default settings.
CHANGE AUTO ADD-USER	Change the system's operations between allowing users to be entered into the system (ON), and prohibiting any new users from being added to the system (OFF). Other than the CAC-GUI, this is the only way to create new user accounts. This setting is saved in the CACconfig.cfg file as one of the default settings.
DELETE / MODIFY USER	Delete or modify a user that is currently listed in the database. If the user is listed as an administrator, this user can not be deleted from the front panel. To delete an administrator, this user must first be changed to a "Normal User" before they can be deleted. Use the keypad as follows for modifying: 1="Normal User", 2="System Administrator", and 0=Delete this user.
ADJUST FAN TEMPS	Adjust the turn-on and turn-off temperatures of the fan cooling system. This sets all of the fans to the same on and off set-points. Note that the alarm setting for the piezoelectric buzzer is set to 18 degrees F above the turn-on temperature. This alarm set-point is not independently adjustable, but tracks the turn-on temperature.

RECONFIGURE SYSTEM	Force the system to query the drawers and then match the drawer numbers to the desired physical location in the cabinet. If a drawer is malfunctioning, that drawer is marked as “Unusable” and flagged not to be used by the system. For systems that have more latch circuits than the number of drawers, the system will ask for these drawers to be closed, and when after a time-out period, these drawers will be marked as “Unusable.”
SYSTEM POWER DOWN!	Before removing power from the system, the cabinet should be shut down gracefully. This selection performs a graceful shutdown. Once the LCD backlight turns off and is blank, power can be safely removed.
RESTART SYSTEM	This option allows the SBC to be rebooted. This may be useful when the system administrator suspects that Windows 7 needs to be rebooted.
QUERY FOR CHECK-IN's	If this option is selected, then the admin can force every user to answer a yes/no question each time they check drawers back in, as to their desire to keep the drawer checked out or check it back in. This allows a user to keep the drawer checked-out and reopen the drawer to get out a cable or other miscellaneous item.
LOCK & UNLOCK SYSTEM	Locking the system will prevent any user from opening the specific drawer locked out. If the whole system is locked out, no drawer can be checked out. In the cases where drawers are already checked-out, those users can check-in their drawers even if the drawer has been locked.

5.3.1 Opening Drawers

While in administrator mode, and the Open Drawer selection activity is chosen, the display will show:

Illustration 16: Admin Open Drawer LCD display.

Using the 0-9 keys followed by the <ENTER> key will select and open the drawer number desired. After the selected drawer is opened, the LCD will prompt the user for the selection of another drawer number. Once finished, the user should press the CLEAR button to go back to the top level menu for other administrator activities. Pressing the CLEAR button one more time or waiting for approximately 20 to 30 seconds without any activity will cause the administrator account to log-out.

If the drawer selected is already checked-out, and the CHECK-IN-QUERY options is enabled, then the administrator is prompted for checking in this drawer or keeping this drawer checked out as follows:

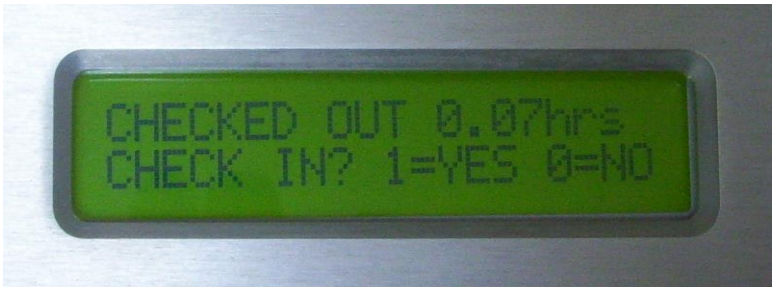


Illustration 17: Admin Opening Drawer already Checked-In.

If 0=NO is selected, the drawer will not be checked-in but the drawer will be opened and the activity log files will record this activity, including the drawer number, user, etc., and save it to the activity log file. If 1=YES is selected, then drawer is opened, checked-in and the check-in/check-out cycle is reset. This activity is also recorded in the activity log files.

For the 0=NO, the system shows that this drawer is still checked-out as follows:

Illustration 18: Administrator Opens Drawer but Leaves Drawer Checked Out.

5.3.2 Add User (Registered Automatically)

There is no administrator selection for adding users, as users are added automatically when the "CHANGE AUTO ADD-USER" option is turned ON as discussed earlier. Independent of most access methods used, the system will query the user for their intentions and if positive, try and register the user when the user is not found in the database. The process is the same for user's with keypad-only PIN, HID RFID, and RFID entry. This also works with Memory-Cards that have been initizlized, but requires a different procedure for blank Memory-Cards, as discussed earlier. For users that are added at the front-panel, this always requires the user to insert their CAC card during the registration process. This is illustrated as follows for prompting the user:

Illustration 19: New Users are Added Automatically if Not Found in the Database.

Note that for this card reader the LED is on the right, so the CAC card needs to be facing up as shown in the following illustration:

Illustration 20: Inserting and Authenticating a DoD CAC Card During Enrollment.

Once the CAC card is inserted, the user is prompted to key in the matching CAC PIN followed by the <ENTER> key. **It is important that the user uses their CAC PIN associated with the CAC card:**

Illustration 21: PIN Associated with the CAC Card must be Typed Followed by the ENTER key.

Once the PIN is authenticated successfully against the CAC card, the user will be added into the database and if in FIRST-AVAILABLE mode, a drawer will automatically open, or the user will be prompted for the drawer number if the system is in FIXED-ACCESS or MULTIPLE-ACCESS modes. If the drawer selected is used or locked or the PIN is incorrect, the system alerts the user as such.

The following example is when the system is in FIRST-AVAILABLE mode, and the next available drawer happens to be drawer 4. In this case the CAC card "person data" information is read as "john doe" and is the default user name for this user. To change this name, once the finished with this process, the administrator can simply use the GUI and edit the name and ID number if so desired.

Illustration 22: Once Successful, the "person" information is Taken from the CAC Card, Concatenated Name is Displayed as in the Example Here as: "johndoe" and Drawer 4 is Automatically Opened and Check out to this New User.

5.3.3 Change Cabinet Mode

The administrator can change the cabinet mode between FIXED-ACCESS, MULTIPLE-ACCESS, FIRSTAVAILABLE, CHECK-IN-ONLY, and CHECK-OUT-ONLY modes. Scroll to the "CHANGE CABINET MODE" as follows:

Illustration 23: Scrolling to "CHANGE CABINET MODE".

and now press the <ENTER> key, and the display shows the selection for FIXED-ACCESS, FIRSTAVAILABLE or MULTIPLE-ACCESS with the LCD showing:

'MODES: 1=1st 2=Fixed'

'3=Mult 4=Cout 4=Cin'

Pressing the 3 button selects the MULTIPLE-ACCESS and the system notifies the administrator it is saving it as a default setting.

Illustration 24: MULTIPLE-ACCESS Mode Selected and Saving as New Default.

5.3.4 Change Auto-Add-User

The administrator can also change the mode for adding or prohibiting new users from being added to the system database. Select the "CHANGE AUTO ADD-USER" option while logged in as the administrator as follows:

Illustration 25: Selecting AUTO ADD-USER to Enable/Disable Adding New Users into the System.

Turn the add-user on or off by using the 1 or 0 keys as follows:

Illustration 26: Option to Enable or Disable the Add New Users Option via 1 or 0 key.

Selecting the 1 enables the add-user option and the display shows the following:

Illustration 27: Adding New Users is Now Enabled..

5.3.5 Delete / Modify User

A user can be deleted by selecting this activity and then scrolling to the desired user to delete or modify using the Up/Down keys. Once the ENTER key is again pressed, the display shows the options for modifying or deleting that user, as shown below.

Illustration 28: Scrolling Up/Down to Find User to Modify or Delete.

Illustration 29: Typing <ENTER> once the user "johndoe" has Been Selected Displays the (0/1/2) Options for for the Administrator to Select.

In this example the administrator scrolls using the Up/Down arrows to find "johndoe" who is registered in the system as an RFID user with person data information ID as: XXXXX0664. Note that neither personal ID numbers nor SSN numbers are recorded automatically, but a 10-digit randomly cabinet-generated sequence number based upon each CAC card used is created if the user is enrolling via the front panel. If enrollment via the CAC-GUI, then most alpha-numeric combinations, and duplicate ID's can be used when entering this information via the GUI.

Pressing the 0 key deletes the user, pressing the 1 key turns the user into a normal-access user, and pressing the 2 key turns the user into an administrator user. When deleting the user, the system does not ask for conformation so care should be taken when deleting. The system will not let an administrator delete an administrator account. To delete an administrator account the account must be modified into a normal user account first and then it can be deleted. This helps prevent accidental administrator lockout.

5.3.6 Adjust Fan Temps

The on and off set-point temperatures for the fan cooling system can be controlled by the administrator. This selection allows the administrator to change the temperature at which the fans will come on and be shut off. The temperature sensors are mounted on the inside of most drawers, so depending upon the equipment in each of the drawers, the fan associated with a 4-drawer-set may be on while another fan associated with a different 4drawer-set may be off. Also note that the piezoelectric buzzer alarm is set to annunciate if either the fans are impeded / obstructed so as to cause excessive current flow to the fans, or if the temperature exceeds the ON setpoint by 18 degrees Fahrenheit (Hot-Alarm Set-point).

Illustration 30: Activity to Adjust the Cooling System On and Off Set-Point Temperatures.

Once this activity is selected, the operator can select the ON temperature for the fans by pressing the 1 key, and pressing 0 key to select the OFF temperature set-point, as prompted below:

Illustration 31: Adjust either the Turn-On Temperature, or Turn-Off Temperature of the Fans.

Pressing 1 will display the Fan temperature adjustment default window as follows:

Illustration 32: Mode to Adjust the ON Temperature of the Fans.

Thereafter for each of these, the Up/Down arrow keys to increment or decrement the temperature set-points can be used. The operator can switch between ON and OFF temperatures simply by pressing the 0 or 1 key again. The <ENTER> key will send the temperature set-points to all of the fan-controller boards, and will take several seconds to complete.

Note that the temperature at which the fans are programmed to turn OFF is at least 5 degrees F below the point at which they are set to turn ON. This is done to add hysteresis so as to prevent the fans from cycling on and off too rapidly.

Below shows the fans being set to turn on above 103 F and turned off below 90 F. Keep in mind that each fan controller may be sensing warmer or cooler spots and all the fans may not turn on or off at the same time.

Illustration 33: Saving the Temperature On/Off Settings of the Fans.

Also, note that once these settings have been saved to the Fan-controllers, these settings are preserved over power cycles and reboots, and can be modified via the CAC-GUI.

5.3.7 Reconfigure System

This item is legacy setup.

If the administrator selects the activity for system reconfiguration and answers yes to reconfigure, the system will try and access all known relay latches in the system and open each of the drawers.

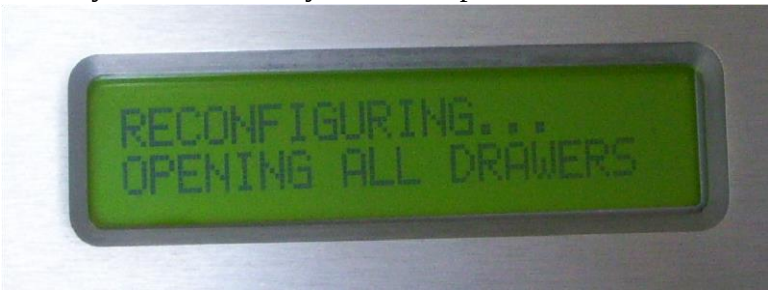


Illustration 34: Reconfiguration for Drawer Number Assignment.

Once all of the drawers are opened, the administrator will be prompted to close them one at a time, starting with drawer number 1, as shown below.

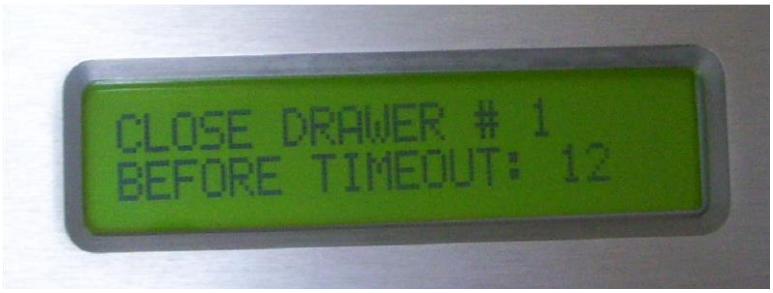


Illustration 35: Close the Drawer for Cabinet Drawer number Assignments.

The system does not care which drawer is numbered 1, 2, etc., as it is up to the system administrator to decide. This allows the drawer numbers to be reassigned in a random fashion if desired. The assignment occurs when

the system instructs the operator to close each of the drawers. Drawer number 1 is the first drawer that is closed, drawer 2 the second drawer that is closed, and so on.

Once all of the drawers are closed, the system will update the port to drawer map file and log the administrator out and will then be ready for normal access. If any drawers are malfunctioning and can not be opened, or the system can not sense that they are closed once opened, the system will flag them as "Unusable" and will not allow the users to access this drawer or drawer-set. This includes extra port drivers for drawers that are nonexistent.

If the administrator is not able to reconfigure the system successfully, then the administrator should shut the entire cabinet down gracefully, and remove and recycle power to the entire cabinet, including any uninterpretable power supplies for both the SBC and the +12VDC power supply that runs the control boards. A second reconfiguration may be necessary, but the system should come up and run stably thereafter.

5.3.8 System Power Down

Power-cycling the system should be done by shutting down the system gracefully. This is done by the administrator selecting the "System Power Down!" Activity as shown below.

Illustration 36: Powering the System Down Gracefully.

Once this activity is confirmed by the administrator for shutdown, the system will power down the SBC and devices attached to it. Several subsystems will not be powered down and will require the administrator to physically remove power, such as the FAN controller and Relay board. Once the LCD display is powered off by the SBC, power can be safely removed from the entire cabinet.

The system can be shut down from the CAC-GUI as well.

5.3.9 Lock-out Drawers

Drawers can be locked out from the CAC-GUI or from the front-panel. Refer to the CAC-GUI Operations section for GUI control for drawer lockout and user lockout. From the front-panel, drawers can be locked-out by the system-administrator so that users cannot open drawers except for checking in. Any number of drawers can be locked, or all drawers at once can be locked or unlocked.

To LOCK or UNLOCK drawers, the system administrator logs in and selects the "LOCK & UNLOCK SYSTEM" as illustrated below:

Illustration 37: System Administrator Selection for LOCK / UNLOCK for the Entire Cabinet.

Pressing ENTER allows the administrator to choose which mode to operate in as shown below:

Pressing the Up key allows the administrator to lock or unlock all of the drawers at one time as shown in the

Illustration 38: Enter Either the Drawer Number to lock or the Up Key to Select All Drawers.

following display:

Illustration 39: Pressing 0, 1, or Down Keys will Select Which Locking Option to Select.

In this example the administrator presses the 1 key to lock all of the drawers in the system.

Illustration 40: Pressing 1 Locks all Drawers.

In the case of selecting a single drawer, as follows, the administrator is prompted to either lock or unlock that particular drawer:

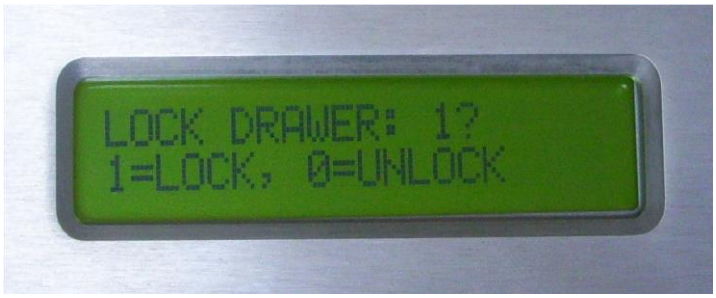


Illustration 41: Pressing 1 Locks Drawer 1, Pressing 0 Unlocks Drawer 1.

Once the "1" is selected and the ENTER key has been pressed, the following display shows the system in the process of locking out drawer 1.

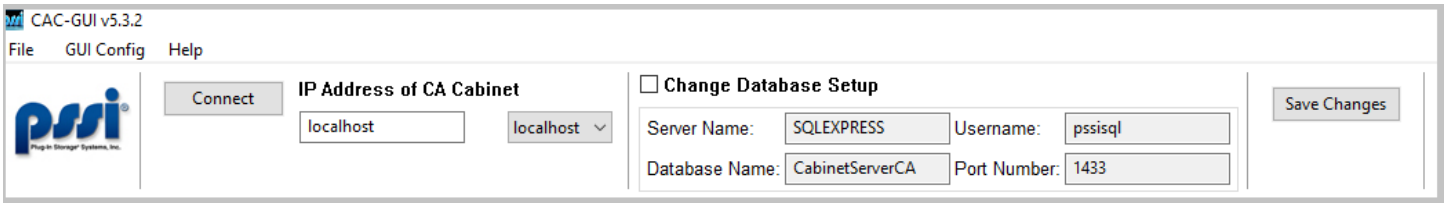
Illustration 42: Display after Selecting to LOCK Drawer 1. No Other Drawers are Affected.

If the selected drawer or entire system has been LOCKED, and later on, a user tries to access a drawer that is checked-in, that user will be denied access and the system will inform the user that that drawer is locked-out.

5.4 Database Parameter Setup

Before the CAC-Manager program is running, some database parameters need to be set properly. The best way to do it is to log into *CAC-GUI* locally at least once.

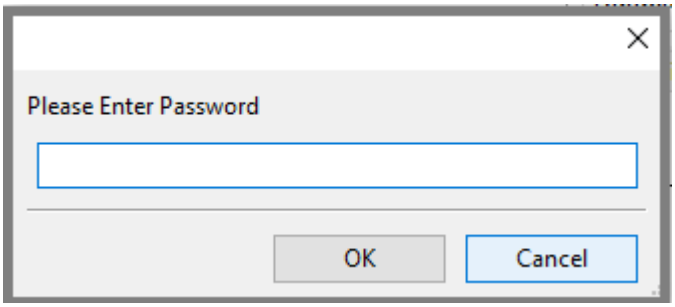
The login information is in the upper section of *CAC-GUI* screen. A screenshot is as following:



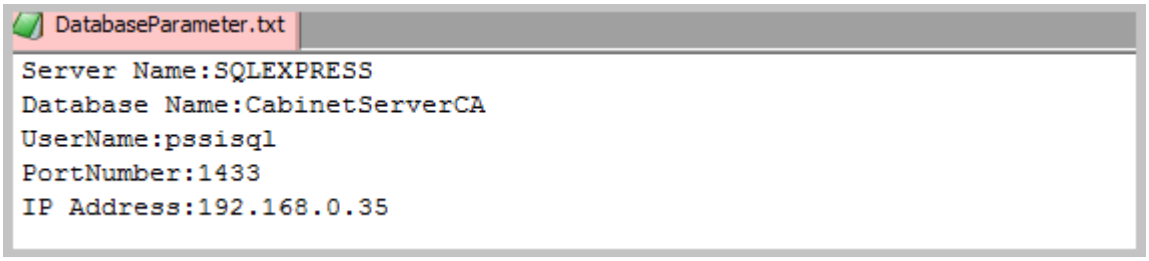
IP address column is filled in automatically when it is in local computer of the cabinet. There is also a pull-down list for all the history IP address for the convenience of login.

The right side of the section is the list of parameters for the SQL Server database: *Server Name*, *Database Name*, *Username and Port Number*. This information is read-only by default. It needs to select *Change Database Setup* option box to enable the information change.

When all the parameters are filled, click *Connect* button, for the first-time login or when the password has been changed, a window will pop up for the input of password. If the password is not correct, it will prompt the user to input again. There are 3 tries before *CAC-GUI* program exits.



After having logged in successfully, the parameters are saved in a txt file with the name of *DatabaseParameter.txt* in folder *C:\Users\PlugInStorage\AppData*. An example of the file content is as following:



The password is encrypted and saved in a different file named *mssql_bytes.bin* in the same folder.

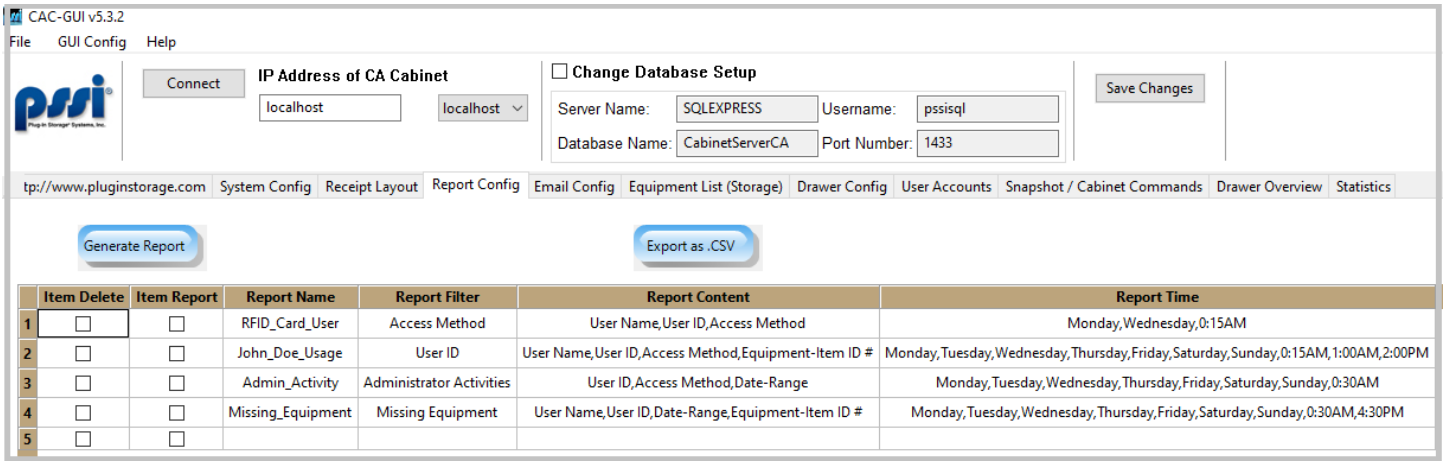
When *CAC-GUI* starts up, it will search the above files and fill the parameter automatically when pressing *Connect* button. If the auto-login fails, a window will pop up for the input of password.

The file *DatabaseParameter.txt* is required for running of *CacManager*; otherwise *CacManager* will go into a loop for database error. After a successful login of *CAC-GUI*, the file is generated and ready for *Cacmanager* program to use.

5.5 Report function setup

The cabinet can generate report from the activity log. The log can be tailored by the filter and content setup; when the report is configured to be sent by email, the time/date of the sending can be set up. The report has two types of files: *.csv* format and *.pdf* format.

Report management locates at *Report Config* tab of *CAC-GUI*. A screenshot of the example of is as following:



	Item Delete	Item Report	Report Name	Report Filter	Report Content	Report Time
1	☐	☐	RFID_Card_User	Access Method	User Name,User ID,Access Method	Monday,Wednesday,0:15AM
2	☐	☐	John_Doe_Usage	User ID	User Name,User ID,Access Method,Equipment-Item ID #	Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday,0:15AM,1:00AM,2:00PM
3	☐	☐	Admin_Activity	Administrator Activities	User ID,Access Method,Date-Range	Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday,0:30AM
4	☐	☐	Missing_Equipment	Missing Equipment	User Name,User ID,Date-Range,Equipment-Item ID #	Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday,0:30AM,4:30PM
5	☐	☐				

The table above lists several reports. There are six columns of the table. The first column *Item Delete* is for removing a report item, when it is selected and click *Save Changes* button on the upper left corner, the related record item will be deleted.

The second column *Item Report* is for generating the report. When it is chosen, if clicking blue button *Generate Report*, a .pdf file will be generated and displayed for the report result; if clicking button *Export as .CSV*, a .csv file will be generated, a popup window will show the path of the file.

The third column is *Report Name*. The report is given a name automatically based on the time stamp when being created, and the user can modify it to a more meaningful name by double clicking it. The report name needs to be unique in the report list.

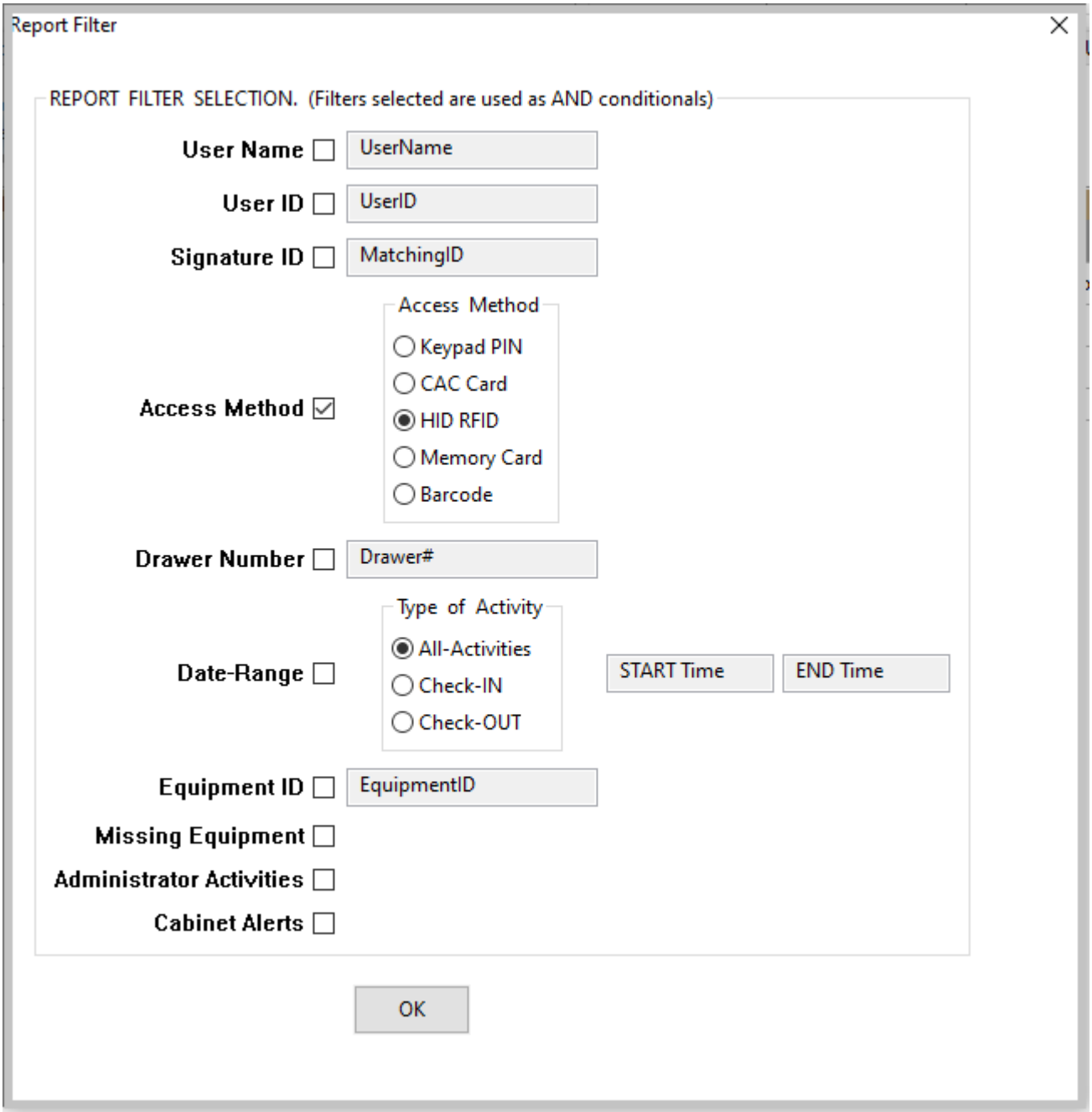
The fourth column is *Report Filter*. The filter is the condition by which the report is generated. The string in the cell is the list of the parameters about the condition.

The fifth column is *Report Content*. The content is the information type to be displayed in the report. The string in the cell is a brief list of the parameters.

The sixth column is the *Report Time*. The time is usually a list of the day of the week and the time of the day. The values shown in the table is a summary of the day/times. This are the times when the report is sent by email.

5.5.1 Report Filter

When clicking the column of *Report Filter* of the table, a window will pop up for the setup of the filter with the qualification information for the report. A screenshot is as following:



There are two types of the filter constraints. The first type is for the general report, The condition can be the combination of any items in the list. The logic is AND; the more the conditions are chosen, the stricter of the constraint. This type of the constraints includes the following parameters:

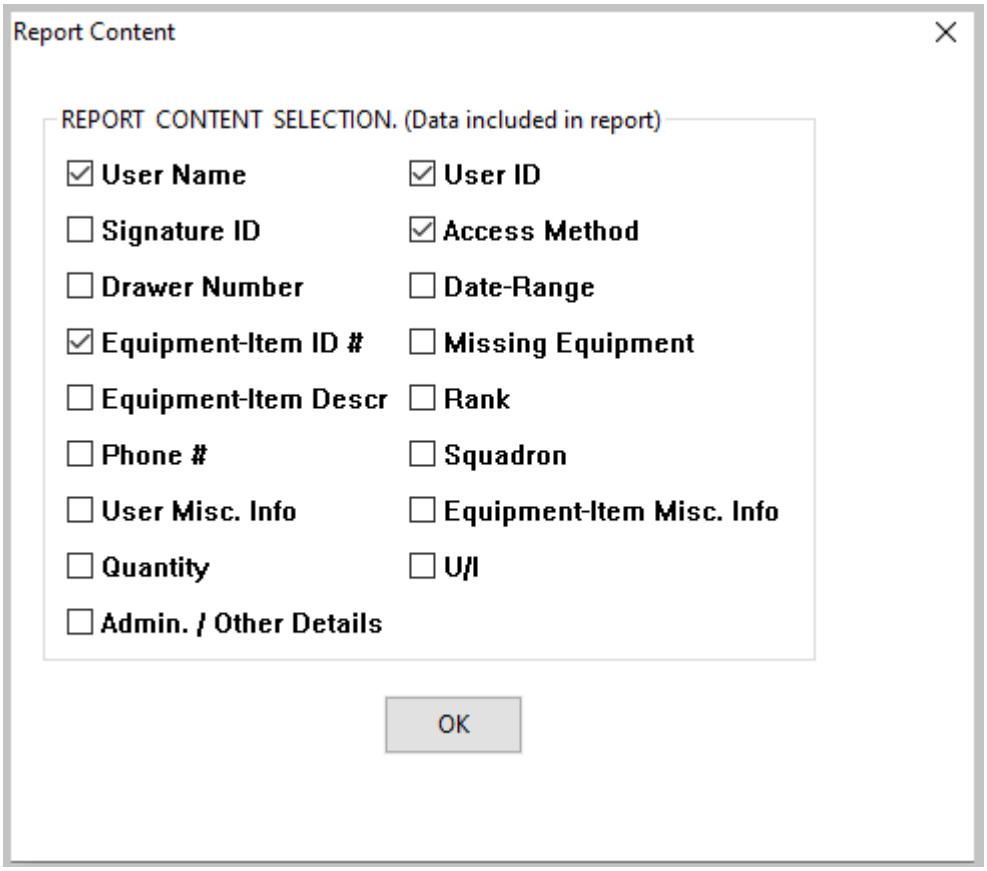
User Name, User ID, Signature ID, Access Method, Drawer Number, Data-Range, Equipment ID.

The second type is for the alert. The selection can be a combination of the alert items, and the logic is OR. The more they are chosen, the more records the report will include. This type of the constraints includes the following parameter:

Missing Equipment, Cabinet Alerts.

5.5.2 Report Content

When clicking *Report Content* column of the table, a window will pop up for the setup of report content. A screenshot is as following:

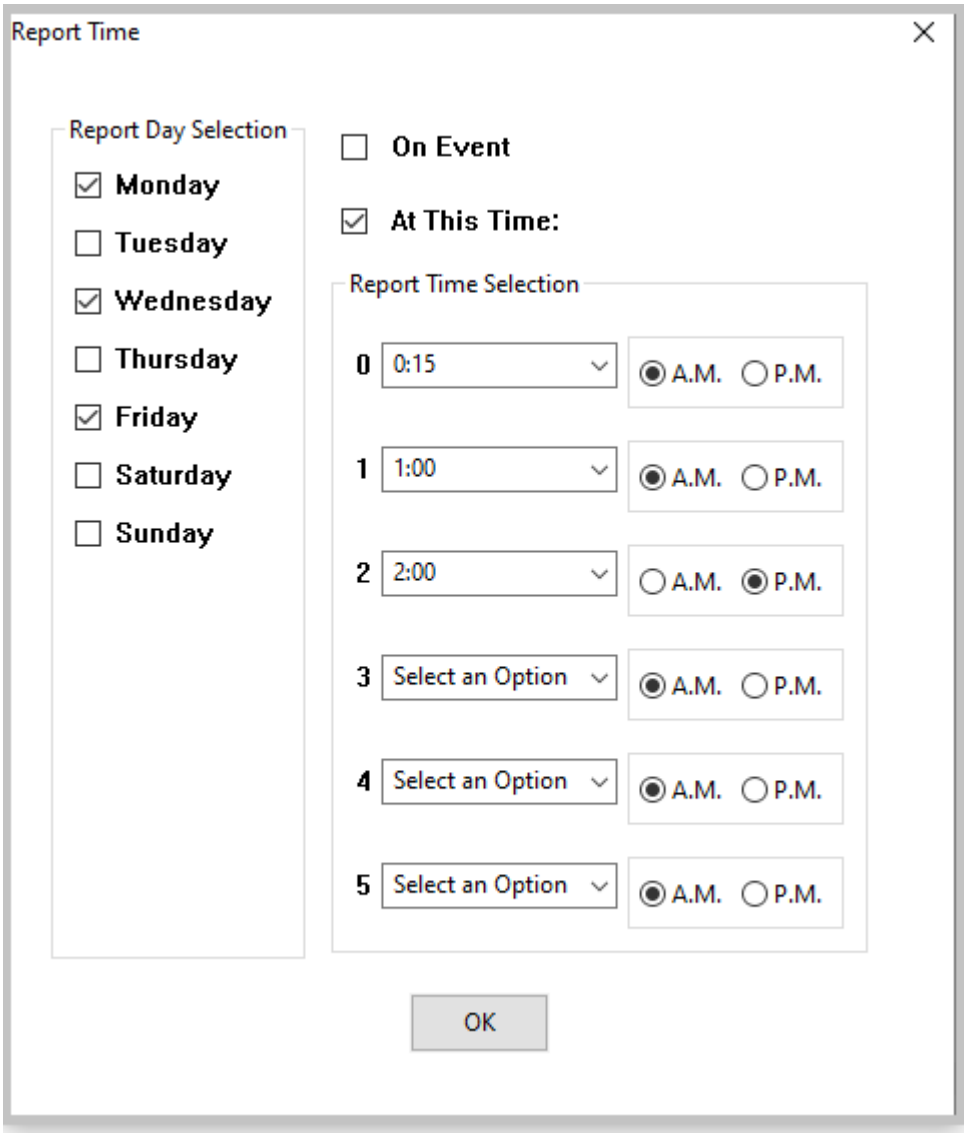


The content includes *User Name, User ID, Signature ID, Access Method, Drawer Number, Date-Range, Equipment-Item ID #, Missing Equipment, Equipment-Item Desc, Rank, Phone #, Squadron, User Misc. Info, Equipment-Item Misc. Info, Quantity, U/I, and Admin. / Other Details.*

Basically, the list of the items are the column names in the report. As there is a limitation for the width for .pdf file, we cannot choose too many columns from the list. For .csv file there is no limitation for the column selection.

5.5.3 Report Time

When clicking the column of *Report Time* in the table, a window will pop up with setup of the report time. It is about on what day and what time to send the report by email. The following is a screenshot of the setup of report time.



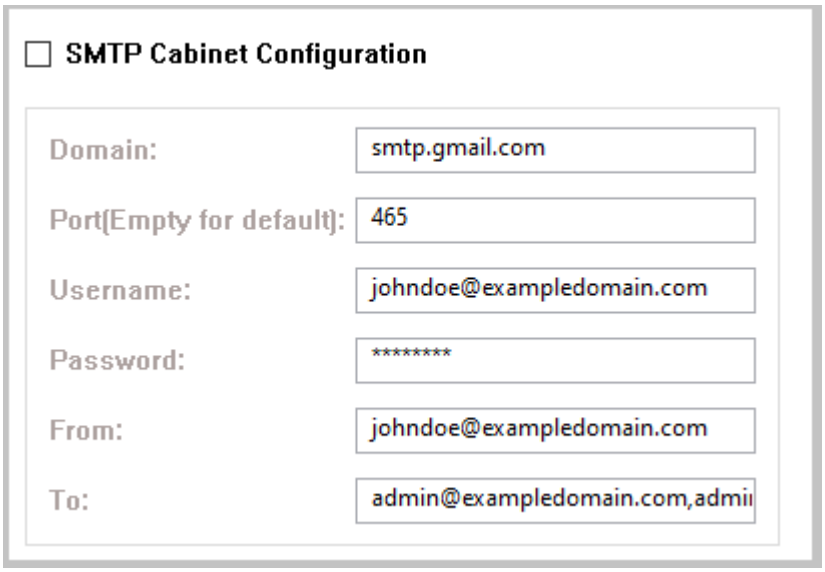
The left part of the screen is the days of the week. The logic of the combination is *OR*. On the right part, *On Event* is real-time report, it is for *Cabinet Alerts* or *Missing Equipment* notification. *At This Time* option is for the time selection. The five options of time selection are the times when the report is sent out.

5.6 Email Configuration

This function is mostly for the preparation of report sending. It includes SMTP accounts setup and the recipient setup. It is in *Email Config* tab of *CAC-GUI* program.

5.6.1 SMTP Cabinet Configuration

This section is about the email account setup. It is for the login of the email account for sending email. A screenshot is as following:

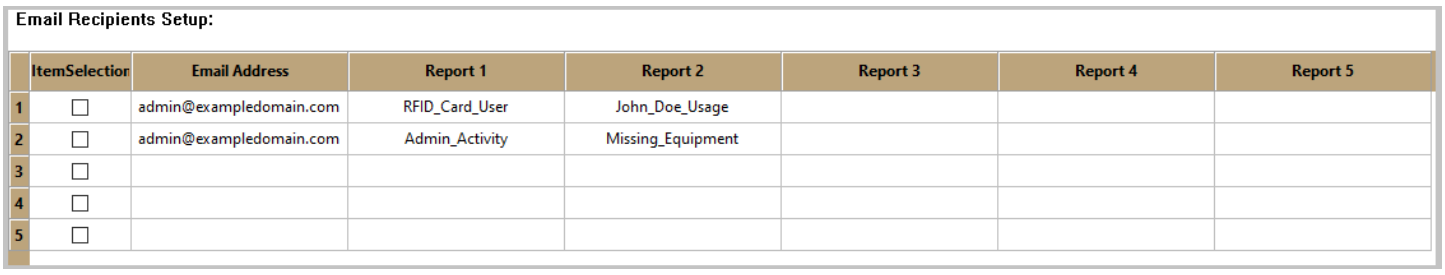


The above screen is an example of sender with *gmail* account. For a *gmail* account, the domain name of the server is *smtp.gmail.com* and the server port is *465*. *Username* is normally the email address of the sender, the *password* is encrypted and saved in the database. *From* section is the sender email address too. *To* section can be left empty and will be filled after *Email Recipients Setup* is done.

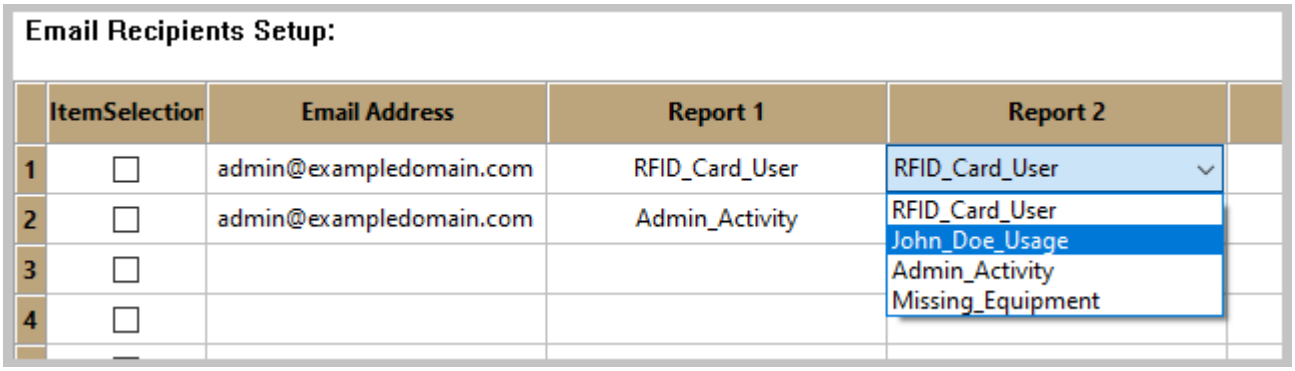
By default, the account parameters are read-only to avoid inadvertent modification. To enable the modification, the user can select checkbox *SMTP Cabinet Configuration*.

5.6.2 Email Recipient Setup

This section setups the email address to receive the reports and what reports to receive. The following is a screenshot:



In the *Email Address* column, the email address can be directly typed in. Each line has five reports, when double clicking the *Report x* column, a pull-down menu will appear, and the user can choose the one for the report and it will become the value of the cell.



The email address does not have to be different from line to line. By default, there are five lines in the table, if it is not enough for sending email, a new line will be added automatically when clicking the last line of the table.

If the user wants to remove a line in the table, choose the option box in *ItemSelection* column and press *Save Changes* at the upper-right corner, the related line will be deleted.

After the input or modification are finished, click *Save Changes* button on up-right corner of the screen, and all the data will be saved to the database.

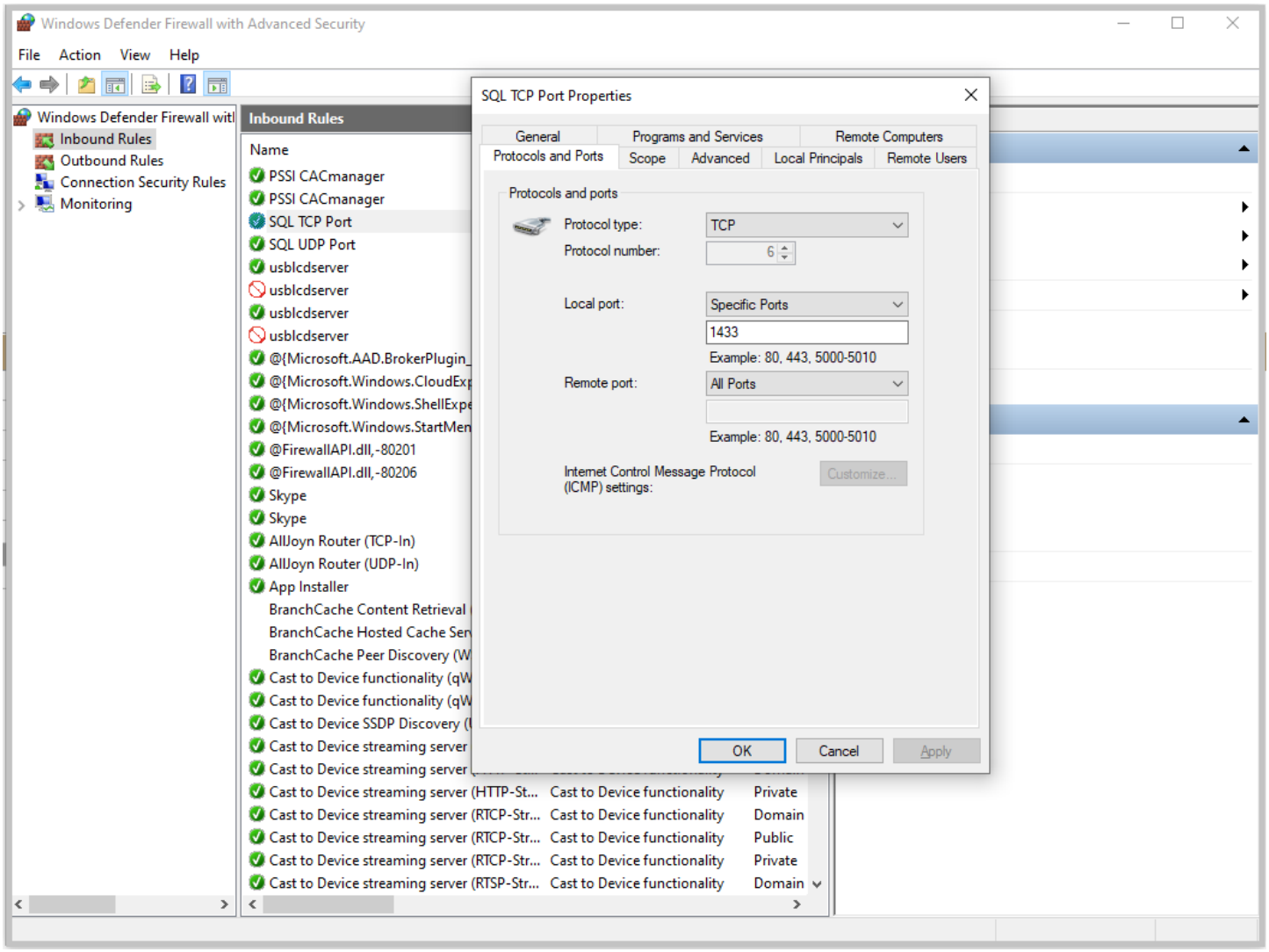
5.7 Firewall Setup

The cabinet is designed to be powered up 24 hours per day, 7 days per week and 365 days per year. The system is not designed to go through power-cycling without properly shutting down the cabinet, so care should be taken to maintain constant power to the cabinet. To further protect the system, an Uninterpretable Power Supply is installed to hold up the power to the SBC and the 12 VDC power supply for the cabinet controller.

Another safeguard utilized to maintain reliable service is a change to Microsoft Windows boot configuration settings. This is done during either the CACmanager installation or the CACmanager upgrade for versions 5.0.0 and higher.

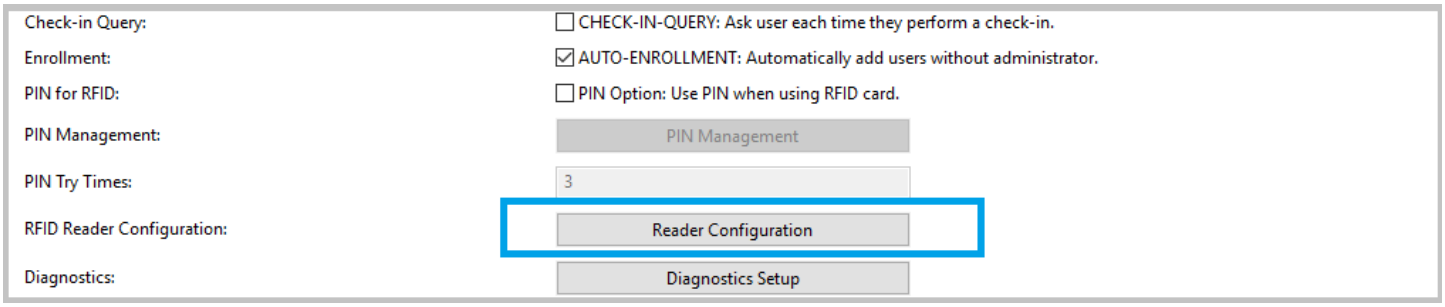
On the cabinet computer running the CACmanager, depending upon the firewall security settings implemented and/or configured by the system administrator on the Windows 10 OS, adjustments may need to be made by the administrator if a third-party firewall has been setup to block certain network traffic. In most cases, where the standard Windows 10 firewall is utilized for network security, no administrator adjustments need to be made. During the CACmanager software installation or update, an adjustment is automatically made to allow traffic into the cabinet OS system to enable SSL communication.

The running of SQL Server needs use two ports. From Firewall setting, needs to set TCP port 1433 and UDP port 1434 to be open. These are default ports with SQL Server, TCP port 1433 can be changed as long as it is consistent with *CAC-GUI*.

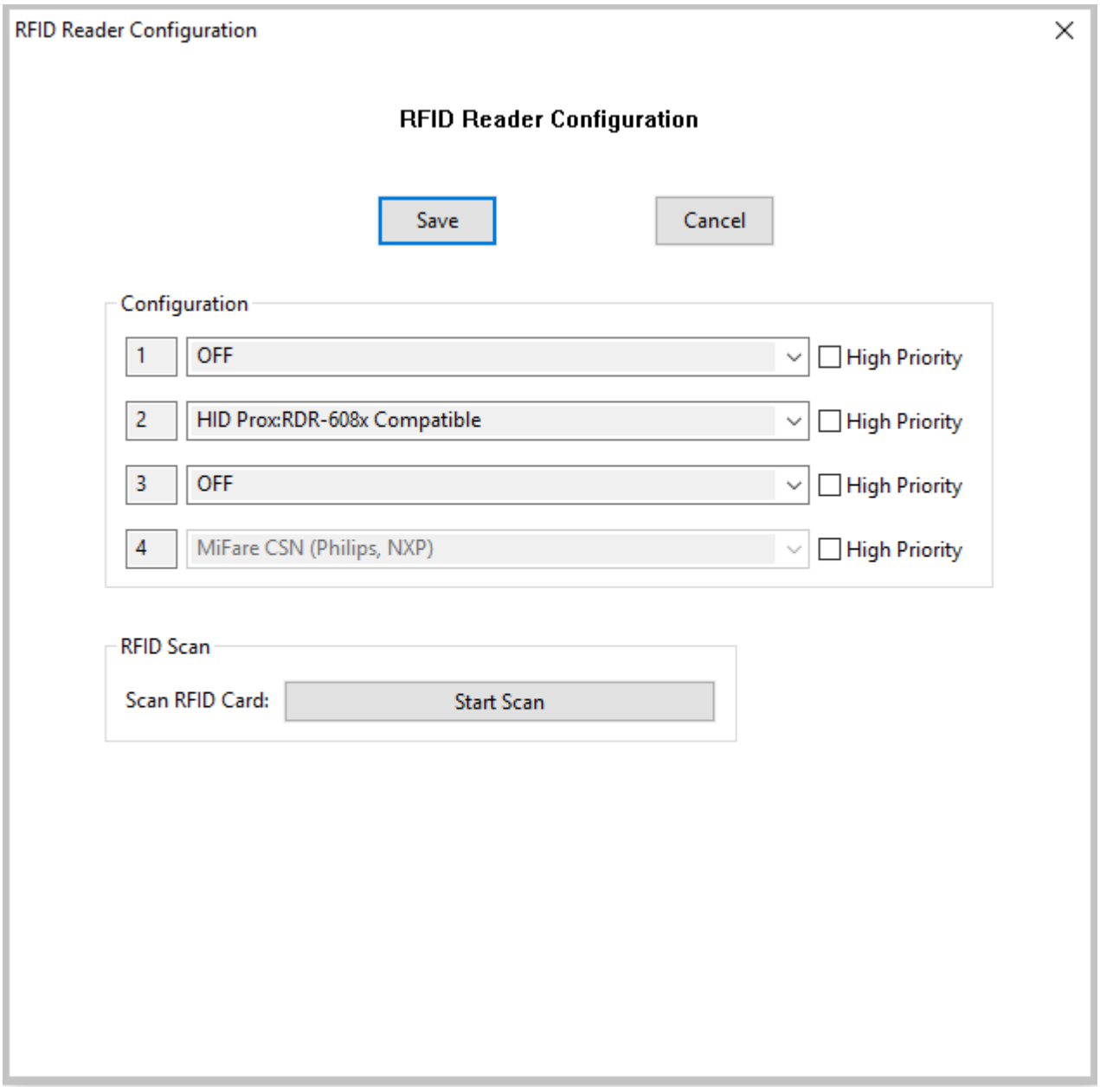


5.8 RFID Reader Setup

RFID reader needs to be configured to accept different RFID cards. It can be done from CAC-GUI. From System Config tab of CAC-GUI, press "Reader Configuration" button, a window will pop up for the configuration platform. The following is the screenshot:



And the following is the window popped up:

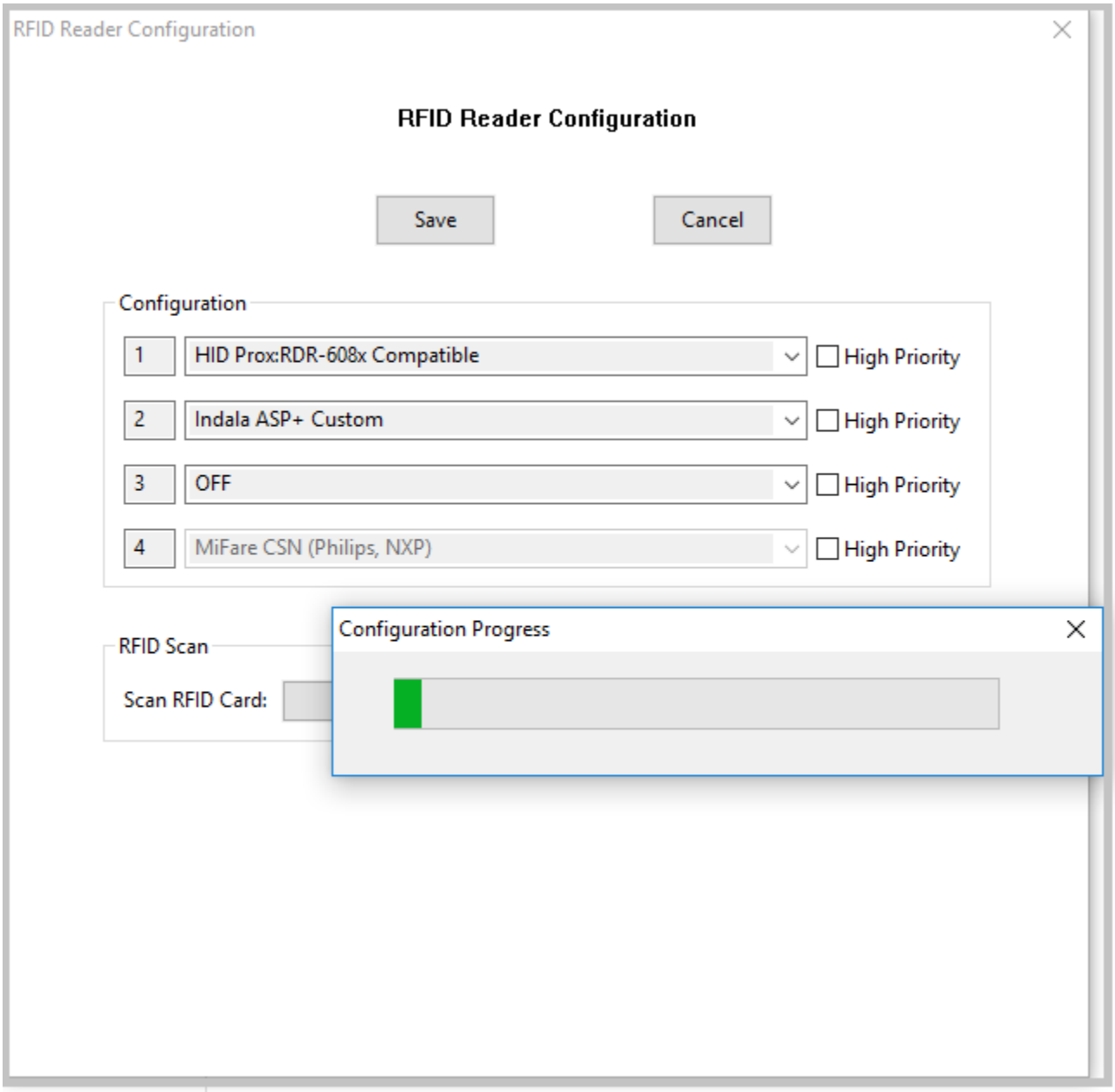


There are four channels in the RFID reader, each channel corresponding to one type of RFID card. There are 73 types of cards altogether. If the user is using one specific type of RFID card much more than other cards, the related channel could be selected with High Priority. When there is no card type is selected for a channel, it displays as "OFF".

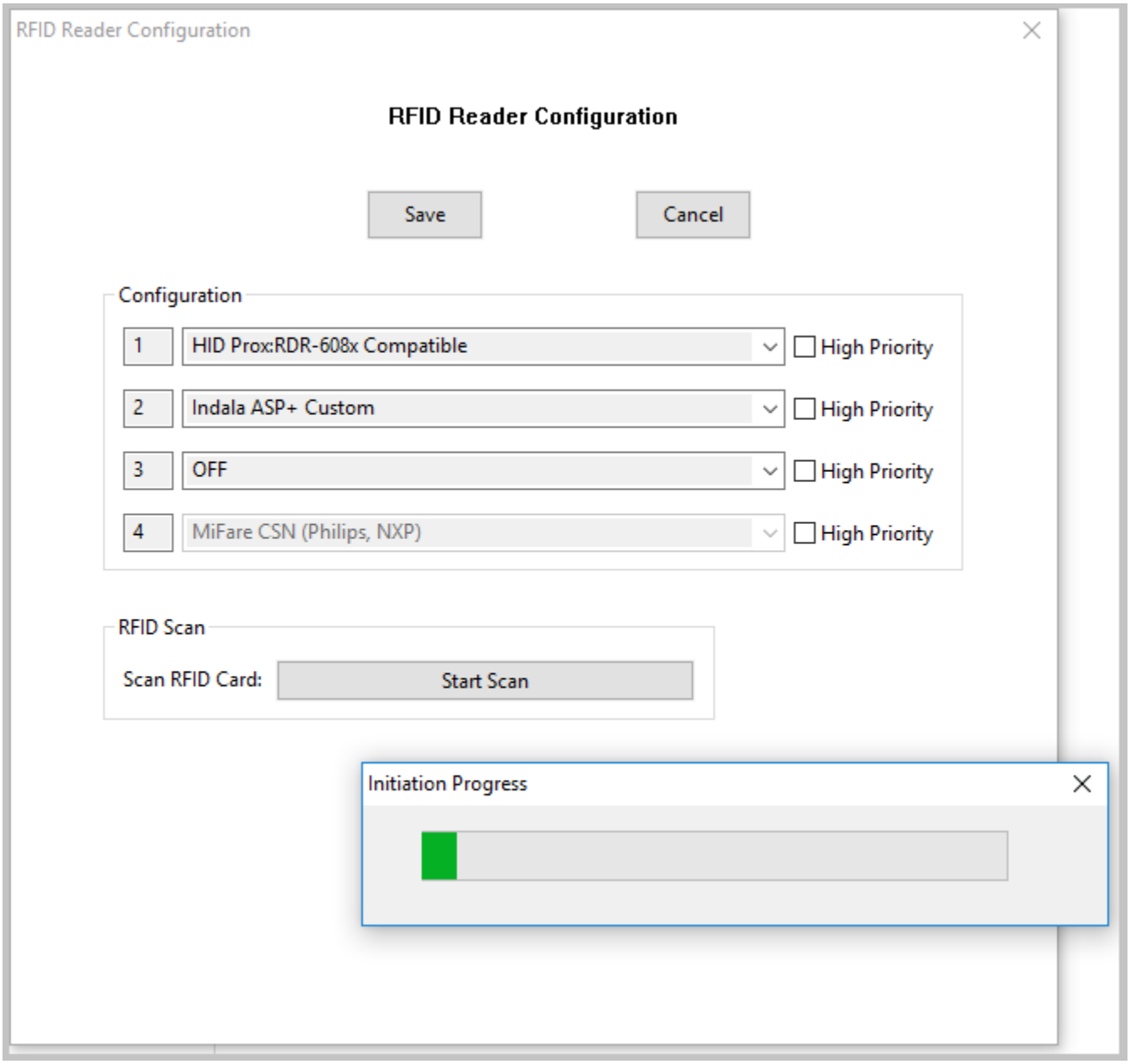
If CAC-Card_RFID is selected for Access Configuration, the 4th channel of RFID reader configuration is chosen as MiFare CSN (Philips, NXP) by default. This is because the built-in RFID function of many CAC-card is using this RFID type.

After the card types have been chosen, prese "Save" button to configure the RFID reader, a window with progress bar will appear, after the saving is done, the window will close.

Attention: if there is no change in the setup, the window will close without configuration when pressing "Save" button.

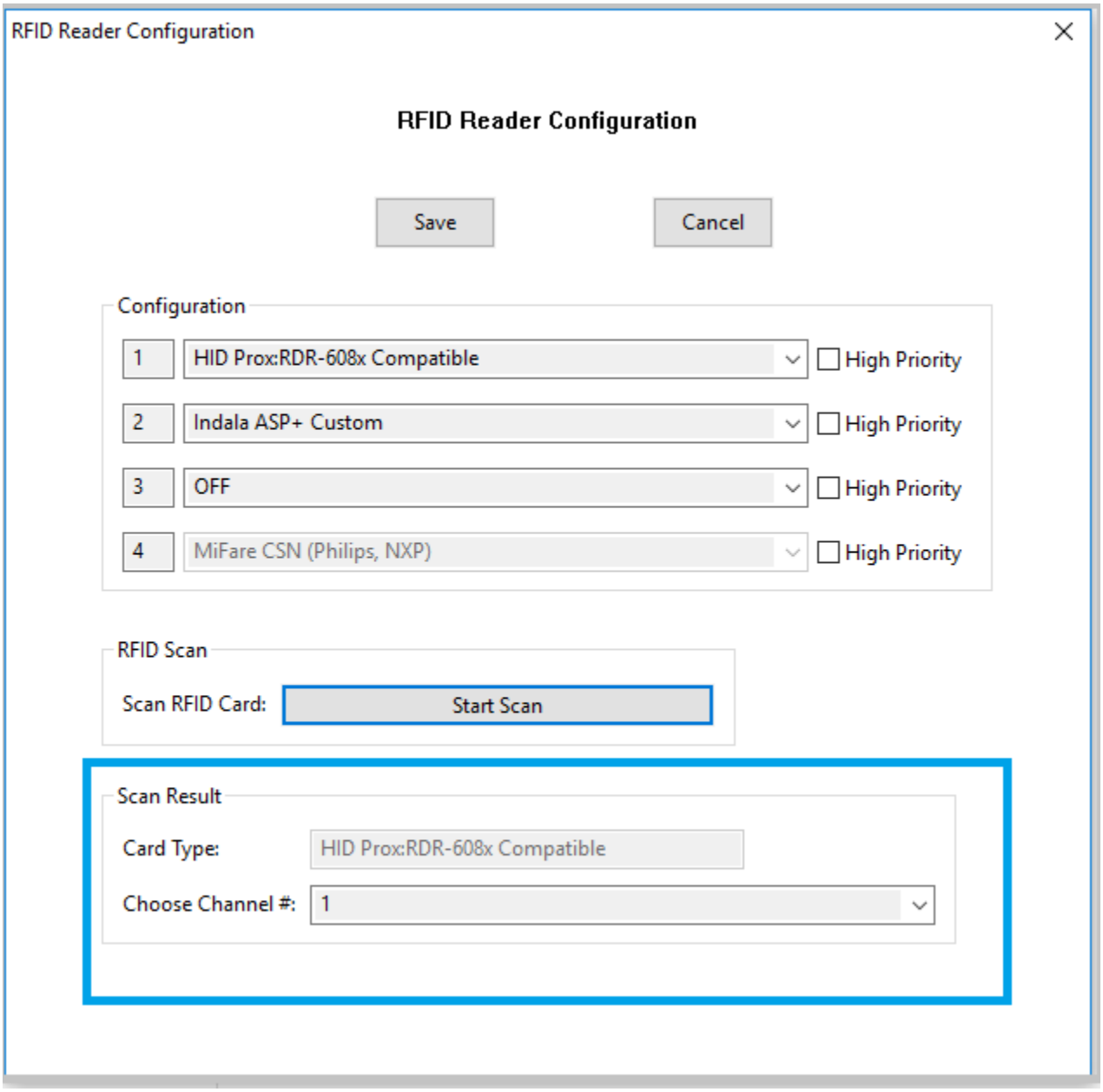


If you are not sure which card type to choose for the configuration, probably you can use the scan function to find it out. To do it, press the "Start Scan" button in the screen, and a progress bar will appear for the initialization of the card reader.



After the initialization is done, there is a reminder that placing the card on the RFID reader. Place the card on the reader and press OK button, and the scan process will start.

After the scan is finished, the scan result will be shown at the bottom part of the screen. The following is the screenshot.



In the scan result section, choose the channel number, and press the “Save” button, the scanned card type will be written to the reader.

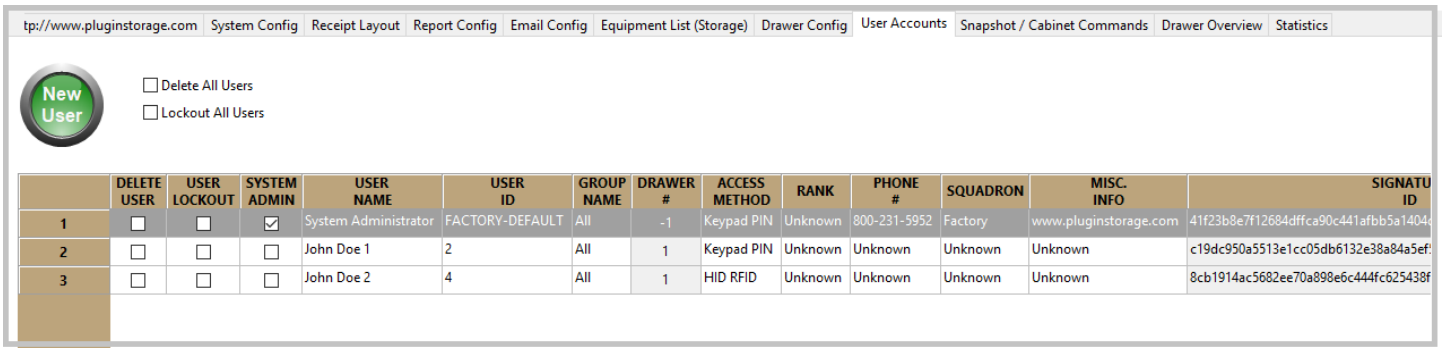
Attention: When doing the card scan, it is better to turn off the access of RFID card; otherwise, the program might automatically add the RFID card to the database as a new user (and open a drawer).

6 USER AND EQUIPMENT

This chapter introduces the assets of the cabinet – user and the equipment. It includes the add/update/delete of the users and equipment, group management, the management of temporary user, and the management of broken device and missing device.

6.1 User Management

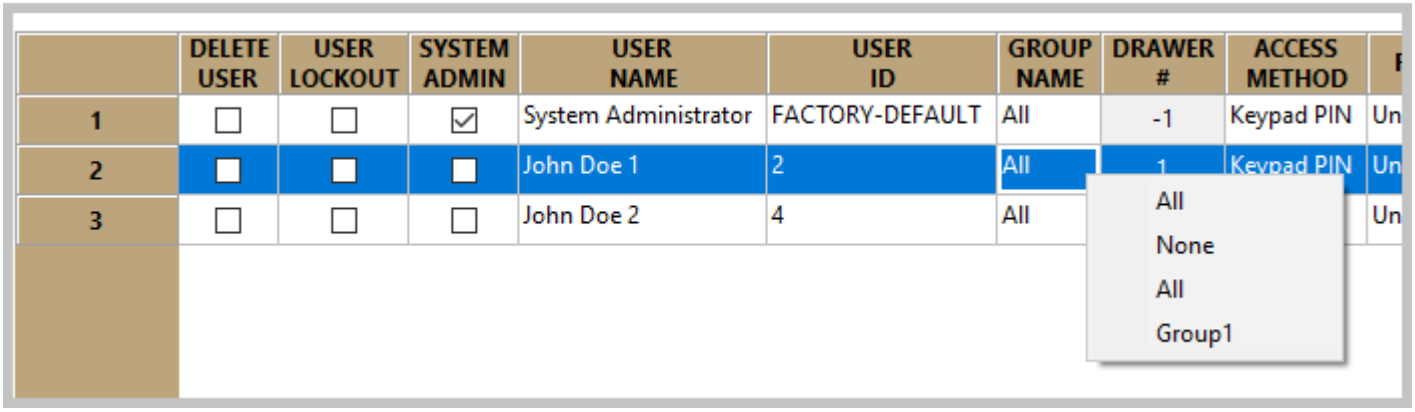
The management of user locates *at User Accounts* tab of *CAC-GUI*. The following is a screenshot:



	DELETE USER	USER LOCKOUT	SYSTEM ADMIN	USER NAME	USER ID	GROUP NAME	DRAWER #	ACCESS METHOD	RANK	PHONE #	SQUADRON	MISC. INFO	SIGNATU ID
1	☐	☐	☑	System Administrator	FACTORY-DEFAULT	All	-1	Keypad PIN	Unknown	800-231-5952	Factory	www.pluginstorage.com	41f23b8e7f12684dffca90c441afbb5a1404
2	☐	☐	☐	John Doe 1	2	All	1	Keypad PIN	Unknown	Unknown	Unknown	Unknown	c19dc950a5513e1cc05db6132e38a84a5ef
3	☐	☐	☐	John Doe 2	4	All	1	HID RFID	Unknown	Unknown	Unknown	Unknown	8cb1914ac5682ee70a898e6c444fc625438f

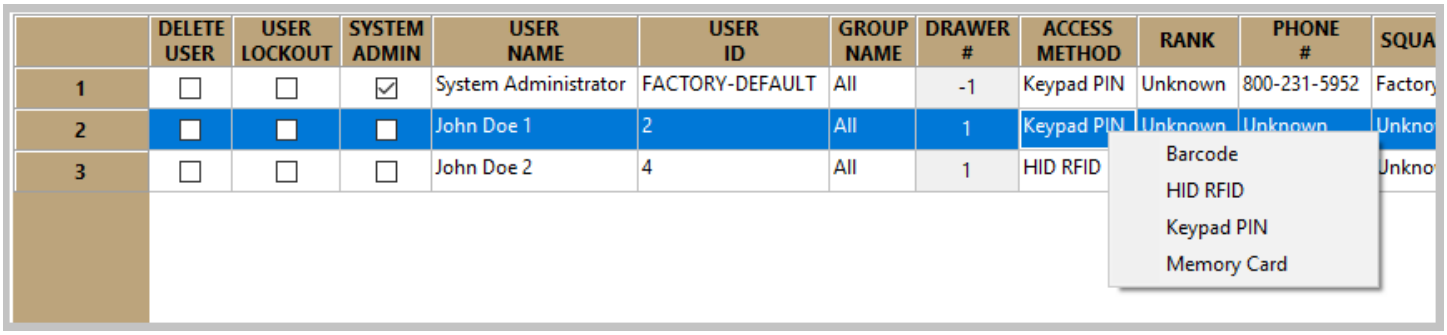
The above table is a user list with detailed information. Column *USER NAME*, *USER ID*, *RANK*, *PHONE #* and *MISC INFO* can be changed by simply typing in the new content.

Column *GROUP NAME* can be changed by choosing another value in the pull-down menu. When left clicking *GROUP NAME* column the pull-down menu will appear.



Column *DRAWER #* can be changed only when the cabinet is in *FIXED-ACCESS mode*, the default value is incrementally added for a new user when in *FIXED-ACCESS mode* ; it will be automatically filled when in other mode (often default value is 1).

ACCESS METHOD column can be changed with the pull-down menu appeared when clicking the cell. A screenshot is as following.



Column *SIGNATURE ID* is automatically generated as the unique identification of the user, and it cannot be directly changed.

Column *DELETE USER* is for user removal. When the checkbox of this column is chosen, and click *Save Changes* button, the related user will be removed from the database.

Column *USER LOCKOUT* is for user locking. When the checkbox of this column is selected, the related user will be temporarily locked out from accessing the cabinet.

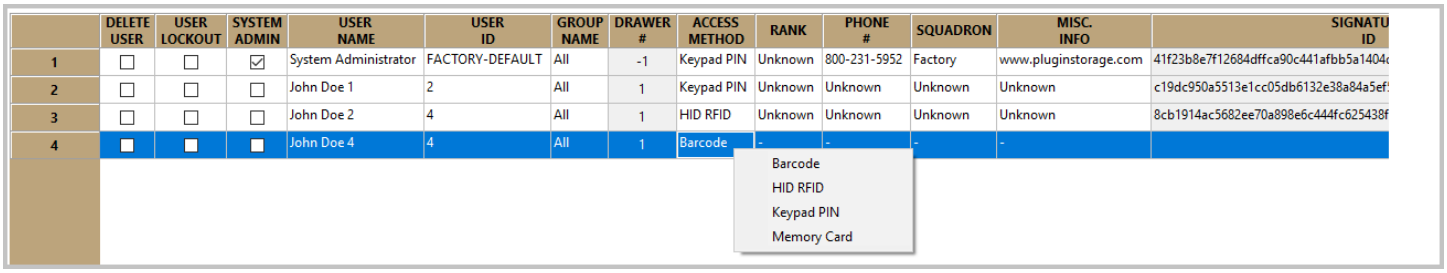
Column *SYSTEM ADMIN* is the setup of administration. When this column is selected, the user will have the privilege of administrator.

In the upper left corner, there is a check box *Delete All Users*, when this box is selected, all the check boxes of *DELETE USER* column of the table will be chosen. Similarly, when checkbox *Lockout All Users* is selected, all the checkboxes in *USER LOCKOUT* column will be chosen.

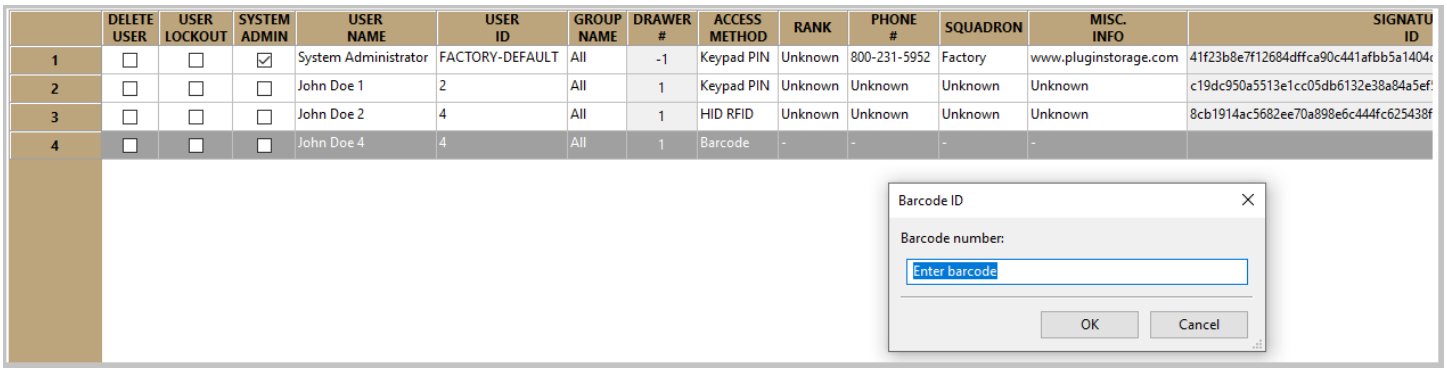
6.1.1 Add New User from CAC-GUI

When clicking the green button from upper-right corner, a new line will be added to the user table, the default *USER NAME* is *John Doe x*, the default user ID is the incrementally the largest, the default *GROUP NAME* is *All*, default *Drawer #* is 1, default value for other columns is "-" or empty.

