Access Portal Readme

Information contained in this document pertains to **major and minor release.**

We recommend backing up an existing database before upgrading

Table of Contents

Installing Portal

Run the Portal installer (Portal.exe) from the DVD or download location. If for some reason you wish to manually install and configure SQL Server 2014, a guideline is provided.

Minimum Requirements

- Microsoft Windows 7
- Microsoft SQL Server 2014 - Express provided on DVD
- The latest versions of Google Chrome () , Mozilla Firefox, Microsoft Internet Explorer
- Some features are not available on all browsers. For example Graphs for reports and Image Capture from a webcam are not supported by Portal on Internet Explorer.

Installation of Client Plugins

Client plugins are used to provide additional functionality to the web browsers. Web browsers cannot connect to hardware connected to a PC normally as this is considered a security risk. By installing the provided client plugins, additional functionality is provided to the browser to allow access to some hardware. For example, accessing a biometric enrollment reader.

Please Update your Plugins if your plugins are from before Portal v1.60 or v1.82 and above.
Plugins are not supported for Chrome 42 and later, because of npapi (plugin support) effective removal. For more information, read: http://www.chromium.org/developers/npapi-deprecation Because of this we have needed to rework how the browser interacts with Tag Readers and other hardware. If you have installed any of the above plugins prior to version 1.60, please uninstall the version you are currently using and install the latest version.

Please upgrade your plugins from the client folder within the installed location.
Plugins have now been merged into a single installer and image capture has been added. The installer now has all plugins with the option to pick which ones you want to install. The new name is ClientInstall.Portal.Plugins.exe.

Client Plugin	Required for

Sagem Enrolment option:
 	
• Select Sagem Enrolment option and follow the prompts
• From *{installed location}\client\morpho\driver\morpho.* run the following **in this order:**
  ○ Open the folder MorphoSmart and run setup.exe. For a 32-bit system, open the folder x86_32 and run setup.exe. For a 64-bit system, open the folder x86_64 and run setup.exe.
  ○ Open the folder SafeNetDongle and run Sentinel System Driver Installer exe.
	Enrolling fingerprints from browser for use on Morpho biometric terminals.

○ Open the folder LicenceProtection and run the SafranMorpho_Licence_Protection_Installer.exe.	
Nitgen Enrolment option ● Select Nitgen Enrolment option and follow the prompts.	Enrolling fingerprints from browser for use on Nitgen biometric terminals or BMTA's.
Suprema Enrolment option ● Select Suprema Enrolment option and follow the prompts.	Enrolling fingerprints from browser for use on Suprema biometric terminals.
Tagreader Enrolment option ● Select Tagreader Enrolment option and follow the prompts.	Enrolling tags from MDE
ClientInstall.Portal.Linphone.exe ● Run ClientInstall.Portal.Linphone.exe and follow the prompts. ● Unfortunately only supported on IE. ○ Chrome is not supported post version 41. ○ Firefox not supported post version 51	Allow VOIP calls to the browser. Specifically added for Morpho Sigma Series, video phone functionality. Some tests have been done on other VOIP clients.
Card Printing option ● Select Card Printing and follow the prompts	Card Printing from printer
Omnikey Enrolment option ● Select Omnikey and follow the prompts	Enrolling tags and writing data to tags.

Upgrading Portal

1. Ensure Portal is not running.
2. Backup the Portal database.
3. Uninstall the existing version of Portal from Windows Control Panel, Programs and Features. All Portal files should be removed at this point, excluding the database and files that were created after the initial install.
4. Using the new Portal installer, follow the prompts to complete installation.
5. The database will be automatically upgraded the next time Portal is started.
6. Run FirmwareUpgrade.exe to upgrade hardware to the latest firmware versions.

Access Portal Revision

This section provides information on all the different releases of portal. This includes information on new features, new hardware support, bugs fixed since the previous version and known issues with the release.

Version 4.4.0

Release Date : 2020-12

New Features & Enhancements

- **LCD Message actions:**
  - Supported by MDTA and BMTA. A firmware upgrade is required for both controller and readers.
  - Assign an icon to an LCD Message action, to enable a custom icon to be shown on the MDTA/BMTA LCD screen, along with the message it is associated with.
  -
  - Manage the icons available, from the Setup > *Icons* menu.
- **Configuration files:** for Suprema and HIK Vision to change specific integration functions (thermal, Wiegand and some device specific settings).
- **Taskbar:** right-clicking on the *Access Portal* icon in the taskbar now shows an additional menu called *Biometric Settings.* This new menu allows users to change the passwords for each of the major brands of biometric integrations.
- **Biometrics view:**
  - When installing a new device, you now have the option to use either the IP address or hostname of the server for communication with the device. This allows sites where the server's hostname fails to resolve to instead make use of the servers IP address.
  - Thereafter, all new installs will automatically make use of the selected means of communication.
  - To change this setting at a later stage, click on the *Settings* button of the install wizard.
- **User Check / Capacity**
  - Right-clicking on an installed device under the Hardware > Biometric Configuration tab in the server app will now show a summary of supported capacity for that device. For example: max databases; max templates / face templates / cards per database.
  - A User Check button has also been introduced, which compares expected user count vs actual on the device. Support included for Morpho, Suprema, HIK Vision (HIK Vision only supports User Check and not capacity)
- **Reports**
  - *Access Per Location Per Day:* total allowed accesses per day, per location. Includes averages.
  - *Enrolment Per Site Per Day:* total enrolments performed per day for each site.

New Hardware

- **HIK Vision DS-K1T671TM-3XF** – must be licensed before it will function within Portal.
- **HIK Vision DS-K1TA70MI-T** – must be licensed before it will function within Portal.
- **HIK Vision DS-K1T341AMF** – must be licensed before it will function within Portal.
- **Suprema –** face reader thermal module integration

- **OSDP Module –** has the same capabilities of the Wiegand Module, with added support for OSDP.

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

See Appendix C for a list of known issues

Version 4.2.5 (Service Pack 1)

Release Date : 2020-10

4.2.0 Service Pack Release with bug fixes only (essentially 4.2.0 but version change to 4.2.5).

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

See Appendix C for a list of known issues

Version 4.2.0

Release Date : 2020-07
Beta Release Date: 2020-02

New Features & Enhancements

- **Expiry Reason Warnings**
    - This is an addition to the Expiry Reasons feature which allows you to specify the number of days, prior to a reason expiring, to start warning of an impending expiration. Requires latest APC / AC controller firmware.
    - From the Modules main menu, select Expiry Reasons and create the reasons along with their validity periods. Enter a value from 1 to 255, representing the number of days prior to expiring that you wish to start warning a user.
    - Readers will have support for new events “Warning Date Expiry Reason 1” to “Warning Date Expiry Reason 30” which will be generated to warn users. One of these events will be assigned per Expiry Reason. From the Expiry Reasons list view you will be able to see which event corresponds to which expiry reason.
- **Translations**
    - Support for installing Portal with the following languages:
      Arabic, Bulgarian, Chinese Simplified, Dutch, English (UK), English (US), French, Greek, Portuguese, Spanish.
    - Note: to change the system language for an existing system, please contact support.

New Hardware

- **Suprema FaceStation 2 FS2-D** – must be licensed before it will function within Portal.

- **Suprema FaceLite FL-DB** – must be licensed before it will function within Portal.
- **Sagem Vision Pass** – must be licensed before it will function within Portal.

Bug Fixes

[See Appendix C for a list of bugs fixed]

Known Issues

[See Appendix C for a list of known issues]

Version 4.1.0 (Beta)

Release Date : 2019-12

New Features & Enhancements

- **Expiry Reasons**
  - This feature allows a user's access to different areas on site to be expired for any of several reasons.
  - Licenses required for this feature to work include both an *Enterprise* license and an *Expiry Reason* feature license.
  - Firmware versions required for controllers are APC firmware v2.19 or AC firmware v10.48.
  - From the Modules main menu, select Expiry Reasons and create the reasons along with their validity periods.
  - From the Tagholder view, under the Expiry Reasons tab you can choose to apply one or more expiry reasons and choose the access groups that will be affected by those reasons.
- **Contextual Help** has been added/updated for the following views:
  - Expiry reasons
- **Aperio**
  - Emergency mode can now be triggered by an input.
    - From the Reader view, select a device that supports inputs.
    - Go to the Actions tab and click on Event Actions
    - Search for and select an input related event. E.g. Input Alarm 1.
    - Search for and select the the *Emergency Mode On* or *Emergency Mode Off* action

belonging to the Aperio device.
    - Emergency mode via Dashboard Command widget
        - From the dashboard, add a Command widget
        - Select either an Aperio hub as the controller; or an Aperio lock as the reader
        - Save the widget.
- **Search**
    - Support has been added for searching using hyphenated door names.

