Operation Manual

PASSIVE SECURITY SCAN

Passive Portal
Concealed Weapons Detection System

PRELIMINARY

1. Introduction

Figure 1.0

The Passive Security Scan™ or Passive Portal is a next generation walk-through weapons and contraband detection system. This patented and trademarked product is a technologically advanced passive scanning system for detecting and identifying concealed threats and contraband. Passive Portal consists of eight highly developed sensors that read the constantly changing variations in the earth's magnetic field. These same sensors have applications in places such as along the San Andreas Fault, where they measure changes in the earth's magnetic field to anticipate earthquake activity. The sensors inside the frame are connected to a microcontroller-controlled circuit board that effectively creates a "curtain" in the doorway.

When the system is activated, a reading is taken between the four sensors on either side of the frame to establish a "normal" or ambient baseline reading of its environment. Because the earth's magnetic field is never static, the system regularly self calibrates. When the subject passes through the "curtain" with something of a metallic nature, an invisible wave of variation is generated where the signal has the greatest strength. The Passive Security Scan software provides a visual indication of where the item is located on the subject as well as an approximation of the size of the item.

We want to thank-you for purchasing the Passive Security Scan system. We at Passive Security Scan

Inc. are always eager to assist you in optimizing the Passive Portal's performance for your application. We encourage you to call us when contemplating a new application or when encountering a problem. To this end, if you have any questions or comments regarding Passive Security Scan or this manual, please feel free to contact us via the following methods:

- phone: 1 (800) 520-9485
- E-mail: dtii@defensetechnologiesintl.com

Important! To ensure the proper and safe operation of the Passive Portal system it is highly recommended that the customer read all the materials provided prior to operating the Passive Portal system.

2. General Description

The Passive Portal gateway is a passive sensing walk-through concealed weapons and contraband detection system that is easy to setup and use. The system has an approximate throughput rate of 1200 persons per hour. The system is equipped with a break-beam infrared sensor that when broken by a person entering the gateway it triggers a scanning/screening operation. The passive sensing means no electromagnetic radiation is emitted from the gateway, unlike commonly used airport metal detectors.

The system utilizes eight highly sensitive sensors that detect variations that occur in the earth's magnetic field when a large metallic object, such as a gun, moves through this field. These sensors are only sensitive to ferromagnetic objects which greatly reduces false positive alarms common in metal detectors due to keys, belt buckles and others metallic objects. The system is a self-contained design, meaning that it is designed to operate in stand-alone mode without the need of having a computer controller connected to it. It can also operate in peripheral mode, where a computer controller unit is attached to the gateway, via a USB cable, to monitor and control its operation. A Bluetooth radio is also available to allow the gateway to be controlled and monitored via Bluetooth enabled devices such as a laptop computer or Android smartphone or tablet.

When a person enters the gateway opening, the passive infrared break-beam sensor detects the person's entrance and triggers the system to scan the person for weapons or other contraband objects as he or she walks through the gateway. When the scan is complete, the gateway presents to the operator the scan results via the light indicators located at the top of the gateway. A green indication means that the person did not have a detectable object. A red indication means that the person possesses an object that meets or exceeds the Maximum level threshold (these thresholds and other terms will be explained further in this manual). The blue indication means that the system is busy and re-calibrating. When this blue indication is off, the system is again ready to scan. There is also a Red-light Green-light indicator on the back of the Passive Portal to help the operator control patron traffic.

The system is designed to automatically save all scan results into its build-in memory in a log file along with the timestamp of the scan. This log file of scan results can be viewed via a computer controller, such as a desktop or laptop or tablet with the Passive Security Scan software installed, which is connected to the gateway via a USB cable or via a Bluetooth device.

The computer controller unit can be a desktop or laptop computer or tablet with the supplied software installed. The software allows security personnel to monitor the gateway results in real time and control various parameters of the gateway's operation. The software also monitors security personnel and operators, recording their actions as they use the program and gateway, to prevent and provide proof of unauthorized changes in the configuration of the gateway parameters and most importantly its alarm threshold set points. Every action preformed by security personnel is logged along with a timestamp of the operation.

If a computer controller is used, the Passive Security Scan software can be configured so that an image of the person who has a Maximum detection level be automatically taken via a standard USB camera connected to the computer controller and aimed at the gateway opening. This picture is then presented to security personnel along with the scan data to positively identify the person of interest. The scan results are also embedded into the picture file to ensure data tracking security for probable cause.

The Passive Security Scan for Windows software can also be configured to send an email alert to authorized security personnel that contains the scan results and image of the person, if a USB camera is used. This greatly aids in the detention of the offending person. Please contact us if you would like to purchase this option.