Click *ACCESS METHOD* column, a small menu will pop up for the access methods, a screenshot is as following:

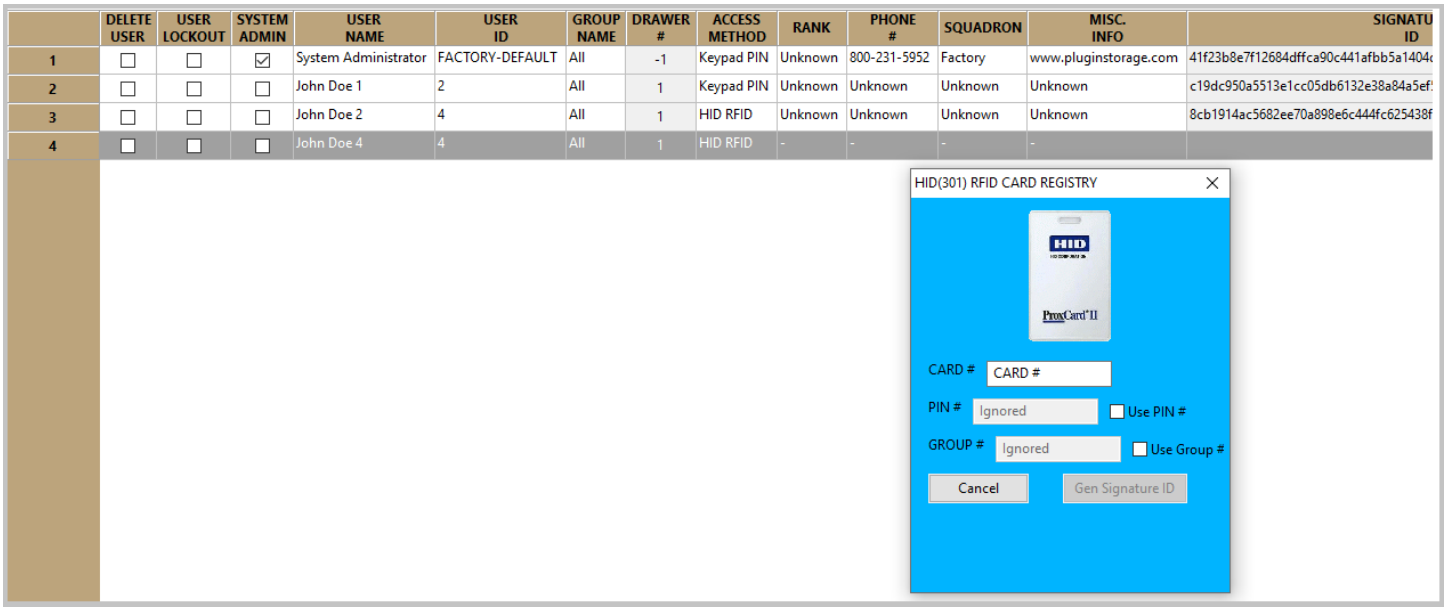


Choose one of the methods from the menu, for example, choose *Barcode*; and then right click *SIGNATURE ID* column to generate the ID, a window will pop up for the input of the barcode number. The screenshot is as following:



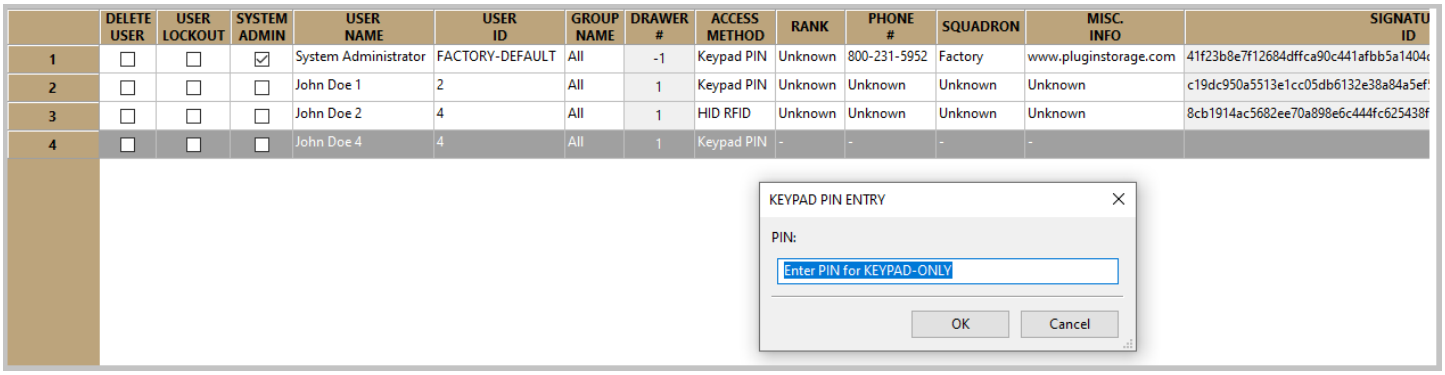
Type in the barcode number, and click OK button, a signature ID will be generated and filled in the cell.

For an access method of *HID RFID*, the screen is as following when right lick *SIGNATURE ID* column:



Normally we just need to type in *CARD #* in the screen and left other text box with the default values and click *Gen Signature ID* button. The signature ID of the user will be generated and filled in the table.

For an access method of *Keypad PIN*, when right clicking the *SIGNATURE ID* column, the following screen will appear:



Similarly, type in the PIN number and click *OK* button, the signature ID is generated and filled into the table.

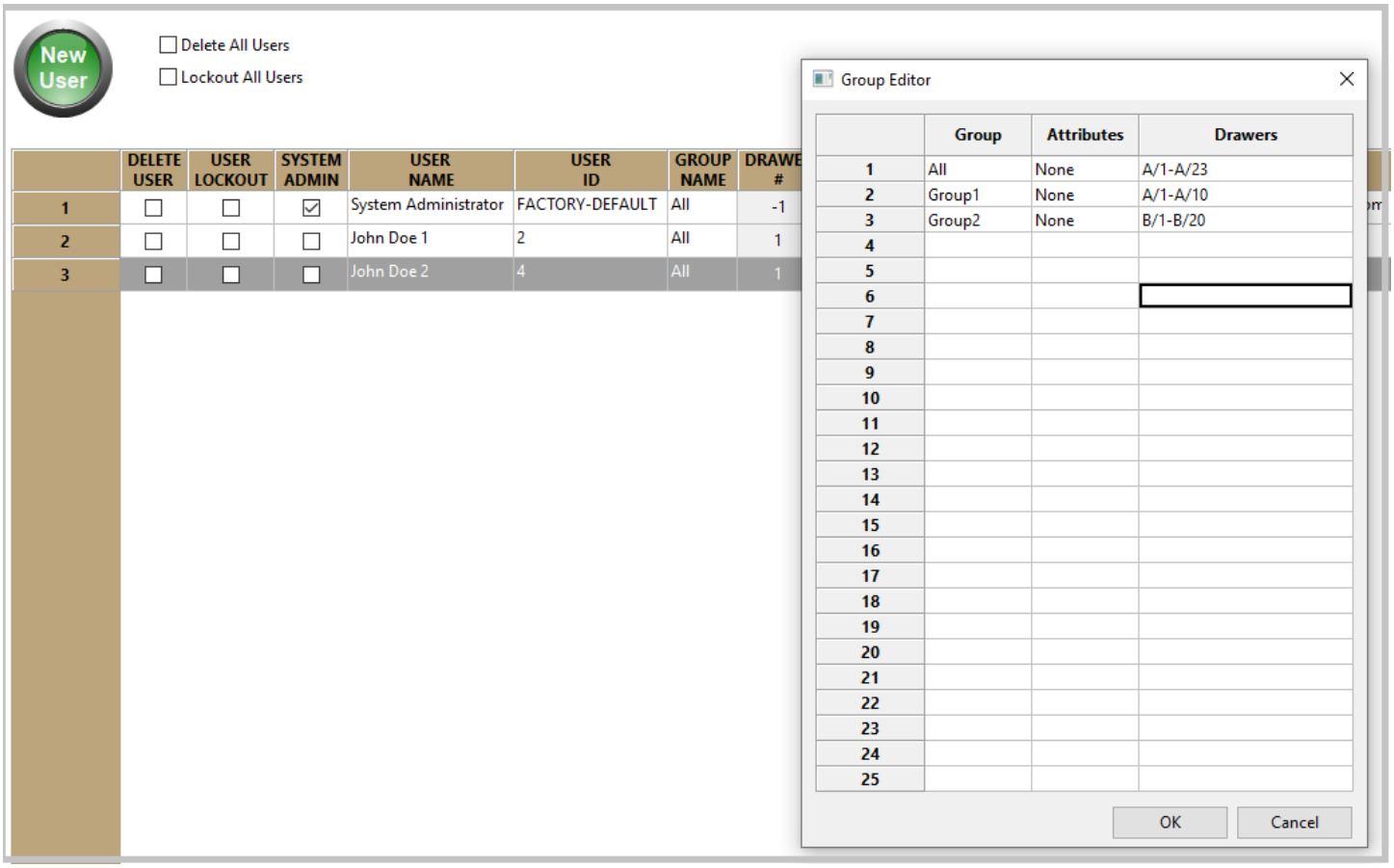
6.1.2 Add New User from Cabinet Panel

When Auto-enrollment is turned on, a new user will be enrolled into the database automatically (discussed in section 5.1). In this situation, When the user accesses the cabinet, it is added as new user into the database based on the information of his/her input.

6.2 Group Management

The users can be organized in some groups based on their tasks, projects or departments.

When **right clicking** *GROUP NAME* column of the user list table, a table will pop up for the list of Groups. The following is a screenshot:



The first column of table *Group Editor* is the group name, the name needs to be unique in the table. The second column is *Attributes*; it is usually set as *None*; the third column is *Drawers*; it is the range of the drawers that members of this group can access.

In *Drawers* column of the table, the drawers are addressed as A/1, A/23, B/1, B/20. The letter A or B or C is the cabinet number, and 1, 2, 23 is the drawer number in its cabinet. More details about cabinet number can be found in section *Cabinet Cluster*.

The default group in the table is group *All*, and its drawer range is *A/1-A/24*. It means group *All* is from the 1st drawer to 24th drawer of the first cabinet.

After the information has been typed in, click *OK* button, and the information will be saved.

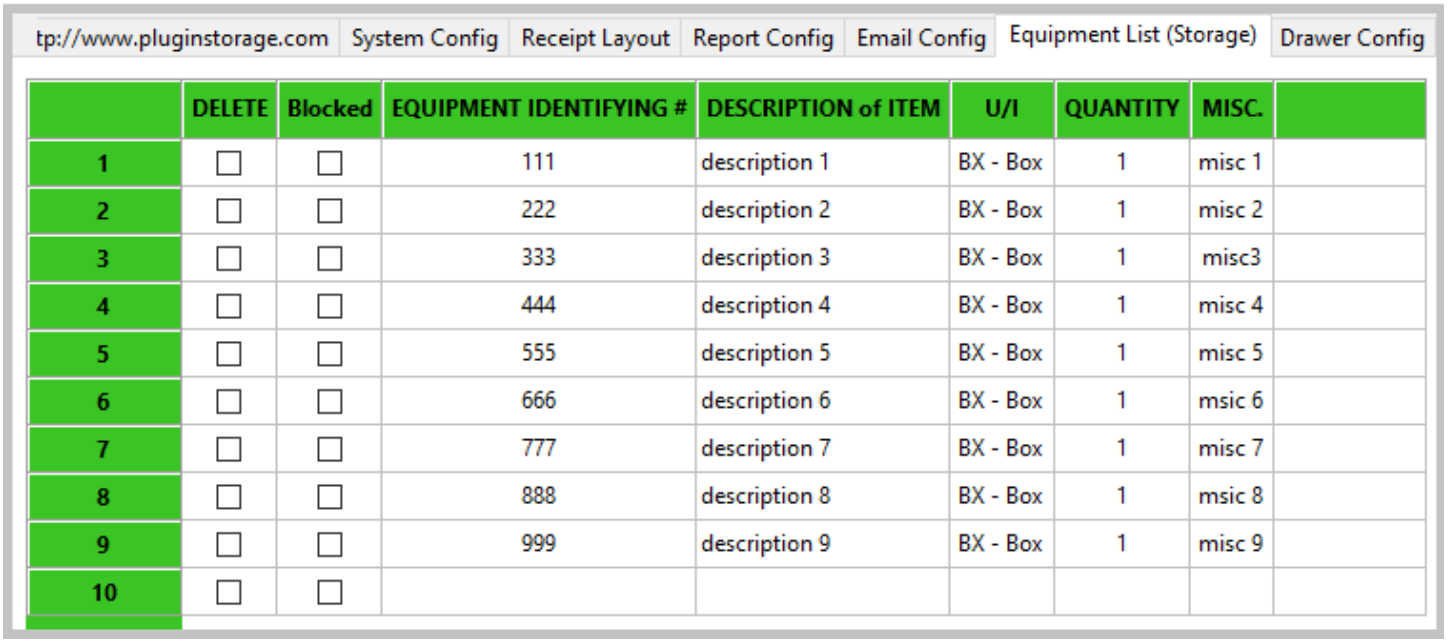
For the group selection of the user, it needs to **left click** *GROUP NAME* column of the related user, and a window will pop up with the group name list. This was discussed in *section 6.1.1*.

6.3 Device Management

The devices are the equipment in the drawers. The device list is shown in tab *Equipment List (Storage)* of *CAC-GUI*.

6.3.1 Equipment list

A screenshot of the equipment list is as following:

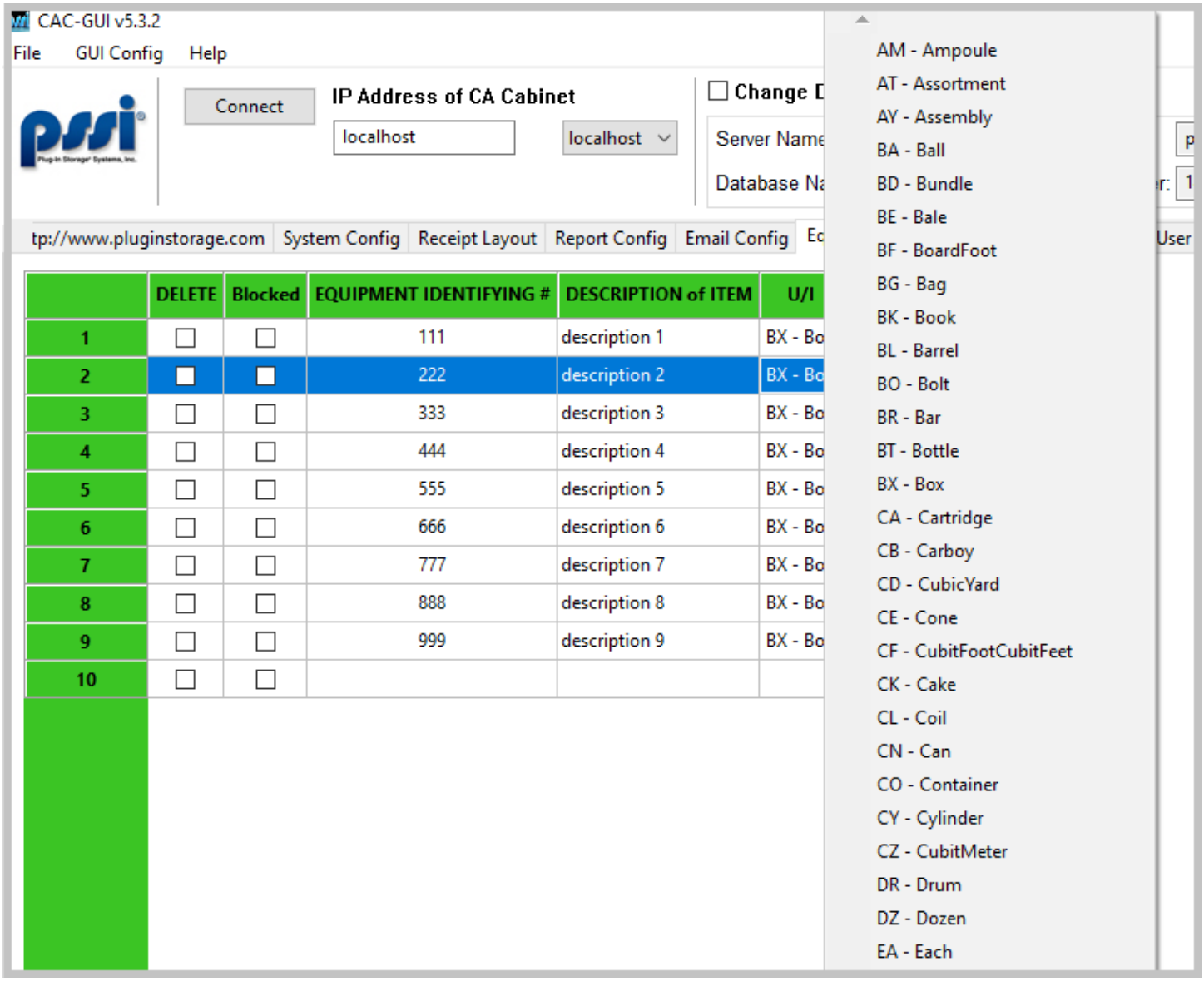


tp://www.pluginstorage.com | System Config | Receipt Layout | Report Config | Email Config | Equipment List (Storage) | Drawer Config

	DELETE	Blocked	EQUIPMENT IDENTIFYING #	DESCRIPTION of ITEM	U/I	QUANTITY	MISC.	
1	☐	☐	111	description 1	BX - Box	1	misc 1	
2	☐	☐	222	description 2	BX - Box	1	misc 2	
3	☐	☐	333	description 3	BX - Box	1	misc3	
4	☐	☐	444	description 4	BX - Box	1	misc 4	
5	☐	☐	555	description 5	BX - Box	1	misc 5	
6	☐	☐	666	description 6	BX - Box	1	msic 6	
7	☐	☐	777	description 7	BX - Box	1	misc 7	
8	☐	☐	888	description 8	BX - Box	1	msic 8	
9	☐	☐	999	description 9	BX - Box	1	misc 9	
10	☐	☐						

The column *EQUIPMENT IDENTIFYING #* is the ID of the device, it needs to be unique in the list, column *U/I* is the unit of the equipment and *QUANTITY* indicates the number of units in the drawer.

When clicking *U/I* column of the table, a window pops up with a list of units to choose. A screenshot is as following:

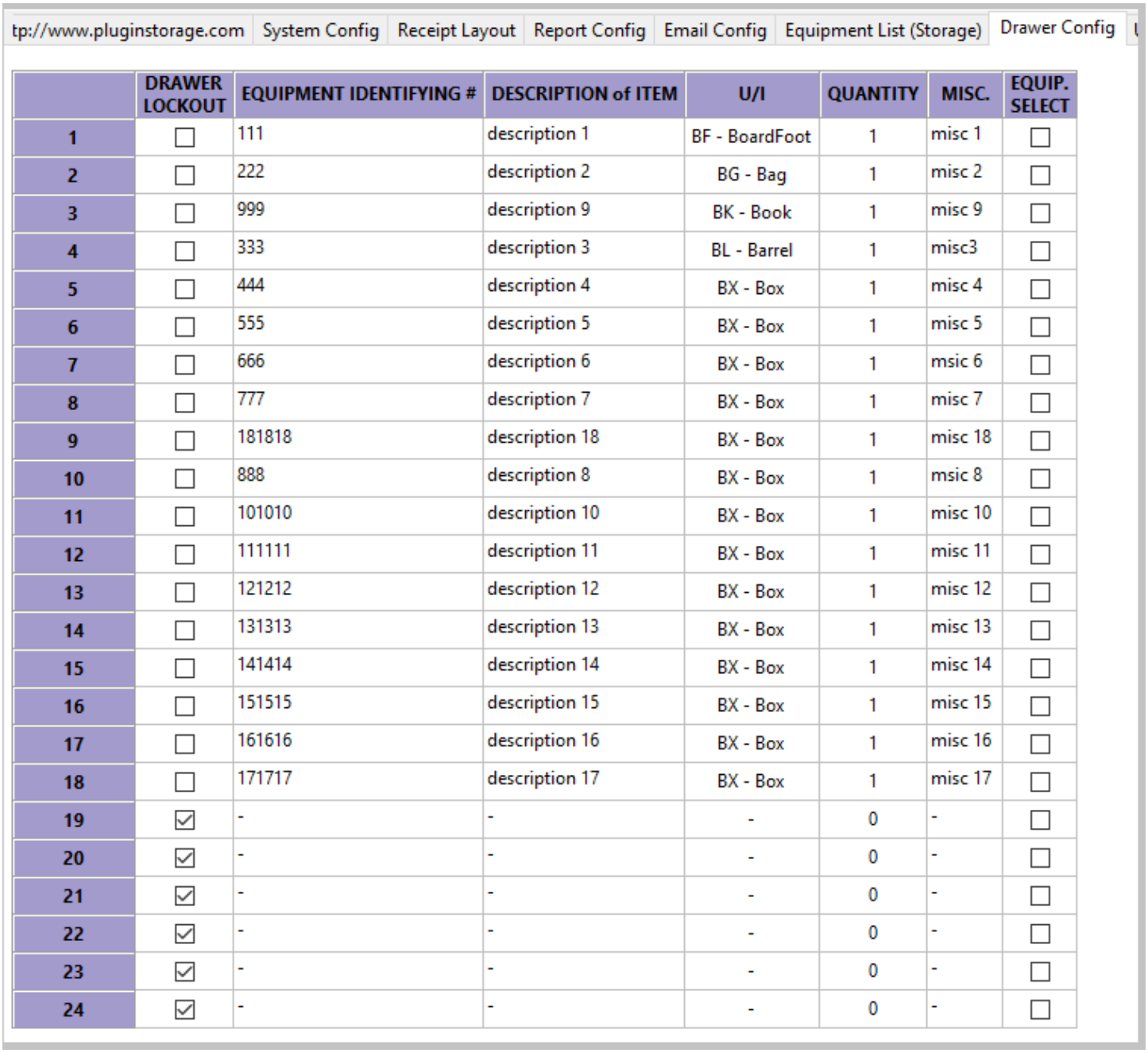


Click the unit in the list and it will be filled in *U/I* column of the related device.

If select the check box of *DELETE* column and click *Save Changes* button from the upper-right corner, the related equipment will be removed from the database. Similarly, when select the check box of *Blocked* column and click *Save Changes* button, and the related equipment will be blocked in the cabinet.

6.3.2 Place Equipment to Drawer

After the equipment is added into the database, it needs to be related to a drawer for the user to checkout and check-in. This process can be done in tab *Drawer Config* of *CAC-GUI*. A screenshot is as following:



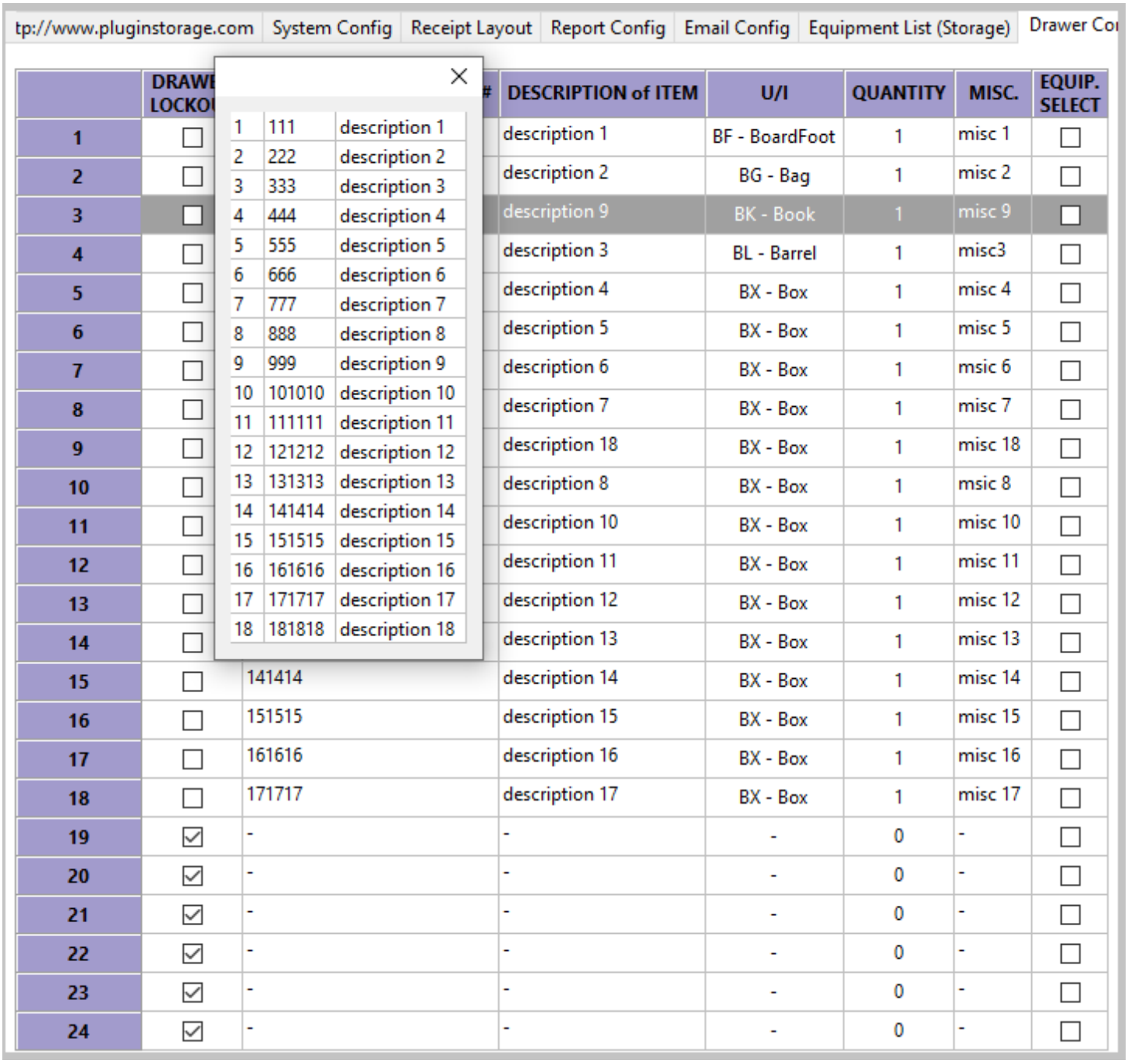
tp://www.pluginstorage.com | System Config | Receipt Layout | Report Config | Email Config | Equipment List (Storage) | Drawer Config

	DRAWER LOCKOUT	EQUIPMENT IDENTIFYING #	DESCRIPTION of ITEM	U/I	QUANTITY	MISC.	EQUIP. SELECT
1	☐	111	description 1	BF - BoardFoot	1	misc 1	☐
2	☐	222	description 2	BG - Bag	1	misc 2	☐
3	☐	999	description 9	BK - Book	1	misc 9	☐
4	☐	333	description 3	BL - Barrel	1	misc3	☐
5	☐	444	description 4	BX - Box	1	misc 4	☐
6	☐	555	description 5	BX - Box	1	misc 5	☐
7	☐	666	description 6	BX - Box	1	msic 6	☐
8	☐	777	description 7	BX - Box	1	misc 7	☐
9	☐	181818	description 18	BX - Box	1	misc 18	☐
10	☐	888	description 8	BX - Box	1	msic 8	☐
11	☐	101010	description 10	BX - Box	1	misc 10	☐
12	☐	111111	description 11	BX - Box	1	misc 11	☐
13	☐	121212	description 12	BX - Box	1	misc 12	☐
14	☐	131313	description 13	BX - Box	1	misc 13	☐
15	☐	141414	description 14	BX - Box	1	misc 14	☐
16	☐	151515	description 15	BX - Box	1	misc 15	☐
17	☐	161616	description 16	BX - Box	1	misc 16	☐
18	☐	171717	description 17	BX - Box	1	misc 17	☐
19	☑	-	-	-	0	-	☐
20	☑	-	-	-	0	-	☐
21	☑	-	-	-	0	-	☐
22	☑	-	-	-	0	-	☐
23	☑	-	-	-	0	-	☐
24	☑	-	-	-	0	-	☐

This drawer list table looks like the one of equipment list, the difference is that the drawer list table has the information of drawer -- the row number in the first line (1,2,3,4,5 ...) is the drawer number.

The first column of the table is *DRAWER LOCKOUT*; when it is selected, the related drawer will be locked out. The meaning of other columns *EQUIPMENT IDENTIFYING #*, *DESCRIPTION of ITEM*, *U/I*, *QUANTITY*, *AND MISC.* is the same as those in equipment list table.

Normally we do not input or change the information of the equipment directly here, but by choosing it from the list. When clicking the last column *EQUIP. SELECT* of the table, a window will pop up with the list of equipment. A screenshot is as following:



	DRAWE LOCKOU	#	DESCRIPTION of ITEM	U/I	QUANTITY	MISC.	EQUIP. SELECT
1	☐	111	description 1	BF - BoardFoot	1	misc 1	☐
2	☐	222	description 2	BG - Bag	1	misc 2	☐
3	☐	333	description 9	BK - Book	1	misc 9	☐
4	☐	444	description 3	BL - Barrel	1	misc3	☐
5	☐	555	description 4	BX - Box	1	misc 4	☐
6	☐	666	description 5	BX - Box	1	misc 5	☐
7	☐	777	description 6	BX - Box	1	msic 6	☐
8	☐	888	description 7	BX - Box	1	misc 7	☐
9	☐	999	description 18	BX - Box	1	misc 18	☐
10	☐	101010	description 8	BX - Box	1	msic 8	☐
11	☐	111111	description 10	BX - Box	1	misc 10	☐
12	☐	121212	description 11	BX - Box	1	misc 11	☐
13	☐	131313	description 12	BX - Box	1	misc 12	☐
14	☐	141414	description 13	BX - Box	1	misc 13	☐
15	☐	151515	description 14	BX - Box	1	misc 14	☐
16	☐	161616	description 15	BX - Box	1	misc 15	☐
17	☐	171717	description 16	BX - Box	1	misc 16	☐
18	☐	181818	description 17	BX - Box	1	misc 17	☐
19	☑	-	-	-	0	-	☐
20	☑	-	-	-	0	-	☐
21	☑	-	-	-	0	-	☐
22	☑	-	-	-	0	-	☐
23	☑	-	-	-	0	-	☐
24	☑	-	-	-	0	-	☐

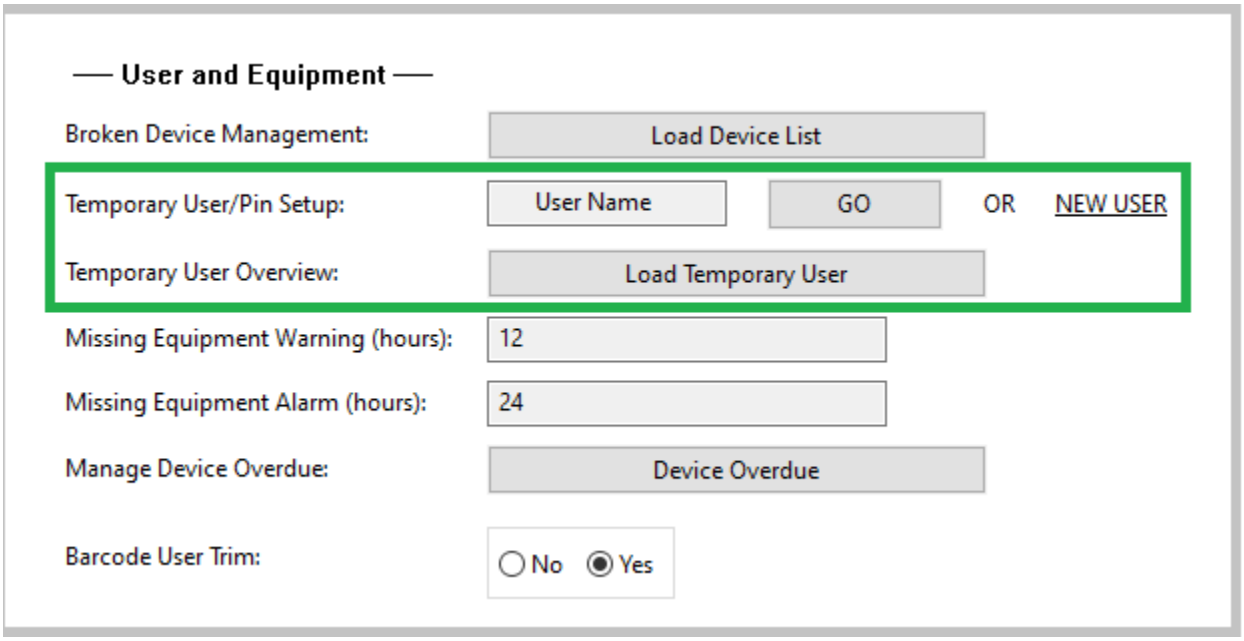
Select the device from the window and the information of the device will be filled into the table.

6.4 Temporary User

Temporary PIN is a special type of Keypad User. It is a method to give user a temporary access to the cabinet; the user can do check-in, check-out action during this period. The time window for the access can be one hour, one day, one week or some customized setting. The Temporary PIN can be sent out by email or message. Only administrator can create and manage the temporary users.

The usage of temporary PIN is the same as keypad user. The user can type in the PIN and then follow the instructions on LCD screen of the cabinet.

The setup of temporary user is from tab *System Config* of *CAC-GUI*. A screenshot is as following:



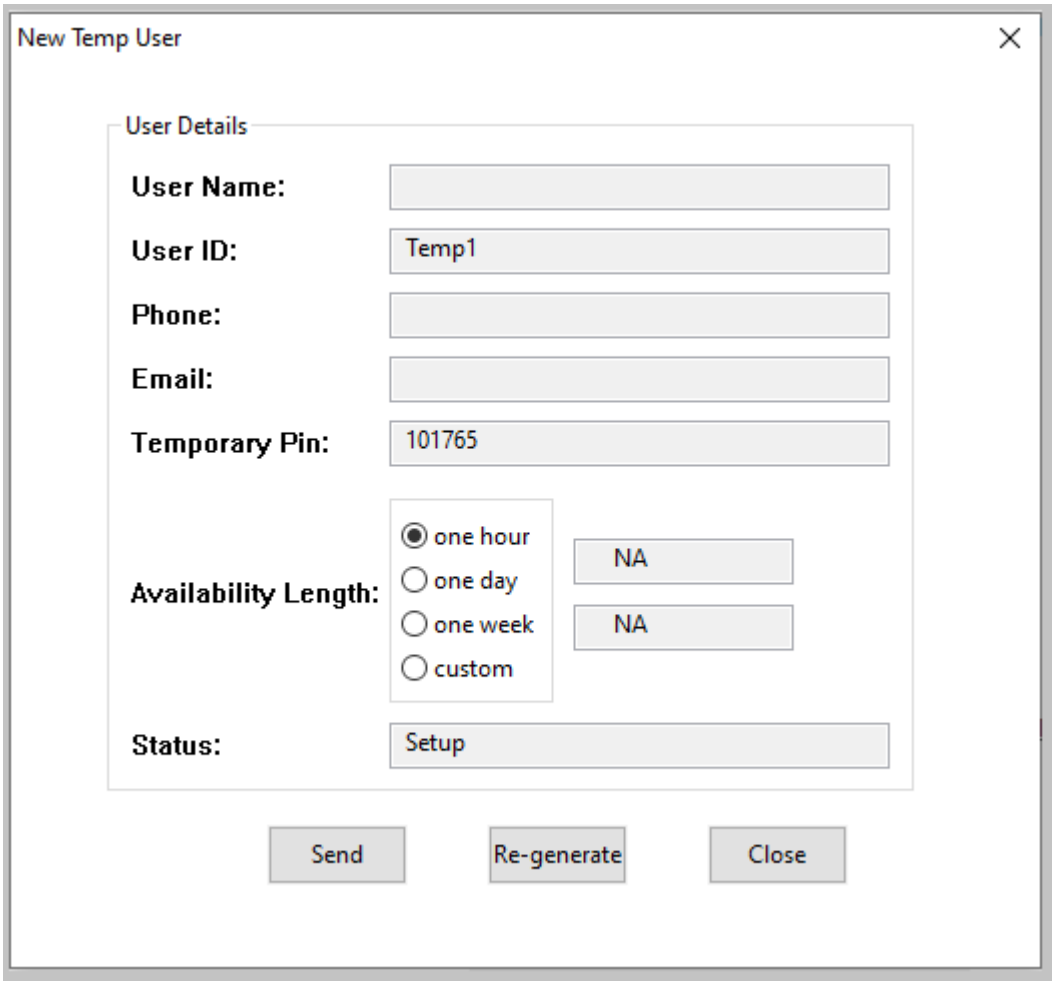
The management of temporary user includes adding new user and update the current user.

6.4.1 Adding New User

There are two types of new user, the first type is the people from outside of the organization, and they do not have a profile in the database. Those people could be visitors or contractors of the company. The second type is the current employee. They have profile in the database, but for some reason they cannot access the cabinet.

6.4.1.1 New User from Outside

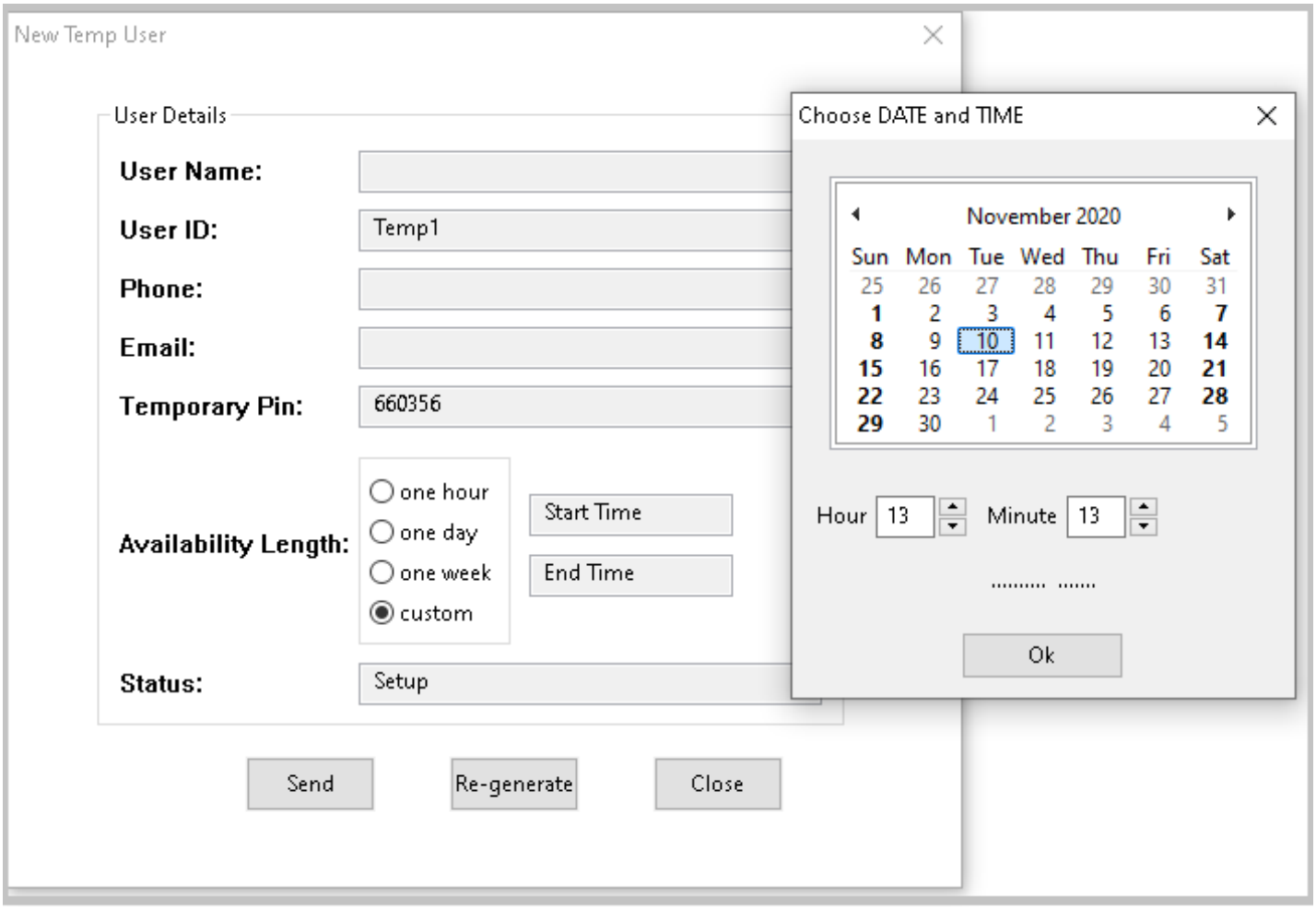
For the new users outside of the organization, they need to input some information for a profile. Click *NEW USER* link from the GUI, a window will pop up for information input. The following is a screenshot.



In the above screen, *User ID* is already filled with a certain value, it is a unique identification number of the temp user and is set by the program; it is read-only.

Temporary Pin is the number that the user input to access the cabinet. It is a 6-digit number, randomly generated by the program. If the number of the PIN does not look very favorable, the admin can press *Re-generate* button, and another PIN will be generated.

Availability Length is the time range from the moment when the PIN is generated to the time when the PIN expires. By default, it is *one-hour*, other values can be *one day*, *one week*, or *custom*. When choosing *custom*, the two fields on the right will become available and be labelled *Start Time* and *End Time*. These are the time when the PIN becomes valid and the time when the PIN expires. The following is a screenshot.

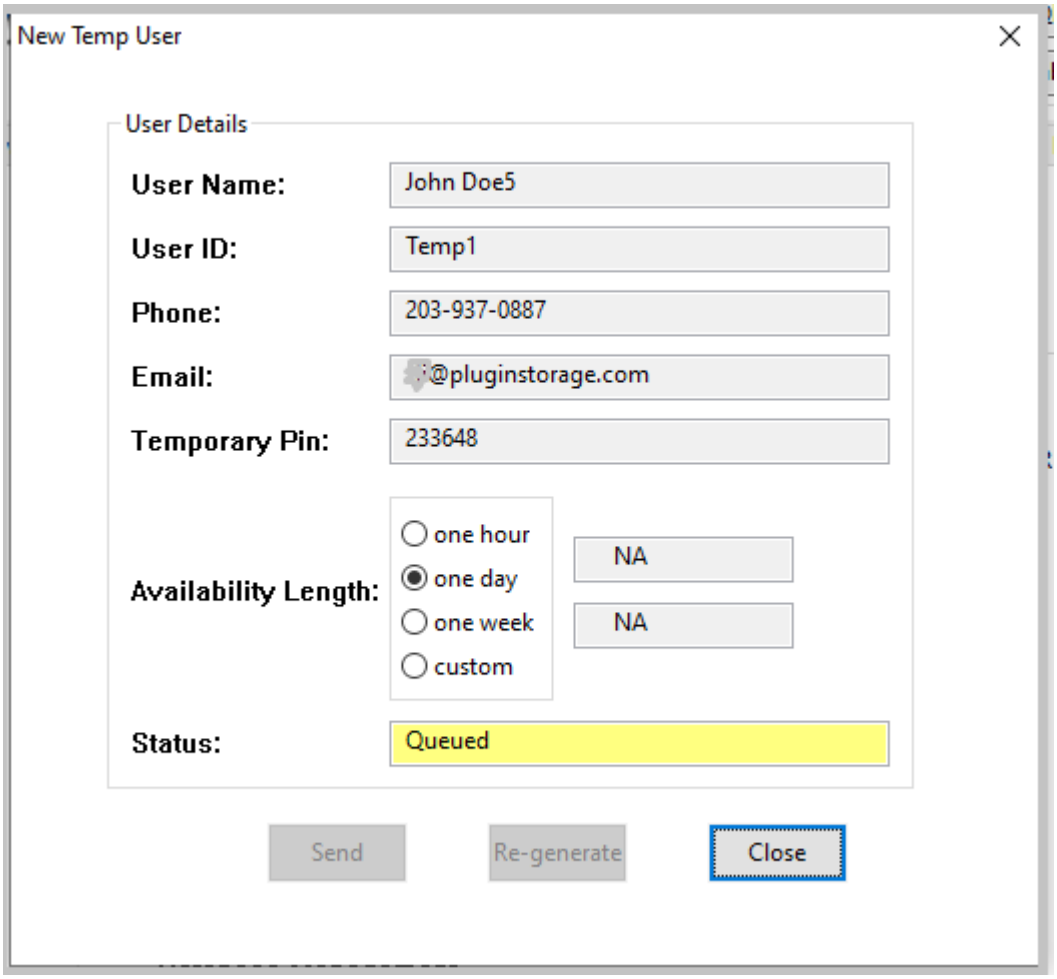


Status section is the current status of the PIN configuraiton. The default value is *Setup*, it is the first status when the PIN has been created. There are more discussions about *Status* later in *section 6.4.2*.

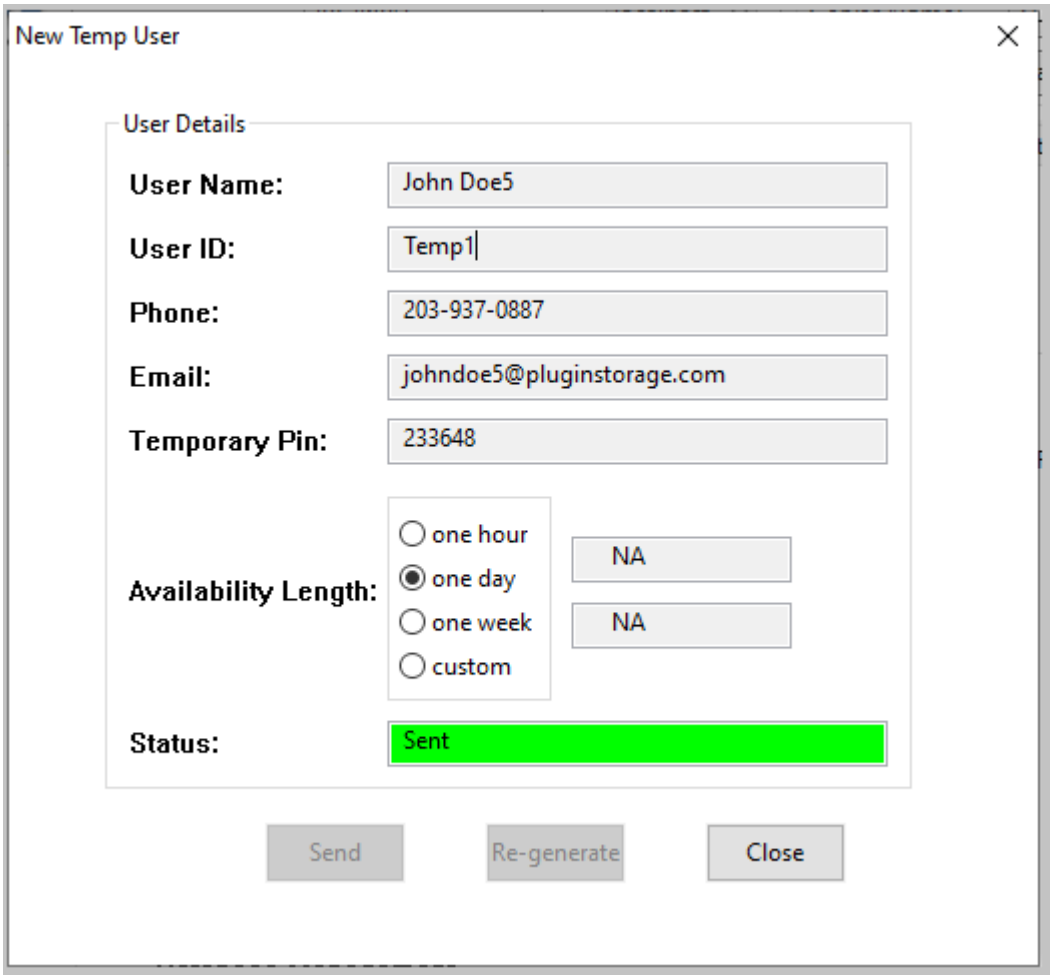
For other fields of the form, *User Name* is normally the name of the user, *Phone* number can be optional; while *Email* is a required field. The program needs to send the PIN to the user's email account; it is an important step before the PIN becomes valid.

After all the information are prepared, click *Send* button and the information will be saved into the database and the PIN is ready to be sent out to the user by email.

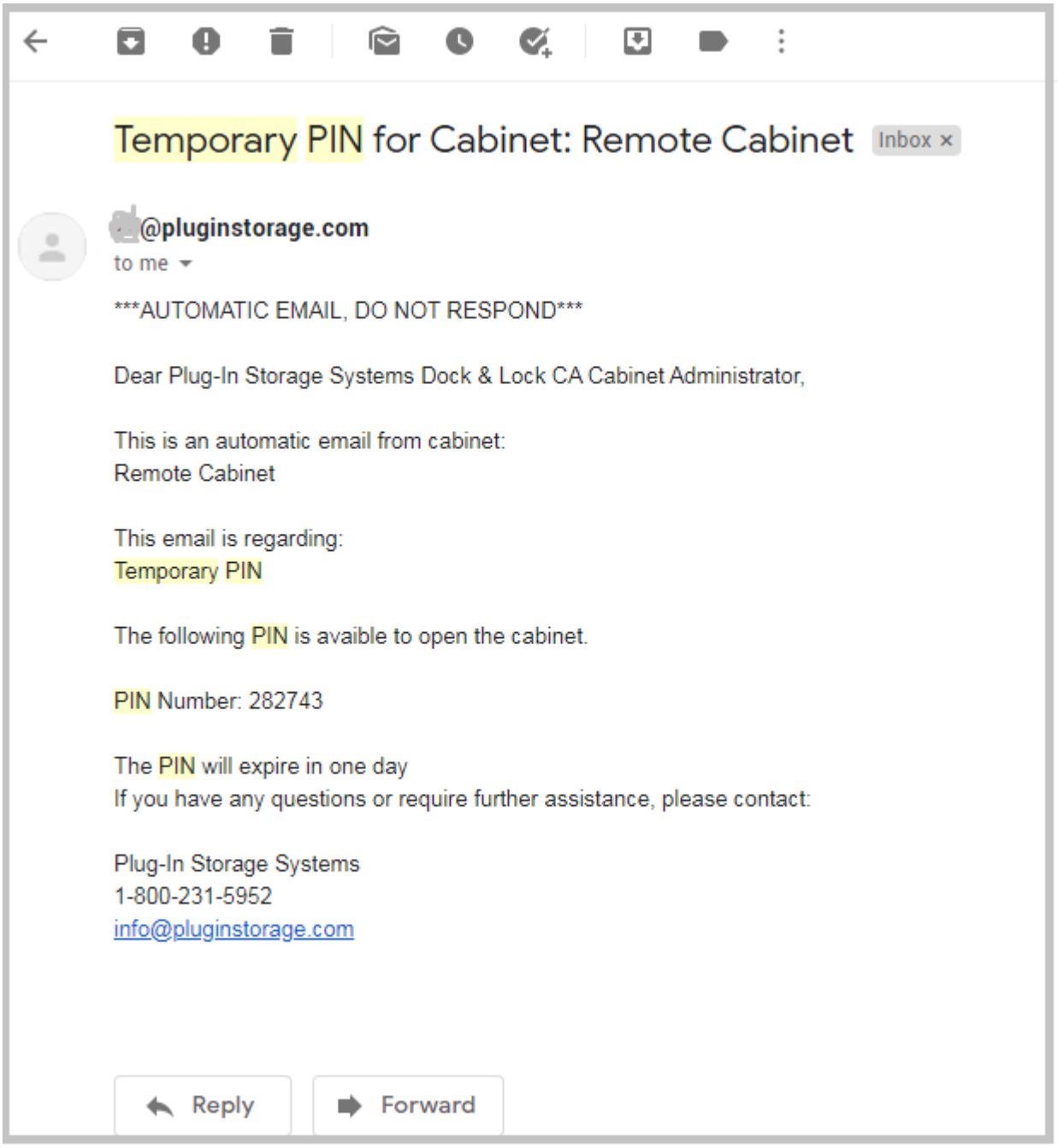
After clicking Send button, a screenshot is shown as following. We can see the status becomes *Queued*; it means the temp PIN is in the queue of email sending.



After several seconds or a minute, the email for the PIN will be sent out, and the status will become *Sent*. A screenshot is as following:



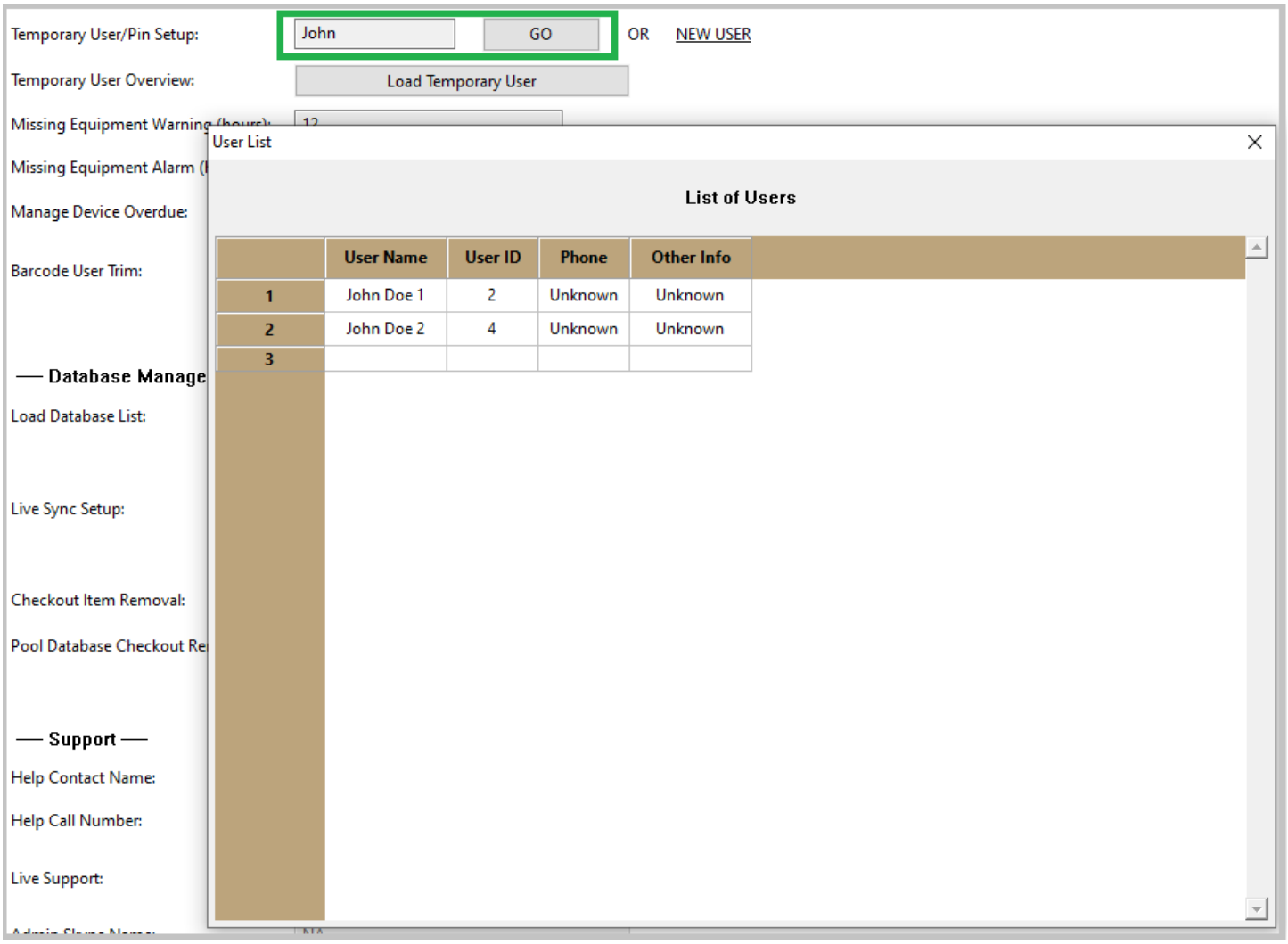
If the user checks his/her email, an email might be found like the following:



6.4.1.2 New User as Current Employee

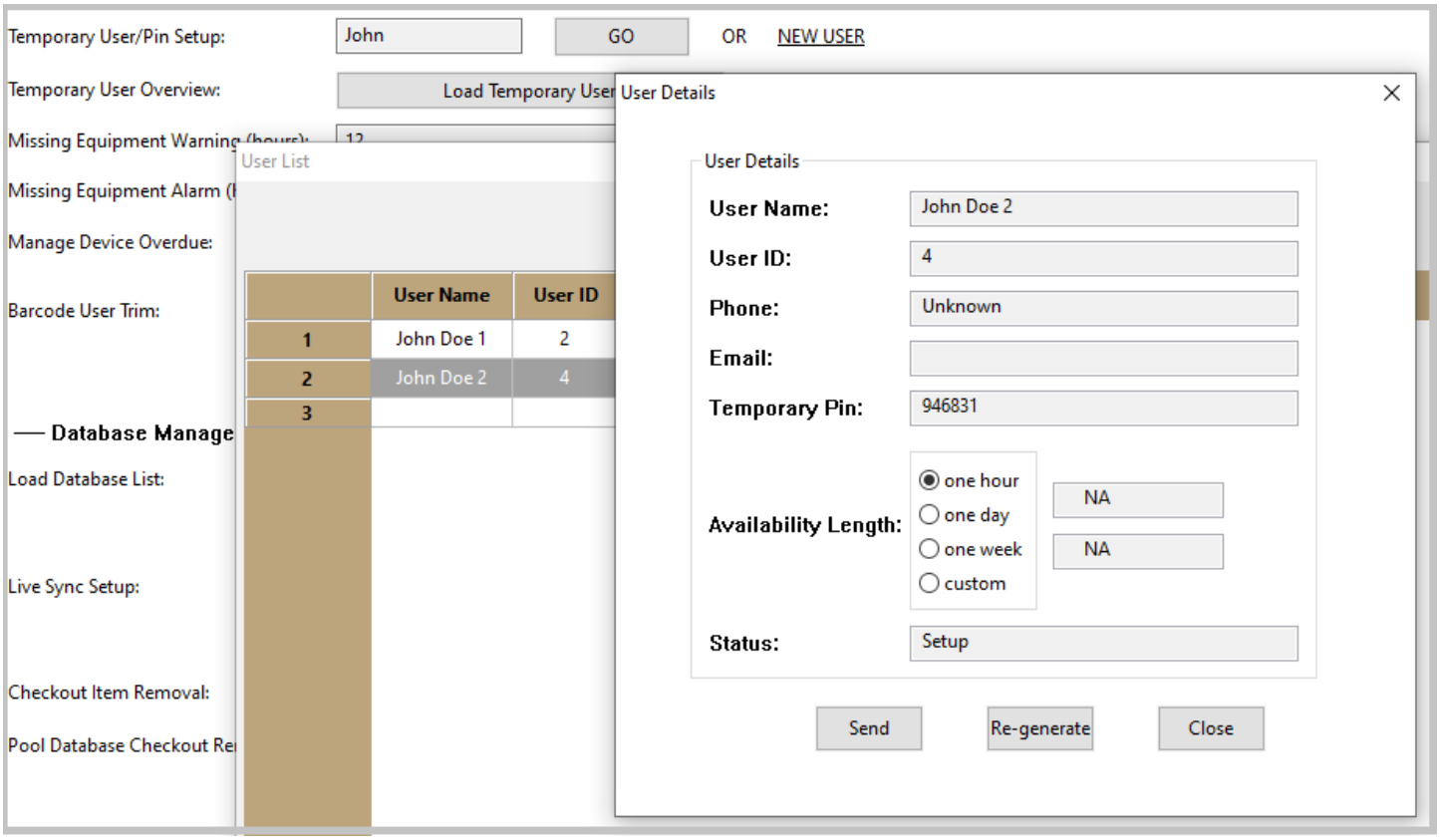
A current employee sometimes does not have their badge at hand, and they might need to be temporarily registered to access to the cabinet. Because they already have a profile in the database, their information can be directly loaded into the profile as temp users.

In the *User Name* section, type in part of the name for the user as a keyword, and click *GO* button, a window will pop up with a list of all the users with their names having the keyword. The following is a screenshot.



In the above screen, type in *John* in the *User Name* section, and the window lists all the users in the database with keyword *John* included.

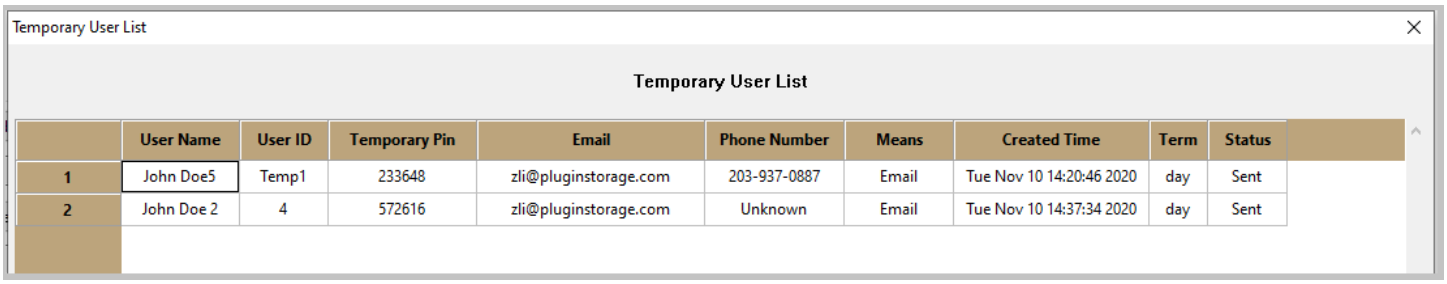
Click the corresponding line in the table, and a window will pop up with the detailed setup for the profile of temp user. If the information is complete and correct, just click *Send* button, and the PIN will be sent out. Make sure email address is correct, because it is required for sending the PIN.



6.4.2 Update Current User

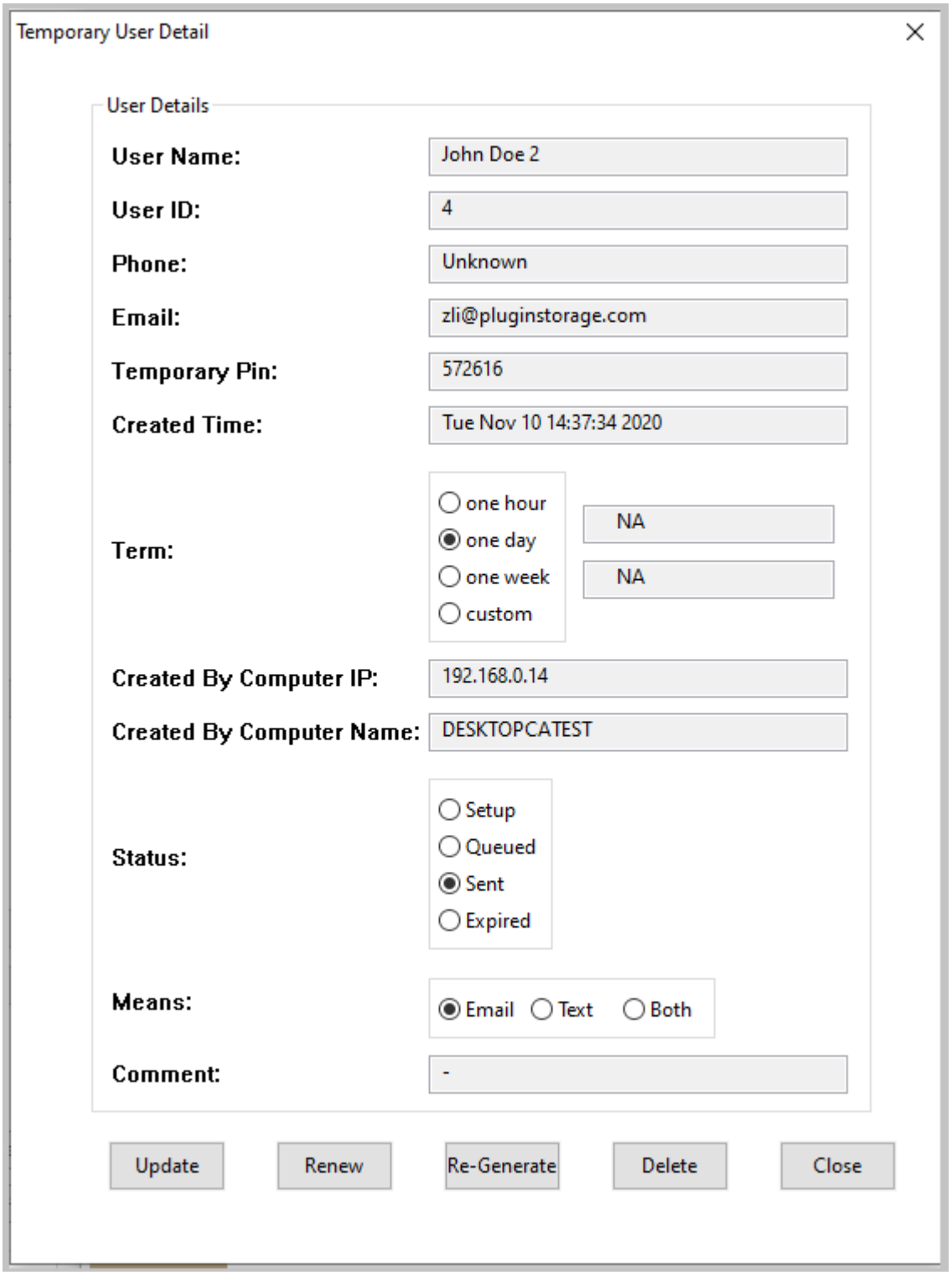
After the temp user has been added in the database, it may need some change for the information, and the PIN might need renewal when it is close to expiration. For these situations, we need to do some update to the configuration of the user.

Click *Load Temporary User* button, and a window will pop up with the list of temp users:



The list is a summary of all the temporary users. It includes the columns *of User Name, User ID, Temporary PIN, Email, Phone Number, Means, Created Time, Term,* and *Status*.

From the list, click the row with the user to be updated, a window will appear with more detailed information as following:



In the information fields, *User ID* is setup by the program as a unique string, which is read-only. *Created Time*, *Created By Computer IP*, *Created By Computer Name* are about a history event, and they are read-only too.

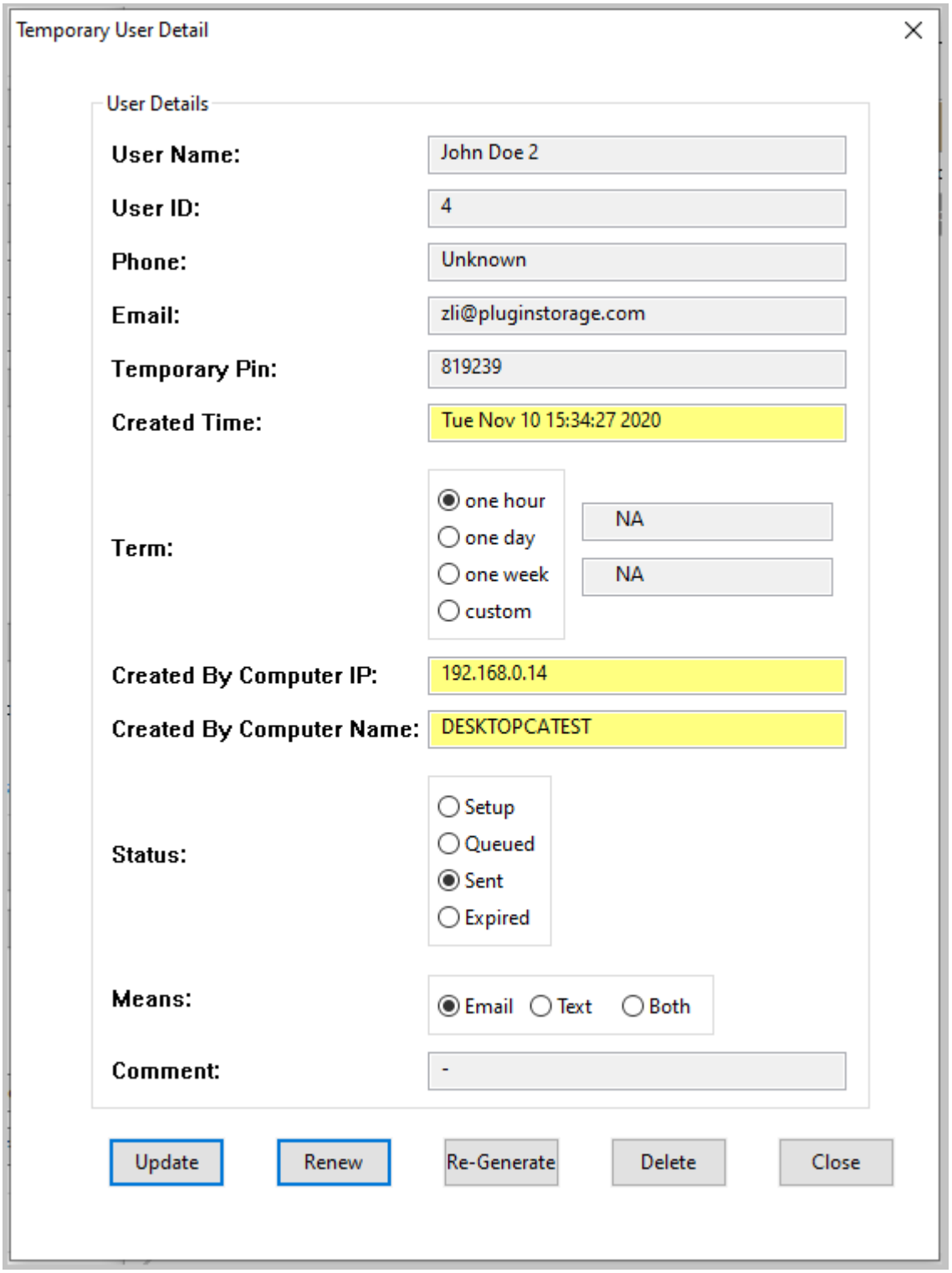
Status field has four status: *Setup, Queued, Sent, and Expired.* When a record is created, the status is *Setup*; after clicking *Send* button, the information enter the queue of email sending, and the status becomes *Queued*; after

the email has been sent, the status becomes *Sent*; when the time expired and the PIN becomes invalid, the status becomes *Expired*.

Means field is about how to send the PIN to the user. It includes *Email*, *Text*, and *Both*. The default setting is sending by email.

When clicking *Re-Generate* button, the PIN will be changed with another number.

When clicking *Renew* button, the PIN will become valid again starting from the moment when the button is pressed. And some fields will change to yellow color to indicate the change. The following is a screenshot.

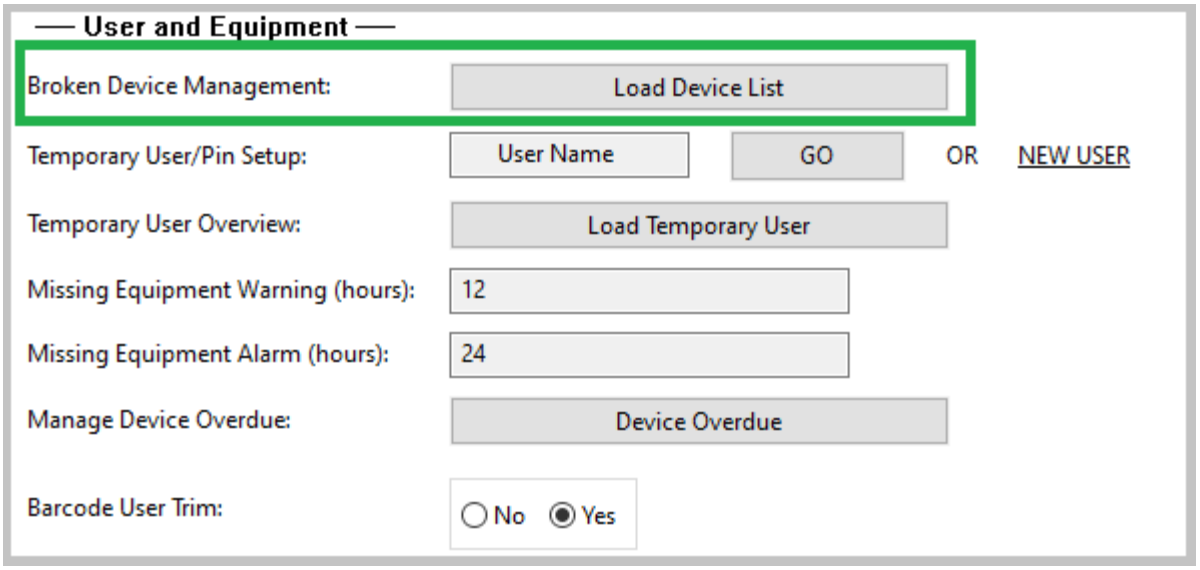


6.5 Broken Device Management

When a broken device is found, it can be reported and be stored into the database. The information can be used for device tracing and process improving.

6.5.1 Broken Device Report

Broken device can be reported from the cabinet keypad or CAC-GUI. The management of broken device locates in tab *System Config* of CAC-GUI. The following is a screenshot:



More details will be discussed in following sections.

6.5.1.1 Broken Device Report from Cabinet

When broken device is reported from cabinet, it can be the administrator to do the report or a regular user to do the report. They follow different path when using the keypad to do the report.

6.5.1.1.1 Broken Device Report from Cabinet by Administrator

After the administrator has accessed the cabinet, the screen will show the instruction for activity selection, a screenshot looks like the following:

Then use the up and down arrow key to browse the menu, and find the option *BROKEN DEVICE* as following:

Press *ENTER* button from the keypad to enter the process of broken device reporting. The next screen looks like the following:

Use the arrow key in the keypad to navigate the device list, find the device to report, and press *ENTER* button.

Normally the device needs to be in checkout state when reporting the broken. If it is not in checkout state, the screen will give a feedback like following:

If the device is in checkout state, it will be reported as broken and added in the database; at the same time, the device is checked in, and the related drawer is locked to prevent further checkout. The responding screen looks like a normal check-in:

6.5.1.1.2 Broken Device Report from Cabinet by Regular User

The broken device can be reported by administrator, and it can also be reported by a regular user.

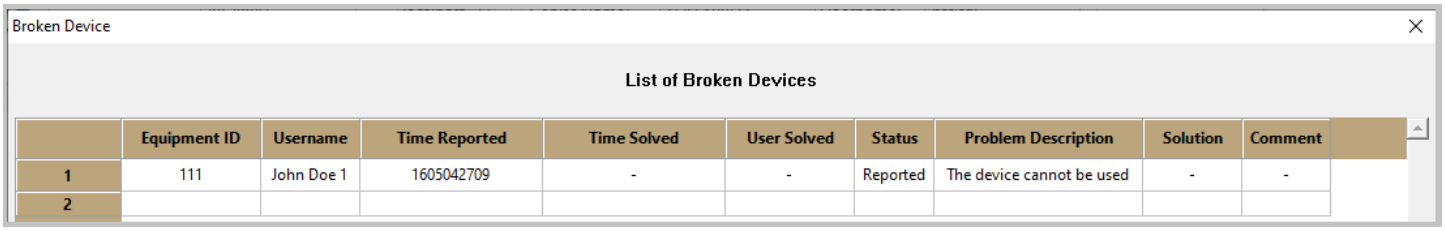
The reporting process for a regular user starts from *HELP* button on keypad. After press *HELP* button, the screen looks like the following:

Use arrow button in the keypad to browse the menu, and choose the one with *REPORT BROKEN DEVICE*, a screen looks like the following:

Scan the badge and place the device in the drawer when the drawer is open. The device will be added into the database as broken, and the device is also labelled as check-in.

