Jakin®ID

SaaS Access Manager Suite
User Manual

The Ultimate SaaS Solution for Managing All ACTAtek Devices

SECURITY

WORKFORCE MANAGEMENT

PAYROLL

Version 1.0.9 October 2023 JakinID

Revision History

Revision	Date	Description	Author
1.0.9	2023/10/11	Added Appendix F. Anti-Pass Back Group Added Appendix G. Health Risk Assessment Added Appendix H. Time off Management Added Appendix I. Payroll Management Added Appendix J. Facial Finger Print Self-Enrollment Added Appendix K. Enhance Security Settings Added Appendix L. Events Log to File Setting Added Appendix M. Payroll API Setting Updated AMS UI with new UI layouts. Updated Hardware Software requirements for AMS Re-Arrange the pages and contents Update Front page	Mohamed Anfas
1.0.8	2018/10/14	Added SaaS AMS Introduction. Chapter 1 Updated Basic System Requirements and compatibilities Added Add new Domain. Added Register Acta Series of Products to AMS Domain Added Login to AMS as Domain Add Upgrade ACTA3 Firmware to support SaaS AMS Added Register Acta Series of Products to SaaS AMS	Mohamed Anfas
1.0.7	2017/06/07	Added Chapter 5 AMS Workforce Management Added Chapter 5 AMS Work force Management Shift Manager – Access Apps Updated Chapter 6 AMS Workforce Management & -Access Control Advance Features. Updated View Terminal List Updated Bulk Edit User Updated AMS UI Updated Network Diagram Added Site/Location Feature Added Site/Location Feature System Diagram	Mohamed Anfas
1.0.6	2015/03/25	Updated Department Association Added AMS Server Unreachable Precautions for APB	Michael
1.0.5	2014/08/11	Updated Operating System Requirements	Michael
1.0.4	2014/05/28	Added Email Setup and User Message	Michael
1.0.3	2014/03/04	Added Terminal Time Zone Configuration in AMS	Michael
1.0.2	2013/11/13	Added Upgrading AMS procedures in Section 7	Michael
1.0.1	2013/08/26	Added Access Apps Shift Manager	Michael

1.0.0	2013/08/02	Official Initial Release	Michael

JakinID Access Manager Suite User Manual

Offices:

Asia and the Rest of the World:

Jakin Technology Ltd.
Unit 901-2, 9/F, Fo Tan Industrial Centre,
26-28 Au Pui Wan Street,
Fotan, Shatin, Hong Kong

Phone: (852) 2319 1333
Fax: (852) 2776 8997
E-mail: sales-row@ACTAtek.com (Sales Enquiries)

Americas (North & South America):

Jakin ID technology Inc.
Suite 200, 10800 Voyageur Way
Richmond, BC V6X 3G9
Canada

Phone: (604) 278 8888
Fax: (604) 278 6082
E-mail: sales-ca@ACTAtek.com (Sales Enquiries)

Europe, Middle East & Africa:

Jakin UK Ltd.
Unit 7 Lightning way,
West Heath, Birmingham B31 3PH
U.K.

Phone: (44) 121 411 2288
Fax: (44) 121 411 2299
E-mail: sales-eu@ACTAtek.com (Sales Enquiries)

Contents:

Chapter 1: Overview

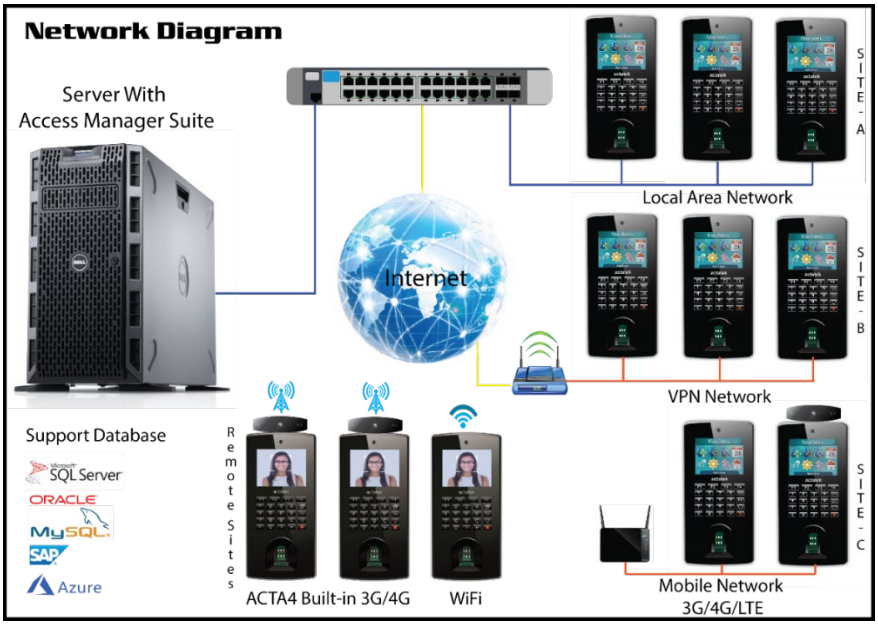
1.1 SaaS AMS Introduction

AMS Software as a service (SaaS) is a software distribution model in which a third-party provider hosts the AMS in their servers and makes them available to customers over the Internet. SaaS is one of three main categories of cloud computing. AMS SaaS Cloud services offer high scalability, which gives customers the option to access more, or fewer, services or features on-demand.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Access Manager Suite (AMS) provides centralized web-based control and management to multiple Acta Series of Products environment setups. It also comes packed with features without any limitation in its software so that the system administrator can have full control of the Acta Series of products at all times, either on site or remotely. In addition, the AMS software gathers event log data from all Acta Series of products into a centralized database to simplify user redundant tasks. To enhance user management, AMS will facilitate all data synchronization of Acta Series of products from user modifications to newly added users. Adding or editing users in the AMS control center becomes an easy process along with managing access groups and rights, departments, open door schedules, and reports.

The AMS software is designed to be robust and versatile so that Acta Series of Products on different networks, either public or private, can connect and communicate in a global scale.1.2 Network Diagram



1.2 System Requirements

Hardware Requirements	
CPU Processor	Core i3 1.20 GHz or faster (32-bit/64-bit)
Memory	8.0 GB or higher
Hard Disk Space	20.0 GB or higher
Network Controller	100 Mbps or higher

Software Requirements	
Operating System	Windows 7 Professional (32-bit/64-bit) or above Windows 8 Professional (32-bit/64-bit) or above Windows Server 2008 R2 SP1 (64-bit) or above Windows Server 2012 (64-bit) or above Windows Server 2016 (64-bit) or above Windows Server 2019 (64-bit) or above Windows Server 2022 (64-bit) or above
Database Server Software Support	Microsoft SQL Server 2008 Microsoft SQL Server 2012 Microsoft SQL Server 2014 Microsoft SQL Server 2016 Microsoft SQL Server 2019 Microsoft Azure SQL Server MySQL Oracle AWS
Microsoft .Net Framework	2.0, 3.5.1, 4.0 & 4.7
Supported Web Browser	Microsoft Edge 108.0 or higher Firefox 3.5 or higher Chrome 6.0 of higher Safari 5.0 or higher

1.3 Microsoft .Net Framework Requirements

AMS Version:	.Net Version Requirement:
1.2.5.5 Build 2022.06.06 Or above (Latest)	Framework.Net 4.7

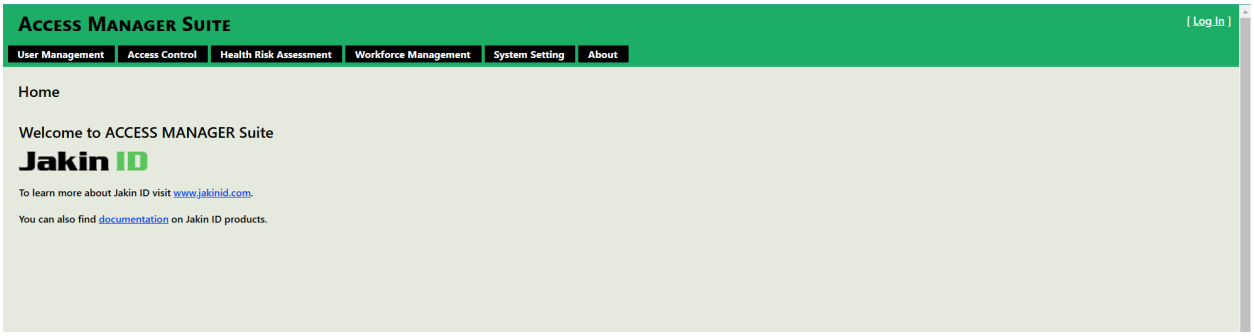
To download Microsoft .Net Framework, follow the link: http://www.microsoft.com/net/downloads

Chapter 2: Configuring SaaS Access Manager Suite

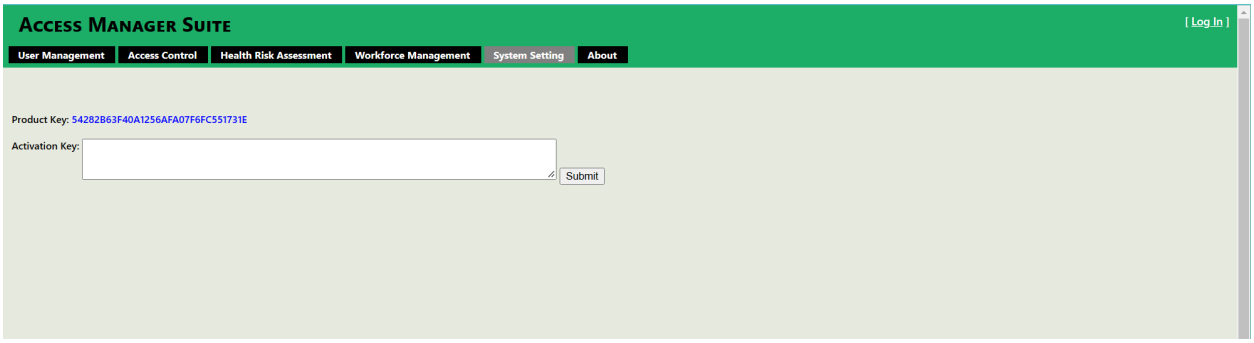
2.1 Accessing AMS

Method	URL
Local computer access to AMS	http://localhost/AccessManager/
Network access to AMS	http://**IP ADDRESS OF SERVER**/AccessManager/ Example: - http://192.168.1.101/AccessManager
Network access to AMS with customized port	http://**IP ADDRESS OF SERVER:PORT NUMBER**/AccessManager/ Example:- http://192.168.1.101:8080/AccessManager

Enter the URL applicable to the method of accessing AMS to the address bar of a web browser.



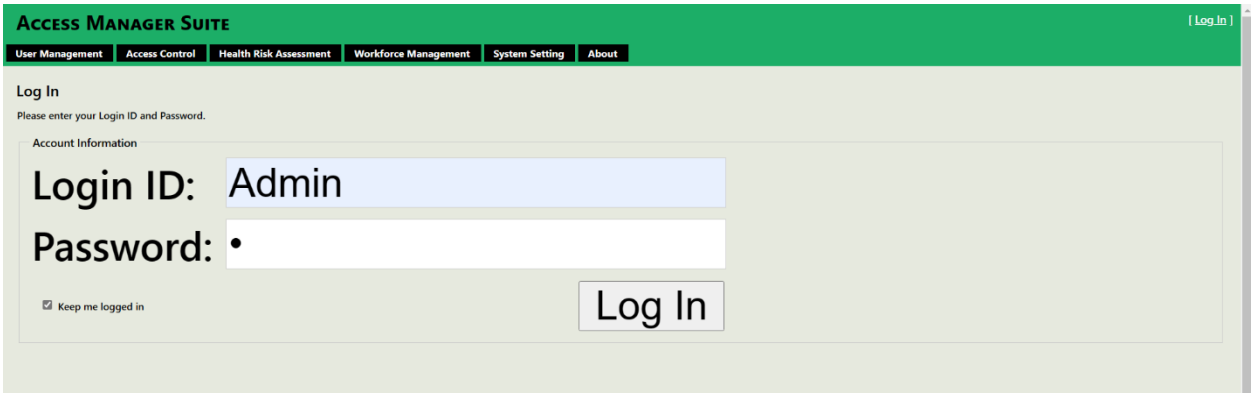
2.2 Activate AMS



Press **Log In** at the top right to obtain the new activation page. Contact JakinID support staff and provide the **Product Key and About tab's screenshot** to them and in return, you should receive an **Activation Key** back.

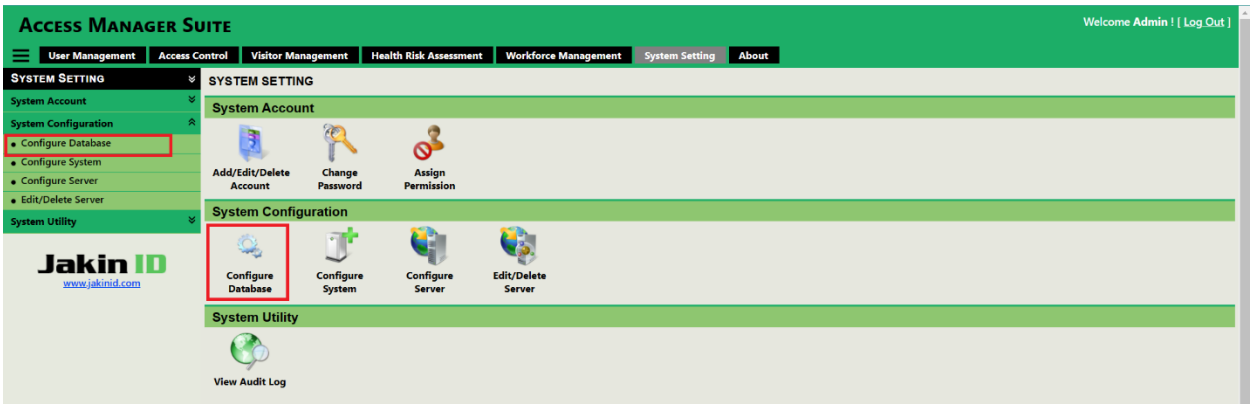
2.3 Log into AMS

Administrator Default Login Details	
Login ID	Admin
Password	1



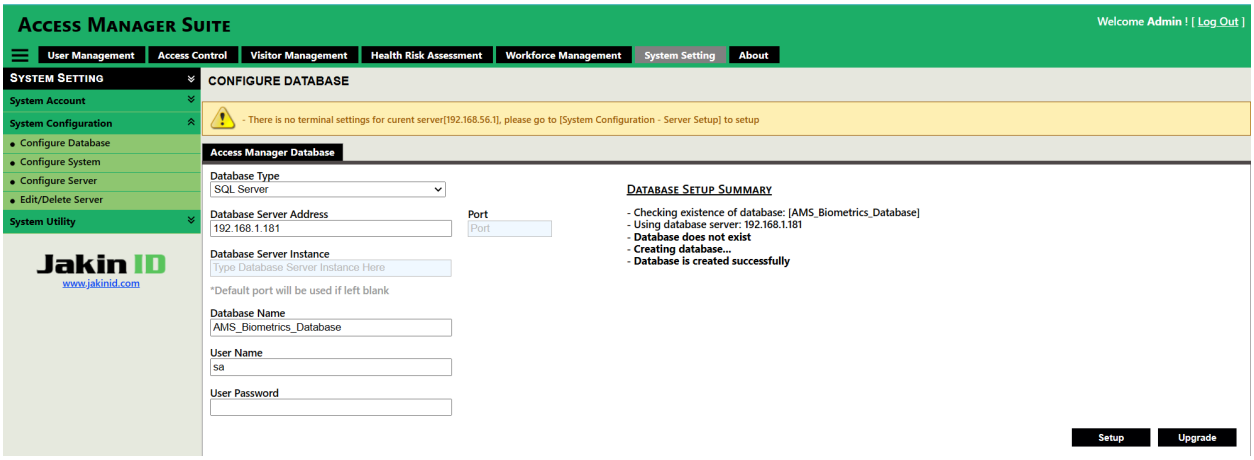
2.4 Setup Database In AMS

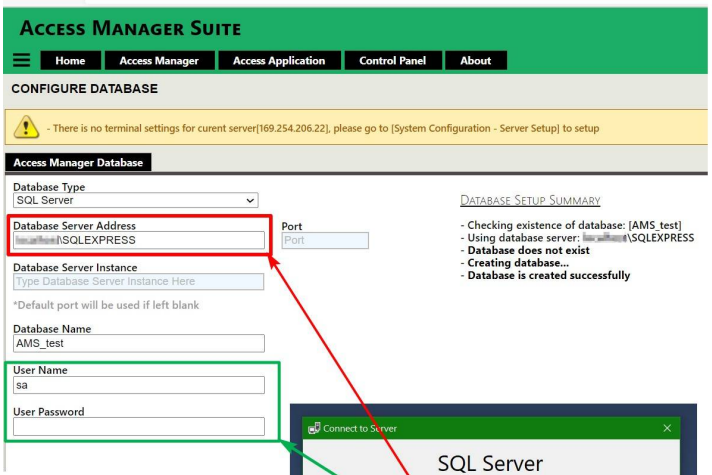
Once you've logged in as an administrator, go to **Control Panel** and then **Database Configuration**.



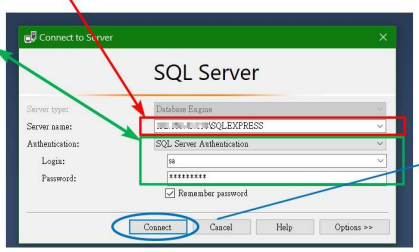
2.4.1 Setup SQL Database Server

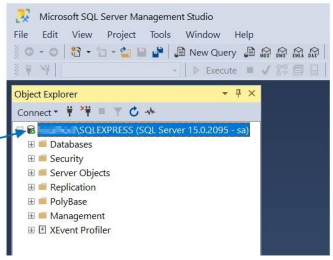
Choose the correct **Database Type**. Enter in the **Database Server Address** which includes either the IP address of the database server followed by the instance or localhost followed by the instance. For the **Database Name**, ensure that you have entered a database name that does not exist in your database server so that is creates a new AMS database. Supply the appropriate **User Name** and **Password** with rights to create the database in your database server. Press Setup to proceed and the successful output can be seen below.





Please use MS SQL Server Management Studio software to verify the Login information/connection profile of SQL server when setting up AMS database.

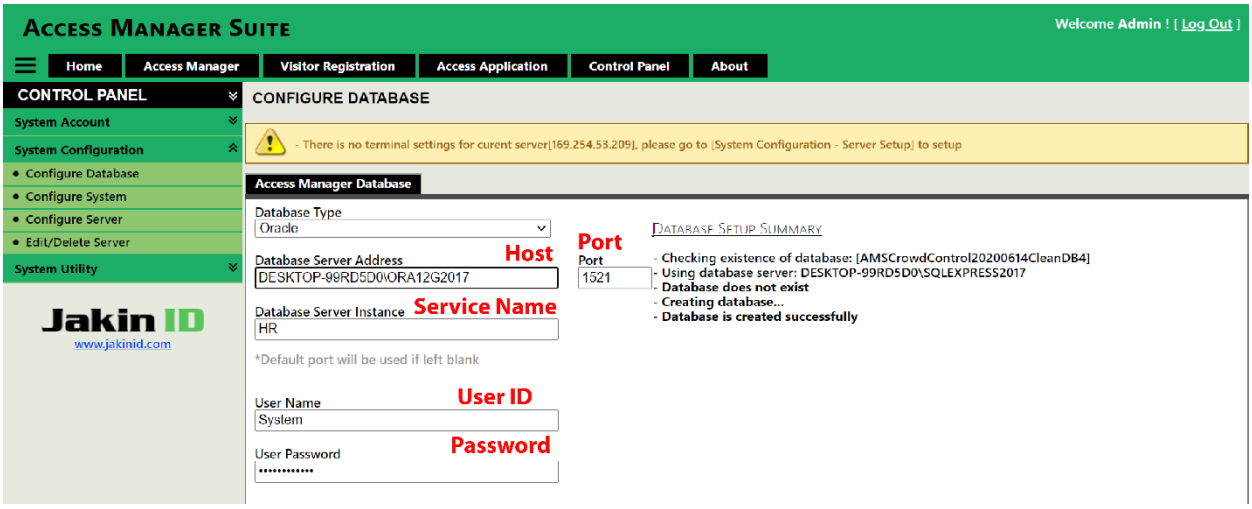




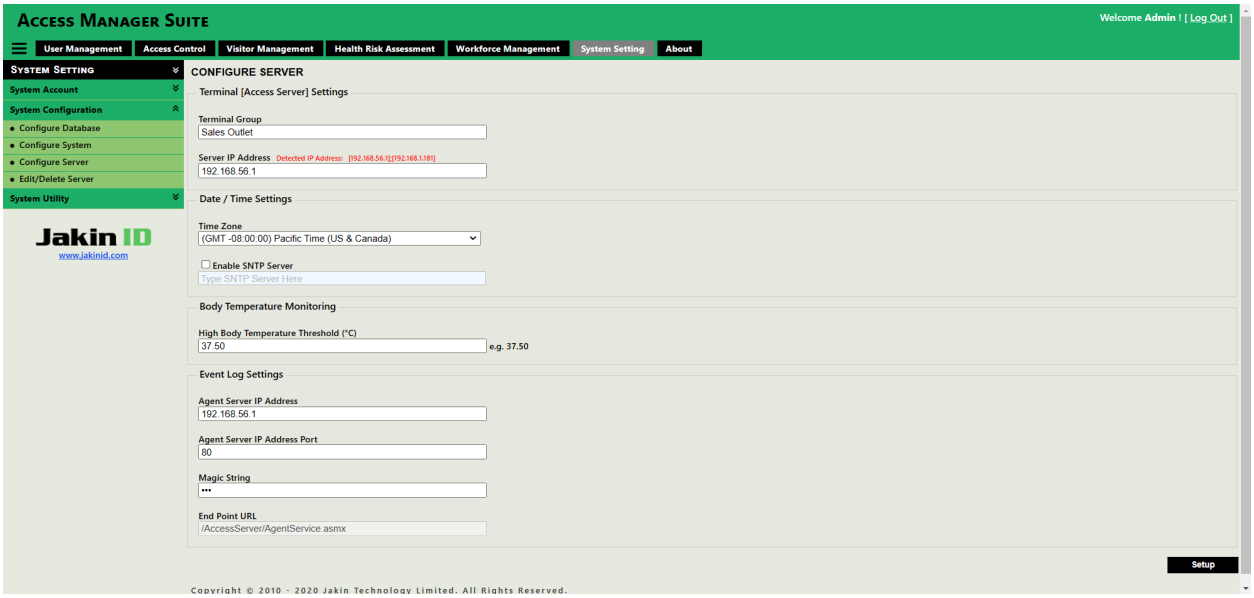
2.4.2 Setup Oracle Database

1. Under Database Type select **“Oracle”**
2. Type the **Database Server Address**. E.g. localhost or IP address * If you are connecting to another server via Intranet. Make sure to include the port number after the IP address separated by colon “:”
3. Key in the **Database Server instance** based on your preference.
4. Key-in the **user’s name** “system” (default user which can create, edit and delete on the database)
5. Enter the **password.**
6. Click **Setup** then the page will appear same as shown on Figure 2.0 as a successful connection.