The Passive Portal is warranted free of defects in materials and workmanship for a period of ninety (90) days. Prior to the return of a unit or any portion thereof, Passive Security Scan Inc. must be consulted with to avoid unnecessary shipping. If the return of the equipment is deemed necessary, a Return Material Authorization (RMA) number will be assigned. This number must be recorded on the outside of the shipping container and on the included packing list.

---

3. System Components and Assembly

Figure 3.0

3.1 Passive Portal Gateway

The Passive Portal gateway includes all the necessary components to operate the system as a stand-alone walk-through weapons detection system. The unit comes with an AC to DC power converter that is compatible with 120/240-volt, 50/60 Hz, AC input. The system can also be powered via the optional 12-volt DC battery or solar panel power supplies. Please ask your representative for more details about these power options if interested. The input power connection is located on the side panel of the Passive Portal gateway, along with the USB control cable port, calibration button, and the on-off switch. The Passive Portal gateway is constructed from light weight aluminum to retain durability and yet be light enough to allow easy relocation.

The Passive Portal system is designed to automatically save all scan results along with the timestamp of the scan into its build-in SD card memory. This log file of scan results can be viewed via the computer controller with the Passive Security Scan software installed and connected to the gateway via a USB cable or via a Bluetooth device, if this option was purchased.

3.1.1 Top Panel LED Indications

The Passive Portal system has three LED indicators to inform the operator of the status of the gateway and the results of a scan when a person walks through the gateway (See figure 3.1.1).

Figure 3.1.1

The topmost indicator is the Red LED indicator, which indicates when lit and accompanied by an audible alarm that the scan resulted in detecting an object that meets or exceeds the Maximum alarm or threshold set point, meaning a weapon or other large ferrous metal item was detected.

Beneath the Red LED indicator is the Green LED indicator, which indicates when lit that a scan resulted in detecting no objects and that the scan levels detected were below the Maximum alarm or threshold set point, meaning it is most likely that the screened person is unarmed or is void of harmful ferromagnetic objects.

The bottommost LED indictor is the Blue LED indicator, which indicates the gateway's status. If the Blue LED indicator is unlit, the gateway is ready for personnel to walk through the gateway to be screened.

There is also a Red light Green light indicator on the back of the Passive Portal to help the operator control patron traffic.

When a person enters the Passive Portal gateway opening, a passive infrared sensor curtain detects the person's movement and triggers the system to scan the person for weapons or other contraband objects. When the Blue LED turns on, this indicates to the operator that the gateway is busy scanning the person for weapons or other potential threats. When the Blue LED indicator turns off, this indicates that the gateway is finished with the scan and that the system is again ready for personnel to walk through the gateway to be screened. After this scan cycle has completed, the resultant condition, i.e. Good scan (Green LED lit) or Maximum alarm scan (Red LED lit) will be shown. This resultant scan condition persists, meaning the last resultant scan condition will remain indicated on the Top Panel LED Indicators until new scan cycle occurs. This gives security personnel a quick visual reference as to the last scan condition or result.

3.1.2 Connection Side Panel

On one the side of the Passive Portal gateway is the Connector and Controls panel. This panel contains the On-Off power switch, the 12-volt DC power input connector, and the USB cable.

3.1.2.1 On-Off Switch

The On-Off switch on the Connection Side Panel applies power to the Passive Portal system. When the power switch is in the 'On' position, the switch gives a visual "On" indication by showing a red indication color along the sides of the toggle paddle of the switch. When the system is turned 'off' this red indication is no longer visible.

When the Passive Portal gateway is first turned on, the gateway goes through a boot up sequence. This boot up sequence can be monitored by watching the Top Panel LED Indicators. When the boot sequence starts, the Red, Green, and Blue LED indicators will all be lit. As the boot up sequence continues each lit indicator will turn off (typically in ten second intervals). First the Red indicator turns off, then the Green indicator turns off, and lastly the Blue indicator turns off, after which the system will self calibrate, as indicated by the Blue LED turning on. When the system is finished calibrating itself to its surroundings, the Blue LED indicator will turn off and the gateway is ready to screen personnel.

Note: Every time that the system is turned "On" this boot up sequence occurs, as depicted by the LED indications described above. This boot sequence includes a required 30-second delay to allow the PIR sensor to calibrate to its surroundings. While the boot up sequence is running, do not allow personnel to enter the Passive Portal gateway. This ensures the maximum sensitivity of the PIR sensor curtain.

3.1.2.2 12-volt DC power input connector

The Passive Portal system includes an AC to DC power converter. The AC to DC power converter is compatible with 120/240-volt, 50/60 Hz, AC input power and provides the gateway 12-volt DC input power. Only the provided AC to DC power converter should be used to power the Passive Portal gateway. If your AC to DC power converter is faulty, please contact your representative for a replacement. Using other AC to DC converters may damage your Passive Portal system. The optional battery and solar power options are also plugged into this connection.