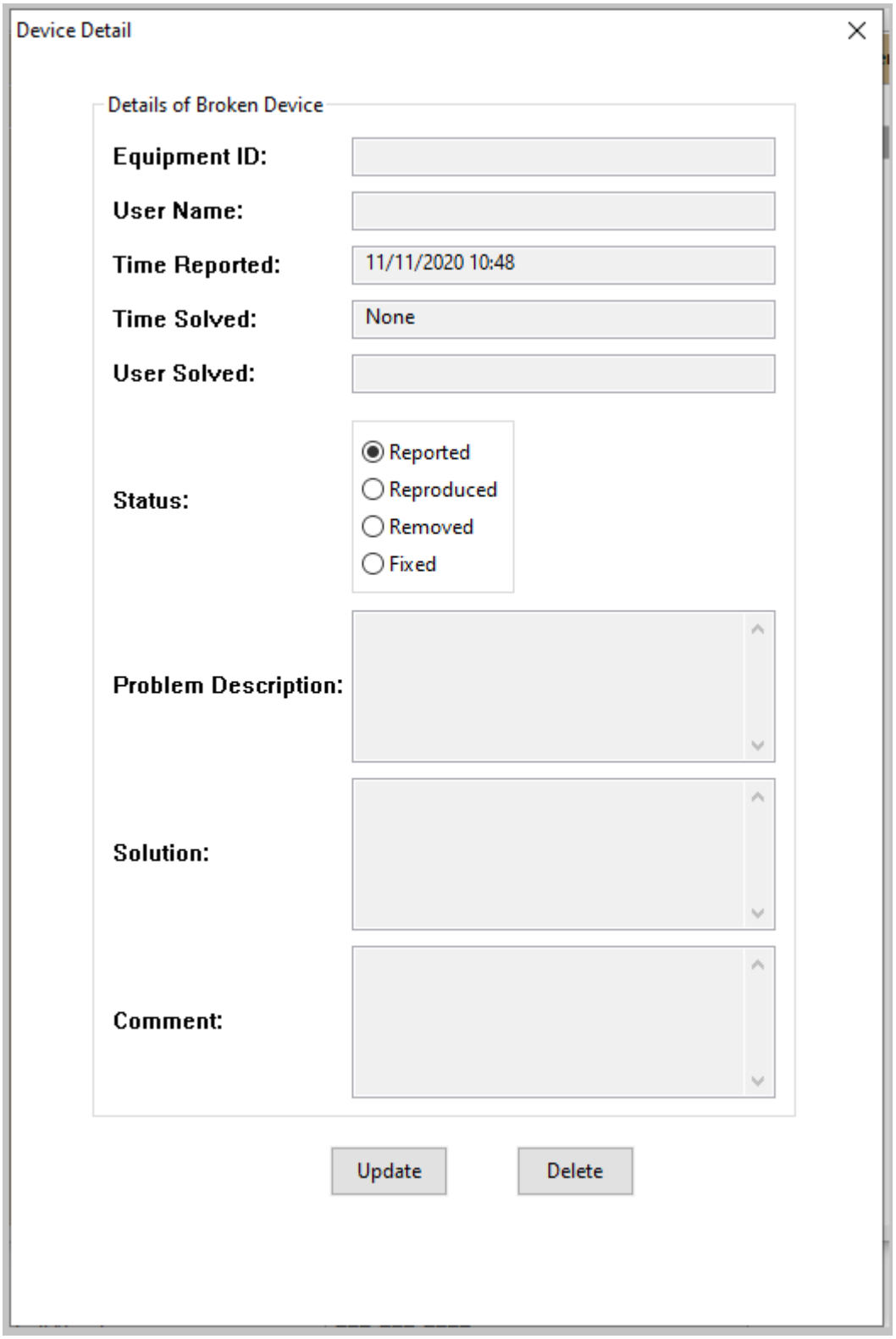
6.5.1.2 Broken Device Report from CAC-GUI

From tab *System Config* of *CAC-GUI*, click *Load Device List* button, a window will pop up with all the broken device records, and the last line of the table is blank. A screenshot is as following:



	Equipment ID	Username	Time Reported	Time Solved	User Solved	Status	Problem Description	Solution	Comment
1	111	John Doe 1	1605042709	-	-	Reported	The device cannot be used	-	-
2									

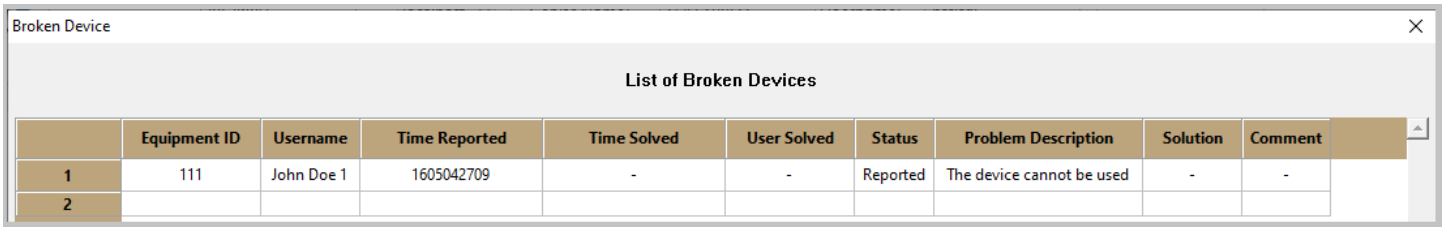
Click the last line, which is blank, a window will pop up with the input of new broken device record. A screenshot is as following:



In the information list of broken devices, *Time Reported* has been filled automatically with the current time stamp. The default value of *Status* is *Reported*. The administrator can fill in *Equipment ID, User Name, Problem Description* and *Comment*, then press *Update* button, the record will be added in the database.

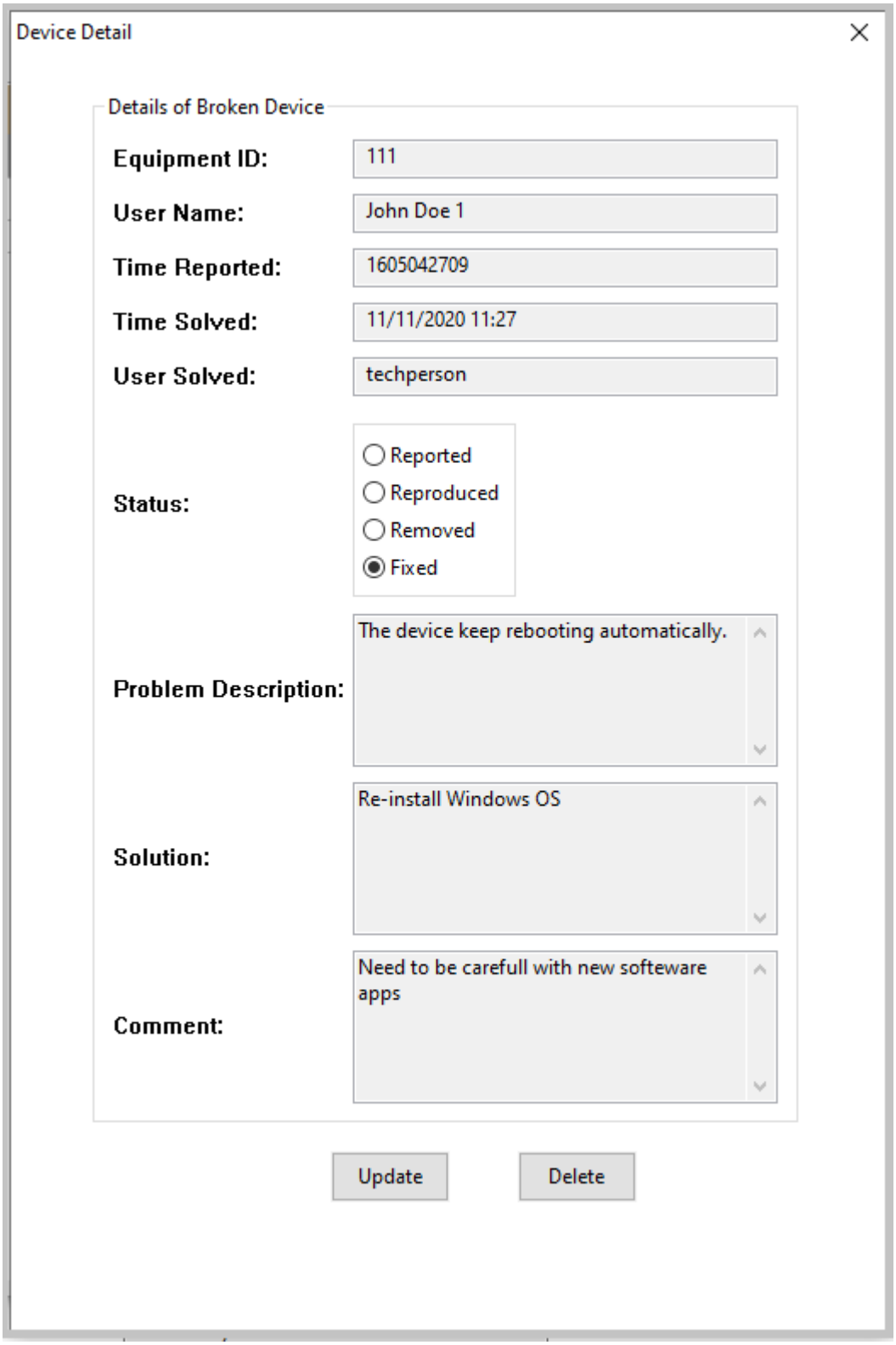
6.5.2 Broken Device Record Management

After the broken device has been reported, the administrator can trace the event and update the status in the database. As indicated in last section, when press *Load Device List* button, a window will pop up with the list of broken devices.



	Equipment ID	Username	Time Reported	Time Solved	User Solved	Status	Problem Description	Solution	Comment
1	111	John Doe 1	1605042709	-	-	Reported	The device cannot be used	-	-
2									

Click a certain record (such as *John Doe 1* in the table), a window will pop up with the details of the record. The following screenshot is an example.



The processing for a broken device has several statuses: *Reported*, *Reproduced*, *Removed*, and *Fixed*. *Reported* is the status that the device has been reported as broken. *Reproduced* is the status that the issue has been reproduced by the maintenance engineers. *Removed* means the device is probably too hard to fix and is removed

from the equipment list. *Fixed* status means the device has been fixed and can be used again. All the statuses need to be manually updated in the process of investigation.

After the device is labelled as *Fixed* status, the administrator needs go to *Equipment List* tab and *Drawer Config* tab of *CAC-GUI*, and make sure the related device and drawer to be **unlocked**.

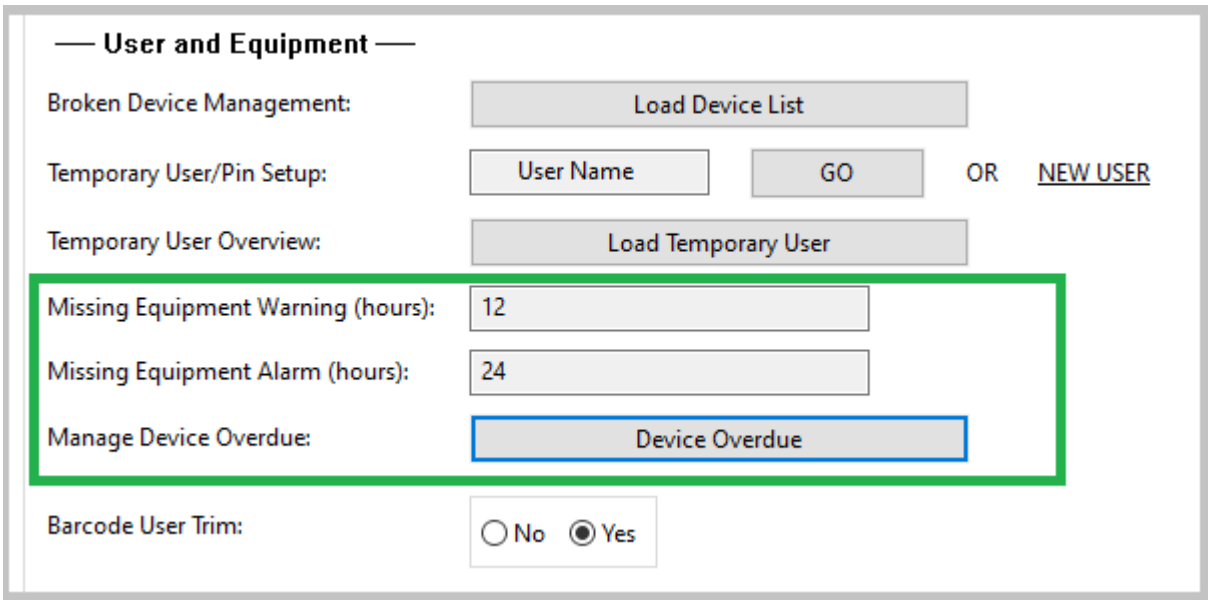
If the record of broken device is a false alarm or it has become obsolete, pressing *Delete* button can remove the record from the database.

6.6 Equipment Overdue

The Equipment needs to be returned after certain time of checkout. If over a defined time range, it is called equipment overdue or missing equipment.

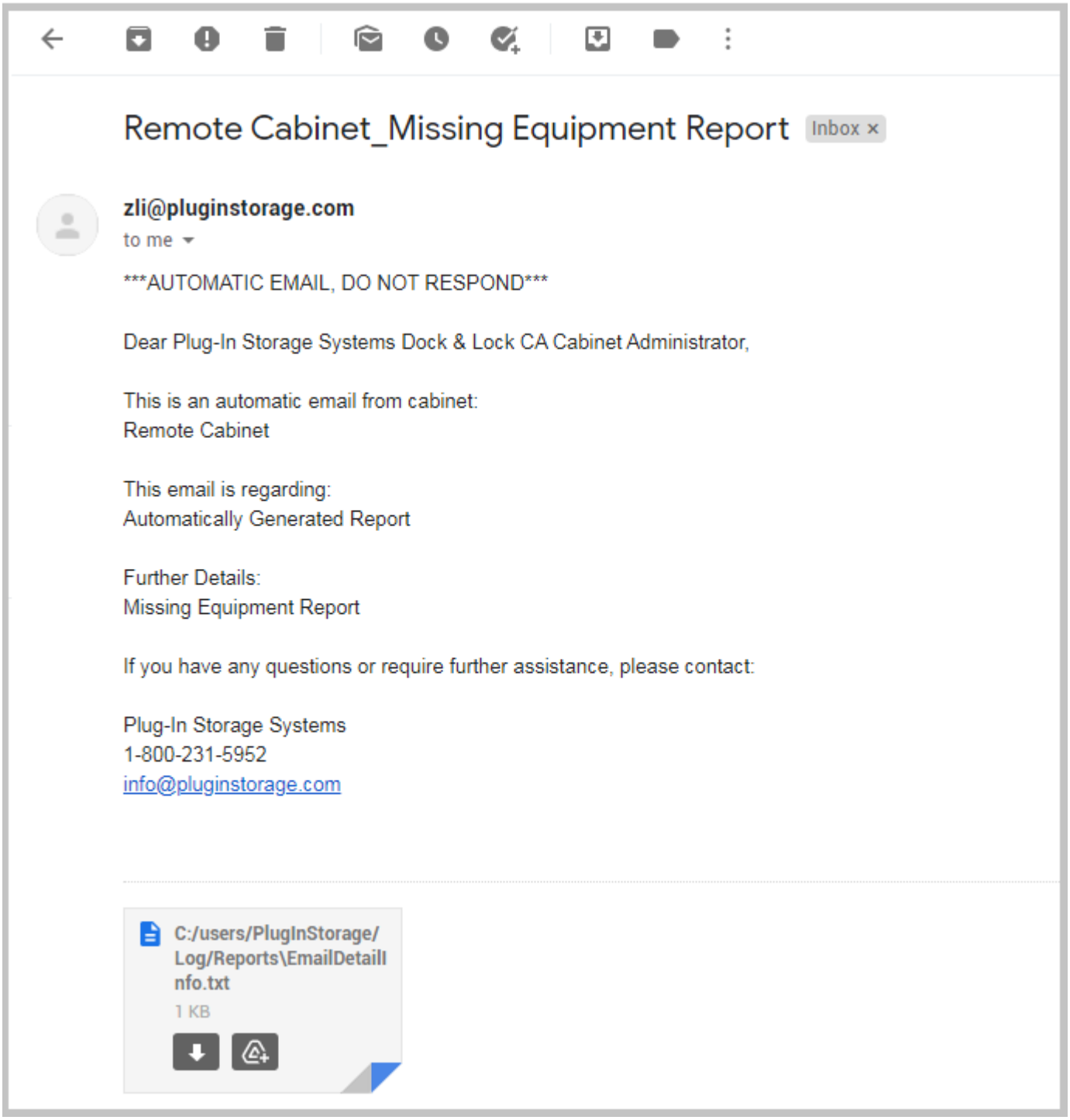
6.6.1 Equipment Overdue Setup

The time range can be set up in *System Config* tab of *CAC-GUI*. The following is a screenshot for the setup:



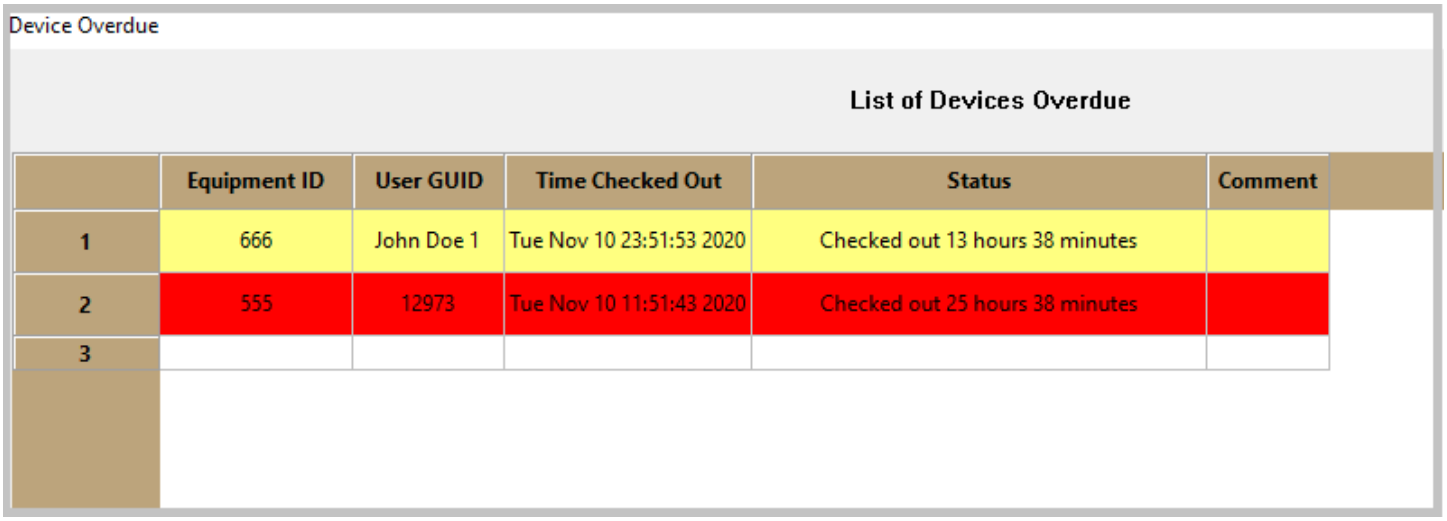
There are two level of alerts for the missing equipment. *Missing Equipment Warning* field is the time for giving a warning; An email will be sent out to the administrator to inform the details about the equipment checkout. At the same time, a record will be added to the database for this checkout. *Missing Equipment Alarm* is the time when the issue needs to be alarmed; it is a more serious level of alert. The default value of *Missing Equipment Warning* is 12 hours; the default value of *Missing Equipment Alarm* is 24 hours.

A screenshot of the email about missing equipment is as following:



6.6.2 Equipment Overdue Record Management

When the time of a device checkout passes over the configured range, a record is added to the database for the details about the checkout. When clicking *Device Overdue* button in *System Config* tab, a window will pop up with the list of the record. The following is a screenshot for the window:

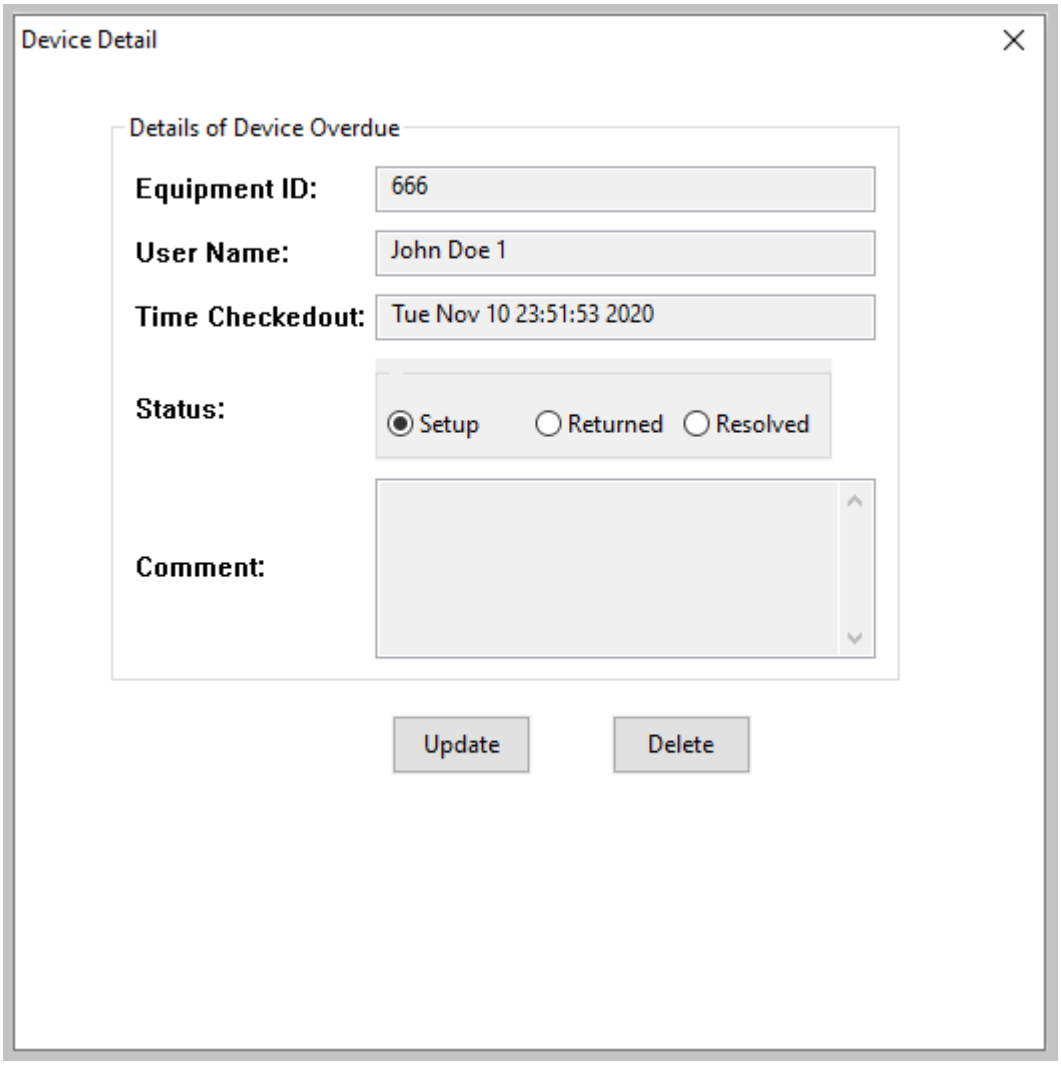

Device Overdue

List of Devices Overdue

	Equipment ID	User GUID	Time Checked Out	Status	Comment
1	666	John Doe 1	Tue Nov 10 23:51:53 2020	Checked out 13 hours 38 minutes	
2	555	12973	Tue Nov 10 11:51:43 2020	Checked out 25 hours 38 minutes	
3					

When the time of checkout has passed the warning hours, the record shows as color yellow; and when the time of checkout has passed the alarm time, the record shows as red.

When click a row in the table, a window will appear will the details about the record. The following is a screenshot:



In the above window, Fields of *Equipment ID*, *User Name* and *Time Checkedout* are read-only; The *Status* includes *Setup*, *Returned*, and *Resolved*. *Setup* is the initial status when the record is created; if the equipment has been returned, the status can be updated to *Returned*; if the equipment has not been returned but somehow the issue has been settled, the status can be updated to *Resolved*. The administrator can write down some comments in *Comment* field if necessary.

If the record is a false alarm or it has become unnecessary in the database, press *Delete* button and the record will be removed.

7 DISPLAY AND ACTIVITY LOG

7.1 Status Snapshot in Real Time

In tab *Snapshot/Cabinet Commands* of *CAC-GUI*, we can see all the major aspects of the cabinet in one page, it includes the status of the drawers, such as it is open or closed, it is checked in or checked out, last time the drawer was opened, the username if it is checked out, the signature ID of the person who checked the equipment out, the equipment ID, and the equipment description. It could have different color when it is in different status.

All the information is in real time; it is updated every one second.

	OPEN DRAWER	DRAWER STATUS	CHECKED IN or OUT	LAST TIME DRAWER WAS OPEN	USER NAME	SIGNATURE ID	EQUIPMENT ID	EQUIPMENT DESCR.
1	☐	Closed	IN	Tue Nov 10 16:11:48 2020	-	-	111	description 1
2	☐	Closed	IN	Wed Nov 11 14:46:32 2020	-	-	222	description 2
3	☐	Closed	OUT	Thu Nov 12 14:41:18 2020	John Doe 1	e38a84a5ef577	999	description 9
4	☐	Open	IN	Tue Nov 03 11:51:17 2020	-	-	333	description 3
5	☐	Closed	IN	Wed Nov 11 14:37:34 2020	-	-	444	description 4
6	☐	Open	IN	unknown	-	-	-	-
7	☐	Open	IN	unknown	-	-	-	-
8	☐	Open	IN	unknown	-	-	-	-
9	☐	Open	IN	unknown	-	-	-	-
10	☐	Open	IN	unknown	-	-	-	-
11	☐	Open	IN	unknown	-	-	-	-
12	☐	Open	IN	unknown	-	-	-	-
13	☐	Open	IN	unknown	-	-	-	-
14	☐	Open	IN	unknown	-	-	-	-
15	☐	Open	IN	unknown	-	-	-	-
16	☐	Open	IN	unknown	-	-	-	-
17	☐	Open	IN	unknown	-	-	-	-
18	☐	Open	IN	unknown	-	-	-	-
19	☐	Open	IN	unknown	-	-	-	-
20	☐	Closed	IN	Wed Nov 11 14:36:25 2020	-	-	555	description 5
21	☐	Closed	IN	Thu Nov 12 14:22:56 2020	-	-	666	description 6
22	☐	Closed	IN	Thu Nov 12 14:41:02 2020	-	-	777	description 7
23	☐	Closed	IN	Thu Nov 12 14:19:20 2020	-	-	888	description 8
24	☐	Closed	IN	Tue Nov 03 12:44:33 2020	-	-	101010	description 10

7.2 Cabinet Overview

Cabinet overview is an overall look to all the drawers of the cabinets. It is similar to the tab *snapshot* (section 7.1) but has more visual effect.

The overview is located at tab *Drawer Overview* of *CAC-GUI*. The following is a screenshot:

In the drawer display, one block represents a drawer, When the color of the block is yellow and the little black briefcase logo is not present, it means the equipment in the drawer is checked out; if the color is light green and the logo of the little black briefcase is shown, the equipment is in the drawer. If the little lock logo in the block is in lock state, it means the drawer is currently closed; if the little lock logo is open and the color is red, it means the drawer is in open state.

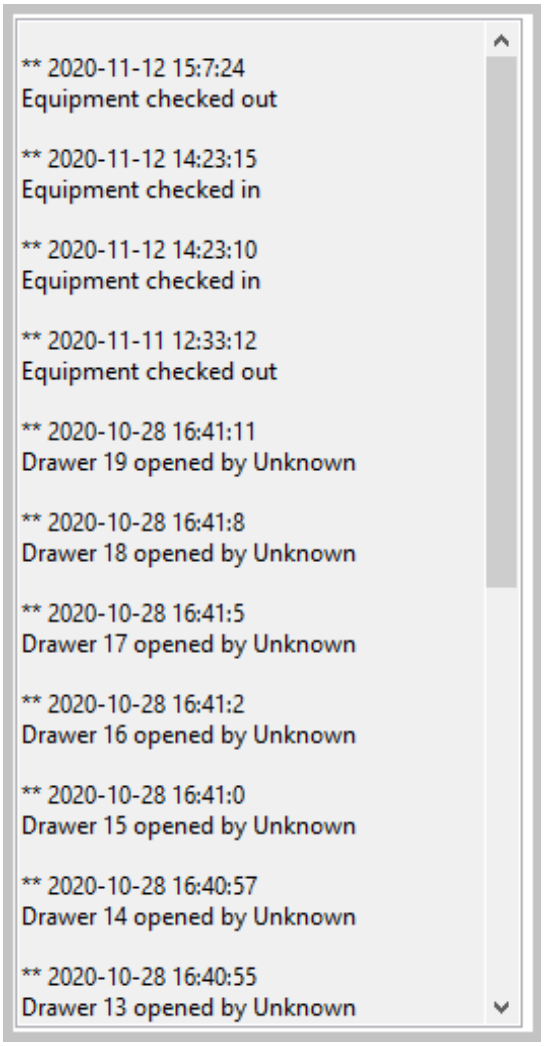
If we want to know more detail about a drawer, just click the drawer block, and a small window will pop up with more details. A screenshot is as following:

In the above example, the summary of drawer 3 is as following:

Drawer Number: 3; *Last Open Time*: 2020-11-12 14:41:18; *Last Open By*: John Doe 1; *Equipment ID*:999; *Equipment Description*: description 9; *Checked Out By*: John Doe 1.

The overview page is also in real time state. When there is a status change with a drawer, such as when the drawer is opening, the block will flash with red color and then go to the new status.

On the right side of the screen, there is a column to display the events about what is happening; it shows the latest 20 events of the cabinet. A screenshot is as following:



This event log only records the events that happening during *CAC-GUI* is in *Drawer Overview* page.

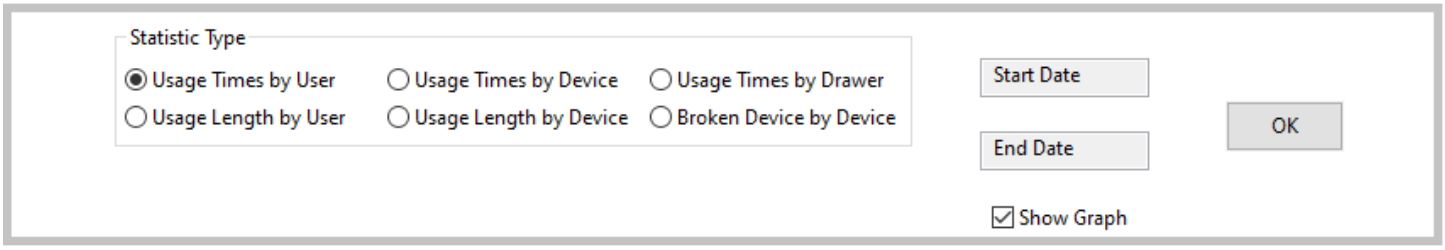
7.3 Statistic Report

Statistic reports are the summaries based on the activity log. It locates at tab *Statistics* of *CAC-GUI*.

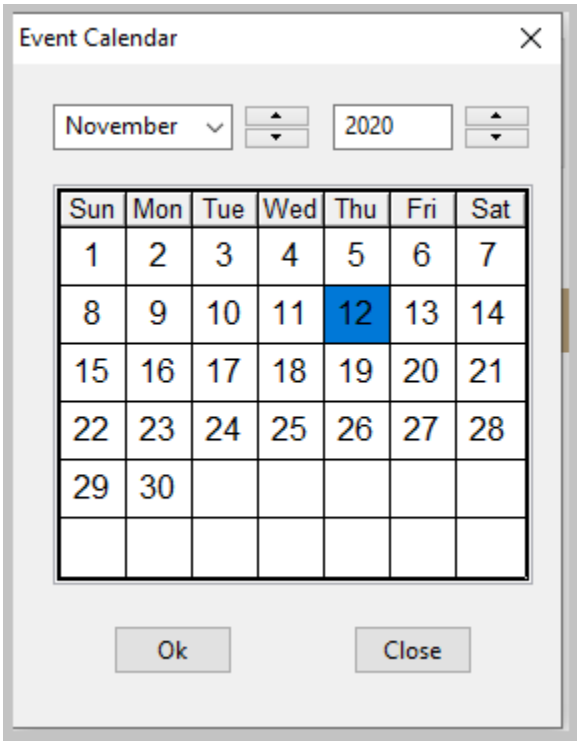
7.3.1 Summary of Statistics and the Setup

The types of statistics include *Usage Times by User, Usage Times by Device, Usage Times by Drawer, Usage Length by User, Usage Length by Device,* and *Broken Devices by Device*.

The flowing is a screenshot:



Fields *Start Date* and *End Date* are used to set up the time range for the statistics, the default value is all the information in the database. When Clicking *State Date* or *End Date*, a window will pop up with a calendar to choose a date. A screenshot is as following:

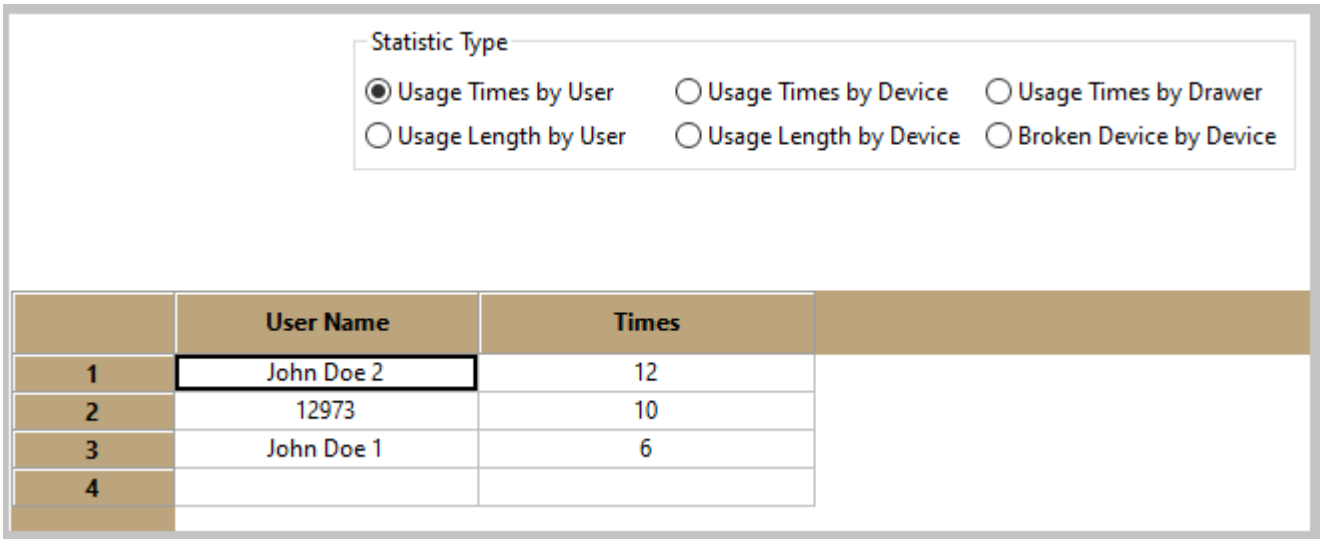


Check box *Show Graph* is for the selection of the graph accompany with the result. If it is chosen, a window with a series of charts will pop up. This will be discussed in later sections.

When clicking *OK* button, the report will be generated.

7.3.2 Usage Times by User

When clicking mode *Usage Times by User* in section *Statistic Type*, or pressing *OK* button with *Usage Times by User* chosen, the table below will display the statistics result:

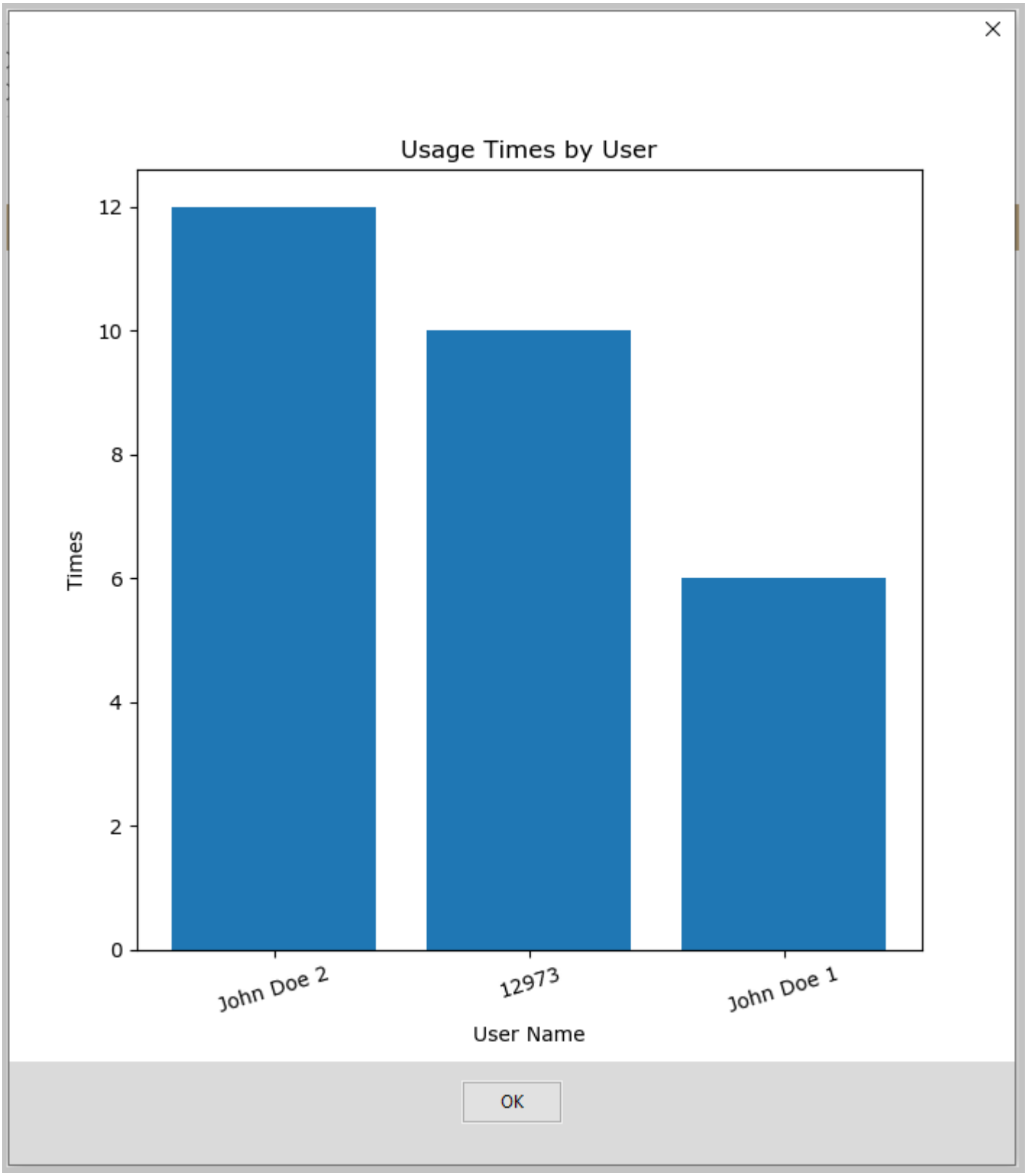


	User Name	Times
1	John Doe 2	12
2	12973	10
3	John Doe 1	6
4		

In the table, we can see *John Doe 2* has checked out and checked-in device 12 times. User *12973* has used the cabinets 10 times, and *John Doe 1* has used the cabinet for 6 times.

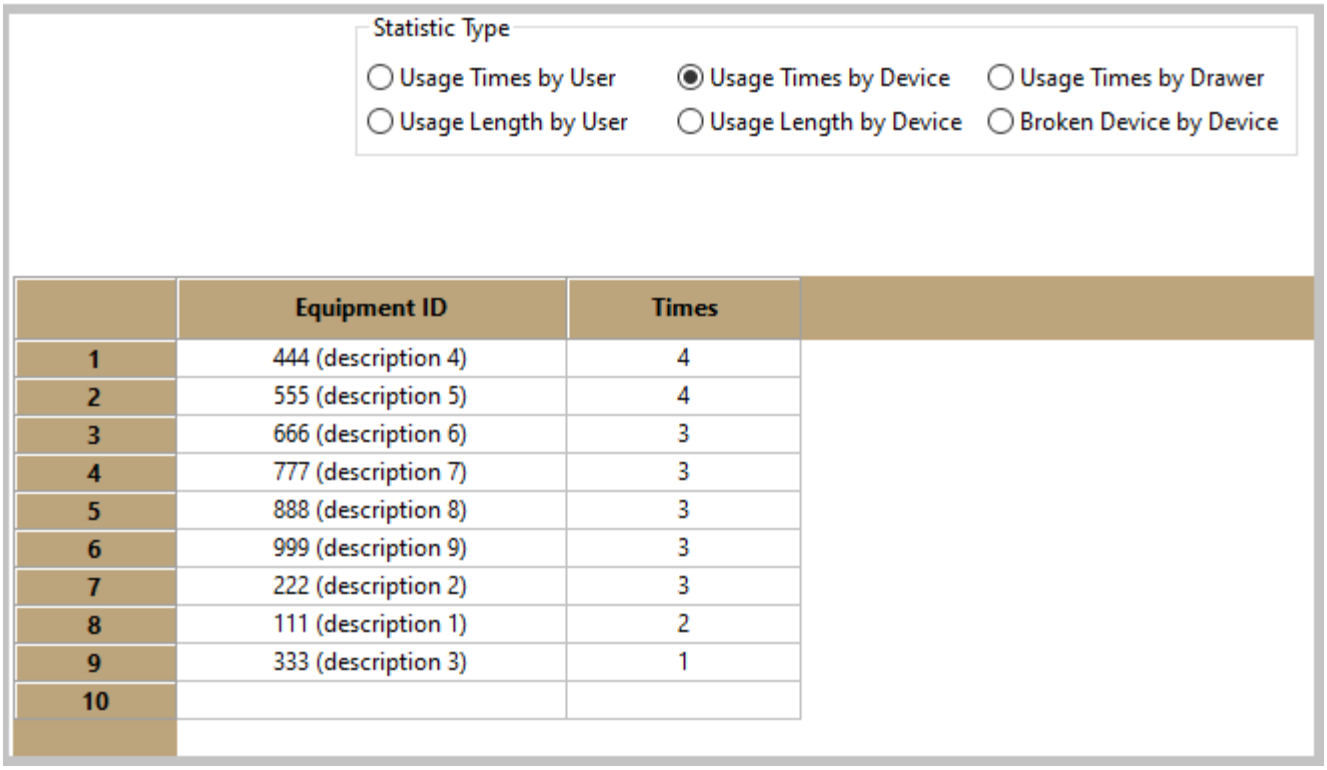
It does not matter which drawer the user has accessed; it calculates the total times the user use the cabinet for the equipment.

If check box *Show Graph* is selected, a window with graph will pop up to illustrate the result of the statistics. The following is a screenshot.


Usage Times by User
12
10
8
6
4
2
0
Times
John Doe 2
12973
John Doe 1
User Name
OK

7.3.3 Usage Times by Device

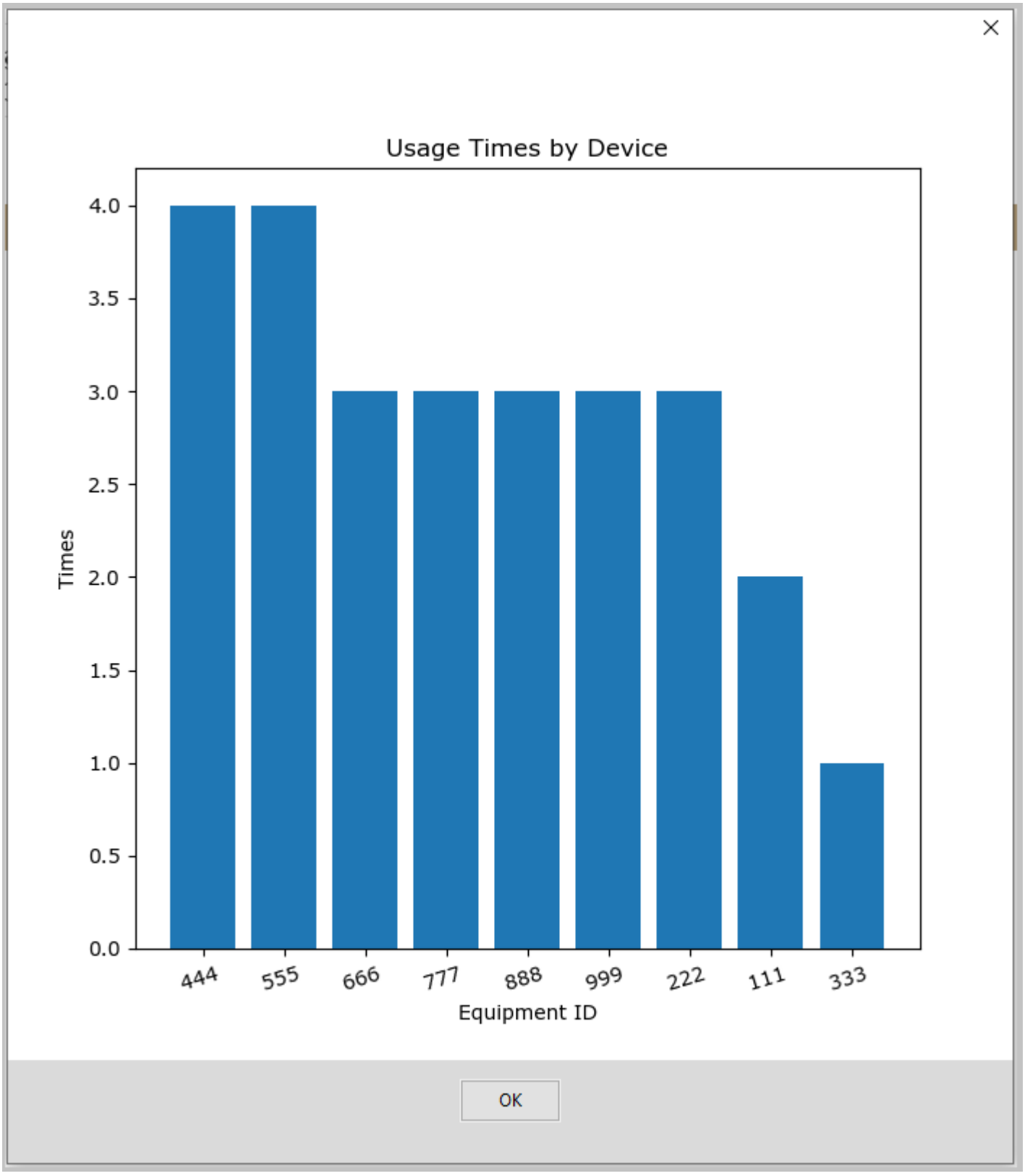
When clicking mode *Usage Times by Device* in *Statistic Type* section, the table will display the related statistics result as following:



	Equipment ID	Times
1	444 (description 4)	4
2	555 (description 5)	4
3	666 (description 6)	3
4	777 (description 7)	3
5	888 (description 8)	3
6	999 (description 9)	3
7	222 (description 2)	3
8	111 (description 1)	2
9	333 (description 3)	1
10		

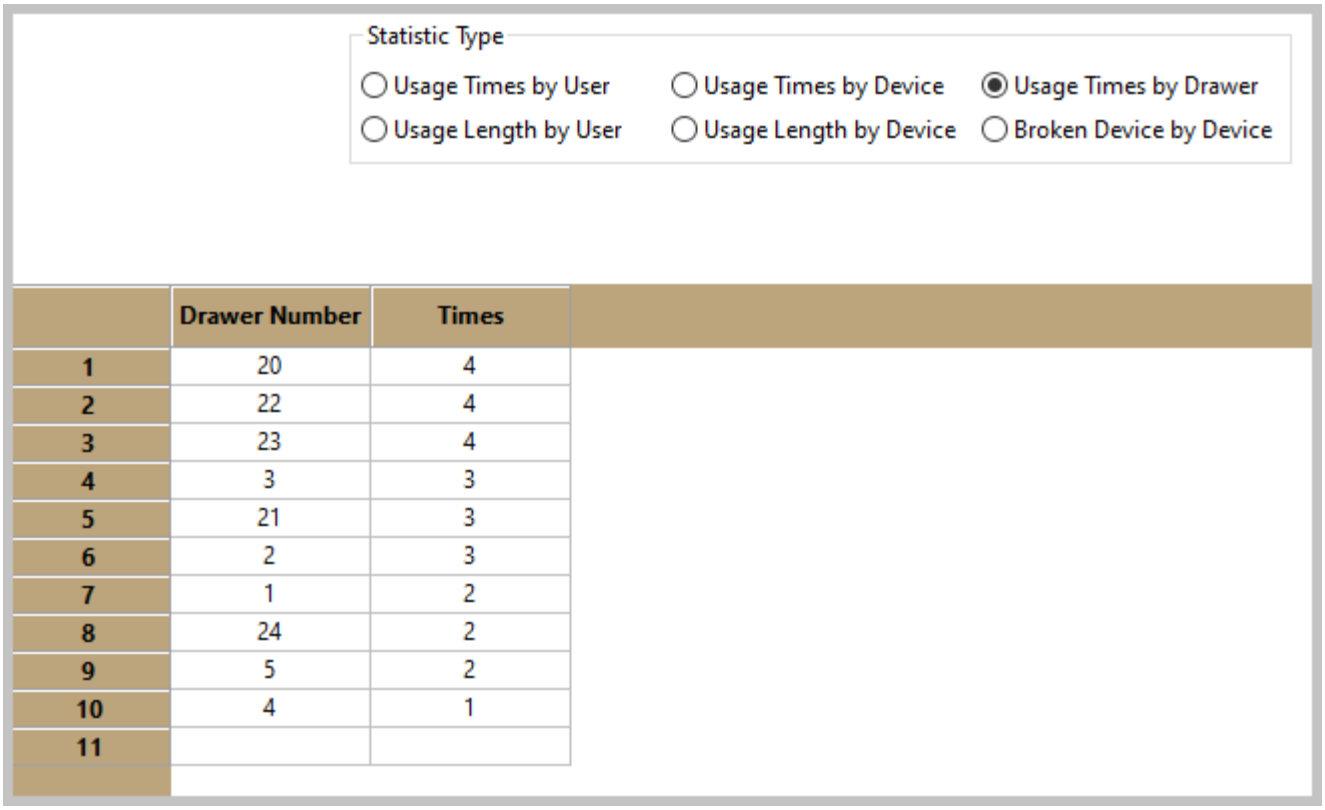
The first column is the *Equipment ID* of the device and the information in the bracket is the description of the device, the second column is how many times the device has been used.

The related graph is as following:


Usage Times by Device
Times
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
444
555
666
777
888
999
222
111
333
Equipment ID
OK

7.3.4 Usage Times by Drawer

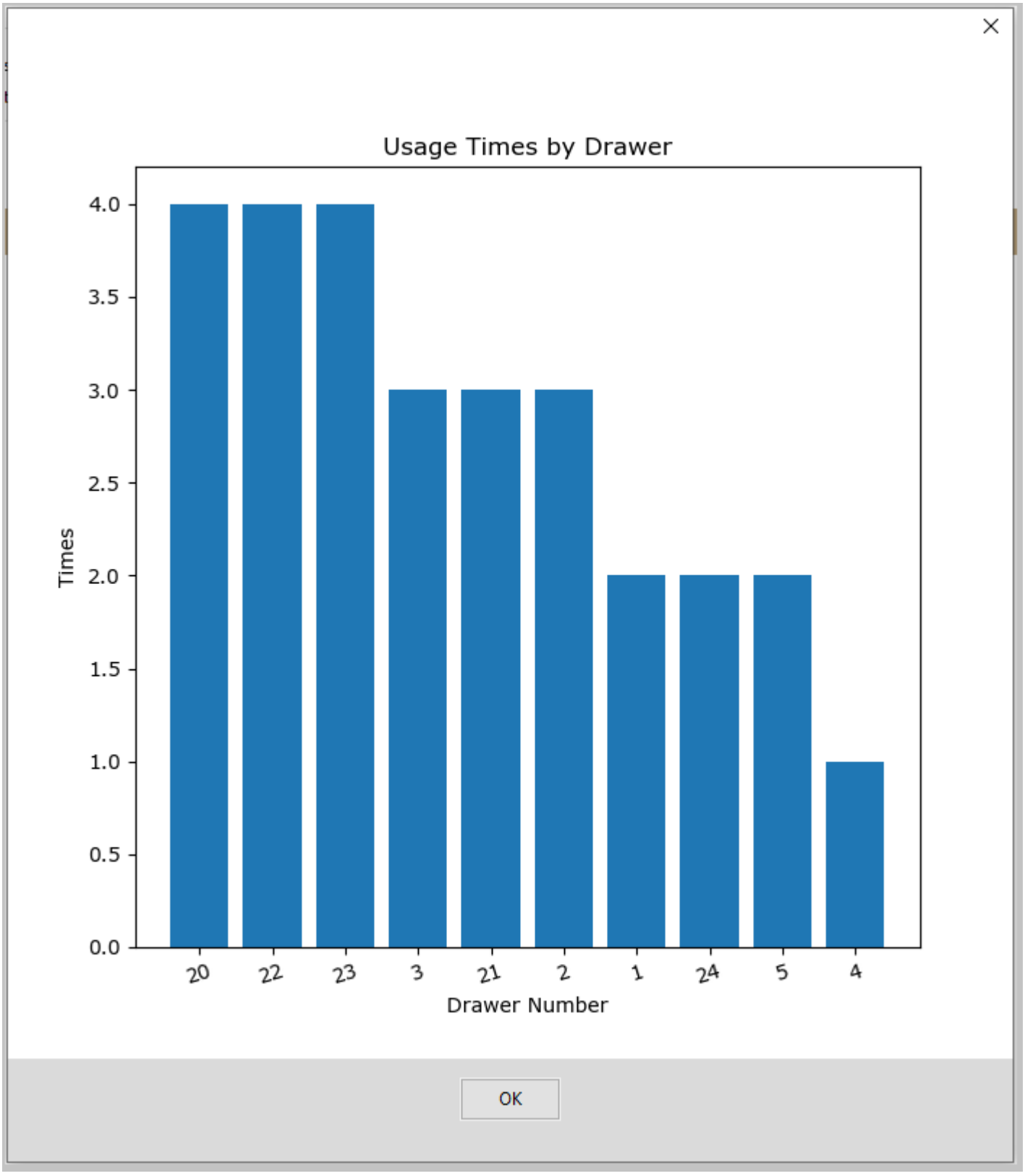
When clicking *Usage Times by Drawer* in *Statistic Type* section, the table will display the statistics result as following:



	Drawer Number	Times
1	20	4
2	22	4
3	23	4
4	3	3
5	21	3
6	2	3
7	1	2
8	24	2
9	5	2
10	4	1
11		

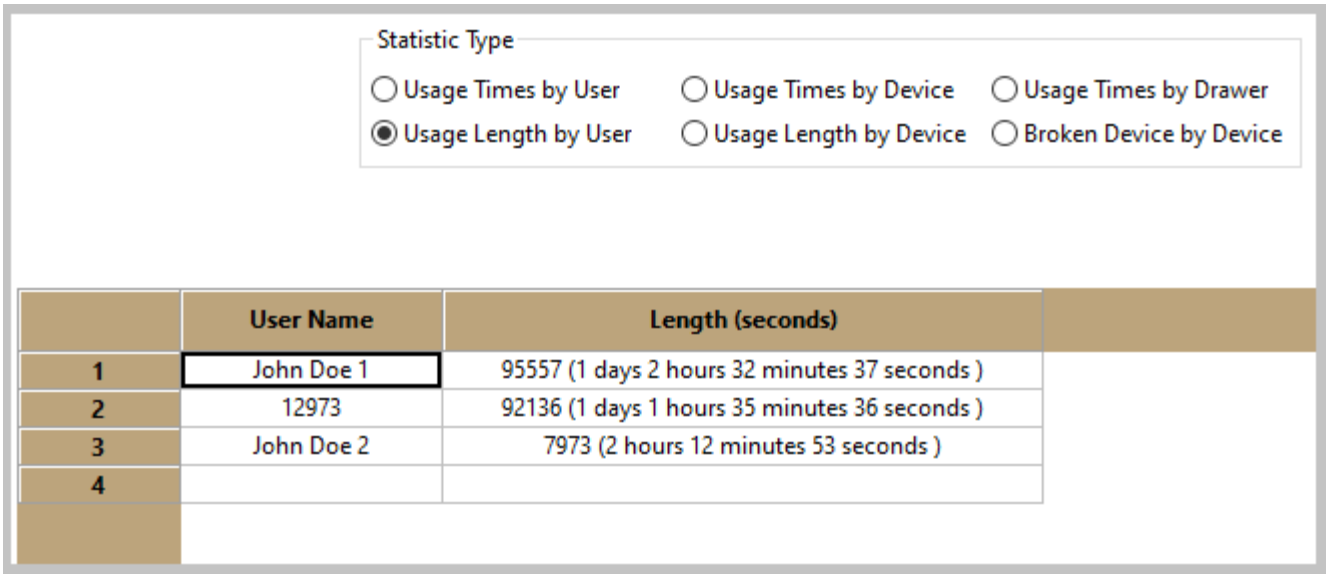
The first column is the drawer number, and the second column is how many times the related drawer has been used.

The graph is as following:


Usage Times by Drawer
Times
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
20
22
23
3
21
2
1
24
5
4
Drawer Number
OK

7.3.5 Usage Length by User

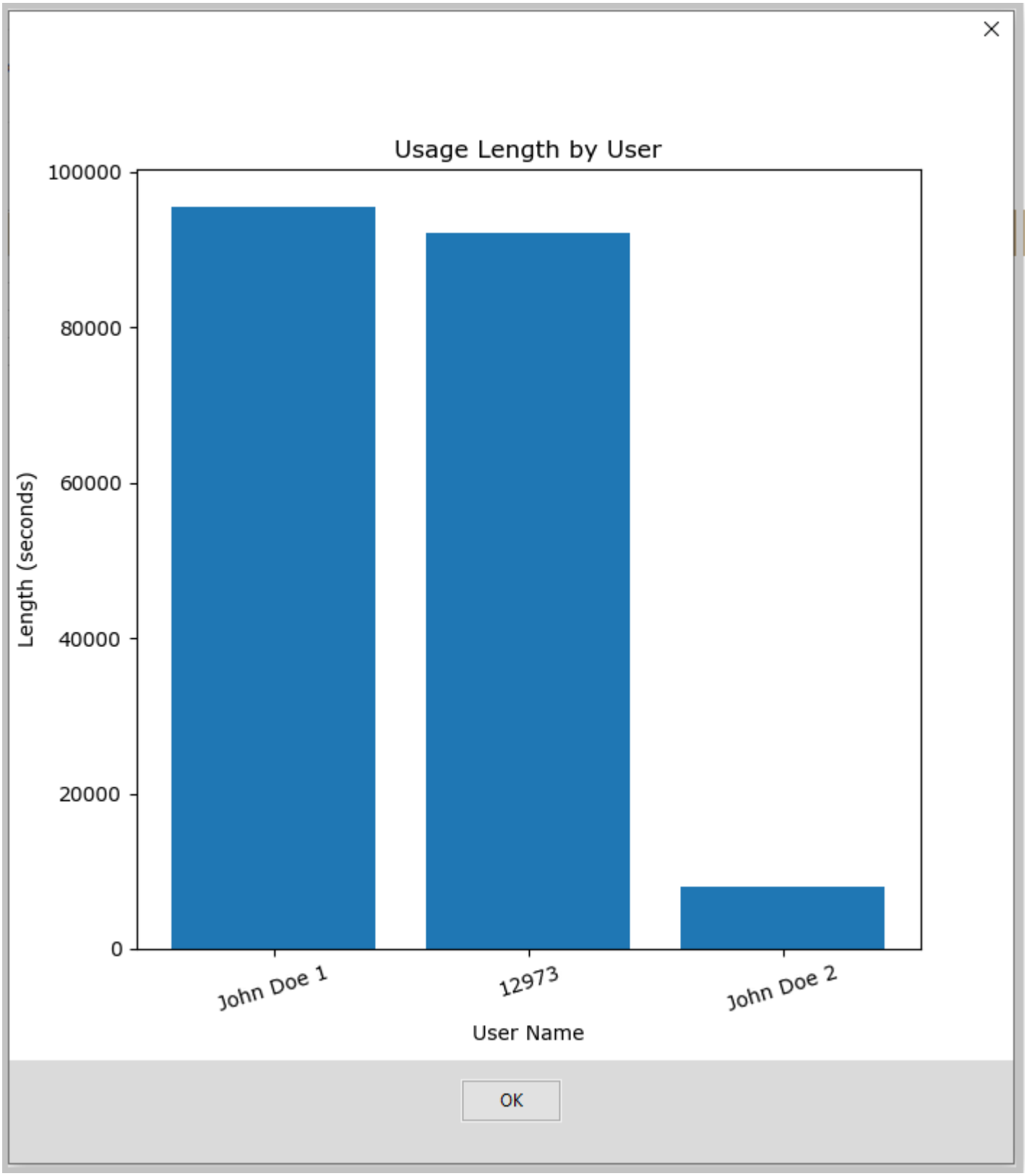
Usage length is the time how long the user has used a device altogether; it includes all the devices the user has used during this period of times. A demonstration screenshot is as following:



	User Name	Length (seconds)
1	John Doe 1	95557 (1 days 2 hours 32 minutes 37 seconds)
2	12973	92136 (1 days 1 hours 35 minutes 36 seconds)
3	John Doe 2	7973 (2 hours 12 minutes 53 seconds)
4		

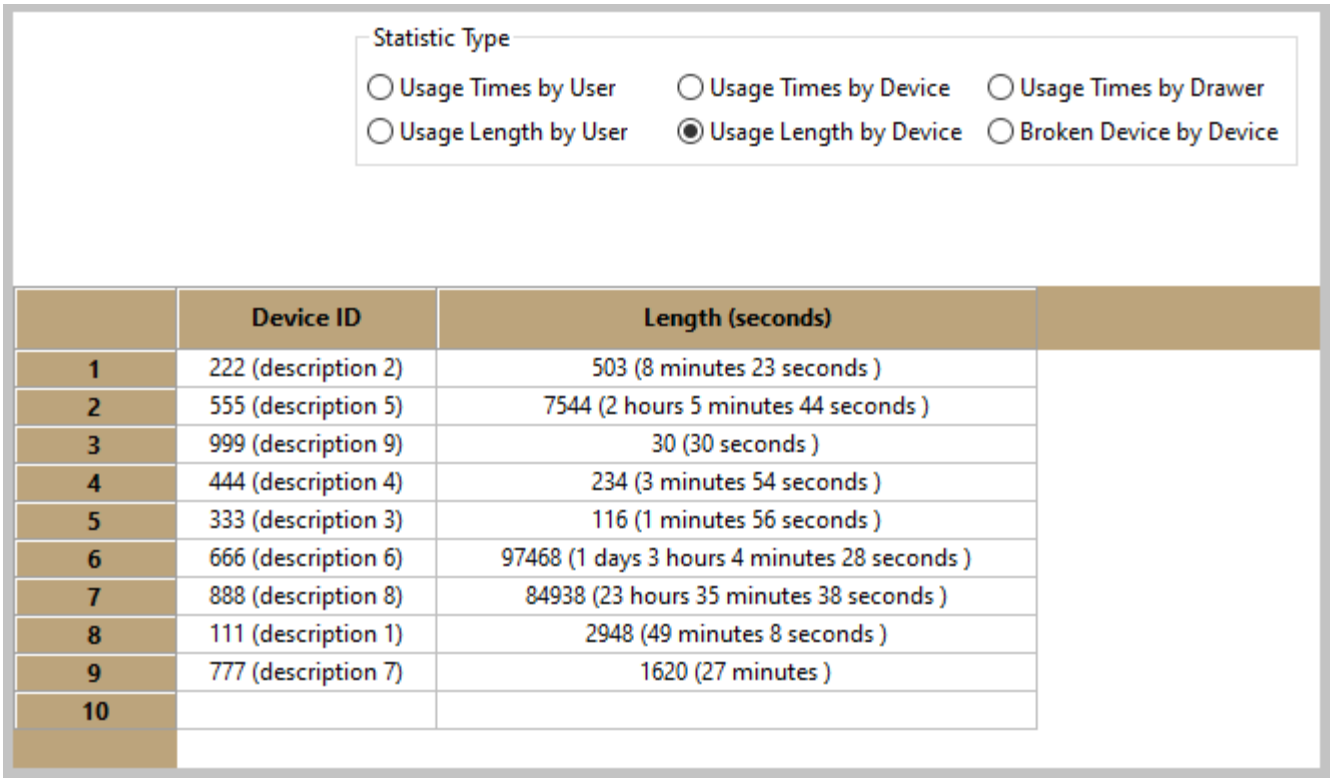
The first column is the user's name, and the second column is how long the user has used all the devices; the unit is in second and it is broken into days, hours, minutes and seconds in the brackets.

The following is the corresponding graph:


Usage Length by User
100000
80000
60000
40000
20000
0
Length (seconds)
John Doe 1
12973
John Doe 2
User Name
OK

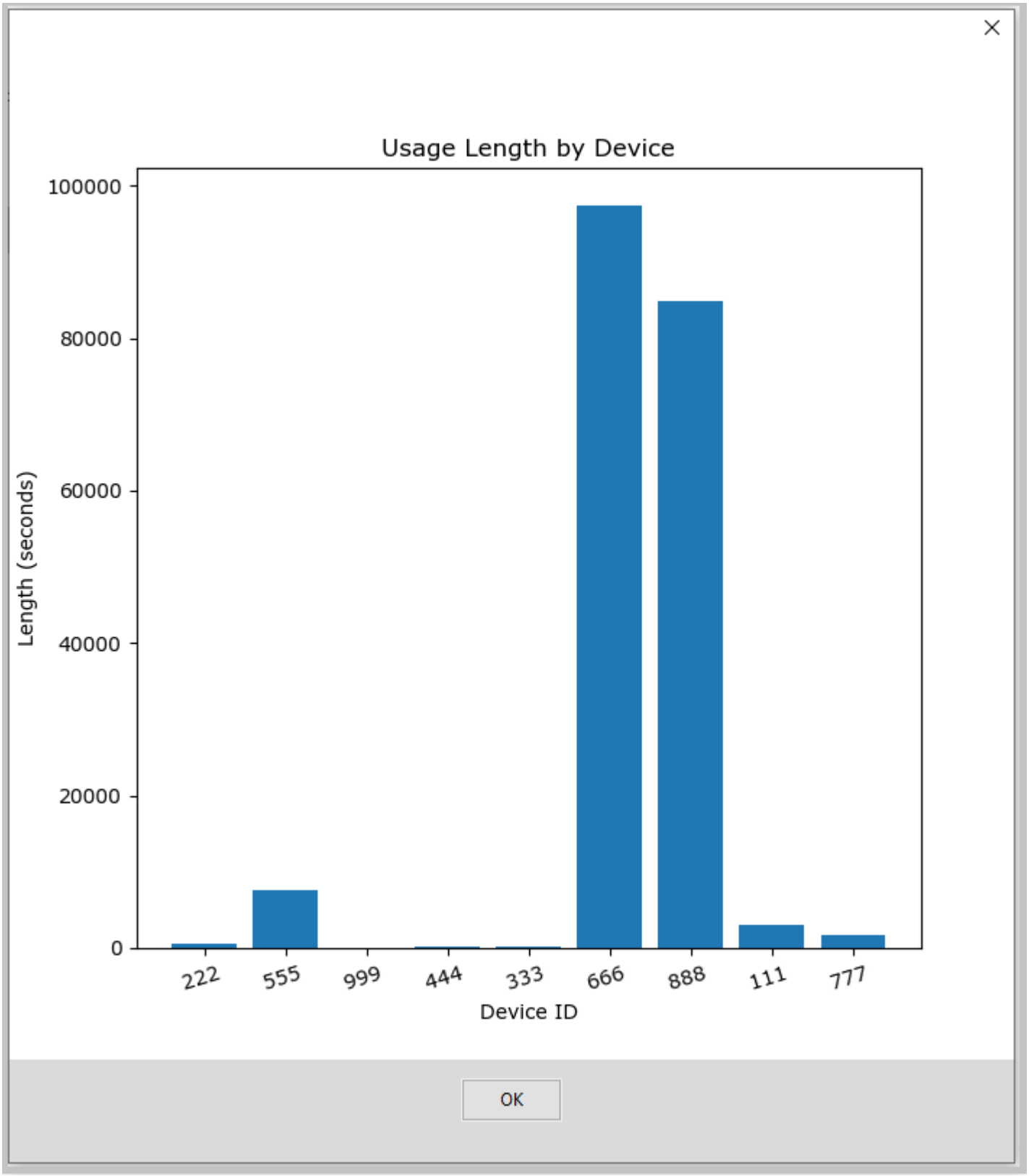
7.3.6 Usage Length by Device

When clicking *Usage Length by Device* in *Statistic Type* section, the table will display the related statistic result. The following is a demonstration screenshot.



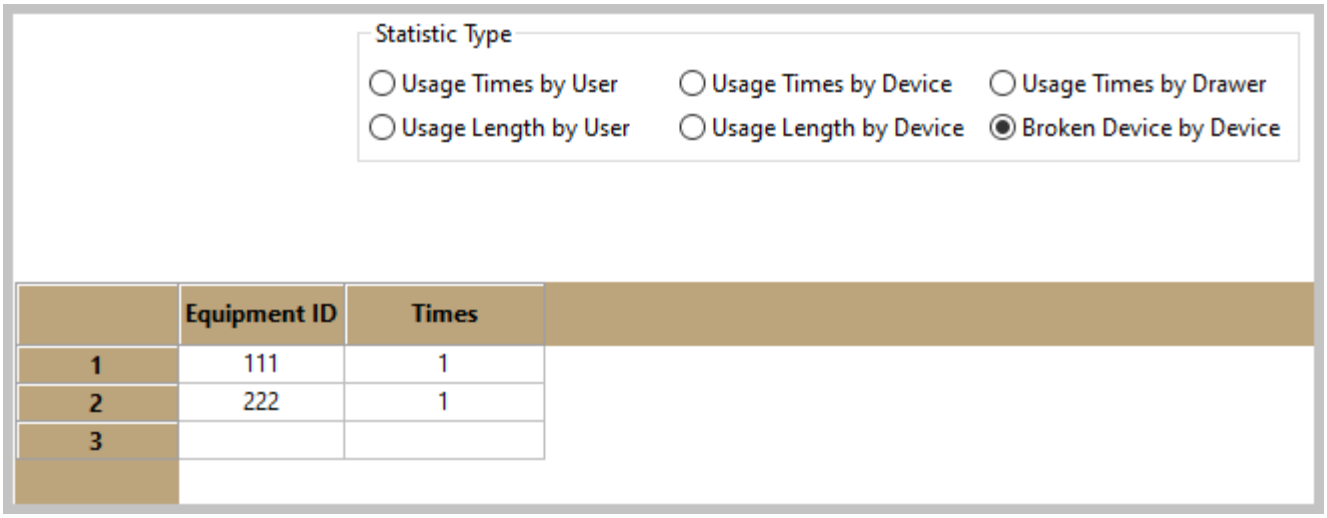
	Device ID	Length (seconds)
1	222 (description 2)	503 (8 minutes 23 seconds)
2	555 (description 5)	7544 (2 hours 5 minutes 44 seconds)
3	999 (description 9)	30 (30 seconds)
4	444 (description 4)	234 (3 minutes 54 seconds)
5	333 (description 3)	116 (1 minutes 56 seconds)
6	666 (description 6)	97468 (1 days 3 hours 4 minutes 28 seconds)
7	888 (description 8)	84938 (23 hours 35 minutes 38 seconds)
8	111 (description 1)	2948 (49 minutes 8 seconds)
9	777 (description 7)	1620 (27 minutes)
10		

The following is a screenshot of the graph.


Usage Length by Device
100000
80000
60000
40000
20000
0
Length (seconds)
222
555
999
444
333
666
888
111
777
Device ID
OK

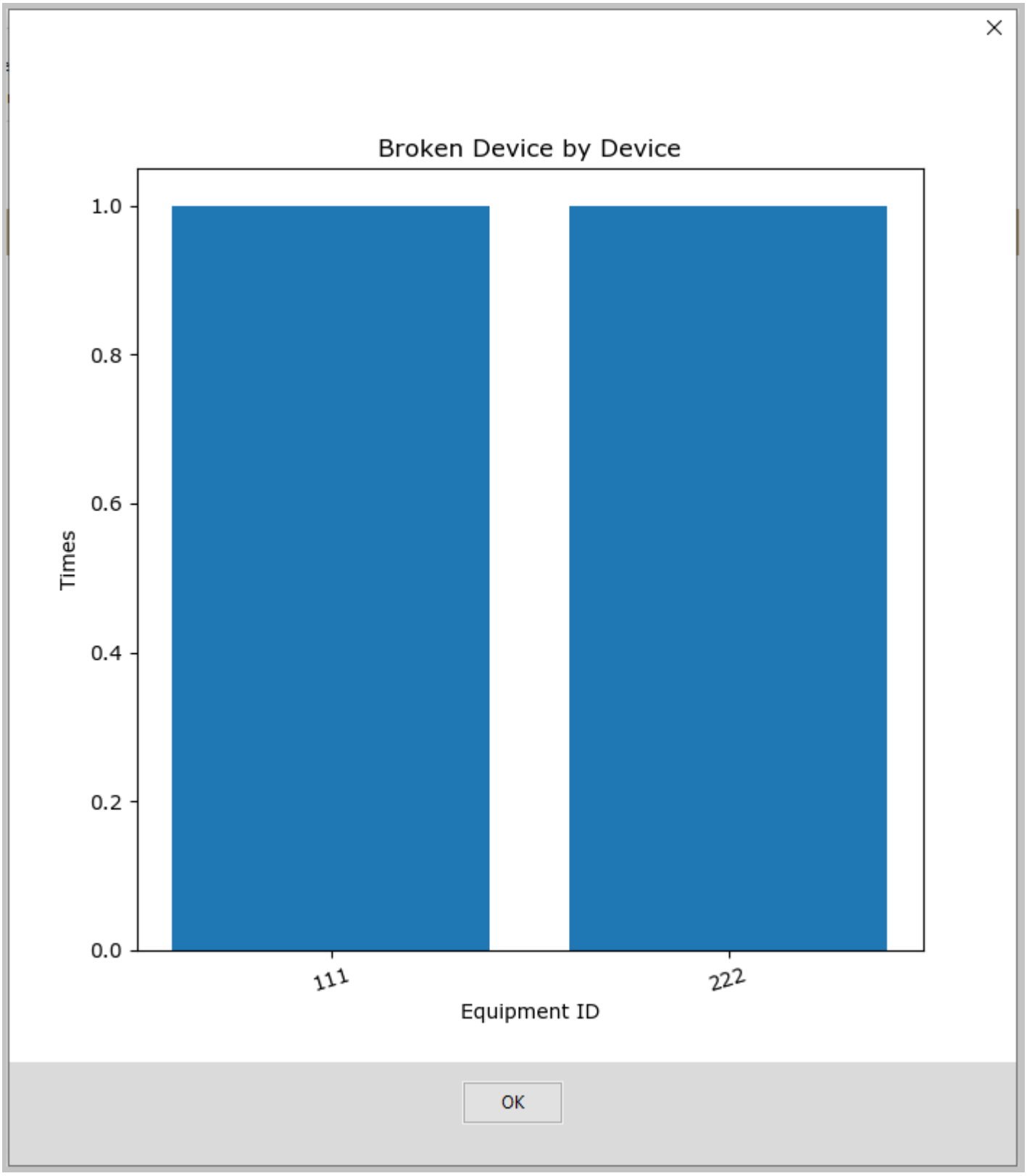
7.3.7 Broken Device by Device

This is the summary of the broken device reported. When clicking *Broken Device by Device* in *Statistic Type* section, the table will display the summary about broken devices.