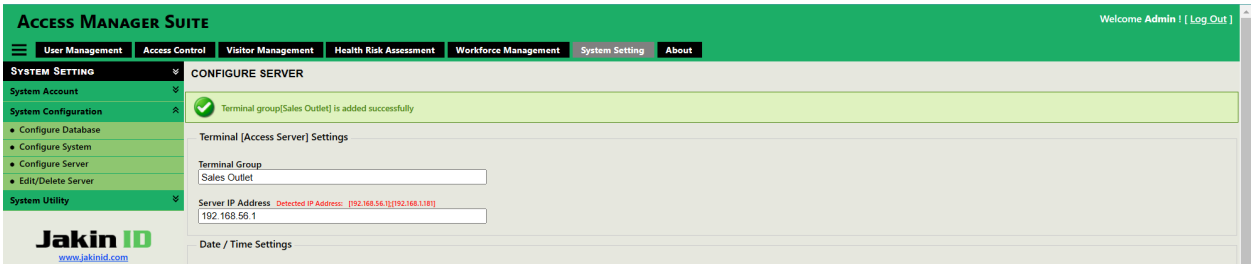
For AMS ver.1.2.5.5 Build 2020.09.11 or above latest version



2.5 Server Setup In AMS

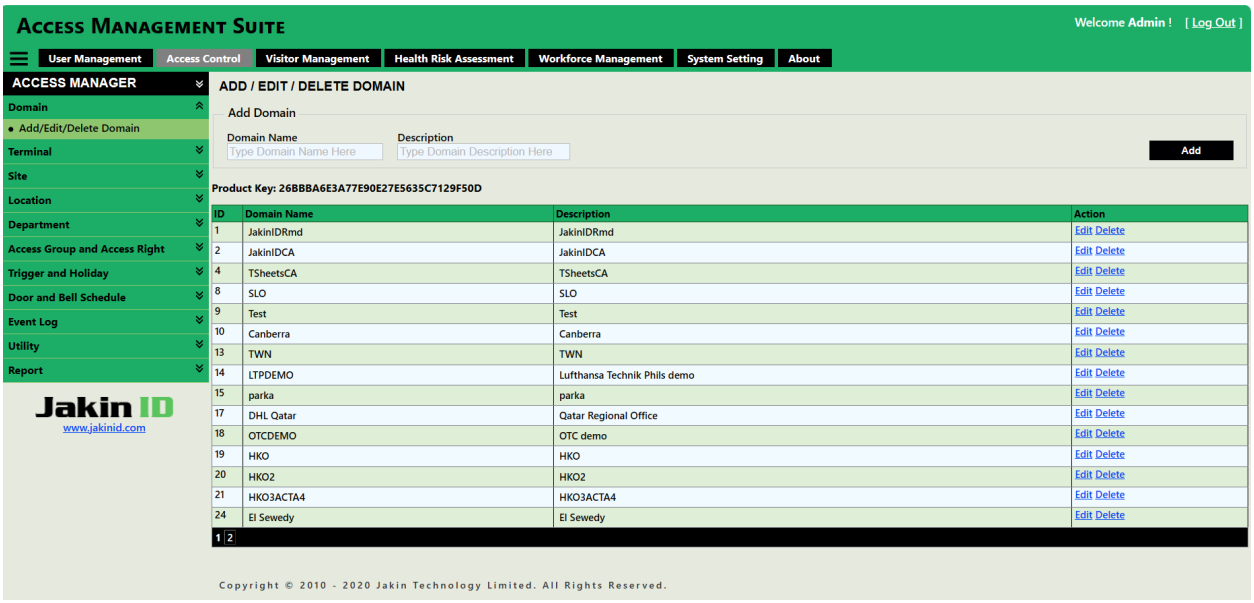


Next step is to go to **Control Panel** and then **Server Setup.** Enter a desired **Terminal Group** name and ensure the **Server IP Address** corresponds to the detected Server IP. Now provide the time zone information in accordance with your region. A public SNTP server is **pool.ntp.org**. Now provide a **Magic String** of your choice which will be used as the encryption and decryption key while transporting event logs over the network. Press the **Setup** button to save changes. A successful message will appear like in the below image.



2.6 Add New AMS Domain

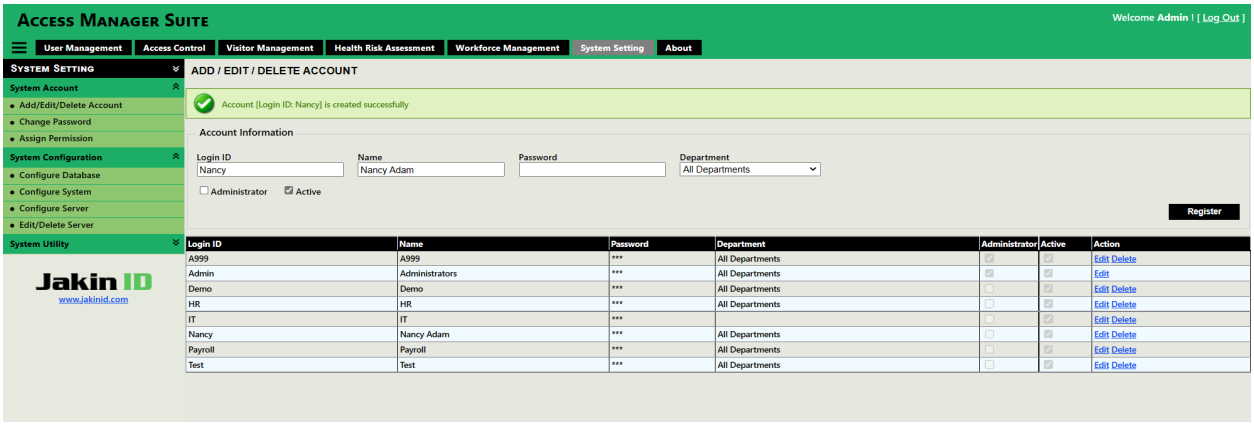
To add new AMS Domain, go into **Access Manager** and then select **Add/Edit/Delete Domain**



Key in the Domain Name and Description based on your preference and select **Add**.

2.6 Add New AMS Login Accounts

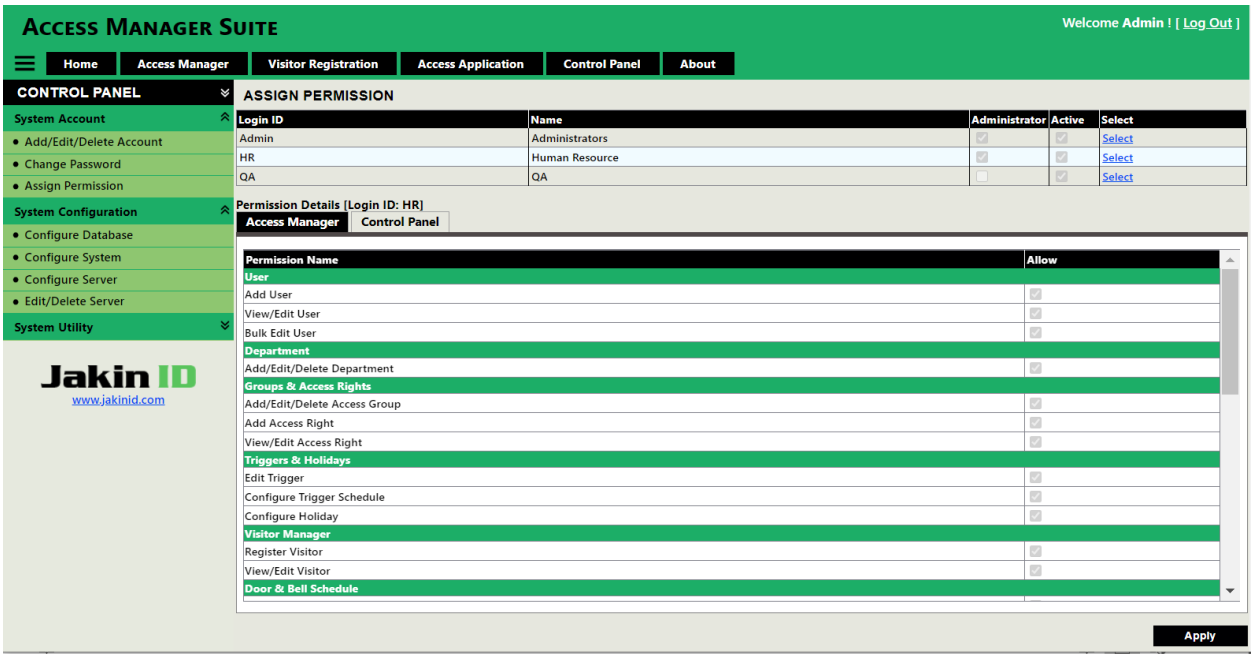
To add new AMS login accounts, go into **Control Panel** and then **Register/Edit/Delete Account** under **System Accounts**.



Provide a new **Login ID**, **Name**, and **Password**. Check the boxes for **Admin** and **Activate** and press the **Register** button to add the new administrator account.

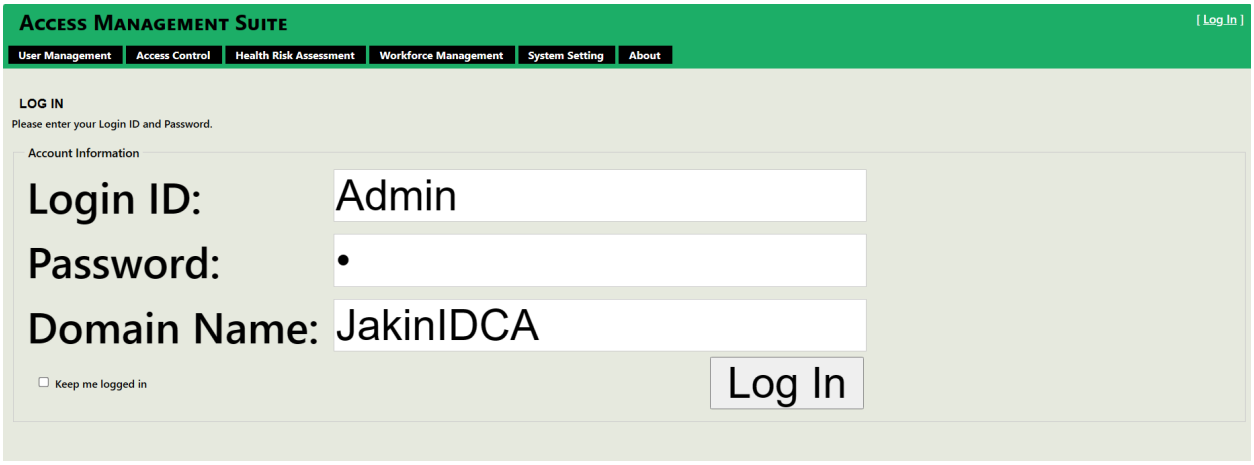
2.7 Assign Permission To AMS Login Accounts

Go into **Control Panel** and then **Assign Permission** under **System Accounts**. Press the **Select** clickable link to change permissions for the corresponding user. Now check and uncheck areas in Access Manager you wish to restrict or grant access for this particular user. Press the **Apply** button to save the changes.



2.8 Login to AMS as Domain User.

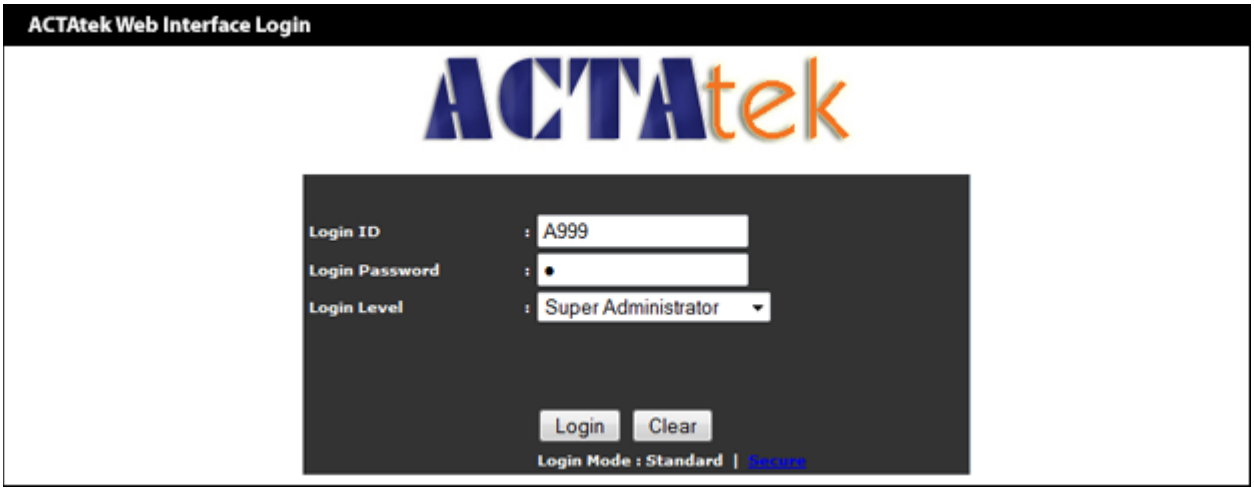
Enter the Login ID/Password and the Domain name and click Log In button to access the SaaS AMS with a particular domain



Chapter 3: Configuring ACTA Series of Products

3.1 Accessing the ACTA Web Interface

Super Administrator Default Login Details	
Username	A999
Password	1



By entering the IP address of the ACTAtek device in a web browser of a computer that is connected to the same network as the ACTAtek, you will be able to bring up the web interface as shown above. Now you will be able to login to the ACTAtek over the network for configuration.

***It is important to use capitalized letters in the Login ID field.**

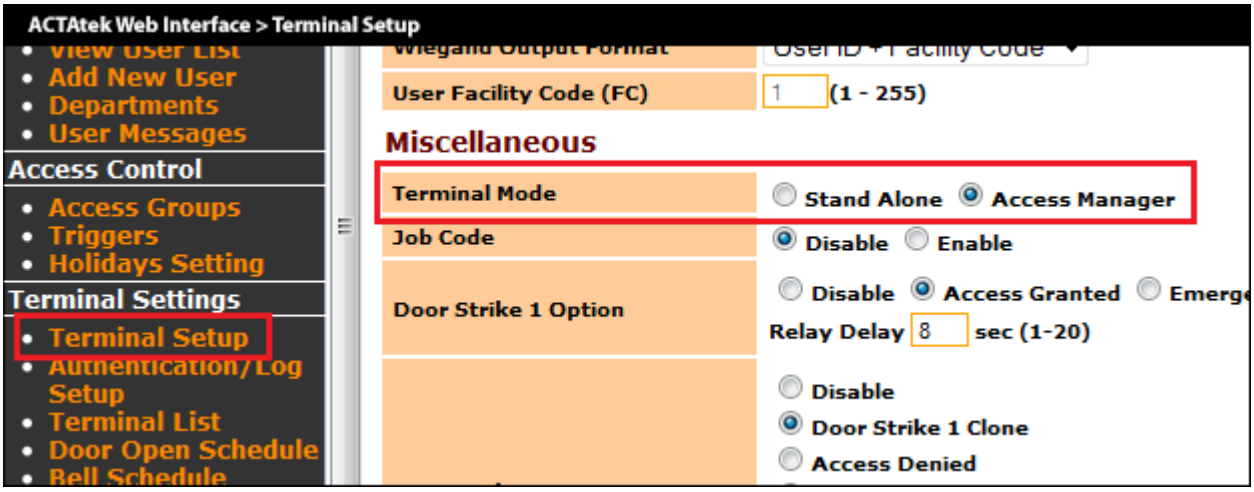
3.2 View Device Information

To obtain the ACTAtek device information such as the current IP address, serial number, connectivity status, and more; press the enter key 6 times on the key pad.

Follow this sequential pattern: ↵ ↵ ↵ ↵ ↵ ↵ on the key pad.

3.3 Enable Access Manager Mode

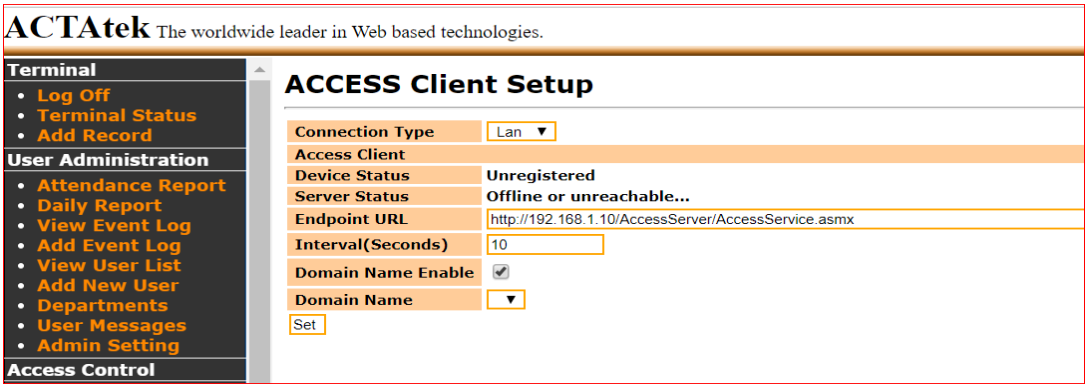
Once you have logged in as super administrator through the web interface of the ACTAtek terminal, click on **Terminal Setup** in the **Terminal Settings** menu. Scroll down on the page and locate the **Miscellaneous** heading. In **Terminal Mode** setting, switch over from **Standalone** to **Access Manager** and press the **Submit** button at the bottom of the page to save the changes.



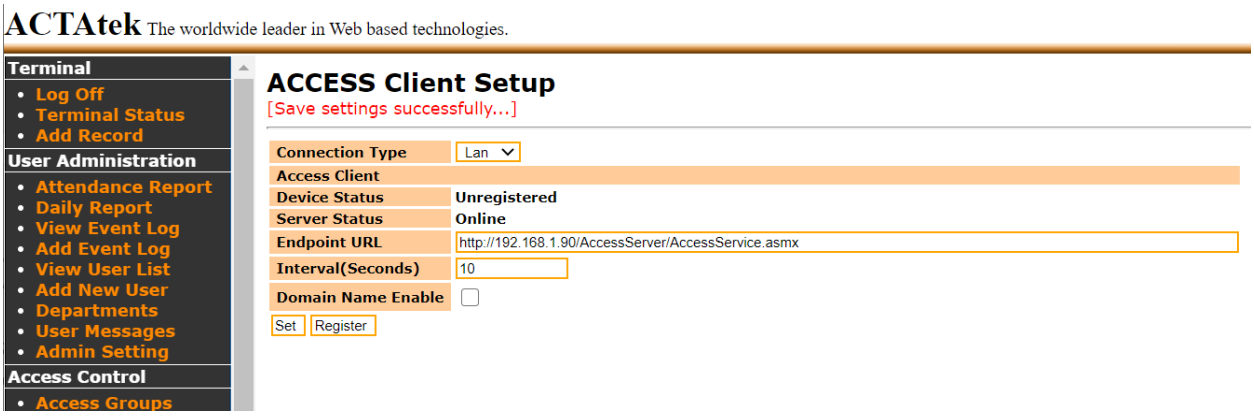
3.4 Register Acta Series of Products to SaaS AMS

After **Access Manager** terminal mode is set, proceed by clicking on **Access Client Setup** in the **Terminal Settings** menu. Provide an **Endpoint URL** that point to the Access Manager Suite Server via an IP address followed by the port and the location. Then select **Domain Name Enable** and Press the **Set** button to test the **Endpoint URL**.

Endpoint URL: http:// IP ADDRESS OF AMS:80/AccessServer/AccessService.asmx
Example: http:// 192.168.0.14:80/AccessServer/AccessService.asmx

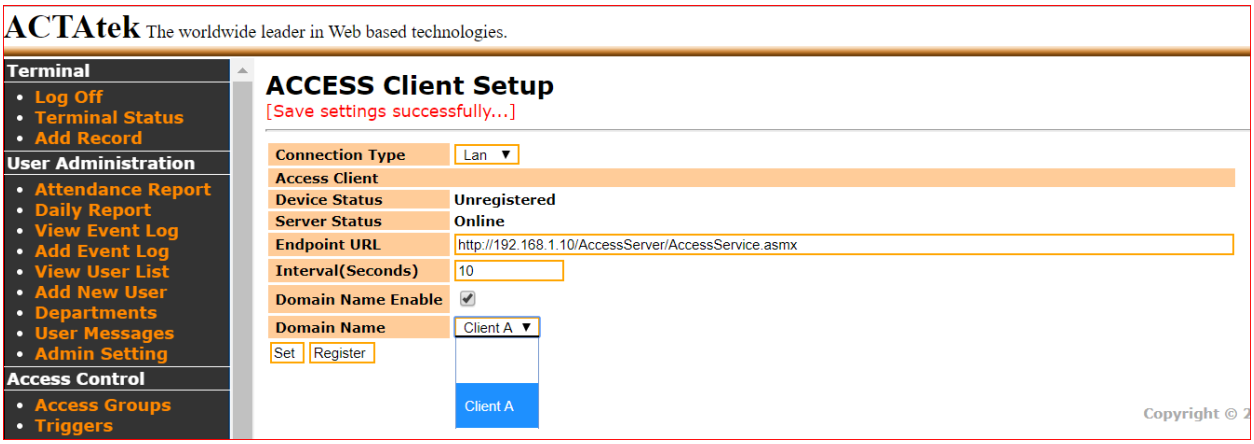


If the **Register** button appears, that means the ACTATEK terminal was able to connect to the Endpoint URL that was provided.