3.1.2.4 USB control cable port

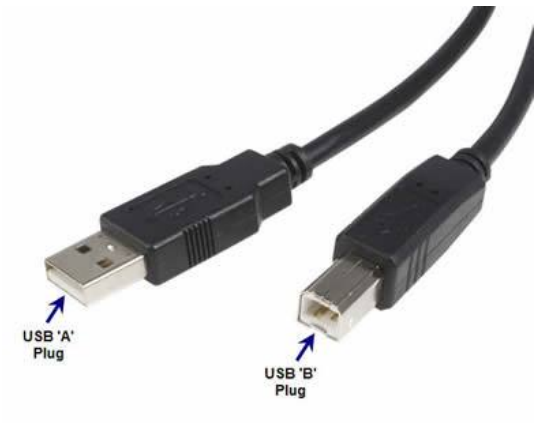


Figure 3.1.2.4

The Passive Portal system includes a standard USB-A to USB-B cable that is used to connect the Passive Portal gateway to the included Windows® based computer controller tablet. This allows system operators to control and monitor the Passive Portal system via the Passive Security Scan

software. The USB-B connector is connected to the gateway at the USB connection located on the Connection Side Panel and the USB-A connector is plugged into a USB port on the Desktop or Laptop computer controller with the Passive Security Scan software installed.

Note: If the USB cable is connected to both the computer controller unit and the Passive Portal gateway, Bluetooth operations are not possible if this option was purchased.

3.2 Passive Security Scan Software

The Passive Security Scan software on the included Windows tablet, allows operators to control and monitor the Passive Portal gateway. This software has many convenient features to aid the operator in determining the size and location of the detected item.

3.3 Assembly and Installation

3.3.2 Unboxing

The Passive Portal is shipped in a custom container which should be kept so that you can ship the Passive Portal system back for warranty repair or upgrades. The box contains:

1. The Passive Portal gateway and a package housing the two stand assemblies and eight (8) assembly screws,

2. The Passive Security Scan computer control tablet with the Passive Security Scan software installed, a charging cable for the tablet,

3. A Passive Portal 120-volt AC to 12-volt DC power supply and the Bluetooth antenna,

4. A USB controller cable and Operations Manual

3.3.3 Assembly

To assemble the Passive Portal, remove the stand assemblies and screws from their package. With the Passive Port still laying down, lift one Passive Portal leg and install that side's stand using four of the included screws. Do the same with the other leg. Ensure all eight screws are properly tightened. Install the Bluetooth antenna on the terminal on top of the Passive Portal frame, and then lift the Passive Portal into the upright position.

4. System Operation

Passive Portal is designed to operate in two distinct modes of operation: Stand-alone and as a Computer Peripheral. Both modes of operation are described below.

4.1 Stand-alone Operation

When the system is in Stand-alone mode, it is not connected to a Computer Controller unit, such as a PC Desktop or Laptop computer. The only difference between the two modes, Stand-alone mode and Computer Peripheral mode, is that in Stand-alone mode, when the Passive Portal system senses an

item that meets or exceeds the Maximum alarm set point setting, the alarm sounds for approximately 5-seconds and the Red LED at the top of the gateway lights up indicating an alarm condition.

To operate the system in Stand-alone mode, the operator ensures that the AC to DC power converter is connected to both a 120-volt AC wall outlet and also to the 12-volt DC power input connector located on the Connection Side Panel. The operator then turns the system on via the On-Off switch also located on the Connect Side Panel.

When the power switch is in the 'On' position the switch gives a visual indication by showing its red indicator color located on the sides of the paddle on the switch. When the gateway is first turned on it goes through a boot up sequence. This boot up sequence can be monitored by watching the Top Panel LED Indicators. When the boot sequence starts, the Red, Green, and Blue LED indicators will all be lit. As the boot up sequence continues each lit indicator will turn off (typically in ten second intervals). First the Red indicator turns off, then the Green turns off, and lastly the Blue indicator turns off, after which the system will self calibrate, as indicated by the Blue LED turning on. When the system is finished calibrating itself to its surroundings, the Blue LED indicator will turn off and the gateway is ready to screen personnel.

Note: To set the Maximum alarm set points it is necessary to run the Passive Portal gateway as a Computer Peripheral using a Desktop, laptop, or smart phone with the Passive Security Scan software installed.

4.2 Computer Peripheral mode using Passive Security Scan software for Windows® and Android®

When the Passive Portal system is connected to a Computer Controller unit with the Passive Security Scan software installed and running, the gateway operates as a Computer Peripheral, meaning that data can pass to and from the Passive Portal gateway and the Passive Security Scan software. In this mode the system operator has additional information available to aid in determining the size and location of detected items via the Passive Security Scan graphical user's interface. Here, scan data is converted to easy to read and understand waveform and item location data (See Figure 4.2).