	Equipment ID	Times
1	111	1
2	222	1
3		

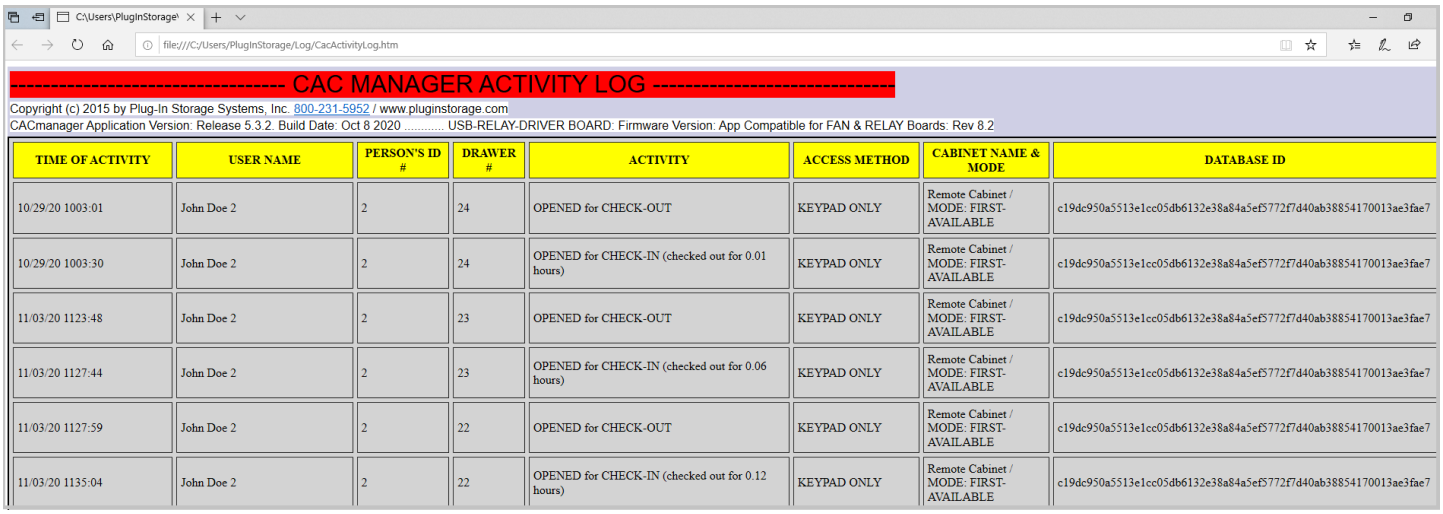
The following is the related graph:


Broken Device by Device
1.0
0.8
0.6
0.4
0.2
0.0
Times
111
222
Equipment ID
OK

7.4 Detailed Activity Log

The administrator might need to verify some specific activities of the cabinet. A detailed running log is available in *.htm* format.

The file locates at *C:\Users\PlugInStorage\Log* with the name *CacActivityLog.htm*; the log has the latest events of the cabinets. The following is a screenshot with an example:



---------- CAC MANAGER ACTIVITY LOG ----------

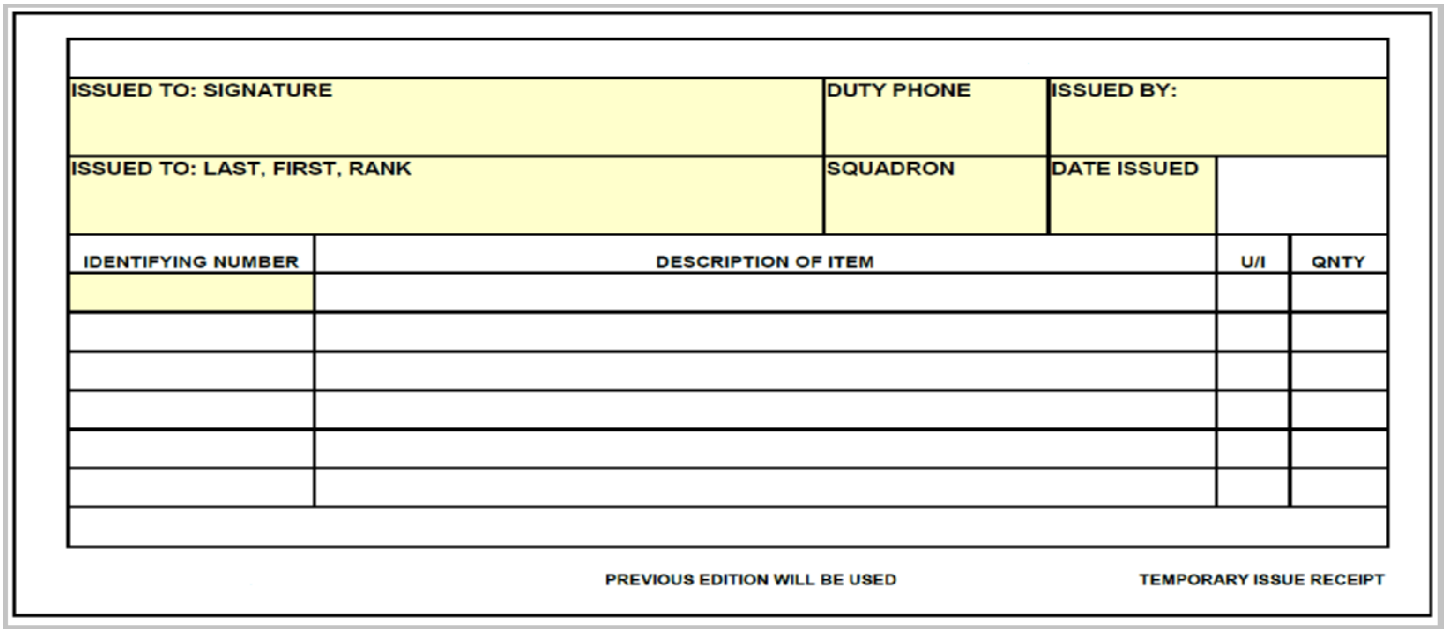
Copyright (c) 2015 by Plug-In Storage Systems, Inc. 800-231-5952 / www.pluginstorage.com

CACmanager Application Version: Release 5.3.2. Build Date: Oct 8 2020 ..... USB-RELAY-DRIVER BOARD: Firmware Version: App Compatible for FAN & RELAY Boards: Rev 8.2

TIME OF ACTIVITY	USER NAME	PERSON'S ID #	DRAWER #	ACTIVITY	ACCESS METHOD	CABINET NAME & MODE	DATABASE ID
10/29/20 1003:01	John Doe 2	2	24	OPENED for CHECK-OUT	KEYPAD ONLY	Remote Cabinet / MODE: FIRST-AVAILABLE	c19dc950a5513e1cc05db6132e38a84a5ef5772f7d40ab38854170013ae3fae7
10/29/20 1003:30	John Doe 2	2	24	OPENED for CHECK-IN (checked out for 0.01 hours)	KEYPAD ONLY	Remote Cabinet / MODE: FIRST-AVAILABLE	c19dc950a5513e1cc05db6132e38a84a5ef5772f7d40ab38854170013ae3fae7
11/03/20 1123:48	John Doe 2	2	23	OPENED for CHECK-OUT	KEYPAD ONLY	Remote Cabinet / MODE: FIRST-AVAILABLE	c19dc950a5513e1cc05db6132e38a84a5ef5772f7d40ab38854170013ae3fae7
11/03/20 1127:44	John Doe 2	2	23	OPENED for CHECK-IN (checked out for 0.06 hours)	KEYPAD ONLY	Remote Cabinet / MODE: FIRST-AVAILABLE	c19dc950a5513e1cc05db6132e38a84a5ef5772f7d40ab38854170013ae3fae7
11/03/20 1127:59	John Doe 2	2	22	OPENED for CHECK-OUT	KEYPAD ONLY	Remote Cabinet / MODE: FIRST-AVAILABLE	c19dc950a5513e1cc05db6132e38a84a5ef5772f7d40ab38854170013ae3fae7
11/03/20 1135:04	John Doe 2	2	22	OPENED for CHECK-IN (checked out for 0.12 hours)	KEYPAD ONLY	Remote Cabinet / MODE: FIRST-AVAILABLE	c19dc950a5513e1cc05db6132e38a84a5ef5772f7d40ab38854170013ae3fae7

7.5 Receipt Generation

When a device is checked out, a receipt can be printed out automatically. The setup of the receipt is located at tab *Receipt Layout* of *CAC-GUI*. The following is the format:



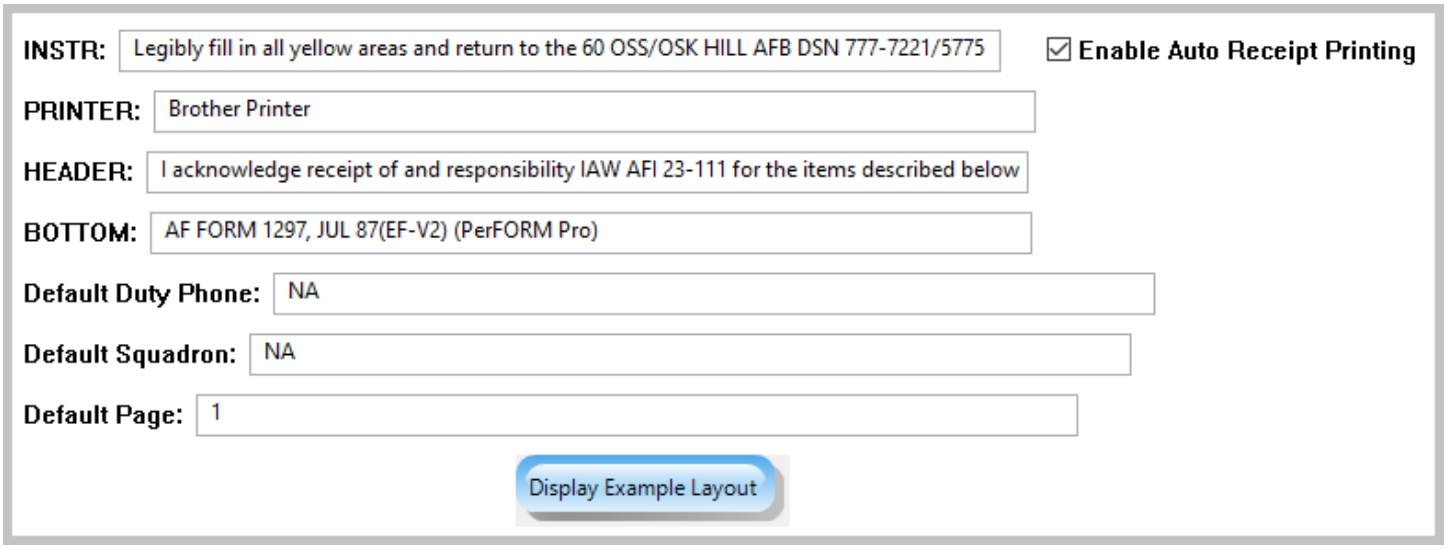
ISSUED TO: SIGNATURE	DUTY PHONE	ISSUED BY:	
ISSUED TO: LAST, FIRST, RANK	SQUADRON	DATE ISSUED	

IDENTIFYING NUMBER	DESCRIPTION OF ITEM	U/I	QNTY

PREVIOUS EDITION WILL BE USED

TEMPORARY ISSUE RECEIPT

The default format of the receipt can be set up with several fields. The following is a screenshot of the fields:



The meaning of the fields is as following:

INSTR: the instruction for the filling of the receipt

PRINTER: the name of the printer to print out the receipt

HEADER: the title of the receipt

BOTTOM: the bottom part of the receipt

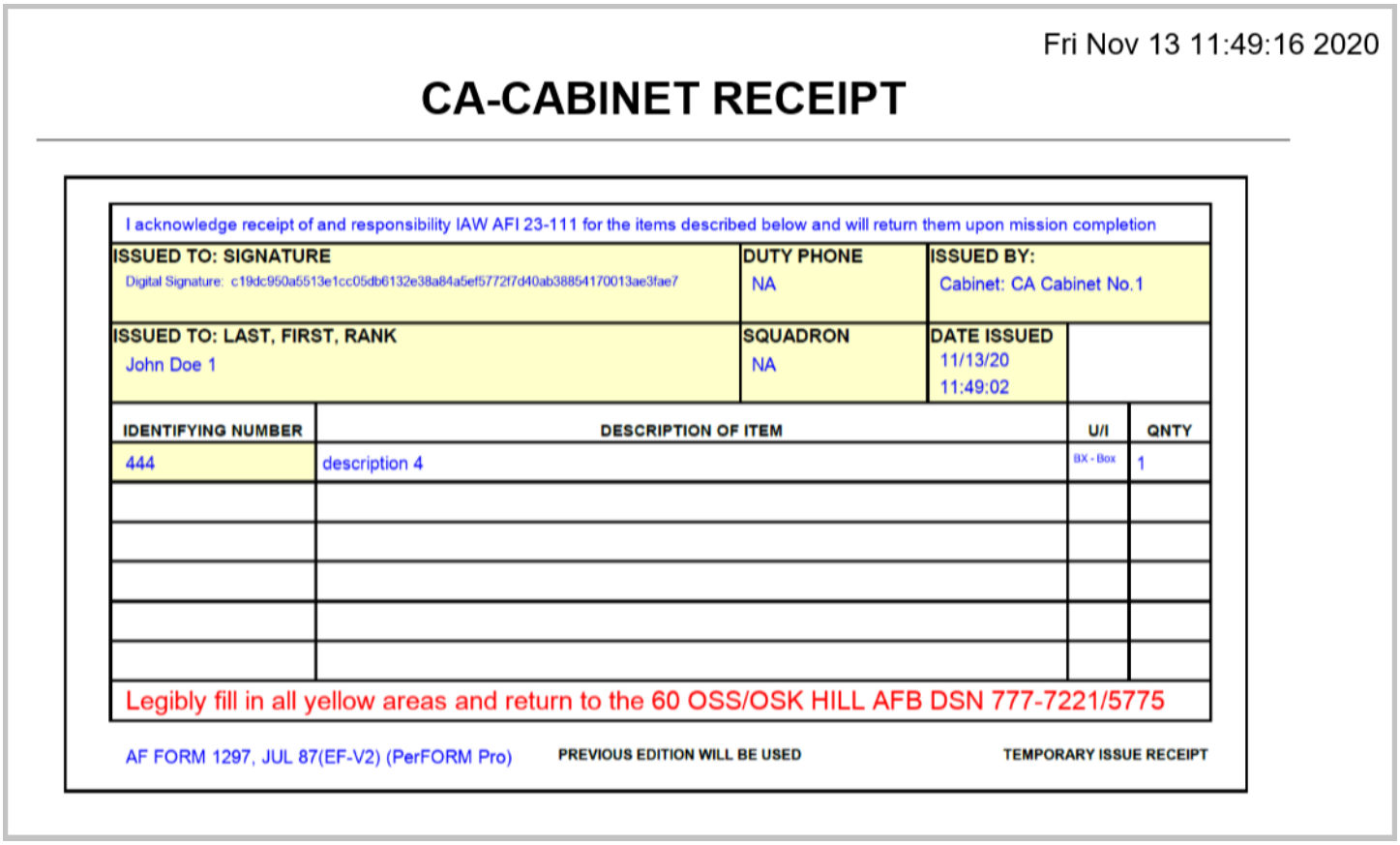
Default Duty Phone: the default value of the phone number for duty

Default Squadron: the default value of the squadron name.

Default Page: the default value of how many copies is printed for the receipt

Enable Auto Receipt Printing: when selected, the receipt will be print out automatically when a device is checked out

An example of the receipt is as following:



Fri Nov 13 11:49:16 2020

CA-CABINET RECEIPT

I acknowledge receipt of and responsibility IAW AFI 23-111 for the items described below and will return them upon mission completion

ISSUED TO: SIGNATURE	DUTY PHONE	ISSUED BY:
Digital Signature: c19dc950a5513e1cc05db6132e38a84a5ef5772f7d40ab38854170013ae3fae7	NA	Cabinet: CA Cabinet No.1

ISSUED TO: LAST, FIRST, RANK	SQUADRON	DATE ISSUED	
John Doe 1	NA	11/13/20 11:49:02	

IDENTIFYING NUMBER	DESCRIPTION OF ITEM	U/I	QNTY
444	description 4	BX - Box	1

Legibly fill in all yellow areas and return to the 60 OSS/OSK HILL AFB DSN 777-7221/5775

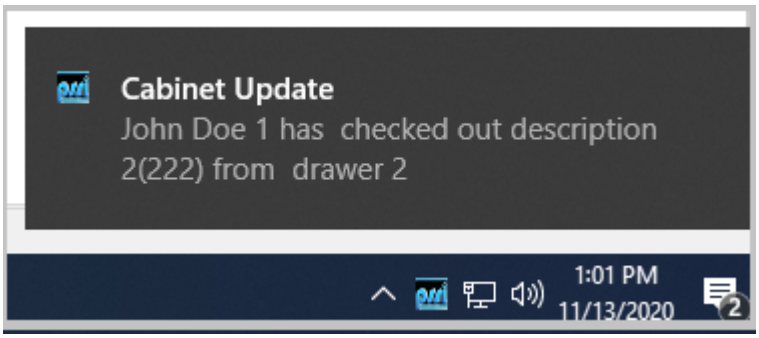
AF FORM 1297, JUL 87(EF-V2) (PerFORM Pro) PREVIOUS EDITION WILL BE USED TEMPORARY ISSUE RECEIPT

7.6 Toast Notification

Toast notification is a real-time window appearing in the screen and fading out after several seconds. It happens when there is a device checked out or checked in. The window appears at the right-down corner of the screen.

The notification includes the person who checkout/check-in the device, the equipment ID and equipment description, and the drawer number.

The following is a screenshot of the example:



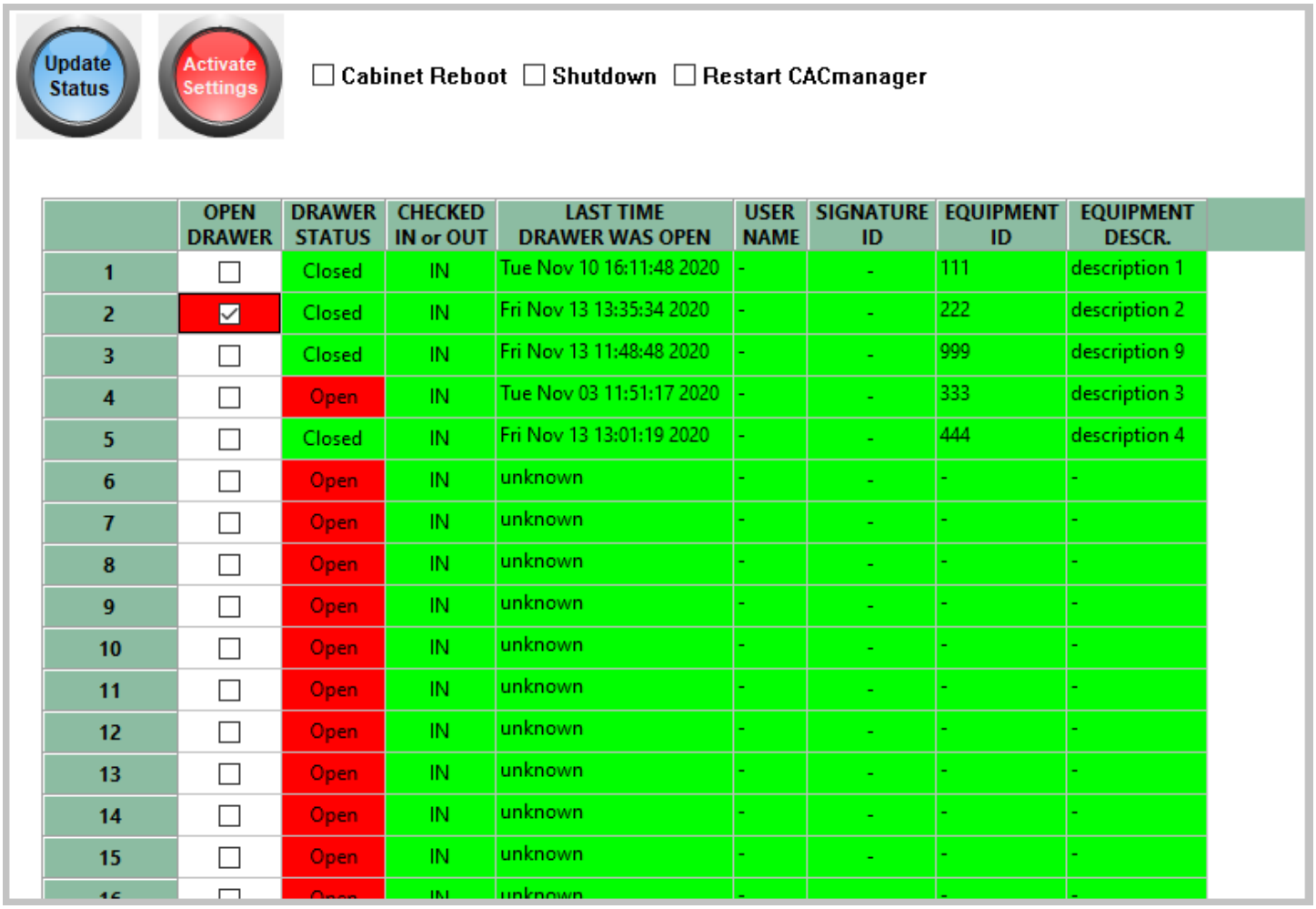
8 REMOTE CONTROL

From *CAC-GUI* to cabinet, some commands can be sent out to control the activity of the cabinet. The entrance of the commands locates at tab *Snapshot/Cabinet Commands* of *CAC-GUI*.

8.1 Open a Drawer

To open a drawer, select the drawer number from the first column of the *Snapshot* table, and press button *Activate Settings* (the red button at upper-left corner), in a couple of seconds the drawer will open, and the drawer status (second column *DRAWER STATUS* of the table) will become red to indicate the drawer is open.

The following is the screenshot of an example:



	OPEN DRAWER	DRAWER STATUS	CHECKED IN or OUT	LAST TIME DRAWER WAS OPEN	USER NAME	SIGNATURE ID	EQUIPMENT ID	EQUIPMENT DESCR.
1	☐	Closed	IN	Tue Nov 10 16:11:48 2020	-	-	111	description 1
2	☑	Closed	IN	Fri Nov 13 13:35:34 2020	-	-	222	description 2
3	☐	Closed	IN	Fri Nov 13 11:48:48 2020	-	-	999	description 9
4	☐	Open	IN	Tue Nov 03 11:51:17 2020	-	-	333	description 3
5	☐	Closed	IN	Fri Nov 13 13:01:19 2020	-	-	444	description 4
6	☐	Open	IN	unknown	-	-	-	-
7	☐	Open	IN	unknown	-	-	-	-
8	☐	Open	IN	unknown	-	-	-	-
9	☐	Open	IN	unknown	-	-	-	-
10	☐	Open	IN	unknown	-	-	-	-
11	☐	Open	IN	unknown	-	-	-	-
12	☐	Open	IN	unknown	-	-	-	-
13	☐	Open	IN	unknown	-	-	-	-
14	☐	Open	IN	unknown	-	-	-	-
15	☐	Open	IN	unknown	-	-	-	-
16	☐	Open	IN	unknown	-	-	-	-

In the above example, drawer 2 is set to be opened.

8.2 Other Actions

From *CAC-GUI*, the administrator can restart the *CACmanager* program, reboot the cabinet or shutdown the cabinet. It can be done by select *Restart CACmanager*, *Cabinet Reboot* or *Shutdown* on the upper side of the screen, and then press *Activate Settings* button (the read button).

The following is the screenshot.

In the above screen, it is setup to restart *CACmanager* program.

9 CABINET CLUSTER AND CABINET NETWORK

For a big team, sometimes one cabinet is not enough to accommodate all the equipment. One solution for this kind of situation is to group the cabinets together by *Cabinet Cluster* or *Cabinet Network*.

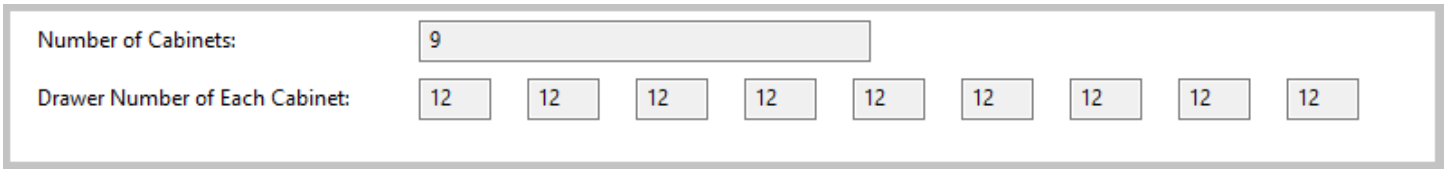
Cabinet Cluster is the structure that several cabinets share one set of control and management system, normally these cabinets are placed side-by-side for the convenience of access. *Cabinet Network* is a structure that several cabinets work independently and at the same time be connected by network to share the information and coordinate the activities.

9.1 Cabinet Cluster

When several cabinets are placed together and share one set of control system, they are forming *a Cabinet Cluster*. The cabinet directly have the access equipment is the *Master Cabinet*, and is normally labelled as *Cabinet A*; and the other cabinets without access equipment are *Slave Cabinets*, normally called Cabinet *B, C, D, E,* etc.

9.1.1 Setup of Cabinet Cluster

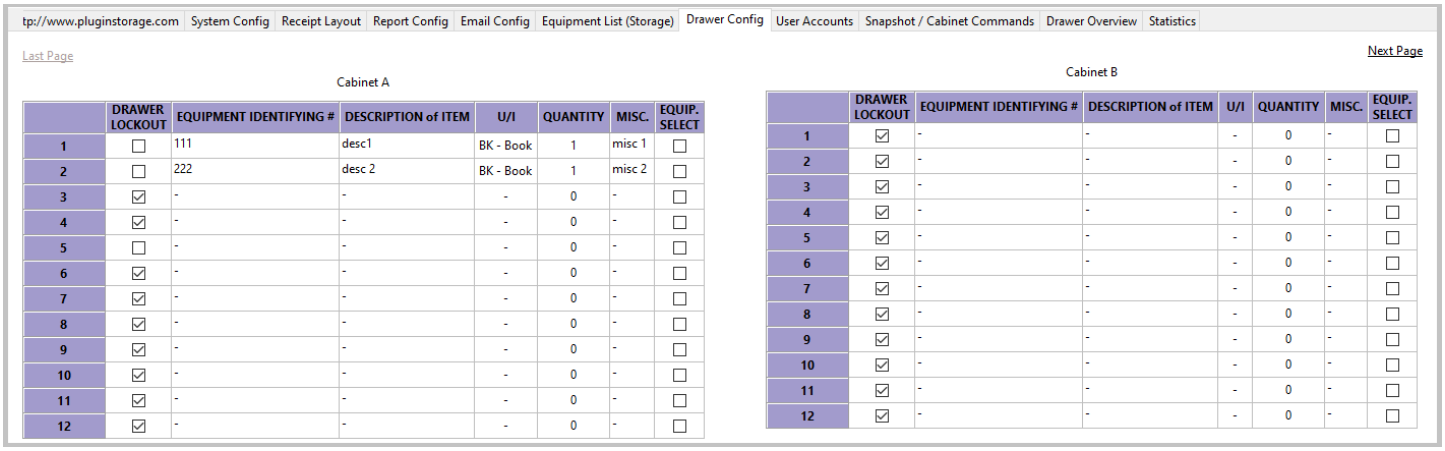
The configuration of cabinet cluster locates at tab *System Config* of *CAC-GUI*. The following is a screenshot.



Number of Cabinet is the total number of the cabinets, the default value is 1. The maximum cabinet number is 10. *Drawer Number of Each Cabinet* is how many drawers each cabinet has, the drawer number can be different for each cabinet.

9.1.2 Drawer Configuration

The process of drawer configuration is to assign the devices to the drawers. For the configuration in cabinet cluster, it also needs to specify the drawer number and the cabinet number. The steps are similar to the setup of single cabinet in *section 6.3.2*. The following is a screenshot.



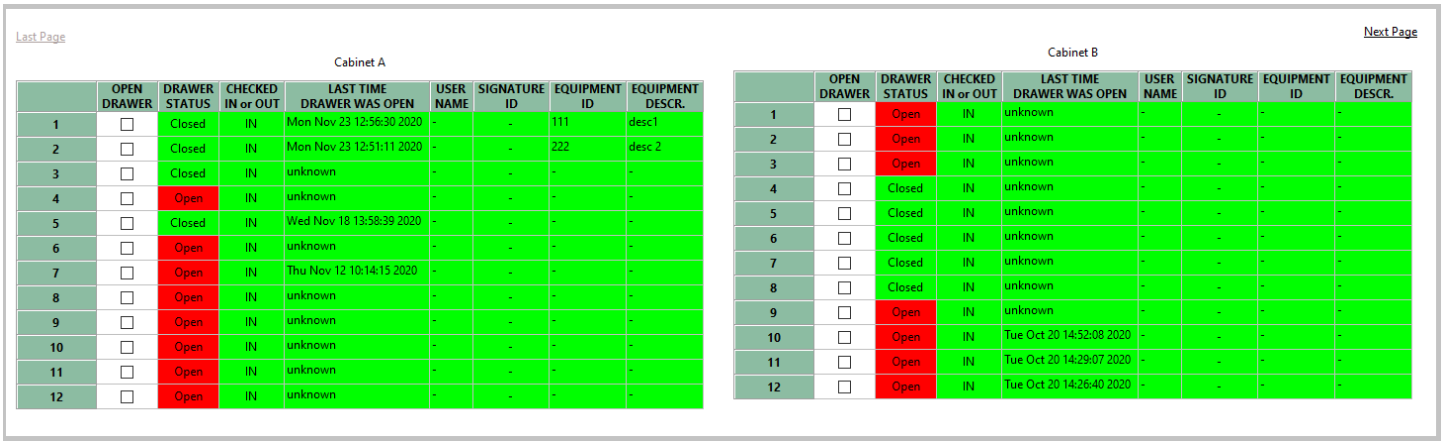
	DRAWER LOCKOUT	EQUIPMENT IDENTIFYING #	DESCRIPTION of ITEM	U/I	QUANTITY	MISC.	EQUIP. SELECT
1	☐	111	desc1	BK - Book	1	misc 1	☐
2	☐	222	desc 2	BK - Book	1	misc 2	☐
3	☑	-	-	-	0	-	☐
4	☑	-	-	-	0	-	☐
5	☐	-	-	-	0	-	☐
6	☑	-	-	-	0	-	☐
7	☑	-	-	-	0	-	☐
8	☑	-	-	-	0	-	☐
9	☑	-	-	-	0	-	☐
10	☑	-	-	-	0	-	☐
11	☑	-	-	-	0	-	☐
12	☑	-	-	-	0	-	☐

	DRAWER LOCKOUT	EQUIPMENT IDENTIFYING #	DESCRIPTION of ITEM	U/I	QUANTITY	MISC.	EQUIP. SELECT
1	☑	-	-	-	0	-	☐
2	☑	-	-	-	0	-	☐
3	☑	-	-	-	0	-	☐
4	☑	-	-	-	0	-	☐
5	☑	-	-	-	0	-	☐
6	☑	-	-	-	0	-	☐
7	☑	-	-	-	0	-	☐
8	☑	-	-	-	0	-	☐
9	☑	-	-	-	0	-	☐
10	☑	-	-	-	0	-	☐
11	☑	-	-	-	0	-	☐
12	☑	-	-	-	0	-	☐

Each page has two cabinets; the link *Last Page* and *Next Page* are used to turn the page.

9.1.3 Snapshot

The *Snapshot* tab is similar to the one with single cabinet, the difference is that it needs to show the status of several cabinets. The tab could have multiple pages. Each page has two cabinets, and the link *Last Page* and *Next Page* are used to turn pages. The following is a screenshot.



	OPEN DRAWER	DRAWER STATUS	CHECKED IN or OUT	LAST TIME DRAWER WAS OPEN	USER NAME	SIGNATURE ID	EQUIPMENT ID	EQUIPMENT DESCR.
1	☐	Closed	IN	Mon Nov 23 12:56:30 2020	-	-	111	desc1
2	☐	Closed	IN	Mon Nov 23 12:51:11 2020	-	-	222	desc 2
3	☐	Closed	IN	unknown	-	-	-	-
4	☐	Open	IN	unknown	-	-	-	-
5	☐	Closed	IN	Wed Nov 18 13:58:39 2020	-	-	-	-
6	☐	Open	IN	unknown	-	-	-	-
7	☐	Open	IN	Thu Nov 12 10:14:15 2020	-	-	-	-
8	☐	Open	IN	unknown	-	-	-	-
9	☐	Open	IN	unknown	-	-	-	-
10	☐	Open	IN	unknown	-	-	-	-
11	☐	Open	IN	unknown	-	-	-	-
12	☐	Open	IN	unknown	-	-	-	-

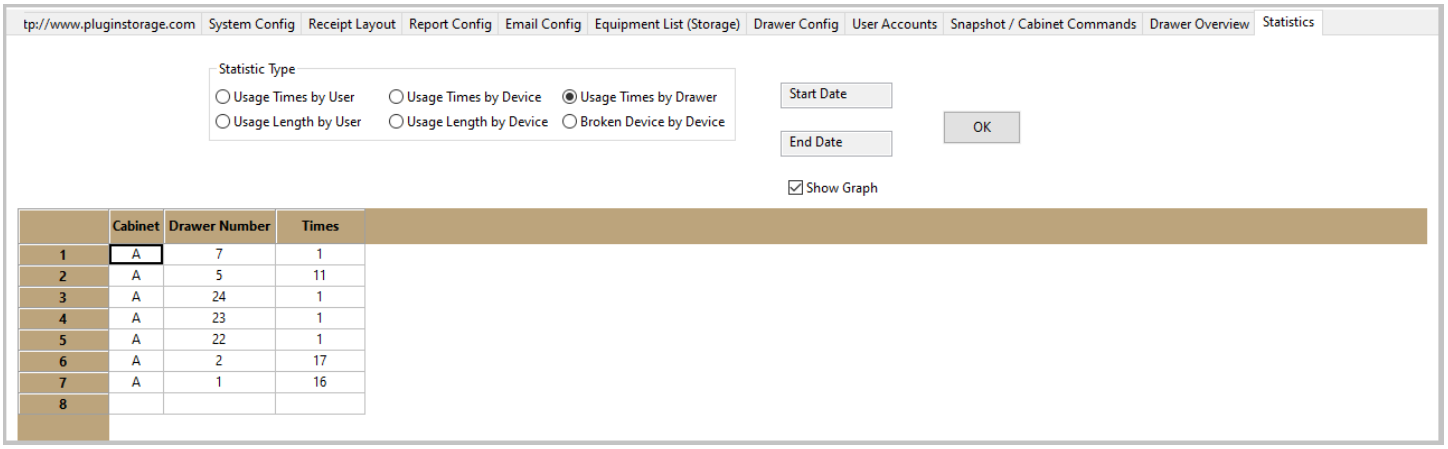
	OPEN DRAWER	DRAWER STATUS	CHECKED IN or OUT	LAST TIME DRAWER WAS OPEN	USER NAME	SIGNATURE ID	EQUIPMENT ID	EQUIPMENT DESCR.
1	☐	Open	IN	unknown	-	-	-	-
2	☐	Open	IN	unknown	-	-	-	-
3	☐	Open	IN	unknown	-	-	-	-
4	☐	Closed	IN	unknown	-	-	-	-
5	☐	Closed	IN	unknown	-	-	-	-
6	☐	Closed	IN	unknown	-	-	-	-
7	☐	Closed	IN	unknown	-	-	-	-
8	☐	Closed	IN	unknown	-	-	-	-
9	☐	Open	IN	unknown	-	-	-	-
10	☐	Open	IN	Tue Oct 20 14:52:08 2020	-	-	-	-
11	☐	Open	IN	Tue Oct 20 14:29:07 2020	-	-	-	-
12	☐	Open	IN	Tue Oct 20 14:26:40 2020	-	-	-	-

9.1.4 Drawer Overview

Tab *Drawer Overview* show the live status of the cabinet; for a cabinet cluster, it displays the status of multiple cabinets. The following is an example.

9.1.5 Statistics

Basically, most statistics functions are the same as the ones with single cabinet, one except is the module *Usage Times by Drawer*. In module *Usage Times by Drawer* it has an extra column *Cabinet* to specify the cabinet. The following is an example.

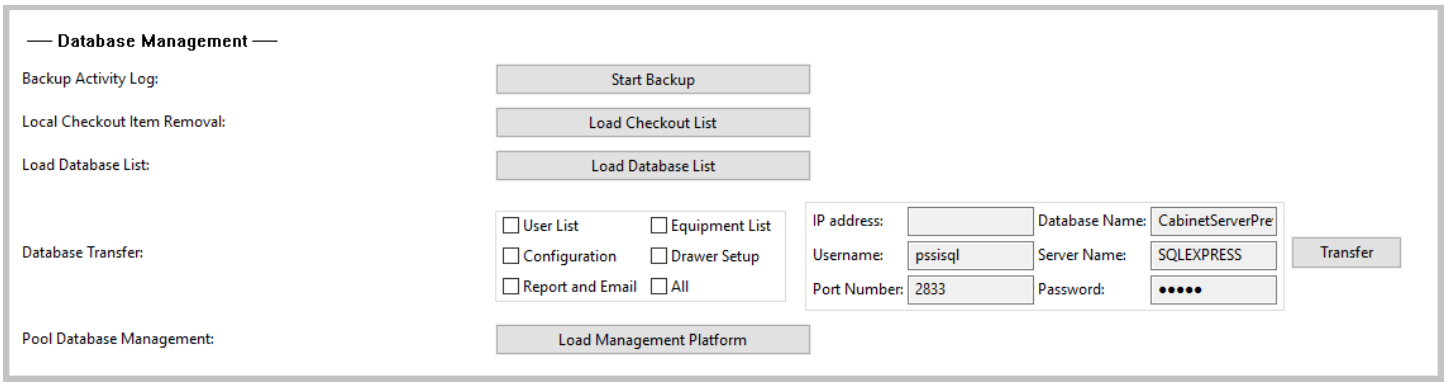


9.2 Cabinet Network and Database Management

Several cabinets can connect together to form a network and share the information of the equipment and the users. Each cabinet has its own database and also communicate with the Pool Database at the same time. The Pool Database or Master Database coordinates all the individual databases; the Pool Database can be placed in a computer of one cabinet or can be configured as Cloud-based server on internet.

9.2.1 Overall of Cabinet Network

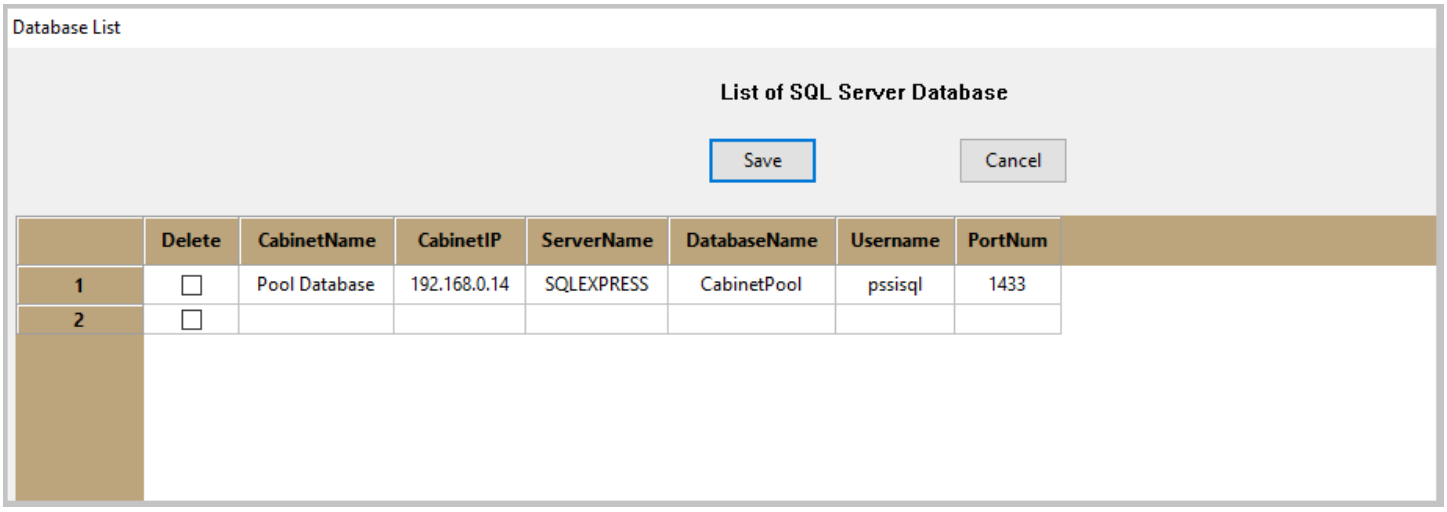
The setup of Cabinet Network locates at *System Config* tab of *CAC-GUI*. The following is the screenshot of the setup.



This section includes Backup Activity Log, Local Checkout Item Removal, Load Database List, Database Transfer and Pool Database Management. The major part is the last one, Pool Database Management. The following sections will give more details to each part.

9.2.2 Load Database List

This module is about the information of the login parameters for the cabinets in the network. As the cabinet needs to communicate with the pool database to sync with other cabinets, the pool database is the most important one. Press *Load Database List* button, a window will pop up with all the information of the databases on the network. The following is a screenshot.



In the table above, column *CabinetName* is normally a meaningful name to call the database, *CabinetIP* is the IP address of the computer where the database locates, *ServerName* is usually *SQLEXPRESS* by default, *DatabaseName* is the real name of the database in *SQL Server*.

When selecting the checkbox of *Delete* column and pressing *Save* button, the record will be removed. Typing in the information on the last line of the table, and a new record is added.

9.2.3 Backup Activity Log

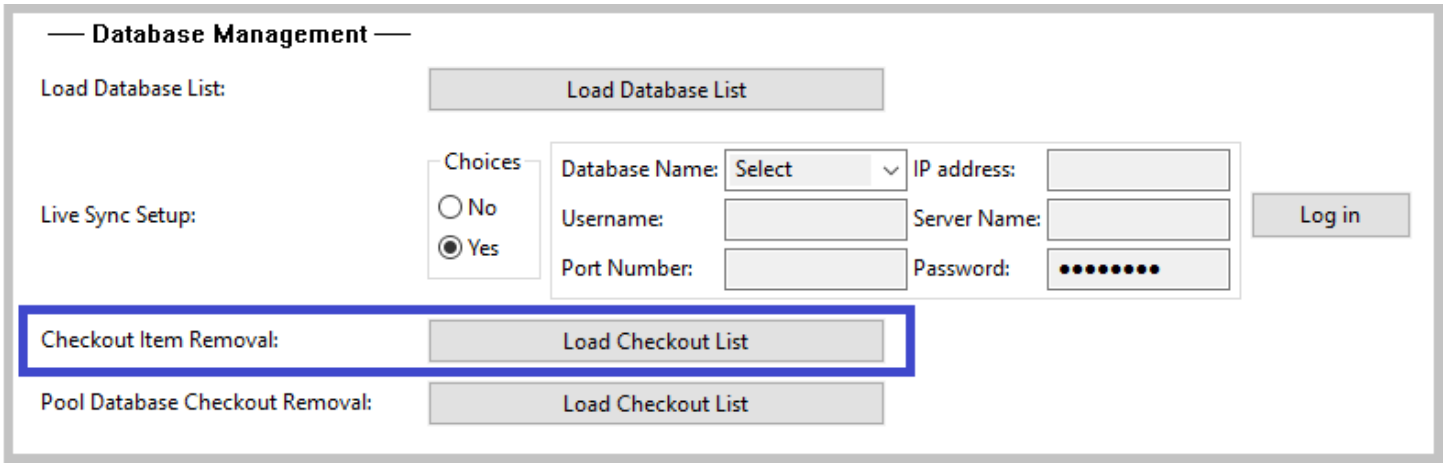
The activity log records all the activities in the cabinet. After several months of usage, the table could become very big. Therefore, the log table needs to be maintained after a period of time in order to keep the performance of the cabinet.

After pressing "Start Backup" button, there will be a window popped up to confirm the action: "This will copy all the activity log to backup table 'CacActivityLogArchive', are you sure to do the backup?", press the "Yes" button and all the log data will be copied the backup table.

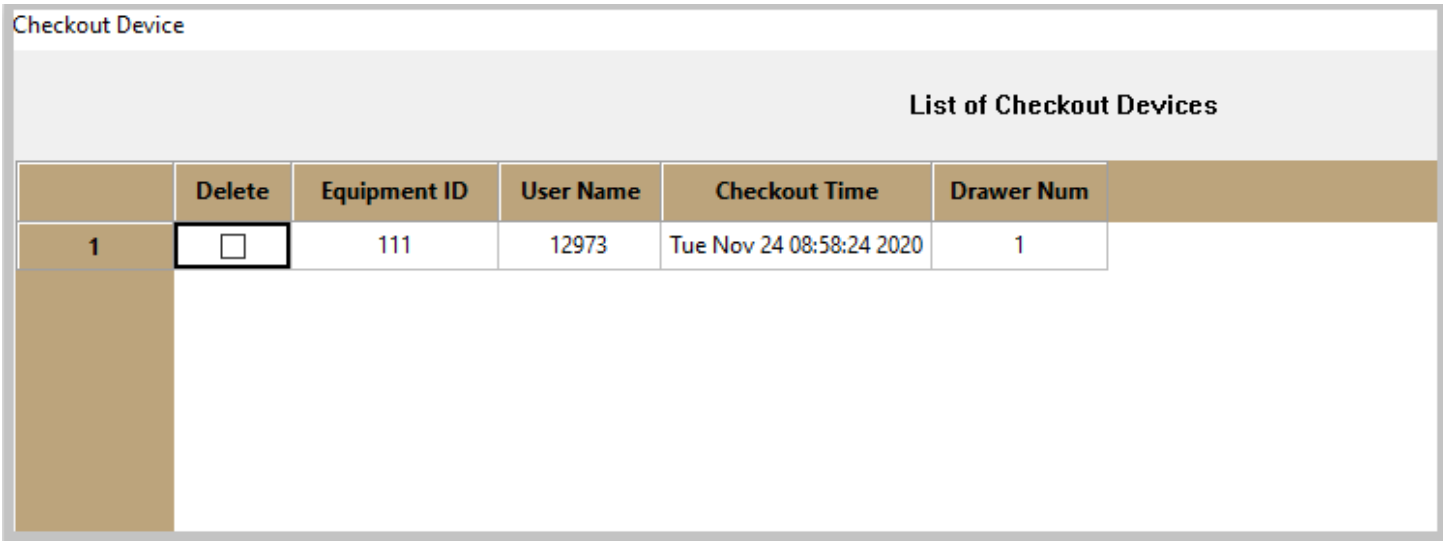
9.2.4 Checkout Item Removal

This function is for maintenance purpose. For example, when a device is checked out by mistake, and it needs to be corrected manually. In these kinds of situation, the checkout needs to be removed manually.

When click *Load Checkout List* button on the line with "*Checkout Item Removal*", a window will pop up with all the items checked out in the local cabinet. The following is a screenshot.

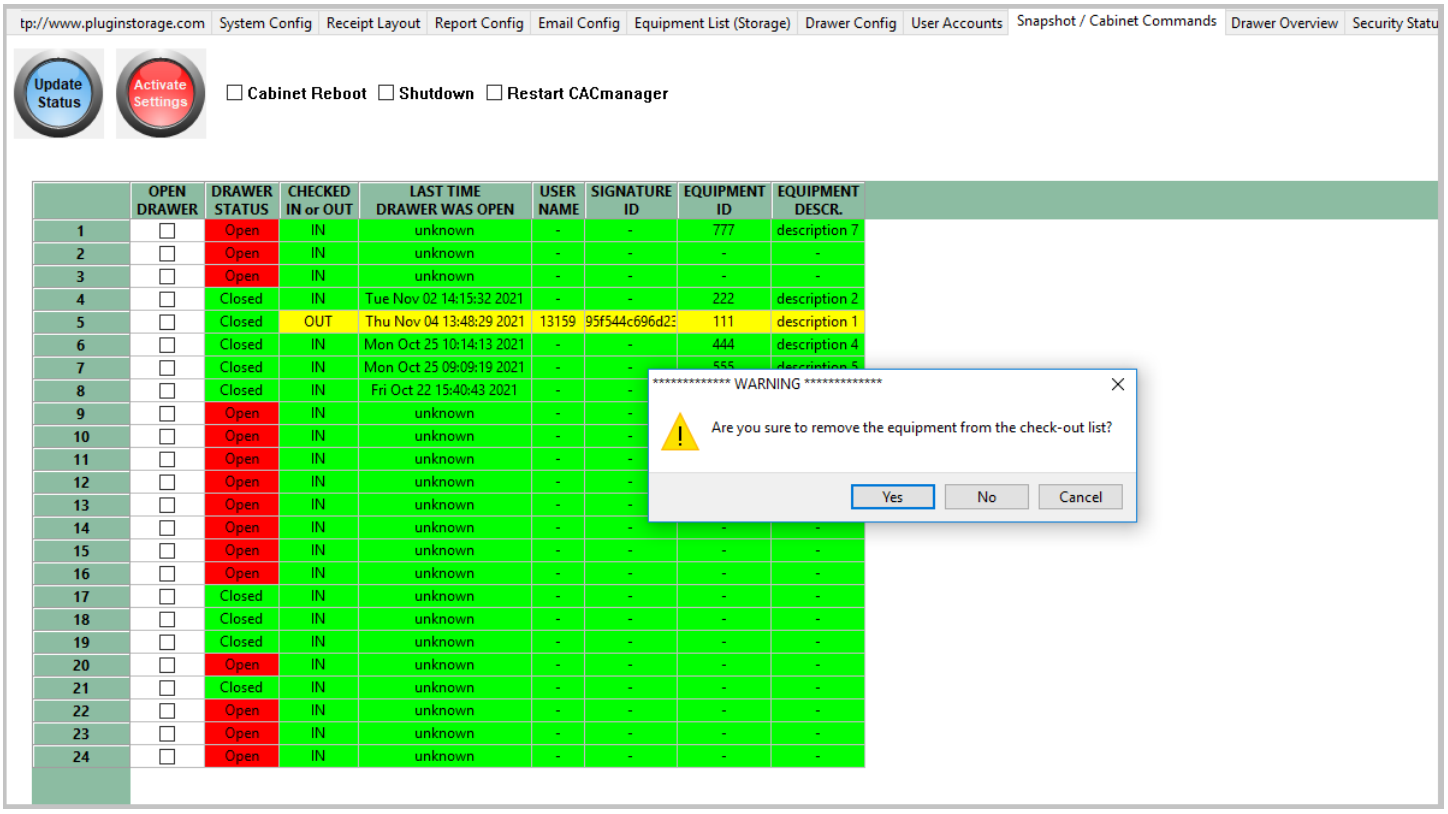


The following is the window with local checkout list:



Select the check box of *Delete* column, and a window will pop up to confirm the removal "*Are you sure you wish to remove this item?*", press *Yes* button to delete the item, or press *No* button to cancel and exit.

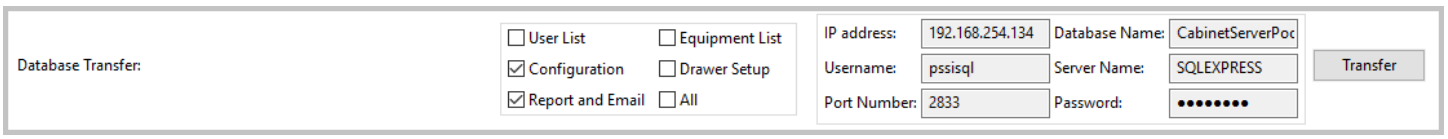
An alternative way to remove the checkout item is to use Snapshot tab. The following is a screenshot.



Right click the line of the checked-out item, a window will pop up to confirm the removing action. Click Yes, and the device will be removed from the checkout list.

9.2.5 Database Transfer

In the initial setup, the administrator needs to input the parameters, loading the user and equipment information and so on. The administrator can probably transfer these kinds of information from another cabinet that already running to the local network, and then do some modifications to the information. This method could make the work easier. The following screenshot shows the interface:



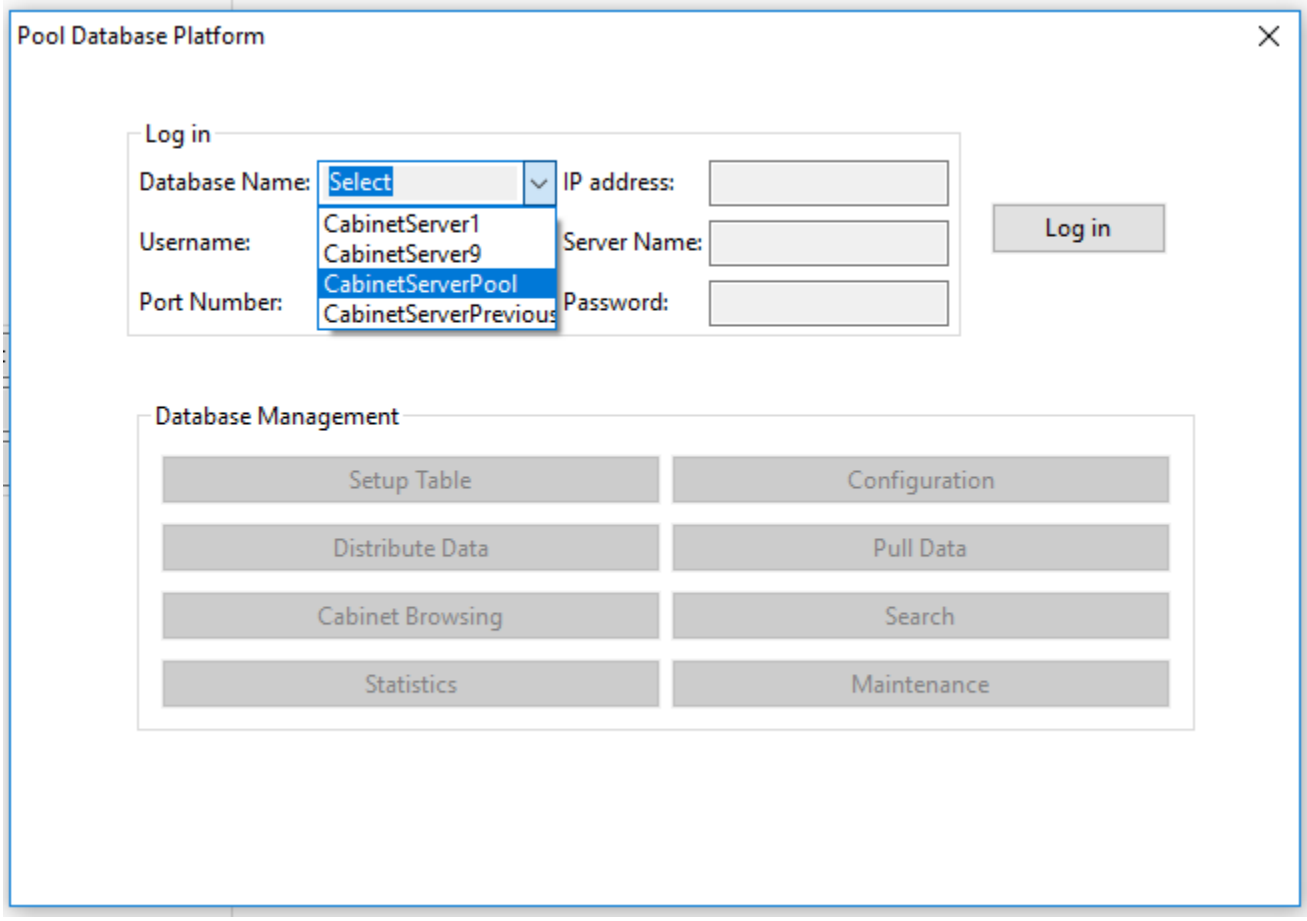
This setup includes the table list and the login information for the target database. The table list includes the several tables that typically used to store the cabinet information, select the one(s) that needs to be transferred. The log in information is already partially filled, the user needs modify the information and type IP address and password.

After pressing button "Transfer", there will be a progress bar to indicating the transfer process, when it is done, the window of progress bar will close, and the content of the table in the target database will appear. Close the window, and the transfer of next table will start; if it is the last table for transfer, the window will close with the transfer is done.

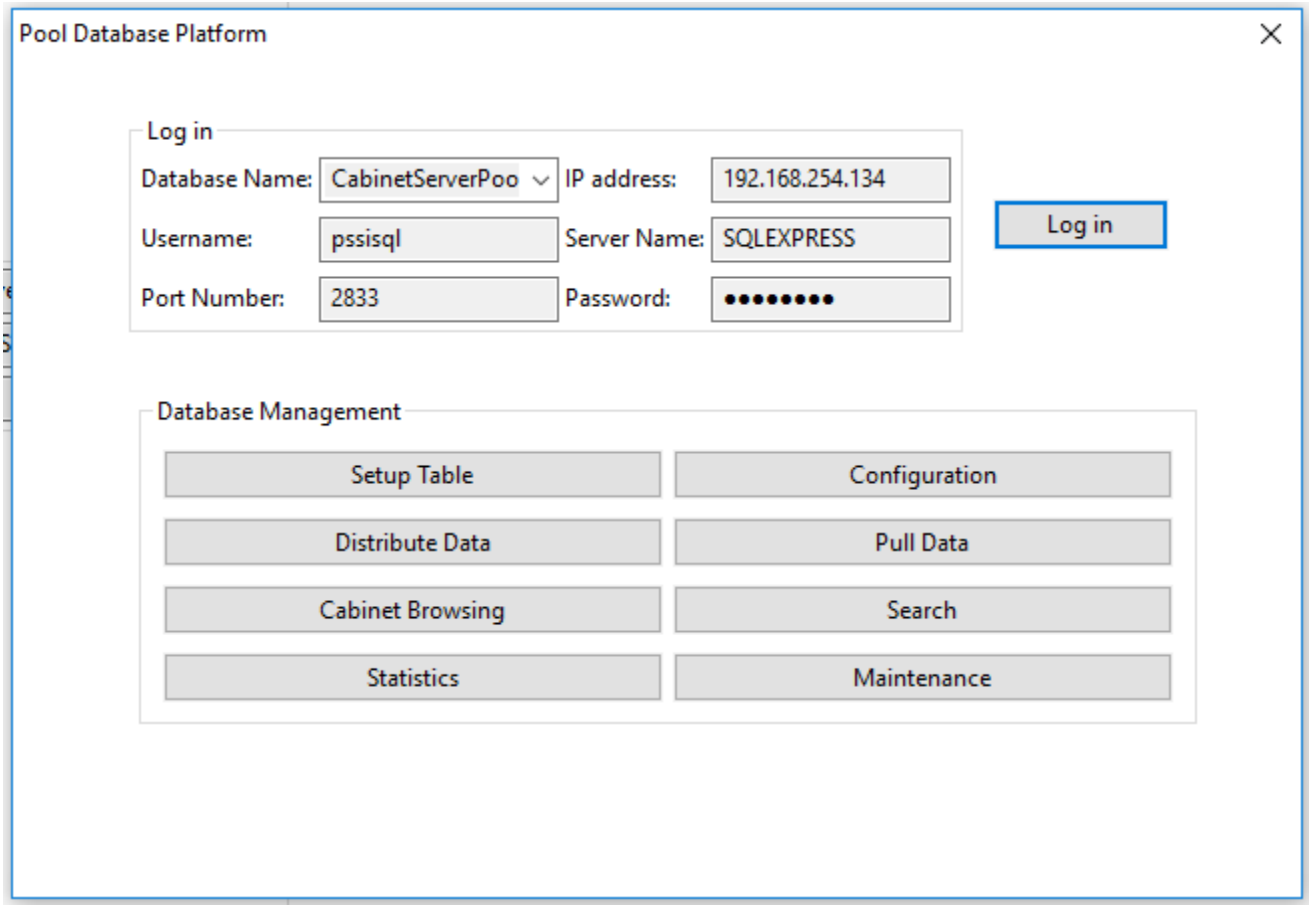
9.2.6 Pool Database Management

A better way to organize the cabinets in the same network is to set up a pool database. The pool database includes the tables that contain the basic cabinet information. They are the user information, device information, system configuration, report setup information, email setup information and so on. The administrator can distribute and collect the information with the individual cabinet, and the cabinet can also sync with the pool database in real time.

Click "Load Management Platform" button, and the platform window will pop up as following:



Choose the pool database from the list of Database Name, other information will be filled, type in the password, and press "Log in" button, the matrix of management button will become enabled.

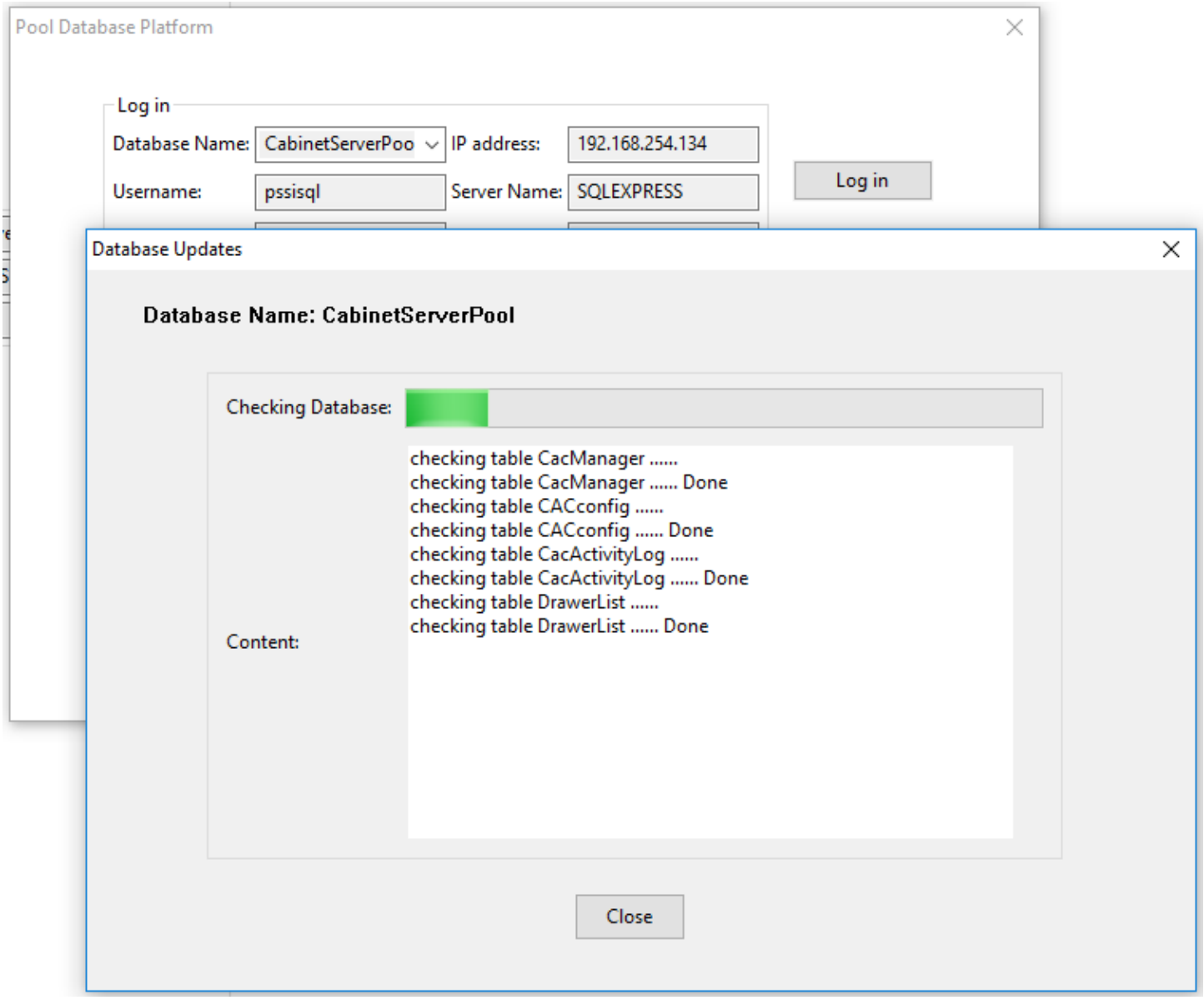


The pool database platform includes eight functions. The following sections are the detailed introduction for each function.

9.2.6.1 Setup Table

This is the creation of the tables in pool database; and if the tables have been created, this function will update them into the latest structure.

After pressing "Setup Table" button, a window pops up with information "This will update the database to the latest, do you want to do the updating?", press "Yes" button, a window will pop up to display the progress.

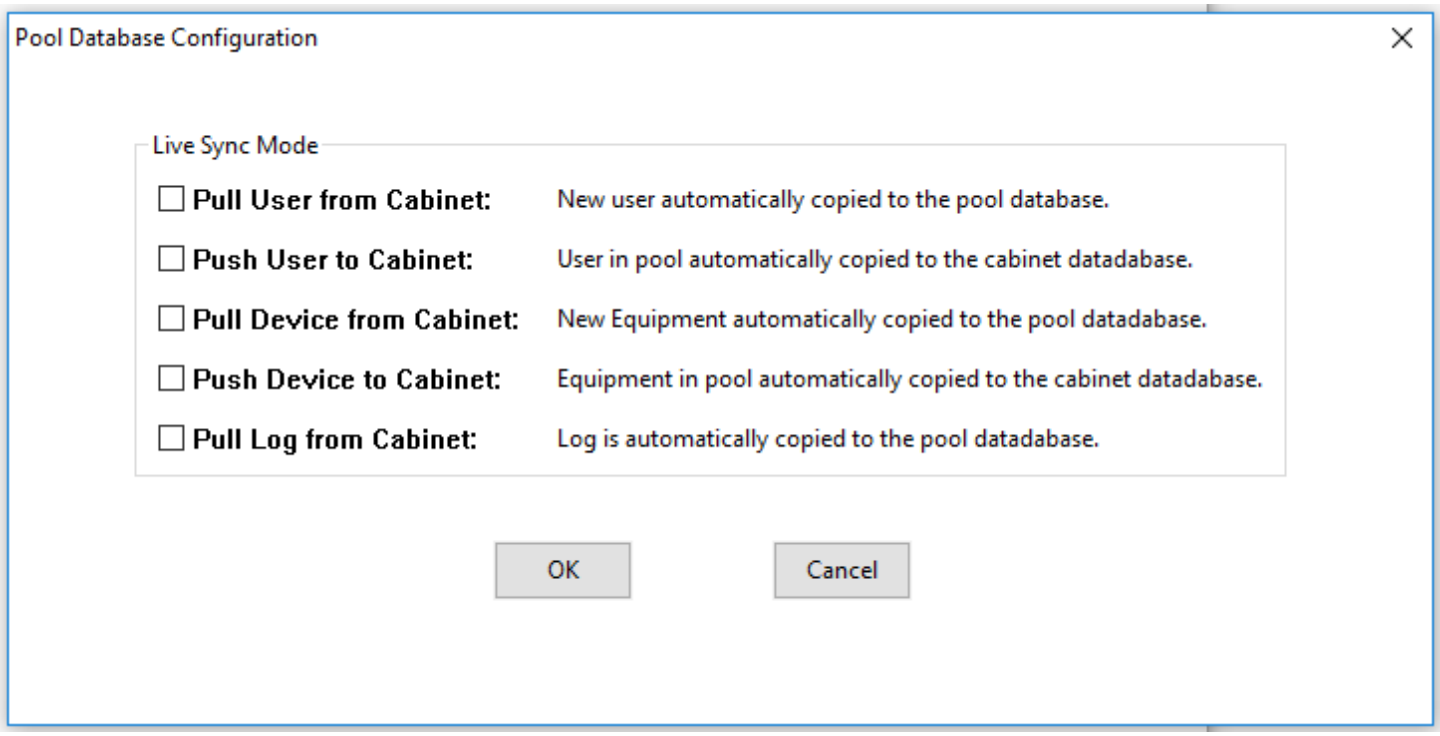


After the updating or creation process is done, the window will display the changes have been done. And the tables in the database are ready.

9.2.6.2 Configuration of Live Sync

The cabinets and the pool database can sync the data in real time. This section is the configuration of information exchange for different items when the cabinet is in live sync state with the pool database.

Press "Configuration" button, and the following window will appear.

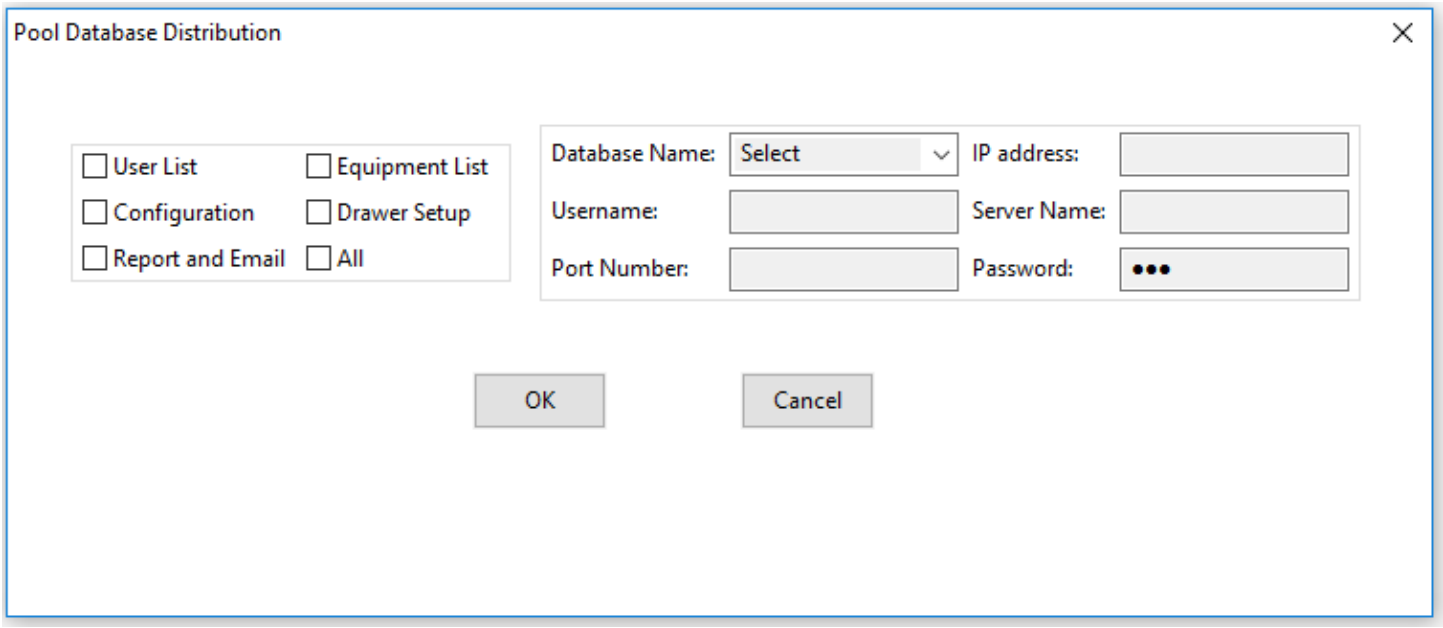


The choice for the sync includes Pull User from Cabinet, Push User to Cabinet, Pull Device from Cabinet, Push Device to Cabinet, and Pull Log from Cabinet. The detailed explanation is shown in the screenshot above.

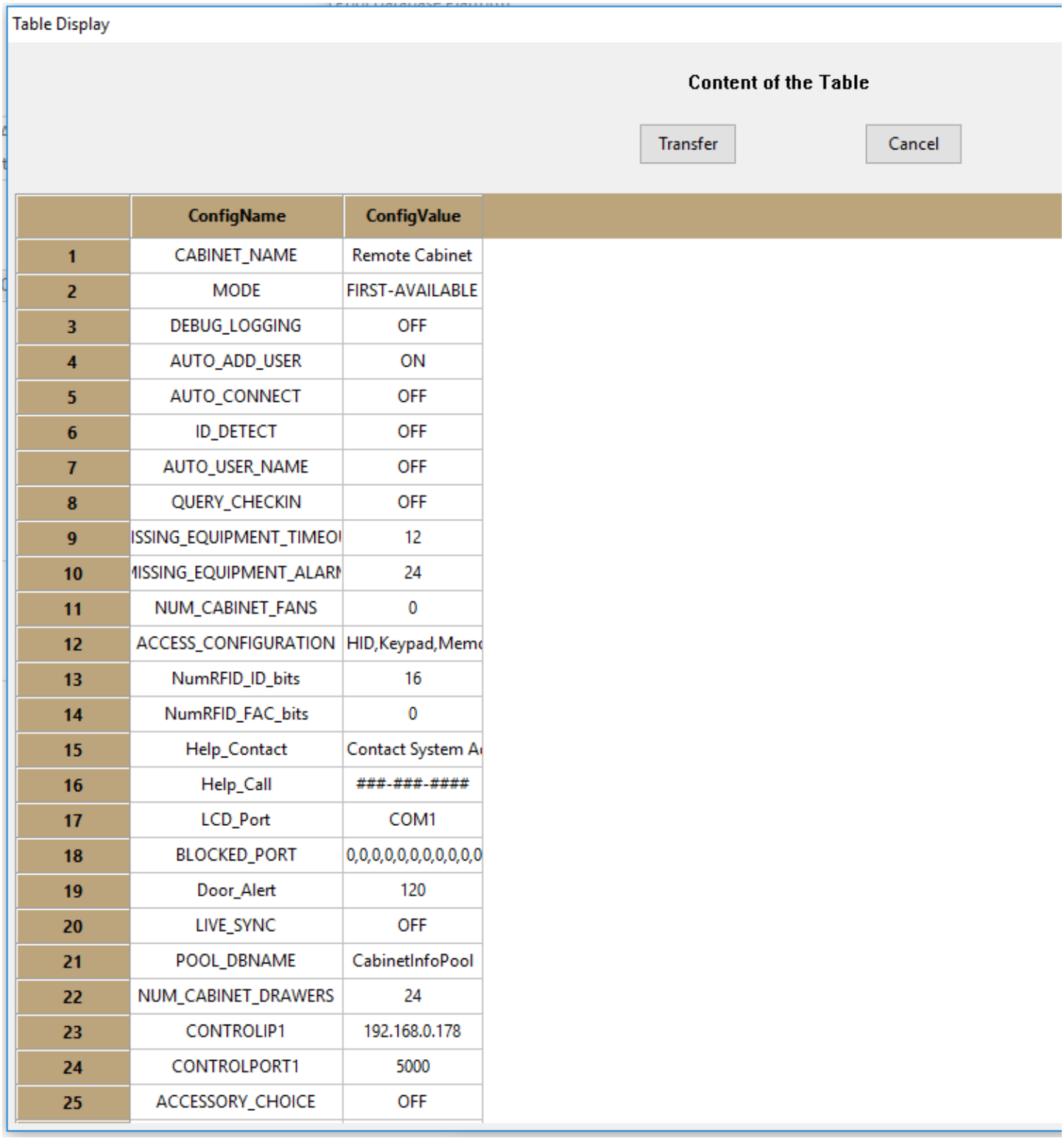
Pay attention this is only the live sync setup to current cabinet. If you want every cabinet in the network to have the same setup with the pool, all the cabinets need to have the same configuration.