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

See Appendix C for a list of known issues

Version 4.0.0

Release Date : 2019-11

New Features & Enhancements

- **General**
    - **Delete Person / Asset** when hovering over a person or asset in the list, a delete icon will now show allowing the person/asset to be deleted along with their transactions.
    - **Scheduled Transaction Deletion** a *Privacy Settings* section under the *Tools* tab in the server app has been introduced to allow transactions to be deleted based on a time schedule.
    - **Delete Access Transactions** access transactions that occurred on or before a selected date, can now be deleted from the *Maintenance Tasks* section under the *Tools* tab in the server app.
    - **Contextual Help** was introduced for some of the most commonly used views.
    - **Site Registration** register your site with us
    - **Batch Operations** at the end of a batch operation, a link will be made available to download the logs for the operation just completed to the client machine. The link will expire in an hour.
    - **Favorites** save your most common enrollment process as a favorite so you can speed up the enrol process. E.g. If you typically enroll cards from an MDE, save that as your favorite.
    - **Eject from zone** The *zone occupancy* report now includes an *Eject From Zone* column which allows you to manually eject a person from the zone. The tag must be valid (e.g. time of day; not

suspended; etc.) in order to be ejected. No actions will be performed when ejecting the person. Controller firmware will need to be upgraded to support this feature.
    - **Find Image** a new dashboard widget is available, where you type in the Id Number of a person and it will show you the person images.
    - **Reports** company and department columns have been added to a number of reports; *zone occupancy* report now supports the *date/time* filter.
    - **Tags Not Used** this report will now show the tags that are not used, instead of just the person the tag belongs to.
    - **Password Reset** to reset a forgotten *Sysdba* account password, you can now go to the *Account* section of the *Security* tab in the server app and enter the new password.
- **Stability and Performance**
    - The lucene indexes will now be created within the Portal directory.
    - Improvements to speed / memory when enrolling people and tags.
    - Improvements to PluginManager resulting in a speed increase of 50% for reading/writing to Seos and Mifare cards.

New Hardware

- **Impro Biometric Reader** – is limited to 1K users and finger only mode, when not licensed. Can be licensed to support card presentation as well as to increase the number of users supported to 5K.
- **iCLASS SE RB25F Mullion Fingerprint Reader** – must be licensed before it will function correctly.
- **Sagem MASIGMA Wave** (*a.k.a. MorphoWave*) – must be licensed before it will function correctly

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

See Appendix C for a list of known issues

Version 3.5.0 (Beta)

Release Date : 2019-08

New Features & Enhancements

- **General**
    - **Tag Types:** support for disabling/enabling additional tag types from the Controller profile > Parameters tab > Enable Tag Types setting. The newly supported types include: Mifare, Felica,

iClass and 15693.

New Hardware

- MorphoWave

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

See Appendix C for a list of known issues

Version 3.0.6

Release Date : 2019-05-13

New Features & Enhancements

- **Stability and Performance**
  - Clear the comms queue for biometrics when performing a sync.
  - Auto Correct feature now defaults to running during quiet hours of the day only.
  - Improved handling of systems with large number of controllers / biometric devices
- **General**
  - Services view now shows the total comms queue.
  - Custom Report Management view can now be given access to from the Operator Profile view.
  - Improved logging for offline devices.

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

See Appendix C for a list of known issues

Version 3.0.4

Release Date : 2019-02-07

New Features & Enhancements

- **Stability and Performance**
  - Improved recovery from Database connection failure
  - Improved the responsiveness of the UI
  - Better handling of systems with large number of controllers / biometric devices.
  - The database port application has been reworked to handle large databases
  - Time consuming reports are not automatically triggered when navigating through report menus.
- **General**
  - Allow admin users to reset user passwords
  - Improved support for starting Portal as a service.
  - Sagem MA devices allow a template check to be performed.
  - The system now saves/remembers your site selections and uses them the next time you login.
  - Server application now has the ability to delete biometric devices that were installed but never licensed

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

See Appendix C for a list of known issues

Version 3.0.2

Release Date : 2018-04-30

New Features & Enhancements

- **Access groups per person, per site changes**

Software License	APC Controller	AC Controller
Basic	8 (Unchanged)	8 (Unchanged)
Pro	25	25

Enterprise	25	100

NOTE: Currently when off-line, door controllers are limited to 10 access groups which are chosen at random. If a person / asset has more than 10 access groups assigned, when a door controller goes offline the person might be denied access.

- **Some tables in the client UI have been given the option to show only selected records.**
  - A filter button will show next to the search box with an option to filter by Show Assignments Only

- **Added a Tools tab to the server application.**
  - New home for the existing Import Person / Asset task.
  - Some Maintenance tasks.

Beta Features

- **Move Controller** Under the tools tab in the server application, a feature has been added to move controllers between sites. This feature is still under development and may change without prior warning.

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

See Appendix C for a list of known issues

Version 3.0.0

Release Date : 2018-03-20

New Features & Enhancements

- **Installer** The installer has been overhauled. Some notable improvements are that we allow specifying the instance of Microsoft SQL Server to connect to and we deploy Microsoft SQL Server Express 2014 instead of 2012.

- **New Look & Feel** The user interface has had an overhaul.

- **Mobile Access** allows credentials to be stored on a tagholders mobile phone, running the mobile access app. This requires special readers, not all readers support mobile access.

- **Mobile Portal**
    - Support for HID tags when using correct head end.
    - Push transactions over WiFI.
    - Sync over WiFi or USB Dock.
    - Pull images over WiFi to reduce the size of sync.
    - Dropped support for Workabout Pro 3 in the latest version of Mobile Portal Software.

- **Tagholder Import from Excel Spreadsheet**
    - Standard Tagholder Fields.
    - Custom Tagholder Fields. (Text Only).
    - Tagholder Image.

- **Data Filters** These filters are used to control the information a user has access to. It is a form of Operator Security and is found in the *Operator Profile* view. Some of the new *Data Filters* are limited in scope to only affect the live transactions view found under *Dashboard*.

    - Limited scope
        i. Site
        ii. Person/Asset type
        iii. Door
    - Affects all applicable views
        i. Company (now also filters Person/Asset types)
        ii. Department (now also filters Person/Asset types)

- **Filter Profiles** these profiles have been dropped and their settings have been moved to the *Operator Profile* view.

- **Event Actions** the reader view now has the ability to assign actions to *all allowed events* and *all denied events* for a selected reader.

- **Transactions** the columns and filters chosen from the *Transactions* view under *Dashboard* are now saved as user preferences against the users account. This means that the system will remember your choices the next time you login.

- **Random Search** when enabled the system will randomly select a *Tagholder* for searching. The *Tagholder* that was selected for searching will be temporarily blocked from gaining access. The frequency of searches can be set as well as a time pattern specifying when random searches will be performed.

- **Features that have moved**
    - **Replace Reader / Controller** this feature has moved to the *Reader* and *Controller* views, respectively.
    - **Select Sites to view** this feature has been moved under the User Filters menu which shows when

you click on the operator name, top, far-right corner of the screen
    - **Live Columns / Filters** these settings found under the *Filter Profile* have been moved under the *Columns* tab and *Filters* tab respectively in the *Operator Profile*.
    - **Live! View** this view has been moved under *Dashboard* and renamed to *Transactions*
    - **Notification Account Settings** this view has been renamed to *Account Settings* and can be found under the *Setup* menu

- **Input/Output devices** from v3.0 onwards, an I/O device is no longer assigned to a door.

- **Lift / Elevator Module** some improvements have been introduced:
    - **Contact State:** choose between *Normally Closed* and *Normally Open* for the I/O relays
    - **Host Timeout:** the *Host Timeout* event is now triggered every 10 seconds.
    - **Lost Communications:** When communication between the hardware and the host machine is lost, the relay states of those I/O devices will revert to normal operation without destination control until the connection is restored.

Known Issues

[See Appendix C for a list of known issues]

Version 2.2.0

Release Date : 2017-09-08

New Features & Enhancements

- **Basic License** The free basic license limits have been relaxed

    - System limit changes are.

Basic License	Old Limit	New Limit
Access Groups (Per Site)	8	100
Doors (Per Site)	8	100
Doors (Per Controller)	8	64
Controllers (Per Site)	1	100
Zones (Per Site)	8	100
Zones (Per Controller)	8	64

Common Zones (Per Site)	NA	64	
Readers (Per Controller)	16	64	

- Reports that have been added to this license.
  i. Access Group Report
  ii. Holiday Report
  iii. Zone Occupancy Report
  iv. Door Access Report
  v. Tag Expiry Report
  vi. Tags Not Used Report

- **Virtual Hardware** The ability to add virtual hardware to a site has been added. This allows a system to be configured by an installer before going to site. On site, replace the virtual hardware with actual hardware.

- **Lift Control** When implementing lift control on a site, an installer would typically use access group actions. With the implementation of this simplistic, purpose designed lift control module, we are attempting to make lift control easier to configure for the installer.
  - This implementation requires the software to be running and the hardware to be online.
  - Only relays on an I/O device can be used for this implementation of lift control.