As shown in the Figure 4.2, the Passive Security Scan main window shows scan results in both waveform data and location data. The waveform data is shown in the left-hand side of the main window and the location data is shown in the right-hand side of the main window. Both the waveform data and location data are referenced as if the person scanned is coming toward the operator through the gateway.

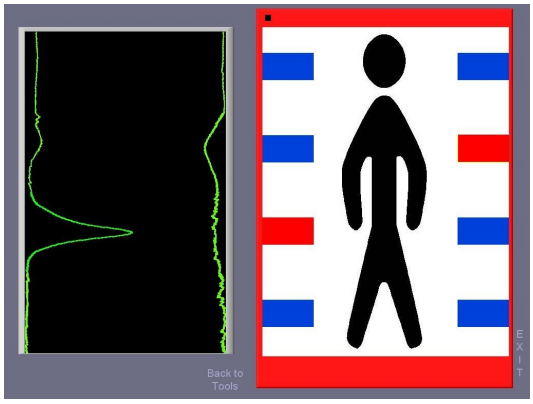


Figure 4.2

In the Figure 4.2 example above, the waveform data shows two wave forms one for the left side sensors and one for the right-side sensors. As you can see, the waveforms in this example show two distinct and different detection peaks, a large peak near the right-hand pants pocket of the person scanned and a smaller peak near the left-hand shoulder region of the person scanned. The location data in this example, shows that the detected items met or exceeded the Maximum alarm set point, so this location data is shown in red near the right-hand side pants pocket region and near the left-hand shoulder region of the person scanned. In this example, the subject had a small firearm in his right-hand pants pocket and a knife in his left-hand coat lapel pocket. The blue location data shows no item was detected by those sets of sensors.

Note: While operating in Computer Peripheral mode, all user movement and actions in the Passive Security Scan software are logged into a log file along with a time stamp of when the movement and action occurred to prevent and monitor unauthorized actions and provide proof of the action.

4.2.1 Using the Passive Security Scan for Windows® and Android®

The Passive Security Scan for Windows or Android software is already installed on the included Window or Android tablet.

4.2.1.1 Starting Passive Security Scan

A Passive Security Scan shortcut icon is placed on the Windows desktop of the tablet. The Android tablet automatically starts Passive Security Scan when powered up. When Passive Security Scan first starts, it is not connected to the Passive Portal gateway. You can connect to the Passive Portal gateway via a connected USB cable or via Bluetooth using the Connect to Passive Scan button.

If connecting via USB, ensure that the USB Cable is connected to both the Computer Controller and the Passive Portal gateway and ensure that the Passive Portal gateway is turned on. If the gateway was turned on or operating prior to connecting the USB cable to both the PC and the gateway, the Passive Portal system will reboot to change operating modes. Please wait until the Passive Portal gateway has finished with its booting process before trying to connect to the gateway via the Passive Security Scan software. Once these conditions are met, click on the Connect via USB button.

If connecting via Bluetooth, the USB cable must be disconnected from the Passive Portal. It is necessary for the operator to know which COM port the Bluetooth Radio, installed in the desktop or laptop, is located (i.e., COM1, COM2, etc.). To find which COM port is used for the Bluetooth Radio, click on the Bluetooth Device icon in the Windows System Tray. This will open a window titled Bluetooth Devices which has tabs. One of the tabs in this window will be named COM Ports. Clicking on the COM Ports tab allows Windows to search and find your Bluetooth Radio and then present to you the COM port that it is on. The COM port to use is the “outgoing” port. If an “outgoing port” is not present, you may need to refresh your devices via the Windows Device Manager. Remember this “outgoing” COM port number, as it will be used to connect the gateway to the Passive Security Scan software.

If connecting via Bluetooth, click on the drop-down list under Please Choose Port for BT heading presented by the Passive Security Scan software. Select the COM port that Windows told you that your “outgoing” Bluetooth Radio was connected to and click on the Connect via BT button. This will connect the Passive Portal gateway to the Computer Controller via Bluetooth.

After the Passive Portal gateway is connected to the Passive Security Scan software, the system will log the user in. Please note that the operator may need to enter a username and password to log in. This depends on Passive Security Scan’s configuration. The software then opens the gateway’s current log file for review and/or possible deletion, depending on the software configuration purchased by the security management and facility security policy. Lastly the software calibrates the gateway. After

calibration is complete, the Passive Security Scan software and the Passive Portal system are ready for patron screening operations.

Note: If the USB cable is connected to both the Computer Controller unit and the Passive Portal gateway, Bluetooth operations are not possible.

Note: Connectivity via Bluetooth or USB cabling is the only difference in operation of the Passive Security Scan for Windows software.