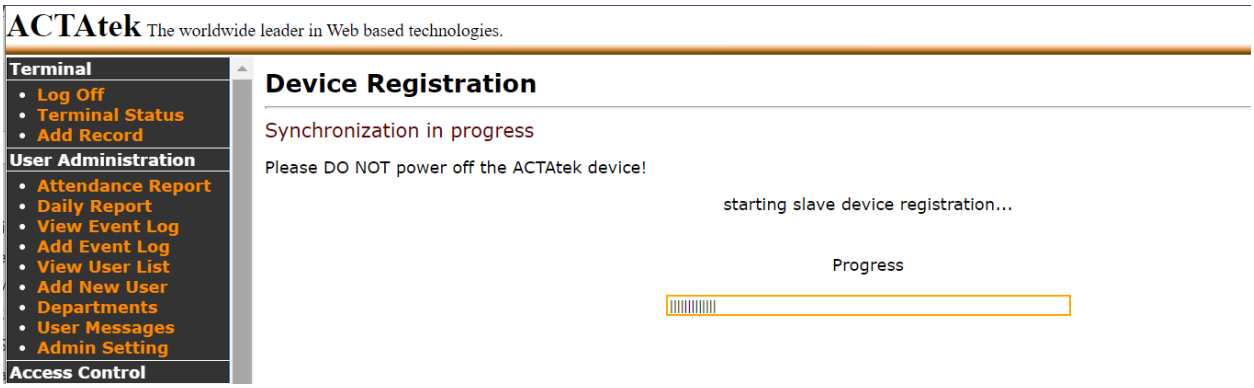


Now Enter your **domain name** on the **domain name** filed and check **set** again

Once done click register button to start the device registration with AMS domain.



Once done click register button to start the device registration with AMS domain.



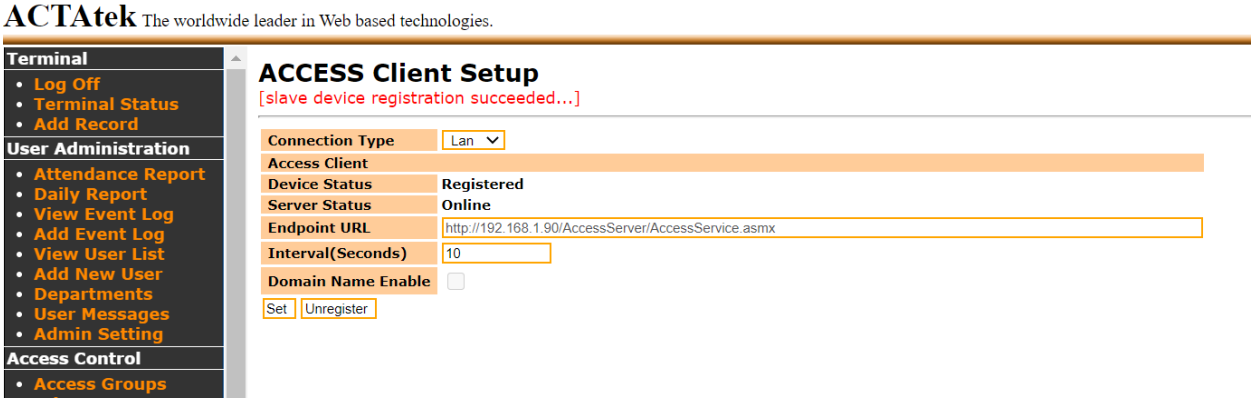
Troubleshooting:

If you are not able to get to the screen with the **Register** button and **Server Status** reports offline, check:

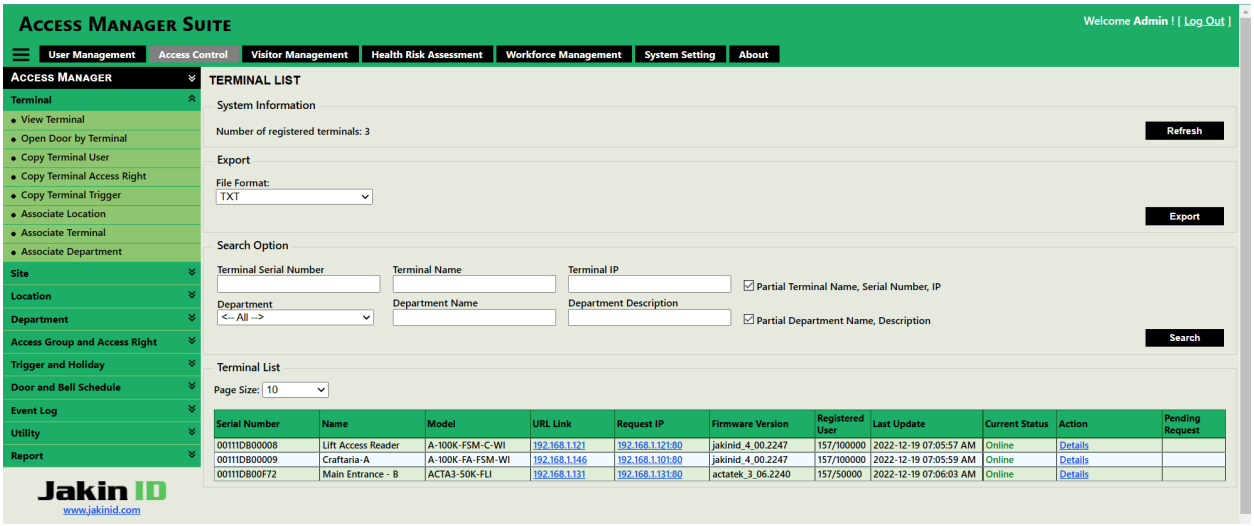
1) Endpoint URL for typing mistakes.
2) The IP address of the AMS server is correct.
3) The firewall settings on the AMS server are set correctly such that port 80 is open.

The ACTATEK terminal that is the first to register to AMS with a clean database will push all its user data from the ACTATEK terminal into the AMS database. All following ACTATEK terminals that will be registering to AMS will have its user data replaced by the downloaded copy from the AMS database during registration.

When the ACTATEK terminal has finished the registration process, a successfully message as indicated below would appear.



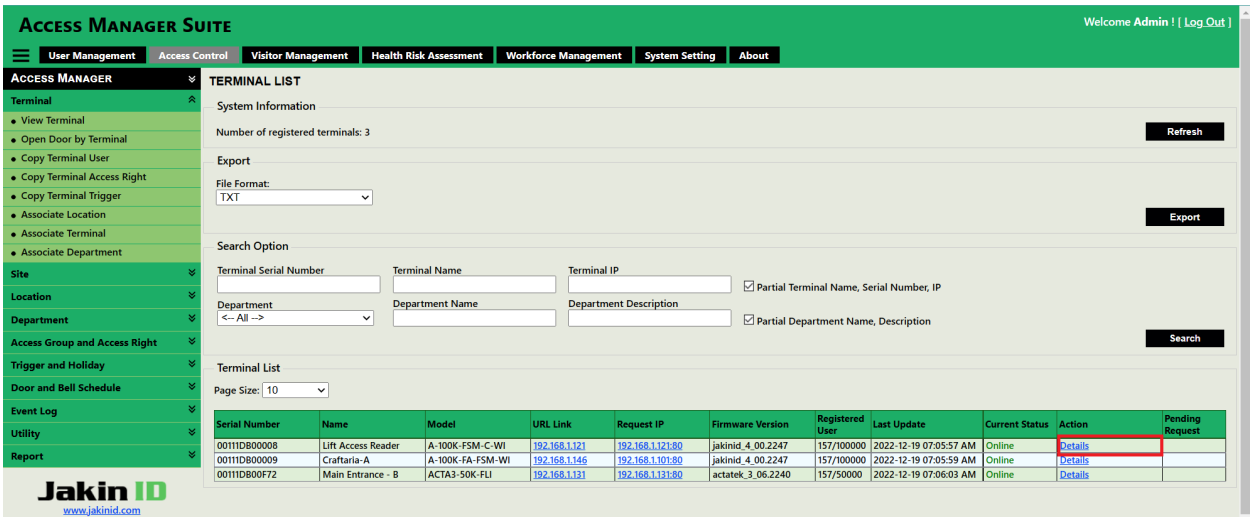
To verify that the ACTATEK terminal is now registered and connected successfully with AMS, you can login to the AMS web interface and press **Terminal List** in the menu. It should now list this registered ACTATEK terminal in the terminal list found in AMS.

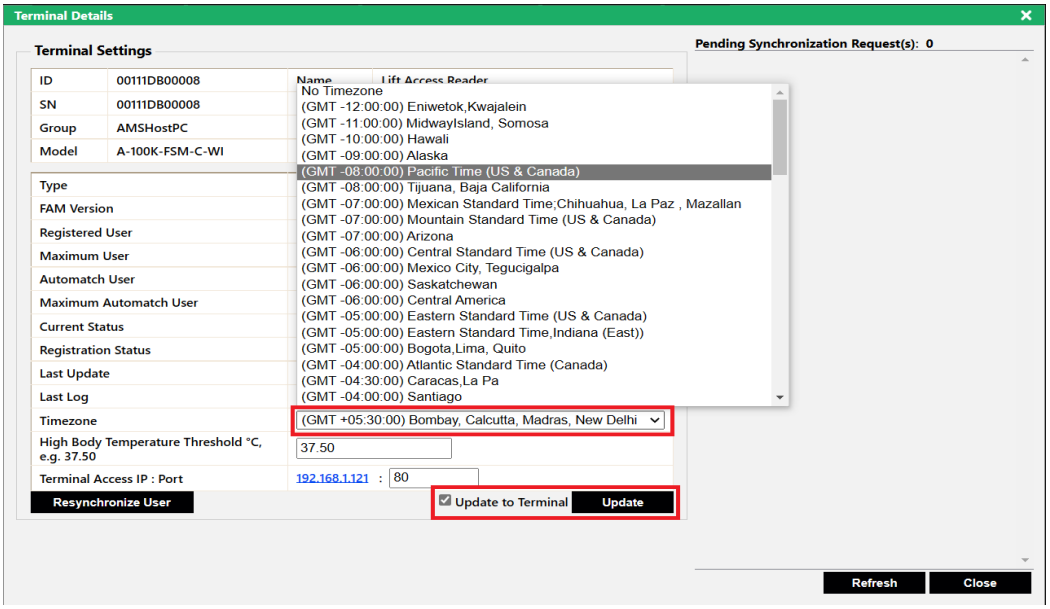

ACCESS MANAGER SUITE
Welcome Admin ! [Log Out]
User Management
Access Control
Visitor Management
Health Risk Assessment
Workforce Management
System Setting
About
ACCESS MANAGER
Terminal
View Terminal
Open Door by Terminal
Copy Terminal User
Copy Terminal Access Right
Copy Terminal Trigger
Associate Location
Associate Terminal
Associate Department
Site
Location
Department
Access Group and Access Right
Trigger and Holiday
Door and Bell Schedule
Event Log
Utility
Report
Jakin ID
www.jakinid.com
TERMINAL LIST
System Information
Number of registered terminals: 3
Refresh
Export
File Format:
TXT
Export
Search Option
Terminal Serial Number
Terminal Name
Terminal IP
Partial Terminal Name, Serial Number, IP
Department
<-- All -->
Department Name
Department Description
Partial Department Name, Description
Search
Terminal List
Page Size: 10
Serial Number
Name
Model
URL Link
Request IP
Firmware Version
Registered User
Last Update
Current Status
Action
Pending Request
00111DB00008
Lift Access Reader
A-100K-FSM-C-WI
192.168.1.121
192.168.1.121:80
jakinid_4_00.2247
157/100000
2022-12-19 07:05:57 AM
Online
Details
00111DB00009
Craftaria-A
A-100K-FA-FSM-WI
192.168.1.146
192.168.1.101:80
jakinid_4_00.2247
157/100000
2022-12-19 07:05:59 AM
Online
Details
00111DB00F72
Main Entrance - B
ACTA3-50K-FLI
192.168.1.131
192.168.1.131:80
actatek_3_06.2240
157/50000
2022-12-19 07:06:03 AM
Online
Details

3.5 Assigning Time Zones to Acta Series of Products

For AMS deployment with ACTA Series of Products located in different time zones, it is important to assign the correct time zone for each ACTATEK to ensure event log data can be collected and displayed at the correct times.

To assign a time zone to an ACTATEK, navigate to **Terminals** and then **View Terminal Lists.** Under the **Action** column, press **Details** which corresponds to that specific ACTATEK. In the **Terminal Time Zone Setting**, select from the dropdown menu of time zones and press the **Update** button to save changes.



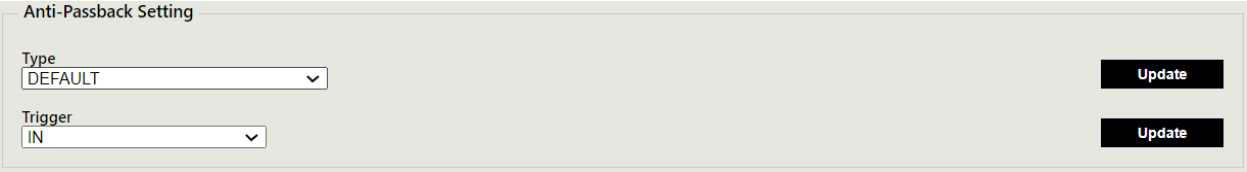


Chapter 4: Access Manager Suite Functionalities

4.1 Auto User Synchronization

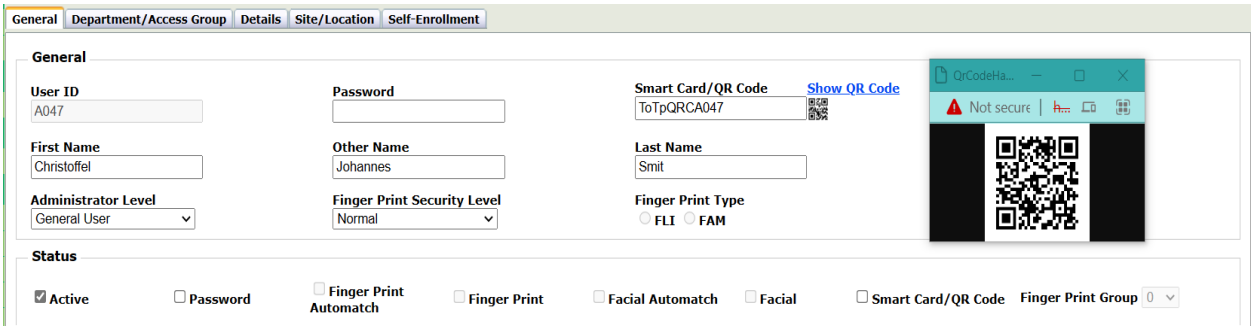
By default, auto user synchronization is set on enabled. All user changes made on the ACTATEK terminals or in Access Manager will propagate updates to all connected ACTATEK terminals to ensure a synchronized state. If you are not sure, leave **Auto User Synchronization** on enabled for the best performance. This feature can be disabled by going into **Control Panel** and then **System Configuration** and selecting **Disabled**. By pressing the **Update** button, the changes will then be saved.

Once the AMS Auto Synchronization has disabled, The AMS can synchronize the newly adding users to a specific or department associated terminals.



4.2 Add Users

To add a new user, go into **Access Manager** tab, then **User Admin** and **Add Users**. The **User ID** and **Password** fields must only contain any of these characters found in "0123456789ABC". The **User ID** must also have a length of 3 or up to 16 characters long. For Facial, Fingerprint and smart card enrollments, this will have to be accomplished on any of the registered ACTA terminals by providing the associated **User ID** to the Face, Fingerprint or smart card enrollment process.



In the status field, ensure **Active** is checked to enable this new user in the system. You may also wish to check **Password** if this user can enter through PIN method otherwise leave it unchecked if you do not wish to let this user authenticate through PIN method.

The admin can also wish to **create a QR code access** method by entering any character's in to **Smart Card/ QR Code** field. Once the user has added, AMS will auto generate a QR code for newly added user. The user QR code now can be view and download by selecting **''Show QR Code''** Additional settings which you may choose to set for any new user are: department & groups, user information, user expiry date, and user notification/messages. All these user settings can be modified in **View/Edit User** if you choose not to set any now.

4.3 View/Edit User

This feature allows you to make any changes **except User ID** to an existing user in the system. You can choose to edit, view, or delete an existing user over Access Manager. To delete multiple users, check the boxes that are associated to the users that you would like to delete and press the **Remove** button.

To narrow down a specific user, the search options allows you to search by User ID, First Name, Last Name, Department, and or Group. To view the search result, press the **Search** button.

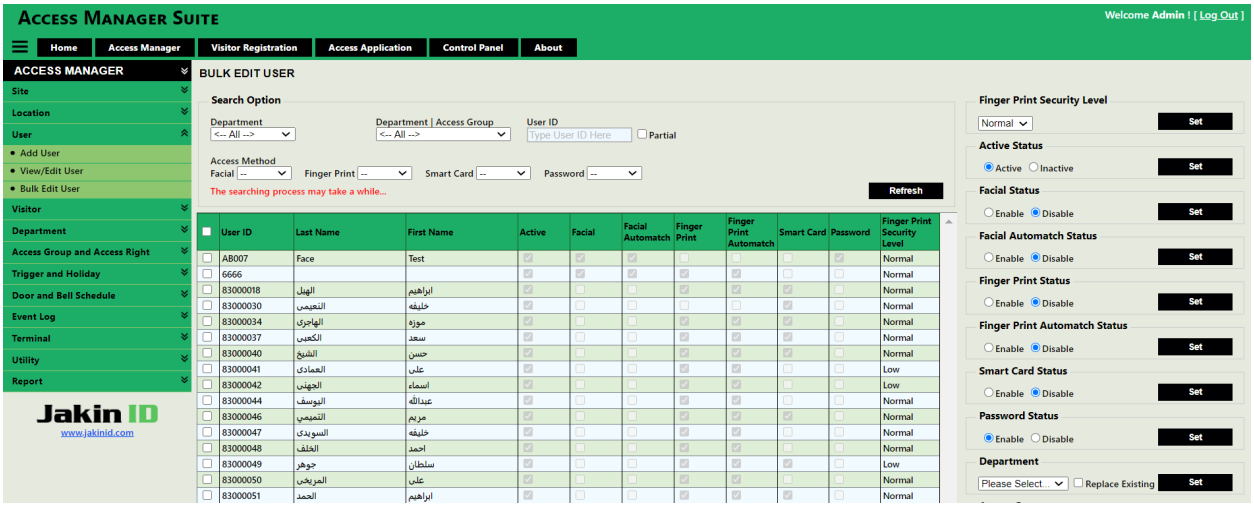
Access Manager > User Admin > View/Edit User

	ID	User ID	Last Name	First Name	Active	Finger Print	Automatch	Facial	Facial Automatch	Password	Smart Card	Finger Print Group	Action
☐	4726	AB007	Face	Test	☑	☐	☐	☑	☑	☑	☐	0	Edit Delete
☐	4731	6666			☑	☑	☑	☑	☑	☐	☐	0	Edit Delete
☐	4703	3006	MATTHEW	ANDREW	☑	☑	☑	☐	☐	☐	☑	0	Edit Delete
☐	4702	3005	NATALIE	MIA	☑	☑	☑	☐	☐	☑	☐	0	Edit Delete
☐	4709	4002	JAMES	MICHAEL	☑	☑	☑	☐	☐	☐	☐	0	Edit Delete
☐	4708	4001	ANTHONY	ISAAC	☑	☑	☑	☐	☐	☐	☐	0	Edit Delete
☐	4707	3010	CAMILA	SOFIA	☑	☑	☑	☐	☐	☐	☐	0	Edit Delete
☐	4701	3004	SOPHIA	EMMA	☑	☑	☑	☐	☐	☐	☐	0	Edit Delete
☐	4692	080000277			☑	☐	☐	☐	☐	☐	☐	0	Edit Delete
☐	4691	40000597	محمد النعيمي	فاطمه	☑	☐	☐	☐	☐	☐	☑	0	Edit Delete
☐	4698	3001	JESSICA	EMILY	☑	☑	☑	☐	☐	☑	☐	0	Edit Delete
☐	4700	3003	ETHAN	JOSEPH	☑	☑	☑	☐	☐	☐	☐	0	Edit Delete
☐	4699	3002	MICHAEL	DAVID	☑	☑	☑	☐	☐	☐	☐	0	Edit Delete
☐	4710	4003	OLIVER	DAVID	☑	☑	☑	☐	☐	☐	☐	0	Edit Delete
☐	4727	A0034	Ava	Emma	☑	☐	☐	☐	☐	☑	☐	0	Edit Delete

4.4 Bulk Edit Users

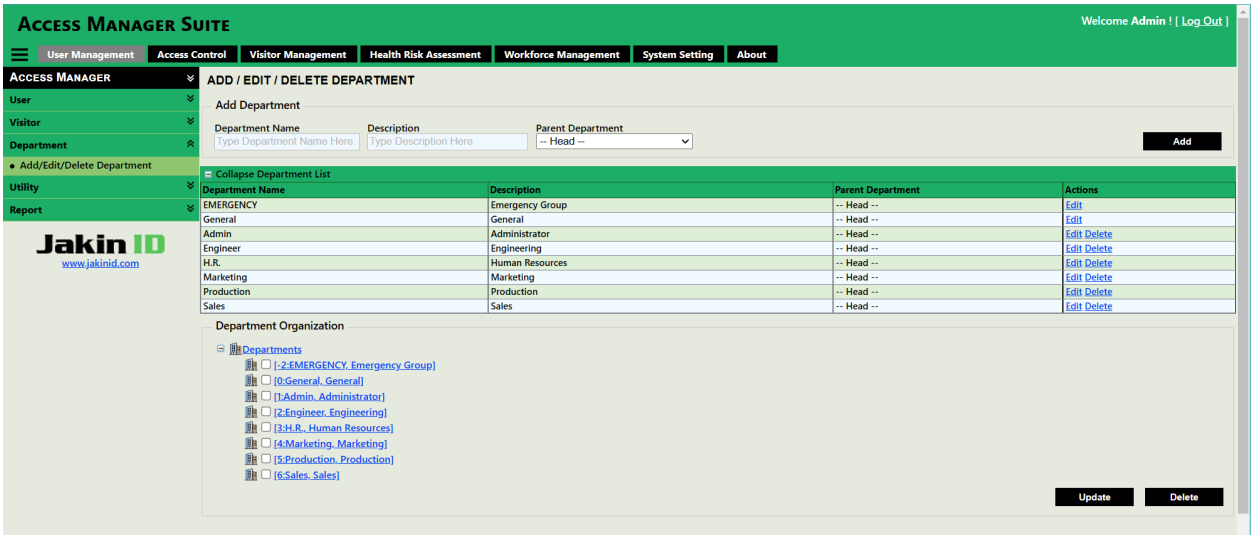
Bulk edit users allow the administrator to make changes to multiple users in Access Manager at the same time. Press the **Refresh** button to reveal a list of users in Access Manager and check the boxes associated to the users that you want to make changes to. Changes include enabling or disabling user settings for: user active status, facial, fingerprint, automatch, password, and smart card. Additionally, adjustable user settings apply to facial, fingerprint quality, departments, and groups. For each change,

press the **Set** button to save the changes to the queue. When all the changes are made, press the **Commit** button to permanently make the changes to the selected users. The registered ACTATEK terminals will now enter **System Maintenance Mode** while these changes are being made.