- **Batch Operations (Access)** Allows the user to quickly perform the following batch operations.
  - **People / Assets (enroll new)** a.k.a batch enrollment.
    i. Template values such as firstname, lastname, department.
    ii. Access Groups
    iii. Floors (Related to the new Lift Control feature).
    iv. Tag Enrollment. (Random PAC, Tag Range, Read Tags, Manually Enter)
    v. Summary
  - **People / Assets (update)**
    i. Select Person / Assets to update (Manual selection or selection VIA CSV import)
    ii. Add Tags
    iii. Update Access Groups (Assign, unassign, replace, update dates)
    iv. Edit Fields
    v. Assign Groups and Floors.
  - **Access Groups (update)**
    i. Select access groups to update.
    ii. Add doors to access groups.
    iii. Remove doors from access groups.
    iv. Replace actions on access groups with new ones.

- **Directory Configuration Updates** Improvements have been made to the directory implementation.

- Added support for user operator profile lookup.
- Switched authentication from comparison to binding. Allows supporting a larger range of LDAP directories.

- **Server Application Updates**
  - **Web Server Configuration (HTTPS, Port Configuration, etc.)** Web server configuration has been moved into the server application UI. We've also added the ability to generate certificates for use by the application web server and a few other options around this feature.
  - **Diagnostics** The server application diagnostics tab has been updated to include graphs and metrics that show the load on the server application.

- **Reports**
  - **Tags Not Used Report** Show current Person/Assets who have not used their tags since a configurable date.
  - **Tag Expiry Report** Show tags that expire in a given date range for current Person/Assets.
  - **Person/Asset Access Report** Show all current Person/Asset records with their assigned access groups, areas and time patterns.
  - **Person/Asset Access History Report** Show current Person/Assets and their tag/access group assignment history.
  - **Network Status Trend Report** Show networked hardware and when they go online or offline.
  - **Hardware Installation Report** Show installed hardware.
  - **Hardware Comms Channels Report** Show controllers, readers and associated channel info grouped by area.
  - **Areas Report** Show areas and the doors that belong to them. Includes door, entry, exit, zone building and floor.
  - **Holiday Report** Added a holiday report that shows configuration information.

- **Custom Reports** If you have a need for a report that is not available as a standard report, please contact support to discuss if a custom report could solve your requirement.

- **Integration**
  - **SQL Staging Table** A table has been added to the database that allows integrators to create or update person / asset records using SQL instead of needing to use the API.

- **Similar Matches**
  - **Areas** Added similar matches for areas. This helps reduce the number of duplicate areas configured for large systems by showing how similar other areas are to the area that the user is currently editing.

- **Dashboard** - Support was added for a restricted public dashboard. The dashboard can be accessed by using the same URL in your browser as normal, by replacing *"Dashboard.html"* with

"PublicDashboard.html"

- **Time Patterns** Access time patterns and device time patterns have been updated to capture an end time instead of a duration.

- **Firmware Upgrade Utility** A new version of the firmware upgrade utility has been released. It encompasses finding controllers on the network and supports upgrading all devices connected to the controller with a single click as well as showing a tree of the controller and the hardware connected to it. The old firmware upgrade utility will be shipped with the new utility for this release but will be removed for the next release.

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

- **Reports** The filter for "Has Templates" has a "yes" and a "no" option. The "no" option returns anyone who has a tag without templates. So if a user has two tags, one with templates and one without, when using the "no" option the tagholder will still be returned.

- **Visitors** Visitors created using Access Portal are not available from Visitor Portal.

- **Anti-virus programs** may cause issues while installing or uninstalling plugins for tag reading or biometric enrollment.

- **Browser cache** The browser cache needs to be cleared after upgrading the software for the latest changes to take effect.

- **Access Portal (x64)** does not support Suprema BioStar v1.xx biometric terminals.

- **Site** There is currently no support for deleting a site that already has people and/or assets saved to it.

- **Maximum Access Group Capacity** This feature is not supported across controllers.

Version 2.0.0

Release Date : 2017-01-19

New Features & Enhancements

- **Dashboard** The addition of a dashboard view. This view is customisable per operator and allows the operator to add widgets to their dashboard that are useful to them. The following widgets are available:
    - **Access Group Capacity Graph** - works with the new max access group capacity feature.
    - **Commands Widget** (Emergency mode, Lockdown, Reset APB, Unlock Door)
    - **Enrollment Graph** - shows information on the number of enrollments for the current week.
    - **IP Camera Widget** - Allows IP camera widgets to be displayed on the dashboard.
    - **Live! Transactions** - A widget that shows live transactions.
    - **Monitor Comms Queue** - A widget the monitors the comms queue and allows stopping and starting of hardware configuration sync.
    - **Monitor Door** - A widget that monitors a door. It shows the latest transaction for the door being monitored. Allows the door to be unlocked remotely and allows the threat level of the door to be changed.
    - **Monitor Tour** - A widget that works with the scheduled tour feature. A tour for a person can be monitored and managed from this widget.
    - **Quick Enroll** - A widget that allows the operator to quickly enroll a new person / asset into the system.
    - **Shortcuts** - Shortcut widgets can be configured to allow fast access to areas of the software the the operator frequently uses.
    - **Visitor Graph** The visitor graph is a graph version of the visitor report.

- **Biometrics**
    - Support for Seos writing templates to card (For Sigma IClass Readers only).
    - Ability to disable uploading to specific biometric devices (For template on card use case)
    - Ability to disable uploading a specific tags, biometric templates to devices. (For when you want to upload some staff to a biometric device but want to use finger on card for other)

- **Maximum Access Group Capacity** - Allow a maximum capacity to be set for an access group. For example, if two companies share a parking area and each company is only allowed 3 parking spaces, this is the feature to use.

- **Doors (Dual tagging)** - A door can be configured to require up to 5 tags from 5 different users before it will unlock.

- **Communications (System Controllers over WAN)** - Added support to allow system controllers to be installed over a WAN. This requires correct router configuration.

- **Move View** - Added view for moving people / assets from one site to another.

- **Filters & Columns**
    - Available to both the Live Transaction view and from reports

        - Input name filter shows the name of the Input associated with a transaction
    - Available only from reports
        - Person / Asset type which allows filtering by Access Only or Access And Time.
        - User Data filter which allows you to filter by the data users have typed into a User Field

- **Supported Device Actions**
    - Reset APB *(Currently only supported with APC System Controllers)*
    - Reset Access Group Count *(Currently only supported with APC System Controllers)*

- **API**
    - Show when controllers comms status changes
    - Support for injected transactions.
    - Support for "with" when requesting data.
    - Support for lucene search.

Beta Features

- **Custom Reports** The ability to import reports specifically written for an individual customer. This feature is still under development and may change without prior warning.

New Hardware

- **IO8 Input/Output Module** This module comes with 8 digital inputs and 8 relays.
- **I8O4 Input/Output Module** This module comes with 8 digital inputs and 4 relays.
- **S4 Module** This module is required for connecting s-bus readers. The module supports up to 4 APB doors by allowing 8 s-bus readers to be connected.
- **S4 Readers** S-bus readers that connect to the S4 module.

OEM Devices

- **Omnikey** Support for the omnikey enrollment reader.
- **Aperio Wireless Locks** Aperio is a technology that enables mechanical locks to be linked to an access
- **Nitgen T1, Biometric Terminal** Allows up to 5, 000 users. (Minus the admin user).
- **Suprema BioEntry W2, Biometric Terminal** Allows up to 100,000 users. (Minus the admin user).
- **Suprema BioStation 2, Biometric Terminal** Allows up to 20, 000 users. (Minus the admin user).
- **Suprema BioStation A2, Biometric Terminal** Allows up to 100,000 users. (Minus the admin user).
- **Suprema BioStation L2, Biometric Terminal** Allows up to 100,000 users. (Minus the admin user).

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

- **Reports** The filter for “Has Templates” has a “yes” and a “no” option. The “no” option returns anyone who has a tag without templates. So if a user has two tags, one with templates and one without, when using the “no” option the tagholder will still be returned.
- **Visitors** Visitors created using Access Portal are not available from Visitor Portal.
- **Anti-virus programs** may cause issues while installing or uninstalling plugins for tag reading or biometric enrollment.
- **Browser cache** The browser cache needs to be cleared after upgrading the software for the latest changes to take effect.
- **Access Portal (x64)** does not support Suprema BioStar v1.xx biometric terminals.
- **Site** There is currently no support for deleting a site that already has people and/or assets saved to it.

Version 1.8.4

Release Date : 2016-08-05

New Features & Enhancements

- **Card Printing**
  - Card Designer now included in the bin folder.
  - Print onto existing tag.
  - Use Fargo Printer to issue new tags.
  - Plugin Manager updated to support printing. Requires upgrade.

- **Visitor Book**
  - Support for customising the layout of visitor book and other UI improvements.
  - Support for Honeywell ™ device for reading South African drivers license, South African vehicle license and new South African card IDs.

- **Person / Asset Access Groups**
  - Ability to set a start date and expiry date for linking an access group to an individual person or asset.

- **User Fields**
  - New Multi-Select user field added.

- **Reports**
    - Fields renamed from the Person / Asset profile now show their alternative names as tool tips from reports as well as an appendix to exported PDF reports.
    - Time Based Report
        - For fully nested zones, transactions were only included from the outermost zone to avoid double clocking. This would cause a time of 00:00:00 to be reported when filtering for a nested zone. Improvements have been made to allow filtering by nested zones.