4.2.1.2 Basic Passive Security Scan Operation

When a scan is triggered by someone entering the Passive Portal gateway, the Passive Security Scan software will show this to the operator by presenting a Scanning indicator at the bottom of the interface. After the scan has finished, these borders will change to another color depending on if the scan was normal, which is typically shown as green, or met or exceeded the current Maximum set point which is typically shown as red. This gives the operator a quick visual indication of the scan results. The typically shown colors are the defaults and the system manager may have set these to other colors (explained further below) depending on security policy.

4.2.1.3 Advanced Passive Security Scan Operations

On the Passive Security Scan main screen, at the lower left-hand side are two buttons; one labeled “Tools and Settings”, the other labeled “Calibrate Gateway”. Clicking on the “Tools and Settings” opens the Tools and Settings screen. Here you will find various parameters to monitor and control the gateway such as the Time of Last Scan, Alarms, Scans Today, reading and setting the gateway’s Real Time Clock, reading, and setting the Maximum Threshold or set point, change Alarm Colors, Show Waveform or Chart from sensors, whether Password log in is required, and usage of Voice Alerts. This screen also has subprograms to Read Gateway Log File, Change User list and passwords, Open the Archive Viewer, Run Diagnostics, Reboot the Passive Scan system, and Update the Firmware. On this screen, you can also calibrate the gateway or return to the Main Screen.

Note: The Tools and Settings window can be password protected to prevent unauthorized movements and actions. Security management may be the only authorized personnel to view this screen to maintain the integrity of the Passive Portal system.

The Time of Last Scan parameter shows the time stamp of the last scan taken and processed by the Passive Security Scan software since it was started. The Scans Today shows the number of scans taken and processed by the Passive Security Scan software since it was started, and the Alarms shows how many scans during the session were alarms.

The “Read Gateway Clock” button sends a command to the Passive Portal gateway. The gateway responds with the current time that was saved into the Real Time Clock chip’s internal memory of the gateway. This clock can be synchronized with the Computer Controller’s time by clicking on the “Set Gateway Clock” button.

The Maximum Threshold, or set point, shown when Passive Security Scan is running, is the currently set Maximum set point that is read when the Passive Portal gateway and Passive Security Scan software were first connected. This setting can be changed by moving the set point slider, or by highlighting and typing in the new setting into the text box next to the slide control. Clicking “Save Settings to Gateway” button saves the new setting to the firmware on the Passive Portal gateway.

Note: While operating in Computer Peripheral mode, all user movement and actions in the Passive Security Scan software are logged into a log file along with a time stamp of when the movement and action occurred, to prevent and monitor unauthorized actions.

The colors presented to the operator for Maximum alarm can also be changed. This is done by clicking either the Maximum color control and then selecting an appropriate color for the set point.

The “Show Waveforms” selection controls whether the waveform graph is populated by the data received from the gateway, to help operators identify the detected item’s location during a scan. The default is to always show the waveform data. The “Show Waveform” button shows the waveform of the last scan.

The “Show Chart” selection controls whether the chart graph is populated by the data received from the gateway, to help operators identify the detected item’s location during a scan. The default is to always show the waveform data. The “Show Chart” button shows the waveform of the last scan.

The “Require User Password” selection, controls if a user is required to log on to the Passive Security Scan software to use it.

The “Use Voice Alerts” selection controls if voice alerts are enabled for alarm conditions. Here, the Passive Security Scan software will inform the user the location of the item detected.

The “Camera Imagery” selection, if this option was purchased and enabled, if checked, allows the use of USB cameras in correlation with the Passive Portal gateway. Here, when a scan is triggered, the USB camera is also triggered to take a snapshot and send it to the Passive Security Scan software for display in place of the patron icon normally displayed. If the camera is properly aligned and aimed at the entry of the gateway, this snapshot will be a picture of the person who is currently being scanned. After a scan and if the person scanned has contraband that meets or exceeds the Maximum set point level, the scan readings are embedded into the image and the image is saved to the Archive folder for future reference. This is very helpful for probable cause and positive identification of an offender that is armed or has contraband. The picture is not saved if the scan readings do not meet or exceed the Maximum set point level.

The “Read Gateway Log File” button opens the gateway log viewer and downloads from the Passive Portal its logged scan data on the built-in SD card. This viewer allows saving the log file to the control computer and allows the ability to delete the log file on the gateway memory.

The “Change User List” button when clicked opens the User List entry program. Here usernames PIN number, passwords, and email addresses to receive alarm alerts can be entered, or users can be deleted. This program is typically customized for end users depending on the needs of security management or end users. The basic program included with Passive Security Scan can be sufficient for many security facilities, if not please contact your Passive Security Scan Inc. representative. The Passive Security Scan software can be set up to automatically send emails to email recipients in the User List. This email consists of the resultant alarm Main Screen and the offending person’s image, if a USB camera is used.