9.2.6.3 Distributing Data

This section is about copy the data from pool database to the cabinet database. After pressing button "Distribute Data", the following window will appear.



From the table list, choose the tables to be copied, and from the Database Name list menu, choose the target cabinet, press “OK” button. The content of the table will be shown in a window.



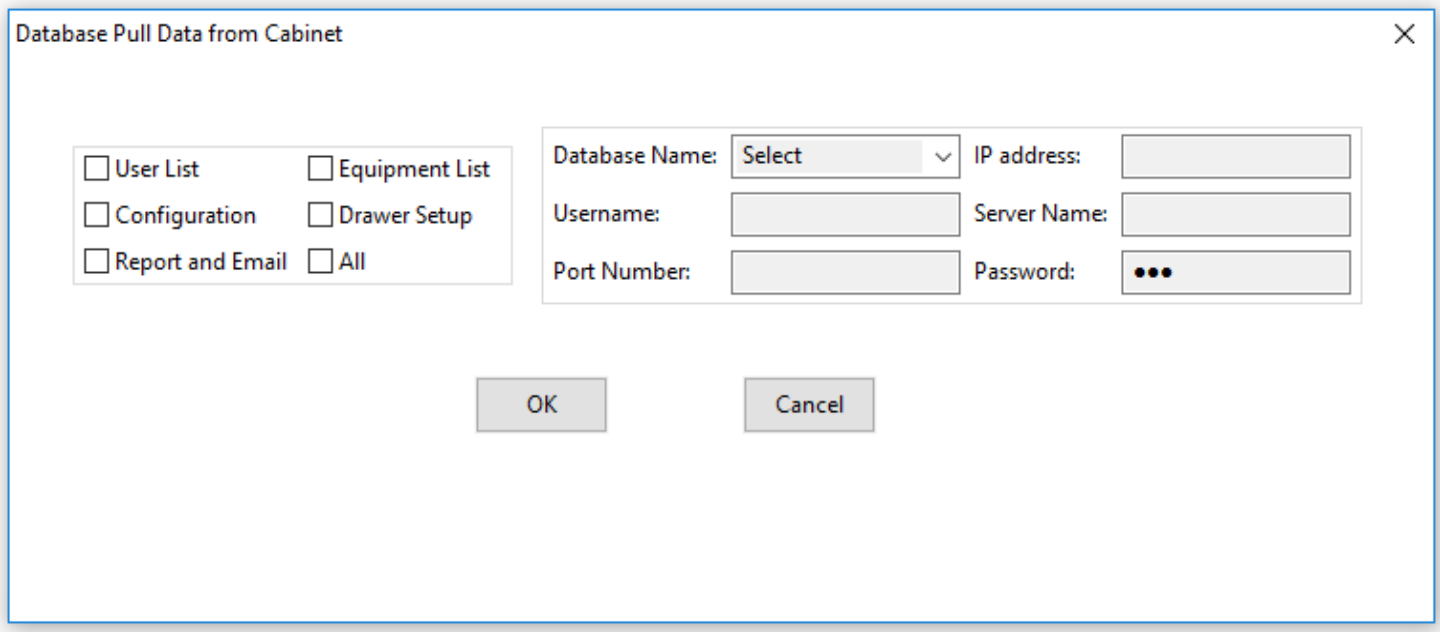
	ConfigName	ConfigValue
1	CABINET_NAME	Remote Cabinet
2	MODE	FIRST-AVAILABLE
3	DEBUG_LOGGING	OFF
4	AUTO_ADD_USER	ON
5	AUTO_CONNECT	OFF
6	ID_DETECT	OFF
7	AUTO_USER_NAME	OFF
8	QUERY_CHECKIN	OFF
9	ISSING_EQUIPMENT_TIMEOI	12
10	MISSING_EQUIPMENT_ALARI	24
11	NUM_CABINET_FANS	0
12	ACCESS_CONFIGURATION	HID,Keypad,Memo
13	NumRFID_ID_bits	16
14	NumRFID_FAC_bits	0
15	Help_Contact	Contact System A
16	Help_Call	###-###-####
17	LCD_Port	COM1
18	BLOCKED_PORT	0,0,0,0,0,0,0,0,0,0
19	Door_Alert	120
20	LIVE_SYNC	OFF
21	POOL_DBNAME	CabinetInfoPool
22	NUM_CABINET_DRAWERS	24
23	CONTROLIP1	192.168.0.178
24	CONTROLPORT1	5000
25	ACCESSORY_CHOICE	OFF

Press “Transfer” button, a progress bar will appear, and the window will close when the transfer is finished.

9.2.6.4 Pulling Data

This is the opposite of last section; it will pull the data from cabinet database to the pool database. Normally this happens in the beginning of the setup of pool database, the administrator needs to build up the prototype of the pool database based on a cabinet. The process is similar to the last section, but in opposite direction.

Press "Pull Data" button, the following window will appear.

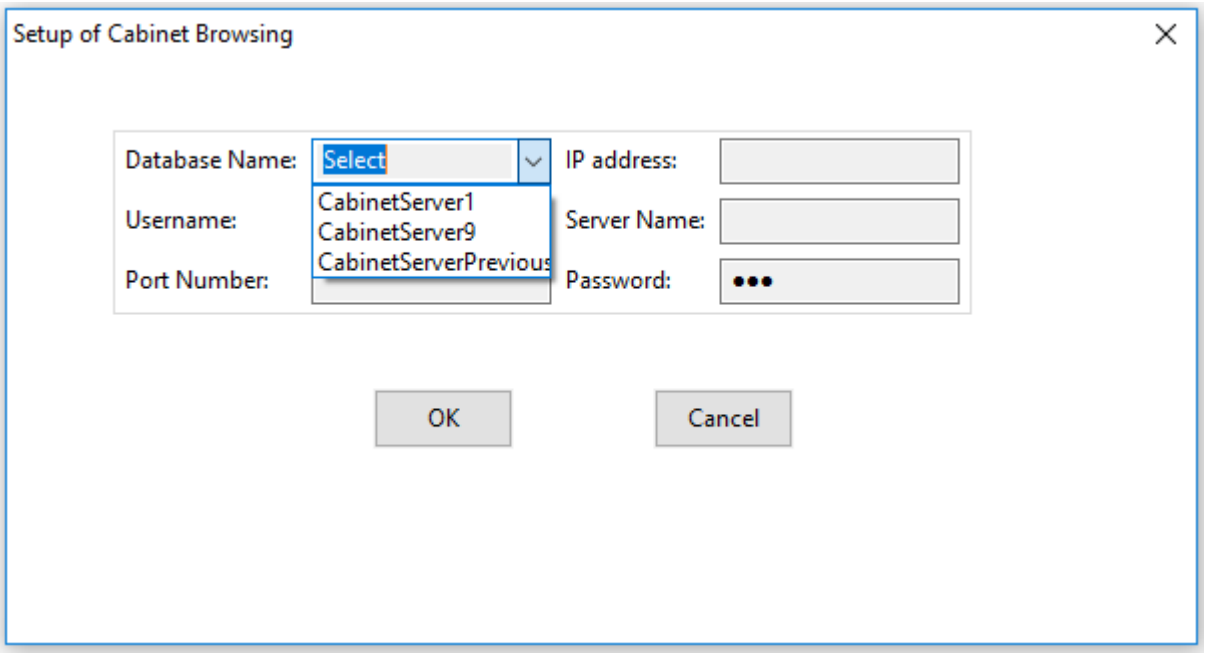


Select the tables to be pulled data from, log in to the source database, and press the "OK" button. The content of the source database table will appear, press the "Transfer" button, the progress bar for the transfer will appear, after the transfer is done, the window will close.

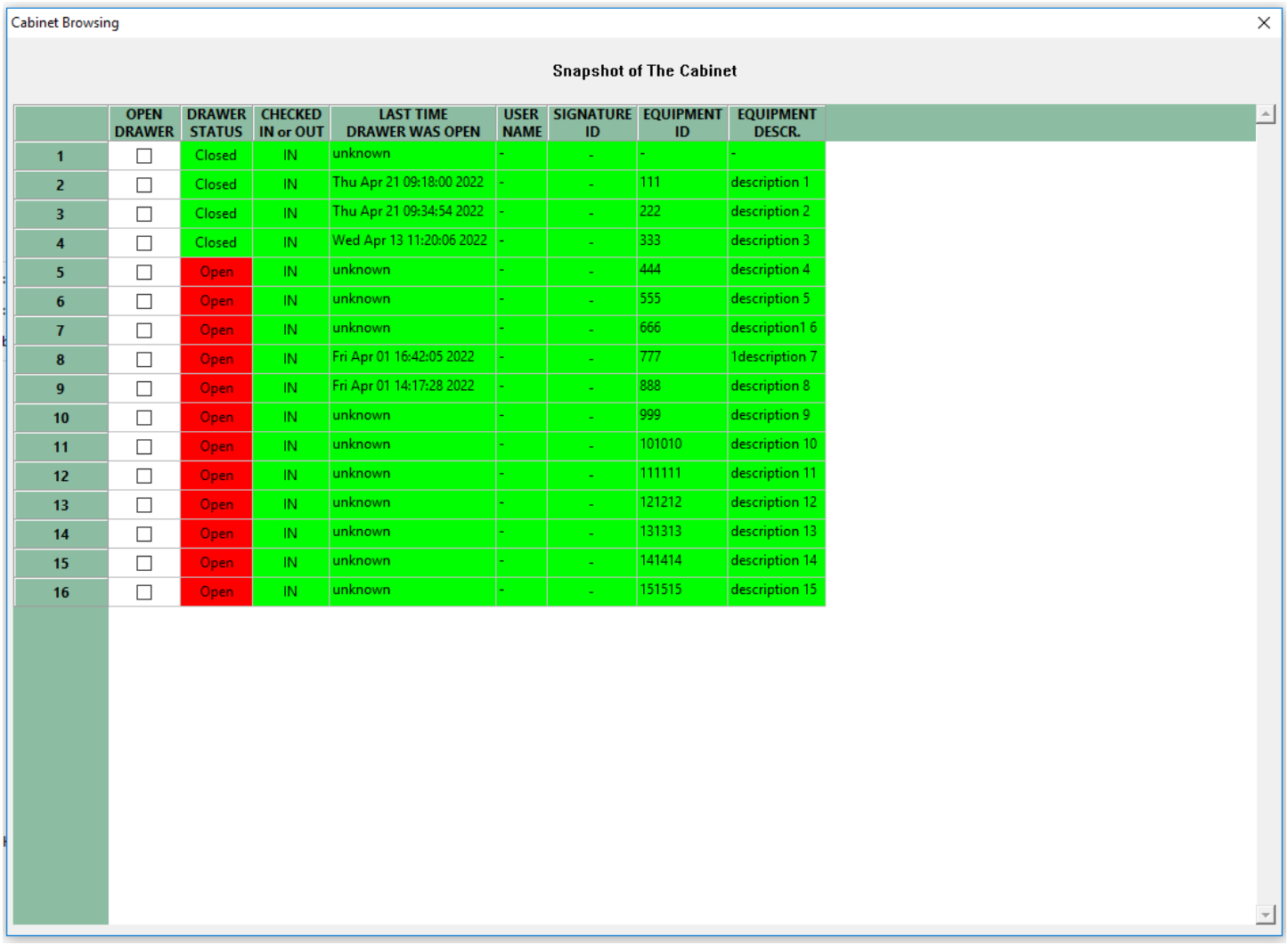
9.2.6.5 Browsing Cabinet

When managing the pool database, the administrator may want to check the situation of each cabinet. This can be done by using the Browsing Cabinet function described in the section.

Press the "Cabinet Browsing" button in the platform window, the following window will appear.



After login to the database, the following window appears to display the general situation of the cabinet.

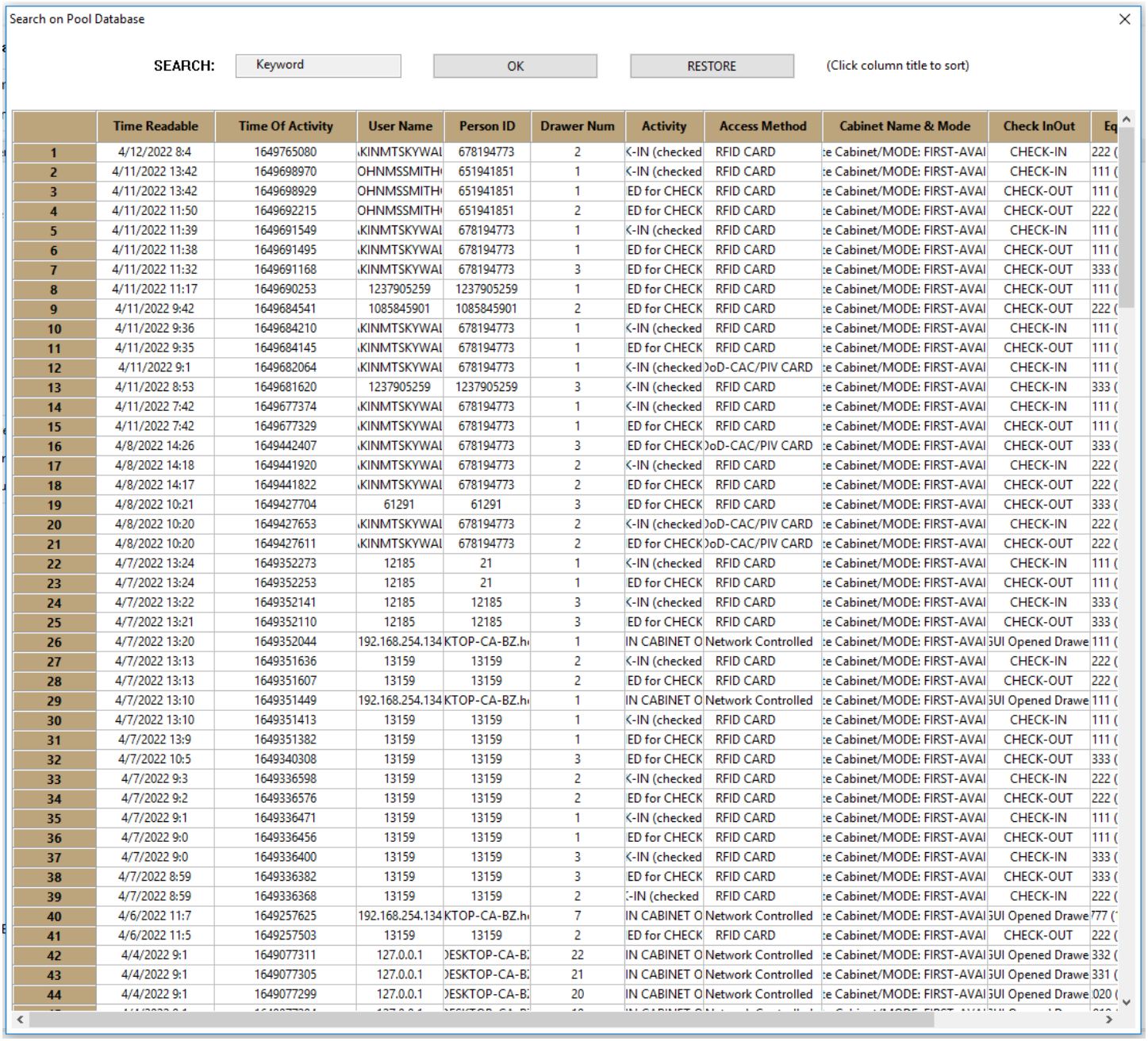


	OPEN DRAWER	DRAWER STATUS	CHECKED IN or OUT	LAST TIME DRAWER WAS OPEN	USER NAME	SIGNATURE ID	EQUIPMENT ID	EQUIPMENT DESCR.
1	☐	Closed	IN	unknown	-	-	-	-
2	☐	Closed	IN	Thu Apr 21 09:18:00 2022	-	-	111	description 1
3	☐	Closed	IN	Thu Apr 21 09:34:54 2022	-	-	222	description 2
4	☐	Closed	IN	Wed Apr 13 11:20:06 2022	-	-	333	description 3
5	☐	Open	IN	unknown	-	-	444	description 4
6	☐	Open	IN	unknown	-	-	555	description 5
7	☐	Open	IN	unknown	-	-	666	description1 6
8	☐	Open	IN	Fri Apr 01 16:42:05 2022	-	-	777	1description 7
9	☐	Open	IN	Fri Apr 01 14:17:28 2022	-	-	888	description 8
10	☐	Open	IN	unknown	-	-	999	description 9
11	☐	Open	IN	unknown	-	-	101010	description 10
12	☐	Open	IN	unknown	-	-	111111	description 11
13	☐	Open	IN	unknown	-	-	121212	description 12
14	☐	Open	IN	unknown	-	-	131313	description 13
15	☐	Open	IN	unknown	-	-	141414	description 14
16	☐	Open	IN	unknown	-	-	151515	description 15

The user can check the situation of each cabinet by login to the related database.

9.2.6.6 Search the Log of the Pool Database

The administrator can search the activity log of the pool database for some more consistent information about a user or device. After press "Search" button of the platform, the following window popped up to display the log.



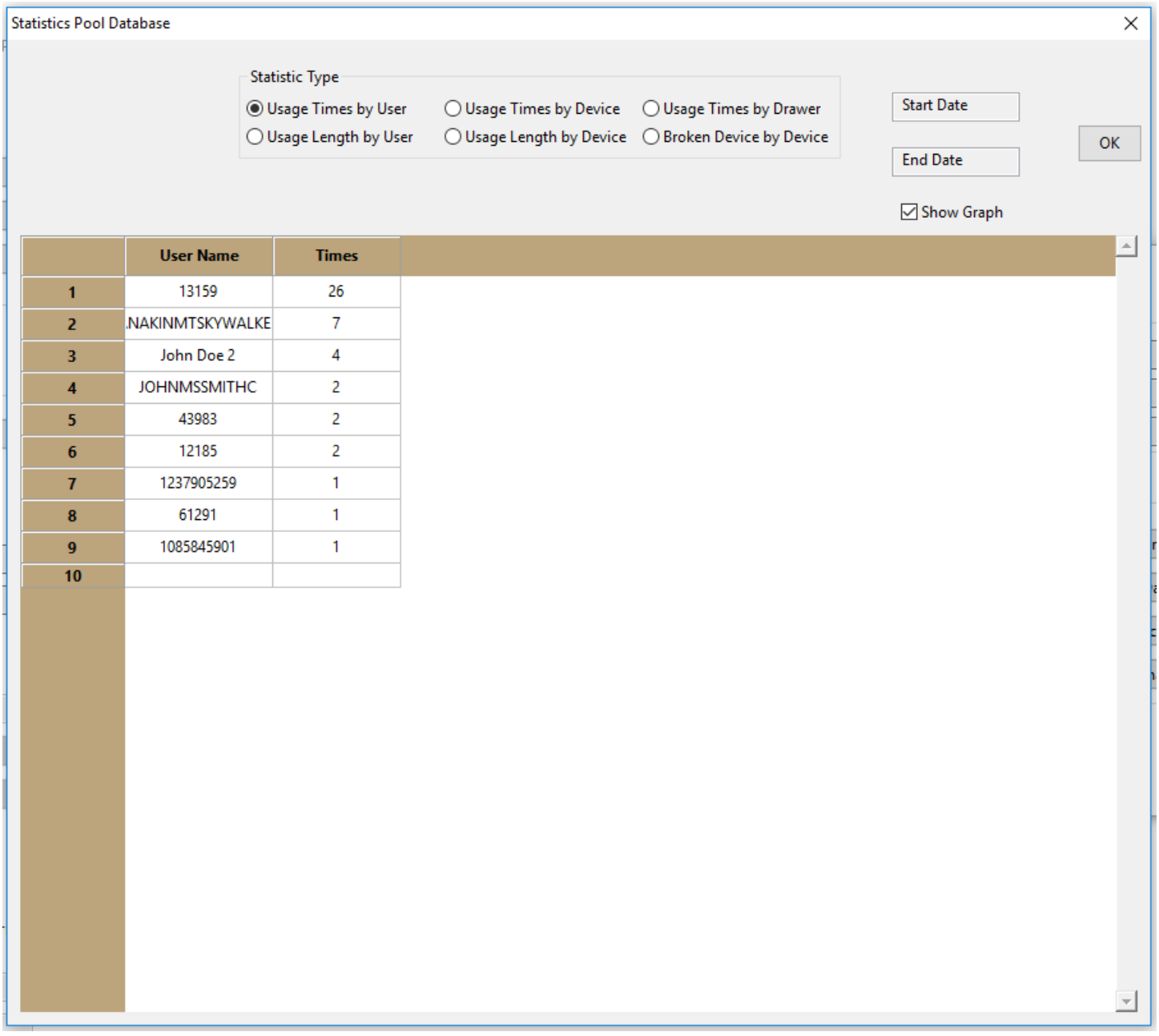
	Time Readable	Time Of Activity	User Name	Person ID	Drawer Num	Activity	Access Method	Cabinet Name & Mode	Check InOut	Eq
1	4/12/2022 8:4	1649765080	.KINMTSKYWAI	678194773	2	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	222 (
2	4/11/2022 13:42	1649698970	OHNMSSMITH(	651941851	1	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	111 (
3	4/11/2022 13:42	1649698929	OHNMSSMITH(	651941851	1	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	111 (
4	4/11/2022 11:50	1649692215	OHNMSSMITH(	651941851	2	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	222 (
5	4/11/2022 11:39	1649691549	.KINMTSKYWAI	678194773	1	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	111 (
6	4/11/2022 11:38	1649691495	.KINMTSKYWAI	678194773	1	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	111 (
7	4/11/2022 11:32	1649691168	.KINMTSKYWAI	678194773	3	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	333 (
8	4/11/2022 11:17	1649690253	1237905259	1237905259	1	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	111 (
9	4/11/2022 9:42	1649684541	1085845901	1085845901	2	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	222 (
10	4/11/2022 9:36	1649684210	.KINMTSKYWAI	678194773	1	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	111 (
11	4/11/2022 9:35	1649684145	.KINMTSKYWAI	678194773	1	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	111 (
12	4/11/2022 9:1	1649682064	.KINMTSKYWAI	678194773	1	K-IN (checked	)oD-CAC/PIV CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	111 (
13	4/11/2022 8:53	1649681620	1237905259	1237905259	3	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	333 (
14	4/11/2022 7:42	1649677374	.KINMTSKYWAI	678194773	1	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	111 (
15	4/11/2022 7:42	1649677329	.KINMTSKYWAI	678194773	1	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	111 (
16	4/8/2022 14:26	1649442407	.KINMTSKYWAI	678194773	3	ED for CHECK	)oD-CAC/PIV CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	333 (
17	4/8/2022 14:18	1649441920	.KINMTSKYWAI	678194773	2	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	222 (
18	4/8/2022 14:17	1649441822	.KINMTSKYWAI	678194773	2	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	222 (
19	4/8/2022 10:21	1649427704	61291	61291	3	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	333 (
20	4/8/2022 10:20	1649427653	.KINMTSKYWAI	678194773	2	K-IN (checked	)oD-CAC/PIV CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	222 (
21	4/8/2022 10:20	1649427611	.KINMTSKYWAI	678194773	2	ED for CHECK	)oD-CAC/PIV CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	222 (
22	4/7/2022 13:24	1649352273	12185	21	1	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	111 (
23	4/7/2022 13:24	1649352253	12185	21	1	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	111 (
24	4/7/2022 13:22	1649352141	12185	12185	3	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	333 (
25	4/7/2022 13:21	1649352110	12185	12185	3	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	333 (
26	4/7/2022 13:20	1649352044	192.168.254.134	KTOP-CA-BZ.h	1	IN CABINET O	Network Controlled	:e Cabinet/MODE: FIRST-AVAI	3UI Opened Drawe	111 (
27	4/7/2022 13:13	1649351636	13159	13159	2	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	222 (
28	4/7/2022 13:13	1649351607	13159	13159	2	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	222 (
29	4/7/2022 13:10	1649351449	192.168.254.134	KTOP-CA-BZ.h	1	IN CABINET O	Network Controlled	:e Cabinet/MODE: FIRST-AVAI	3UI Opened Drawe	111 (
30	4/7/2022 13:10	1649351413	13159	13159	1	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	111 (
31	4/7/2022 13:9	1649351382	13159	13159	1	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	111 (
32	4/7/2022 10:5	1649340308	13159	13159	3	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	333 (
33	4/7/2022 9:3	1649336598	13159	13159	2	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	222 (
34	4/7/2022 9:2	1649336576	13159	13159	2	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	222 (
35	4/7/2022 9:1	1649336471	13159	13159	1	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	111 (
36	4/7/2022 9:0	1649336456	13159	13159	1	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	111 (
37	4/7/2022 9:0	1649336400	13159	13159	3	K-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	333 (
38	4/7/2022 8:59	1649336382	13159	13159	3	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	333 (
39	4/7/2022 8:59	1649336368	13159	13159	2	:-IN (checked	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-IN	222 (
40	4/6/2022 11:7	1649257625	192.168.254.134	KTOP-CA-BZ.h	7	IN CABINET O	Network Controlled	:e Cabinet/MODE: FIRST-AVAI	3UI Opened Drawe	777 (
41	4/6/2022 11:5	1649257503	13159	13159	2	ED for CHECK	RFID CARD	:e Cabinet/MODE: FIRST-AVAI	CHECK-OUT	222 (
42	4/4/2022 9:1	1649077311	127.0.0.1	)ESKTOP-CA-B	22	IN CABINET O	Network Controlled	:e Cabinet/MODE: FIRST-AVAI	3UI Opened Drawe	332 (
43	4/4/2022 9:1	1649077305	127.0.0.1	)ESKTOP-CA-B	21	IN CABINET O	Network Controlled	:e Cabinet/MODE: FIRST-AVAI	3UI Opened Drawe	331 (
44	4/4/2022 9:1	1649077299	127.0.0.1	)ESKTOP-CA-B	20	IN CABINET O	Network Controlled	:e Cabinet/MODE: FIRST-AVAI	3UI Opened Drawe	020 (

Type in the keyword to search, and press "OK" button, and the table will show only the items with the keyword included. Press "RESTORE" button to display to full list of the log.

Clicking on the title of the column can sort the list in increasing or decreasing order based on the related column.

9.2.6.7 Statistics Based on Pool Database

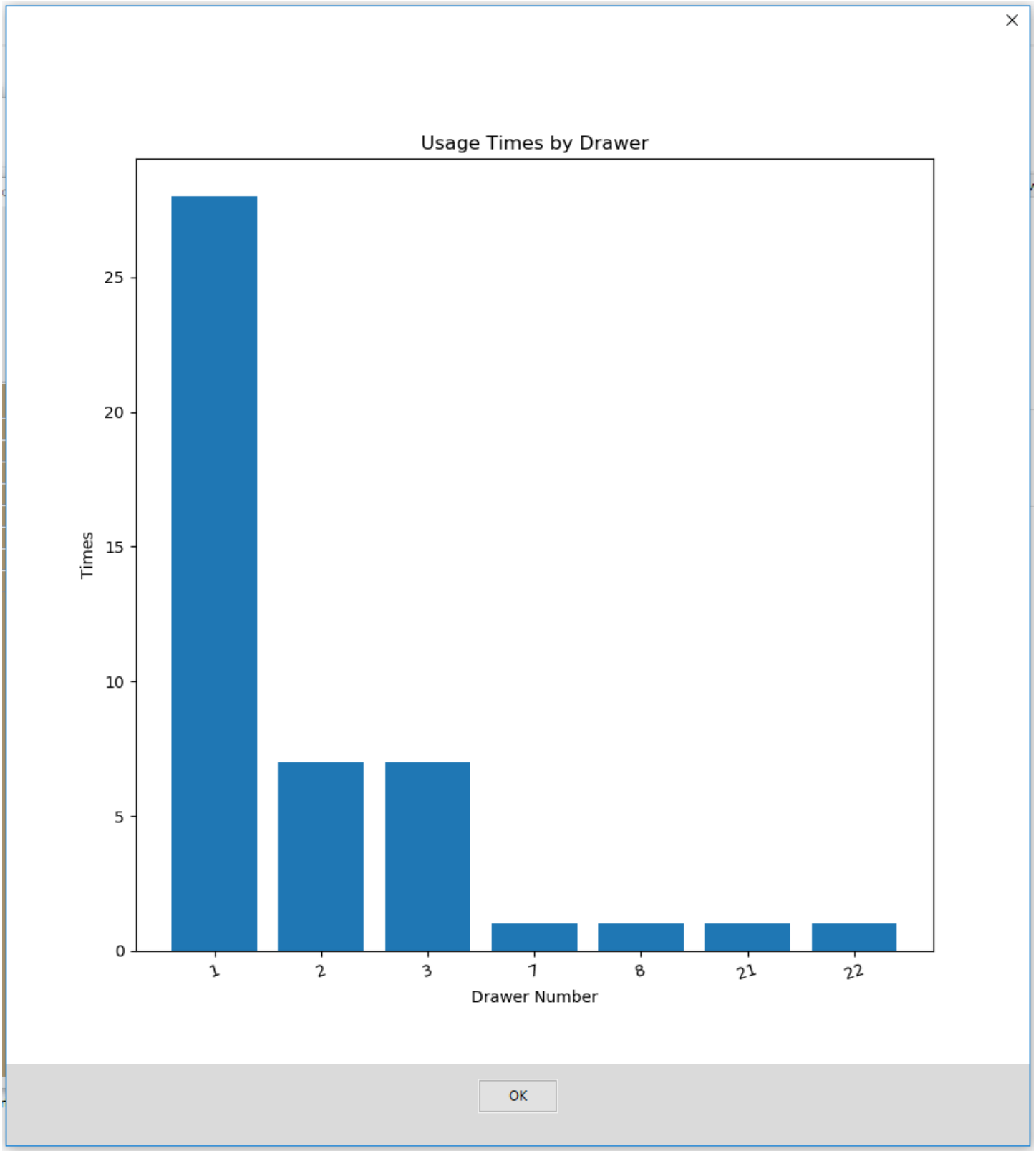
Some statistic result can be generated based on the activity log of the pool database, and the chart can be shown to reflect the result. Press "Statistics" button in the platform, and the following window will pop up.



	User Name	Times
1	13159	26
2	.NAKINMTSKYWALKE	7
3	John Doe 2	4
4	JOHNMSSMITHC	2
5	43983	2
6	12185	2
7	1237905259	1
8	61291	1
9	1085845901	1
10		

The statistic types include Usage Times by User, Usage Times by Device, Usage Times by Drawer, Usage Length by User, Usage length by Device, and Broken Device by Device.

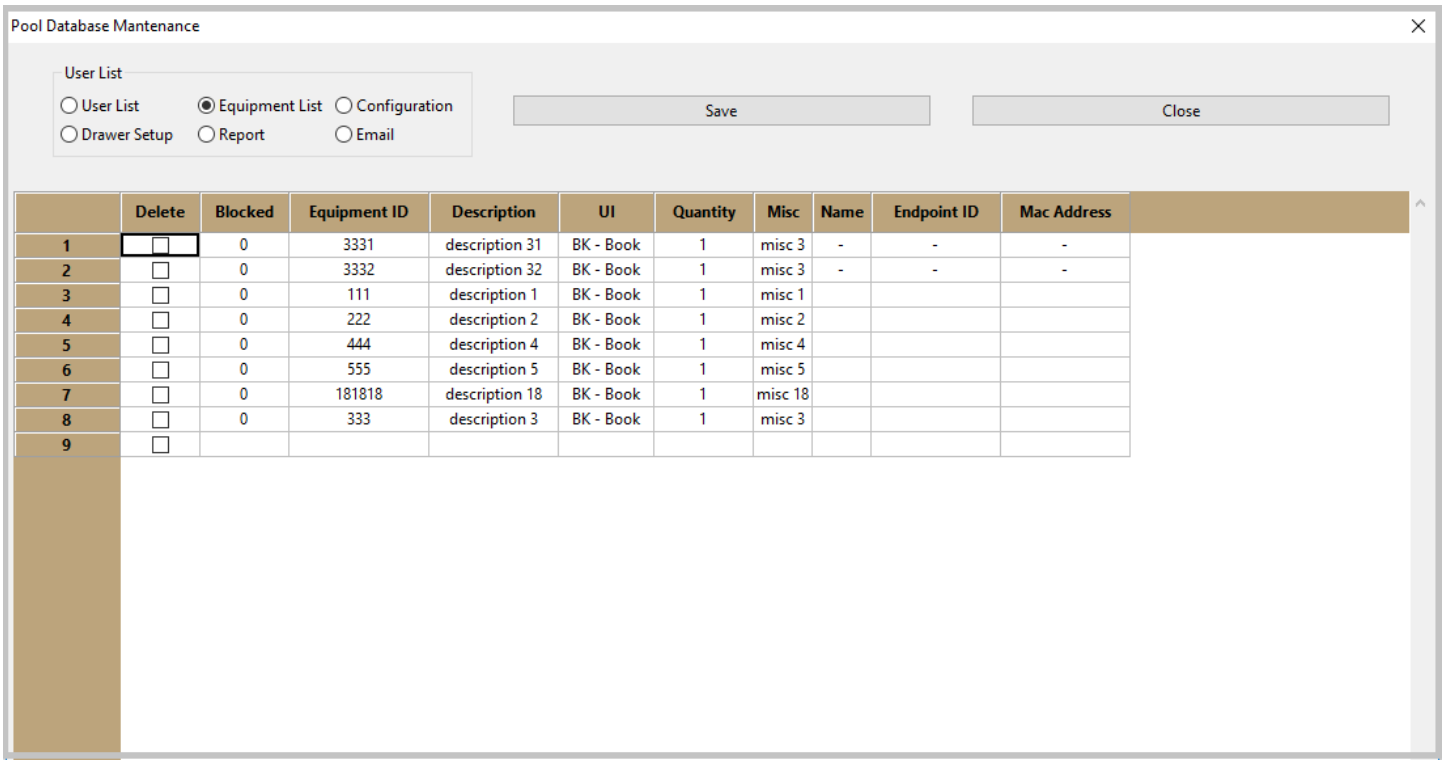
For each statistic type, there is a table to show the details. If Show Graph is selected, there will be a graph popping up to illustrate the result of the table. The following is a screenshot.


Usage Times by Drawer
Times
0
5
10
15
20
25
1
2
3
7
8
21
22
Drawer Number
OK

If the user wants to narrow down the searching result, there are fields of Start Date and End Date to define the searching boundary.

9.2.6.8 Maintenance of Pool Database

The database in the pool database needs to be modified in some circumstances. The tables that can be changed include User List, Equipment List, Configuration, Drawer Setup, Report and Email Setup. The user can add, delete, or change the items in the table. The following is a screenshot.



	Delete	Blocked	Equipment ID	Description	UI	Quantity	Misc	Name	Endpoint ID	Mac Address
1	☐	0	3331	description 31	BK - Book	1	misc 3	-	-	-
2	☐	0	3332	description 32	BK - Book	1	misc 3	-	-	-
3	☐	0	111	description 1	BK - Book	1	misc 1			
4	☐	0	222	description 2	BK - Book	1	misc 2			
5	☐	0	444	description 4	BK - Book	1	misc 4			
6	☐	0	555	description 5	BK - Book	1	misc 5			
7	☐	0	181818	description 18	BK - Book	1	misc 18			
8	☐	0	333	description 3	BK - Book	1	misc 3			
9	☐									

After the table is ready, press "Save" button, and the table will be saved into the database. Click on the name of different tables, and the screen will display the content of corresponding table.

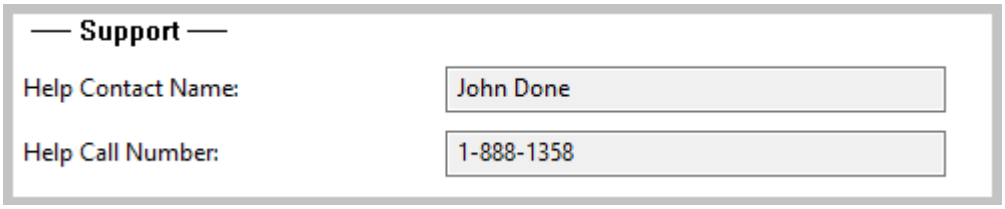
10 CABINET SUPPORT

When the cabinet has an issue, usually people will look for help. There are several ways the user can do. The user can find the phone number and the name to call the administrator; the administrator can run the diagnostics program from *CAC-GUI*; they can also talk to the support center with video conference from *CAC-GUI*.

10.1 Help Information on Cabinet Keypad

When press *HELP* button on the cabinet panel, it shows on the LCD screen with the first line "*HELP ACCESS*", and the second line "*SELECT ACTIVITY*:". Use the arrow button roll the menu and choose "*CONTACT INFORMATION*" by pressing *ENTER* button, and the LCD screen will show the name and phone number of the contact person.

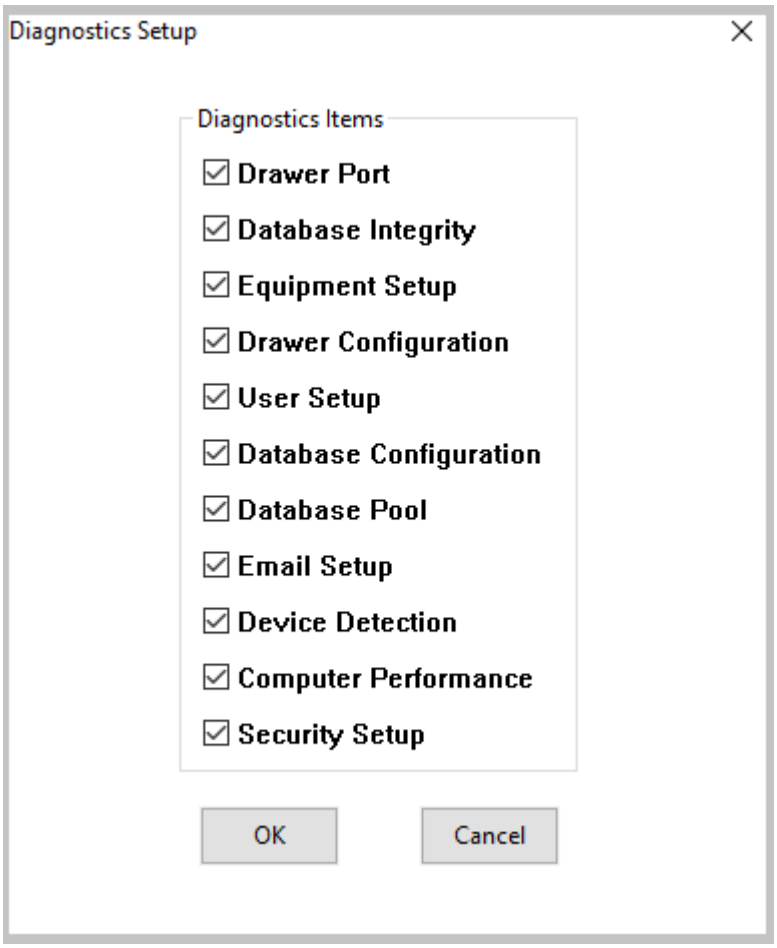
The name and the phone number of the contact person can be set up in *System Config* tab of *CAC-GUI*. The following is a screenshot of the setup:



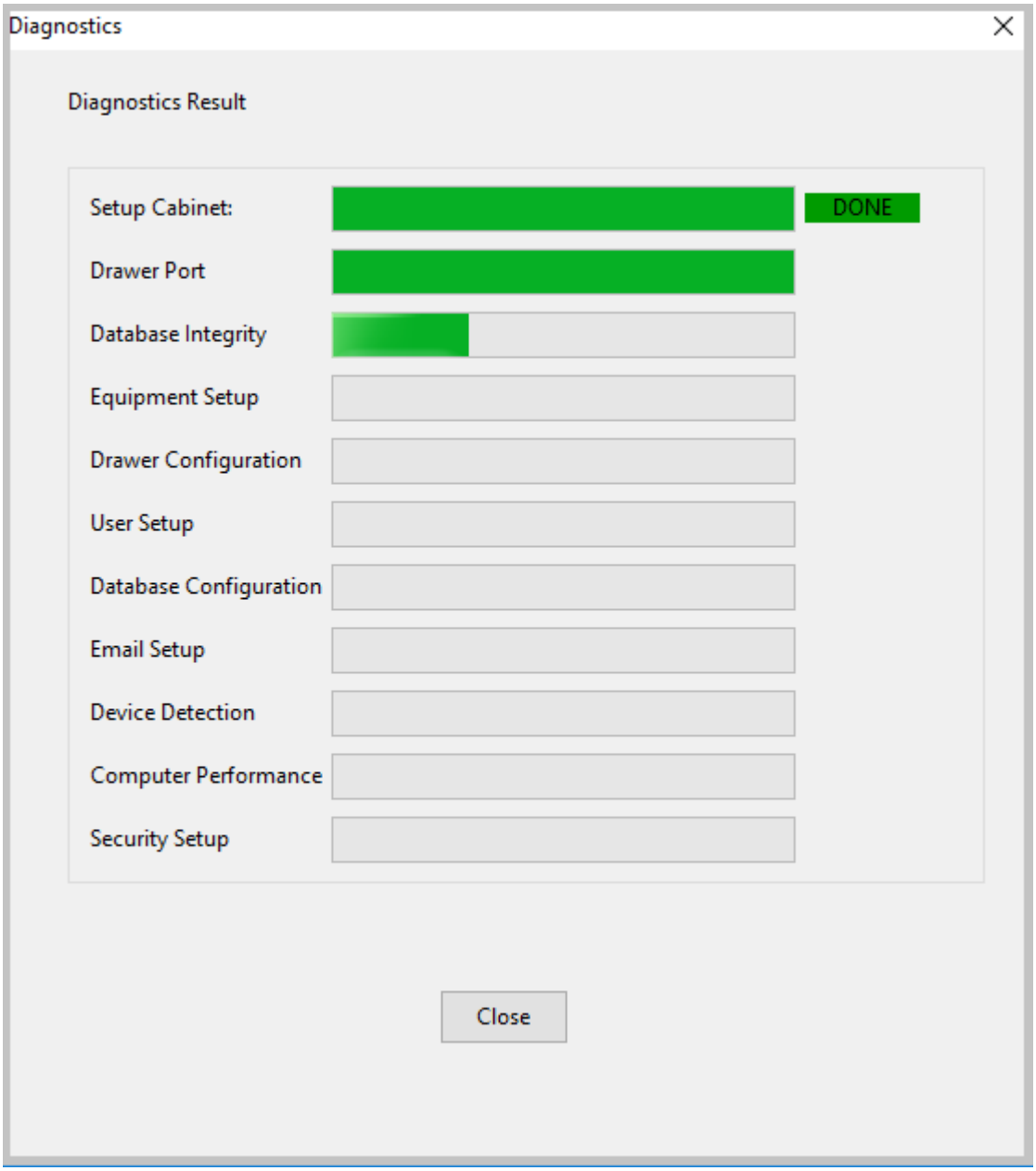
10.2 Diagnostics

Before contacting the support center, it is better to check the major modules of the cabinet and see if there are any problems. This can be done by running *Diagnostics* module located in *System Config* tab of *CAC-GUI*.

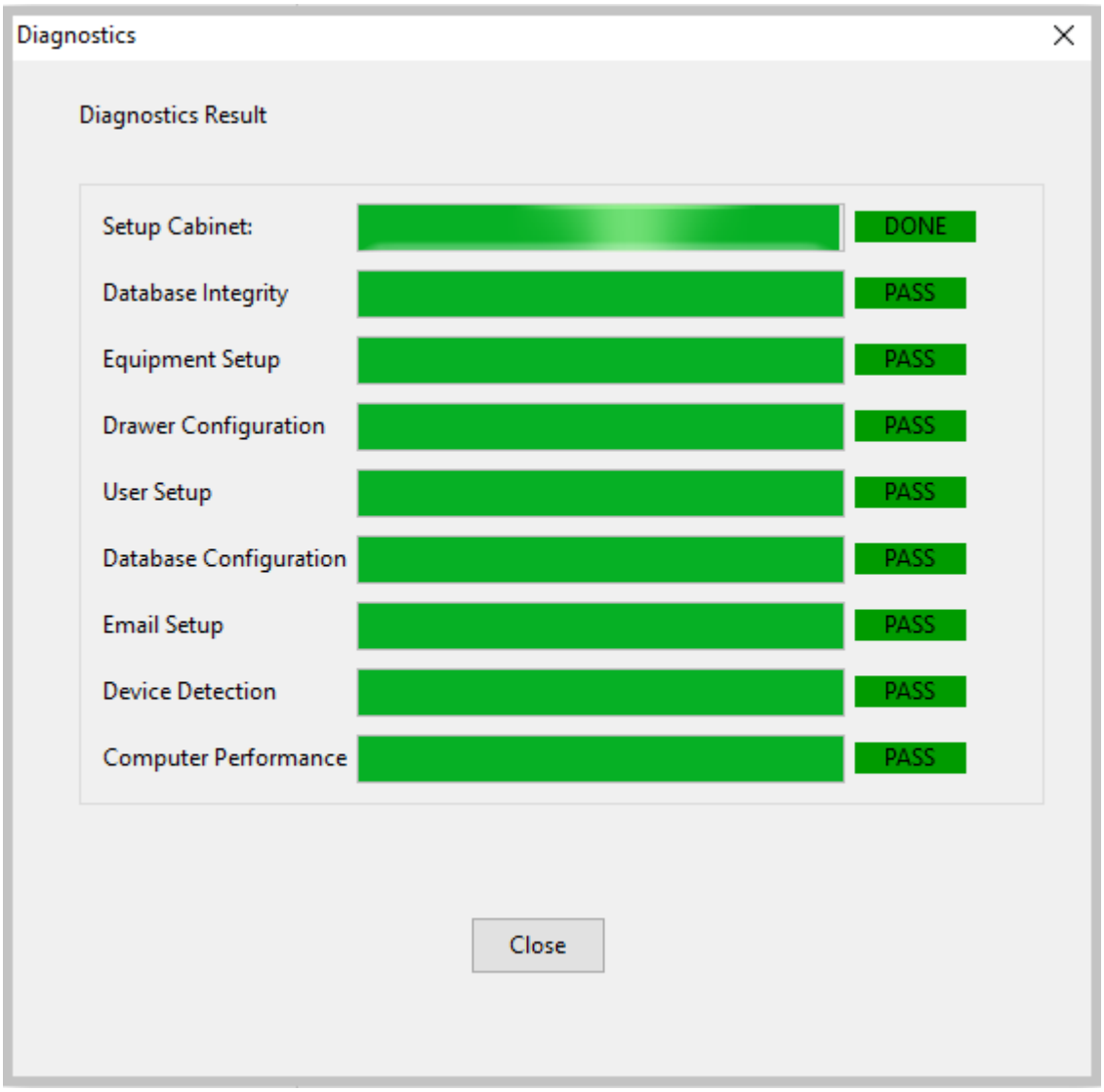
After pressing *Diagnostics Setup* button, a window will pop up with the list of testing items. The default setup is including all the items. The following is a screenshot.



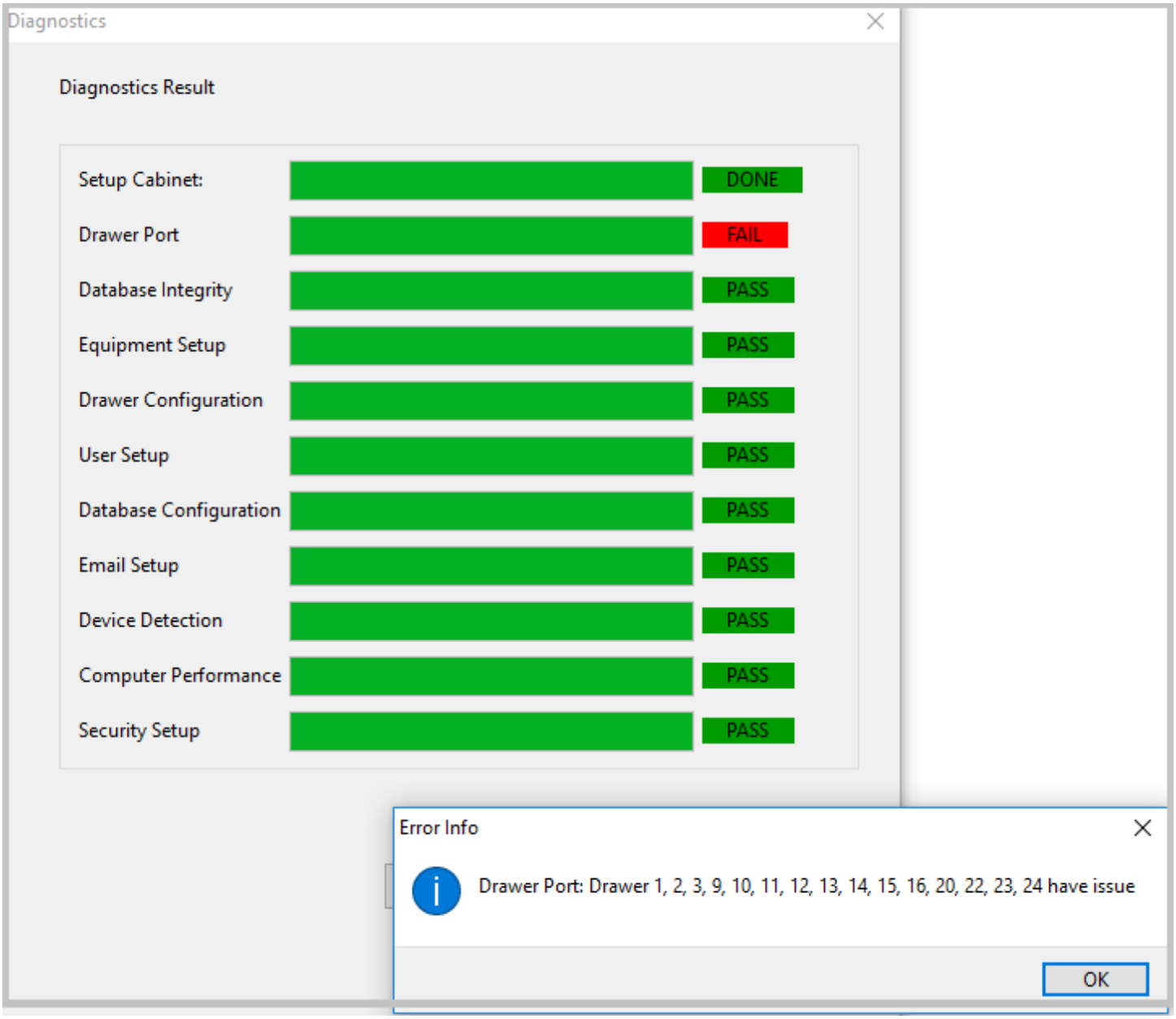
When the selection is done, press *OK* button to start the checking process.



After the diagnostics is done, if there is no issue, the window will show the result as following:

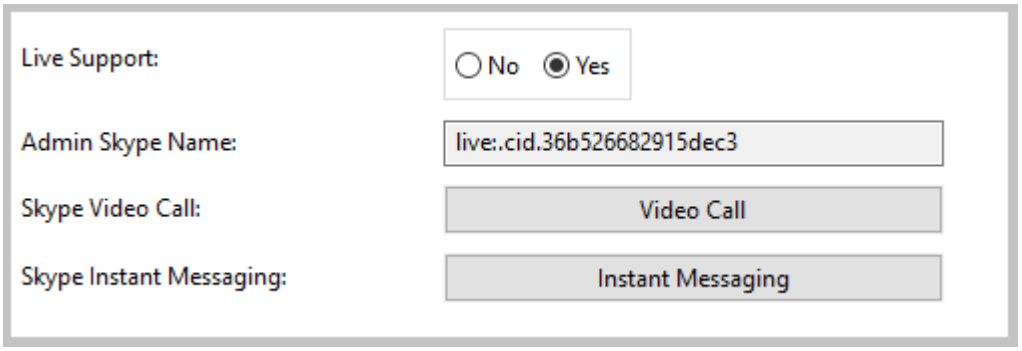


If there are issues in the result, the window will show the failed items, and a window will pop up to display the details of the failure. A screenshot is as following:



10.3 Live Support

Live support is the process that the cabinet administrator talks to the support center by video conference about the details of an issue; this can also be done by instant messaging. This function module requires both sides have *Skype* installed. The setup locates at *System Config* tab of *CAC-GUI*. The following is a screenshot.



Live Support option needs to be *Yes* to enable the function. *Admin Skype Name* is the Skype Name of the support center. Be attention that the *Skype Name* is not the login name.

Skype Name can be found by the following steps:

i) Select your profile picture
ii) Select *Skype Profile*, and both your *Skype Name* and account you have signed in with are displayed in your profile

After setting up *Admin Skype Name*, press *Video Call* button, and a video call will be placed to the support center.

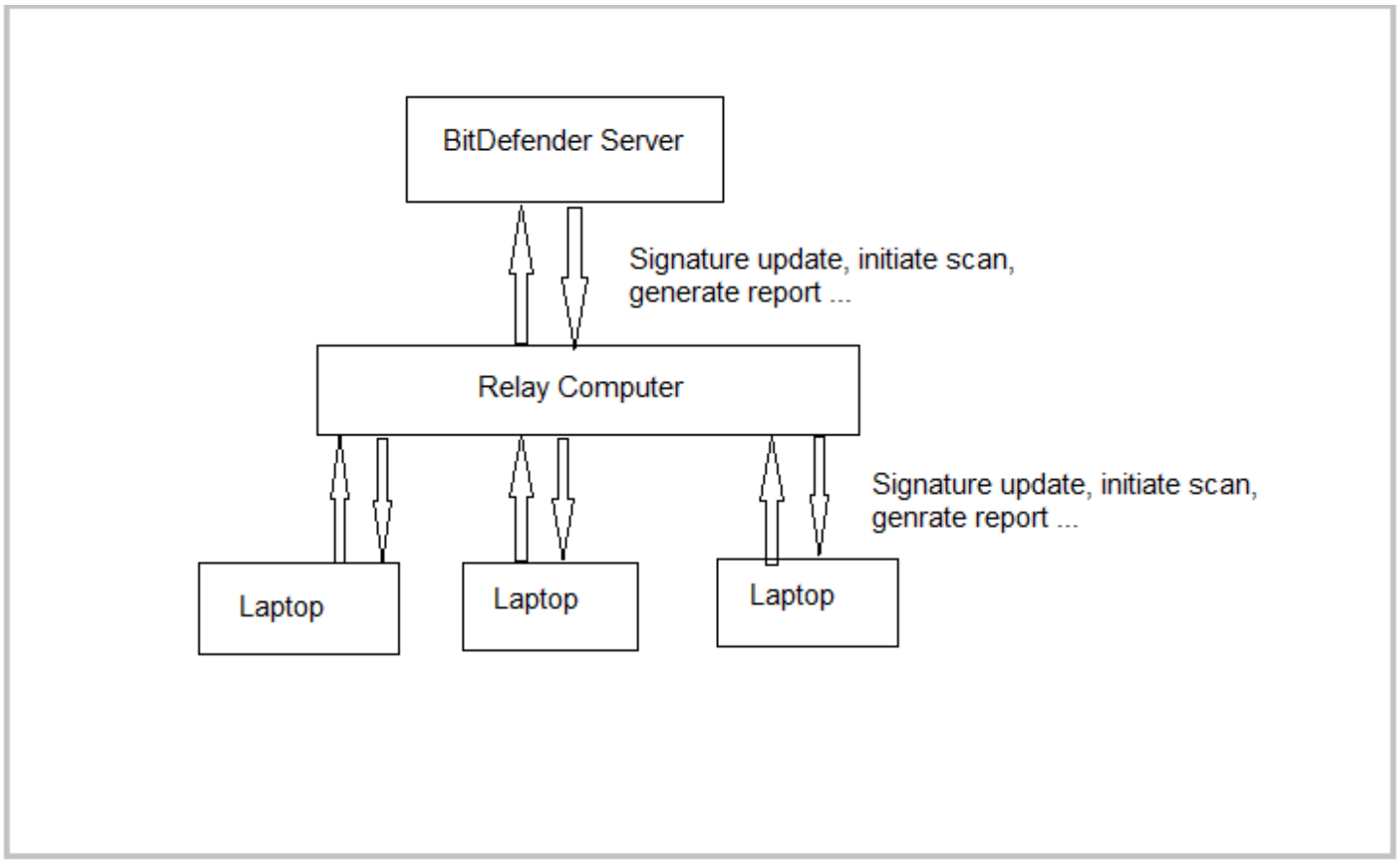
If the user would like to use messaging instead of video, button *Instant Messaging* is available for the function.

11 SECURITY FUNCTION

Security is becoming an import issue in the IT industry. Windows Operational System has a set of tools to monitor the computer security issues and prevent the malware to come through, such as Firewall and Account protection, but these native tools are not effective enough to counter with the hacker techniques that are changing and growing every day. We are using the security technology from BitDefender, which is a world leader of cybersecurity software, to manage the security issues of the computers in the cabinet. In the following sections we will describe the principle and the configuration process of the functions.

11.1 Security Function Principle

There are two layers in the computer network structure of the cabinet. It is similar to the client-server structure, the cabinet computer works as a relay whose function is like a server, it directly communicates with the BitDefender website to update the virus signature, deploy package modules, and execute the API functions. The laptop computers in the cabinet are like the client. These computers do not directly communicate with the outside environment; all their communications will come through the relay computer. The following diagraph is an illustration of this structure.



The relay computer and the laptop computers are all called endpoints. A software packages needs to be installed to the endpoints to do the real-time monitoring and the defense. The installer of the software package can be downloaded from BitDefender management portal.

A set of APIs is used to handle the communication with BitDefender, it can get the list of the endpoints, read the malware status, initiate a scan for the endpoint, get the scan result, and generate/download the report, etc. The relay computer runs a program to manage all the security issues in the computer including itself.

When a laptop computer is checked in to the cabinet, the relay computer immediately initiates a scan to the laptop. When the scan has finished, the relay computer reads the malware result and generates a set of reports. The result and the reports are parsed and written to the database and the data are displayed in CAC-GUI in real-time. If malware is found in one endpoint, the related drawer will be locked, a warning message is displayed in the LCD screen of the computer, and an alert email can be sent to the administrator.

Besides the malware status, the attack attempts are also recorded and displayed, including anti-phishing activity, firewall activity, data protection, and the blocked websites.

11.2 Security Server Setup

BitDefender has two versions of applications: Cloud version and On-premises version. For the Cloud version, BitDefender will host the security server for the management of endpoints. For the On-premises version, the client needs to install the server in the local network. The following sections will have more details for the local server setup.

11.2.1 Server Installation

BitDefender provides several methods to install the security server. The server can be installed as a virtual machine in the format of VirtualBox, Nutanix, Hyper-V, etc. It can also be installed directly on Ubuntu Linux OS. The following steps in the chapter are based on the installation on Ubuntu Server 20.04.

11.2.1.1 Ubuntu Installation

For the installation of Ubuntu server, mostly it will follow the Official Ubuntu Installation Guide, but we need to pay attention to the following configuration:

- Network: DHCP for initial deploy
- Full name new user: bdadmin
- Username: bdadmin
- Encrypt home directory: No.
- Select to install only Standard system utilities and OpenSSH server.

*** Remember the IP address of the computer during the installation, and it will be used in next section

11.2.1.2 Server Installation

The server installation needs to be done remotely. Use SSH connect to the server computer as user bdadmin, and then run the following commands.

```
sudo -i

sed -ri 's#^GRUB_CMDLINE_LINUX_DEFAULT=.*#GRUB_CMDLINE_LINUX_DEFAULT="netcfg/do_not_use_ifupdown=true net.ifnames=0 biosdevname=0 console=tty1 console=ttyS0,115200n8 earlyprintk=ttyS0,115200 rootdelay=300"#' /etc/default/grub

update-grub2

apt -yq install ifupdown

echo -e 'auto lo\niface lo inet loopback\n\nauto eth0\niface eth0 inet dhcp' > /etc/network/interfaces

apt -yq install resolvconf

ln -sf /run/resolvconf/resolv.conf /etc/resolv.conf

systemctl disable systemd-resolved

mv /etc/apt/sources.list /etc/apt/sources.list.orig

echo "deb https://download.bitdefender.com/repos/deb-hydra20-unified bitdefender non-free" > /etc/apt/sources.list.d/deb-hydra20-unified.list

curl -sS http://download.bitdefender.com/repos/gzrepos.key.asc | apt-key add -

export DEBIAN_FRONTEND="noninteractive"

timedatectl set-timezone UTC

timedatectl set-local-rtc false

chmod -x /etc/update-motd.d/*

apt clean

apt update

apt -yq dist-upgrade

apt -yq --allow-unauthenticated install gzinstallwizard
```

/opt/bitdefender/scripts/createInstallerXml.sh

apt autoremove --purge snapd

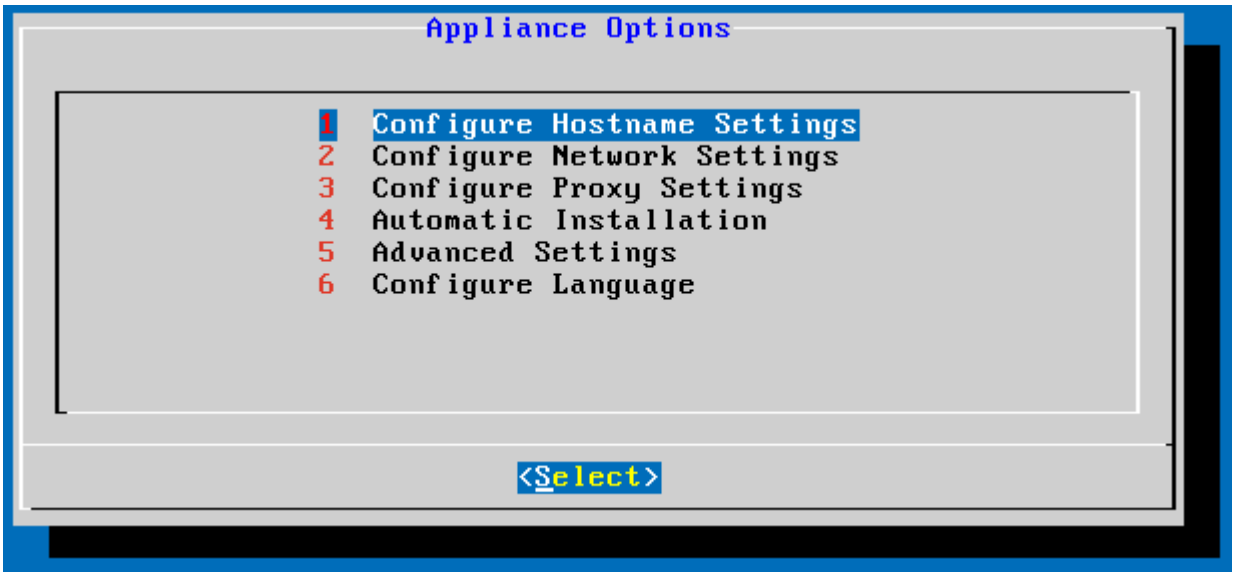
apt -yq autoremove

reboot

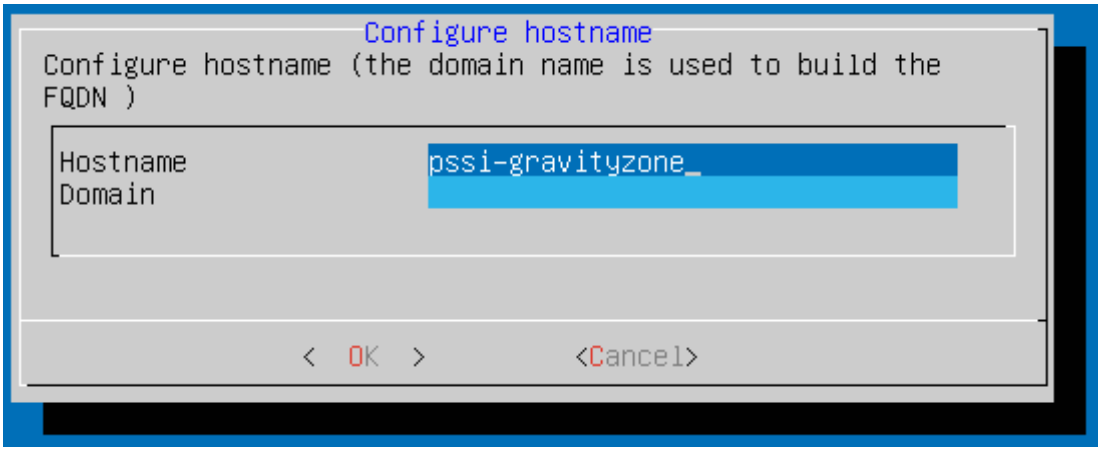
After running the commands above, the BitDefender server has been installed on the computer.

11.2.2 Server Configuration

After the server is installed, we need to set up the server roles and applications. From the server computer, log in the GUI as user bdadmin. And the following screen will appear:

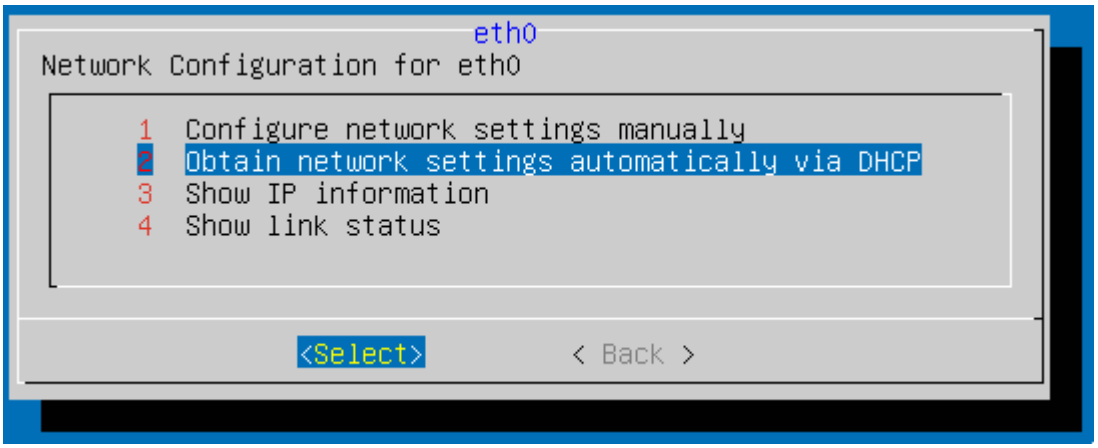


Click Configure Hostname Setting, and type in the Hostname, leave the Domain field empty (only for Linux Computer, for Virtual Machine, this field normally needs to be filed with the IP address).



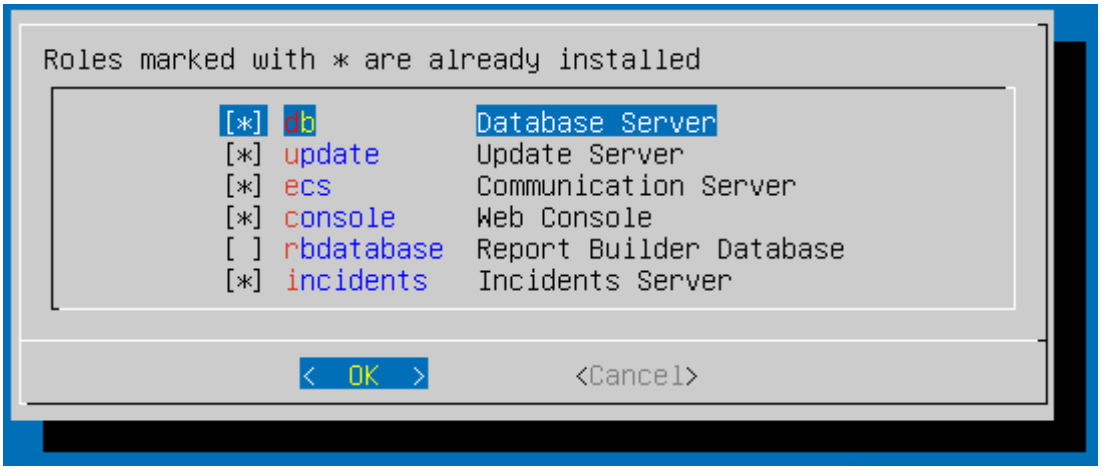
After the value is setup, press OK button to return to the Appliance Options screen.

Press Configure Network Settings, and then choose eth0, and press Select, in the next screen, choose Obtain network settings automatically via DHCP, (this is suggested for the first-time setting, can come back to change it with Configure network settings manually to a static IP address).



The IP address can be verified by clicking Show IP information and read the result.

Click Back, return to the Appliance Option screen. Configure Proxy Settings and MDM Communication Server can be skipped for now. Click Advanced Settings and click Install/Uninstall Roles in the next screen, then click Add or remove roles, in the window popped up, chose Database Server, Update Server, Communication Server, Web Console, and Incidents Server. (Do not choose Report Builder Database), press OK button, and the installing process will start.



*** If there is an error during the installation, choose the same options and do it again.

Going to the Advanced Settings and install Security Server by clicking on Install Security Server. When all the roles are installed, it will include 6 servers: Database Server, Update Server, Communication Server, Security Server, Web Console, and Incidents Server.

If the user has the need to build more sophisticated reports, Report Builder Database role needs to be installed. The database needs to be in a separate computer. The computer needs to install Ubuntu Server and BitDefender Server, the steps are the same as that in section 11.2.1 and 11.2.2. In the server configuration section, click Add or remove roles, and choose Report Builder Database. (Choose no other roles/applications in this computer) and follow the instructions.

11.2.3 Certification Setup

The computer needs to install the certification to use Control Center from a website browser; otherwise, the browser will display "Not Secure" to the Control Center webpage.

11.2.3.1 Certification Generation

Start a computer with Linux Ubuntu OS (Either Ubuntu Desktop or Ubuntu Server), open a terminal, find an appropriate folder, run the following command to generate a root certification:

openssl req -newkey rsa:2048 -days 365 -x509 -keyout rootkey.pem -out root.cer -sha256 –subj "/C=US/O=XX/CN=XX/"

In the line above, "C" represents country, "O" represents organization, "CN" represents common name.

You may notice that root.cer and root.pem has been generated.

And then run the following two command to generate ssl certificate.

openssl req -new -newkey rsa:2048 -keyout sslkey.pem -out ssl.csr -sha256 -subj "/CN=XX/" -batch

openssl x509 -req -days 365 -sha256 -in ssl.csr -CA root.cer -CAkey rootkey.pem -CAcreateserial -CAserial root.serial -out ssl.cer -extfile <(printf "extendedKeyUsage = serverAuth \n subjectAltName=IP:192.168.0.xx")

As discussed before, “CN” is for common name, and the IP address needs to be set as the one with Security Server.

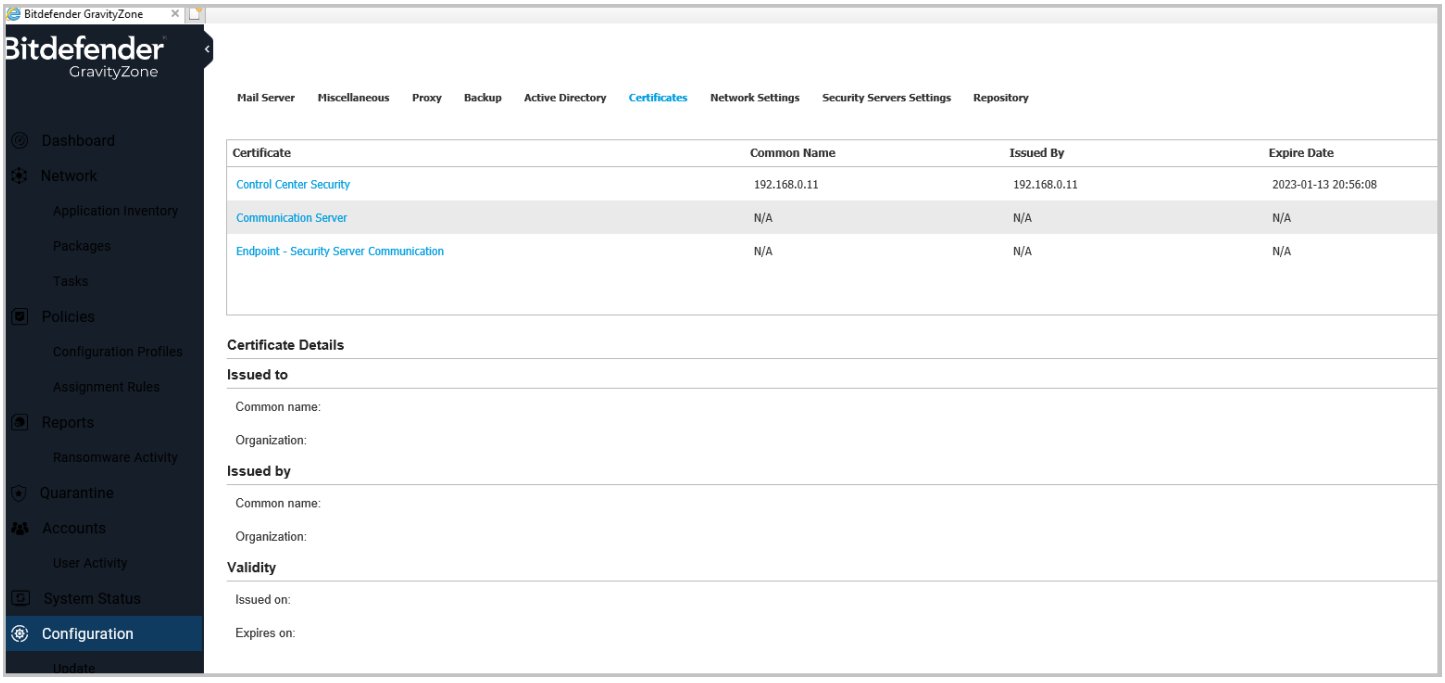
After running the commands, file ssl.cer and sslkey.pem have been generated.

For a Windows or Linux computer, the above certificates are good enough; for a Mac computer, more certificates are required. More information is available at the following link:

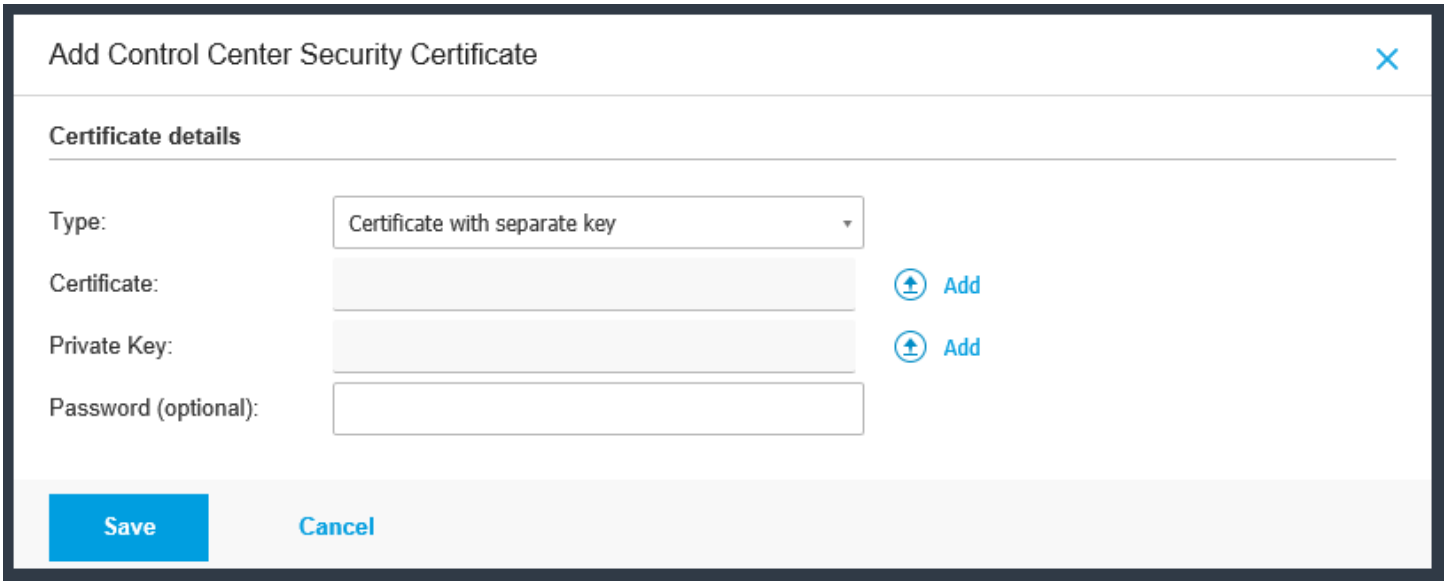
https://help.gravityzone.bitdefender.com/en/77212-80030-control-center.html#UUID-03ed7a7b-c0a5-c272-890a-a5f3a5b8536f

11.2.3.2 Certification Upload to Control Center

The certificate generated in last section needs to be uploaded to the security server from Control Center. After login to Control Center, go to Configuration on the left pane. And then choose Certificates from the list, the following is the screenshot.