- **Install**
    - Support for scanning on a specified range of ip addresses has been added to allow searching for and installing devices on different ranges.

- **Unit Discovery**
    - Ability to update the IP address used by portal to communicate with a discovery enabled device when changing the address to a static IP.
    - Ability to force an IP address to change added to the web version of Network Configuration. Previously a device would roll-back its IP if portal could not communicate with it after changing the address.

- **Operator Security**
    - Ability to specify fields to be made Read Only per Operator profile.
    - Ability to select which Departments can be seen, edited and assigned by an operator.
    - Directory Authentication using LDAP (Lightweight Directory Access Protocol).

- **Support Diagnostic Bundle**
    - SYSDBA has the ability to export a diagnostic bundle for support purposes. The diagnostic bundle does not contain any sensitive information. It gathers system information that can assist a technical support consultant to diagnose and solve support issues.

- **Portal Server**
    - Ability to uninstall a biometric device by right-clicking on it and selecting the correct option.
    - Updated functionality to discovery tab. *(See Unit Discovery above)*.

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

- **Reports** The filter for “Has Templates” has a “yes” and a “no” option. The “no” option returns anyone who

has a tag without templates. So if a user has two tags, one with templates and one without, when using the “no” option the tagholder will still be returned.

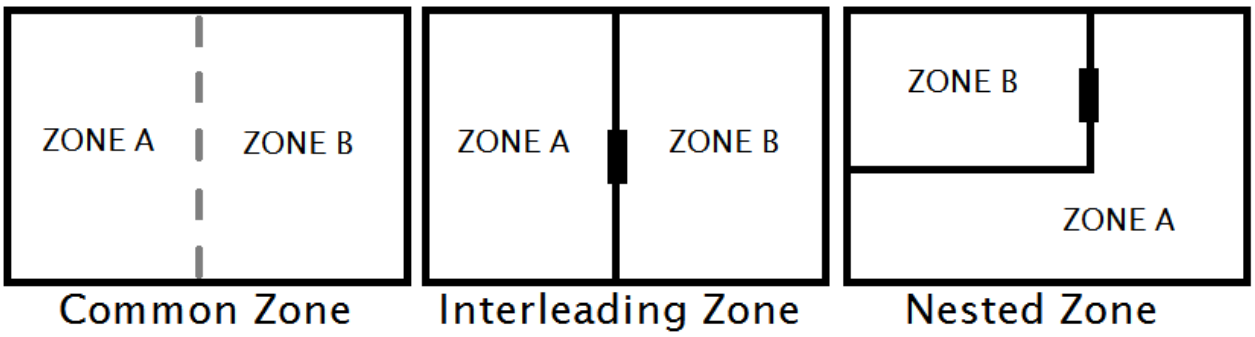
- **Visitors** Visitors created using Access Portal are not available from Visitor Portal.
- **Anti-virus programs** may cause issues while installing or uninstalling plugins for tag reading or biometric enrollment.
- **Browser cache** The browser cache needs to be cleared after upgrading the software for the latest changes to take effect.
- **Access Portal (x64)** does not support Nitgen OEM biometric terminals or Suprema OEM biometric terminals.
- **Site** There is currently no support for deleting a site that already has people and/or assets saved to it.

Version 1.8.2

Release Date : 2016-03-11

New Features & Enhancements

- **Advanced Zone Configuration**
    - **Common Zones** A common zone is used when zones belonging to different controllers must have Anti-passback (APB) applied as these zones form a single physical work area. Strict APB is required for this feature.
    - **Interleading Zones** A door can be configured as leading from one APB zone to another APB zone. This feature is used to force people to follow a logical path of tagging In and Out.
    - **Nested Zones** This feature is used when a zone is physically contained within another zone on the same controller. A person cannot tag at a door in Zone B without having clocked into Zone A. A person cannot clock out of Zone A without having clocked out of Zone B.



Advanced Zone Configuration

- **Door Access Report** Shows people / assets with access to a specific door.
- **Audit Report** The audit report shows changes made to the database when an operator performed some task. For example, when a user creates a new Tagholder, this will appear in the Audit Report. The audit report also show record modifications, deletions and some other auditable tasks that don't change database records.
- **Access Group Report** The Access Group Report shows access groups, their area name and access time pattern.
- **Default Access Group Assignment** The Operator Profile now has the ability to specify whether new people or assets should automatically receive the Default Access Group or not.
- **Change password** An operator no longer requires access to the Operator Logins view in order to change their own password.
- **Reason Codes** A door can be configured to require a reason code on tag presentation. Up to 99 reason codes with configurable names are available.
- **Manually creating a tag** Additional tag types are available when creating a tag manually. Previously we only allowed creating HID and Quad Tags manually. The tag type is used to apply different truncation rules.
- **Search by tag code** A read tag button is available from the Tagholder / Asset Views and from the Tag View. This allows searching for a Tagholder / Asset / Tag by clicking the read tag button.
- **Data Filters** The Operator Profile now has the ability to specify an Access Group filter which will be applied to all views in Access Portal thereby limiting which access groups an operator can assign or edit.

Bug Fixes

[See Appendix C for a list of bugs fixed]

Known Issues

- **Reports** The filter for “Has Templates” has a “yes” and a “no” option. The “no” option returns anyone who has a tag without templates. So if a user has two tags, one with templates and one without, when using the “no” option the tagholder will still be returned.
- **Visitors** Visitors created using Access Portal are not available from Visitor Portal.
- **Anti-virus programs** may cause issues while installing or uninstalling plugins for tag reading or biometric enrollment.
- **Browser cache** The browser cache needs to be cleared after upgrading the software for the latest changes to take effect.
- **Access Portal (x64)** does not support Nitgen OEM biometric terminals or Suprema OEM biometric terminals.
- **Site** There is currently no support for deleting a site that already has people and/or assets saved to it.

Version 1.8.0

Release Date : 2015-12-11

New Features & Enhancements

- **Linking Management** This view shows how an item is linked to other items in the system. For example: Tagholder John Doe has 2 vehicles and a laptop linked to him and he is linked to the Estate My Coastal Estate.

- **Bulk Update** This view allows settings to be updated across multiple selected items. For example: update the APB Override status for all tagholders linked to the Estate: My Coastal Estates. The view is accessed via Linking Management.

- **Visitor Management** Replace **Dashboard.html** in the url with either **Visitor.html** or **VisitorLogin.html** to load the Visitor Book in kiosk mode or secure mode. Secure mode requires an operator to login and thus has access to features such as Open Door, whereas Kiosk mode is available without logging in and therefore has limited features available.

- **Vehicle Profile** This profile has been included as standard. It is used with visitor management to capture vehicle information.

- **Visitor Report** A new report that shows visitors and who those visitors visited. Some data provided includes, Expected Arrival, Actual Arrival, Expected Departure, Actual Departure and Visit Status.

- **Asset Linking Report** This report has been upgraded to the reports v2 framework used by all new reports since v1.6

- **All Reports** Some minor improvements have been made to the styling of exported PDF files and the report displayed in the browser.

- **MorphoCheck** Support for translations, pac code and loading the person's image

- **Operator Profile** Ability to enable/disable Quick Enroll, Open Door, One Time Pin.

- **Portal Server** Ability to Full Upload to a single biometric device, replace a single biometric device and show additional information when right-clicking the record. Ability to enable/disable all biometric devices.

- **Live! view** Ability to navigate to the Door view from Live! by clicking on the link. Only available if the Operator Profile has access to the Door view.

- **64 Bit Support** A 64-bit version of the Java Runtime Environment (JRE) is being deployed for large enterprise sites. The 32-bit version of the Java Runtime Environment (JRE) is limited to 1GB of RAM which is sufficient for most small to large sites. *Launched using .\portal\bin64\portal.exe*

    - Nitgen OEM biometric terminals and Suprema OEM biometric terminals are not currently supported when running Access Portal under the 64-bit JRE.

New Hardware

- Support for Morpho Sigma Lite.

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

- **Reports** The filter for “Has Templates” has a “yes” and a “no” option. The “no” option returns anyone who has a tag without templates. So if a user has two tags, one with templates and one without, when using the “no” option the tagholder will still be returned.
- **Visitors** Visitors created using Access Portal are not available from Visitor Portal.
- **Anti-virus programs** may cause issues while installing or uninstalling plugins for tag reading or biometric enrollment.
- **Browser cache** The browser cache needs to be cleared after upgrading the software for the latest

changes to take effect.

- **Person/Asset Profile** When changing an Asset profile to a Person profile, people of this type of profile will still appear in the list of assets that can be assigned to a person until the Access Portal server has been restarted.
- **Access Portal (x64)** does not support Nitgen OEM biometric terminals or Suprema OEM biometric terminals.
- **Site** There is currently no support for deleting a site that already has people and/or assets saved to it.

Version 1.6.0

Release Date : 2015-07-31

New Features & Enhancements

- **Splash Screen** Portal now shows a Splash Screen when loading to indicate progress.