4.5 Add/Edit/Delete Departments

Departments are used for associating users and ACTAtek devices into main groups. This feature allows the administrator to add, edit, or delete departments in Access Manager. Departments also help categorize users and will be the foundation for setting up **Access Groups** and **Access Rights**. To associate users to departments, you will edit a selected user in **View/Edit User** and in the **Department** tab, check the listed departments relevant to this user and press the **Update** button to save the changes.

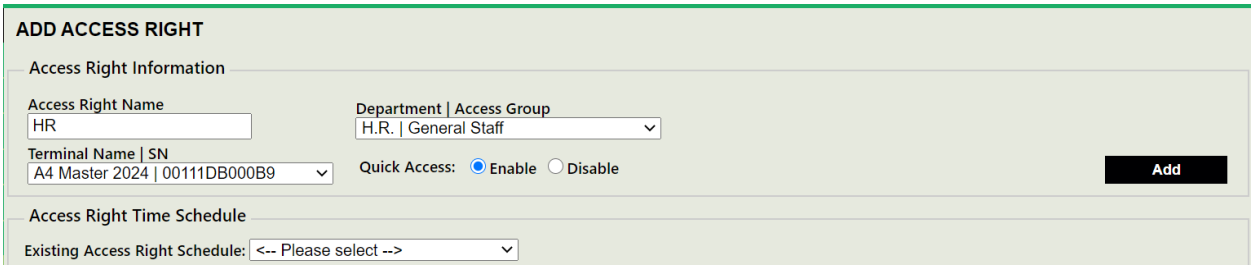


4.6 Add/Edit/Delete Access Group

The default settings of Access Manager already have predefined access groups. The administrator may choose to customize or remove irrelevant access groups and departments to personalize their setup and environment. Setting up an access group is the next step in creating an access right. Access groups are used to distinguish different levels of access in a department.

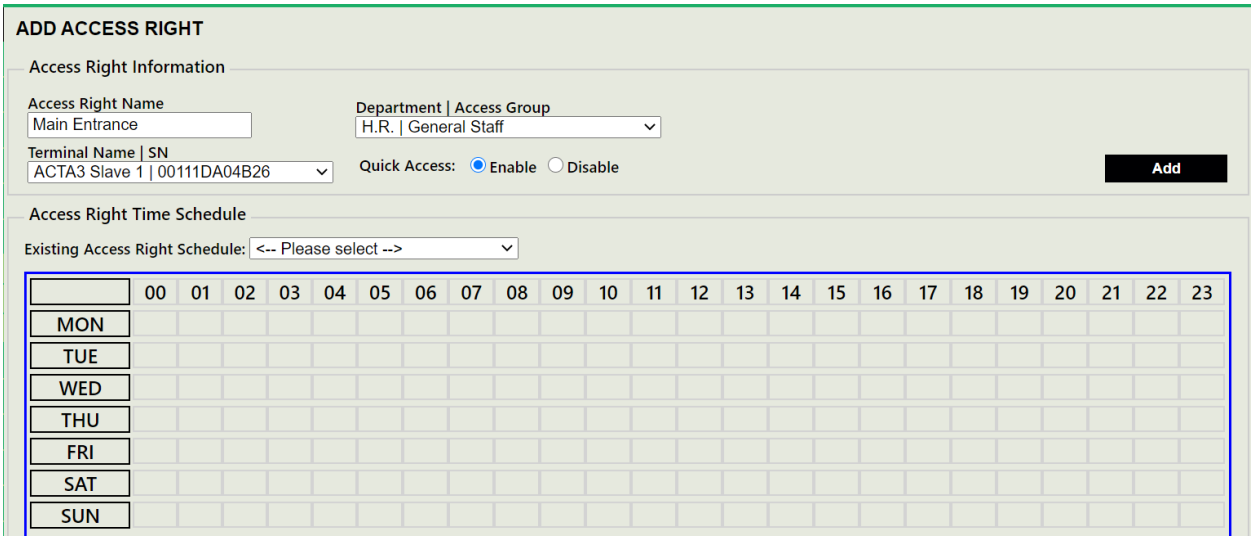
4.7 Add Access Right

An access right is an access control policy used for binding an ACTATEK terminal to an access schedule with the associated department and access group. This will enforce users in that associated department and access group to the access schedule as defined by the administrator. The advantage of using access rights is that it will provide the access control rules to ACTATEK terminals. For example, using access rights can limit certain user groups to certain ACTATEK terminals. Additionally, it can restrict the time and days when a user can have access.

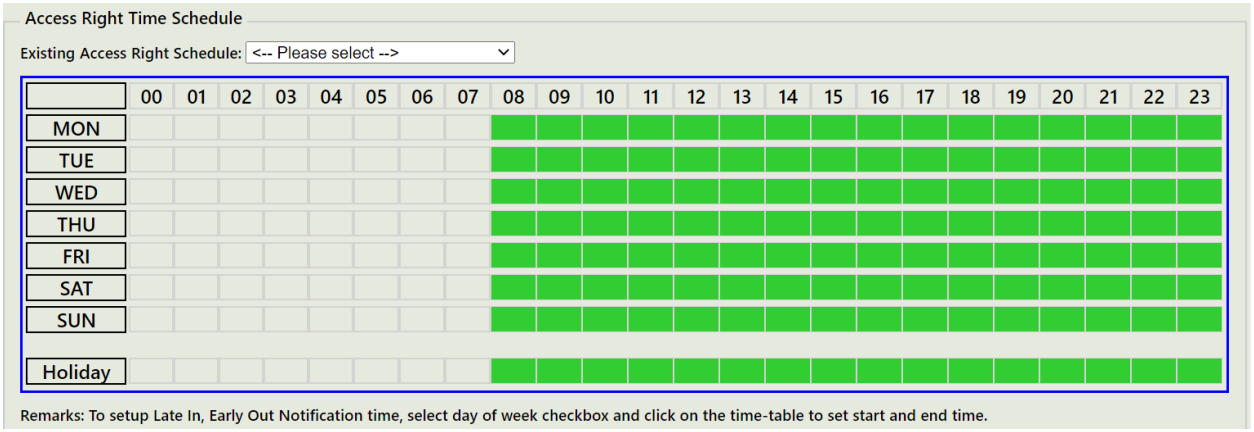


To setup an access right, provide an **Access Right Name** followed by selecting a **Dept/Group Name** from the list which this access right will affect. Users in this department and access group will have this policy applied to them. Next, select an ACTATEK terminal from the **Terminal Name / SN** list to apply this access right to and set **Quick Access** to enable.

In the **Day & Time** field, the administrator defines the restrictions and the rules in terms of a schedule. By default, the schedule has all time and days of the week disabled which can be referenced below by the light grey dots.



After making setting changes to the **Day & Time** field, press the **Modify Time** button to review the changes made. The filled black dots are set for enabled while the light grey dots are set for disabled.



In the example above, the affected department and access group can only access the ACTATEK terminal on every Tuesday from 07:00 to 17:59.

Press the **Add** button to add this access right to Access Manager. Notice that this access right only affects a single ACTATEK terminal therefore to have this access rights affect all your ACTATEK terminals, you will have to add a new access right for each individually ACTATEK terminal. Use the existing access right schedule drop down list to load any already defined access schedules.

If an access right does not exist in Access Manager for a particular department and access group, this means that the users belonging to this group will not have access to any of the ACTATEK terminals and they will receive an access denied message upon authentication.

To associate users to this department and access group, you will edit a selected user in **View/Edit User** and in the **Group** tab, check the listed department and group relevant to this user and uncheck all that

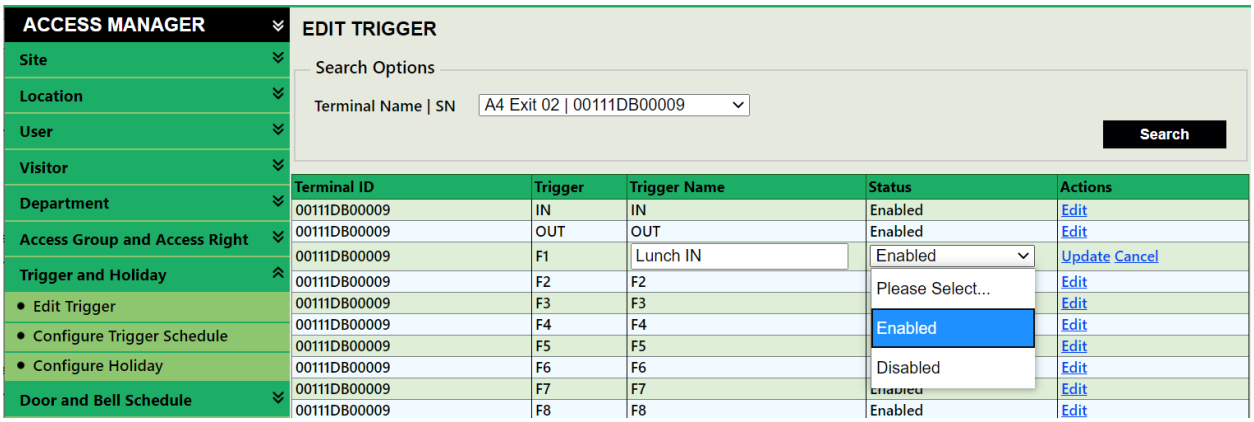
are no longer relevant. Press the **Update** button to save the changes. A user can belong to more than one access groups.

4.8 View/Edit Access Right

The administrator can view/edit/delete any defined access rights in Access Manager by using this functionality. By default, all registered ACTATEK terminals will create an access right with the department **General** and group **General Staff**. This means all newly registered users will have access to all the ACTATEK terminals in the system. The administrator may want to remove these default access rights so that the newly registered users must be placed in their correct department and group before allowing them access on the ACTATEK terminals.

4.9 Edit Triggers

Make changes to the trigger name/value for an individual ACTATEK terminal by clicking **Edit** for the corresponding trigger and terminal ID you wish to edit. The administrator can choose to disable all unused triggers by clicking on the edit action and selecting disabled and then followed by clicking on **Update**.



Make all trigger changes to an individual ACTATEK terminal and you can use the **Copy Trigger** function found in the **Terminal** menu to copy triggers from this ACTATEK terminal to all the remainder ACTATEK terminals if they share the same triggers to reduce redundant work.

4.10 Trigger Schedule Setup

Based on a schedule, the administrator can choose enable or disable triggers. To setup this functionality, select an ACTATEK terminal from the drop down list. In the Day & Time field, select a trigger ID, time frame, date, and specify either enabled or disabled. To save this schedule, press **Modified Time** button

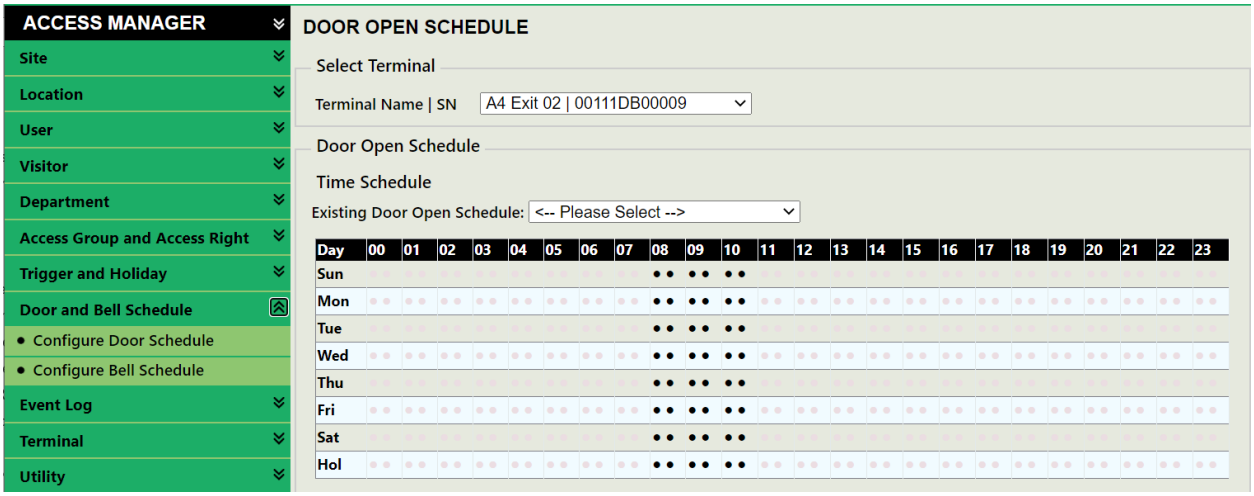
and the changes will now reflect on the trigger schedule field. When ready, press the **Setup** button to make the final changes. By default, the trigger schedule settings are on disabled and affect no days of the week unless checked.

4.11 Holiday Setup

The administrator can specify days that are considered as holidays. Simply select the date from the calendar and type in a descriptive description. Press the **Add** button to save it in Access Manger. The administrator can remove any existing holidays that were added previously. The use of holidays is for grouping days that can be affected by a schedule. For example, access rights are affected by a schedule therefore an administrator can define an access right to deny all entries for specific access groups on holidays since the law may forbid the staff from working and entering the facility.

4.12 Door Open Schedule

The administrator may set an open-door policy to enforce any doors controlled by the ACTATEK terminals to be opened based on a set scheduled and closed otherwise. By default, the schedule settings are on disabled and affect no days of the week unless checked. In the **Day & Time** field, set enabled with a selected time frame and check all days that will be affected by this change. By pressing **Modify Time**, this will update the **Time Schedule** to reflect the future modifications. Notice that the black filled dots represent enabled and the light grey dots represent disabled. The example below indicates the door will remain open on every Monday from 00:00 to 23:59.



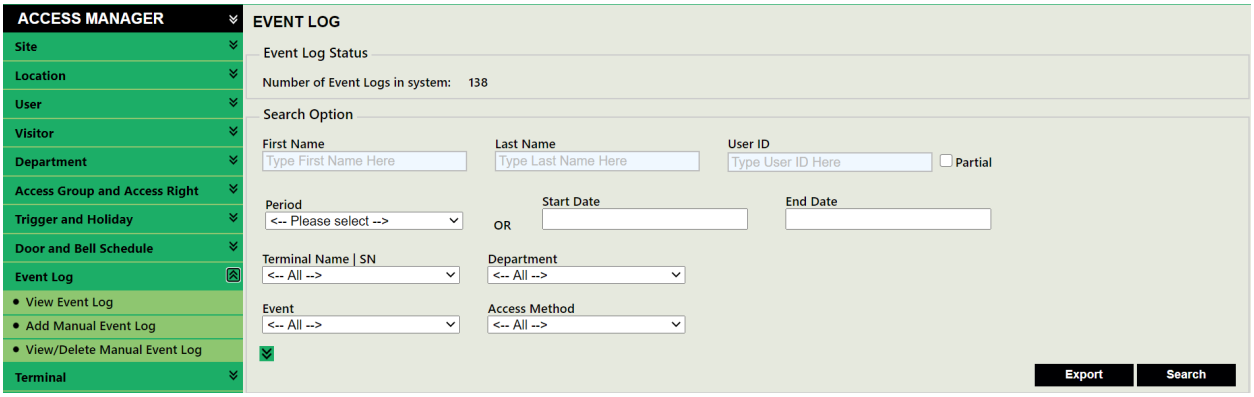
Ensure to select an ACTATEK terminal in the drop-down list to affix this schedule to so the affected ACTATEK terminal will know to leave its door open. Press the **Setup** button to finalize all the changes to the ACTATEK terminal. For all remainder ACTATEK terminals, you may choose to use an existing open-door schedule that has been applied to another ACTATEK terminal or create another customized open-door schedule if necessary.

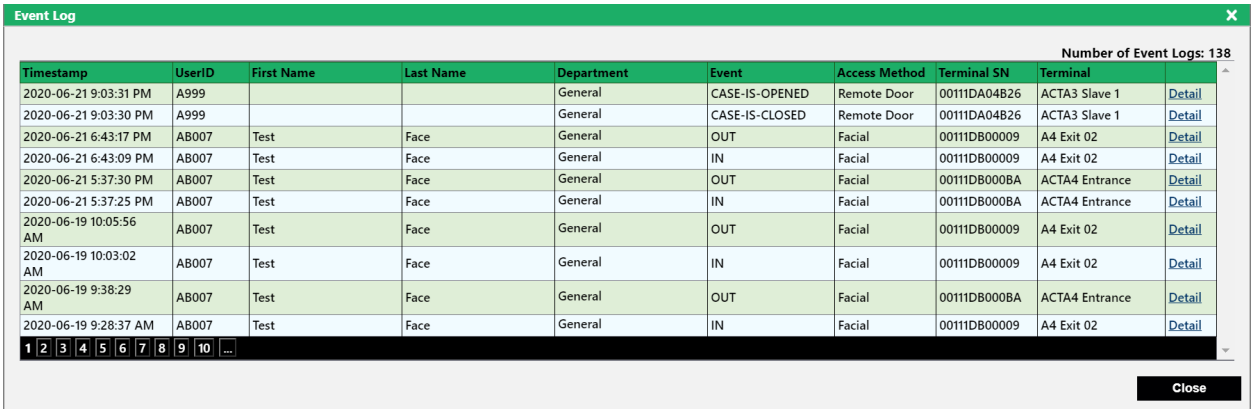
4.13 Bell Schedule

If any of the ACTATEK terminal is connected to a bell ringer, the administrator can set the bell to ring based on the programmed bell schedules. By default, there is no bell schedule in Access Manager. To add a new bell schedule, select an ACTATEK terminal from the drop-down list for this schedule to take place and configure the Day & Time fields. Check the days in the week for this schedule to come into effect and press the **Setup** button to save all changes.

4.14 View Event Logs

Administrators can view event logs that have been collected from the ACTATEK terminals in real time. Additionally, the administrator may choose to use the search option to search for specific events and export the results in a CSV file. The **View Event Log Viewer** button shows all event logs collected in real time with the newest at the top of the list. By pressing on the Search button, the results will be displayed as a static page.





4.15 Add Manual Event Logs

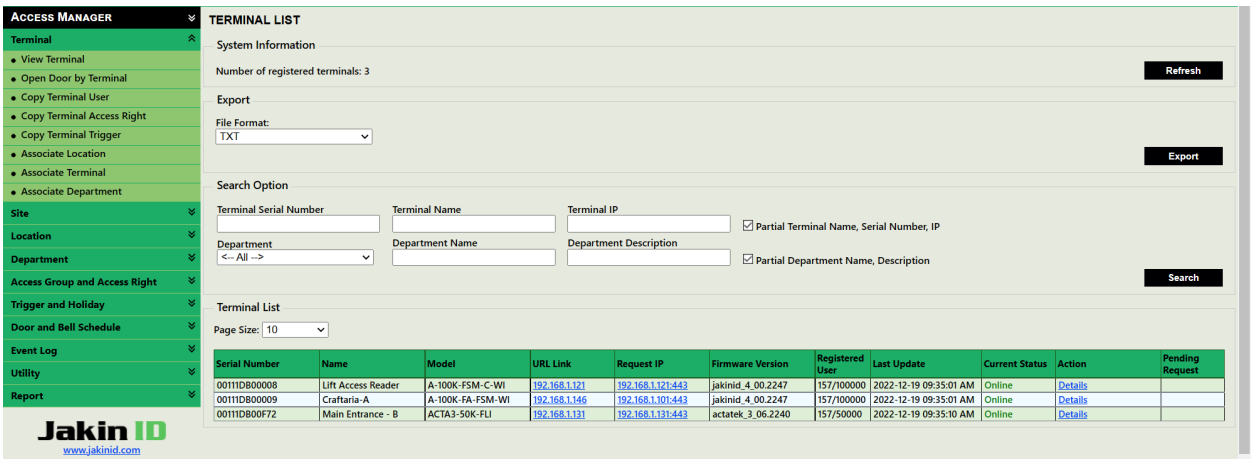
The administrator can add events to Access Manager for corrections in the system. To begin, specify the **User ID** of an existing user. Now select the terminal ID, the appropriate event trigger, the date, the time, and leave a remark as a reason to add this manual event. Press the **Add** button to complete the process and the manual event will be added into Access Manager which can then be searchable in **View Event Logs**.

4.16 View/Delete Manual Event Logs

The administrator can view all event logs that have been added manually into Access Manager and delete any incorrect manual events. Put a check in the boxes to the corresponding events and press the **Remove** button to permanently delete them.

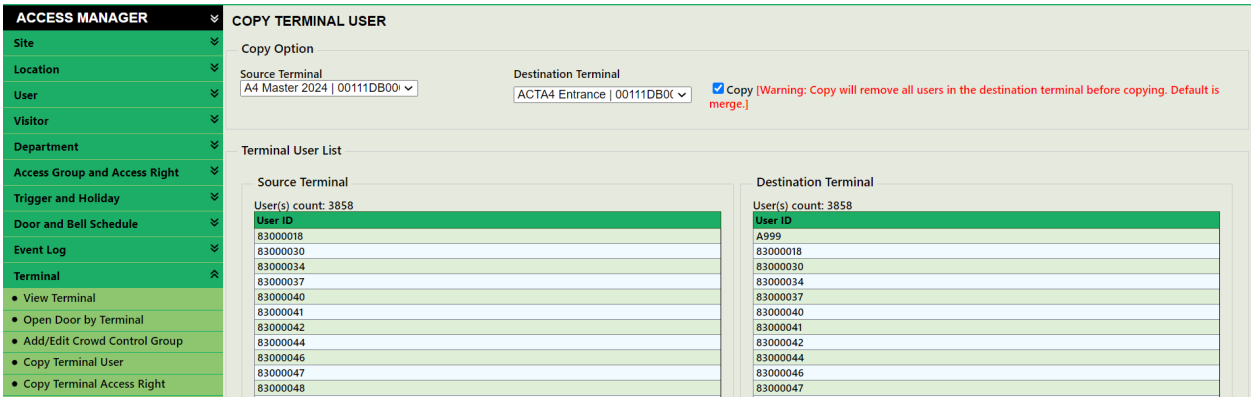
4.17 View Terminal List

View Terminal List shows the status and details of all registered ACTATEK terminals. This page will provide the ACTATEK terminals' serial number, model, IP address, firmware version, user count, device's online/offline status and sync information. Additionally, the administrator may choose to use the search option to search for specific department associated terminals and export the List in a CSV/TXT file.By pressing on the Search button, the results will be displayed as a static page.