The “Open Archive Viewer” allows users to review archived scans or imagery of persons scanned if a USB camera is utilized. When clicked on, the Historical Image Viewer program is opened and the last scan or image of a person with contraband is shown along with the readings of the scan superimposed on the image. The user can call up any dates available in the archive folder to review all images taken by Passive Security Scan.

The “Run Diagnostics” button runs the on-board diagnostics routine in the firmware. The routine returns data from the Passive Portal to allow system checks on each sensor and system calibration.

The “Reboot Passive Scan” button reboots the Passive Portal remotely via the Passive Security Scan software.

The “Update Firmware” button will install the latest update received by management. Please consult your security management and Passive Security Scan representative for more information. This control can be password controlled.

4.2.2 Using the Passive Security Scan Android® Tablet

4.2.2.1 Starting Passive Security Scan

The Passive Security Scan tablet can be turned on by either pressing the Power button located on the top of the tablet or when the power cable is plugged in either into the tablet with 12-volt DC battery, or when the 120-volt AC adapter is plugged into a wall socket. When Passive Security Scan first starts, it is not connected to the Passive Portal gateway. You can connect to the Passive Portal gateway via a connected USB cable or via Bluetooth using the Connect to Passive Scan button.

If connecting via USB, ensure that the USB Cable is connected to both the Passive Security Scan Tablet and the Passive Portal gateway and ensure that the Passive Portal gateway is turned on. If the gateway was turned on or operating prior to connecting the USB cable to both the PC and the gateway, the Passive Portal system will reboot to change operating modes. The Passive Security Scan Tablet will automatically detect the USB connection.

If connecting via Bluetooth, the USB cable must be disconnected from the Passive Portal and the Passive Security Scan Tablet. Pressing the Connect button opens a dialog box where you can connect to the Passive Portal, or scan for the Passive Portal’s Bluetooth radio. Pressing Scan for Devices initiates this process. Once the Passive Portal radio is found, press its listing to connect via Bluetooth.

After the Passive Portal gateway is connected to the Passive Security Scan software, the Passive Security Scan software and the Passive Portal system are ready for patron screening operations.

Note: If the USB cable is connected to both the Passive Security Scan Tablet and the Passive Portal gateway, Bluetooth operations are not possible.

Note: Connectivity via Bluetooth or USB cabling is the only difference in operation of the Passive Security Scan for Windows software.

4.2.2.2 Basic Passive Security Scan Operation

When a scan is triggered by someone entering the Passive Portal gateway, the Passive Security Scan software will show this to the operator by presenting a Scanning indicator at the bottom of the interface. After the scan has finished, these borders will change to another color depending on if the scan was normal, which is typically shown as green, or met or exceeded the current Maximum set point which is typically shown as red. This gives the operator a quick visual indication of the scan results. The typically shown colors are the defaults and the system manager may have set these to other colors (explained further below) depending on security policy.

4.2.2.3 Advanced Passive Security Scan Operations

On the Passive Security Scan main screen, at the lower left-hand side are three buttons; one labeled “Connect, one labeled “Settings”, and another labeled “Calibrate”. Clicking on the “Settings” opens the Settings screen. Here you will find various parameters to monitor and control the gateway such as the Time of Last Scan, Alarms, Scans Today, reading and setting the gateway’s Real Time Clock and tablet clock, reading, and setting the Maximum Threshold set point, change Alarm Colors, Show current scan data, usage of Voice Alerts, and usage of USB webcam. This screen also has subprograms to Read Portal Log File, Open the Archive Viewer, Run Diagnostics, Reboot the Passive

Scan system, and Reset Defaults of the tablet and Passive Portal. On this screen, you can also calibrate the gateway.

The Time of Last Scan parameter shows the time stamp of the last scan taken and processed by the Passive Security Scan software since it was started. The Scans Today shows the number of scans taken and processed by the Passive Security Scan software since it was started, and the Alarms shows how many scans during the session were alarms.

The “Set Tablet Time” opens a dialog to allow you to connect to the Internet via Wi-Fi. Once connected the network local time is used. This must be done every time the tablet is disconnected from power as the tablet does not have an internal battery to save the time. The “Read Portal Clock” button sends a command to the Passive Portal gateway. The gateway responds with the current time that was saved into the Real Time Clock chip’s internal memory of the gateway. This clock can be synchronized with the Computer Controller’s time by clicking on the “Set Portal Clock” button. To set your time zone, long press the date and time reading. This will open a dialog to allow you to select your preferred time zone. Pressing Done will update the tablet to this new time zone.