- **Reports** Removed the reliance on IIS for reports and improved on data security as described below:
    - Improvements to data security.
        - User profiles can be granted access to or denied access to data in any column for viewing or filtering (See changes to filter profiles).
        - Users from the same operator profile can see reports created by their members.
        - Only SYSDBA and the user that created the report can edit the report.
        - SYSDBA can see all reports and edit all reports.
        - Reports created by SYSDBA can only be seen and edited by SYSDBA,
        - Existing reports created prior to upgrading to v1.6.0 of Access Portal will be available using the SYSDBA login.

- **Filter Profile** The Filter profile now has the ability to control whether a column or filter is available for use in reports. This helps to prevent users who are allowed to view reports from seeing information they do not have authorisation to see.

- **Visitor Profile** A new default *Person / Asset* profile has been created for visitors. This profile will be used with "*Visitor Portal*". All visitors that are created by "*Visitor Portal*" will appear in *Portal* under Visitors. The profile contains additional user fields that cannot be edited or deleted.

- **Person profile vs Asset profile** The *Person/Asset* profile now has the ability to define whether it represents a *Person* or an *Asset*. The main difference between the two being that a *Person* can have one or more *Assets* assigned whereas an *Asset* can not.

- **Custom Fields** The *Custom Field* view now has the ability to assign a selected custom field to be used in reports as columns or filters, as well as the option to show the custom field in views represented by

Person/Asset profiles for the purpose of capturing data.

- **Database Connection Pooling** Allows multiple connections to the database. Faster processing of some tasks. Specially in the case where tasks are performed in parallel such as uploading configuration data to multiple devices.

- **Portal Installer** The installer for Access Portal has been updated to include a few new features. You now have the option to automatically install an instance of SQL Server Express 2012 for use with Access Portal. The installer will install SQL Server, configure it, create a SYSDBA user with administrator privileges and attach the Portal database to the new instance. Here are some rules with regards to the new installer:
    - If Portal is already installed, the installer will not attempt to install Portal again. To upgrade to the latest version you will need to uninstall the existing Portal installation and install the new version.
    - If SQL Server Express 2012 is already installed, the installer will not attempt to install it again.
    - The installer makes use of files found in the dependencies folder which is included on the DVD with the installer.
    - If you wish to manually install Portal or SQL Server Express 2012, you may still do so.

- **Minimum Resolution** The minimum resolution has been lowered to 1024x768 to allow support for laptops.

- **Time Triggered Actions** The Time Triggered Actions view is now available when running Access Portal without a license.

- **Disable Biometrics** Ability to disable biometric devices from the biometrics tab on the Portal Server application.

- **Scheduled Tours** A timeline has been added to the Active Tours view for each tour that is in progress. The timeline shows all points in the tour and the current progress and status of the tour.

- **Videophone Widget** Videophone support has been added to the browser to allow calls into the Access Portal web application. A person on site can make use of a Morpho Sigma Series reader to phone a receptionist or control room to request some action or provide some information. (Also tested with some other VOIP clients) The widget shows automatically when receiving a call. Outgoing calls are currently not supported. Requires the Linphone VOIP plugin. *(Do not install the plugin from the linphone website. Use the "Downloads" menu in Access Portal to download the installer)*

- **Images** have been updated to keep their aspect ratio. Previously a thumb image and an unaltered image would be captured with the maximum resolution of the thumb being 100x100. The thumb image is now derived by scaling down the saved image to a maximum resolution of 148x148 and the previously unaltered image is scaled down to a maximum resolution of 1024x768.

- **Auto Generate Id Number** the *Person/Asset* profile now has the option to automatically generate the unique identifier (e.g. Id Number) when a new person or asset of that type is created.

- **Swap Readers** The *Door* view now has the ability to swap its Entry and Exit readers around at the click of a button.

- **Scan IP Range** The *Portal Server* now has the ability to scan an IP Range when searching for Morpho Biometric devices to install.

- **Network Status** The *Network Status* view shows the current status of all network devices in the system except Nitgen terminals. This view is only available to the SYSDBA login.

Bug Fixes

See Appendix C for a list of bugs fixed

Known Issues

- **Reports** The filter for "Has Templates" has a "yes" and a "no" option. The "no" option returns anyone who has a tag without templates. So if a user has two tags, one with templates and one without, when using the "no" option the tagholder will still be returned.

- **Visitors** Visitors created using Access Portal are not available from Visitor Portal.

- **Anti-virus programs** may cause issues while installing or uninstalling plugins for tag reading or biometric enrollment.

- **Browser cache** The browser cache needs to be cleared after upgrading the software for the latest changes to take effect.

- **Person/Asset Profile** When changing an Asset profile to a Person profile, people of this type of profile will still appear in the list of assets that can be assigned to a person until the Access Portal server has been restarted.

- **Network Status** When changing the site filter while on the Network Status view, the view will need to be reloaded, by going to the main menu and back, before it will accept the changes..

Version 1.4.0

Release Date : 2015-02-11

New Features & Enhancements

- **Basic License** A free basic license was introduced which allows the use of a limited set of views and applies the system limits of the APLite system. Running Portal without a software license will put it into this mode.
    - 1 Site
    - 1 000 Tagholders
    - 3 000 Tags
    - 3 Tags per Tagholder
    - 8 Access Groups
    - 8 APB Doors
    - 1 Controller
    - 18 Holidays

- **Live! Transaction Viewer (Client)** Enhancements have been made to the Live! transaction viewer which includes the following.
    - Ability to unlock a door from the transaction viewer.
    - Clicking on a Transaction Summary widget will display a larger version of the Tagholder image if one is available.
    - Improved layout for mobile devices and devices that have a screen resolution lower than 1280 x 800.

- **Live! Transaction Viewer (Server)** A tab has been added to the Portal Server application that allows viewing transactions without needing to open a browser.

- **Client Connection Manager** A tab has been added to the Portal Server application that allows viewing currently connected client connections, along with the IP address that they are connecting from, the view that they are currently on and the username that they have used to connect.

- **Tagholder Images** The ability to capture up to 3 images per tagholder has been added.

- **Threat Level Management** Allows the configuration of 4 threat levels. Activating a threat level can force the readers into a specified mode and / or tell those readers to drive or disable their relays. Readers can be grouped by common behavior. Tagholders with notification e-mail addresses specified can be chosen to be notified of any threat level changes. Below are some noteworthy configuration options:
    - Door mode patterns are ignored while a reader is in a threat level.
    - If a reader is told to go into a mode that it does not support, it will fall back to it's default mode instead.
    - While a threat level is active it will still respond to changes to the mode and relay state behavior
    - The software does not need to remain online for the threat levels to keep working.
    - If a controller was offline while a threat level change occurred via the software, it will be updated as soon as it comes back online.

- **Diagnostics and System Resource Monitor** A tab has been added to the Portal Server application that allows monitoring of CPU usage and thread states.

- **Uninstall** Support has been added for uninstalling IP enabled readers.

- **New reports**
    - Zone Occupancy (APB Zone Occupancy)
    - Time Based Reports (combines Hours Worked, First In and Last Out reports). Only takes transactions from APB zones into account for accuracy.

New Hardware

- *Support for Suprema Series biometric Readers*
    - *BioLite Net*
    - *BioEntry W*
    - *BioEntry Plus*

- **Support for hand-held terminal with integrated biometrics**
    - MorphoCheck

Bug Fixes

[See Appendix C for a list of bugs fixed]

Known Issues

- **Scheduled Tour Tag** Adding a new tag with Scheduled Tour enabled will not show in the Tagholders view under Scheduled Tours menu until you either resave the tag or restart Portal.

Version 1.2.0

Release Date : 2014-07-01

New Features & Enhancements

- **Scheduled Tour.** Allows the creation of multiple scheduled tours that can be assigned to a tagholder. A tagholder assigned a tour, clocks at tour checkpoints within a configured time to prevent an alarm. Below are some noteworthy configuration options:
    - Access Groups determine which checkpoints are available during tour creation.

    - Access Groups with Access Time Patterns that have zero durations will prevent standard access, but still allow tour related events.
    - Inhibit Reader input does not inhibit reader access for this tag.
    - Scheduled Tour events will be raised during Locked and Lockdown modes.
    - Any type of tag can be used as a Scheduled Tour tag.
    - An expiry date on the tag is honoured.
    - Suspend and Suspend with Alarm tag status is honoured.
    - A pin code may be used with this tag.
    - Scheduled Tour In and Out events will be raised.

- **Morpho Biometric Templates.** Added support for two templates per tag. Previously only one template was captured per tag.

- **Health Checker.** New configuration summary. Automatic fault finder. Limit checking and consolidating biometric templates to a single tag.

- **Person / Asset Profiles.** This new type of profile allows fine-grained control of information captured during enrolment. For example, a *Contractor* profile based on the *Tagholder* profile may only require the *Basic* and *Contact* information to be captured. A *Vehicle* profile may only define a registration number and model field. Vehicles and contractors enrolled against these new profiles can be assigned to a standard *Tagholder*. The *Asset History* view reports on assignments by date and type of profile.