Click Control Center Security from the list, a window will pop up as following:

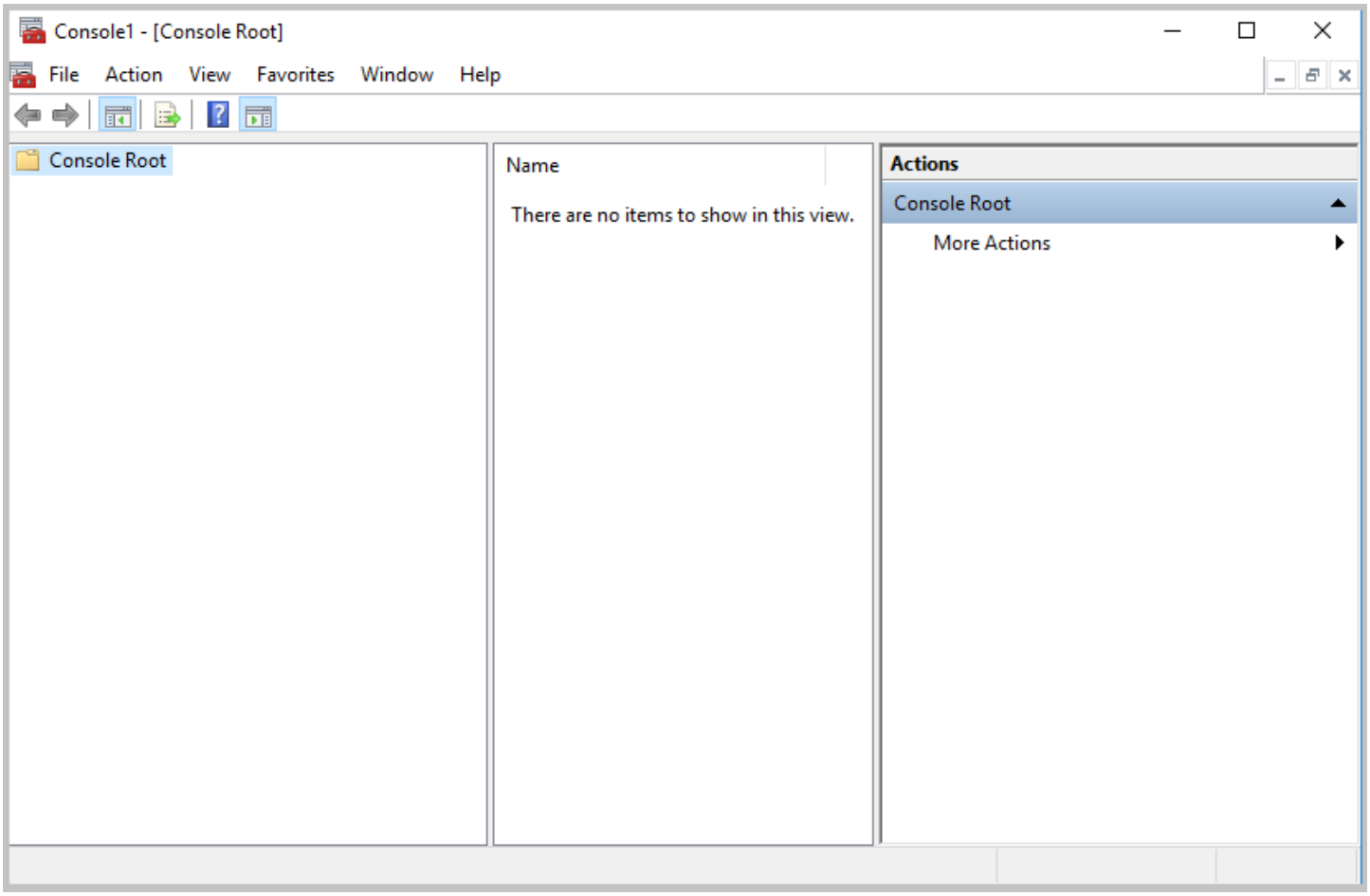


Click Add button to upload the certificate and the related private key, type in the password if needed, and click Save Button. The certificate has been uploaded to the server.

11.2.3.2 Certification Installation to Computer

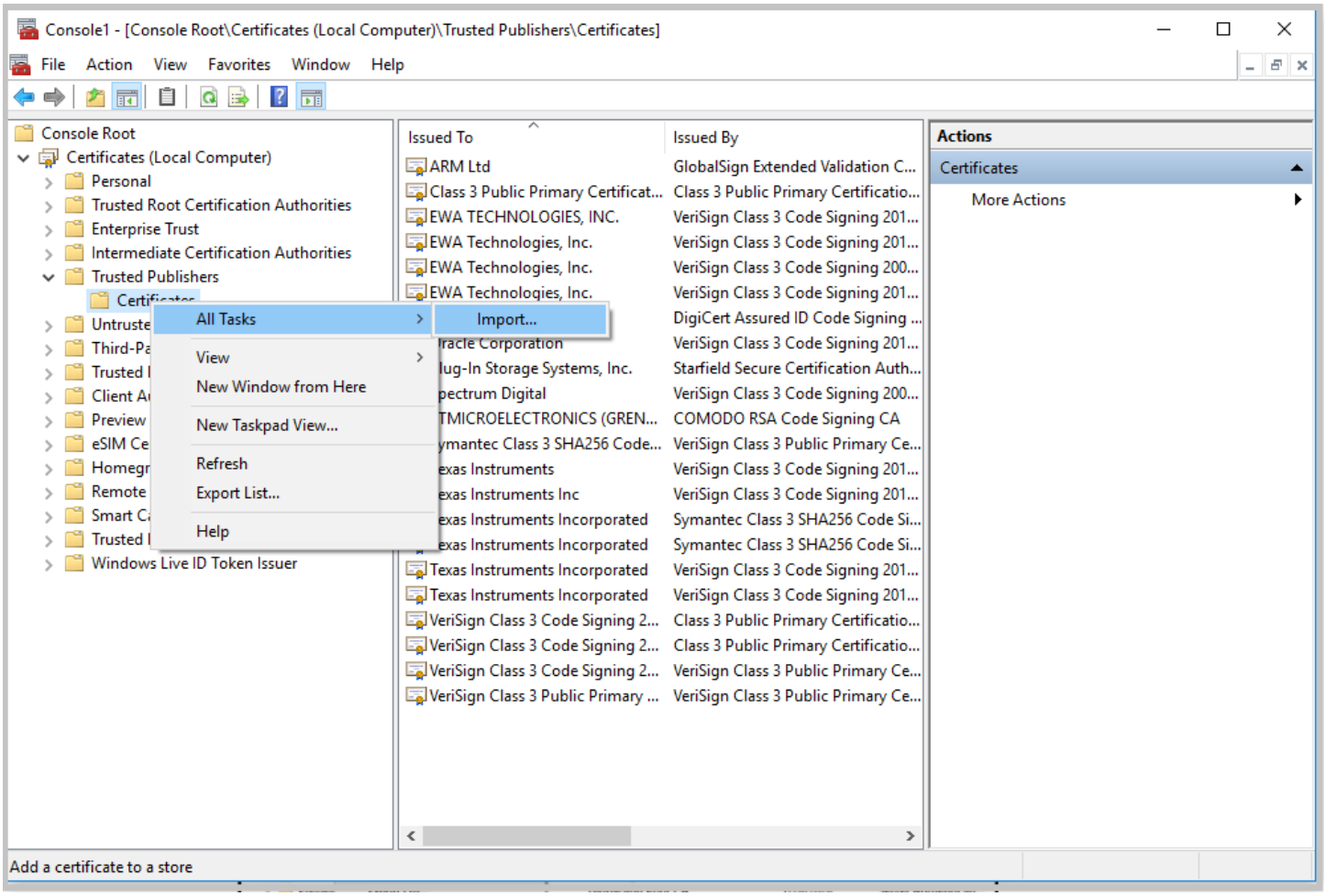
The following is the process of install the certificate to the Computer with Windows 10. The steps are as follows:

Launch MMC by typing Run, and input mmc.exe in the window, the program will start as following:

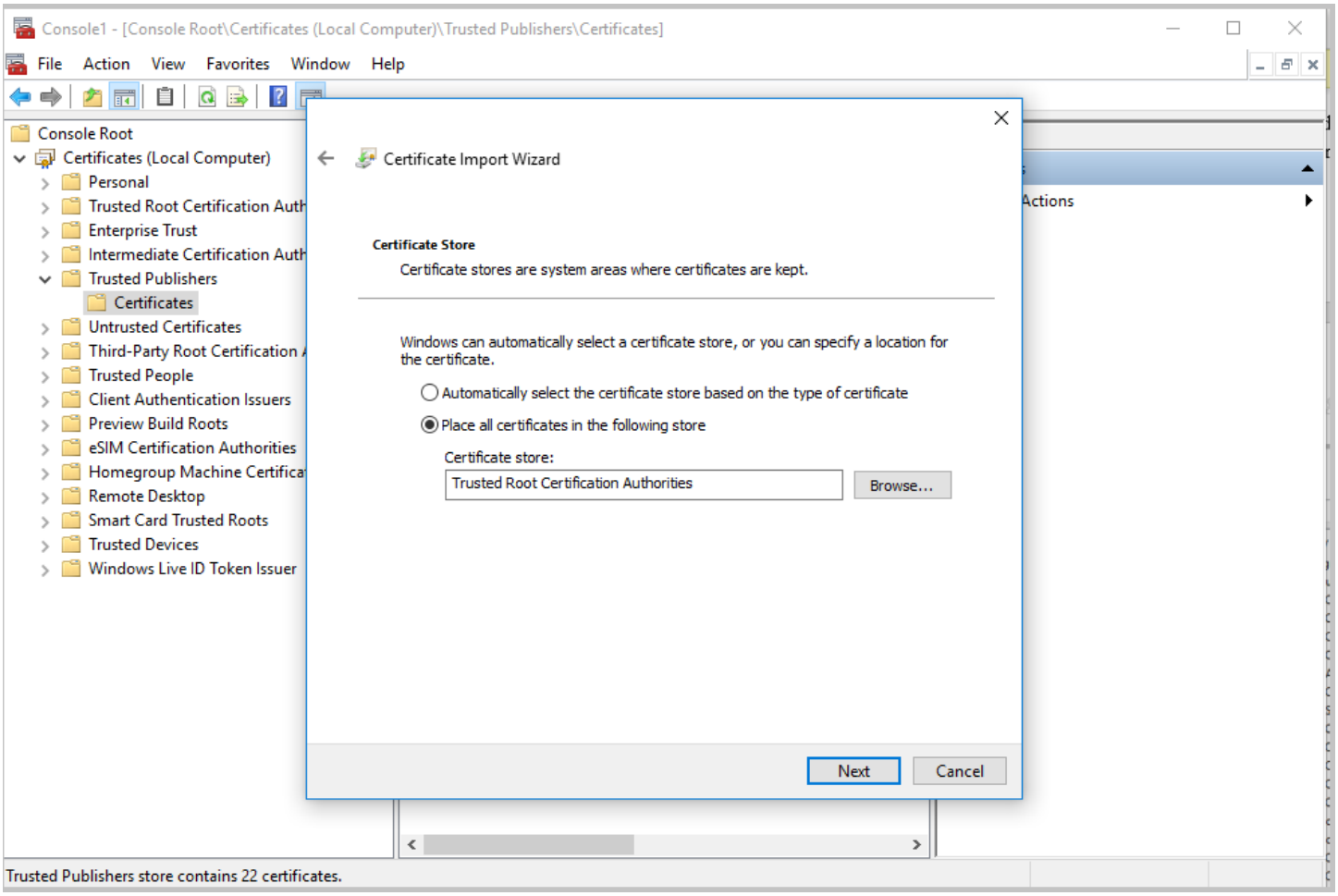


The following is the steps:

- From menu File, choose Add/Remove Snap-in
- Choose Certificate, and press Add
- In the window popped up, choose Computer Account
- In the window popped up, choose Local Computer, and press OK
- The left lane will have a new item Trusted Publishers, right click on the item, from the window popped up, choose All Tasks and then choose Import



- In the popped-up windows choose Next, browse to the location of certificate, then choose Browse and choose Trusted Root Certificate Authorities, Click Next and Finish.
- The computer has been uploaded to the computer now



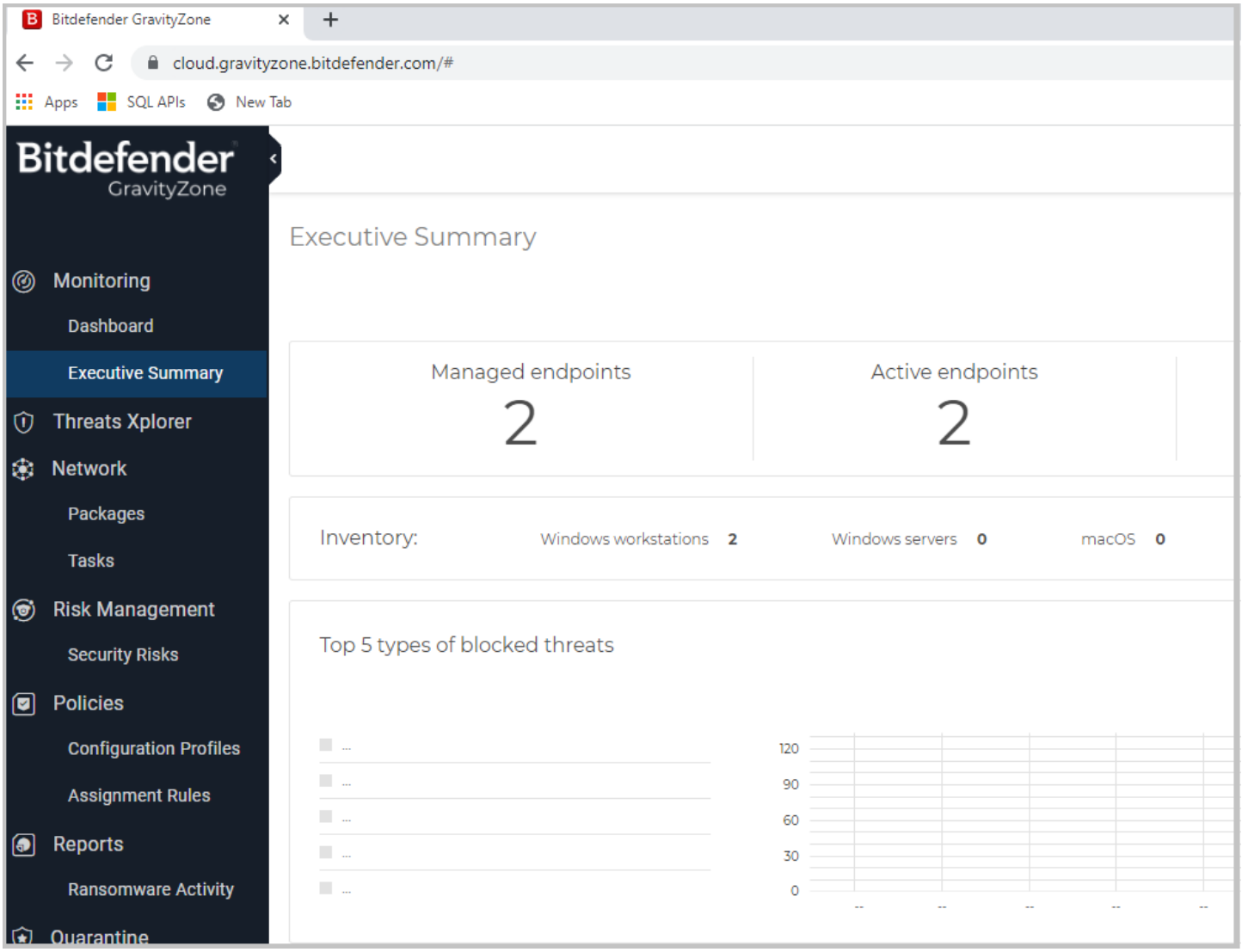
11.3 Security Parameter Setup

A series of parameters needs to be set up to build the network structure. It includes the configuration on the BitDefender server and the setup on CAC-GUI.

11.3.1 Configuration on Server

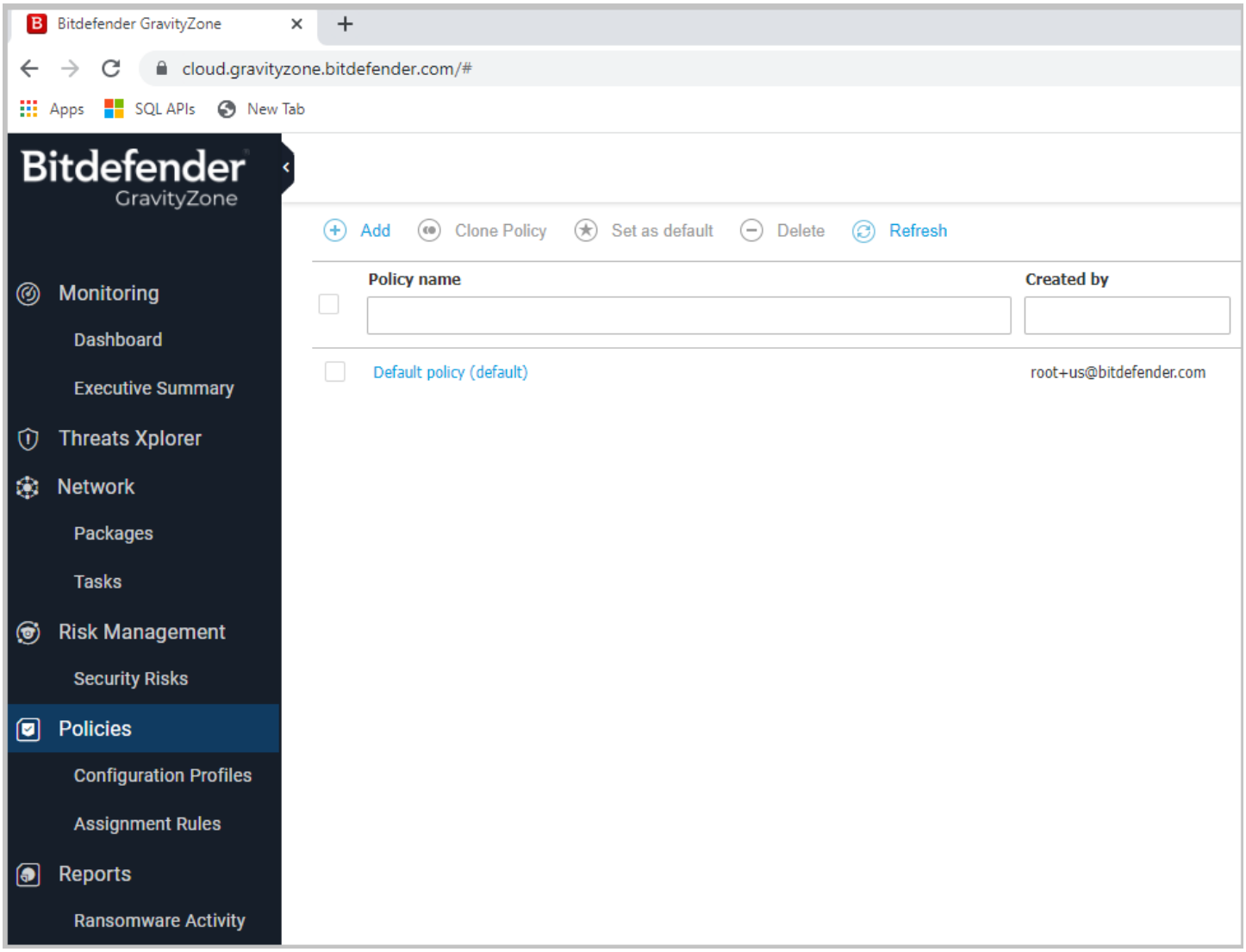
The server's name and the portal in BitDefender is called GravityZone. A profile and an account need to be created to log in to the server, some help from the BitDefender support team might be required to set up the license. The website address for the configuration is: https://gravityzone.bitdefender.com/.

After logging in, the screenshot is as following:

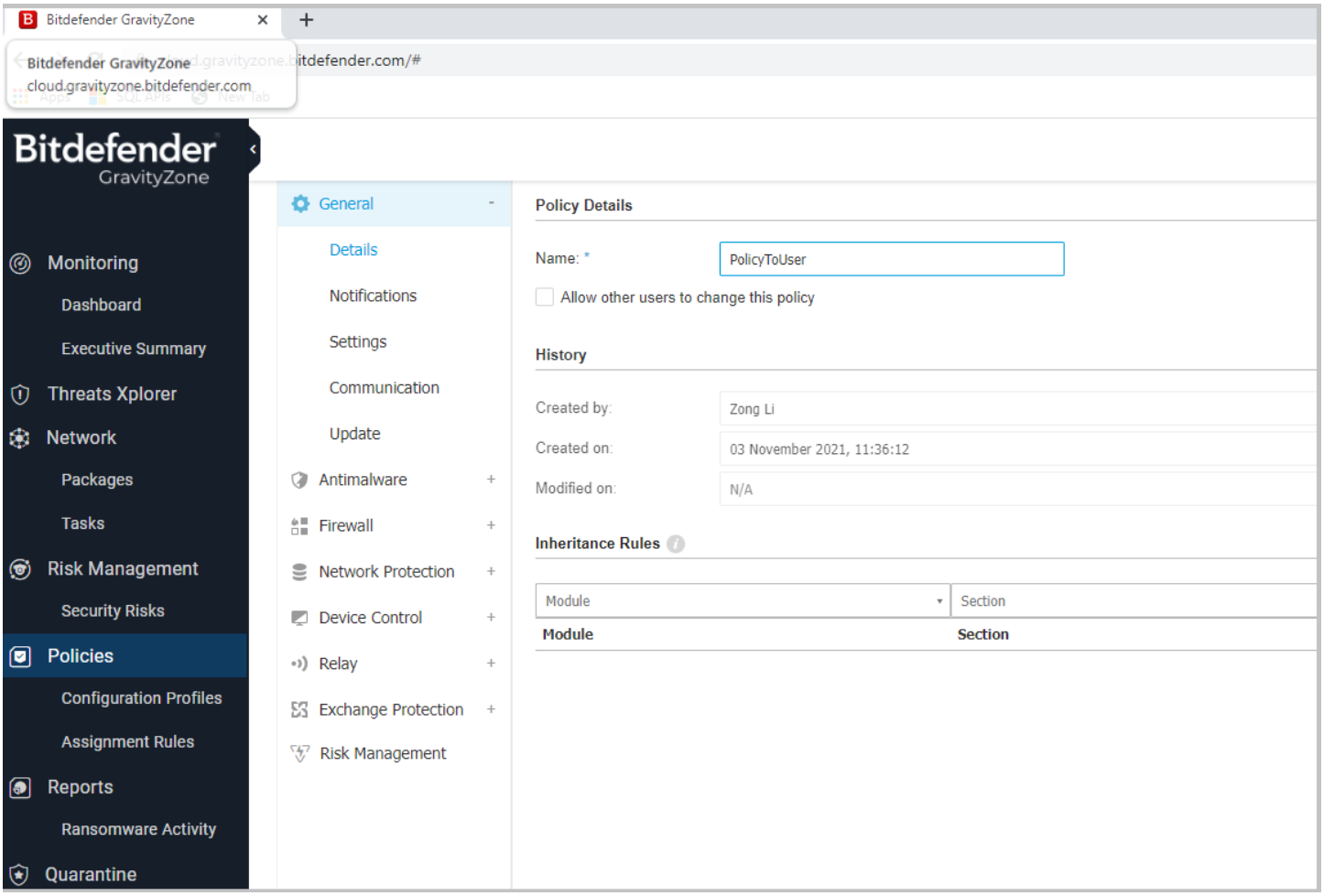


11.3.1.1 Policy Creation

Click Policies on the left pane of the screen to set up the policy for the organization. Policy is a set of rules to monitor and check the endpoints. The following is the screenshot:



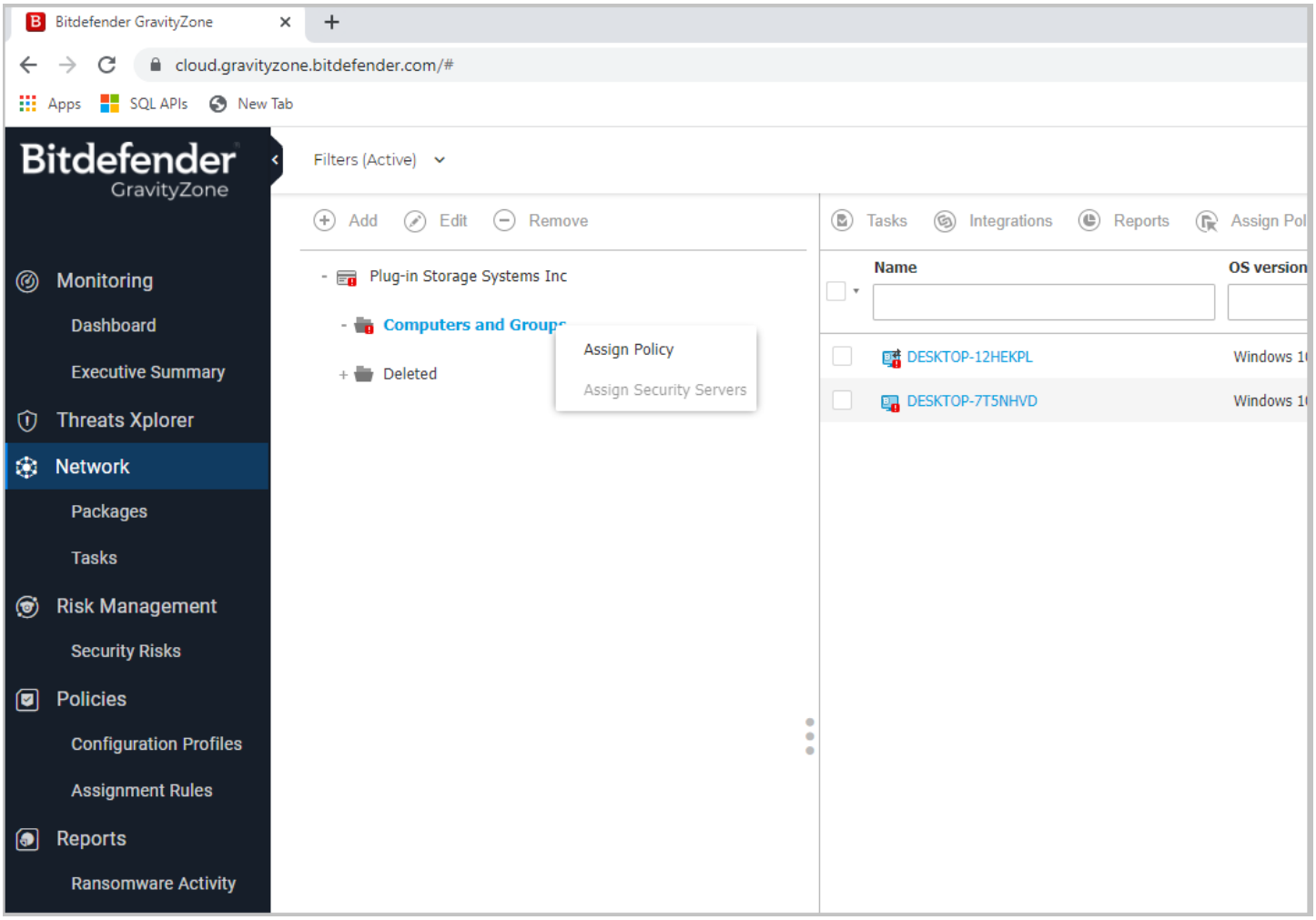
A Default policy is already created for the GravityZone account. Normally the default policy is good enough for the security management, but if the user has the need to create a new policy, can click Add on the top of the screen, a new screen will show up as following.



Choose from the left panel of the screen to set up the details of Update, Antimalware, Firewall, Network Protection, Device Control, Relay, etc. and press the Save button on the bottom of the screen to save them.

11.3.1.2 Policy Assignment

When an account is created, the organization name is already given, and a folder of Computers and Groups is available by default. When the user right clicks the organization name or name of Computers and Group, a small window will pop up to let the user assign the policy name. The following is the screenshot.

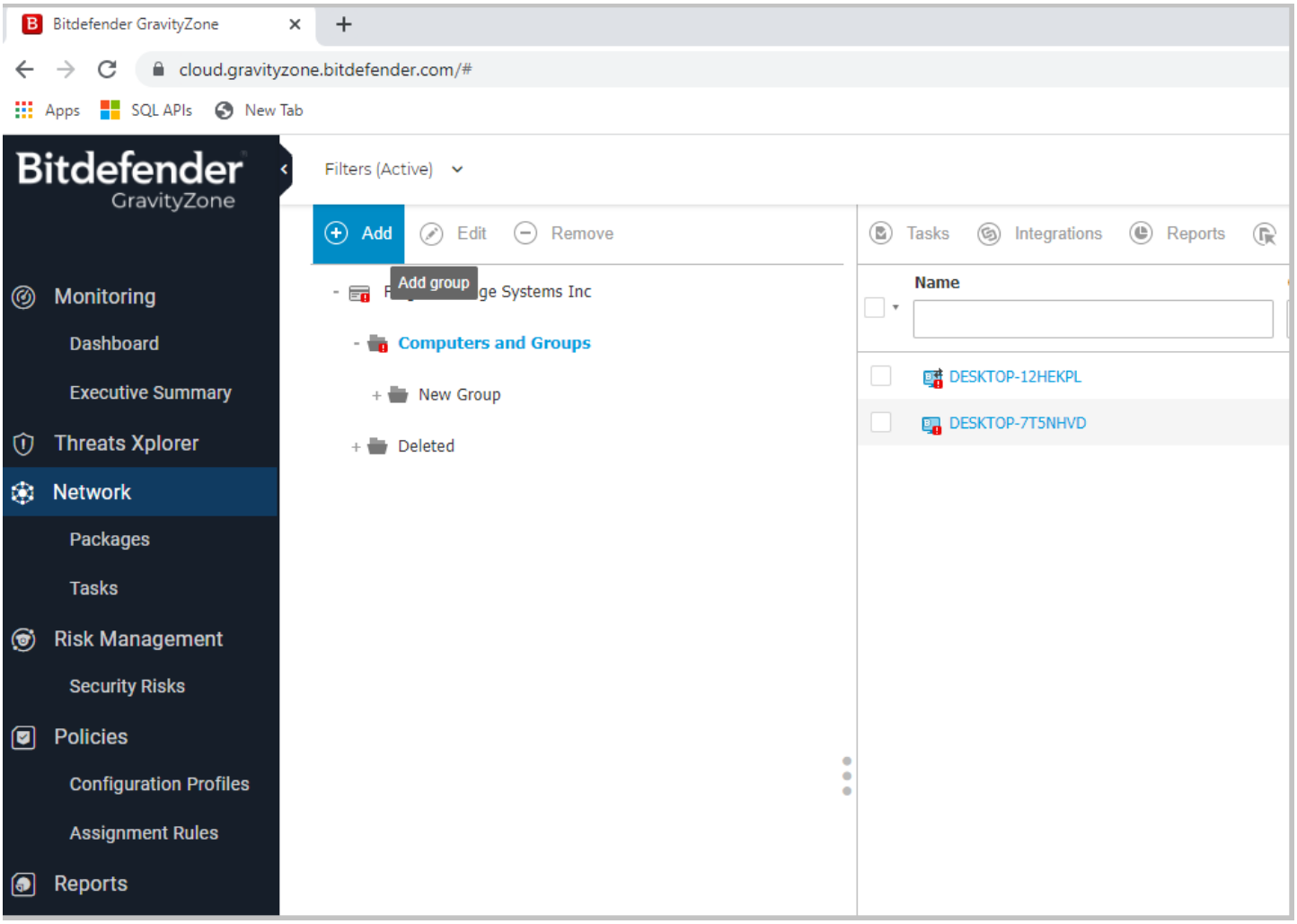


Choose the appropriate policy and all the computers in the folder will following this policy.

11.3.1.3 Group Management

After the policy setup is done, the user can add the endpoints into the group of the organization. If there are too many computers in the organization, some sub-groups can be created under Computer and Groups. For example, if the organization has several cabinets, and each cabinet has different set of laptop computers, the user can create new groups and place the computers of the different cabinet into different groups. Click Add in the screen to add new group.

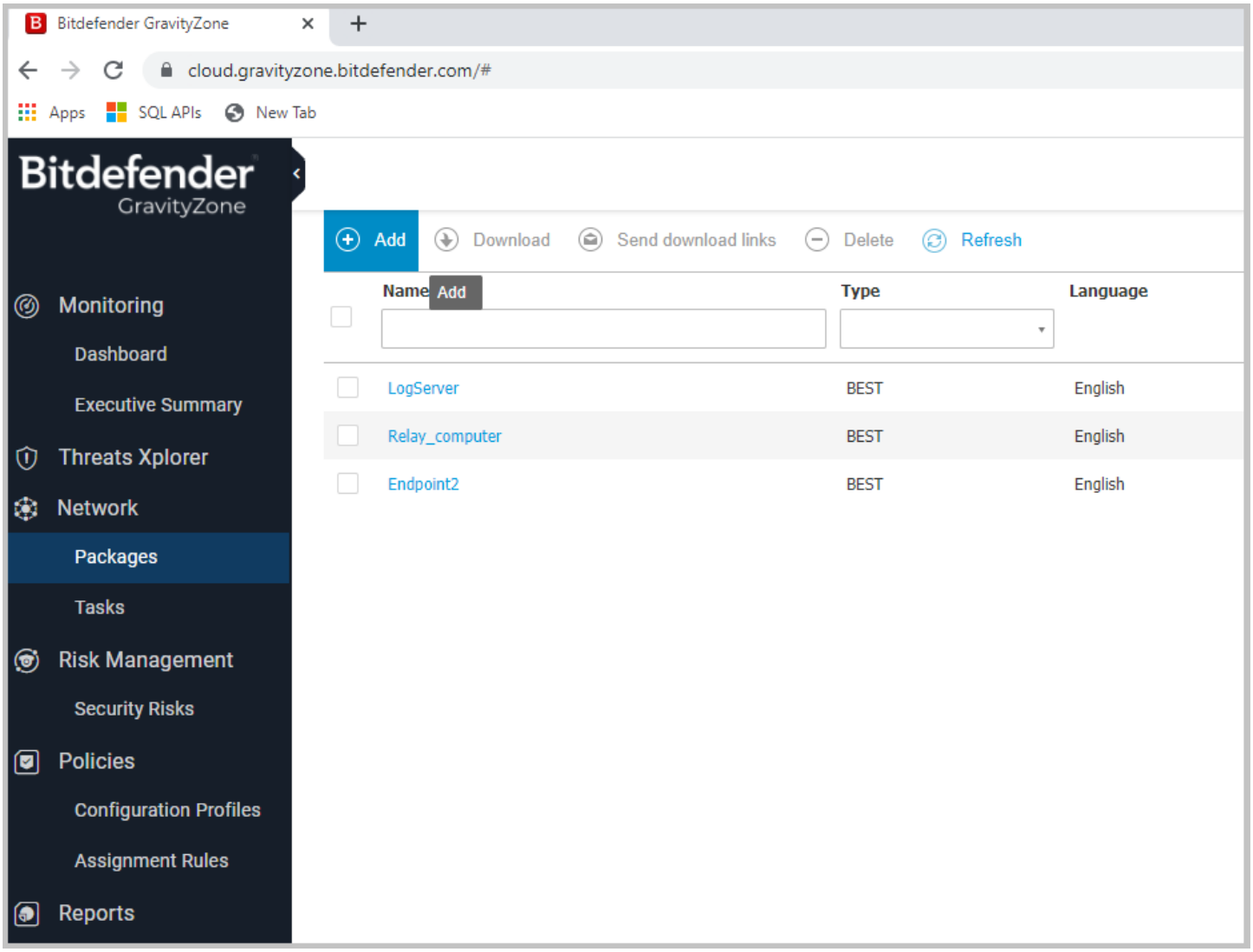
If the user wants to move an endpoint from one group to another group, can use drag-and-drop method to do it.



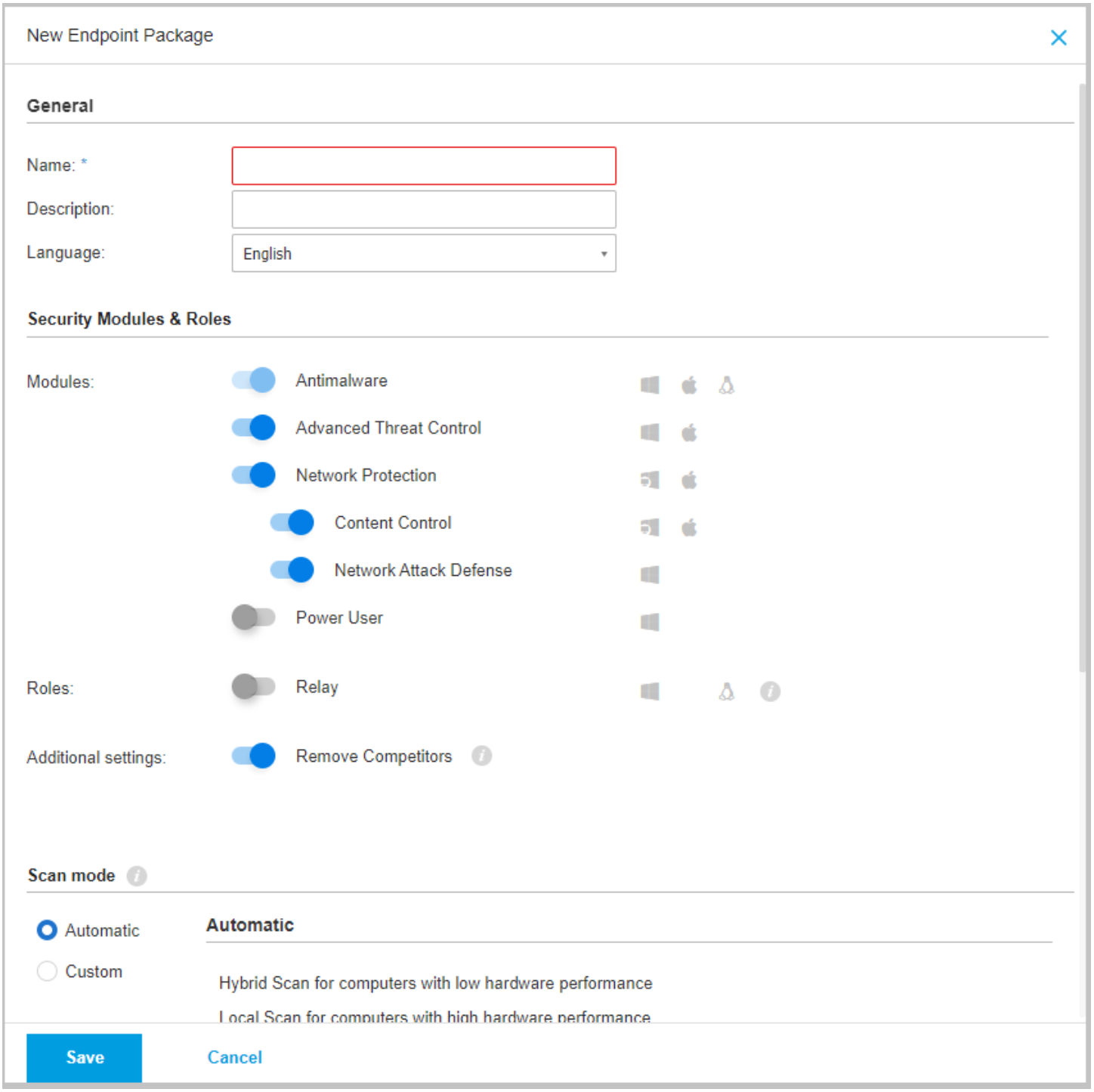
11.3.1.4 Endpoint Adding

After the BitDefender software package is installed to the computer, the endpoint will appear on the network list automatically. The software package can be created with the following steps.

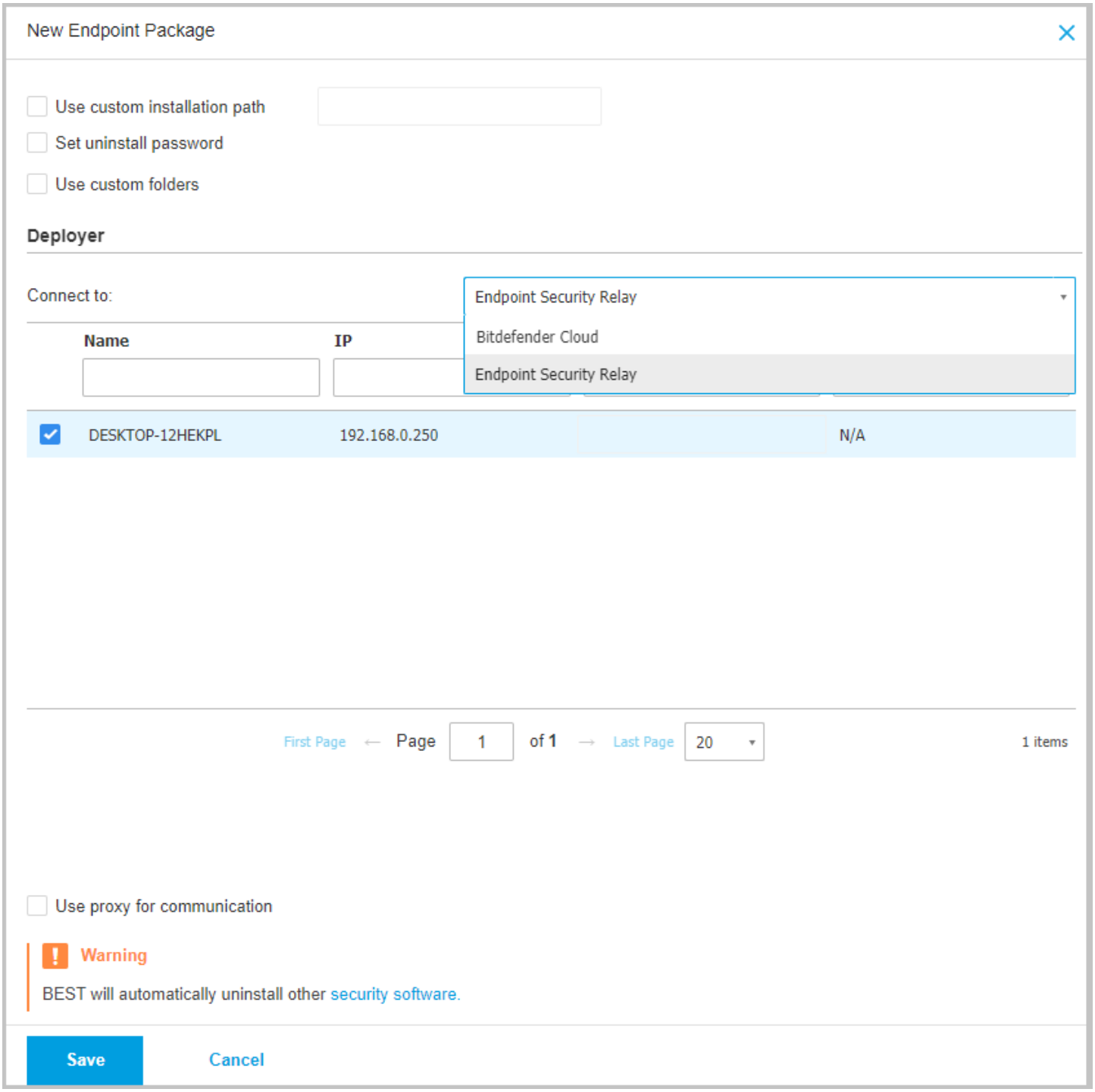
Click Package from the left panel, then click Add on top of the screen. The following is the screenshot:



After clicking Add button, a screen will show up as following. Fill in the blanks and select the appropriate option. Be attention to Relay option for the Role setup, if Relay is chosen, this package is for the relay computer; otherwise, it is for the other computers (such as laptop computer) in the cabinet.



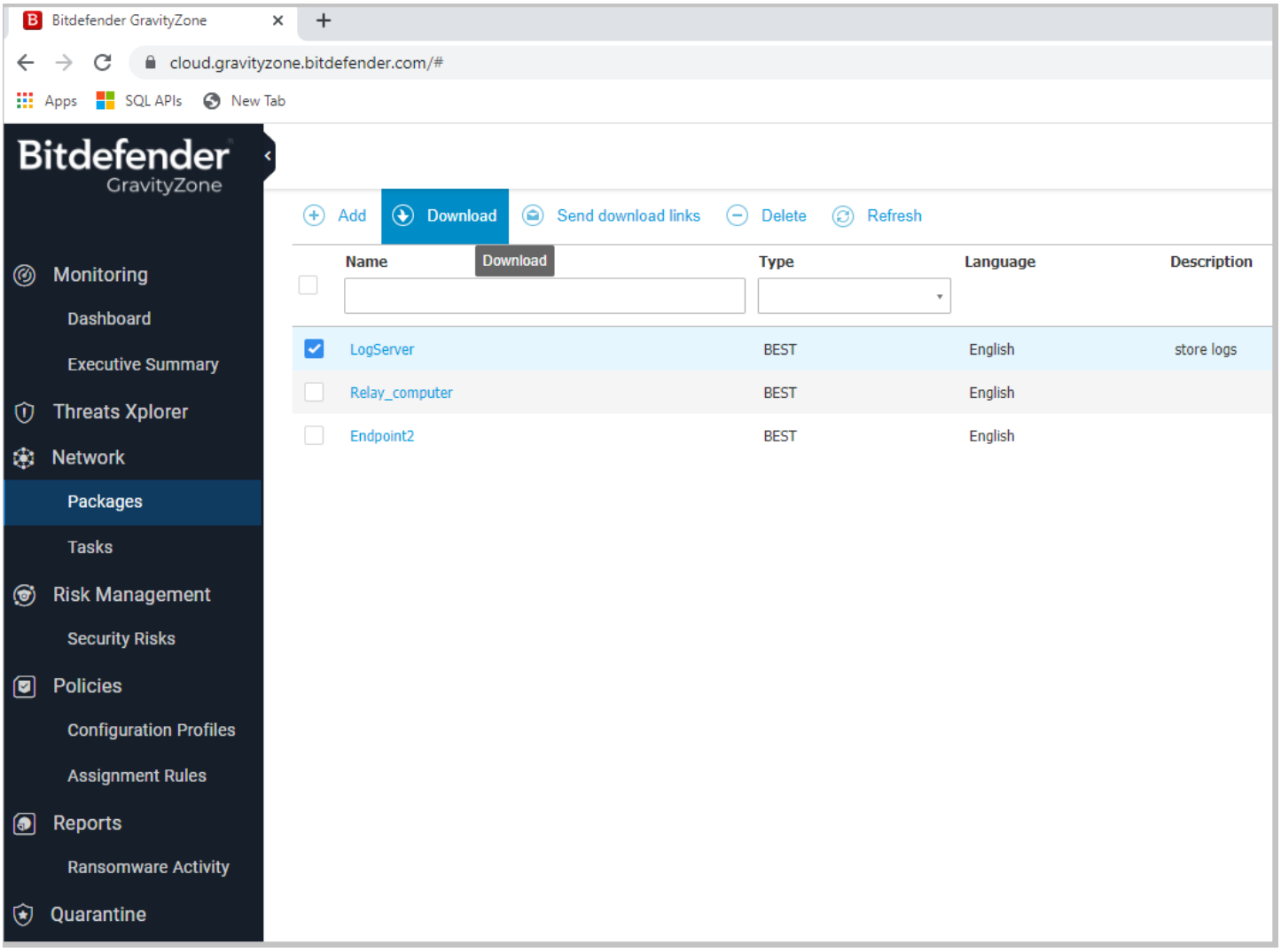
Move the vertical progress bar to see the bottom part of the screen as following:



In the Deployer section, if choosing Endpoint Security Relay, the package update can be done through the relay computer, be careful when selecting the relay endpoint in the list; it needs to match the information of the relay computer

After all the information are setup, press Save button to create the package.

Click Package from the left panel, a new window will appear. Select the appropriate package, and Press Download, and the installer will be downloaded to the local computer.

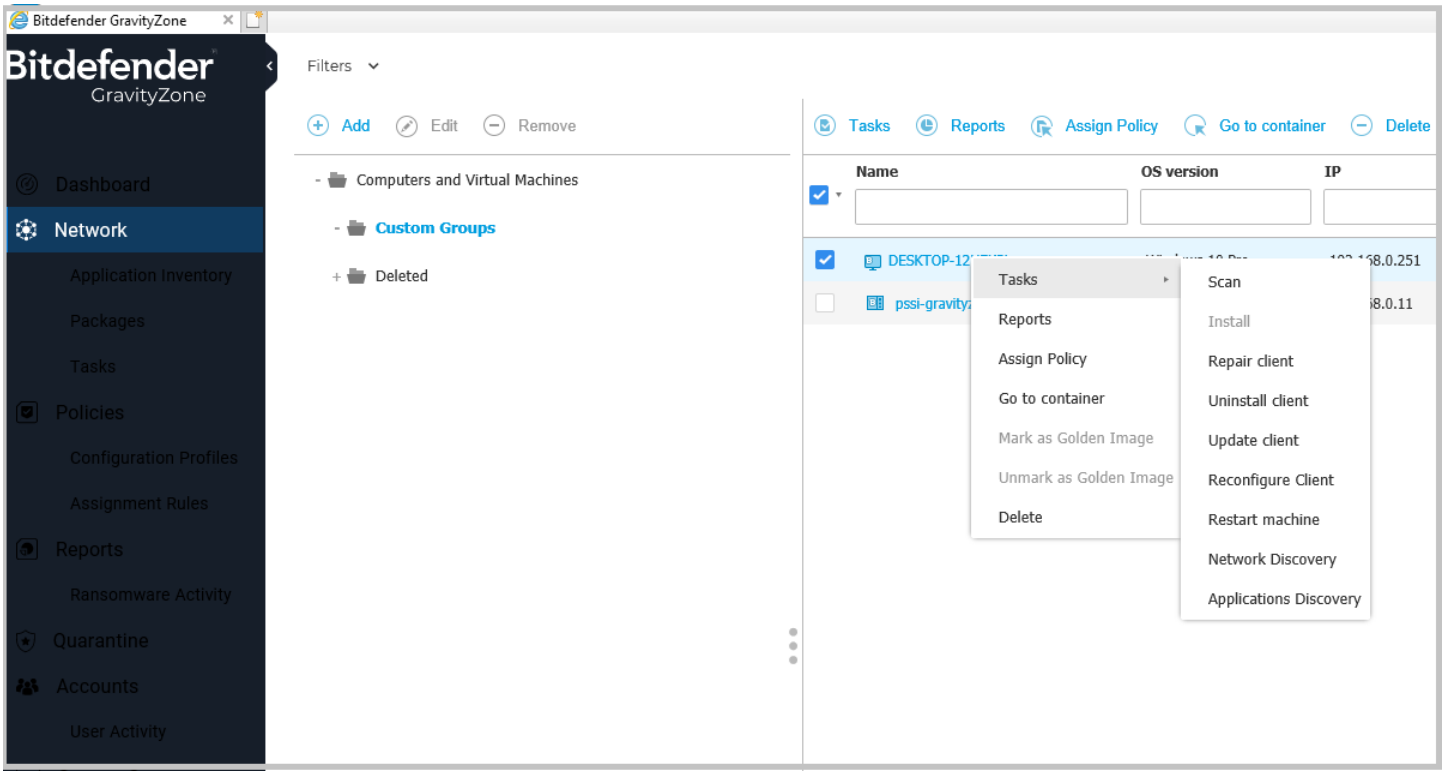


After the downloading is done, copy the package to the endpoint computer and install the software.

11.3.1.5 Package Remote Deploy

The security agent can also be deployed to the computer remotely. The steps are as follows:

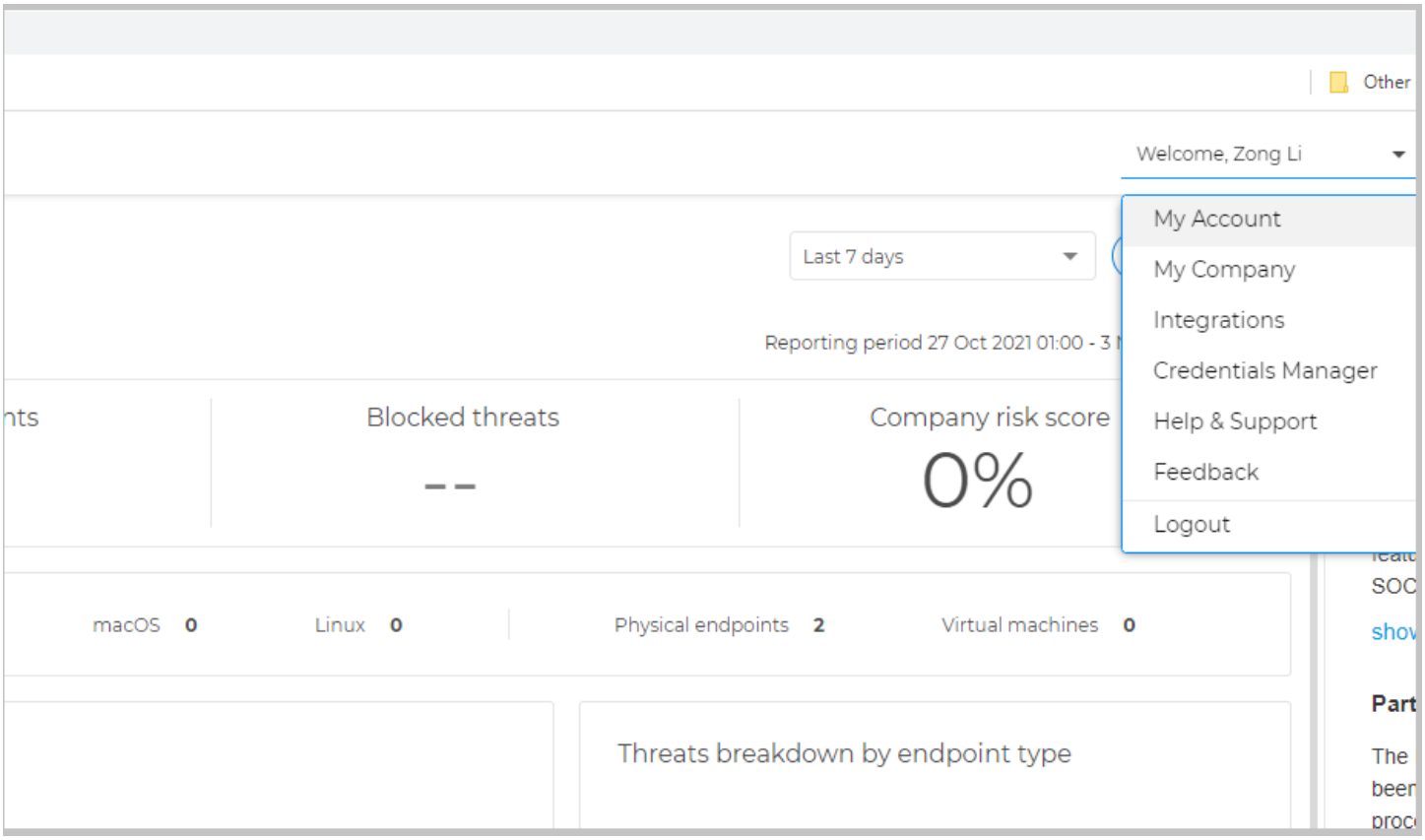
Login to Control Center, from the left lane, choose Network, browse to the endpoint to which you want to install the package, right click on it, from the window choose tasks, and then choose Install, find the package you want to install, and click Save, the installation process will soon start. The following is a screenshot:



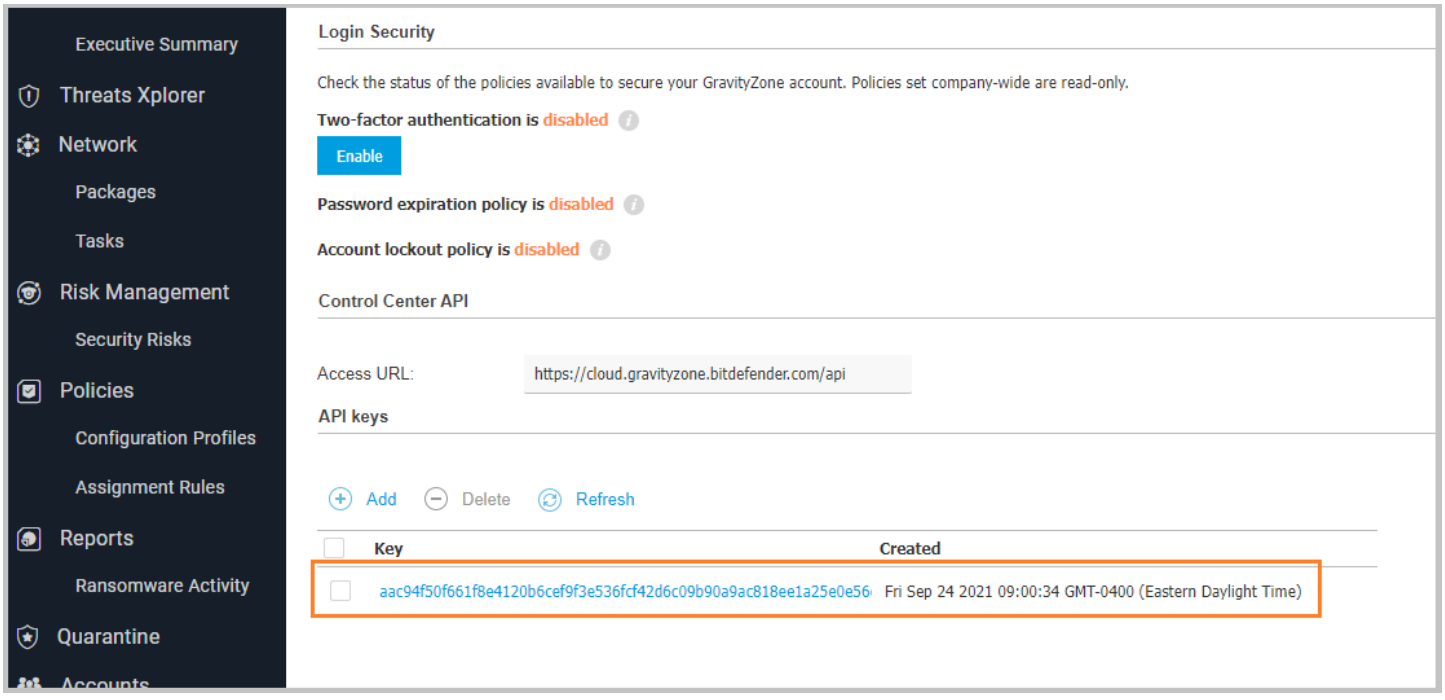
11.3.1.6 API Type Choosing

The program in the cabinet needs the APIs to communicate with the GravityZone server, The API can be configured with the following steps.

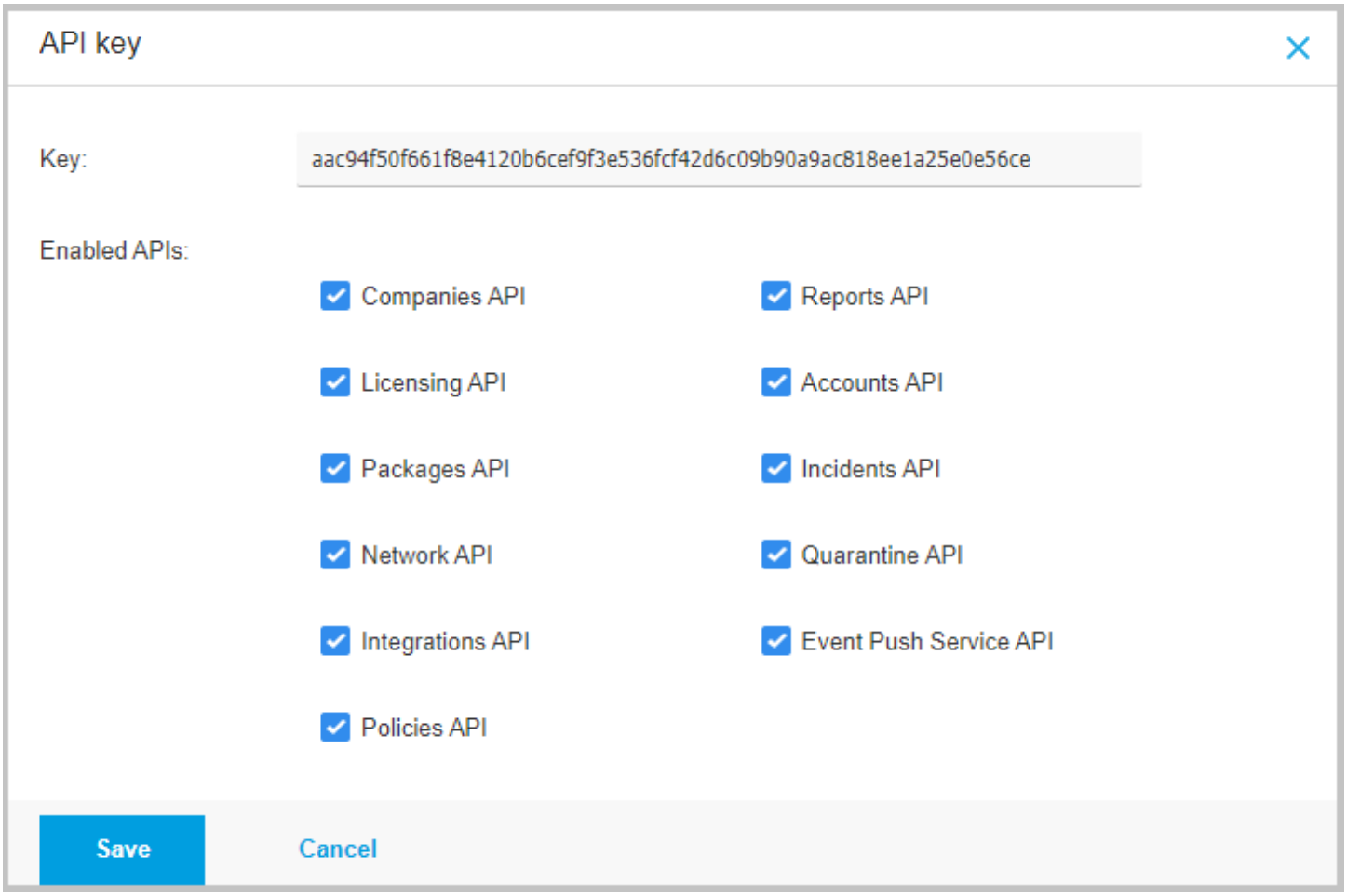
From the pull-down menu of the profile, choose My Account, and a new window will appear.



In the new window, the API keys section list all the API sets. The user can add other API sets by clicking Add, but normally the default key set is sufficient to cover all the API usage.



Press one set of keys (circled with orange frame in the image) to set up more details. A new window will pop up as following.



Normally we will enable all the APIs, but specifically we need to make sure Companies API, Reports API and Network API are selected.

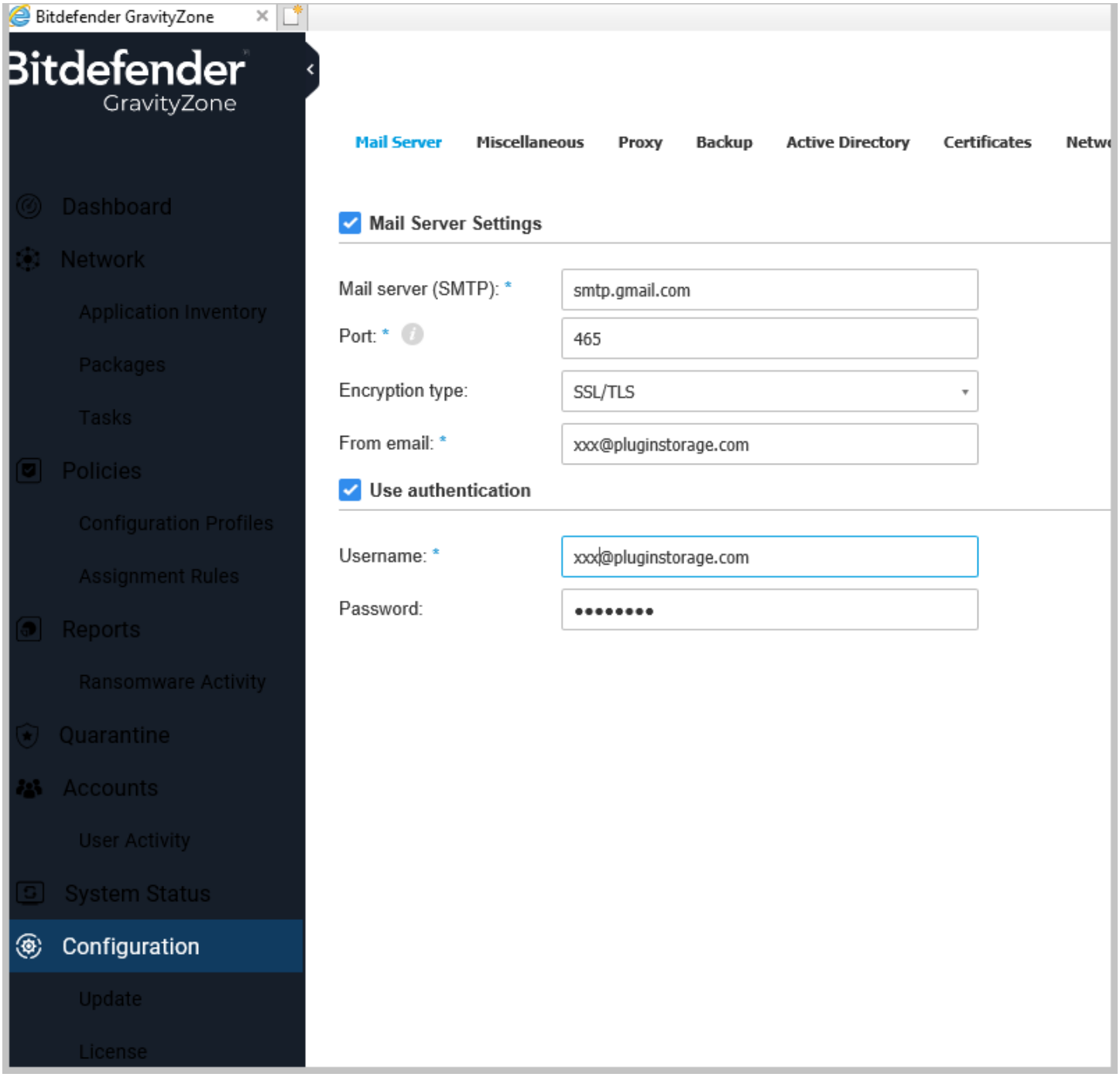
Pay attention to the Key value, it will be required in later section of this manual for CAC-GUI setup.

11.3.1.7 Email Server Setup

When there is some problem in the Security Server or the Security Network, Control Center will send out email to information the administrator by email.

The email for the administrator can be configured as follows:

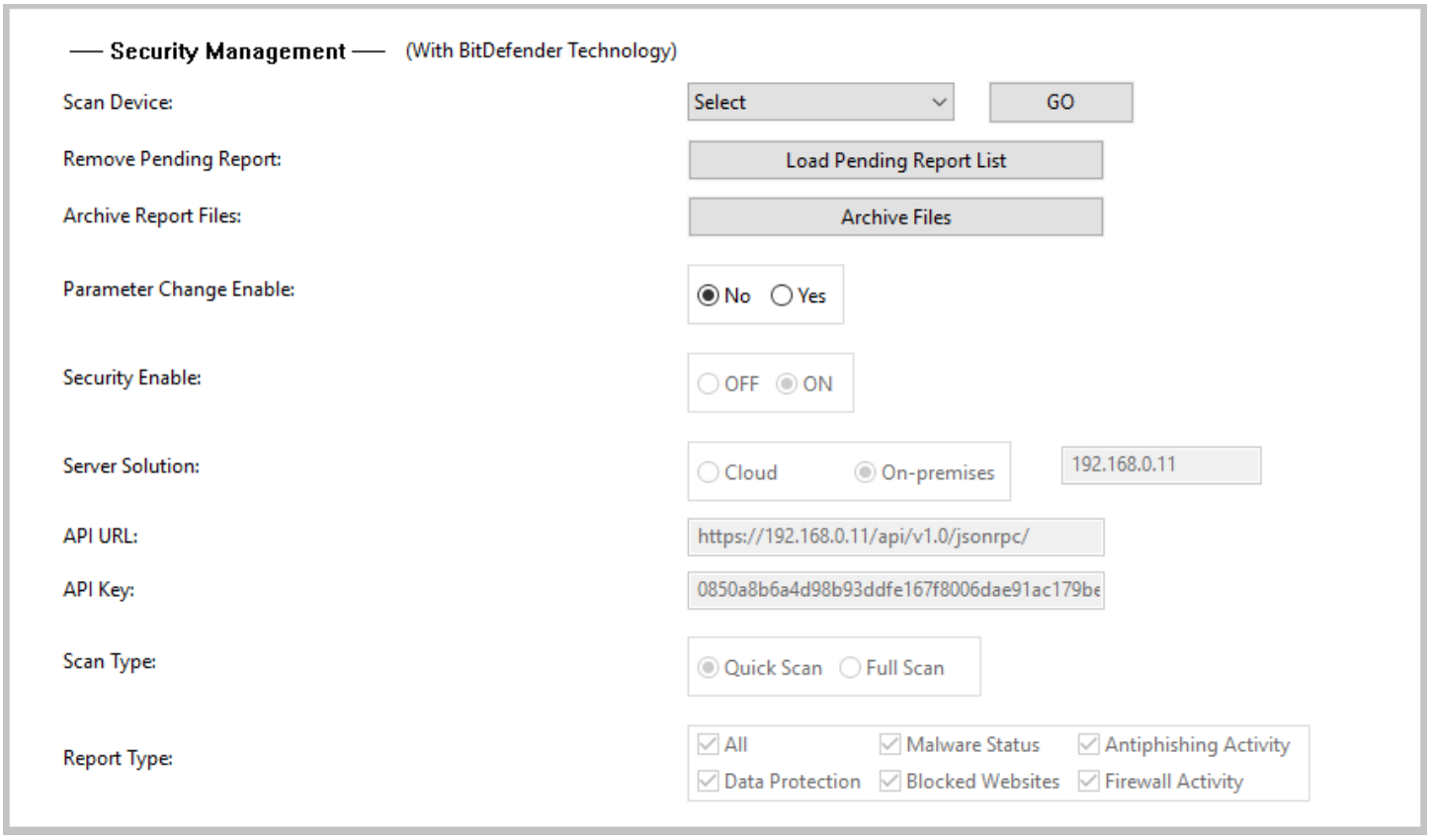
Log in to Control Panel, and choose Configuration from left pane, by default the right section of the screen will display the setup of email server. The following is a screenshot:



Fill in the value about the mail server and the user authentication; and click Save button. And the email server has been configured.

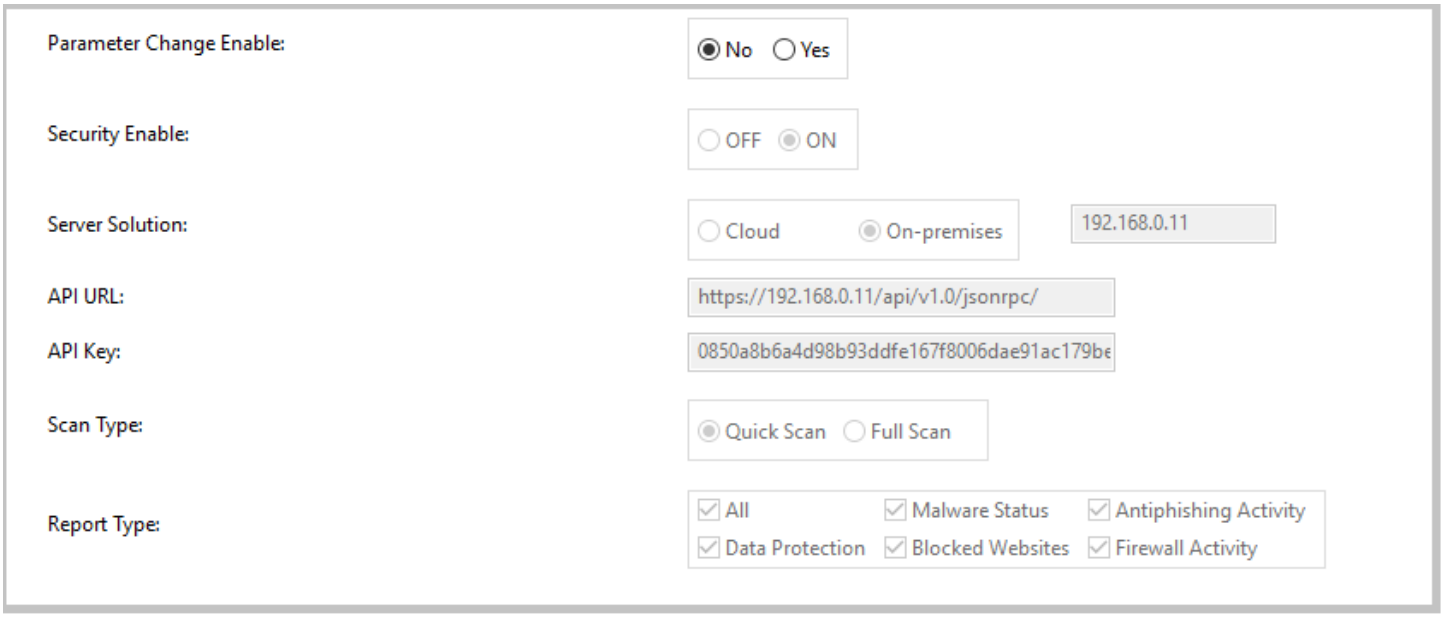
11.3.2 Configuration On CAC-GUI

Some parameters in CAC-GUI need to be set up in order to use the security function. It is in the System Config tab. The following is the screenshot.



The section in the blue frame is related to the security parameter setup. The following is the detailed description for each parameter.