4.18 Copy Terminal User

Copy terminal user allows the administrator to copy the user data found in Access Manager or in another ACTATEK terminal as the source to another ACTATEK terminal as the destination. When auto user synchronization is disabled, copy terminal users may be deemed useful.



4.19 Copy Group Access Right

Copy group access right allows the administrator to copy the access rights associated to the source terminal to a destination terminal as selected in the drop down list. In addition, access rights are listed to show which access rights will be copied over to the destination terminal from the source terminal.

4.20 Copy Trigger

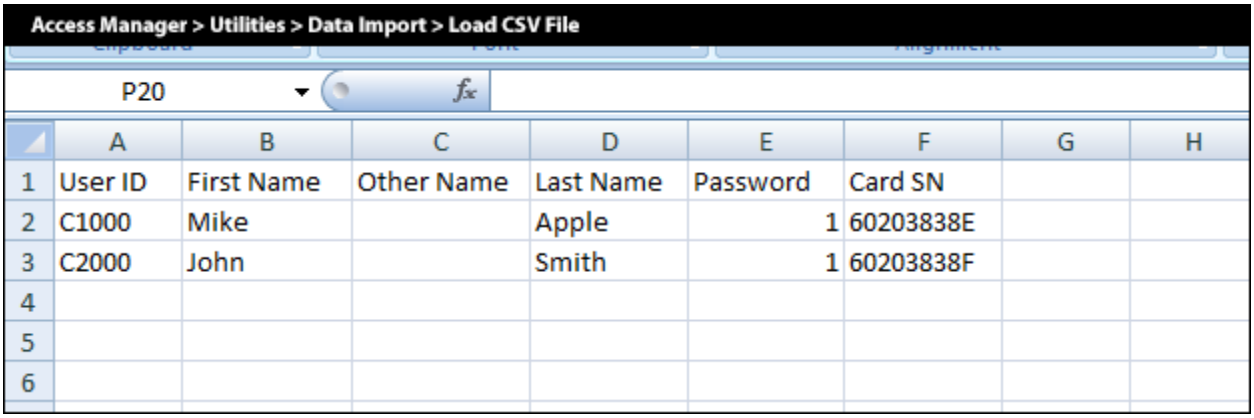
Copy trigger allows the administrator to copy the triggers found in one ACTATEK terminal to another. Select an ACTATEK terminal to use as the source and another ACTATEK terminal as the destination. Press **Copy** button to save the changes.

4.21 Department Association

Department association allows the administrator of AMS to associate specific ACTATEK terminals to a department in AMS. Secondary AMS administrators which are configured with rights to a specific department can now manage all details that belong to their department. To accomplish this, select an ACTATEK terminal from the terminal list and select a department and press the **Associate** button to add this association. Once devices associated with departments they will synchronize each other according to associated group of devices

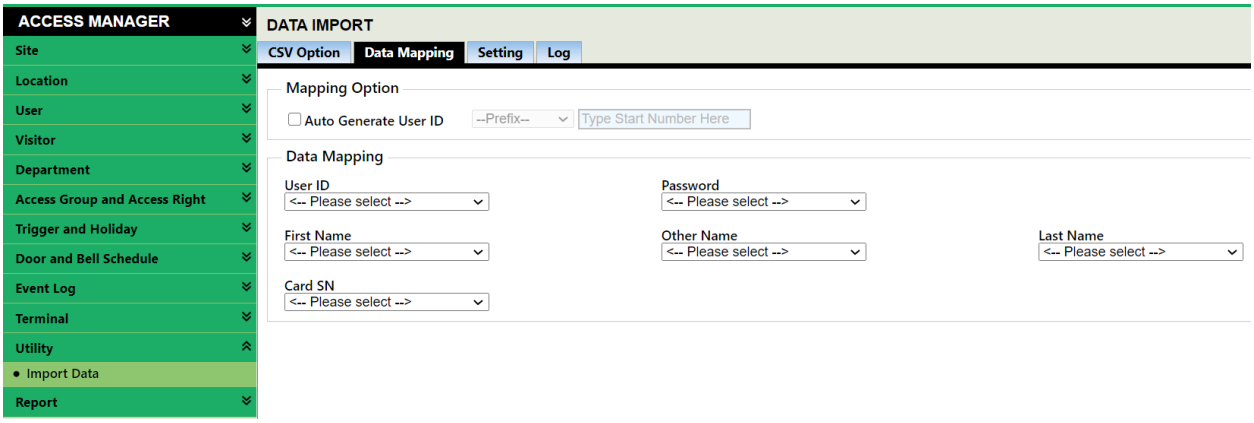
4.22 Data Import

The data import utility allows the administrator to import multiple users into Access Manager using a CSV file. Firstly, set your delimiter and check **First row contains field names**. Next, press the **Browse** button and select the CSV file containing the user's information. Press **Load** button and it will read the CSV file into Access Manager.



	A	B	C	D	E	F	G	H
1	User ID	First Name	Other Name	Last Name	Password	Card SN		
2	C1000	Mike		Apple	1	60203838E		
3	C2000	John		Smith	1	60203838F		
4								
5								
6								

Now press the **Data Mapping** tab to configure all additional settings for the users which will contain user level and privileges, departments, groups, and user status.



Press the **Import** button to import the configured settings and users to Access Manager.

Chapter 5: Access Manager Workforce Management

5.1 Reports

To run reports, the administrator has the options to filter by user ID, department, and time frame. Press the **View Report** button in each report section to generate the report as required. When the report is finished generating, you may choose to export it as an Excel, Word, or PDF file.

Daily In/Out Report:
Shows a report with the first IN event and last OUT event of the day with the total working hours.

Detail Report:
Shows a report with sequential IN and OUTs event of the day with the total working hours.

Absent Report:
Shows a report of users that were absent or present on the day.

Late Report:
Shows a report of users that were late with the restriction where the administrator specifies the finished time.

User Status Report:
Shows a report of users with a status (anyone that has punched in with a trigger) on the day of. The administrator may choose to add filters to only display a specified trigger before pressing the **View Report** button.

Roll Call / Fire Report:
Shows a report of users with a status of "IN" or "OUT" or both as specified by the administrator prior to searching.

Auto In/Out Report:
Shows a report with sequential IN and OUTs event of the day with the total working hours if the AMS has Auto In/Out feature on.

Healthcare Report:
The AMS Healthcare report brings up other events for other users accessed the same terminals within the same time interval together with the infected user. This report brings up potential risky users for further investigation. usually, the Date Time interval will not be more than 3 months.

Enter the user ID of contagious carrier, date time range and extended hours after each event to search for potential infected persons by contacts.

Shift [Auto] Report:
Shows a report with sequential IN and OUTs event of the particular shift with the total working hours.

5.2 Lunch In/Out

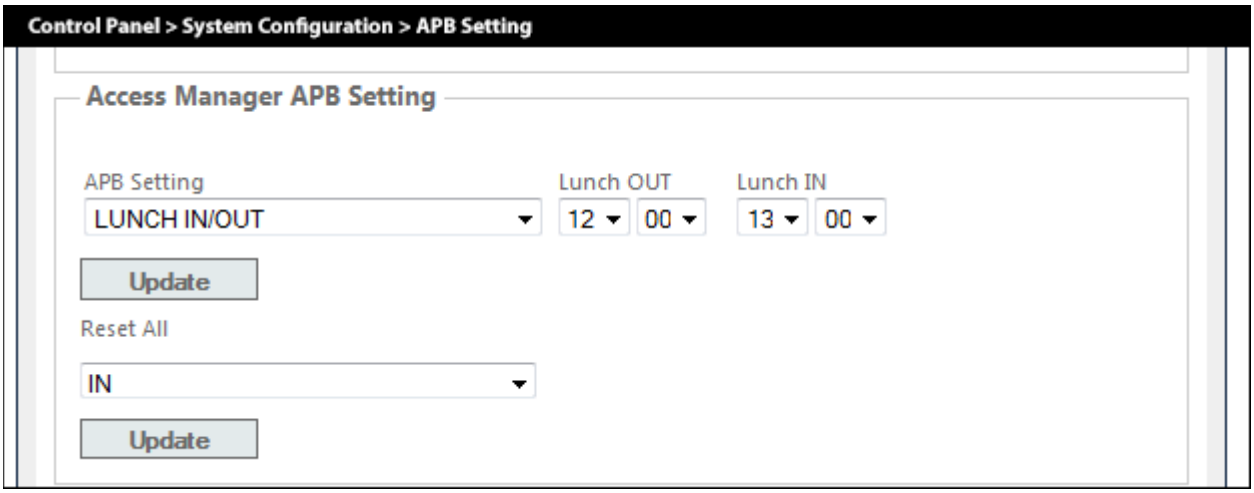
The **Lunch In/Out** feature is used when you would like to enforce a lunch time period so no users can punch in from break until the set time is reached. If they try to punch back in from break before the set time has reached, it will reject them on the ACTATEK terminals.

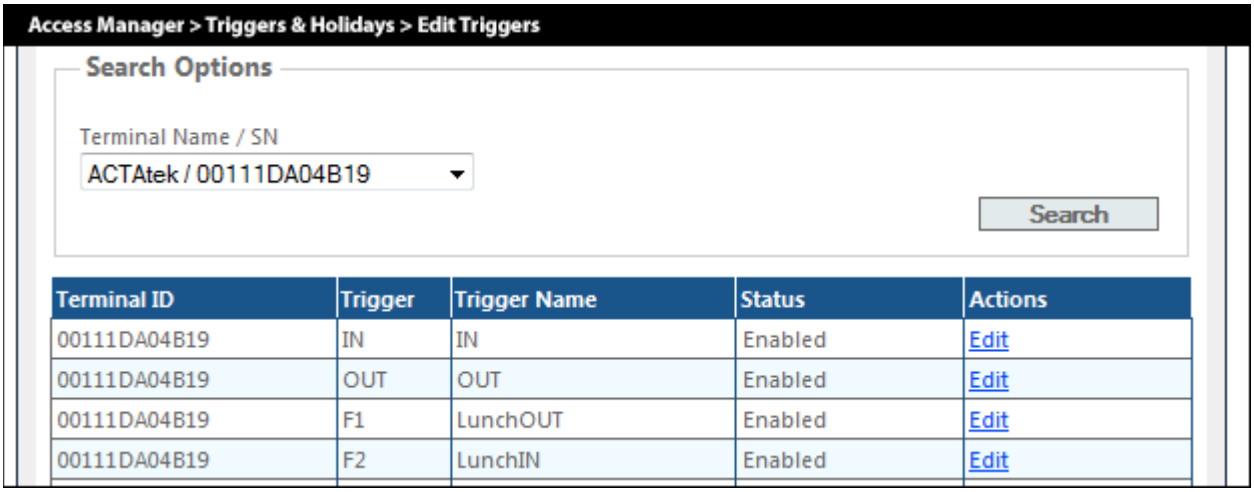
To enable this feature, go into the **Control Panel** tab and then **System Configuration**. Change **APB setting** to **LUNCH IN/OUT** and press **Update** button to save. Set a **LUNCH OUT** time to allow LUNCHOUT trigger to be used when the user goes on their break. Set a **LUNCH IN** time to allow LUNCHIN trigger to be used after their break is over. The ACTATEK terminal will allow LUNCHIN trigger after the time has passed the set LUNCH IN time in AMS.

Next**, Edit Triggers** on an ACTATEK terminal through the AMS web interface.

Set F1 to "LunchOUT" and F2 to "LunchIN" **or** F3 to "LunchOUT" and F4 to "LunchIN."

Use **Copy Trigger** function and copy them over to all remainder ACTATEK terminals.





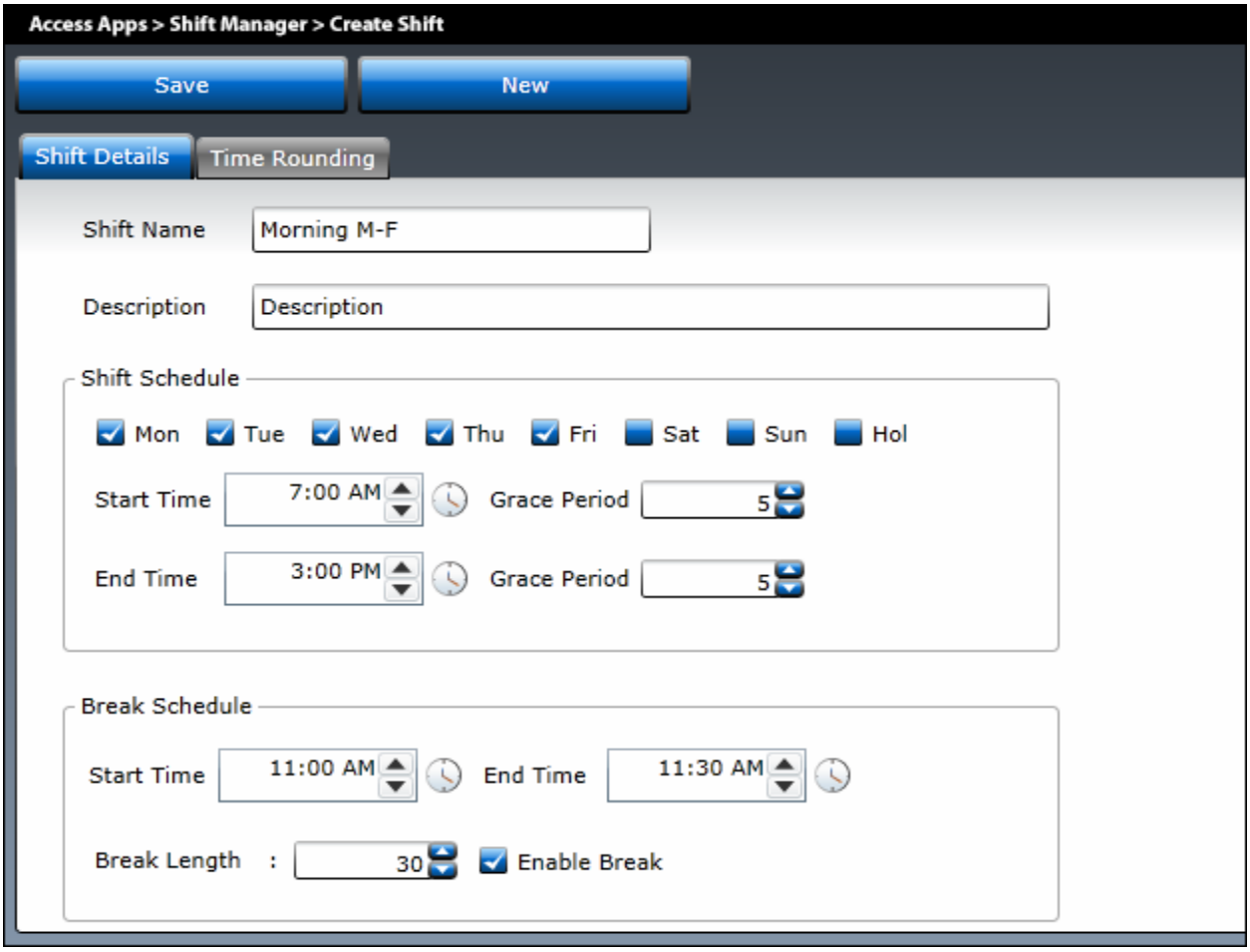
When the user presses the F1 shortcut key on the ACTATEK terminal, it will bring them to the LunchOUT trigger and etc. When the user punches with trigger LunchOUT, it will signify to AMS that the user is on lunch break. When the user punches in with trigger LunchIN, it will be accepted if the punch was made after 13:00 as seen in the images above or else they will be rejected.

5.3 Access Manager Suite Work force Management Shift Manager – Access Application

5.3.1 Create New Shifts

For every unique shift that comprises of different working hours, you will have to create them individually in **Shift Manager**. Provide a **Shift Name** and **Description** such that it can easily be recognized in the later steps. Fill out the necessary information in the **Shift Schedule** section such that it meets your shift's criteria. **Grace Period** is the time specified in minutes that allow employees to punch after or before the **Start/End** time without facing any penalties in their assigned shifts.

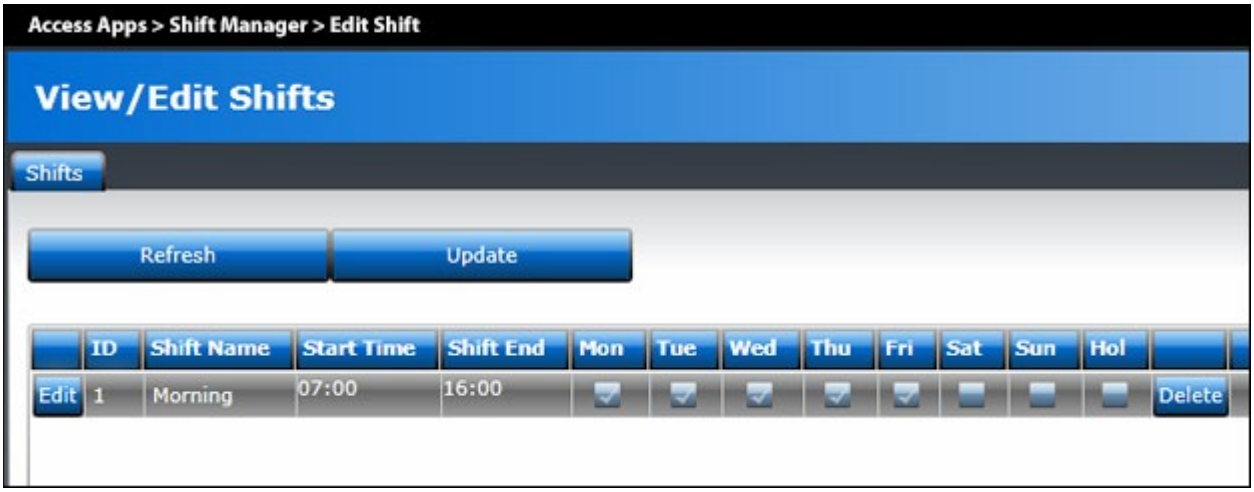
Break Schedule can also be configured on the same page. The **Start Time** is the time specified to allow breaks to occur. The **End Time** is the time specified to no longer allow breaks. Choose a **Break Length** in minutes and check **Enable Break** if breaks are allowed in this shift. Press the **Save** button to finish.



5.3.2 View/Edit Shifts

By pressing on **Edit Shift** in the menu, you will be displayed a list of shifts that is currently present in **Shift Manager**. As an administrator, you can choose to delete or edit an existing shift entry.

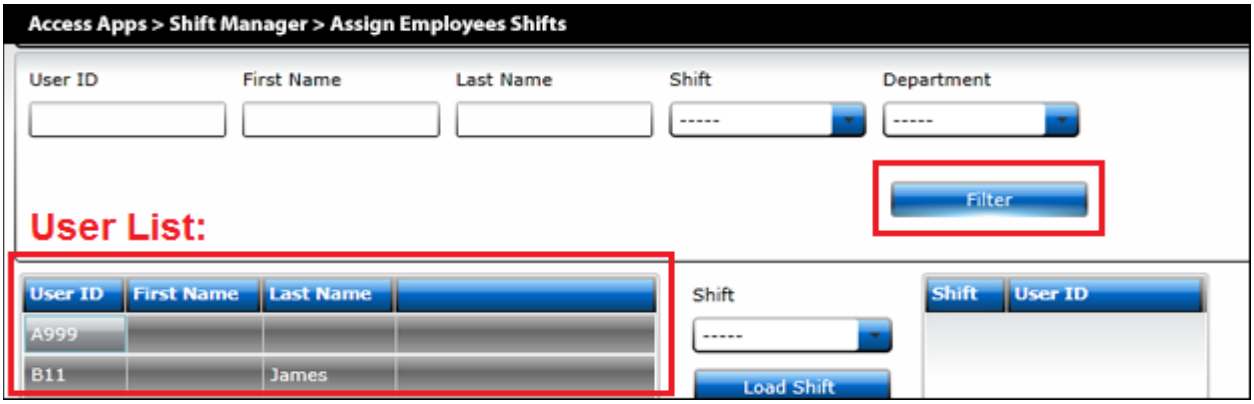
To edit an existing shift, press the **Edit** button that is aligned on the same row as the shift you want to make changes to. Make all changes to the shift and press **OK**. Press the **Update** button to save the changes to **Shift Manager**. If you forget to press the **Update** button, you will lose all changes that you have made.



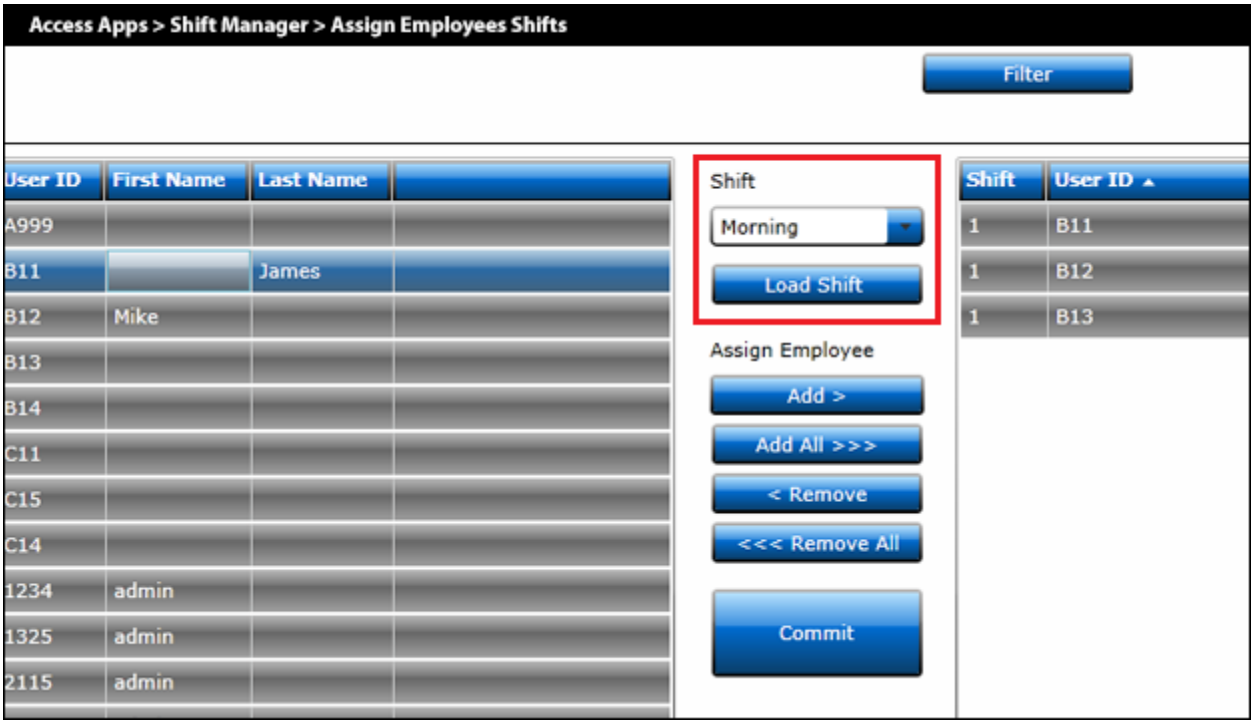
To delete a shift, press the **Delete** button that is aligned on the same row as the shift you wish to delete. Press the **Update** button to save the changes to **Shift Manager**.