- **New User Fields**. Single select group, list lookup, and date user fields provide finer control of enrolment options.

- **Improved Searching**. Allows the user to search using wider search terms. For example, readers can now be located based on logical address, fixed address, IP address, name, etc. In addition, all search results are now grouped and ordered - making scanning through search results easier.

- **Image Capture.** Image capture now allows uploading an image from a file.

- **Offline support for BMTA, Antenna, and Wiegand Modules**. Offline operation now fully supported on these units.

- **End Of Line Sensing.** Added configuration of End of Line sensing on digital inputs.

- **Custom Logo.** Added the ability to display a custom logo on the landing page.

- **Custom menus and submenus.** Support for adding custom menus and submenus to the menu view. This allows integration of third party web applications by simply providing a URL.

- **Menu Changes.** Access Time Pattern and Area views are now both available as menu items. These menu

items were previously only available through the Access Rights view.

- **License and Revision Information.** The About view has been updated to include the software license and software revision.

- **Automatic Database Upgrade.** The server application will automatically apply database upgrade scripts on startup.

- **Access Override.** This new status type gives the tag special privileges as described below:
    - Access Groups are ignored except to determine which site to allow access to.
    - Inhibit Reader input does not inhibit reader access for this tag.
    - Locked and Lockdown modes do not prevent access for this tag.
    - Any type of tag can be used as an Access Override tag.
    - An expiry date on the tag is honoured.
    - Suspend and Suspend with Alarm tag status is honoured.
    - A pin code may be used with this tag.
    - Access Override In and Out events will be raised.

New Hardware

- **Support for Morpho Sigma Series**. Introducing support for the Morpho Sigma Series. Highlighted features include VOIP configuration that provides point to point VOIP calls.

- **Support for Digital IO Module.** Introducing support for the new 4 channel Digital IO module. This cluster module provides four relays and eight digital inputs which can be used to expand IO control.

Bug Fixes

[See Appendix C for a list of bugs fixed]

Version 1.0.0

Release Date : 2013-11-25

Initial Release

This is the initial major release of Access Portal to the public. We will use this as our baseline to compare future major releases and service packs to.

Appendix A

Licensing and Controller Limits

This section will always be updated to match the current release.

Software Main Views Available to different licenses

Area	BASIC	PRO	Enterprise
About	✓	✓	✓
Access Group Report	✓	✓	✓
Access Groups	✓	✓	✓
Access Time Patterns	✓	✓	✓
Areas	✓	✓	✓
Batch Operations	✓	✓	✓
Common Zone	✓	✓	✓
Controller Profiles	✓	✓	✓
Controllers	✓	✓	✓
Dashboard	✓	✓	✓
Device Time Patterns	✓	✓	✓
Door Access Report	✓	✓	✓
Doors	✓	✓	✓
Holiday Report	✓	✓	✓
Holidays	✓	✓	✓
Install	✓	✓	✓
Live!	✓	✓	✓
Network Settings	✓	✓	✓
Operator Logins	✓	✓	✓
Person / Asset Report	✓	✓	✓
Reader Profiles	✓	✓	✓
Readers	✓	✓	✓
Services	✓	✓	✓
Sites	✓	✓	✓
Tag Expiry Report	✓	✓	✓

Tags Not Used Report	✓	✓	✓
Tagholders	✓	✓	✓
Time Based Reports	✓	✓	✓
Time Triggered Actions	✓	✓	✓
Transaction Report	✓	✓	✓
Truncation Formats	✓	✓	✓
Truncation Rules	✓	✓	✓
Zone Occupancy	✓	✓	✓
Zones	✓	✓	✓
Absenteeism Report	✗	✓	✓
Account Settings	✗	✓	✓
Active Tours	✗	✓	✓
Areas Report	✗	✓	✓
Audit Report	✗	✓	✓
Behaviour (Threat Level)	✗	✓	✓
Buildings	✗	✓	✓
Companies	✓	✓	✓
Custom Menus	✗	✓	✓
Custom Report Management	✗	✓	✓
Departments	✓	✓	✓
Directory Configuration	✗	✓	✓
Hardware Comms Channels Report	✗	✓	✓
Lifts / Elevators	✗	✓	✓
Linking History	✗	✓	✓
Linking Management	✗	✓	✓
Live! (Threat Level)	✗	✓	✓
Messages	✗	✓	✓
Move	✗	✓	✓
Network Status	✗	✓	✓
Notifications	✗	✓	✓
Operator Profiles	✗	✓	✓

Person/Asset Access History Report	✗	✓	✓
Person/Asset Access Report	✗	✓	✓
Person/Asset Profile	✗	✓	✓
Reason Codes	✗	✓	✓
Routes (Scheduled Tours)	✗	✓	✓
Tagholders (Scheduled Tours)	✗	✓	✓
Threat Level History Report	✗	✓	✓
User Fields	✗	✓	✓
Vehicle	✗	✓	✓
Visitor	✗	✓	✓
Visitor Book	✗	✓	✓
Visitor Report	✗	✓	✓
Hardware Installation Report	✗	✗	✓
Network Status Trend Report	✗	✗	✓

Limits Enforced By Software

Area	Basic	Pro	Enterprise (APC)	Enterprise (AC)
System				
Sites	1	25	1 000	1 000
Tagholders	1 000	125 000	1 000 000	1 000 000
Tags	3 000	250 000	1 000 000	1 000 000
Access Groups	100	125 000	250 000	250 000
Doors	100	5 000	10 000	10 000
Per Site				
Tagholders	1 000	5 000	10 000	1 000 000
Tags	3 000	10 000	10 000	1 000 000
Access Groups	100	5 000	10 000	10 000
Controllers	100	200	200	200
Common Zones	64	64	64	64
Zones	100	200	500	500
Doors	100	200	500	500
Time Triggered Actions	100	200	500	500
Holidays	32	32	32	32
Access Time Patterns	128	128	128	128
Device Time Patterns	250	250	250	250
Per Controller				
Zones	64	64	64	64
Doors	64	64	64	64
Readers	64	64	64	64
Per Tagholder				
Tags	3	4	10 000	1 000 000
Access Groups	8	25	25	100
Per Common Zone				
Zones	32	32	32	32

Controller Firmware Limitations

Area	APC	AC
System		
Unit Type	164	150
Per Site		
Tagholders	10 000	1 000 000
Tags	10 000	1 000 000
Access Groups	10 000	10 000
Per Access Group		
Actions	20	10
Per Person		
Access Groups	10	255
Tags	10 000	1 000 000
Per Event		
Actions	25	128

Appendix B

Guide to manually configure SQL Server

SQL Server Configuration

From version 1.4.2 of Access Portal, and installer is available that will configure SQL Server Express 2012 for you. However if you wish to manually configure SQL Server Expres, the following will guide you.

- Run the installer for Microsoft SQL Server 2014 (*Express Edition provided on the DVD*). When given the authentication options, choose **Mixed Mode Authentication**. This means that you can logon to SQL Server using either windows authentication or as a user defined in SQL Server. The Access Portal server connects to SQL Server using the "sysdba" user defined in the Portal database.

  If for some reason you missed this step, you can change the server authentication options in SQL Server Management Studio after installation, by right-clicking on the server in object explorer, and selecting Properties. In the Properties dialog, select Security. Change Server Authentication to ***SQL Server and Windows Authentication mode****.*

- The Portal database must be attached manually. Open SQL Server Management Studio, expand the server name and right click on Databases. Select the Attach option. From the Attach Databases dialog, select Add, then browse to C:\Portal\database and select the PORTAL.mdf file. An entry will be added to the Databases To Attach table. Scroll to the right in the table until the "Owner" column becomes visible. Select "sysdba" from the dropdown menu that appears. Select OK and to save and close the dialog.

  A common problem during this step is that SQL server does not have permission to access the database files. There are two options to resolve this.

  The first option is to change the account that the SQL Server service uses. Open Services under Administrative Tools in Control Panel. Find the SQL Server Service and open its properties. Change the "Logon As" account to "Local System Account".

  The second option is to change the file permissions on the database folder. Open C:\Portal\Database\ in Windows Explorer. Right-click on the Database folder. On the Security tab, edit the permissions to include the user account that the SQL Server service is running as.