The Alarm Setpoint, shown when Passive Security Scan is running, is the currently set Maximum set point that is read when the Passive Portal gateway and Passive Security Scan software were first connected. This setting can be changed by pressing the + or – buttons, or by pressing the Alarm Setpoint readout, which will open a numerical keyboard to allow you to type in the new setting into the text box. Pressing the “Done” button closes this keyboard. You must press the “Set Setpoint” button to save this setting to the Passive Portal’s firmware.

The colors presented to the operator for Alarm Color can also be changed. This is done by clicking the Alarm Color control and then selecting an appropriate color for the set point. This can also be done for the Safe Color.

The “Current Scan Data” button shows the last scan result.

The “Run Diagnostics” button runs the on-board diagnostics routine in the firmware. The routine returns data from the Passive Portal to allow system checks on each sensor and system calibration.

The “Read Portal Log File” button opens the gateway log viewer and downloads from the Passive Portal its logged scan data on the built-in SD card. This viewer allows saving the log file to the control computer and allows the ability to delete the log file on the gateway memory. It is suggested to delete this log file from the Passive Portal occasionally as to not fill up its internal memory.

The “Use Voice Alerts” selection controls if voice alerts are enabled for alarm conditions. Here, the Passive Security Scan software will inform the user the location of the item detected.

The “Scan History” button opens a list of all alarm scans for the session, each of which can be pressed to open that scan data for review.

The “Open Archive Viewer” allows users to review archived scans or imagery of persons scanned if a USB camera is utilized. This program is much like a common file browser with the date folders containing scans, log, and diagnostic files. The user can call up any dates available in the archive folder to review all images taken by Passive Security Scan. Long pressing on the date folders or any of the individual files allows you to send these files to another person’s email account via your Gmail or Outlook account. This is useful for sending daily reports of the Passive Portals operation.

The “Use Camera” button allows the use of USB cameras in correlation with the Passive Portal gateway. Here, when a scan is triggered, the USB camera is also triggered to take a snapshot and send it to the Passive Security Scan software for display in place of the patron icon normally displayed. If the camera is properly aligned and aimed at the entry of the gateway, this snapshot will be a picture

of the person who is currently being scanned. After a scan and if the person scanned has contraband that meets or exceeds the Alarm Setpoint, the scan readings are embedded into the image and the image is saved to the Archive folder for future reference. This is very helpful for probable cause and positive identification of an offender that is armed or has contraband. The picture is not saved if the scan readings do not meet or exceed the Maximum set point level.

The “Reset Defaults” button when clicked resets the Alarm Setpoint, the Alarm and Safe colors, if Camera is used, if Voice Alerts are used, to factory settings. It also, if the Passive Portal is connected, synchronizes the Alarm Setpoint with the Passive Portal to factory settings.

The “Reboot Passive Scan” button reboots the Passive Portal remotely via the Passive Security Scan software.

To check for updates for the Passive Security Scan software long press the Software Version number. Here a dialog will open to prompt you to connect to Wi-Fi and then Update the system. If an update is available, it will be automatically downloaded and installed. After successful installation, the tablet will reboot.

Pressing “Exit” turns off the Passive Security Scan software and tablet. This is the preferred way to turn off the tablet so that data is not lost. The power button can also be used to turn off the tablet or restart it.

The basic program included with Passive Security Scan can be sufficient for many security facilities, if not please contact your Passive Security Scan Inc. representative. The Passive Security Scan software can be set up to automatically send emails to email recipients in the User List. This email consists of the resultant alarm Main Screen and the offending person’s image, if a USB camera is used.

Setup Considerations of the Passive Portal:

The Passive Security Scan, or Passive Portal, is a stand-alone structure that resembles a door frame. When setting up the Passive Portal there are a few space factors to consider. The first space factor to take into consideration is where people who are waiting to walk through the Passive Portal (scannees) will stand. Ideally, there would be no wait for use of the Passive Portal, but this is probably unrealistic in a school environment where the entire population of students will be arriving over a very short period.

Your school should determine how many scannees will arrive and at what rate. Most detection programs will need to operate indoors, or under a shelter, and your school needs to provide a comfortable environment for those waiting. This usually means that there must be enough shelter for the queue of scannees that might build up at any one time and that they should not be overly crowded. There should also be some way of clearly forming a line for scannees to stand in if they will be arriving at a much greater rate than can be processed; eliminating the opportunity for cutting in line would clearly be important in a school to reduce possible fights.

To avoid sending conflicting signals to the Passive Portal, the scannee waiting in line to use the Passive Portal next should be kept back 3 feet from the current user walking through the Passive Portal. It is suggested that a line of tape or paint be placed at this distance, or a mat/rug of the appropriate length can be used. Operators of the equipment and scannees who have already walked through also need to be at least 3 feet or more from the portal in all directions.
It is recommended that tables be placed on either side of the Passive Portal area, to provide an enclosed secure zone to pipe students into that zone, and to allow bags and other stowage items to be searched if an alarm condition is given. In some schools, plastic bins or trays are provided so that students can place metal items in these trays for visual inspection and to help reduce false positives.