5.3.3 Assign Shifts to Employees

On the menu, press **Assign Employee Shifts** and press the **Filter** button to obtain the list of users present in **Access Manager**.



At the top, you can search by using the **Filter** option such that only users that meet the filter requirements either by **User ID, First Name, Last Name, Shift, and/or Department** will be presented in the user list. If no filter options are used and the **Filter** button is pressed, it will list all the users found in Access Manager.



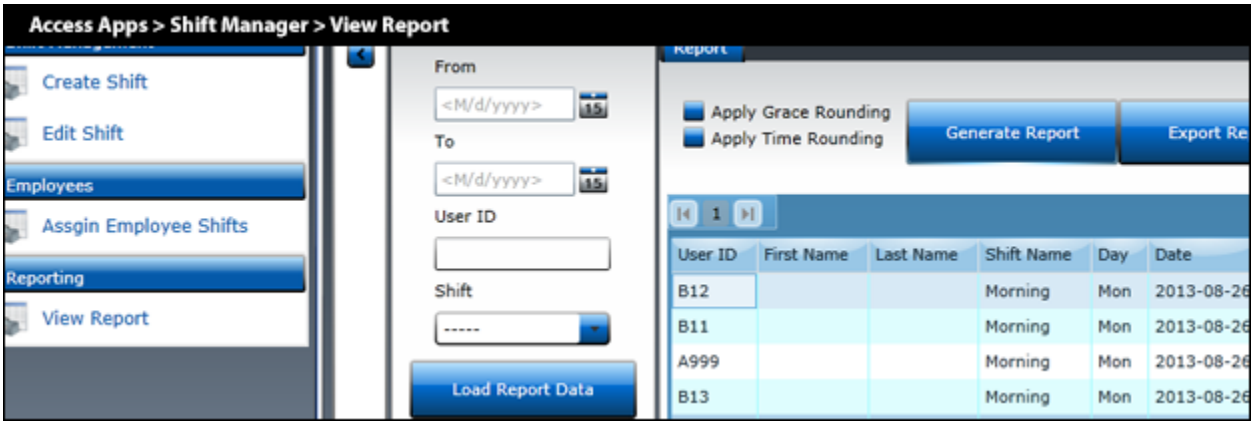
To assign employees or users to shifts created in **Shift Manager**, choose a specific shift in the drop down menu and press the **Load Shift** button. This will associate the selected shift into **Shift Manager** thus now the **Assign Employee** options are available. Select employees from the left user list and press the '**Add >**' button to associate that user to the loaded shift. All existing or newly added users associated to the loaded shift will appear in the user list on the right side. To remove any users from the loaded shift, simply click on that user in the right user list and press the '**< Remove**' button.

To finalize all changes, always press the **Commit** button to save the changes to **Shift Manager**.

5.3.4 Reporting

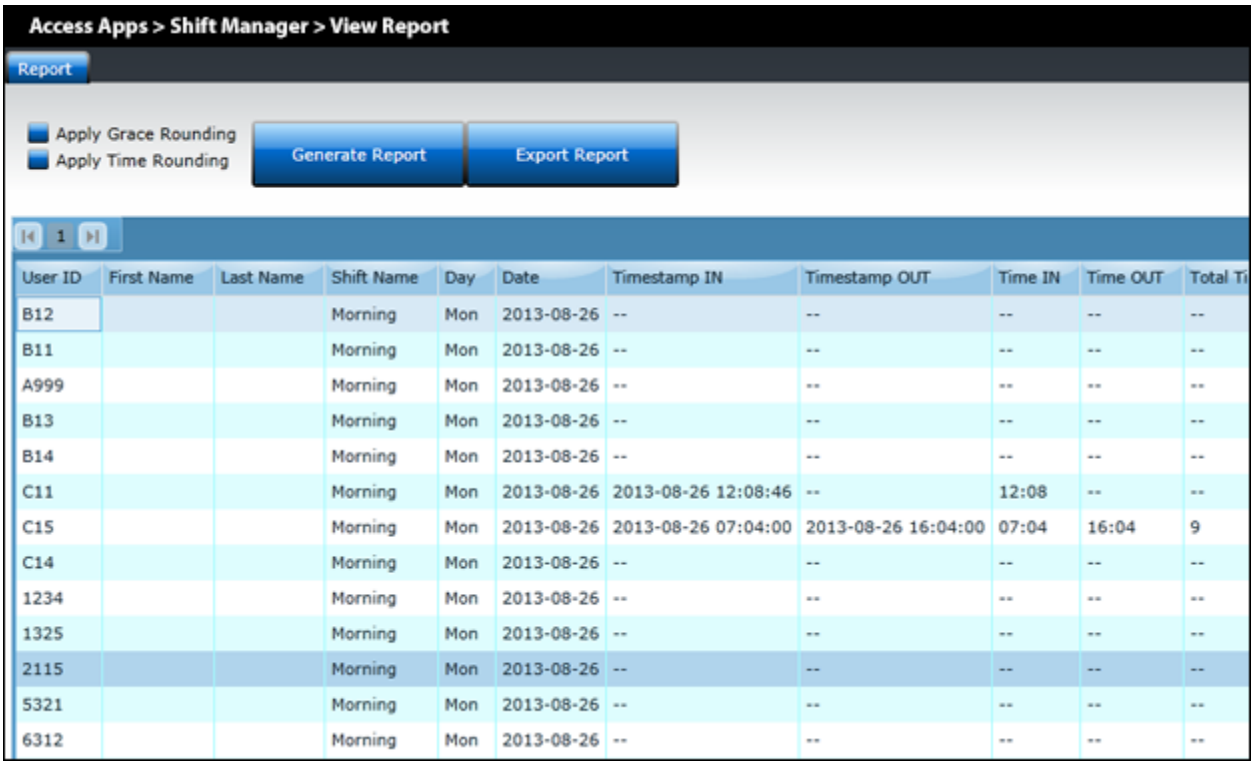
Press the **View Report** button in the menu to generate report in **Shift Manager**. Shift Manager Reporting gives you the flexibility to filter by **User ID** and also by **Time**. By specifying a **User ID** and a **Time**, you can generate a user report for the week, or for 2 weeks, or for the month, and even for the year. By leaving the User ID field out, you can generate reports containing all employees. Daily reports can also be generated for auditing purpose.

For every changes made in the filter criteria, you will need to press **Load Data Report** button such that it will acquire the event data related to the filter from Access Manager.



Then afterwards, press the **Generate Report** button to create the report from the gathered event data. The **Export Report** button allows you to save the generated report on the page to CSV file type which can be opened later with any spreadsheet software.

Grace Rounding and **Time Rounding** options can be checked if they are applicable to the reporting as required. Press **Generate Report** button to update the report such that the rounding options are taken account for.



User ID	First Name	Last Name	Shift Name	Day	Date	Timestamp IN	Timestamp OUT	Time IN	Time OUT	Total Ti
B12			Morning	Mon	2013-08-26	--	--	--	--	--
B11			Morning	Mon	2013-08-26	--	--	--	--	--
A999			Morning	Mon	2013-08-26	--	--	--	--	--
B13			Morning	Mon	2013-08-26	--	--	--	--	--
B14			Morning	Mon	2013-08-26	--	--	--	--	--
C11			Morning	Mon	2013-08-26	2013-08-26 12:08:46	--	12:08	--	--
C15			Morning	Mon	2013-08-26	2013-08-26 07:04:00	2013-08-26 16:04:00	07:04	16:04	9
C14			Morning	Mon	2013-08-26	--	--	--	--	--
1234			Morning	Mon	2013-08-26	--	--	--	--	--
1325			Morning	Mon	2013-08-26	--	--	--	--	--
2115			Morning	Mon	2013-08-26	--	--	--	--	--
5321			Morning	Mon	2013-08-26	--	--	--	--	--
6312			Morning	Mon	2013-08-26	--	--	--	--	--

Chapter 6: Access Manager Suite Workforce Management and Access Control Advance Features

6.1 APB Requirements

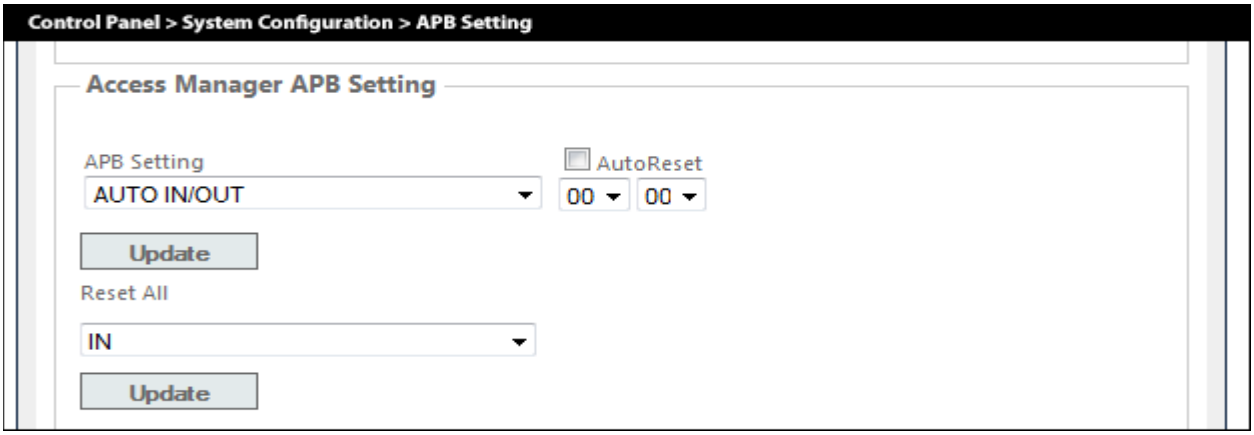
Software & Firmware	Version
Access Manager Suite	1.2.5.5 Build 2021.02.11 or newer
ACTA 3 Firmware	3_06.2030 or newer
ACTA4 Firmware	4_00.2047 or newer

The APB advance features will require the Access Manager Suite Server to reside on the same local area network as the ACTATEK terminals for the best possible outcome. Authentication is determined by the status of the users from the Access Manager Suite Server when working with multiple ACTATEK terminals therefore a low latency network is required.

In any event where the Access Manager Suite Server goes offline or the ACTATEK terminal loses communication with AMS server, the ACTATEK terminal will not be able to request a server-side authentication and instead record an ID UNKNOWN event record while the ACTATEK terminal screen shows ID Reserved AMS Offline during the punch.

6.2 Auto In/Out

The **Auto In/Out** feature allows the ACTATEK terminal to use server-side authentication to automatically determine the IN or OUT status of a user during authentication and records a preceding punch event based on the user's previous event. To enable this feature, go into the **Control Panel** tab and then **System Configuration**. Change **APB setting** from **DEFAULT** to **AUTO IN/OUT** and press **Update** button to save. The ACTATEK terminals will now only show **AUTO** on the LCD screen.

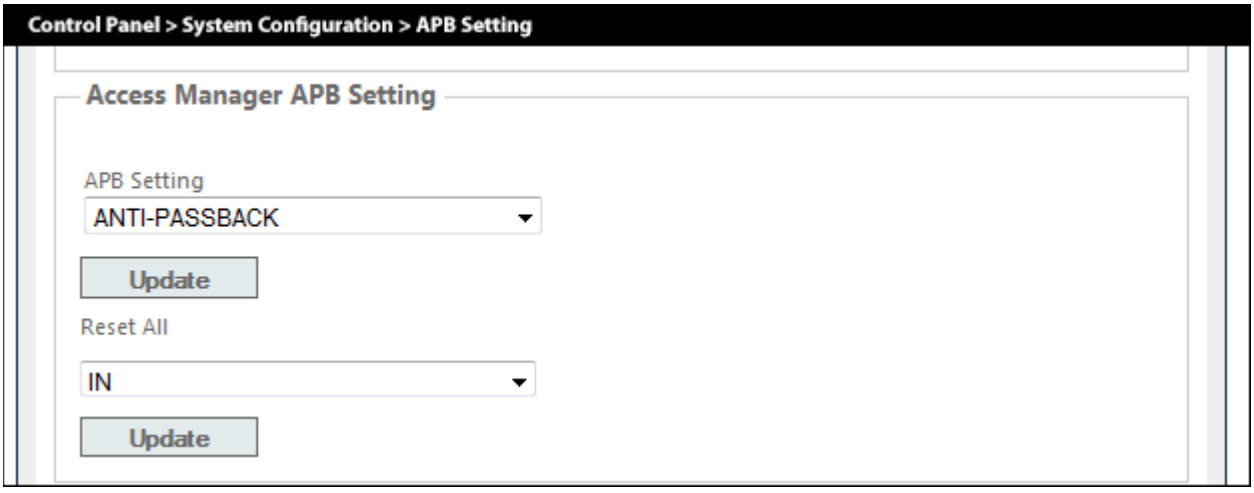


If the Auto Reset box is checked, it will reset the Auto In/Out system such that all users will punch **IN** event after the specified time has been reached on the ACTATEK terminal per day no matter if they have last punched IN or OUT.

Reset All can be used at anytime by pressing the **Update** button. This will reset all users with the status you have selected. For example, if all user status is reset with **IN** status Auto In/Out system will determine the next punch as an **OUT** event for all the users.

6.3 Anti-Passback

The **Anti-Passback** feature is used for controlling area of access such that the user must proceed with **IN** event and then forced to use **OUT** event and not **IN** again. An example scenario where Anti-Passback would be used is to ensure that the user enters through the first door with ACTATEK terminal set on IN and then exit using the second door with ACTATEK terminal set on OUT.

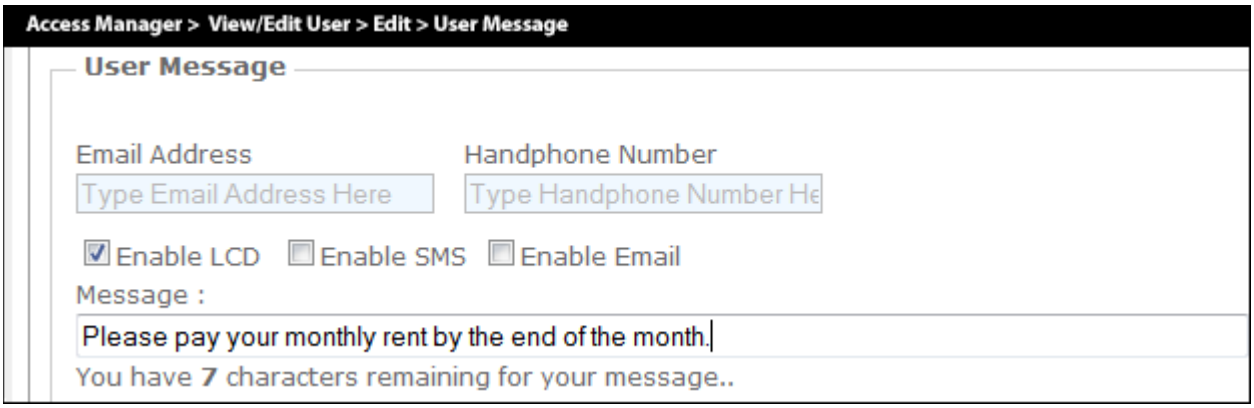


To enable this feature, go into the **Control Panel** tab and then **System Configuration**. Change **APB setting** to **ANTI-PASSBACK** and press **Update** button to save. To use this feature, only triggers **IN** and **OUT** will be affected by Anti-Passback.

Anti-Passback feature when enabled requires active network communicate between ACTATEK terminals and AMS server as authentication requests is validated by the AMS server. In any event where the AMS server goes offline or the ACTATEK terminal loses communication with the AMS server, the ACTATEK terminal will not be able to request a server side anti-passback validation and instead record an **ID UNKNOWN** event while the LCD screen shows **ID Reserved AMS Offline** during the punch. User status remains unchanged where there occurred an incommunicable anti-passback authentication at an ACTATEK terminal.

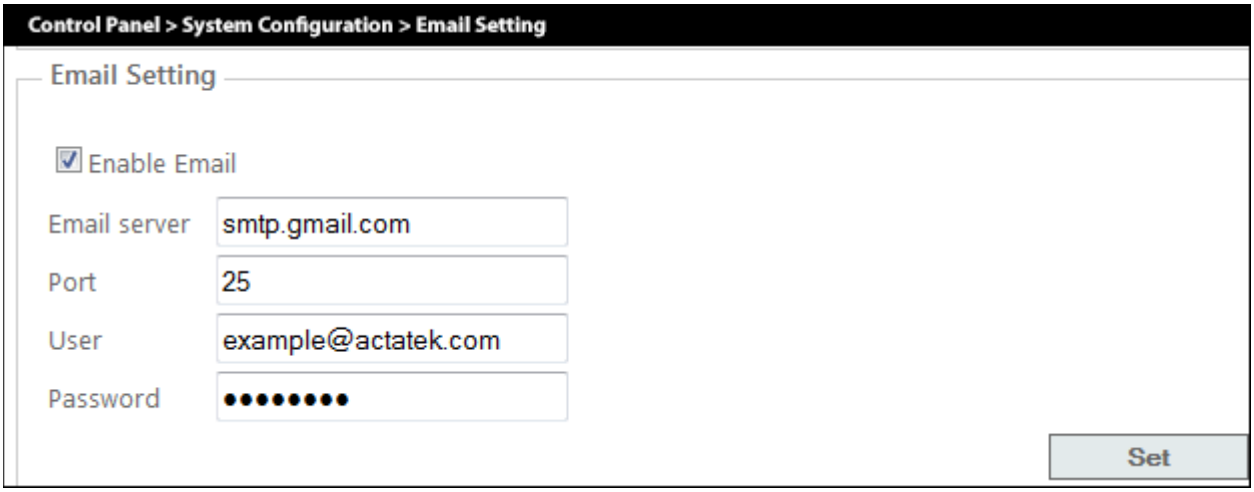
6.4 User Message

To leave a message for a user that can be viewed on the LCD screen of an ACTATEK upon a successful authentication, go to **View/Edit User** and select the user by pressing **Edit** in the **Action** column. Navigate to the **User Message** field and check **Enable LCD** followed by typing the message in the **Message** field and then pressing the **Update** button to submit the user changes. To remove an active user message, uncheck **Enable LCD** for the user.



6.5 Send Email

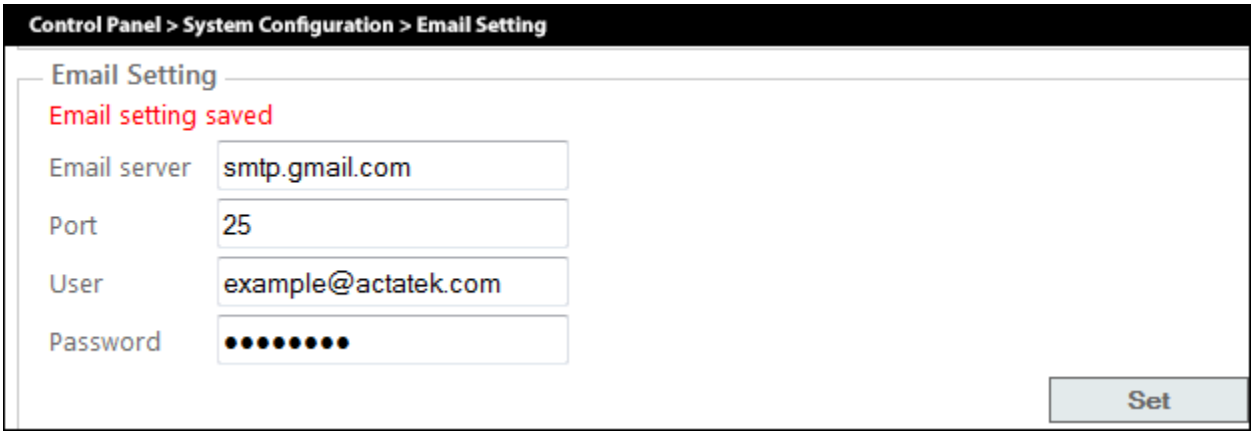
To configure AMS to send email notifications to users, go to **Control Panel** and then **System Configuration.** Navigate to the **Email Setting** and provide SMTP credentials into email server, port, user, and password fields. Check the **Enable Email** and press **Set** to save email settings.



It is recommended to start with a Gmail account with the below settings:

Example Settings	
Email Server	smtp.gmail.com
Port	25
User	*GMail username*
Password	*GMail password*

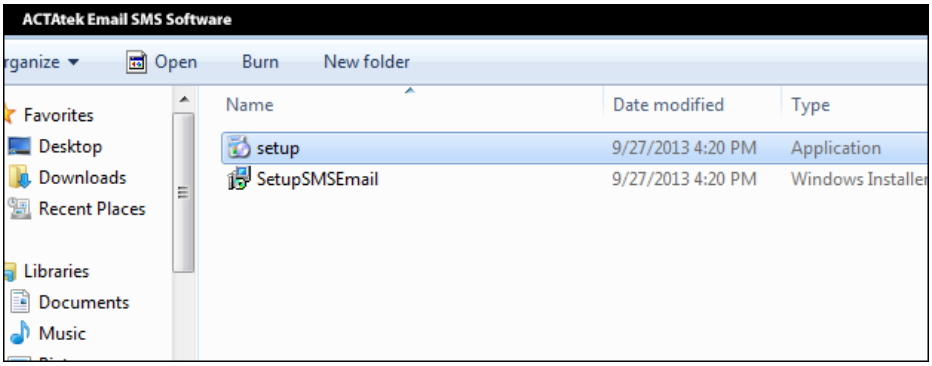
If you do not have a Gmail account, you can create one. The Gmail account that is supplied to AMS will be the email address that will send out emails to the users.