- SQL Server does not need to run on the same server as the Access Portal software. Connections to a remote server via hostname or IP address are also possible. By default *SQL Server Express* blocks remote connections. Open **SQL Server Configuration Manager.** Expand the SQL Server Network Configuration option. Select Protocols. Double click TCP/IP. On the Protocol tab, change **Enabled** from **No** to **Yes**. On the IP Addresses tab, change **Active** and **Enabled** to **Yes** for all the IP Addresses that are required to allow connections. Also change all **TCP Ports** to **1433.** This can be quickly done by setting the TCP Port to 1433 for the IP All option, which is the last IP Address option in the list of IP Addresses. On the main page of SQL Server Configuration Manager, expand **SQL Native Client.** Select Client Protocols, double click **TCP/IP.** Change the **default port to 1433** and **Enabled** to **yes.**

Appendix C

Bug Fixes and Known Bugs

Bug Fixes

Version 4.4.0

- **Misc**
  - Inhibit Scanner input: now limits number of readers it can inhibit to 10.
  - Scan Network dialog: ip range fields were overflowing onto the next line.
  - Scheduled Transaction Cleanup: improved handling of large datasets.
  - Scheduled Transaction Cleanup: allow a minimum of 7 days' worth of transactions to be kept for GDPR purposes. It was previously limited to 30 days minimum.
  - Delete Access Transactions maintenance task: improved handling of large datasets.
  - Search: searching for a person by an updated custom field value would not work.
  - Custom reports: some text entry filters did not work.
  - Readers view: uninstalling a reader would fail if the controller was offline at the time.
  - Readers view: select a biometric device for use with distributed templates would cause a favorites / enroll message to show.
  - Bulk Operations: detailed feedback is redirected to the report pdf that is generated. Only progress reports (e.g. 2 of 10) will be reported on screen during the operation.
  - Bulk Operations: improved handling of larger operations for over 1000 records. Some speed improvements have been noted as a result.
  - Batch Enroll: enrolling tags using Range option would fail.
  - Biometrics: improvements for scanning on subnets.
  - Biometrics view: fix for uninstalling a device
  - Biometric discovery: would not pick up units that had IP's that were not on DHCP
  - Biometrics view: would not show the new firmware version after upgrading until another network scan was performed.
  - Biometrics: fix for automatic upload of new templates to legacy Morpho devices.
  - Enrolment menus: unable to load these menus from a non-SYSDBA login.
  - Logging: fixed logging of API operations.
  - Operator Logins: when deselecting the Reset Password option the fields would remain enabled.
  - Inhibit Scanner: counts shown within the tabs for selected readers would remain as zero.
  - Pagination: improvements for loading the next set of records by scrolling to the bottom of the table.
  - Custom Fields: after updating a custom field value for a selected person record, searching using the new value would not work until you restarted the server.
  - Server app: removed the warning that shows when the database name has changed.
  - Graphics module: the IO modules were not able to be dragged and dropped onto the floorplan.

    - Graphics Runtime: removed the options to acknowledge alarms using either Password or Tag. These are not supported on Portal and never worked.
    - Graphics Designer/Runtime: general fixes to make it compatible with Portal.
    - Installer: unable to select individual items if Access Portal is not selected
    - Installer: in some cases the desktop shortcut would point to the wrong path to the installation.
    - API: fix for inserting new Time Pattern records with a specified start time and duration.
    - HIK dll: fix for issue where the dll would prevent the installation folder from being cleaned up after an uninstall.
    - PluginManager: would not start up after a windows restart.
    - PluginManager: would not expand when clicked on in the system tray
    - Visitor Book: would load a blank page when using Visitor.html or VisitorLogin.html in the url.
    - Tag Expiry report: date filters using ranges such as Last Week; This Month; etc. would not work and would default to showing results for the current date instead.
    - Access Groups: groups named using special characters (e.g. IT) would disappear from the list and be filtered out of searches.
    -
    - HIK: new finger enrolments won't work until a full upload is done.
    - HIK: when on a network that does not have DHCP or has MAC authentication, the device would not get a valid IP address when DHCP gets turned on at install time. The IP would be 0.0.0.0. We now allow the IP address to be edited after installing.
- **Suprema:**
    - Setting time to UTC+ would be overwritten by Portal on full upload. Now set via config file which Portal uses.
    - Mifare cards would not work on Suprema units

Version 4.2.5 (Service Pack 1)

- **Suprema:**
    - Scanning subnet when server PC has more than 1 network adapter, can also scan by IP range.
    - Suprema wrapper dll updates to attempt to overcome dll not found errors in Portal.
    - Face Enrolment fixed.
- **Morpho:**
    - Downloader fix where time sync kept looping.
    - Communication tweaks to improve stability.
- **XML API Wrapper:**
    - Fix for expiry reasons.
- **Languages:**
    - Bulgarian updates.

Version 4.2.0 (Beta)

- **Impro Biometric Reader:**
    - Improvements for reporting the queue count per device in the Biometrics view

    - Uninstalling a device that is still in secure mode will now warn that a factory default is required and provide the option to perform one.
    - Allow the user to retry or skip when an error occurs during finger capture.
    - Factory Default is no longer blocked when the device is busy.
- **Tags:**
    - Write to card now allows encoding of card only. No fingerprints required.
    - MorphoWave enrolment now prompts the user to present their hand.
    - Replacing a card that has templates will now cause an upload of that tag.
- **Services:**
    - An upload queue will no longer build up for Aperio devices, which do not support the queue.
    - Fix for running Portal as a service using Local System User. Fixes file permission problems.
- **Port app:**
    - Some fixes and improvements.
- **Database Upgrade:**
    - When upgrading a database that is close to 10G in size, we now ask for confirmation that the database has been backed up first. This is necessary to prevent issues caused by exceeding the database file size limit imposed by SQL Server.

Version 4.1.0 (Beta)

- **Batch Operations:**
    - Shows duplicate entries in the pdf report
- **Card Printing:**
    - Status messages show for too short a time before disappearing.
    - Print Tag and Read Tag And Print buttons were missing from the Printing tab.
- **Tags**
    - A standard write to card for Morpho devices would ask the user to select which fingers to write. We now always just write the two fingers that have been enrolled and do not prompt for finger selection.
    - Tag encoding was forcing a finger to be encoded when choosing to encode the PACs only.
    - The Printing tab no longer had the Print Tag and Read And Print buttons.
    - The status message on the Printing tab would show for too short a time.
- **API**
    - The profile and setting names were not returned via an API call.

Version 4.0.0

- **Access Time Pattern:** Wrong times were being sent to the controller.
- **API:** Automatically initiated transaction broadcast.
- **Batch operations:**
    - APB override / tag status / tag expiry dates not being saved.
    - Could not update tag expiry dates.

- **Biometrics:**
    - Templates did not get uploaded to MA500.
    - Writing template to card using Omnikey did not work because user could not select finger/template.
    - Fingkey: Could not be uninstalled.
    - Nitgen: Broadcasting status change based on address instead of its serial number.
- **Controller:**
    - Did not allow non-standard port settings, as configured in discovery, to be used.
    - Controller firmware version: was no longer updated in the database.
- **Dashboard:**
    - Commands Widget: Given Permission denied warning, but can still operate the command.
    - Transaction viewer displaying previous tag number when presenting current one.
    - Unable to select a colour for a widget.
- **Database Port:**
    - IO8 units should not have been added to location.
    - IO8 units port as wrong unit type.
    - Update script: Was needed to resolve startup errors on database port application.
- **Doors:**
    - Readers from non-related Controllers were available for selection.
    - Unable to assign other Zones to door after selecting the first Zone.
- **Enrolment:**
    - Performance degradation experienced after 30+ enrolments.
    - Tag Expiry: Credentials that were automatically created with the same start and expiry dates and times (00:00:00). Engine interpreted this from today 00:00:00 till tomorrow 00:00:00.
    - Morpho Enrolment (Legacy Readers): Can't save to reader databases 1 to 4 only the default database (database 0).
- **Glasspane:** Removed before the install/uninstall has completed.
- **Holidays:** When selecting start date higher than end date needed to adjust end date to match.
- **Image Capture:**
    - Camera: Capture dialog loaded twice when button was pressed multiple times.
    - Crop and undo buttons enabled after save was executed.
- **Install / Replace:**
    - Deleting a door would not default the assigned readers to their original names.
    - I/O units fail to install if there is no default Input/Output profile (all types affected).
    - Readers: Could not replace Virtual Reader with 485 Reader.
    - Server: Stated errors when installing BMTA units.
    - Virtual Controller and Reader: replacing virtual devices before adding them to door resulted in a system failure.
    - Search table: Did not refresh after replacing a reader. The replaced reader was showing a row with no information.
- **Jetty:** Needed updating to 9.4.20.
- **Login:** Often took two attempts before you were allowed in.
- **Lucene:** unable to add Lucene index / read index / write index issues.

- **Reports**
    - Custom Report: Deleting a custom report caused a Null Pointer Exception in queue builder.
    - Person/Asset report: Tag APB override filter did not work.
    - Threat Level History report loaded the details view every time filter was deleted.
    - Visitor Report: Adding new report after selecting the Graph tab caused the view not to load the details tab.
    - Transaction Report: Export did not show the event being filtered by.
- **Operator Security**
    - Default view: Operator profile set with default view only loaded the Dashboard at login.
    - Dashboard not available to non-sysdba logins.
    - Operator Profile: Permission did not allow the use of Vehicle / Visitor views.
- **Reader Profile:**
    - Buzzer volume parameter ambiguous.
    - Door Mode Patterns: Default time patterns from all sites showed in selection.
- **Sync**
    - Synch BIO only: Did not upload all biometric template types (only BMTA).
- **Uninstall / Delete:**
    - User Login: It was not possible to delete a user login that had dashboard widgets / saved columns & filters.
    - Deleting visitor: Failed to delete if the visitor was linked.
    - Unable to uninstall controller (FK on DiscoveryGroup).
- **Upgrades**
    - MDR upgrades: ignore errors when address out of bounds.
    - Firmware Upgrade: Did not correctly read the version from the ec3.tar.gz.
- **Zones:** Views displaying the icons in the wrong place.