It is very important that there be neither space nor opportunity for members of the population, including employees, to walk around the Passive Portal. Very definitive boundaries must be established to prevent circumvention of the system and prevent pass back of contraband, where such prohibited items are handed from outside the screening area to those who have already successfully cleared the scanning process.

In schools, the Passive Portal and personnel will generally be located directly within the front or main student entrance. Unfortunately, the design of most schools does not lend itself to a comfortable staging area for this process. There is usually not nearly enough interior or covered space to allow for all the students waiting to enter the system. This may mandate that the Passive Portal staging area be located further within the facility, which may place administrative offices outside the cleared area. Conscious decisions must be made, and potential risks must be realized when designing your weapon detection program.

Keep in mind that any population that is aware that it must regularly go through the scanning process will soon compensate and adjust their routine. These adjustments will generally be that: (1) the population will attempt to take fewer prohibited items with them into the facility, (2) scannees will learn which otherwise acceptable items in their possession will still cause an alarm and will tend to shy away from these items, and (3) the population will allow for the additional few minutes in their schedule, perhaps even going so far as to come early enough to miss the main rush.

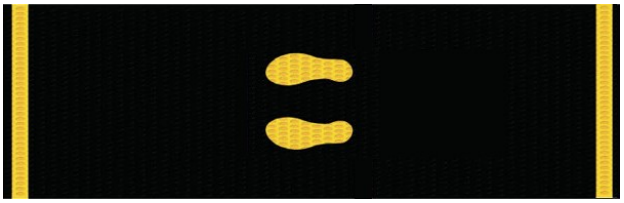
The Scanning Procedure:

Your school will need to develop specific procedures and policies as to the logistics of its metal detection program. This will include how to process or direct a student who has caused an alarm. The rest of this section will familiarize your school with what to expect and to provide some general recommendations. Once the Passive Portal has been set up and has been demonstrated to operate accurately in its current position and with its current settings, the operator will not be required to adjust the control settings.

Some points for the operator to be aware of are:

a. Do not allow the scannee to proceed through the portal too fast. There are prompting LED lights to control the throughput rate. This will ensure that the scannee has not gone through the portal so fast that he or she could have been inadequately scanned.
b. Make certain that no other person is located within a 3-foot radius of the equipment while a scan is being performed. This includes the operator unless he or she is devoid of any metal on his or her person.
c. Provide a rescan of any person who causes an alarm, even if he or she can identify what must have caused the alarm, such as a belt buckle or necklace. Confirm that this person no longer causes an alarm after the offending item is removed from his or her possession.
d. Do not allow anyone on the outside of the cleared area the opportunity to hand something to a person who has already been cleared by the portal on the inside of the cleared area.
e. The instructions provided to students, employees, and visitors need to be as short and simple as possible. The following example instruction set could be provided to students and employees in the student handbook and should be posted at the entry to the weapon detection area.
    a. Remove any metal items from your body or pockets and put them in the provided tray.
    b. Stay back from the Passive Portal until signaled by the operator to proceed.

c. Walk at a moderate pace through the Passive Portal, one person at a time, being sure to momentarily place your feet on the footprints at the base of the Passive Portal before proceeding.



d. If an audible alarm sounds as you go through the Passive Portal, follow the directions of the security officer for further scanning or search.
e. If the Passive Portal activates, the scannee will be asked a second time to remove metal objects from his/her person and to walk-through the Passive Portal a second time.
f. If the Passive Portal activates a second time, personnel conducting the search is to approach the student and/or person and explain the investigating process and investigate fully what caused the alarm. When a student's or designated other's bag or parcel activates the Passive Portal, the personnel conducting the search is to request him/her to open the container in question so that the officer can look for weapons. The administration shall monitor each search for compliance with school guidelines.

About False Positives and Alarms:

False alarms, or false positives can be extremely annoying to scannees and can increase the manpower required to support a metal detection program. Constant false-positive alarms can also cause the operators of a system to become desensitized to alarms, so that they eventually fail to fully investigate the sources of all alarms. A system set more toward false negatives can slightly increase the risk of a weapon entering the facility but generally helps a metal detection program to run as smoothly and quickly as possible. In such a program, when an alarm does occur, the operators will be more likely to take it seriously and to investigate fully what caused the alarm. Many school system programs will be set in this manner. The Passive Portal is additive; it will generate an alarm based on the total response received from the metal detected on a scannee. An alarm does not necessarily mean just one suspicious item has been detected. Because of this, a scannee who has multiple “borderline” items on his other body has a better chance of causing a false alarm.