Email setting saved message will appear when all the settings are set correctly with SMTP server communication is established. If error message **Error Logging In** is present, this means either the email setting has problems or your Internet Service Provider may have blocked SMTP port. Please contact your Internet Service Provider for more details.

Now download and install 'ACTA SMSEmail 'Software on the server or computer running Access Manager Suite.

http://www.ACTAtek.com/Downloads/support/kw/ams/SetupSMSEmail_1.2.5.5.zip



Start the AMS SMSEmail service in administrator mode after installation.

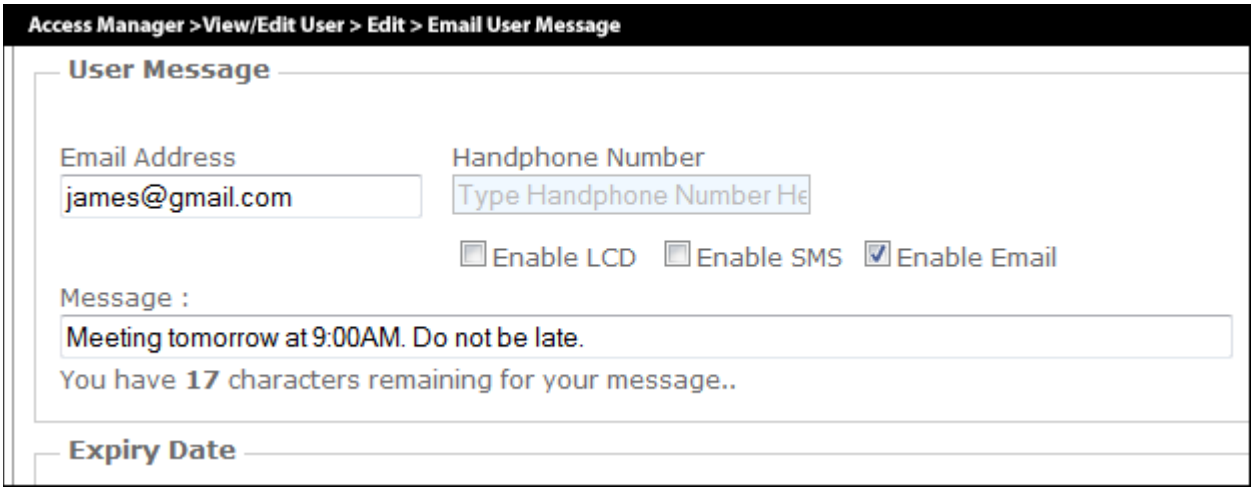
Once the SMSEmail service has installed and running go to ''C:\ProgramData\ACTAtek\AccessManager\SMStexts'' and set the values to enable and send out the alerts

Set following value as example = 20,0,1,1

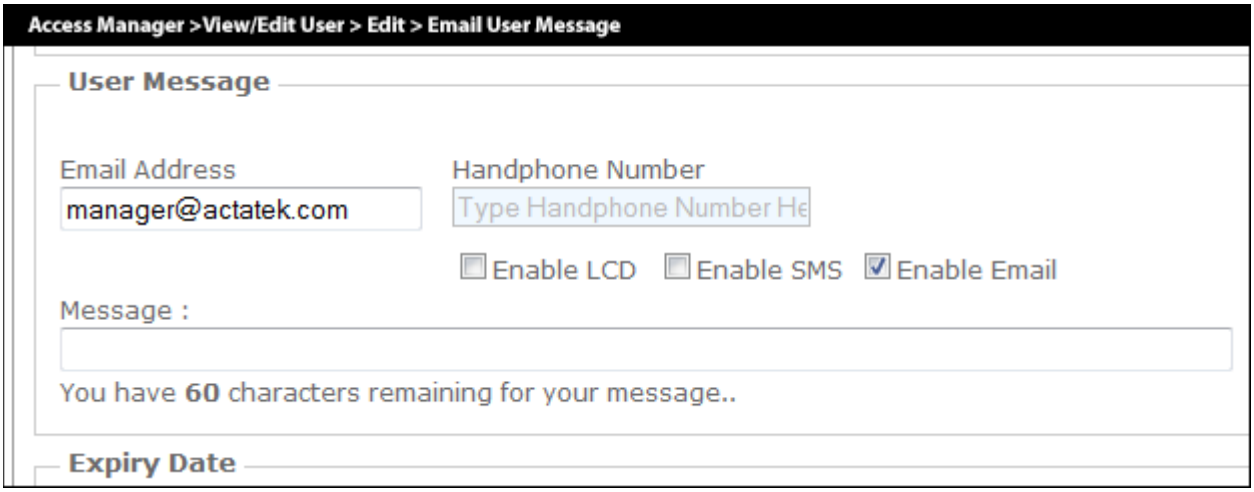
a:Running Interval in Seconds (positive number, 0 is invalid)
b:Not Used
c:0=Stop, 1=Process SMS
d:0=Stop, 1=Process Email

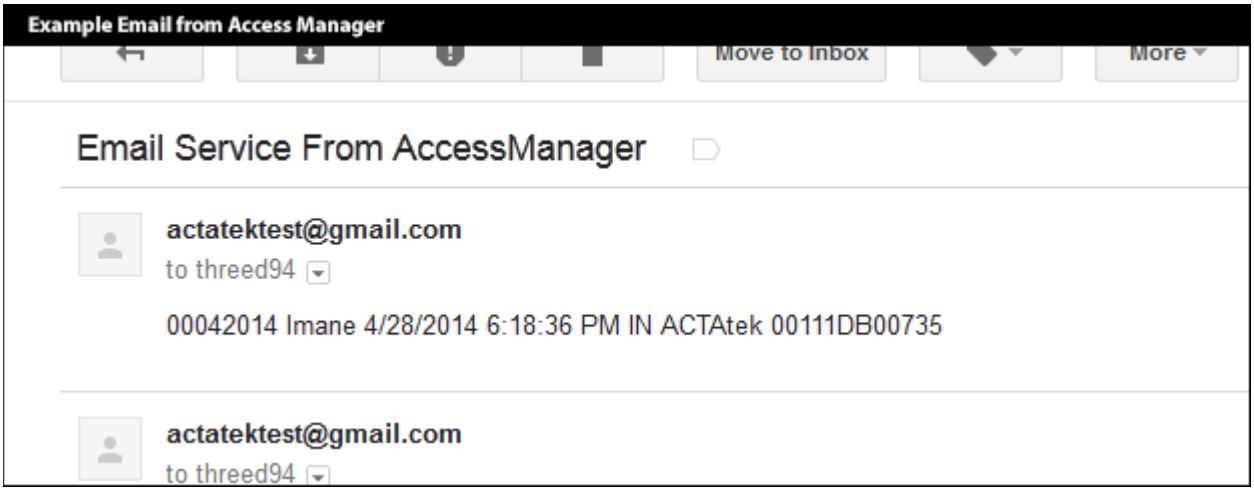
This value is the refresh time for the AMS Email SMS service to check for pending emails created by Access Manager to be sent out.

To leave an email message for a user, go to **View/Edit User** and select the user by pressing **Edit** in the **Action** column. Navigate to the **User Message** field and check **Enable Email** and provide the user's email address followed by the message in the **Message** field. Press the **Update** button to submit the user changes. To stop sending the email message on authentication, uncheck **Enable Email** for the user.



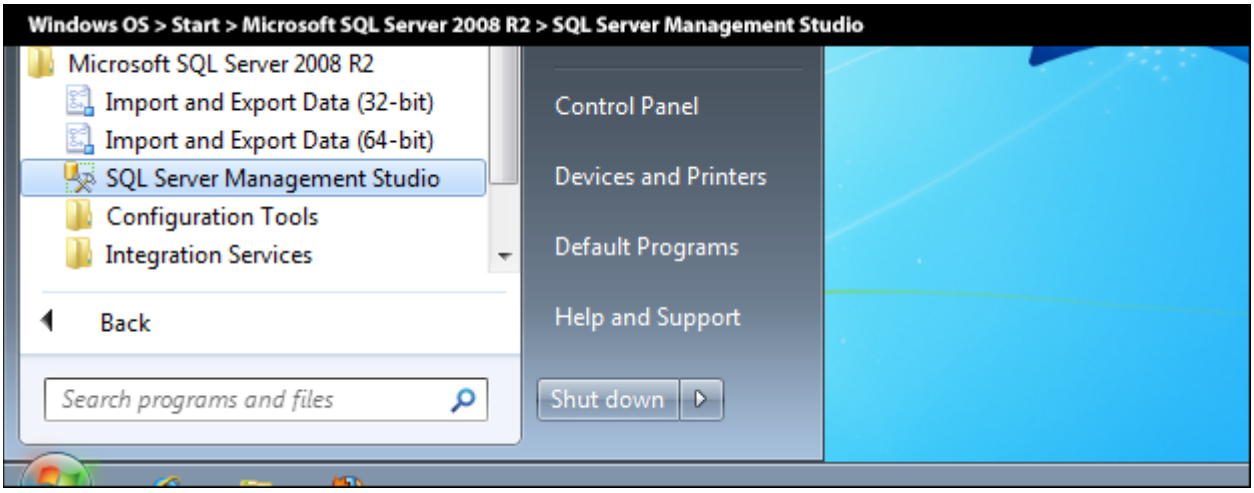
To send email alerts to a specific person instead of the user, supply the email address of the specific person (Parent/Manager/Boss) into the user's profile and that email address on file will receive emails when and what time this user has authenticated.


Access Manager >View/Edit User > Edit > Email User Message
User Message
Email Address
manager@actatek.com
Handphone Number
Type Handphone Number He
Enable LCD
Enable SMS
Enable Email
Message :
You have 60 characters remaining for your message..
Expiry Date


Example Email from Access Manager
Move to Inbox
More
Email Service From AccessManager
actatektest@gmail.com
to threed94
00042014 Imane 4/28/2014 6:18:36 PM IN ACTAtek 00111DB00735
actatektest@gmail.com
to threed94

Chapter 7: Backup AMS Database

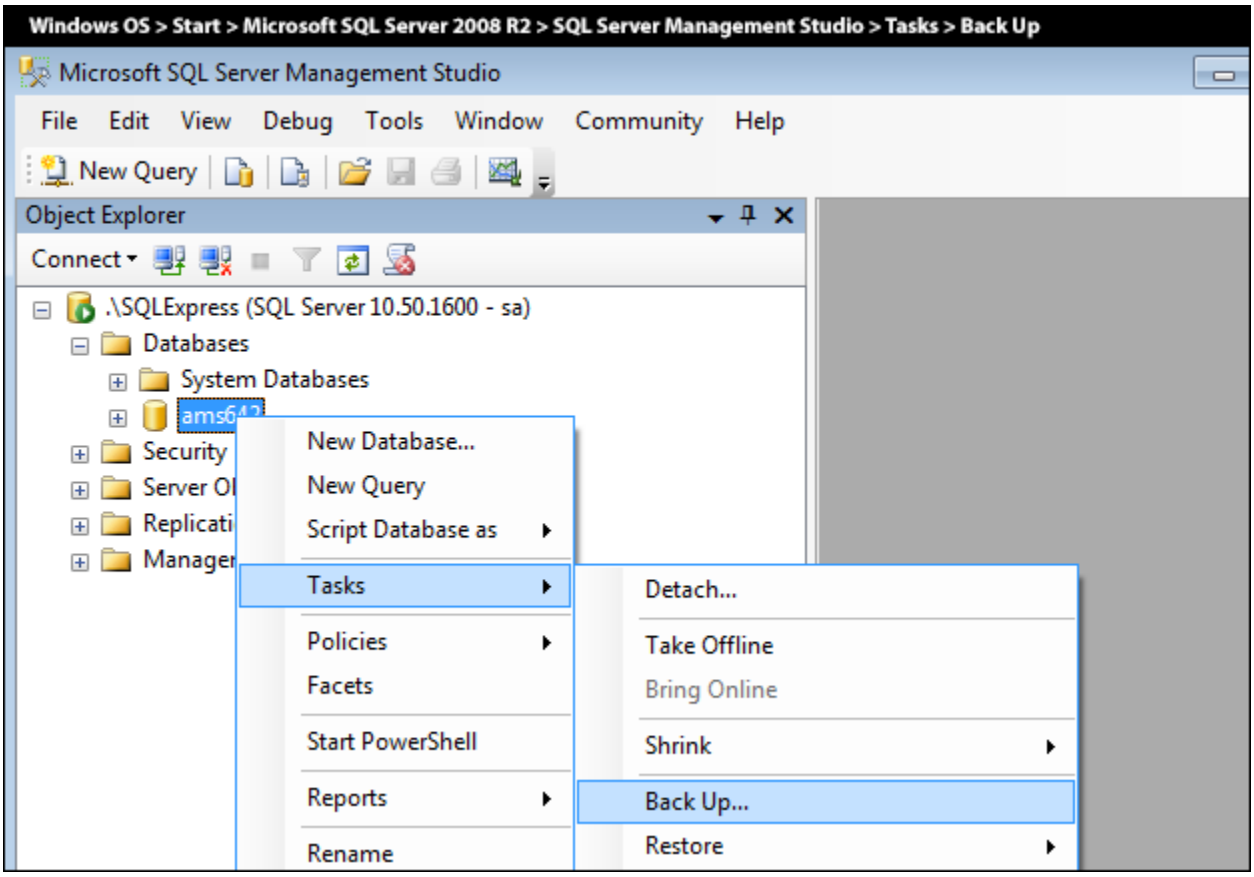
7.1 Database Backup



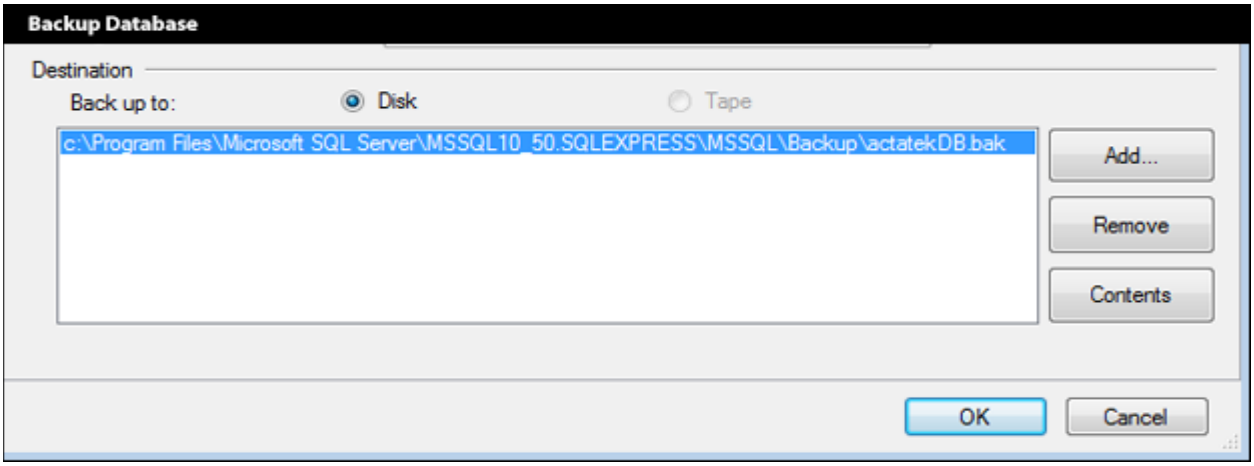
Run **SQL Server Management Studio** and log in using either SQL Server Authentication or Windows Authentication. If the SQL Server is installed on your local computer, by default the server name is:

[Local Access] .\SQLExpress
or
[Network Access] **IP ADDRESS OF SQL SERVER**\SQLExpress

Once you have connected to the SQL Server, in the **Object Explorer** located on the left, expand **Databases** to display the current databases in the SQL Server. Right click on the database you wish to back up and select **Tasks** and then **Back Up...**



Back Up Database window will now appear and by default, the setting is set to backup the database in full. In the **Destination** field, you will find the location where the backup database will be stored. Press **OK** button when you are ready. Upon completion, a success message will appear.

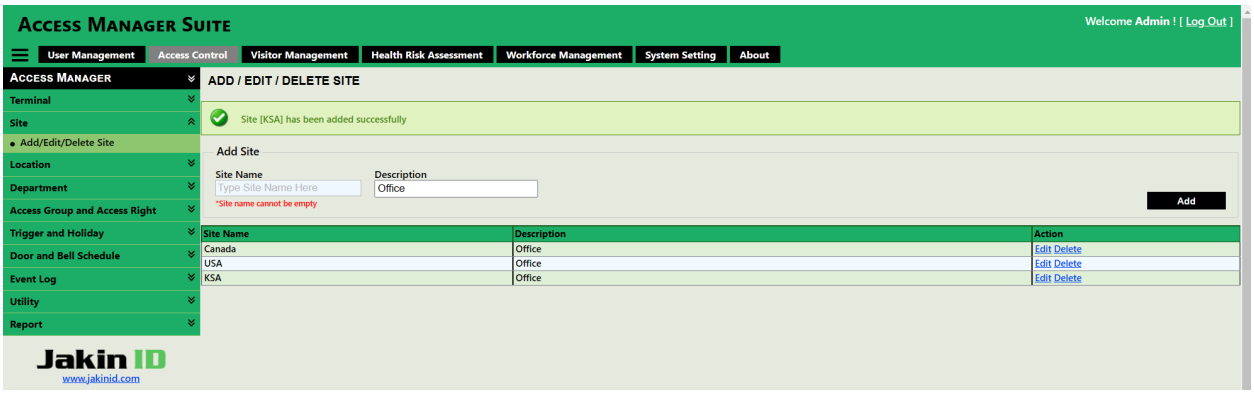


Appendix A. Site/Location Feature

The Access Manager terminal data is organized into sites/Location, each site/location will have terminal assigned to it. Terminals in a site/location will share the same user, departments and groups.

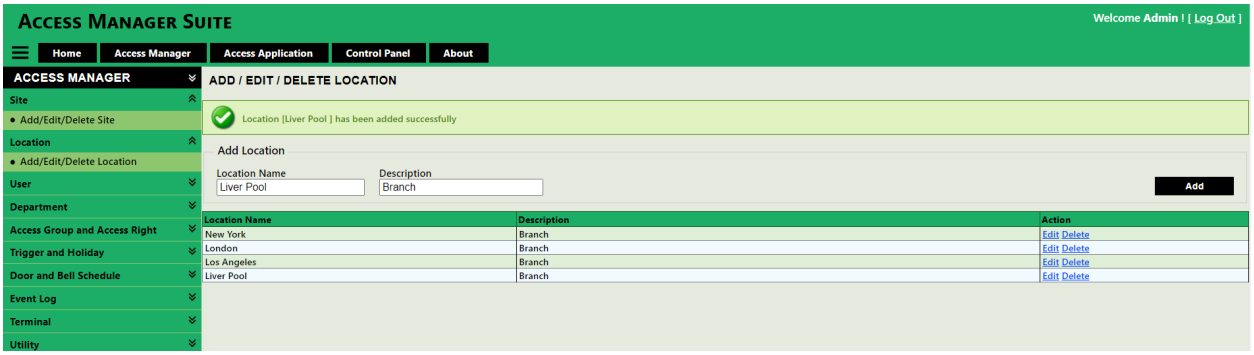
Add/Edit/Delete Site

This feature allows the administrator to add, edit, or delete sites in Access Manager. Site also help categorize users and will be the foundation for setting up **Associate Location**. To associate users to sites, you will edit a selected user in **View/Edit User** and in the **Site/Location** tab, check the listed Site relevant to this user and press the **Update** button to save the changes.



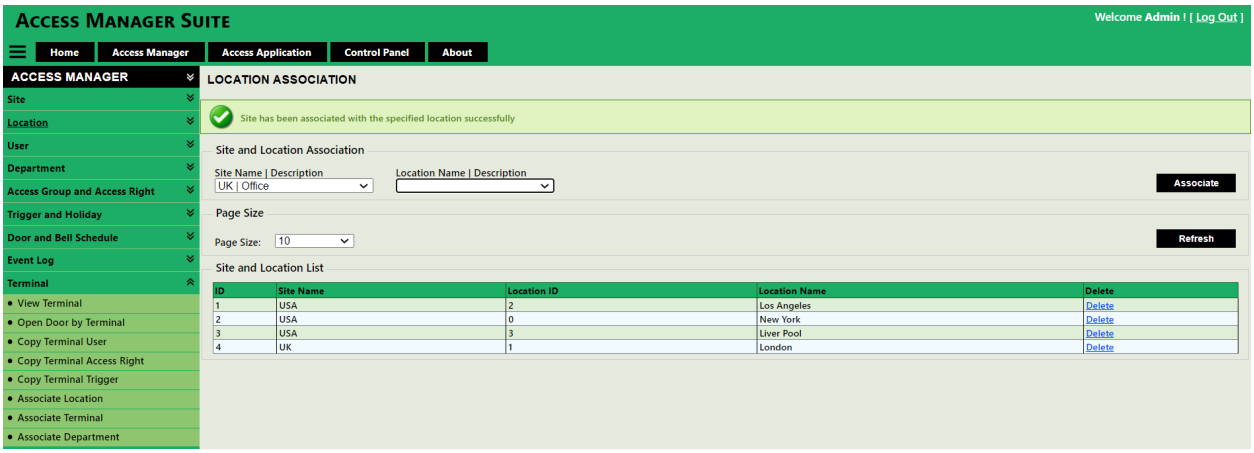
Add/Edit/Delete Location

This feature allows the administrator to add, edit, or delete Location in Access Manager. Location also help categorize users and will be the foundation for setting up **Associate Terminal**. To associate users to location, you will edit a selected user in **View/Edit User** and in the **Site/Location** tab, check the listed location relevant to this user and press the **Update** button to save the changes.