Parameter Change Enable is for the protection of the security parameters. Normally it is set to No, and therefore the related security parameters are disabled. When the user clicks Yes, a window will pop up to confirm the action. The window looks like following:



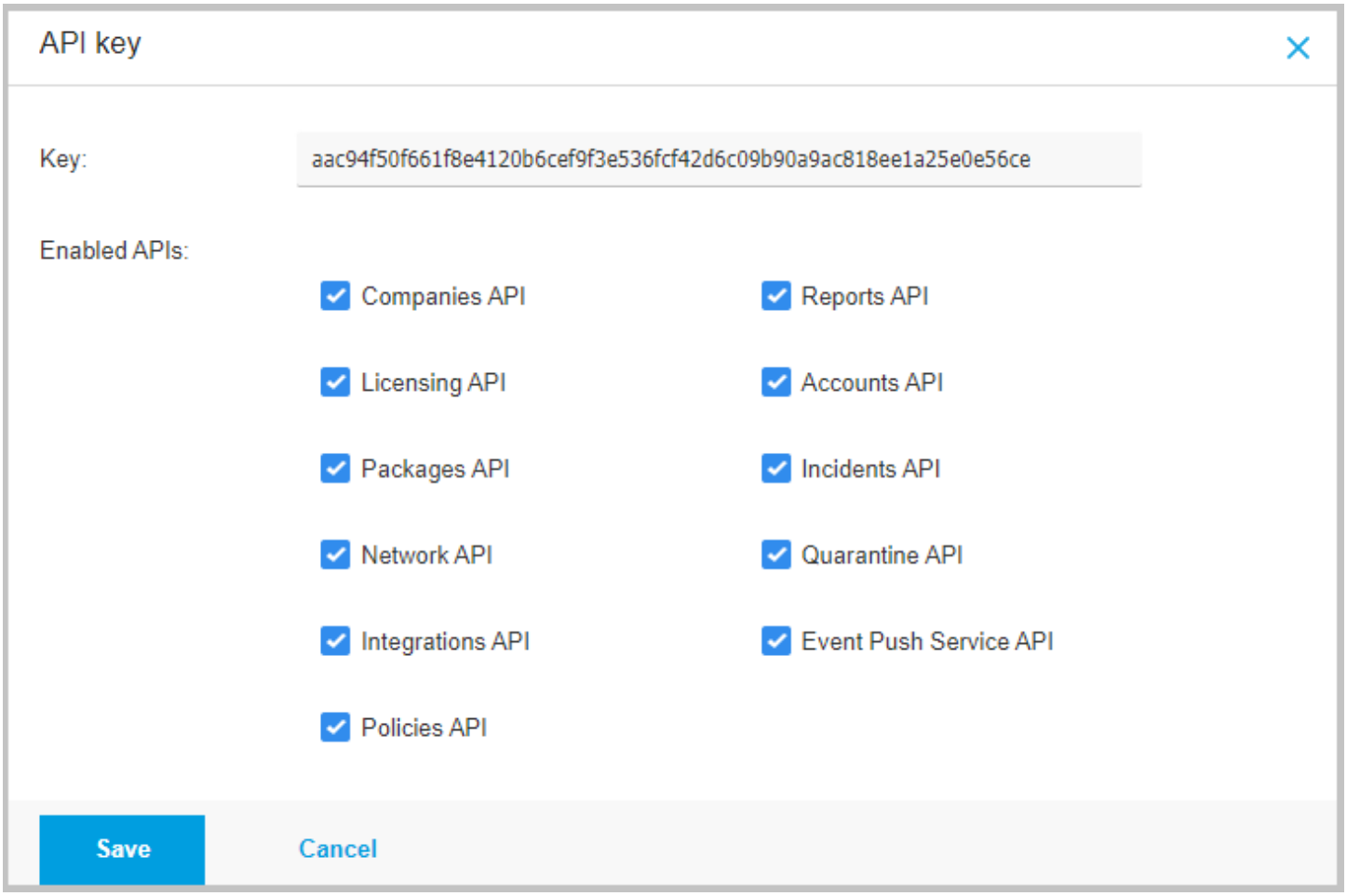
Press Yes and the parameter setup will become enabled; the user can therefore modify the parameters.

Security Enable is the switch for the security feature. If it is ON, all the security functions discussed in this chapter are available; otherwise, all the functions are disabled. The default selection for this parameter is OFF.

Server Solution is about the selection of server location. If it is Cloud, the security server of BitDefender is used; if it is On-premises, a local security server needs to be setup, and the IP address of the local server can be filled in the following field.

API URL is the webpage address that the security APIs communicate with. The default address is https://cloud.gravityzone.bitdefender.com/api/v1.0/jsonrpc/; it may change when BitDefender updates their API version.

API Key is the authorization string when the API communicates with the server. It needs to be copied from the GravityZone portal discussed in section 11.2.1.5. The screenshot is also copied to the following:

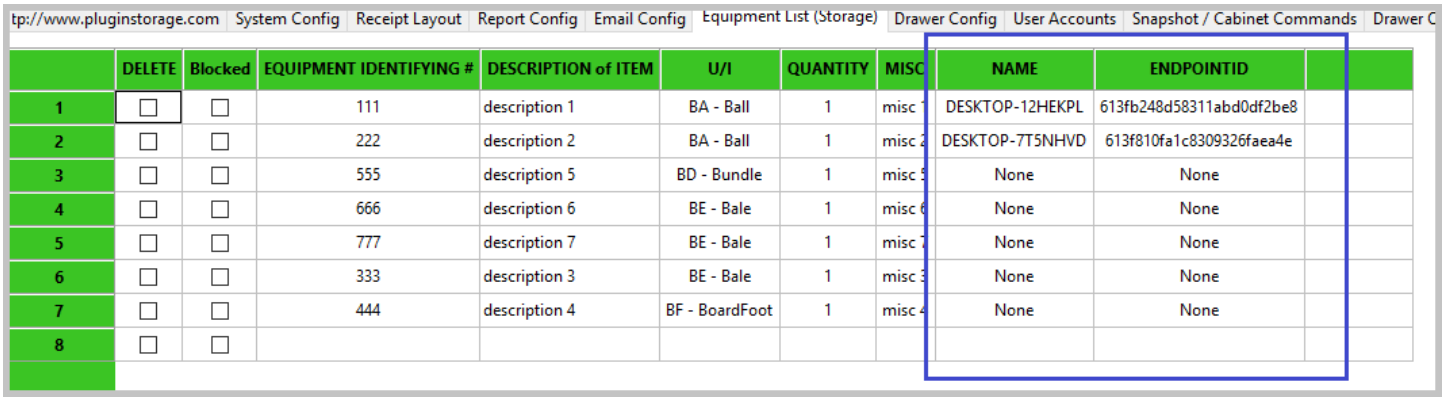


Scan Type is the type of the scan to the endpoints. Normally Quick Scan is good enough to read the malware status and generate the report.

Report Type is a set of selections to the type of the report, it includes Malware Status, Antiphishing Activity, Data Protection, Blocked Websites, and Firewall Activities. Usually just chose All to include all the reports.

11.4 Setup on Equipment List

When the security function is enabled, there will be two more columns appeared in the Equipment List tab; the names of the two columns are NAME and ENDPOINTID. The following is the screenshot. The two new columns are the ones in blue frame.



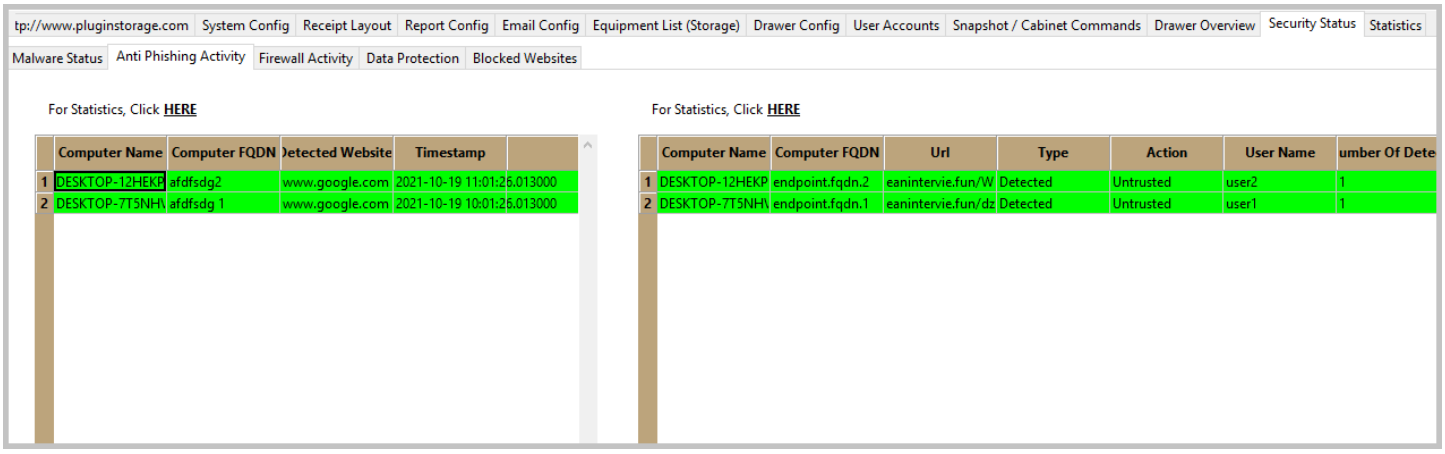
	DELETE	Blocked	EQUIPMENT IDENTIFYING #	DESCRIPTION of ITEM	U/I	QUANTITY	MISC	NAME	ENDPOINTID
1	☐	☐	111	description 1	BA - Ball	1	misc 1	DESKTOP-12HEKPL	613fb248d58311abd0df2be8
2	☐	☐	222	description 2	BA - Ball	1	misc 2	DESKTOP-7T5NHVD	613f810fa1c8309326faea4e
3	☐	☐	555	description 5	BD - Bundle	1	misc 5	None	None
4	☐	☐	666	description 6	BE - Bale	1	misc 6	None	None
5	☐	☐	777	description 7	BE - Bale	1	misc 7	None	None
6	☐	☐	333	description 3	BE - Bale	1	misc 3	None	None
7	☐	☐	444	description 4	BF - BoardFoot	1	misc 4	None	None
8	☐	☐							

NAME column is the name of the laptop computer, it can be copied from Control Panel -> System and Security -> System. This is the unique readable identification for the laptop computer used for the security functionality.

ENDPOINTID is the identification for security API and other functions, this value can be left empty during the initial setup, and the program will fill it up when the cabinet start running. The endpoint ID will be used in the security functions for the identification of the computers.

11.5 Real Time Display of Security

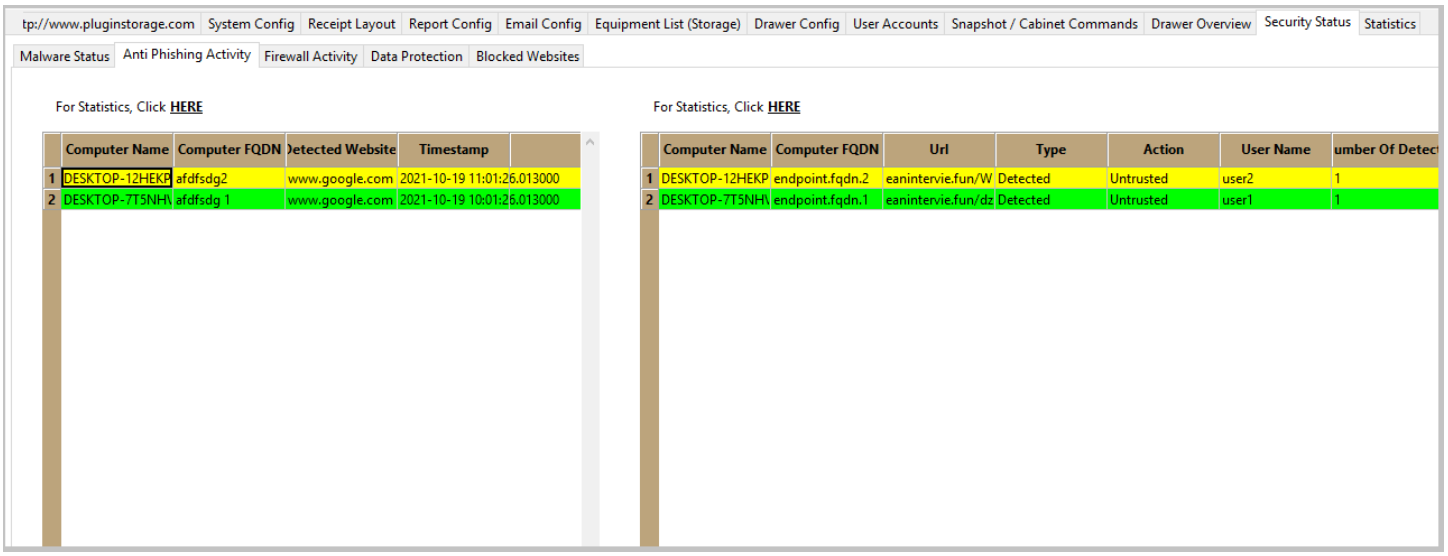
When Security function is enabled, a new tab called Security Status will appear in the CAC-GUI screen. The Security Status tab includes five sub-tab that corresponding to five types of reports. The following is the screenshot.



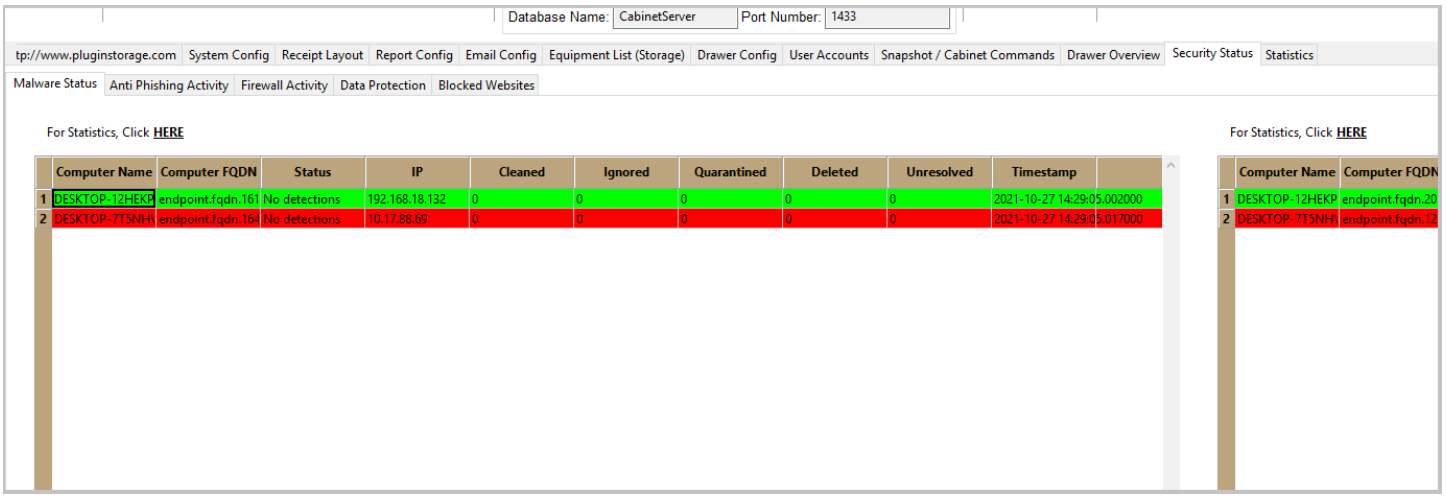
The display order for the list of the computer is the same as the order in Equipment List tab, the data of the tables are read from the reports after the scan for the related device has finished. If there is no malware or attempted attack happened, there will be no record written to the database and no new data are displayed in the GUI.

11.5.1 Scan Status

Normally the display of a device is in green, it means there is no scanning going on for this device. When a device is scanning for malware, the related item will become yellow.

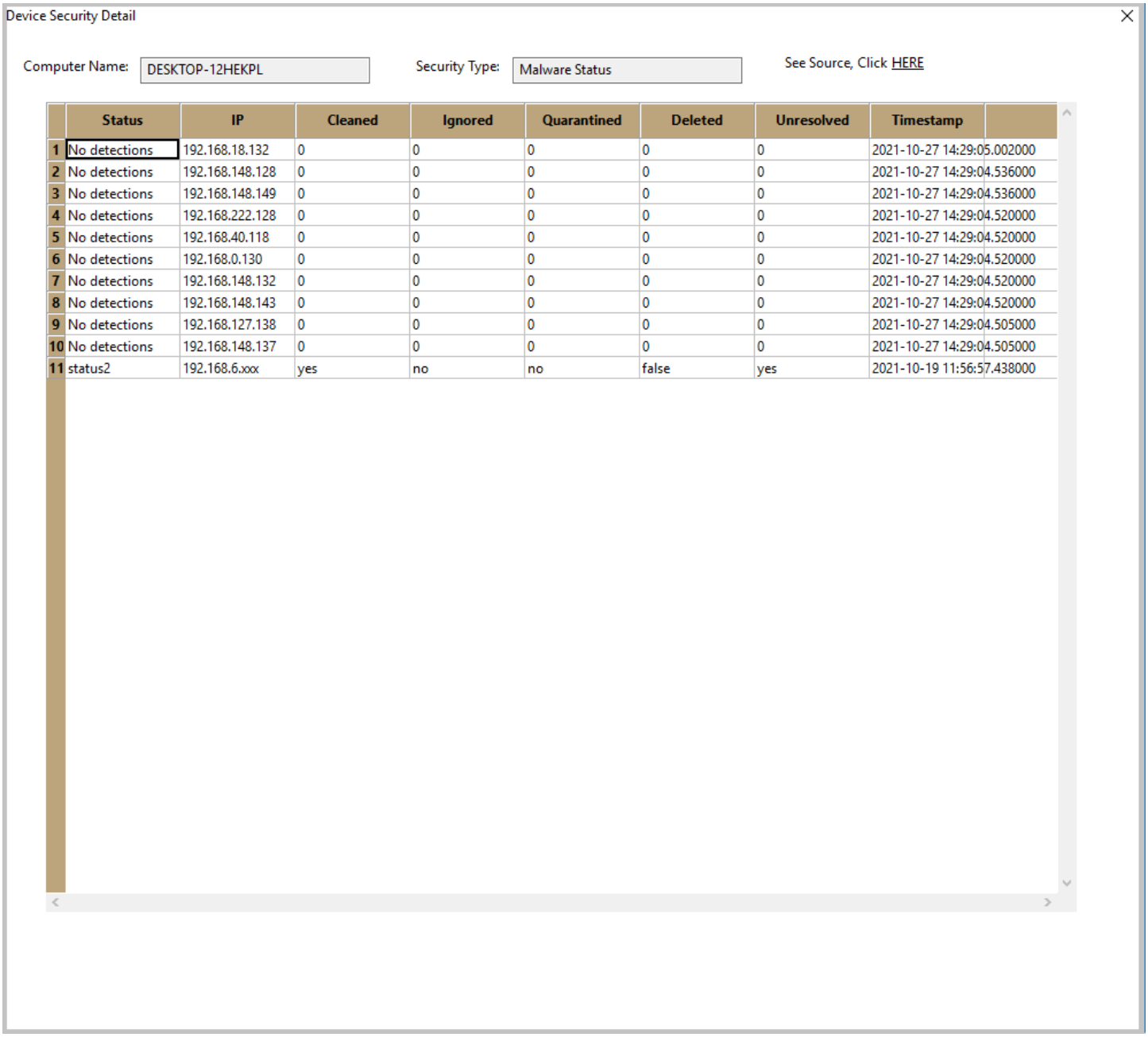


When malware is found in a device, the related line will become red.



11.5.2 Scan History

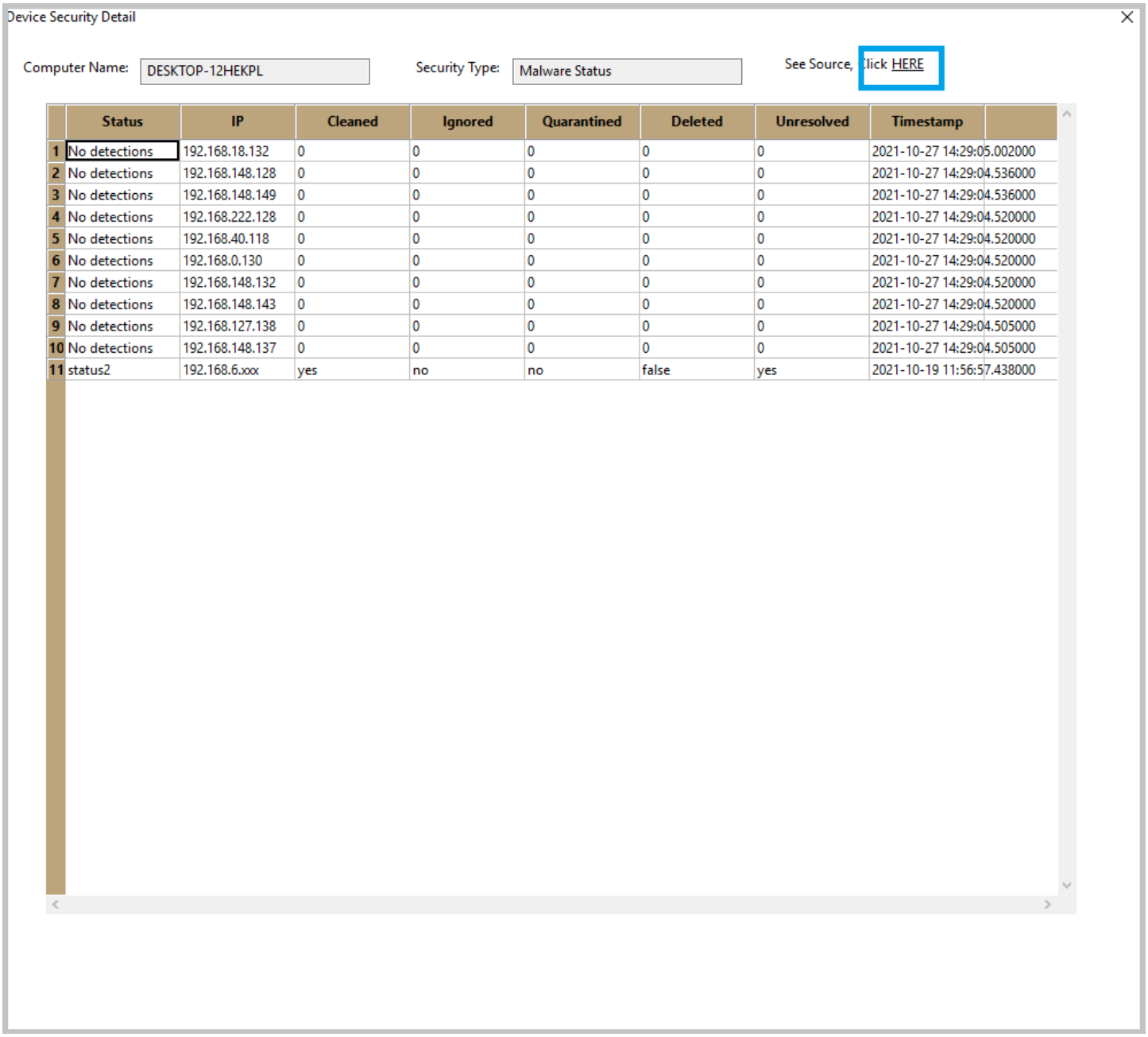
When clicking a specific line in the table in Security Status tab, a window will pop up to display the scan history of the device and the related table. The following is a screenshot.



	Status	IP	Cleaned	Ignored	Quarantined	Deleted	Unresolved	Timestamp
1	No detections	192.168.18.132	0	0	0	0	0	2021-10-27 14:29:05.002000
2	No detections	192.168.148.128	0	0	0	0	0	2021-10-27 14:29:04.536000
3	No detections	192.168.148.149	0	0	0	0	0	2021-10-27 14:29:04.536000
4	No detections	192.168.222.128	0	0	0	0	0	2021-10-27 14:29:04.520000
5	No detections	192.168.40.118	0	0	0	0	0	2021-10-27 14:29:04.520000
6	No detections	192.168.0.130	0	0	0	0	0	2021-10-27 14:29:04.520000
7	No detections	192.168.148.132	0	0	0	0	0	2021-10-27 14:29:04.520000
8	No detections	192.168.148.143	0	0	0	0	0	2021-10-27 14:29:04.520000
9	No detections	192.168.127.138	0	0	0	0	0	2021-10-27 14:29:04.505000
10	No detections	192.168.148.137	0	0	0	0	0	2021-10-27 14:29:04.505000
11	status2	192.168.6.xxx	yes	no	no	false	yes	2021-10-19 11:56:57.438000

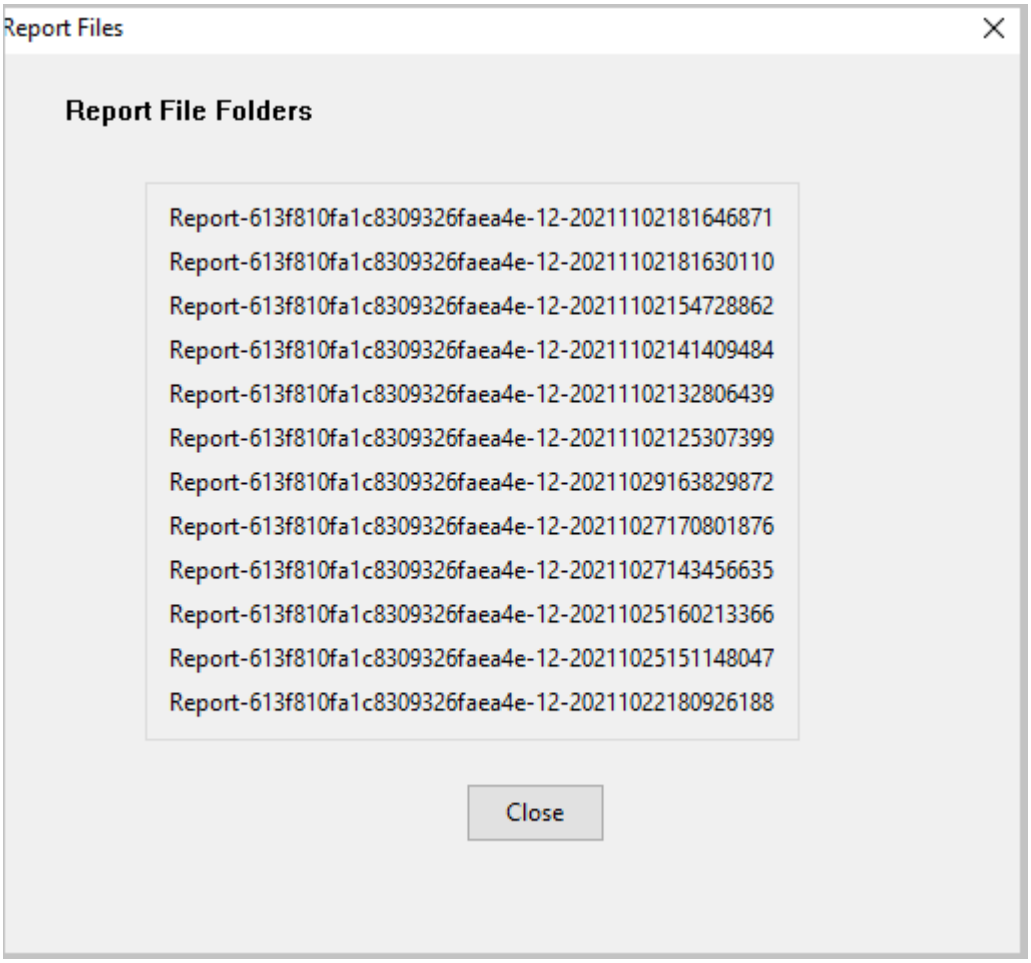
11.5.3 Scan Result Source Files

If the user wants to check the source files of a device related to the table, he/she can click HERE link on the screen, it is shown in the following screenshot (in the blue frame).

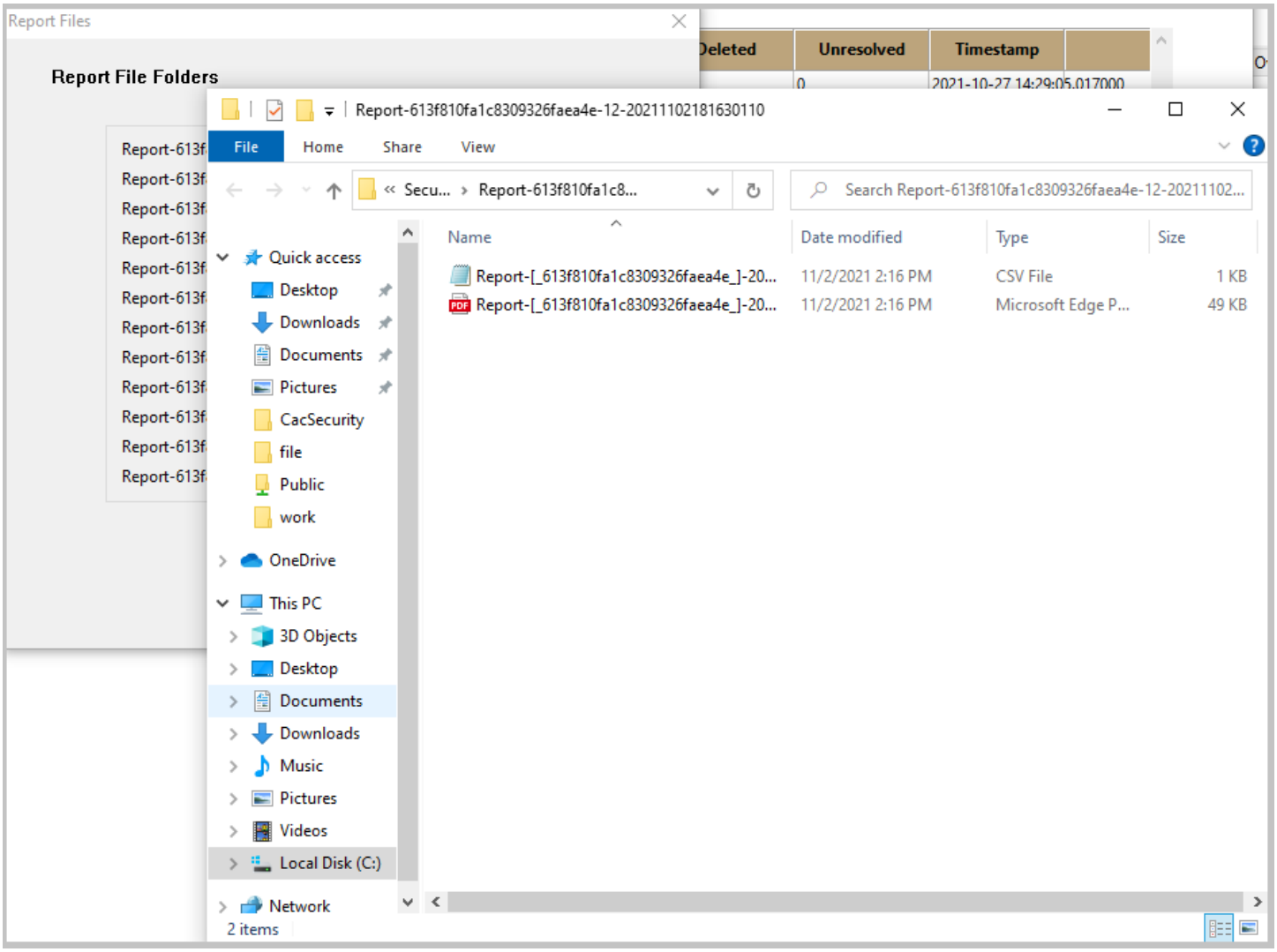


	Status	IP	Cleaned	Ignored	Quarantined	Deleted	Unresolved	Timestamp
1	No detections	192.168.18.132	0	0	0	0	0	2021-10-27 14:29:05.002000
2	No detections	192.168.148.128	0	0	0	0	0	2021-10-27 14:29:04.536000
3	No detections	192.168.148.149	0	0	0	0	0	2021-10-27 14:29:04.536000
4	No detections	192.168.222.128	0	0	0	0	0	2021-10-27 14:29:04.520000
5	No detections	192.168.40.118	0	0	0	0	0	2021-10-27 14:29:04.520000
6	No detections	192.168.0.130	0	0	0	0	0	2021-10-27 14:29:04.520000
7	No detections	192.168.148.132	0	0	0	0	0	2021-10-27 14:29:04.520000
8	No detections	192.168.148.143	0	0	0	0	0	2021-10-27 14:29:04.520000
9	No detections	192.168.127.138	0	0	0	0	0	2021-10-27 14:29:04.505000
10	No detections	192.168.148.137	0	0	0	0	0	2021-10-27 14:29:04.505000
11	status2	192.168.6.xxx	yes	no	no	false	yes	2021-10-19 11:56:57.438000

After clicking HERE link, a window will pop up to display all the file names of the related documents. The following is the screenshot.



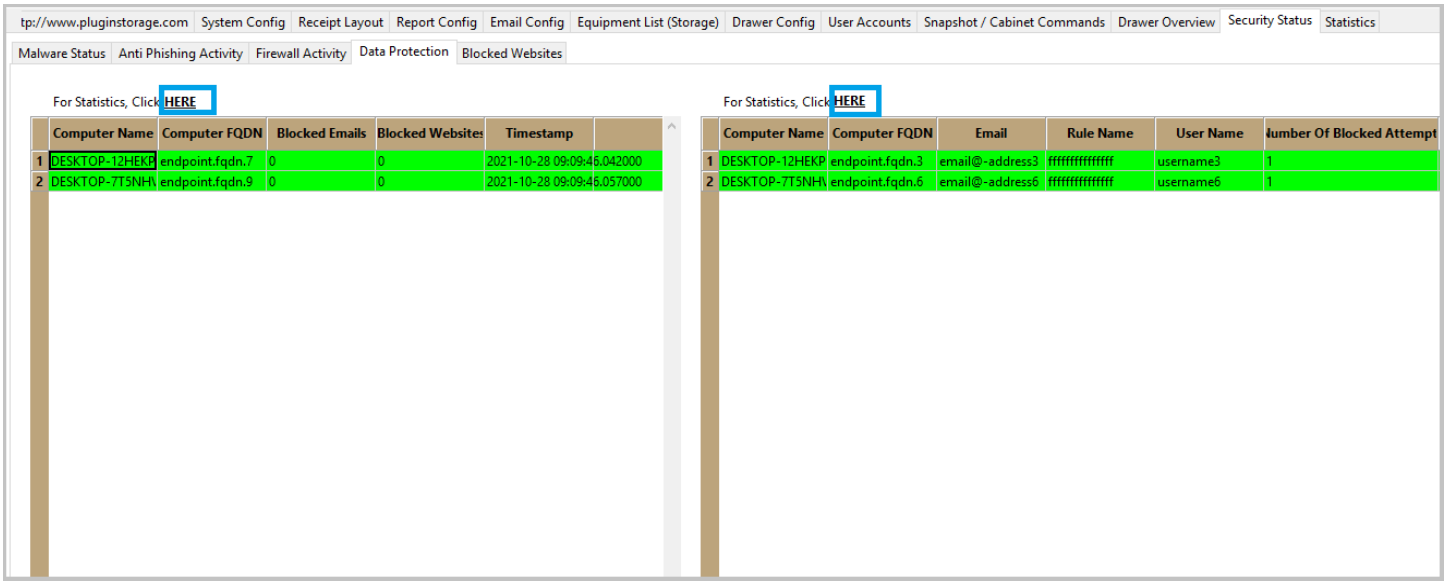
When clicking a specific name, a File Explorer window will appear to bring the user to the directory of the files. The following is a screenshot.



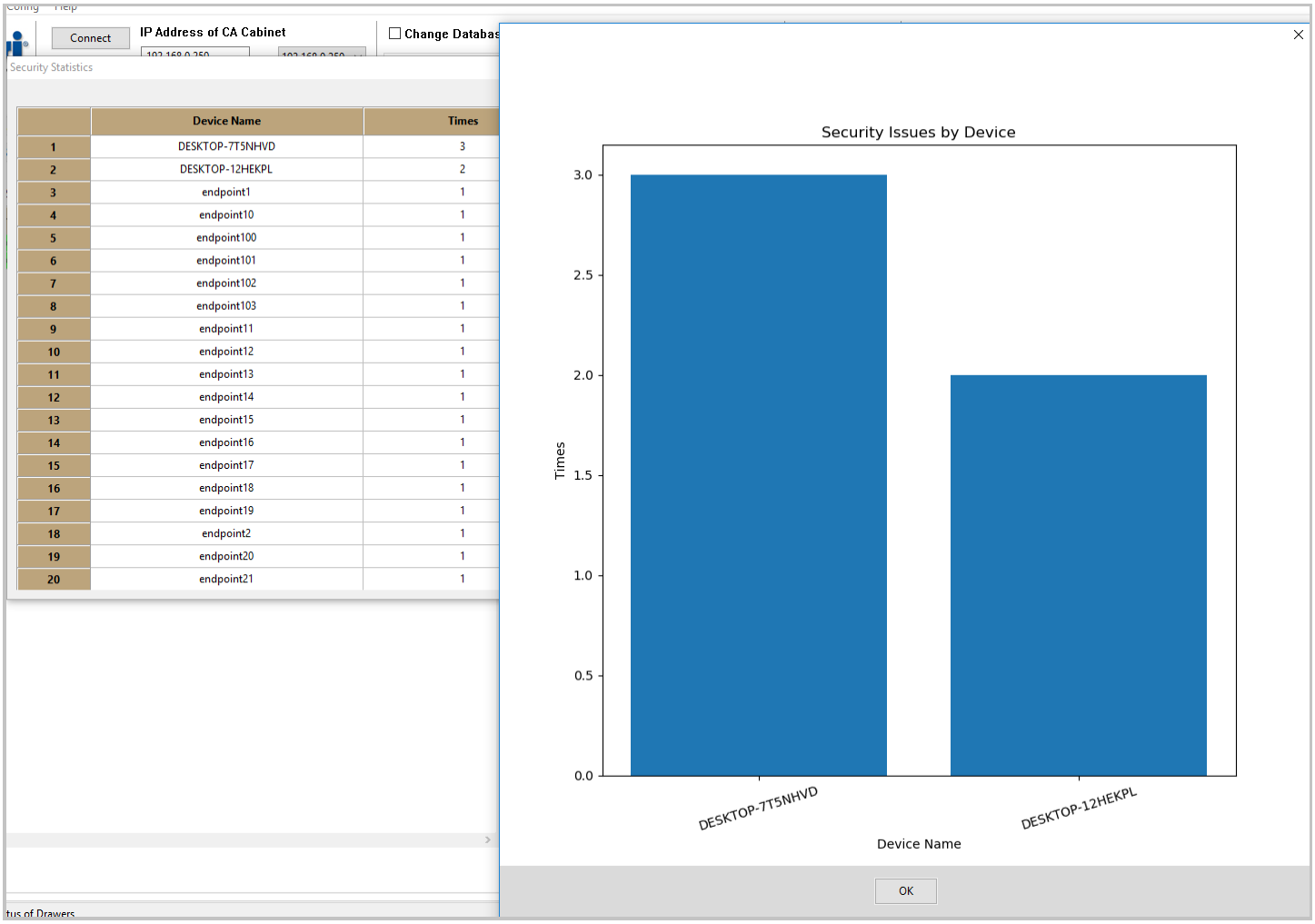
There are two files in the folder. One file is .csv file that can be opened with Notepad or Microsoft Excell, it includes all the data information for the scan. If there is no threat found in the scan, the file only has the header names of the columns. Another file is a .pdf file; it shows a chart to illustrate the scan result.

11.5.4 Scan Statistics

When the user wants to check the statistics of the scan result related for a specific table, he/she can click the HERE link on the screen (indicated in the blue frame in the image):



When clicking the HERE link, a window with the scan result of the threats and a window with the chart will appear. The following is a screenshot. Only the devices that are in Equipment List tab and that have a valid EndpointID will be shown in the statistics chart.



11.6 Email Alert and Daily Report

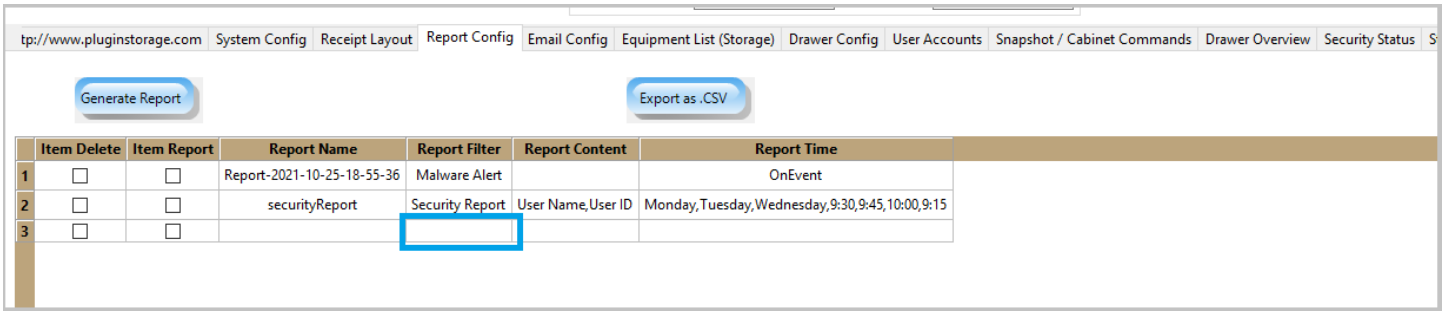
When a device is infected with malware, an email alert will be sent to the administrator. If there are some attacks to the device but they are blocked successfully, there will be NO alert; if the device has detected the malware but the malware has been removed successfully, there will be NO alert either. The goal of the security function is to make the device never be infected.

The cabinet can also generate reports for the security activities and email them to the administrator.

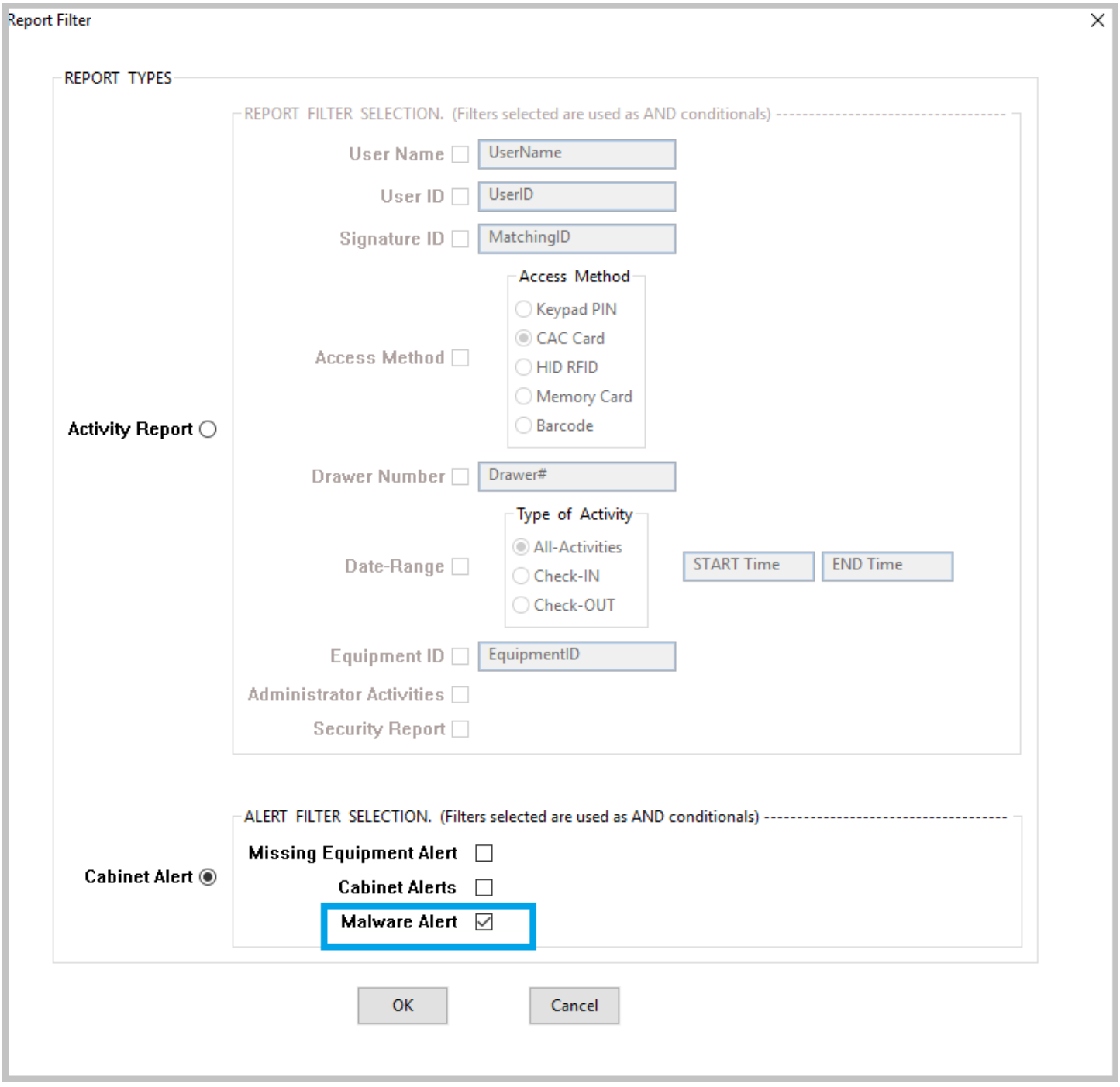
11.6.1 Email Alert

In order to enable the email alert function, a report needs to be created from Report Config tab and is assigned to the administrator.

In a new line of report table, click Report Filter column, the following is the screenshot to indicate the place (in blue frame).

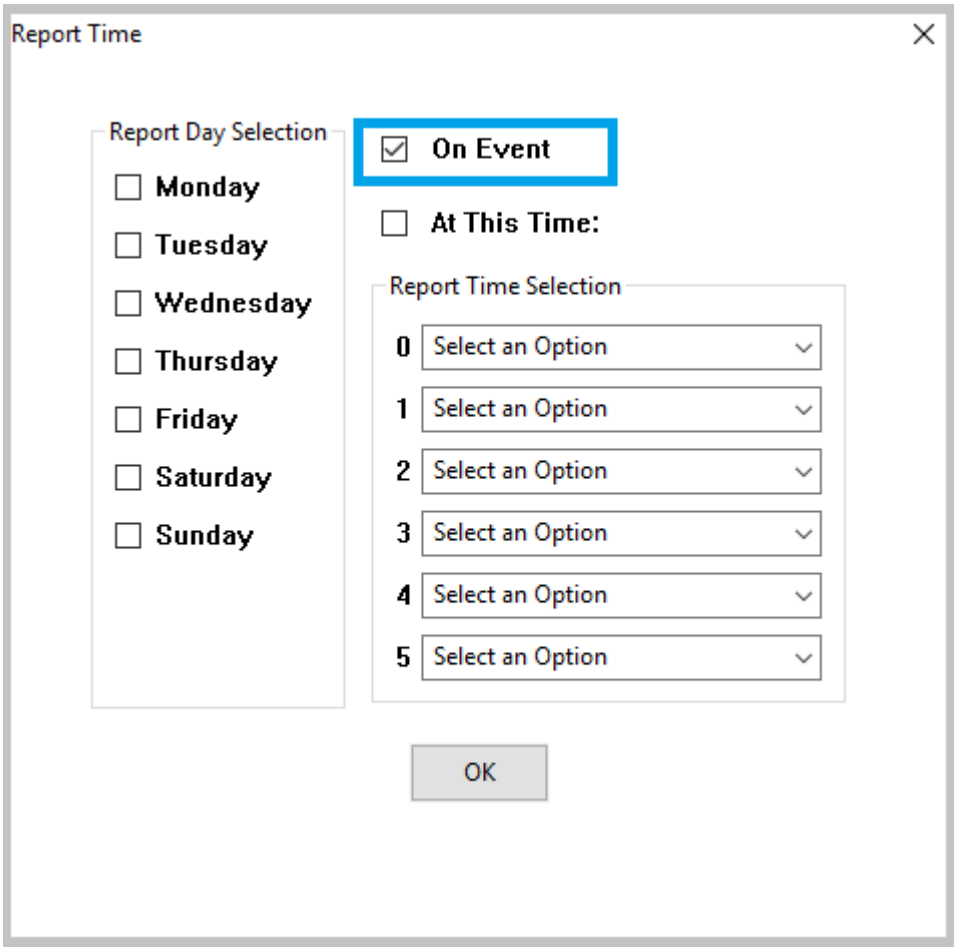


A window will pop up for the selection of Report Filter.



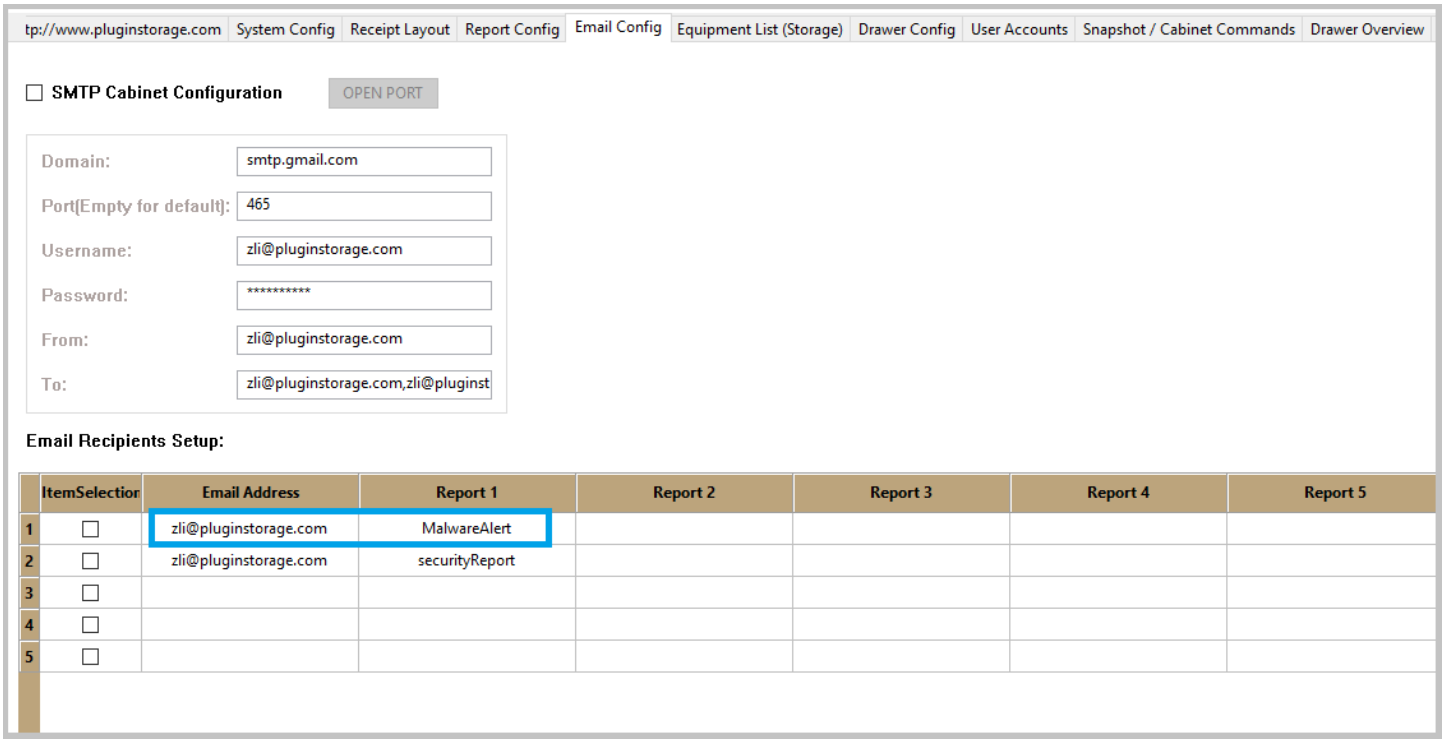
Choose Malware Alert (Indicated in the blue frame) and press OK button.

In the related Report Time column, select On Event. The following is the screenshot for the setup.

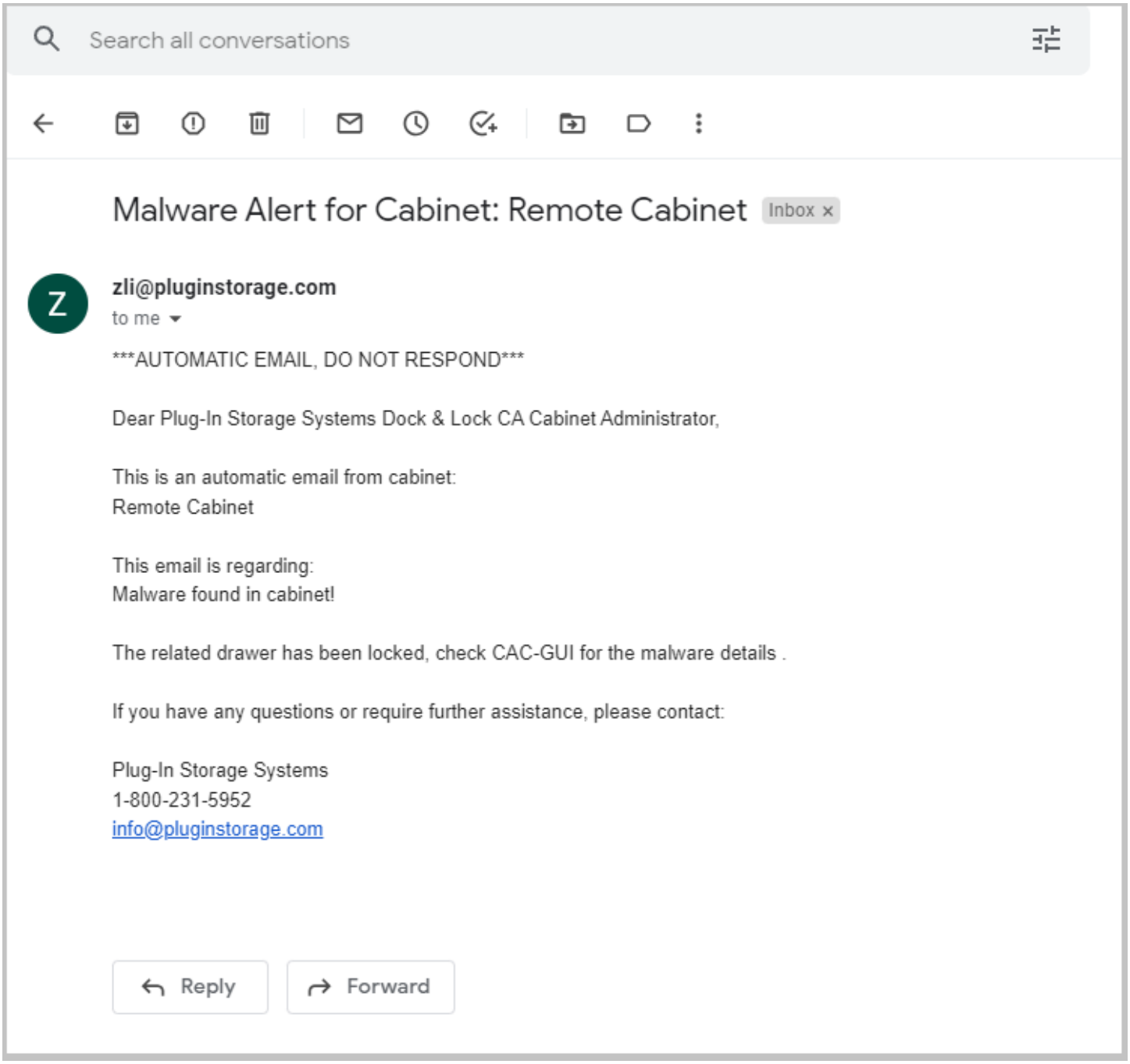


Press OK button, and save the page, the report creation has finished.

After the report has been created, it needs to be assigned to an administrator. The user can go to Email Config tab, type in the email address of the administrator, and choose the report name for malware alert in the list. The following is a screenshot.



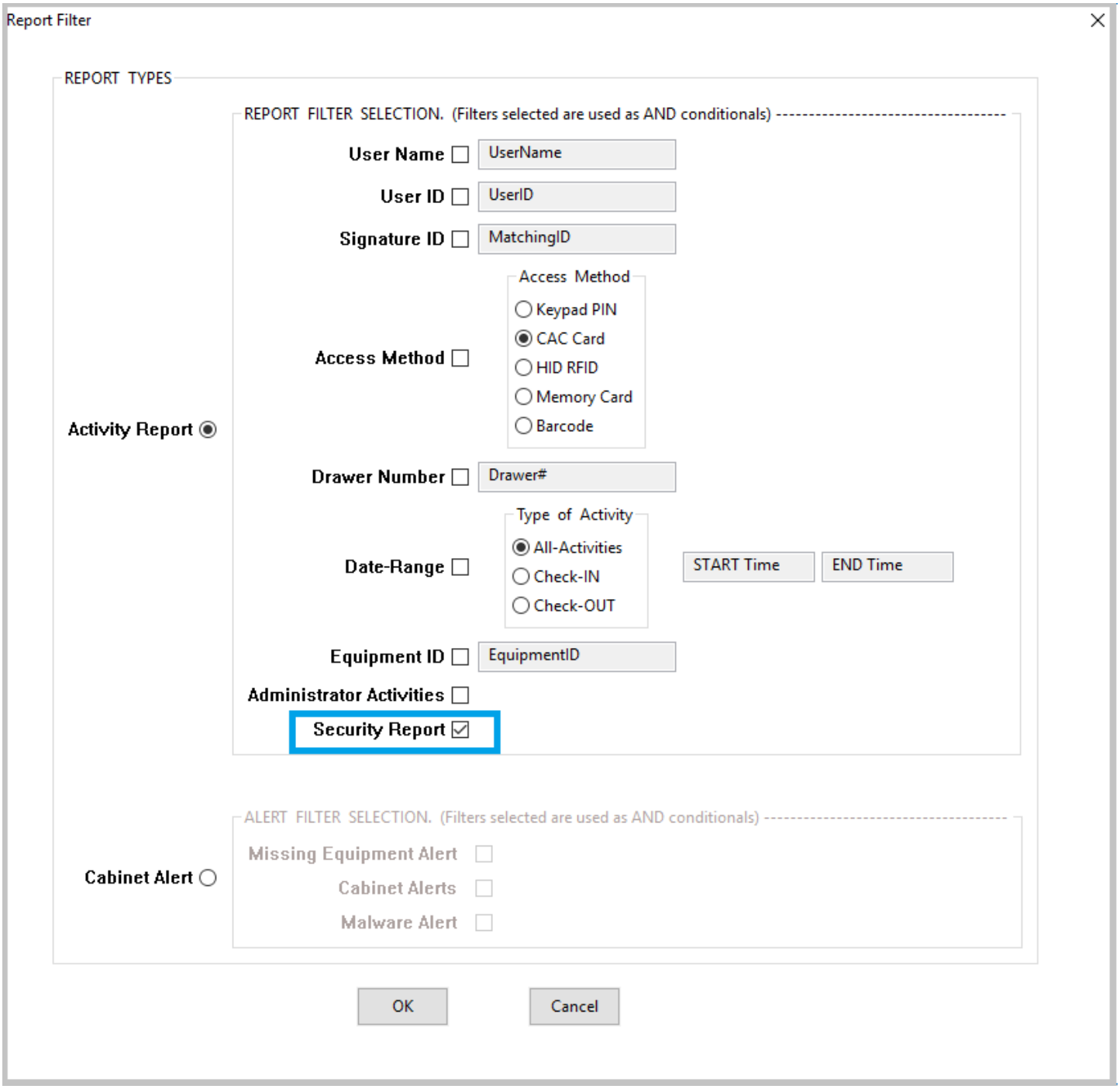
After the email configuration is done, when a device is infected with malware, the administrator will receive an alert as following:



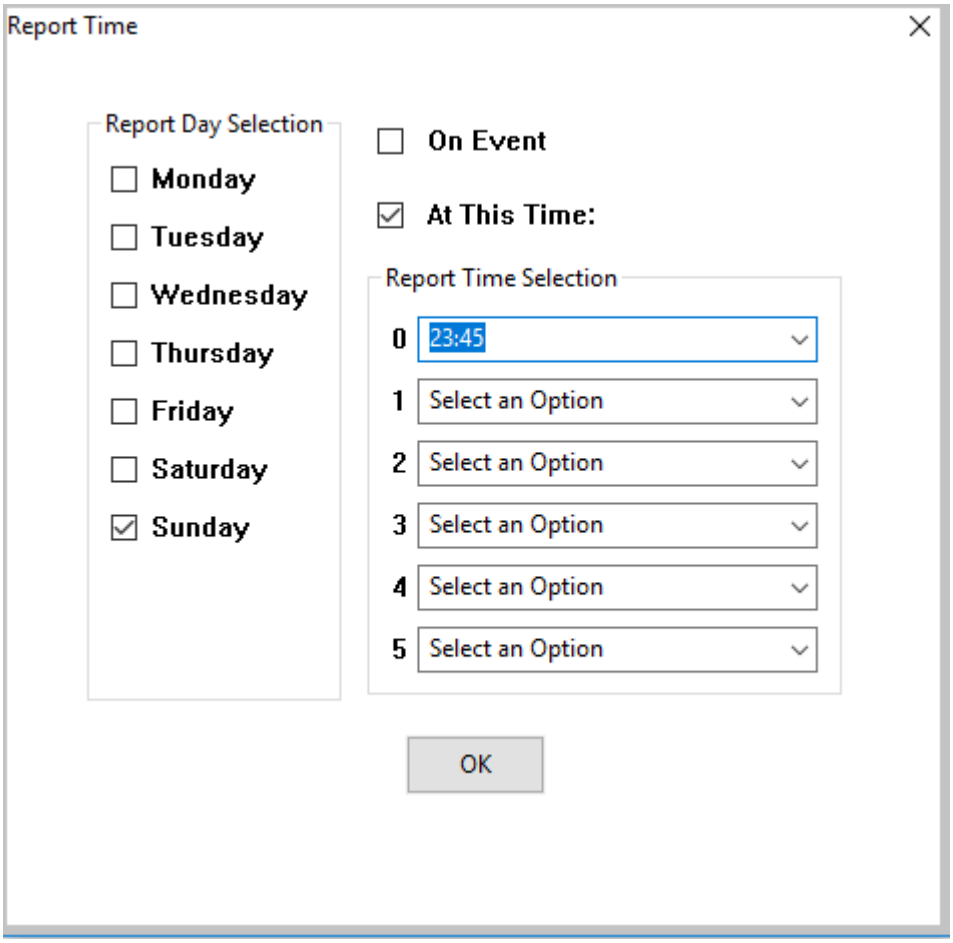
11.6.2 Security Report

The cabinet can summarize all the security activity for the devices and generate a set of reports and send them to the administrator by email.

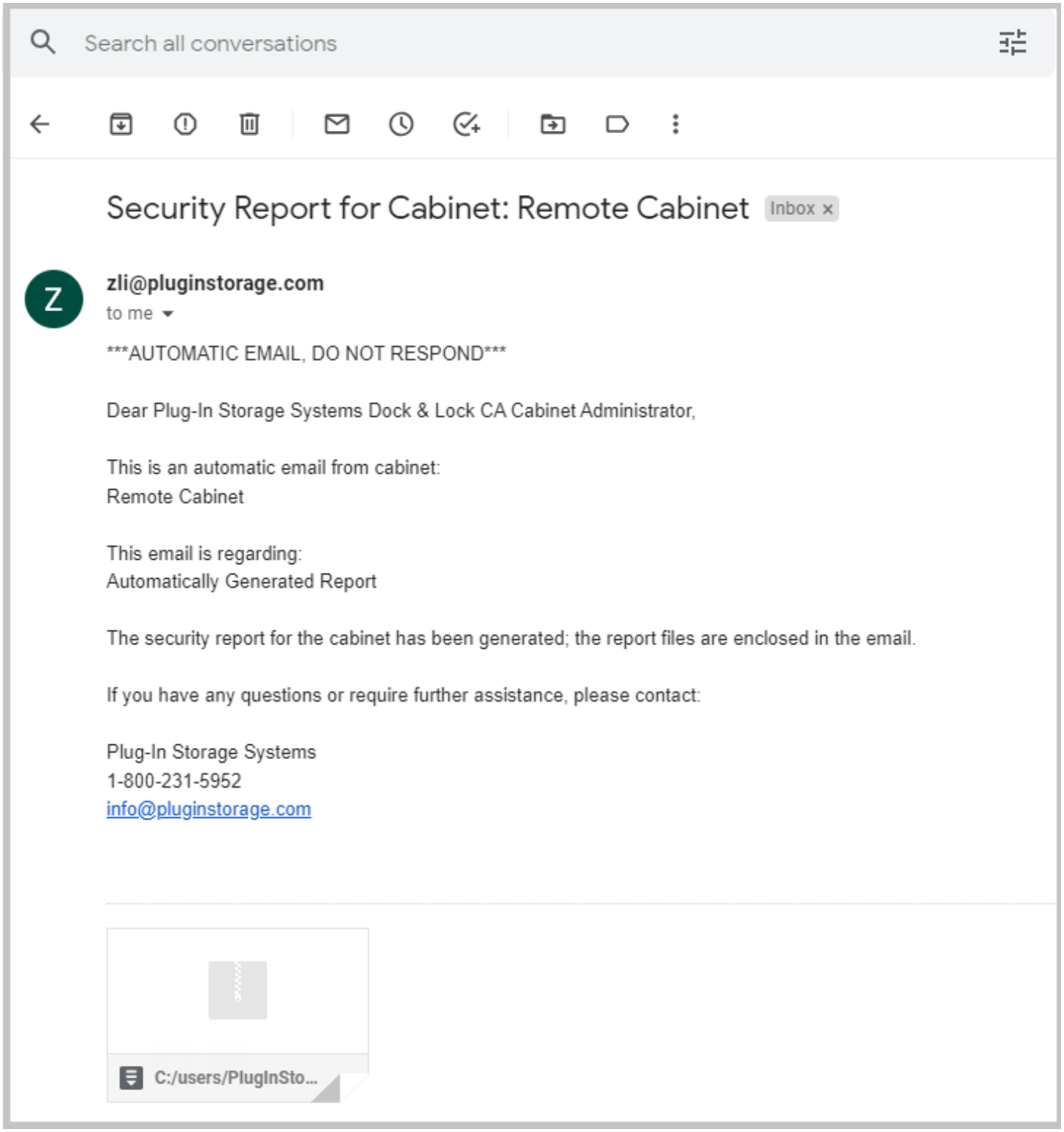
The process of the report setup is similar to that of the security alert. For the security report, Security Report needs to be chosen instead of Security Alert. The following is a screenshot.



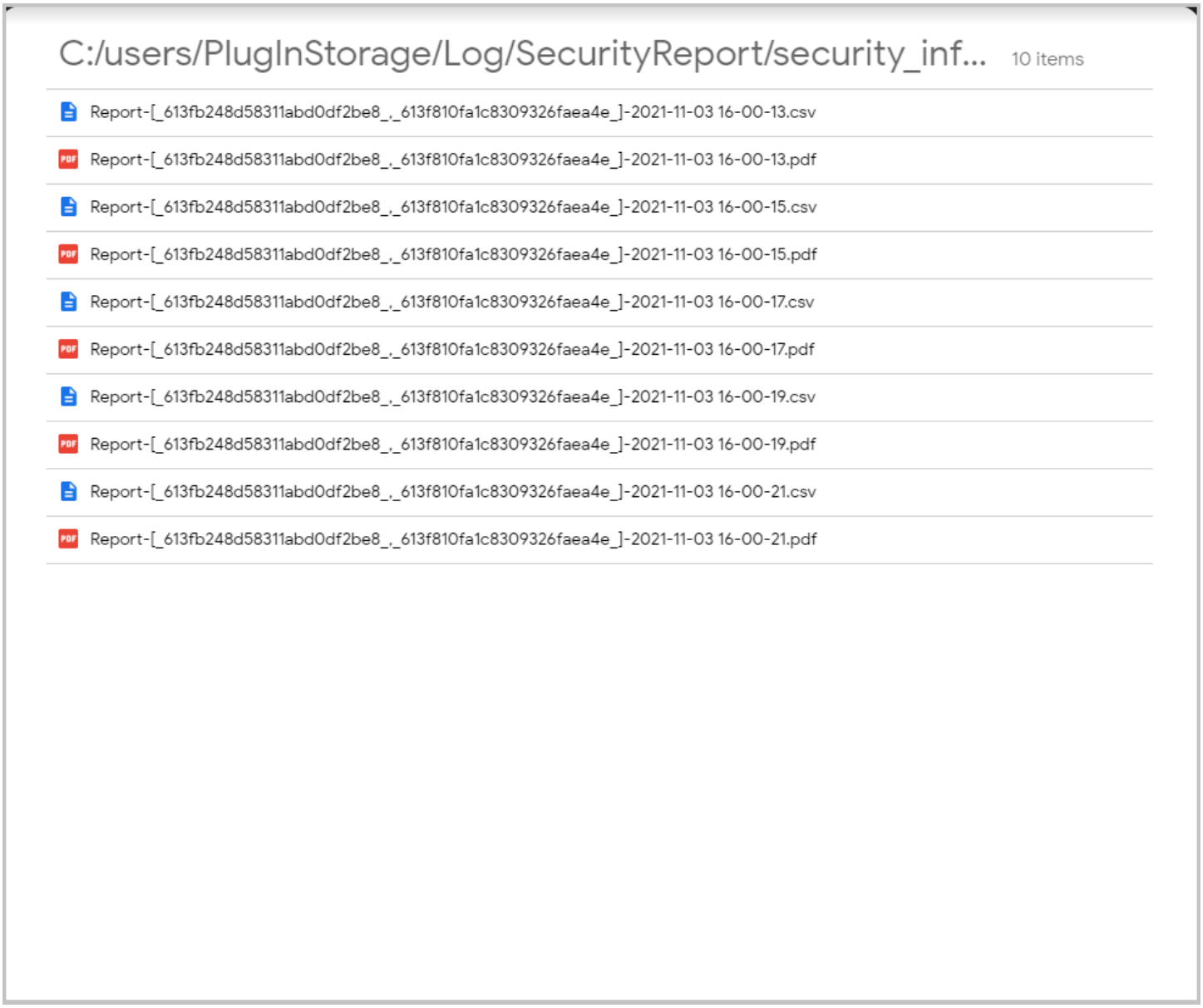
For the report time, the user can choose a specific time for the report. If it is a daily report, the time could be every night; if it is a weekly report, the time could be the night of the Sunday (or any day of the week). The following is a screenshot.



An email for the security report is like the following.

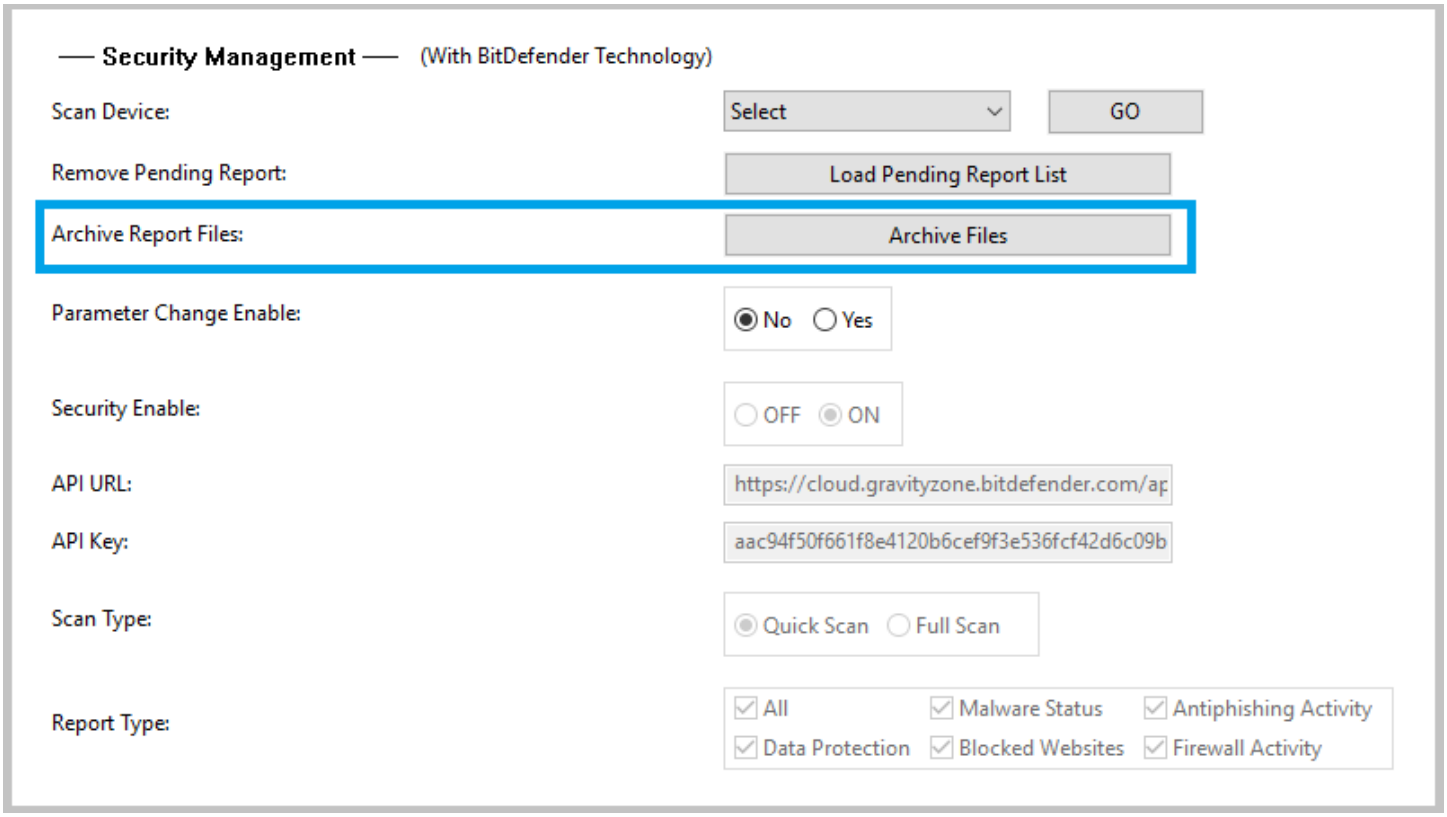


The file enclosed in the email is in .zip format, it normally includes 10 files; these files are in .csv format and in .pdf format for malware status, Antiphishing activity, firewall activity, data protection and blocked websites. The following is a screenshot of the list.