Version 3.5.0 (Beta)

- Various bug fixes.

Version 3.0.6

- **Access Groups:** The Tagholder view would no longer show the Access Groups tab in some cases.
- **Columns/Filters:** Fix for duplicates showing in reports and Operator Profiles.
- **Custom Reports:** Fixed import and delete of custom reports.
- **Profiles:** Fix for issue where saving a new Input/Action would sometimes fail and ask for all fields to be filled in.
- Various minor bug fixes.

Version 3.0.4

- **Image Capture:** Fixed image capture which was broken with the Chrome Version 71 update.

- Various minor bug fixes.

Version 3.0.2

- **Internet connection:** The v3.00 release did not allow a user to connect to the web client if the server did not have an internet connection.
- **Unicode characters** The v3.00 release did not show unicode characters on the server application. This caused unsupported glyph characters to be displayed in the server transaction viewer.

Version 2.2.0

- **Aperio Integration:**
  - Threat level would only work under very specific conditions.
  - Time sync would sometimes fail.
- **API:** Controller online/offline status was only reporting for one controller.
- **Nitgen Biometrics:** After updating the Nitgen SDK to support the T1 reader in 2.0.0, it was noted that the nitgen integration had been broken. The integration has been rolled back to that of version 1.8.4 to resolve this issue. This also means that the nitgen T1 is not supported in Portal.
- **Time Based Report:** A condition existed that would only load the first few people / assets for the report.

Version 2.0.0

- **Date range filters** on some reports, such as absenteeism report, were not working.
- **Mobile Portal** was receiving denied biometric in for valid finger presentations. To update, copy the latest Mobile Portal cab installer to the Mobile Portal device and install it.
- **Tag Truncation Rules:** the view for creating custom tag truncation rules was repopulating the bytes from the tag mask when being cleared making custom rule creation difficult.

Version 1.8.4

- **Time Based Report:** Zone information for interleading transactions were incorrectly stored. If a time based report was run while filtering for time in a specific zone, the wrong times could have been calculated. (**Only a problem if a zone filter was used**. Transactions automatically get corrected with this update).
- **Multi-Site:**
  - Device Actions
  - Multi-Site person / asset access groups.

Version 1.8.2

- **Software:**
    - Nitgen / BMTA Portal Plugin Manager Issue. If different fingers were selected from the UI at enrollment to a previous enrollment, the possibility existed that the previous person's templates would be saved to the current enrollment. *(Applicable to Portal 1.60 and 1.80. Please uninstall and reinstall Portal Plugin Manager and required Portal Clients).*
    - Uploading more than 50 templates to a suprema OEM terminal took longer than it should.
    - Web Based Live! Transaction Viewer would not show transactions, depending on the time zone of the site.
- **Firmware:**
    - APC would require a full-upload after a power failure. *(Applicable to APC's on version 2.0 only)*
    - BMTA would not recognise some valid fingers. (Applicable for BMTA's running as an entry and exit reader / Users needed to press IN or OUT).

Version 1.8.0

- Adding an Out Buzzer action saves with the wrong direction which caused it to not be given to Entry readers.
- Exporting to csv / pdf from Asset Linking view throws exceptions and fails
- Uninstalling controllers from the Install view

Version 1.6.0

- **Operator Security:** Improved enforcing of Operator Security for all views.
- **Safe IP:** Safe IP requires an IP address to be sent to a unit so that it knows that only communications from this IP address is allowed. The IP address that is sent it the one configured in the site table, which is not configured for the default site unless a user configures it. We will now attempt to automatically set the IP address for each site after a DB upgrade was performed if a site does not have a valid IP address.
- **Suprema Biometrics:**
    - search failed when suprema devices not yet supported by Portal were found or if devices found had a device ID / serial number that when converted to hex was shorter than 8 characters.
    - Some supported suprema units were not being detected by Access Portal because of an unexpected ID being returned by some units.
- **System Resource Usage:** Improved system resource usage and memory usage.
- **Tag Truncation:** The wrong tag code was generated for tag codes using a truncation format that made use of the drop-zero bits function.
    - Truncation format that **had** this bug.
        - 26-bit Normal
        - 26-bit Raw
        - 37-bit Normal (UK)
        - 37-bit Raw (UK)
        - H10302 37 Bit Raw 35 Bit Tagcode(US)

        - H10304 37 Bit Raw 19 Bit Tagcode (US)
    - Truncation formats **without** this bug.
        - Standard 16-bit
        - Standard 24-bit
        - Standard 32-bit
        - Standard 40-Bit
        - Untruncated

    The untruncated tag code is always stored for all tags. If you need to re-truncate your tags code, change the truncation format on the required tag type to **untruncated** then change it back to the original truncation format.

Version 1.4.0

- **APC Discovery:** Changing ports or setting safe-IP on a cluster controller in APC mode had a bug. Requires firmware upgrade to APC.
- **Biometrics:**
    - New Nitgen terminals would only show in the Biometric Configuration tab after restarting Portal Server.
    - Performing a biometric enrollment would upload templates to biometric terminals that had the same ID as the access control readers that the user had access to. (This would only have been a problem with distributed templates. Full upload to temporarily work around the problem)
- **Inputs:** When installing a reader that supports Door Open Sensing, the reader would not be given support for the DOS Door Closed events.
- **Mobile:** Loading Portal from a mobile device had a bug which prevented the menus from showing.
- **Time Synch:** Time on hardware was being synchronized to the server time regardless of the time zone set for the site. The time zone of a site is now used to calculate the offset to send to hardware. This should only be noticeable if you have a site in a different time zone to the server.

Version 1.2.0

- **Biometrics**: On systems using third-party biometric readers, it was possible for the software to reach a state of continuously uploading incompatible records to a biometric reader, resulting in it becoming unusable.
- **Inhibit Reader:** Inhibit Reader settings were lost during a full upload. A single inhibit reader input is now restricted to five readers. Readers can now be removed from an inhibit reader input.
- **Live Transactions:** Live transactions refresh more often. Improved responsiveness under high transaction load.
- **Minor UI Improvements:** Various minor user interface improvements.
- **Operator Security:** Removed the link to the user profile view for the logged in user.
- **Quick Enroll:** Quick enrol option removed for tags that have already been enrolled on a different site.
- **Running multiple instances of portal:** Can now only start a single instance of the Portal Server application.

Known Issues

- **Access Portal (x64):** does not support Suprema BioStar v1.xx biometric terminals.
- **Anti-virus programs:** may cause issues while installing or uninstalling plugins for tag reading or biometric enrollment.
- **Batch Enrolment:** Cancelling unsaved changes will not work
- **Browser cache:** The browser cache needs to be cleared after upgrading the software for the latest changes to take effect.
- **Card Printing:**
    - Printed color differs from card designer color
    - Does not ask for the server details on installation.
- **Device Time Patterns:** Editing DPT 1 will change DTP 2 unit configurations as well
- **FW Upgrade Tool:**
    - the current version of the FW Upgrade tool does not have support for upgrading the Application Controller. Contact our support department for help with Application Controller upgrades
    - Doing a full Firmware upgrade will not indicate when it is finished.
- **Login:** After 30min the system will log you out if no activity but you have to start a new session because the valid username and password will not work.
- **Maximum Access Group Capacity:** This feature is not supported across controllers.
- **Morpho Wave:** New hand does not replace the old
- **Plugin Manager:** Messages get queued.
- **Replace:** Replacing a 485 BMTA that is set to In/out will not display the second fixed address for selection to replace.
- **Reports:**
    - The filter for “Has Templates” has a “yes” and “no” option. The “no” option returns anyone who has a tag without templates. So if a user has two tags, one with templates and one without, when using the “no” option the tagholder will still be returned.
    - Tag Expiry Report: Tag showing wrong expiry state as long as end date is set to today (end time is irrelevant).
- **Search Table:** does not always load the next set of results when scrolling to the bottom of a table.
- **Sync** syncing two units every now and then gets in a bad state
- **SIGMA biometric reader:** Readers go "offline" with a socket error - they are not offline
- **Transaction Viewer:** Special characters can disrupt the transaction viewer
- **Visitors:** Visitors created using Access Portal are not available from Visitor Portal.
- **Browser Tabs:** when multiple tabs are open in the browser, some views do not refresh correctly

Version 1.8.0

- **Site** There is currently no support for deleting a site that already has people and/or assets saved to it.

Version 1.6.0

- **Person/Asset Profile** When changing an Asset profile to a Person profile, people of this type of profile will still appear in the list of assets that can be assigned to a person until the Access Portal server has been restarted.

- **Network Status** When changing the site filter while on the Network Status view, the view will need to be reloaded, by going to the main menu and back, before it will accept the changes.

Version 1.4.0

- **Scheduled Tour Tag** Adding a new tag with Scheduled Tour enabled will not show in the Tagholders view under Scheduled Tours menu until you either resave the tag or restart Portal.