11.7 Archive Source Files

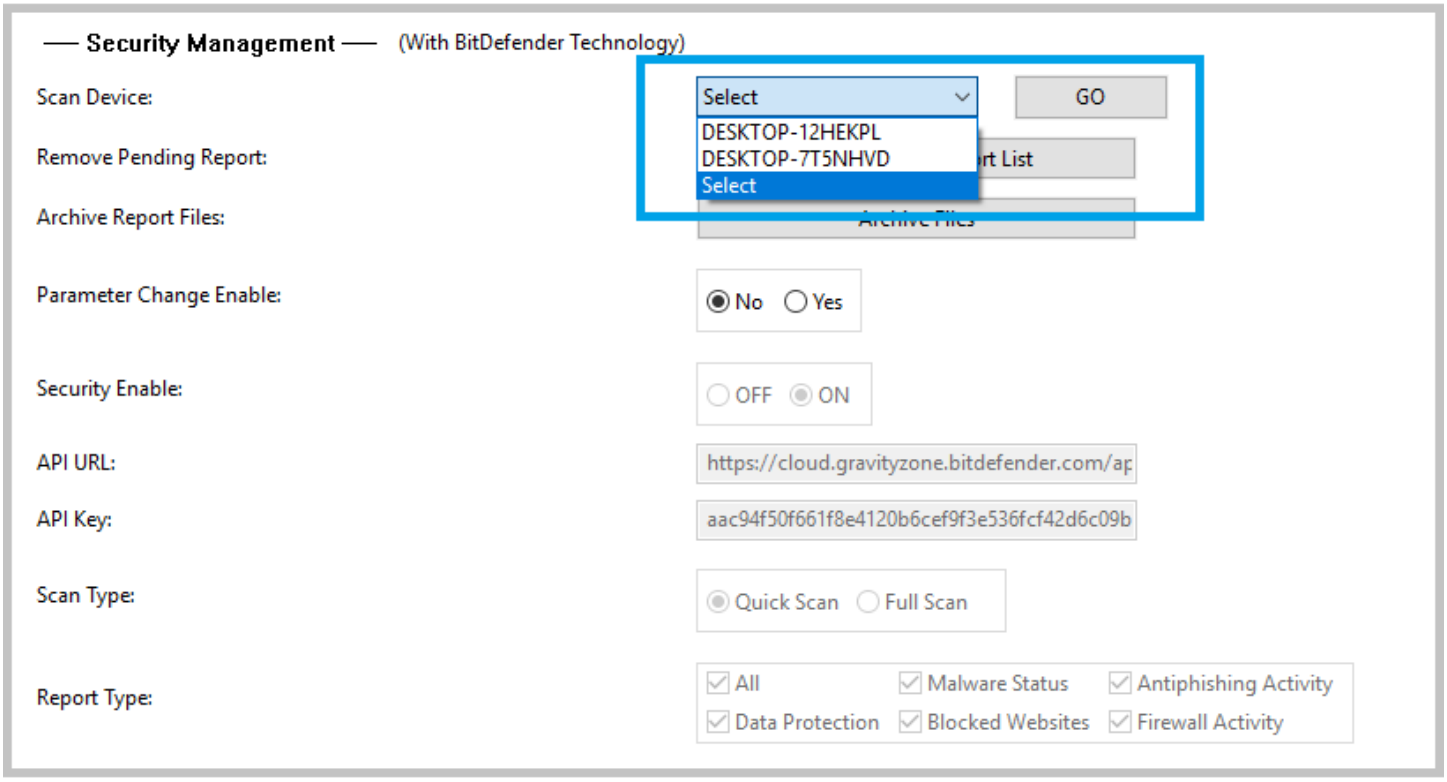
The generated report files are saved in folder C:\Users\PlugInStorage\Log\SecurityReport, six .zip files and six related folder are created for each check-in action of the devices, so the number of files and folder could increase rapidly. The administrator might want to archive the files to a different folder to increase the efficiency of the cabinet actions after a while. The archive can be done from System Config tab of CAC-GUI. The following is a screenshot.



After Archive Files button is pressed, all the files in C:\Users\PlugInStorage\Log\SecurityReport is moved to C:\Users\PlugInStorage\Log\SecurityReport\Archive by default. The administrator may move the files to another place if he/she wants.

11.8 Manually Scan

Normally a device is scanned for malware when it is checked in, but the administrator may also scan the device manually if he/she choose to do it. This can be done from System Config tab of CAC-GUI. The following is the screenshot.

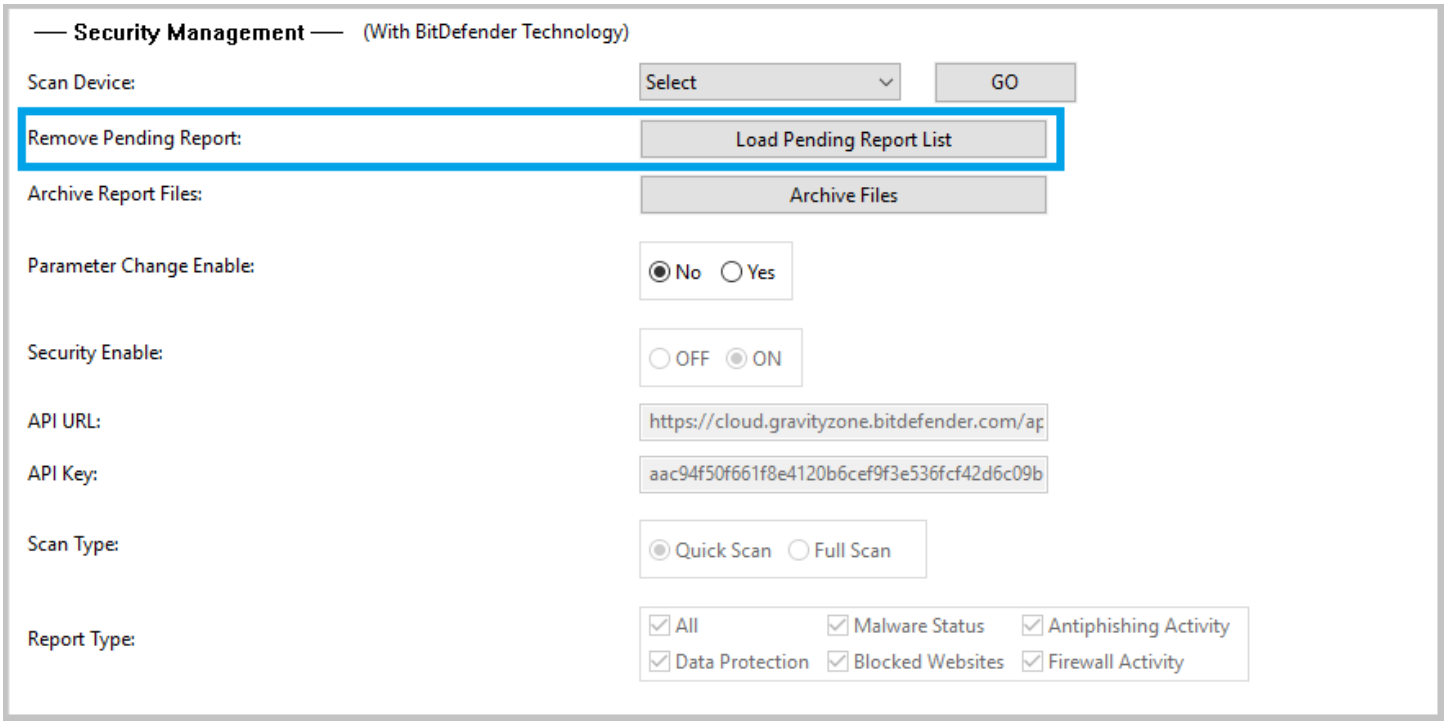


From the pull-down menu of Scan Device, choose the related computer name, and press GO button, the cabinet will scan the device and read the status/report. The status and the report will be available at CAC-GUI as soon as the scan has finished.

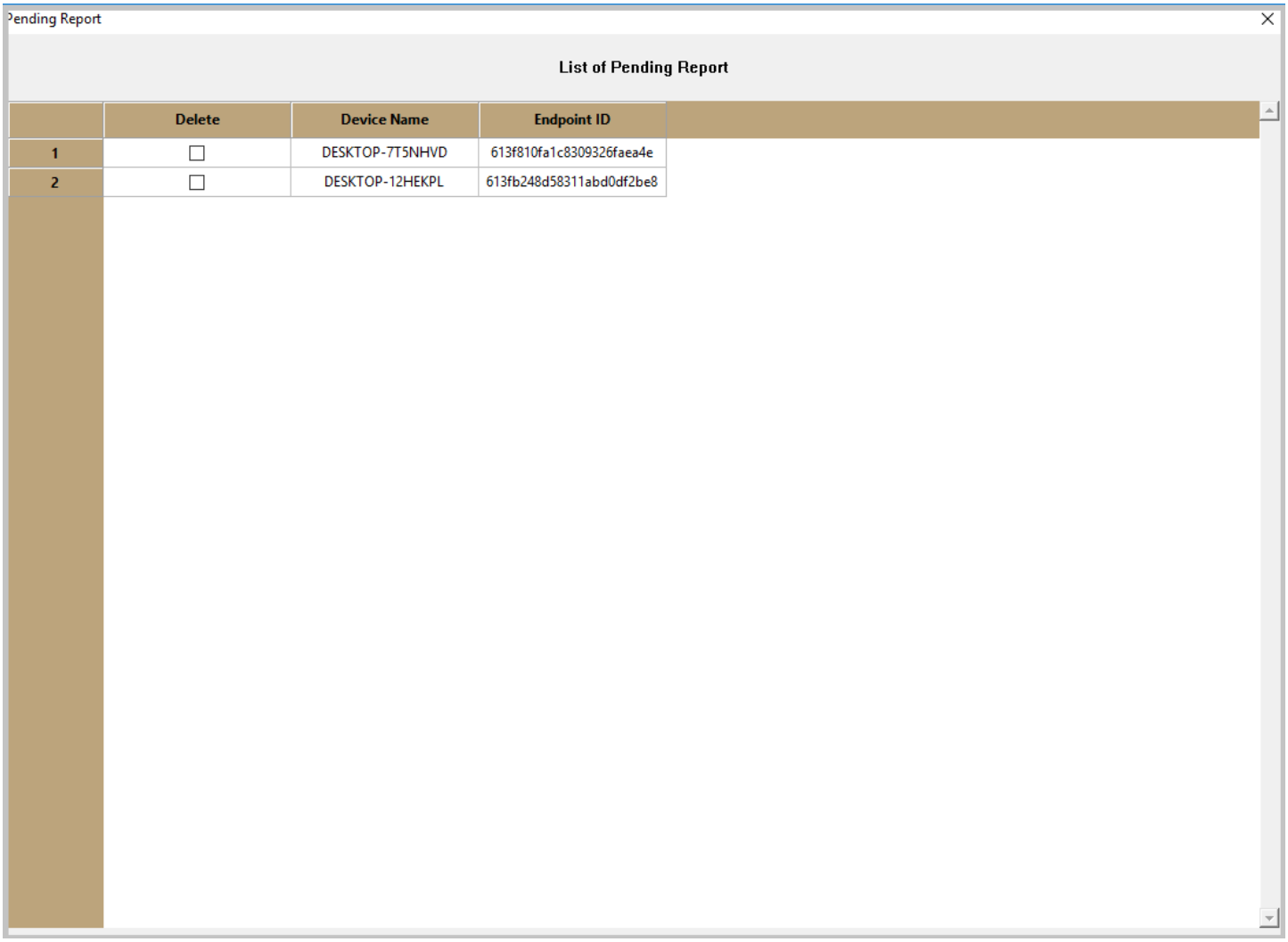
11.9 Manually Remove Pending Scan

When a device is in scanning state, the related line in Security Status tab will remain yellow. After the scan is finished, the color of the line will become green again. Normally the scan will finish in a while after it is initiated, but occasionally the scan can be stuck somewhere and cannot finish, or the result cannot be synced to BitDefender server. In these situations, probably the administrator wants to remove the scan.

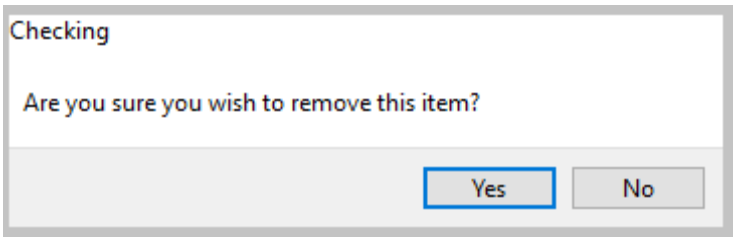
The removing action can be done from System Config of CAC-GUI. The following is the screenshot.



Click Load Pending Report List button, a screen will pop up to display all the pending scans.



Click the Delete column of the line that scan is to be deleted, and a window will pop up to confirm the action.

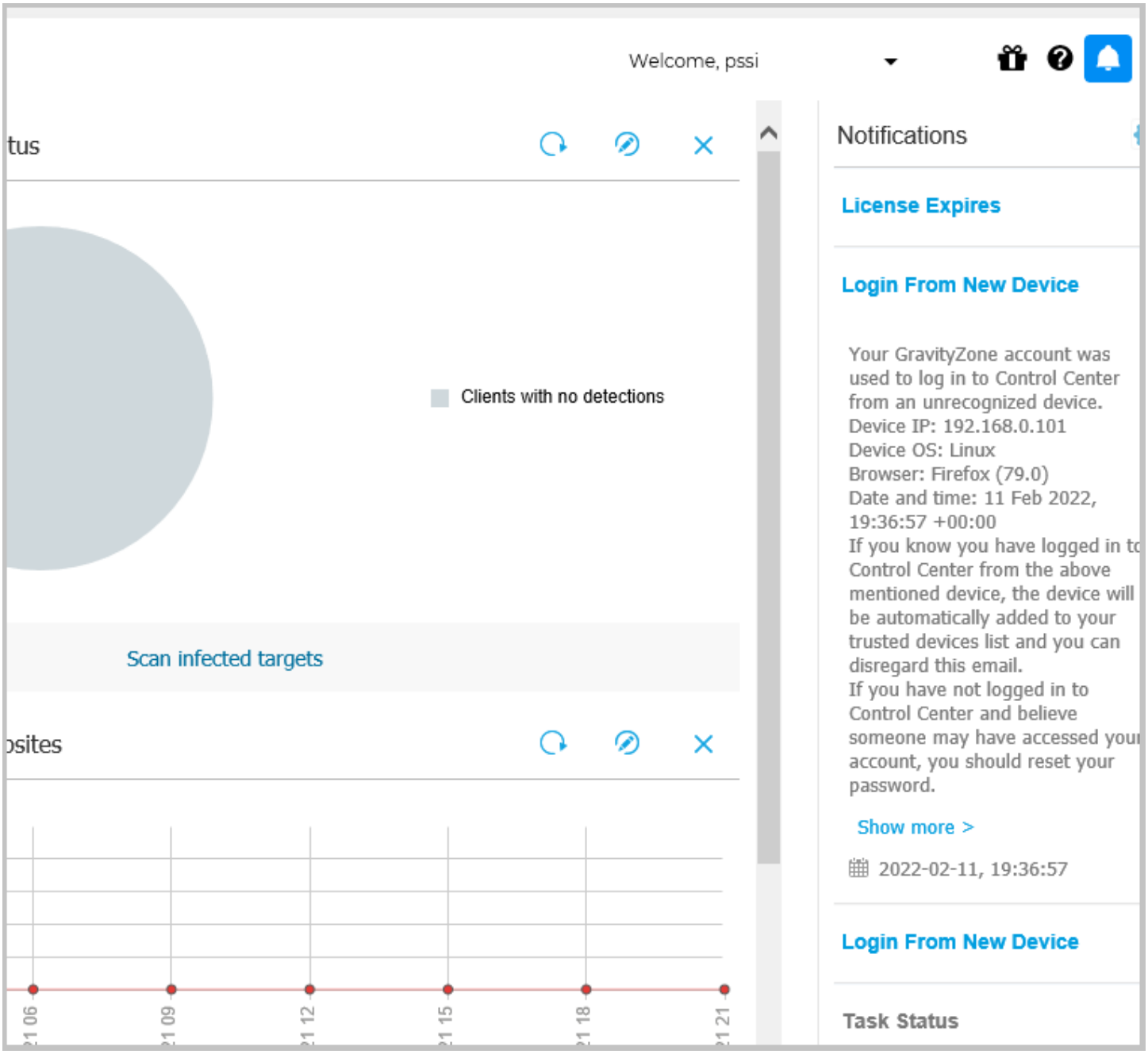


Press Yes button and the related scan action will be removed.

11.10 Syslog Server Functionality

Syslog server is the service or computer to receive the notification from GravityZone server, this functionality is only available to On-Premises mode.

When some special events happen, GravityZone will generate some notifications, normally the information can be found on the left side of the screen in the Control Panel. These notifications are also sent to the Syslog server at the same time if proper configuration is done. The following is the screenshot:



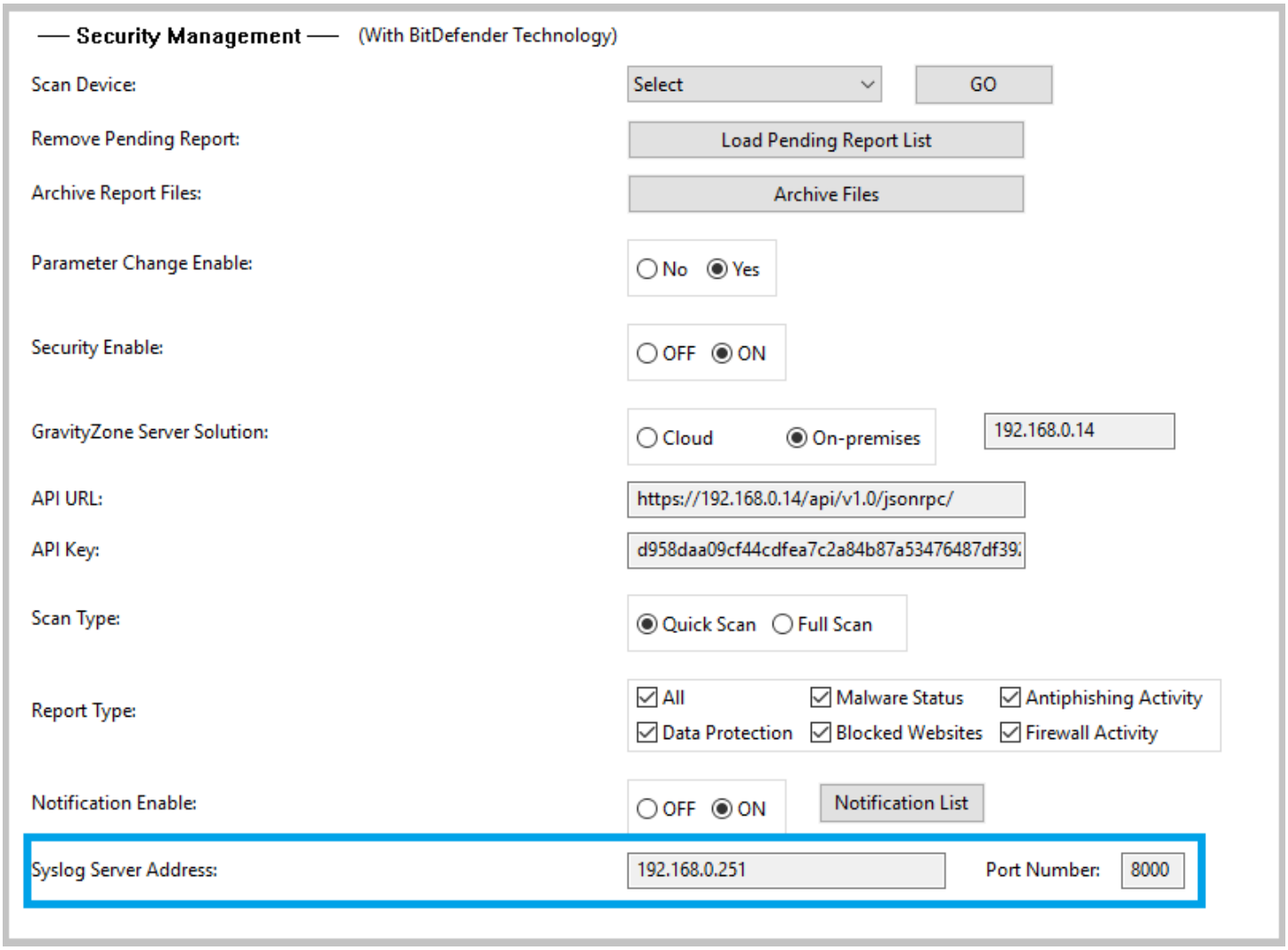
The notification includes the following types:

Malware Outbreak, License Expires, Deployments have reached or exceeded license limit, License Limit Is About To Be Reached, Update Available, Exchange License UsageLimitHasBeen Reached, Invalid Exchange User Credentials, Login From New Device, Upgrade Status, Authentication Audit, Anti-phishing Event, Firewall Event, ATC/ID Sevent, User Control Event, Data Protection Event, Product Modules Event, Security Server Status Event, Product Registration Even, Overloaded Security Server Event, Task Status, Outdated Update Server, Amazon EC2 Trial Expiresin7 Days, Amazon EC2 Trial Expires Tomorrow, Amazon EC2 Licensing event, Amazon EC2 Cancelation event, Amazon EC2 Invalid credentials.

11.10.1 Syslog Server Setup on CAC-GUI

The user needs to run the installer of Syslog server in the computer to install the program. The server can be in a dedicated computer, or in a computer shared with other programs (such as the CacManager).

Notification Enable needs to be set to ON, and the IP address and the port of the Syslog server needs to be configured from CAC-GUI. The following is the screenshot to do it.

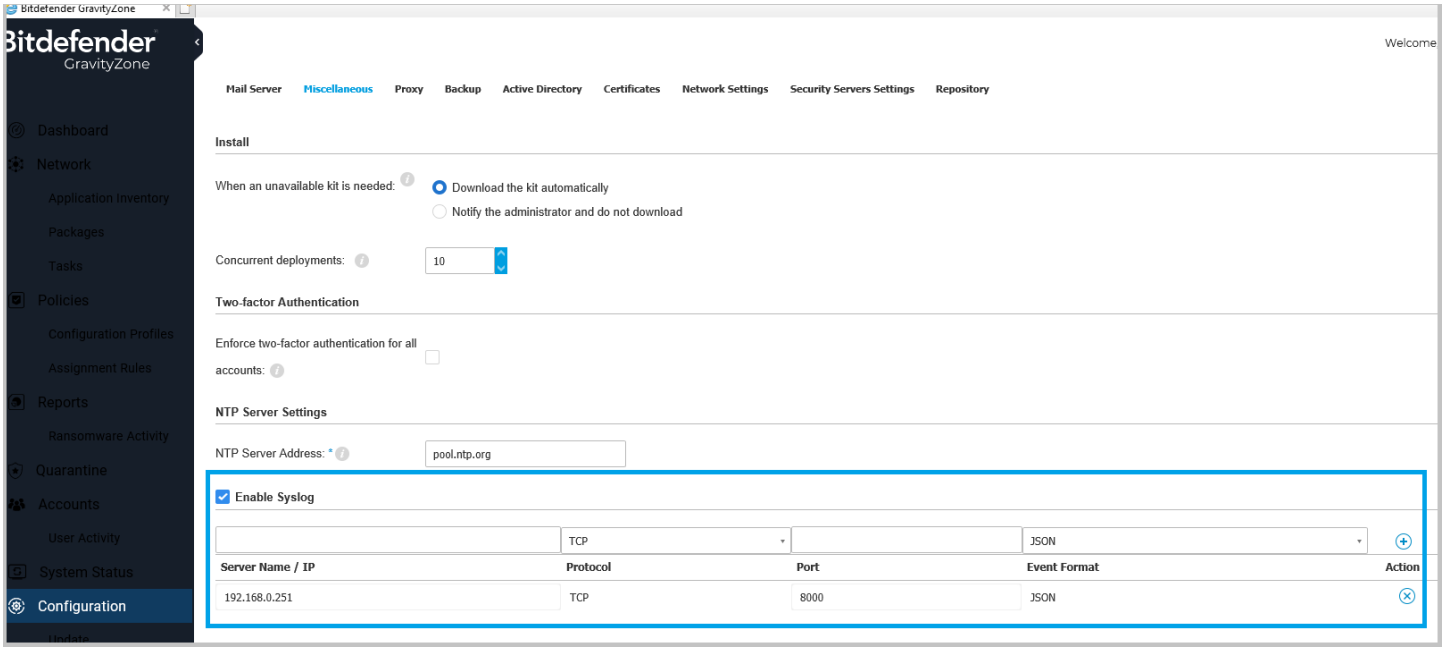


In the example of above screen, The IP address of the server is 192.168.0.251, and the port number is 8000.

11.10.2 Syslog Server Setup on GravityZone

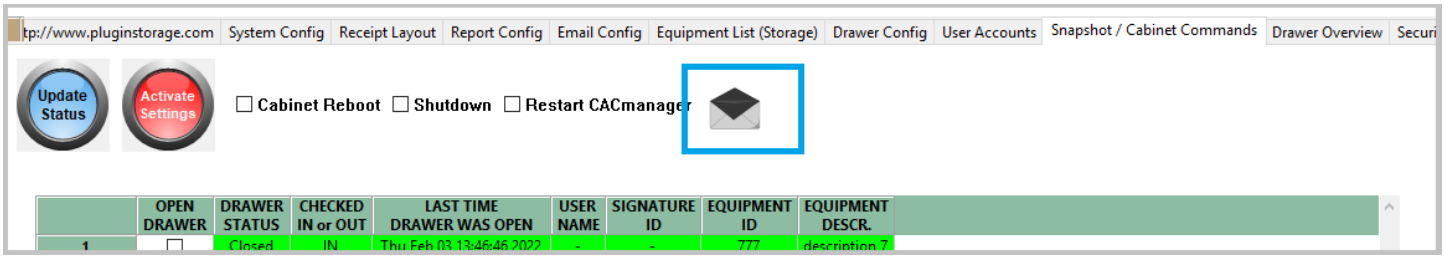
Besides the setup of CAC-GUI, GravityZone also needs similar configuration. Syslog function needs to be enabled from the Control Center of GravityZone, and the IP address/port also needs to be configured for Syslog server to be functional.

The steps for server setup are as follows: enter Control Center, click Configuration on the left panel, and then click Miscellaneous on the menu, the setup screen will appear. Tick Enable Syslog item, and type in Server Name/IP, choose Protocol TCP, type in the port number, choose JSON in the Event Format, and press Save button, the setup will be saved in the database. The following is the screenshot.

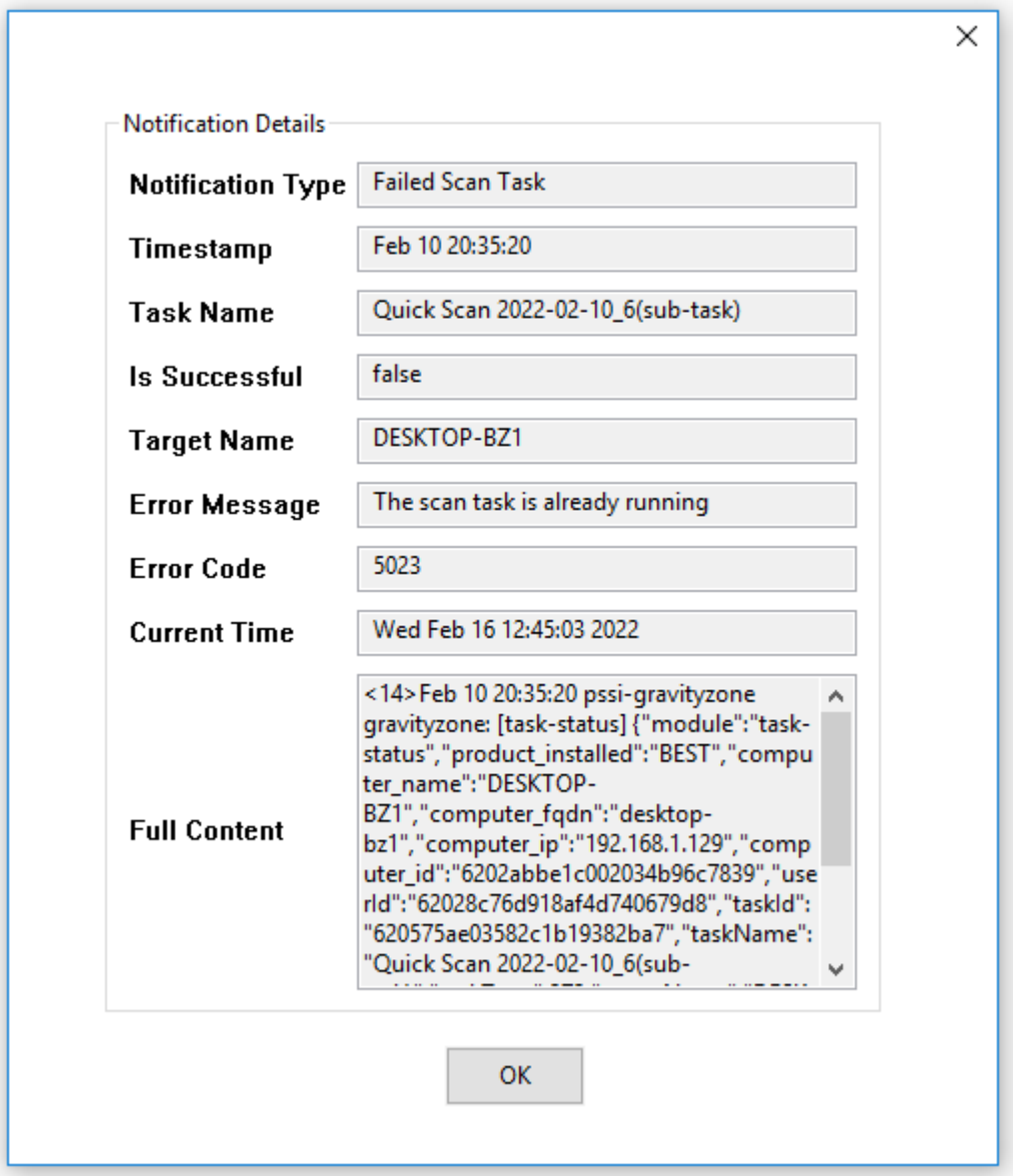


11.10.3 New Notification Alert

When a new notification is received from Syslog server, the information is saved in the SQL database, and an alert is created in Snapshot/Cabinet Commands tab of CAC-GUI. An animated envelop logo will appear on the top part of the screen. The following is the screenshot.

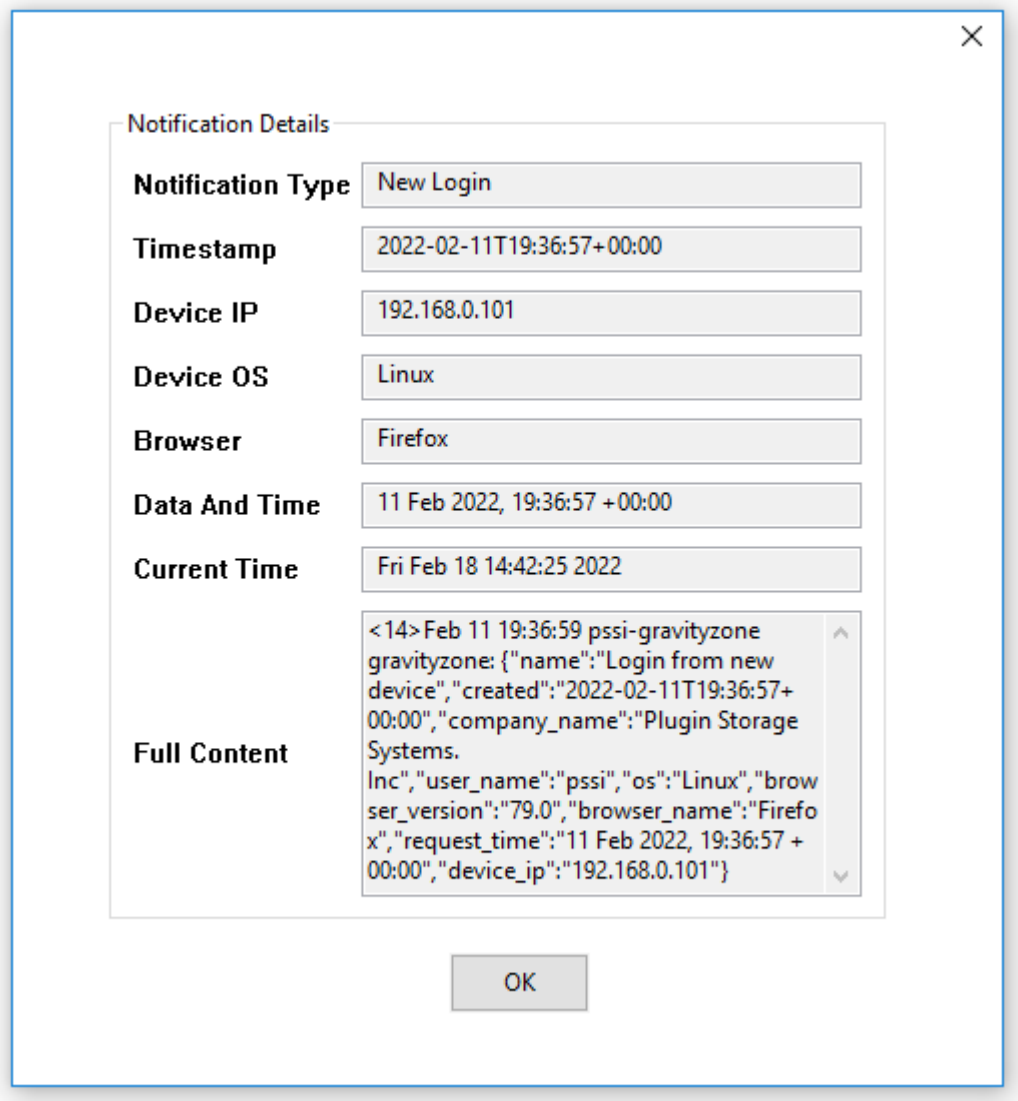


When clicking on the envelop logo, a window will pop up to display the content of the news notification. The following is the screenshot of the popped-up window:



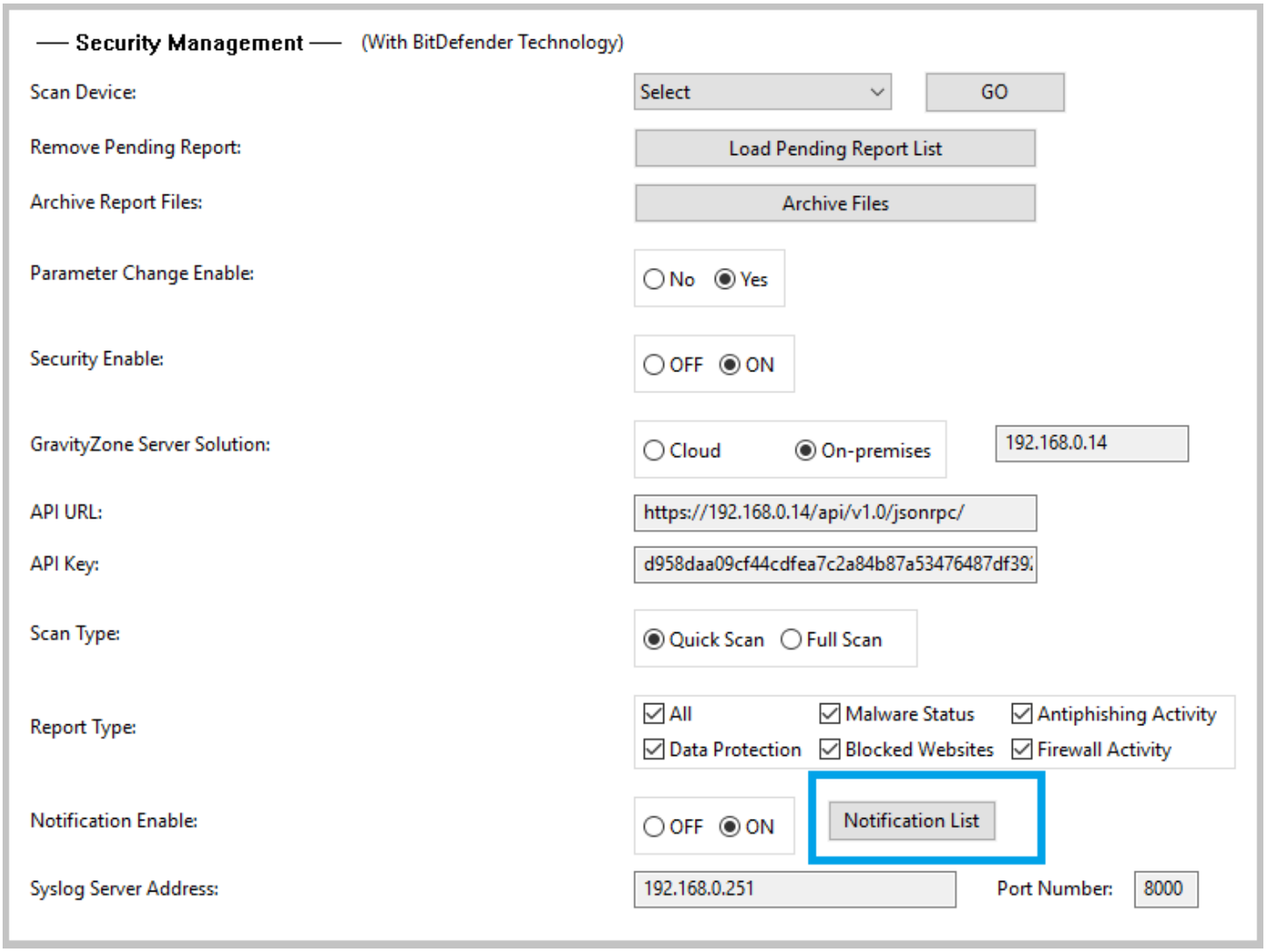
The above notification is about an event of failed scan task. The table shows the basic information about the task and its result. The last item Full Content is the full text about the notification which contains all the information about it. After clicking OK button, the window will close, and the envelop logo will disappear too.

The following screen shows a notification about Login from New Device.

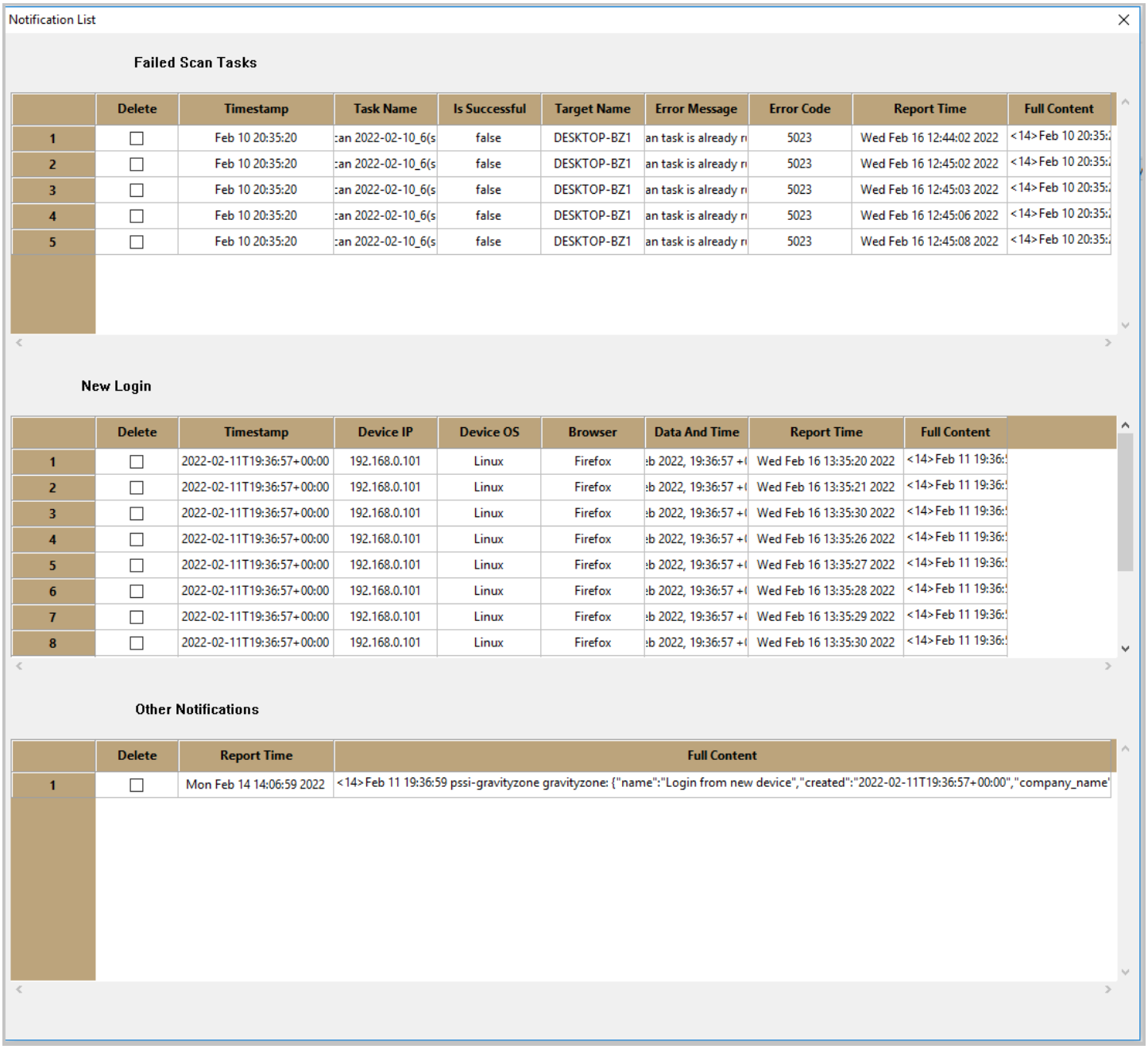


11.10.4 Notification List

When a new notification is created, it is saved in the database. The history list of notification can be browsed from CAC-GUI. The following is the screenshot.



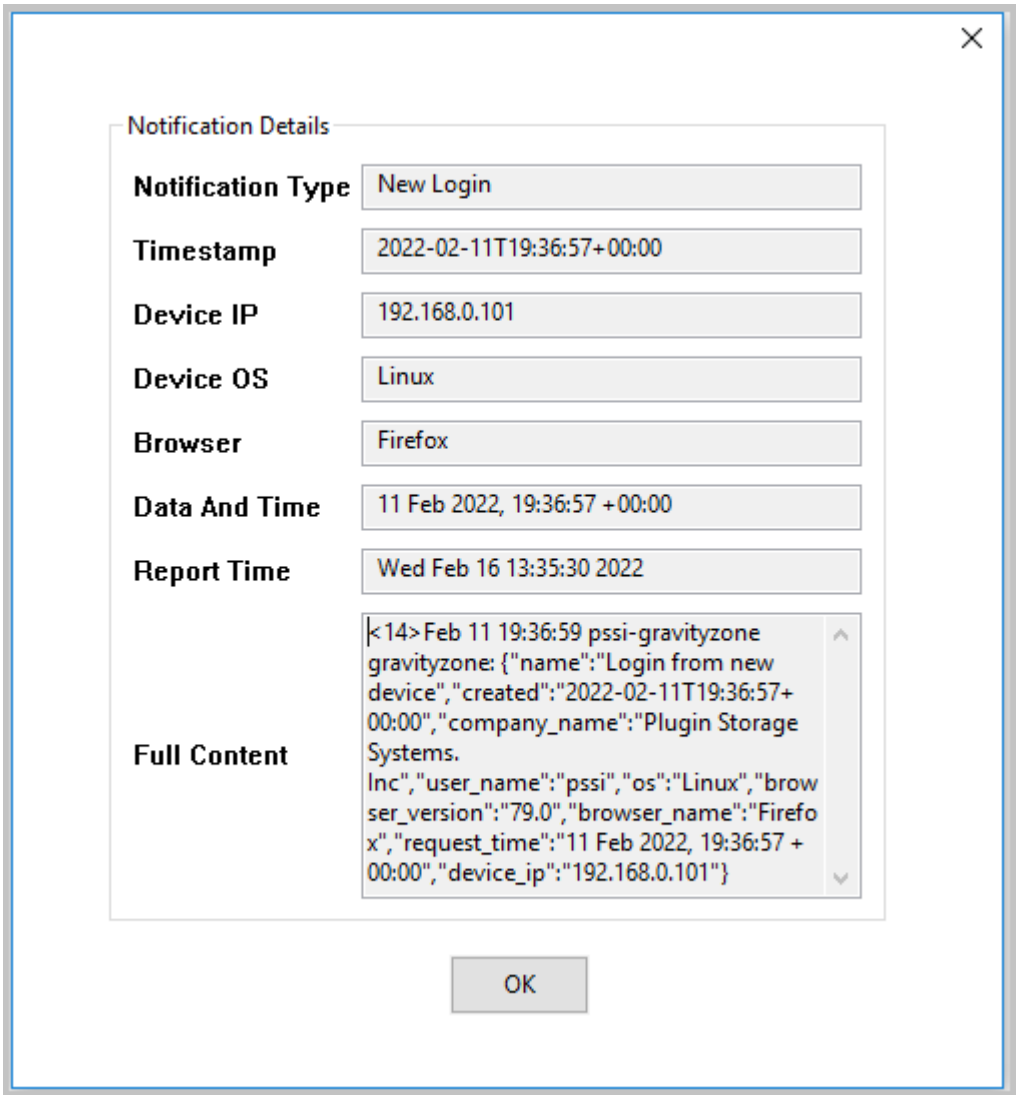
After pressing Notification List button, a window will pop up with the list of notification history. The popped-up window is as follows.



There are 3 tables in the windows. The first one is Failed Scan Tasks, the second table is New Login, and the third one is Other Notifications. The two most common tables are Failed Scan Tasks and New Login, all the other types are classified in the Other Notifications.

If you want to delete a notification item, you can click on the checkbox of the Delete column of the related item line, and a window will pop up to confirm the action “Are you sure to delete the item?”, press Yes button, and the notification item will be removed from the database.

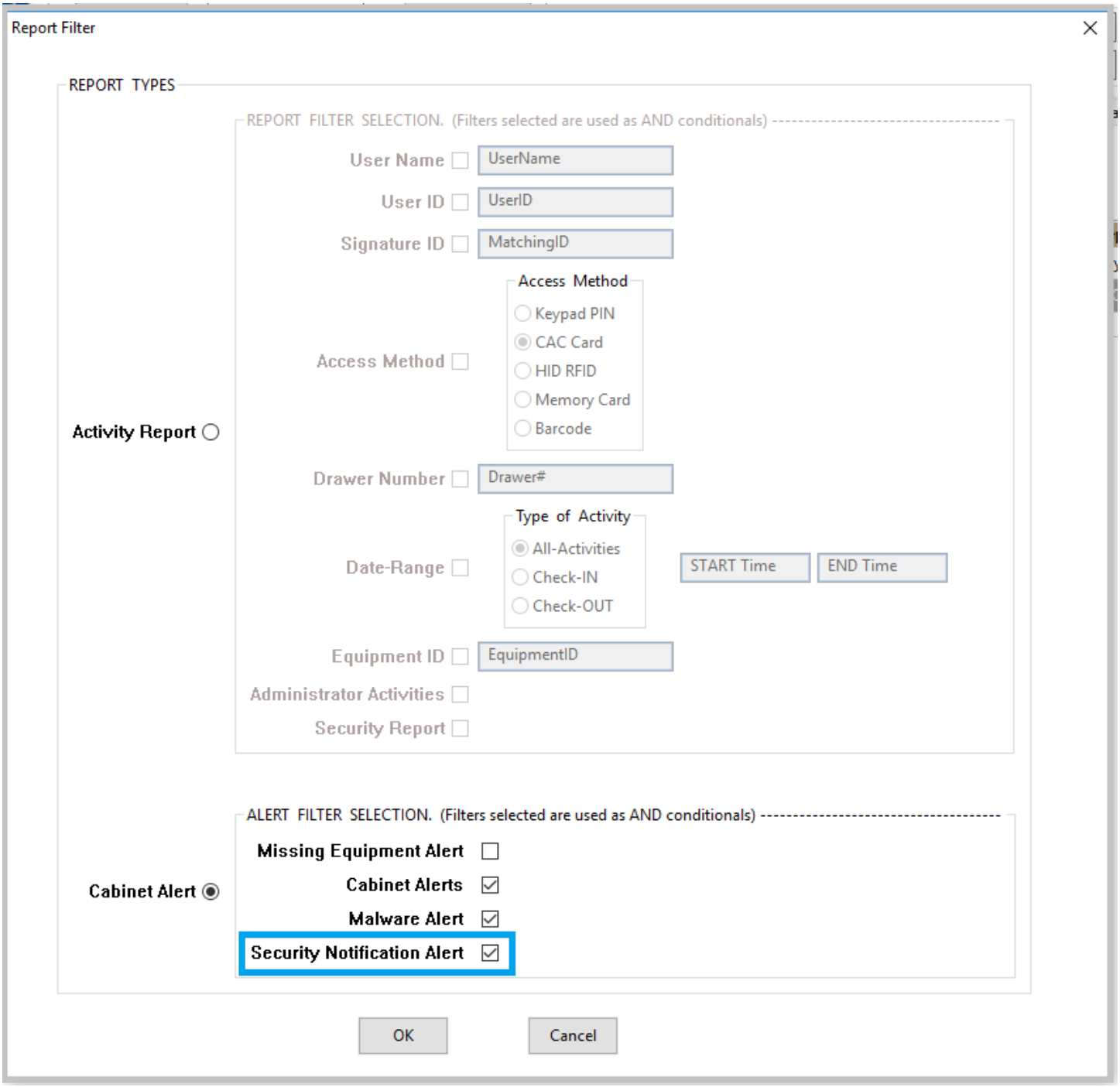
If you want to check the details of the notification, you can click any column except Delete, and a window will pop up to display the details. The following is the screenshot.



11.10.5 Email Alert about Notification

When a new notification is generated, an alert can be sent to the administrator by email with proper configuration. This process can be done from CAC-GUI.

From Report Config tab, click Report Filter column on a new line, a window will pop up about the filter setup. Choose Cabinet Alert radio box, and then check Security Notification Alert checkbox, and press OK button. The following is the screenshot.



In the related report item, click Report Time column, a window will pop up for setting up time. By default, On Event checkbox is already selected, press OK button, and the setup will be saved.

For more details about the report and email setup, see section 5.5 and section 5.6.

After the report and email configuration is done, an email will be sent to the related email address in real time when a notification is generated. A sample email looks like the following:

Gmail

Security Notification Alert for Cabinet: Remote Cabinet

1 message

zli@pluginstorage.com <zli@pluginstorage.com>
To: zli@pluginstorage.com

AUTOMATIC EMAIL, DO NOT RESPOND

Dear Plug-In Storage Systems Dock & Lock CA Cabinet Administrator,

This is an automatic email from cabinet:
Remote Cabinet

This email is regarding:
Automatically Generated Report

A new Security Notification is generated for BitDefender GravityZone. The following is the details:

Notification Type: New Login
Timestamp: 2022-02-11T19:36:57+00:00
Device IP: 192.168.0.101
Device OS: Linux
Browser: Firefox
Data And Time: 11 Feb 2022, 19:36:57 +00:00
Report Time: Wed Feb 16 13:35:24 2022
Full Content: <14>Feb 11 19:36:59 pssi-gravityzone gravityzone: {"name":"Login from new device","created":"2022-02-11T19:36:57+0
+00:00","device_ip":"192.168.0.101"}

If you have any questions or require further assistance, please contact:

Plug-In Storage Systems
1-800-231-5952
info@pluginstorage.com

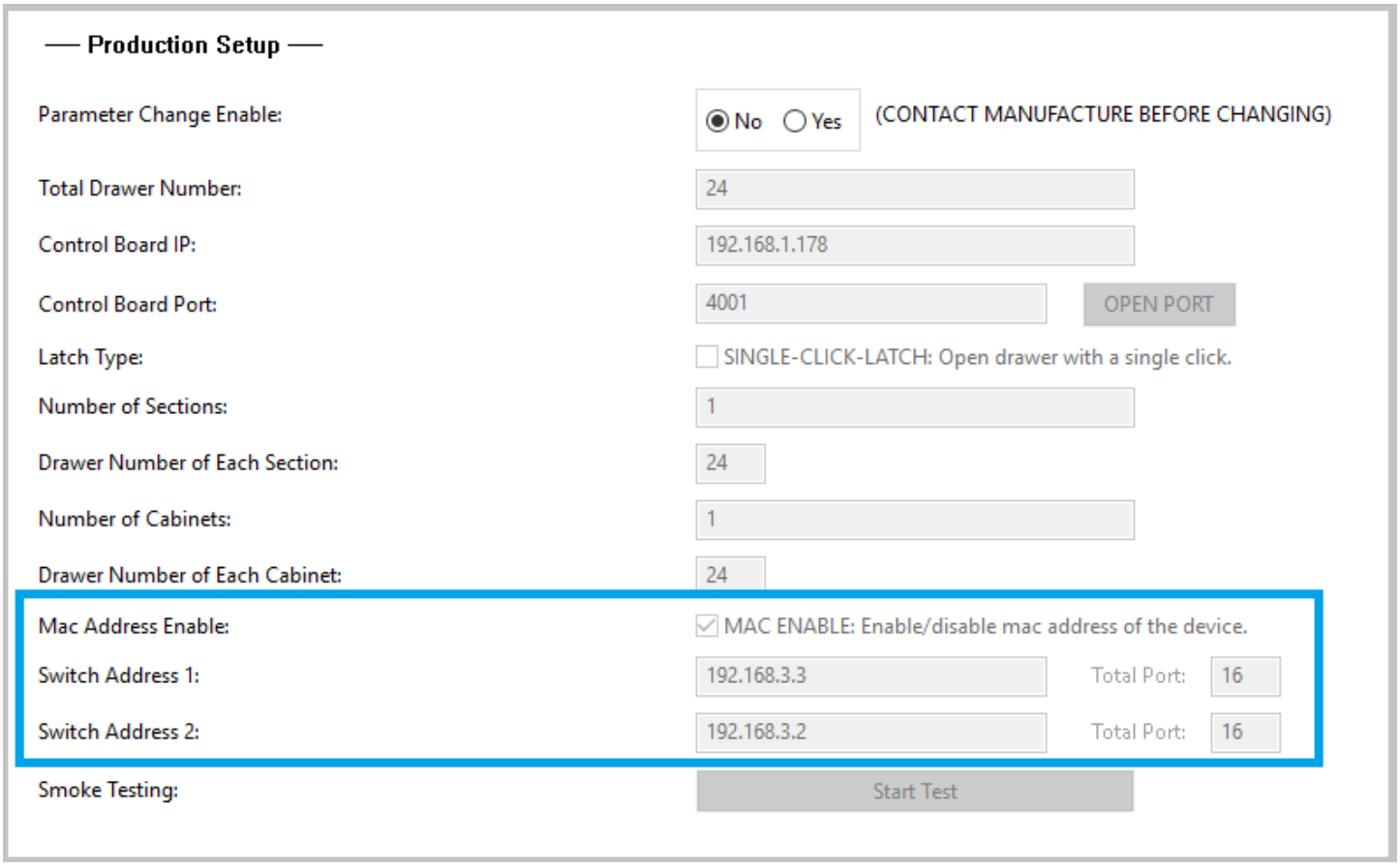
12 MAC Address-based Management

The check-in and checkout activities of a device is normally determined by the drawer status in the CA cabinet. As an alternative solution or a supplement, the activities can also be traced and determined by the status of device MAC address. The MAC address we are using is initially the identifier of the network adaptor located in the device. The number is a unique Identification and can be used to represent the equipment. The advantage of using MAC address to represent a device is that the Equipment ID may be changed in different context, while the MAC address normally will not change for a certain device.

To effectively read the MAC address, the cabinet use a network device (normally a switch) to continuously scan the local network and record the connected device. By using this method, the cabinet can determine the cabinet status in real-time.

12.1 MAC Address Function Setup

When the MAC address function is enabled, all the related information will be displayed; while it is disabled, all the related functions will be hidden and will not be displayed. The MAC address function needs one or more network switch; it is a hardware-related functionality, the configuration locates at the Production Setup section in System Config tab. The following is a screenshot.



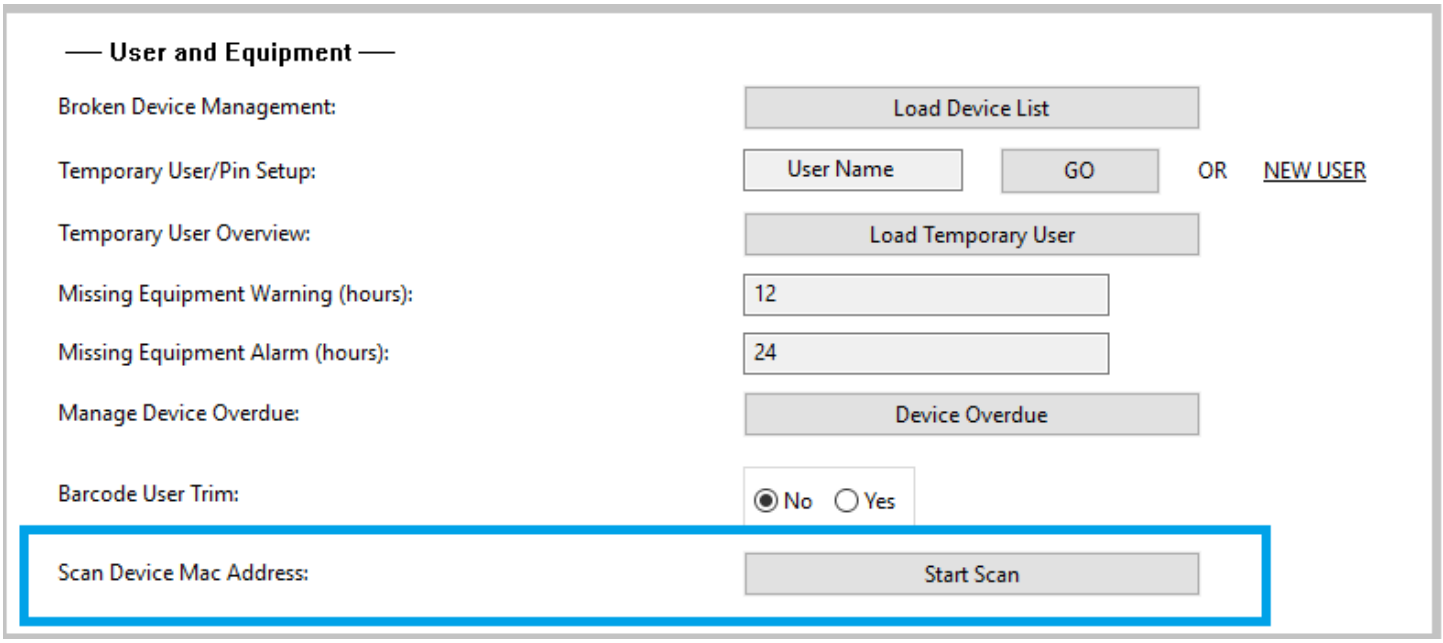
As discussed before, the content in Production Setup section is disabled by default. To enable the edition of this section, it needs to change Parameter Change Enable from No to Yes.

MAC Address Enable Needs to be set selected in the diagram. The field of Switch Address 1 needs to be filled, and the parameter of Total Port of the switch needs to be filled too. The default total port number is 16. Normally one switch is enough for the cabinet, but one more switch might be needed for a master-slave cabinet structure.

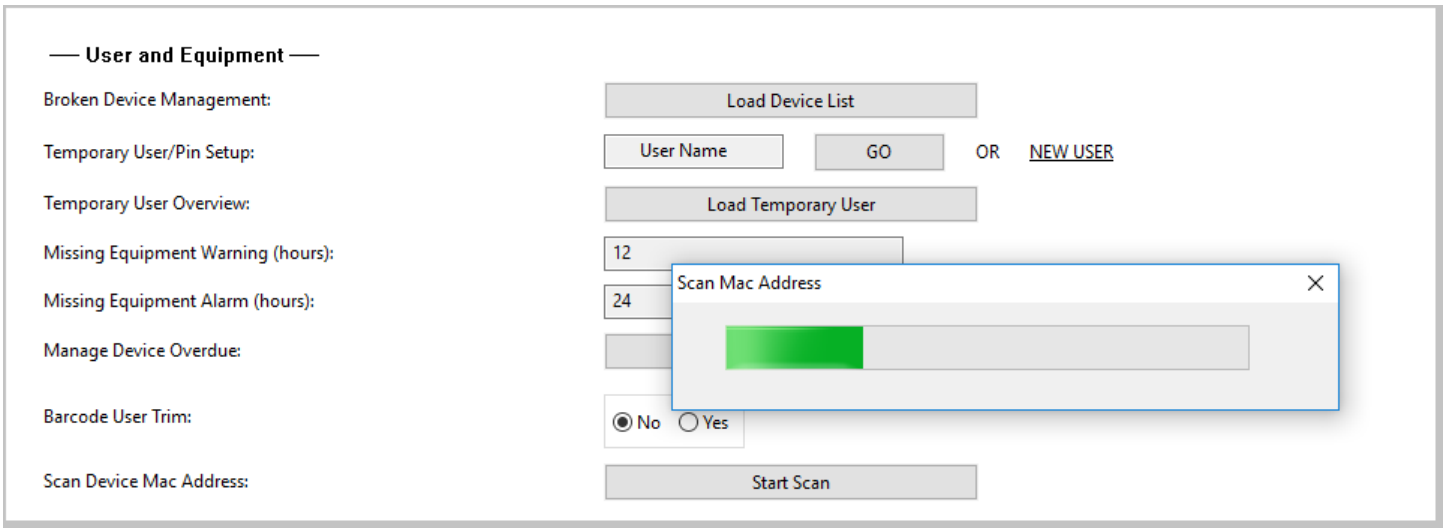
12.2 MAC Address Scan

The MAC address of the device is read in CacManager program and is written to the database. There are two types of scans: the initial scan and the regular monitoring scan.

The object of the initial scan is to read the MAC address of the device and match it with the Equipment ID. The interface of the scan locates at System Config Tab. The following is the screenshot:



Connect the device to the related port of the switch with an ethernet cable, and press Start Scan Button, the scan will begin, and a progress bar will appear as follows:



After the scan is done, the screen will be redirected to the Equipment List tab. The Mac Address column of the table is filled with the scan result. If there is no device connected to the related port, the number will be None.

	DELETE	Blocked	EQUIPMENT IDENTIFYING #	DESCRIPTION of ITEM	U/I	QUANTITY	MISC.	NAME	ENDPOINTID	MacAddress
1	☐	☐	111	description 1	BA - Ball	1	misc 1	DESKTOP-12HEKPL	613fb248d58311abd0df2be8	None
2	☐	☐	222	description 2	BA - Ball	1	misc 2	DESKTOP-7T5NHVD	613f810fa1c8309326faea4e	a0:ce:c8:c1:4e:c2
3	☐	☐	666	description 6	BE - Bale	1	misc 6	None	None	None
4	☐	☐	777	description 7	BE - Bale	1	misc 7	None	None	a0:ce:c8:c1:4e:c8
5	☐	☐	333	description 3	BE - Bale	1	misc 3	None	None	a0:ce:c8:c1:4e:c6
6	☐	☐	444	description 4	BF - BoardFoot	1	misc 4	None	None	None
7	☐	☐	555	description 5	BD - Bundle	1	misc 5	None	None	a0:ce:c8:c1:4e:c4
8	☐	☐	888	description 8	BF - BoardFoot	1	misc 6			00:60:ef:31:06:39
9	☐	☐								

The second type of scan is a continuous monitoring process in CACmanager program. If the MAC address function is enabled, CACmanager will keep running this process automatically. The scanning result will be written in the database to be analyzed to determine the cabinet activities.

12.3 MAC Address Display

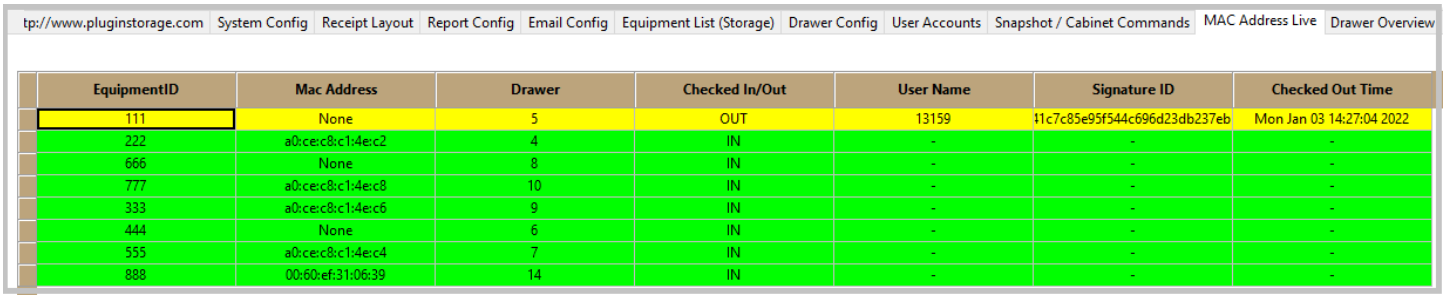
The MAC address value of the device can be seen from the Equipment List tab, Drawer Config tab and the MAC Address Live tab. The Equipment List tab is shown is section 12.2, it matches the MAC Address with related equipment. The table acts as the property description of the device, normally do not need to be modified frequently.

Drawer Config tab also displays the MAC address as one of the properties of the device. It is shown as following:

tp://www.pluginstorage.com | System Config | Receipt Layout | Report Config | Email Config | Equipment List (Storage) | Drawer Config | User Accounts

	DRAWER LOCKOUT	EQUIPMENT IDENTIFYING #	DESCRIPTION of ITEM	U/I	QUANTITY	MISC.	MAC ADDRESS	EQUIP. SELECT
1	☑	111	description 7	BE - Bale	1	-	-	☐
2	☑	-	-	-	0	-	-	☐
3	☑	-	-	-	0	-	-	☐
4	☐	222	description 2	BA - Ball	1	misc 2	a0:ce:c8:c1:4e:c2	☐
5	☐	111	description 1	BA - Ball	1	misc 1	-	☐

MAC Address Live tab is a real-time display based on the device MAC address. It will be hidden when the MAC address function is disabled. The following is a screenshot:

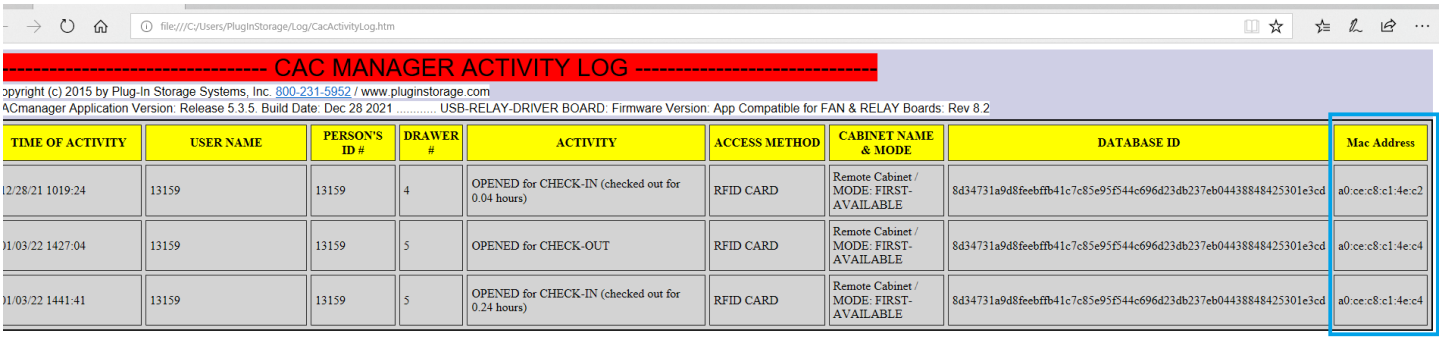


EquipmentID	Mac Address	Drawer	Checked In/Out	User Name	Signature ID	Checked Out Time
111	None	5	OUT	13159	41c7c85e95f544c696d23db237eb	Mon Jan 03 14:27:04 2022
222	a0:ce:c8:c1:4e:c2	4	IN	-	-	-
666	None	8	IN	-	-	-
777	a0:ce:c8:c1:4e:c8	10	IN	-	-	-
333	a0:ce:c8:c1:4e:c6	9	IN	-	-	-
444	None	6	IN	-	-	-
555	a0:ce:c8:c1:4e:c4	7	IN	-	-	-
888	00:60:ef:31:06:39	14	IN	-	-	-

When the device is checked out, the table will display the person who checked out the device and the related information, and the line will become yellow; if the device is still in the cabinet, it is also shown in the table.

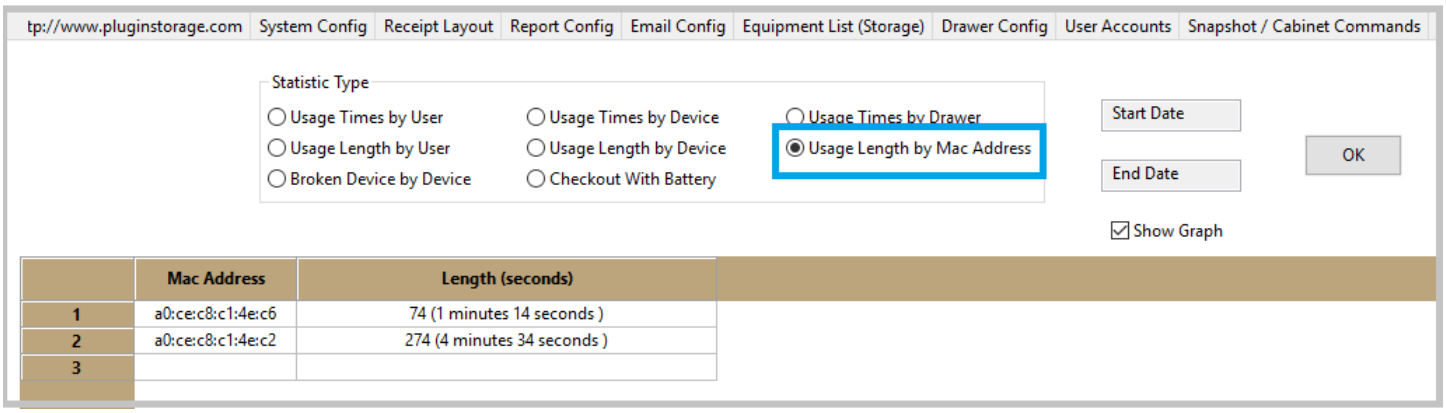
12.4 MAC Address-related Log, Statistics and Diagnostics

When MAC address function is enabled, an additional column Mac Address is added to the log file. The following is a screenshot.



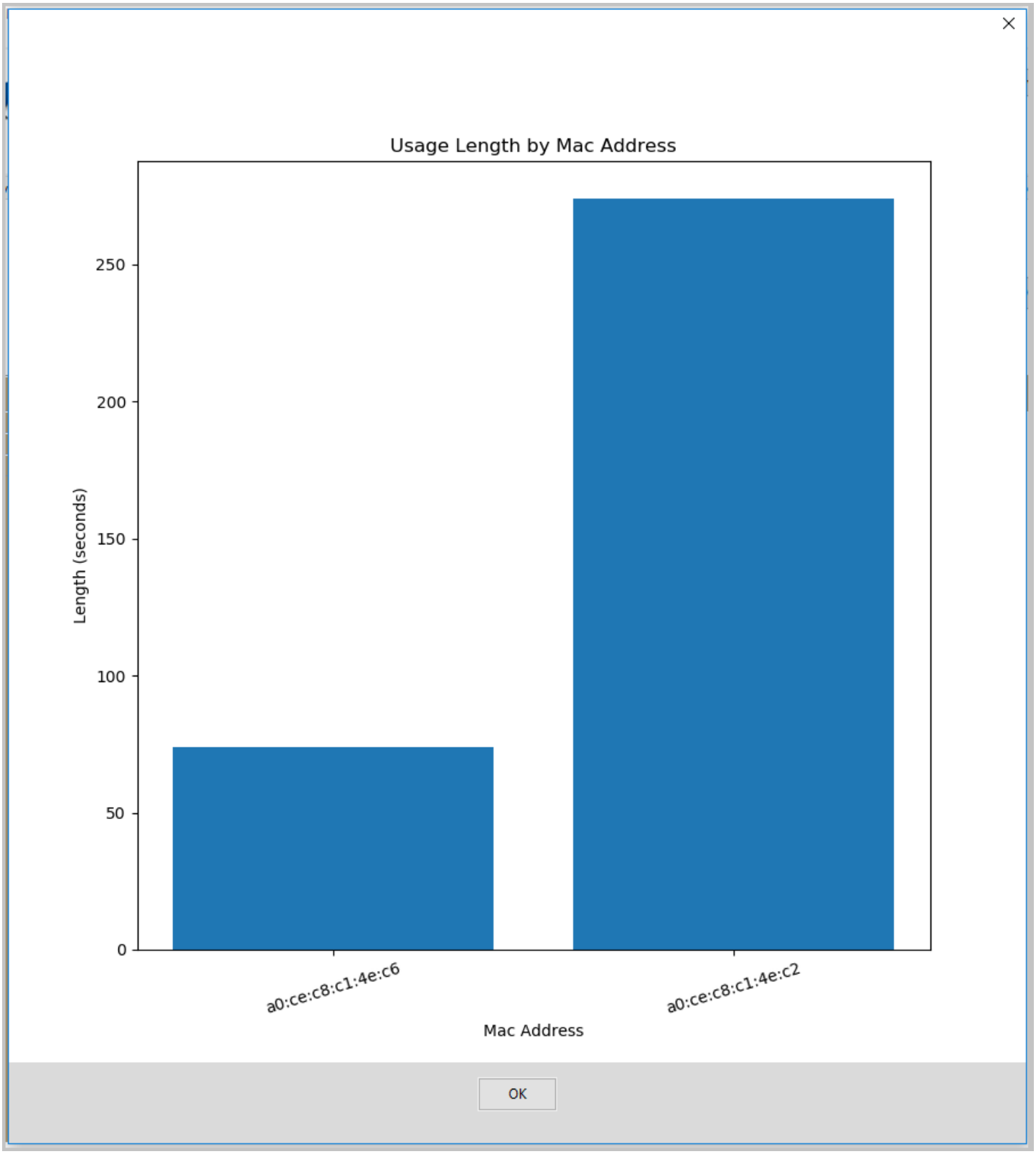
TIME OF ACTIVITY	USER NAME	PERSON'S ID #	DRAWER #	ACTIVITY	ACCESS METHOD	CABINET NAME & MODE	DATABASE ID	Mac Address
12/28/21 1019:24	13159	13159	4	OPENED for CHECK-IN (checked out for 0.04 hours)	RFID CARD	Remote Cabinet / MODE: FIRST-AVAILABLE	8d34731a9d8feebffb41c7c85e95f544c696d23db237eb044388484253 01e3cd	a0:ce:c8:c1:4e:c2
01/03/22 1427:04	13159	13159	5	OPENED for CHECK-OUT	RFID CARD	Remote Cabinet / MODE: FIRST-AVAILABLE	8d34731a9d8feebffb41c7c85e95f544c696d23db237eb044388484253 01e3cd	a0:ce:c8:c1:4e:c4
01/03/22 1441:41	13159	13159	5	OPENED for CHECK-IN (checked out for 0.24 hours)	RFID CARD	Remote Cabinet / MODE: FIRST-AVAILABLE	8d34731a9d8feebffb41c7c85e95f544c696d23db237eb044388484253 01e3cd	a0:ce:c8:c1:4e:c4

A statistics summary related to MAC Address is available in Statistics tab of CAC-GUI. The following is the screenshot:



	Mac Address	Length (seconds)
1	a0:ce:c8:c1:4e:c6	74 (1 minutes 14 seconds)
2	a0:ce:c8:c1:4e:c2	274 (4 minutes 34 seconds)
3		

The table displays the total length of the using for the devices. The following is a screenshot of the diagram related to the statistic table.


Usage Length by Mac Address
Length (seconds)
250
200
150
100
50
0
a0:ce:c8:c1:4e:c6
a0:ce:c8:c1:4e:c2
Mac Address
OK

If some MAC address-related function looks not normal, it can be analyzed by running the diagnostics program. The following is the setup for the diagnostics program, MAC Address is selected by default. After running the function, the details of the issue can be shown in the screen. More details can be found in section 10.2.