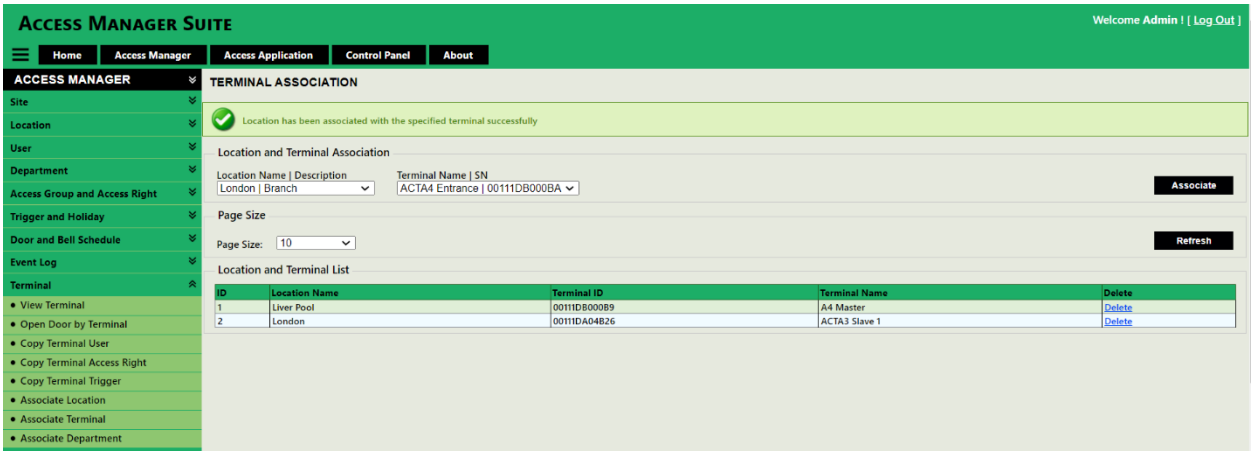
Associate Location

Associate location feature allows the administrator of AMS to associate specific site to one or multiple Location. To accomplish this, select a site name from the site list and select a location and press the **Associate** button to add this association.

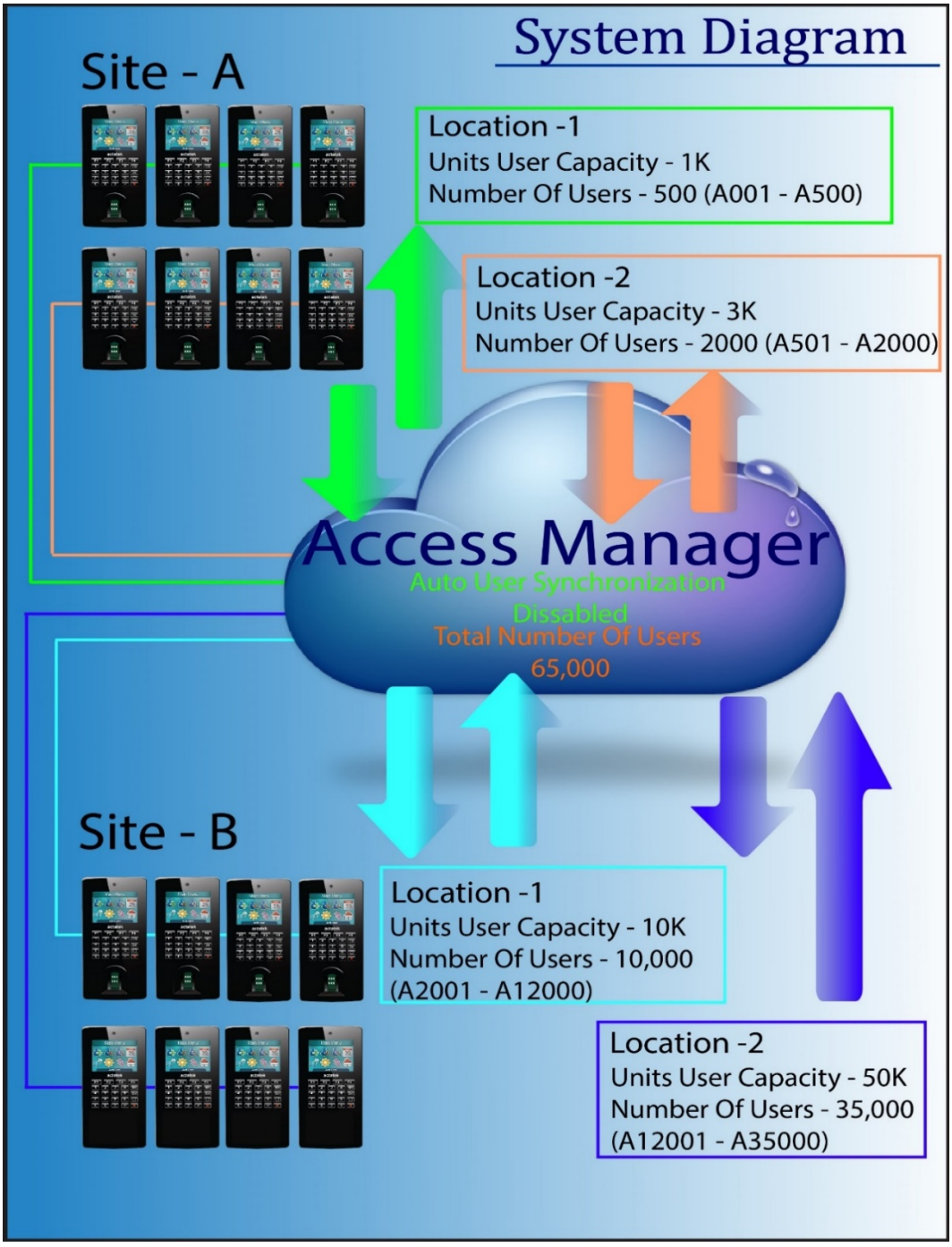


Associate Terminal

Associate Terminal feature allows the administrator of AMS to associate specific ACTATEK terminals to a location in AMS. To accomplish this, select an ACTATEK terminal from the terminal list and select a location from Location name list and press the **Associate** button to add this association.



Site/Location Feature System Diagram



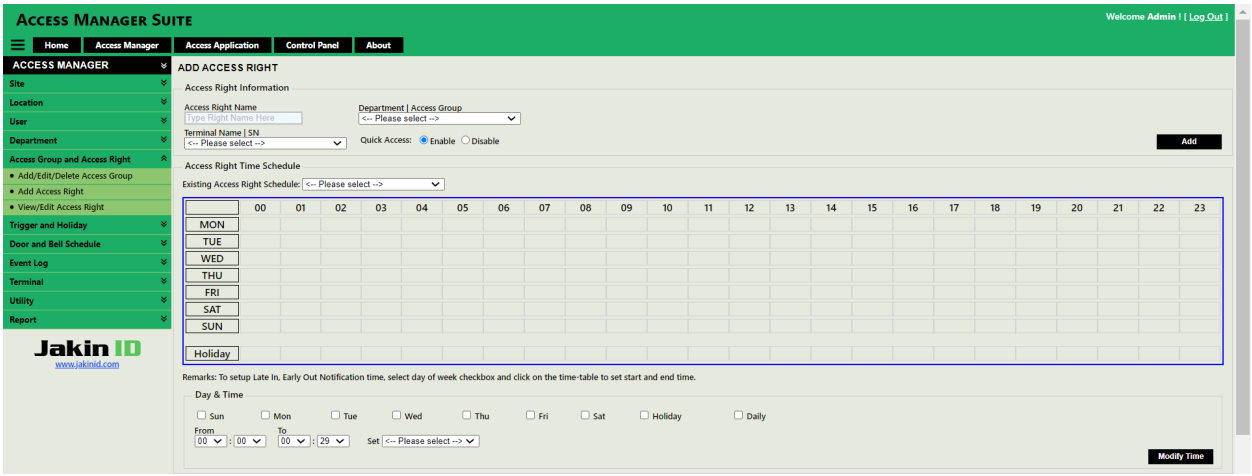
Appendix B. Late IN Early OUT Notification (Email SMS)

The AMS administrator can set-up Email and SMS notification alerts to selected users or managers. Upon users making late IN and early OUT and it will alert to configured user and managers.

Please kindly refer to **chapter 6.5** Send email **(page number 40**) to install and configure the AMS SMSemail Service. So as to enable and send out Late IN and Early OUT notification alerts.

To set or change the Late In, Early Out time, Go to **AMS** and then Select **Add Access Rights.** The default settings of Access Manager already have predefined access groups. The administrator may choose to customize or remove irrelevant access groups and departments to personalize their setup and environment. Access Rights are used to distinguish different levels of notification alerts.

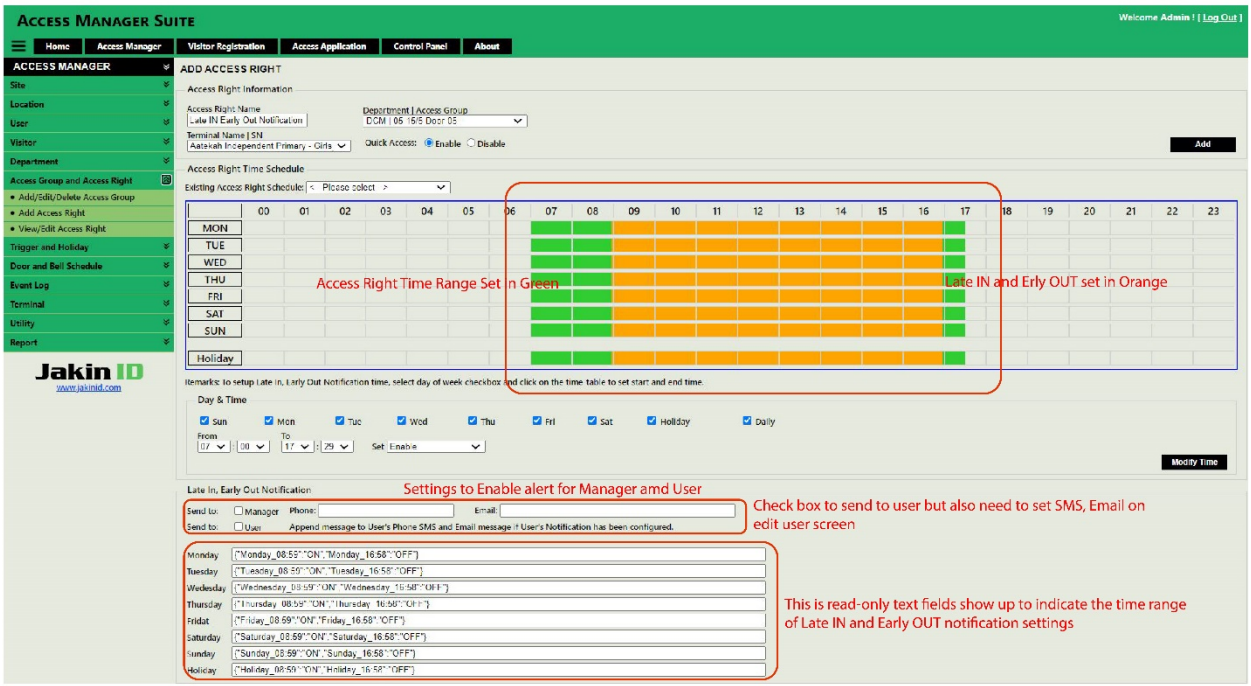
An access right is an access control policy used for binding an ACTA terminal to an access schedule with the associated department and access group. This will enforce users in that associated department and access group to the access schedule as defined by the administrator. The advantage of using access rights is that it will provide the access control rules to ACTA terminals. For example, using access rights can limit certain user groups to certain ACTA terminals. Additionally, it can restrict with the time and days when a user can have access. Also, the admin can create specific time range top of the access right time schedule to get Late In, Early Out Notification.



To setup an access right, provide an **Access Right Name** followed by selecting a **Dept/Group Name** from the list which this access right will affect. Users in this department and access group will have this policy applied to them. Next, select an ACTA terminal from the **Terminal Name / SN** list to apply this access right to and set **Quick Access** to enable.

In the **Day & Time** field, the administrator defines the restrictions and the rules in terms of a schedule. By default, the schedule has all time and days of the week disabled which can be referenced below by the green color.

After making setting changes to the **Day & Time** field, press the **Modify Time** button to review the changes made. The filled green color area set for enabled while the light grey color set for disabled.



To set or change the Late In, Early Out time, orange time setting mouse click on left side to point the earlier time and then mouse click on right side to point the later time. once select the time frame will over-write and change orange time setting of right side (later time).

To remove existing orange time setting, put mouse on left, e.g. 02:00am, click and click. All orange setting for the day will be removed. Ready to set the new time range again.

To set same orange time setting for multiple days, select checkbox on the days first, e.g. Mon, Tue, Fri, then set all 3 selected days at the same time.

Appendix C. Configure Access Manager Crowd Control Occupancy Limit and Notification.

With Access Manager Crowd Control enabled at System Settings, Access Manager can be configured to control Occupancy up to a configurable Occupancy Limit. Access Manager can also send out SMS, Email notification when the current occupancy reached a high occupancy alert Level, which is configurable.

System Settings to Enable Crowd Control and Crowd Control Notification

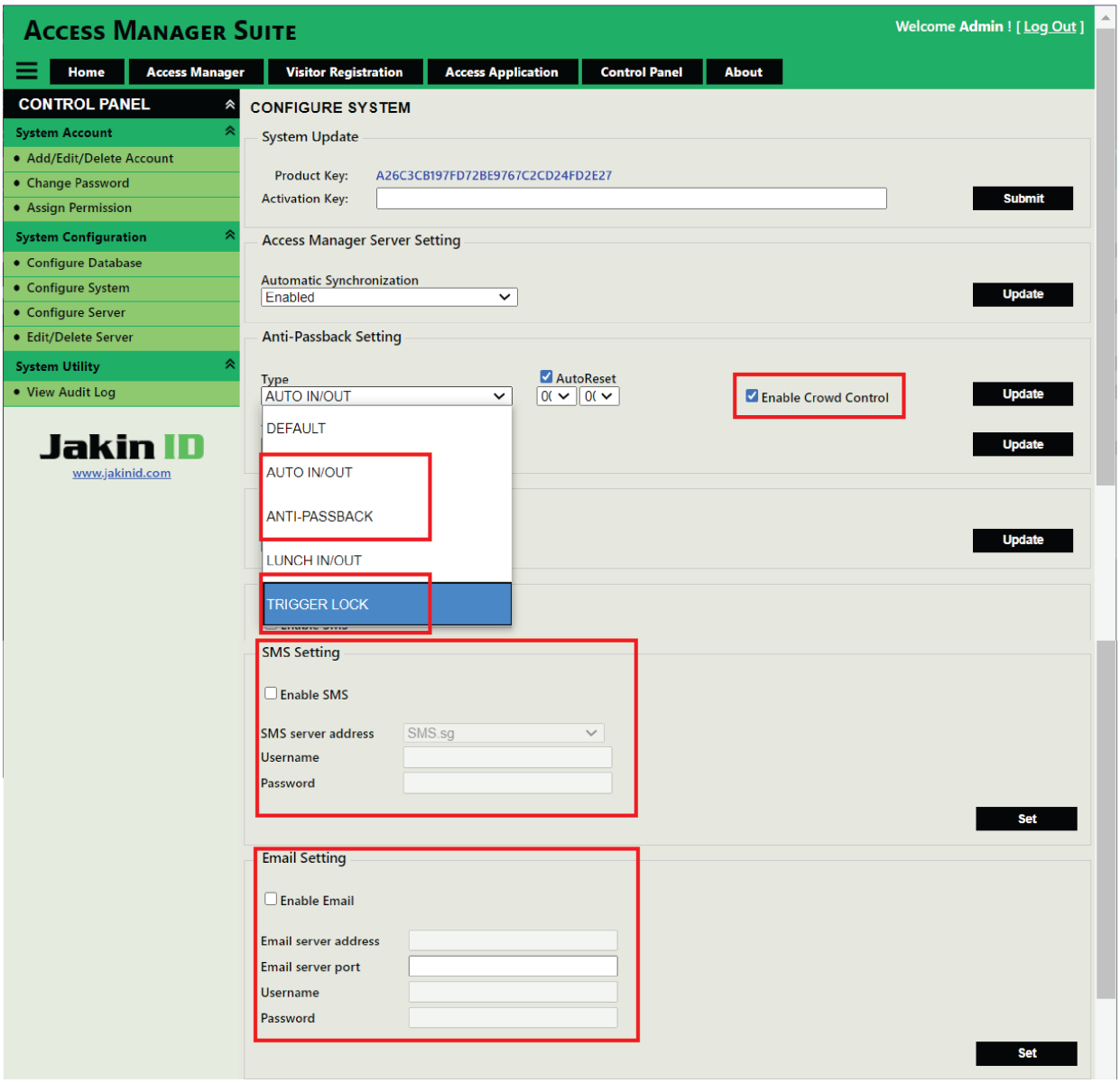
>> Enable/Disable Crowd Control :- Control Panel > System Configuration > Configure System > **Anti-Passback Setting > Enable Crowd Control**

Example: http://localhost/AccessManager/Account/SystemUpdate.aspx

Crowd Control supports Anti-Passback modes: **AUTO IN/OUT, ANTI-PASSBACK, TRIGGER LOCK**

To Set up Crowd Control Notification at high Occupancy Notification Level Configure SMS and Email server connection ready. Control Panel > System Configuration > Configure System > **SMS Setting and Email Setting**
Install SetupSMSEmail_1.2.5.5 and ensure SMS Service is Running.
http://www.ACTAtek.com/Downloads/support/kw/ams/SetupSMSEmail_1.2.5.5.zip

Please kindly refer to **chapter 6.5** Send email **(page number 40**) to install and configure the AMS SMSemail Service



Add/Edit Crowd Control Group or Delete the Group

Occupancy is counted as total of users with IN events to single or multiple Terminals within a Crowd Control Group which can be added or edited at **Access Manager > Terminal > Add/Edit Crowd Control Group**

Enable: Occupancy Limit, Checkbox to enable/disable Occupancy Limit
Occupancy Limit: Limit to reject/disallow additional IN event until someone get OUT of the facility.

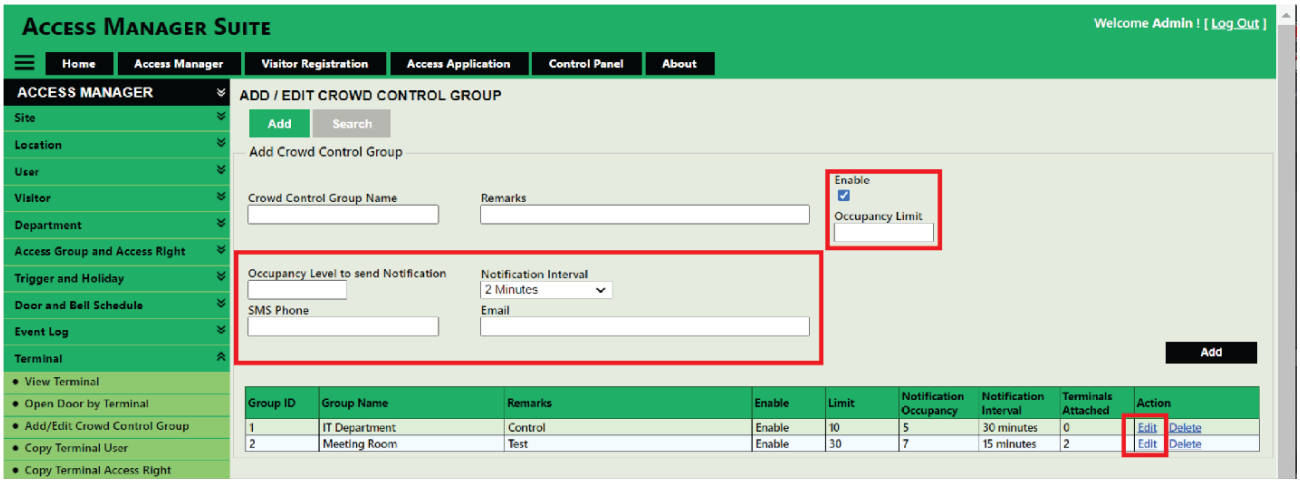
Notification Level: Could be any number below or equal to Limit to receive notification once reaching the notification Level. Or leave blank to not set if don't want to receive notification.

Notification Interval: Time interval in Minutes/Hours to pause before sending out another high occupancy **SMS/Email notification**, e.g. with at least 15 minutes apart.

Enable: [x] checked
Occupancy Limit: e.g. 50
Notification Occupancy Level: 40
Notification Interval: 15 minutes

With settings above, the 40th Occupancy will trigger to send notification once in every time interval set. User still can get IN the facility. In 15mintes later, any IN event if still reaching or over **Notification Occupancy Level**, will send another notification.

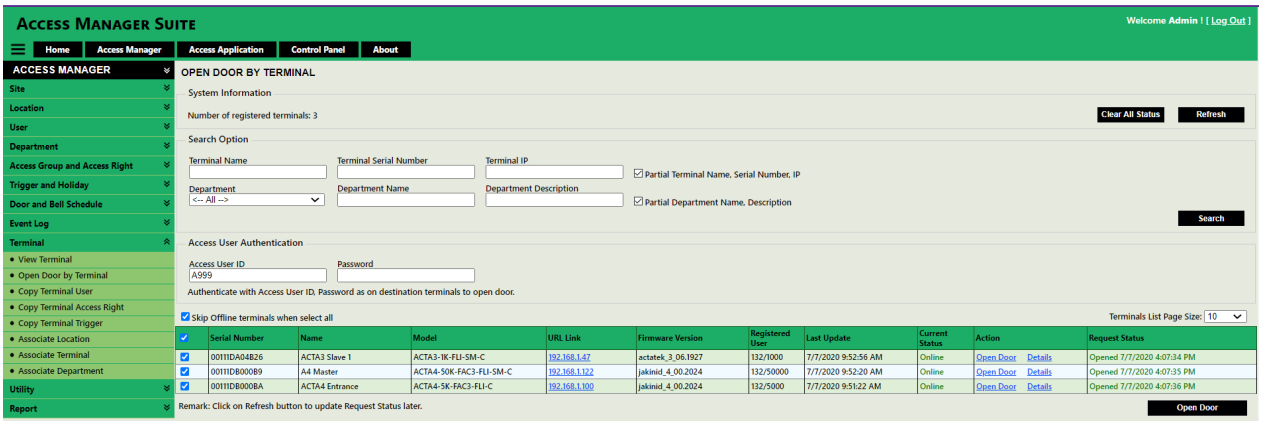
Occupancy 50 as maximum Limit to reject/disallow the 51st user to get IN until someone get OUT.



Appendix D. Open Door by Terminals.

With Access Manager Open Door by Terminal feature the system administrator can now open the access control device's doors remotely from AMS interface.

To open the door, select the Terminal or Terminals >> assign the device's access user ID and password and then click **Open Door** button.



Once AMS trigger to open the terminal's door, Request Status panel will update the time frame of the operation.

Appendix E. Visitor Registration

With the Access Manager's Visitor Management feature, provide a quick and easy way for system admin or supervisor to Register the visitor to access sites or specific building zones. They simply **login to the AMS** and click the screen on **Visitor Registration** to capture the visitor's image and then enter the visitor's details. Information on the badge. It can be configured to include details such as visitor and Name, Purpose of visit, expiry date and etc.

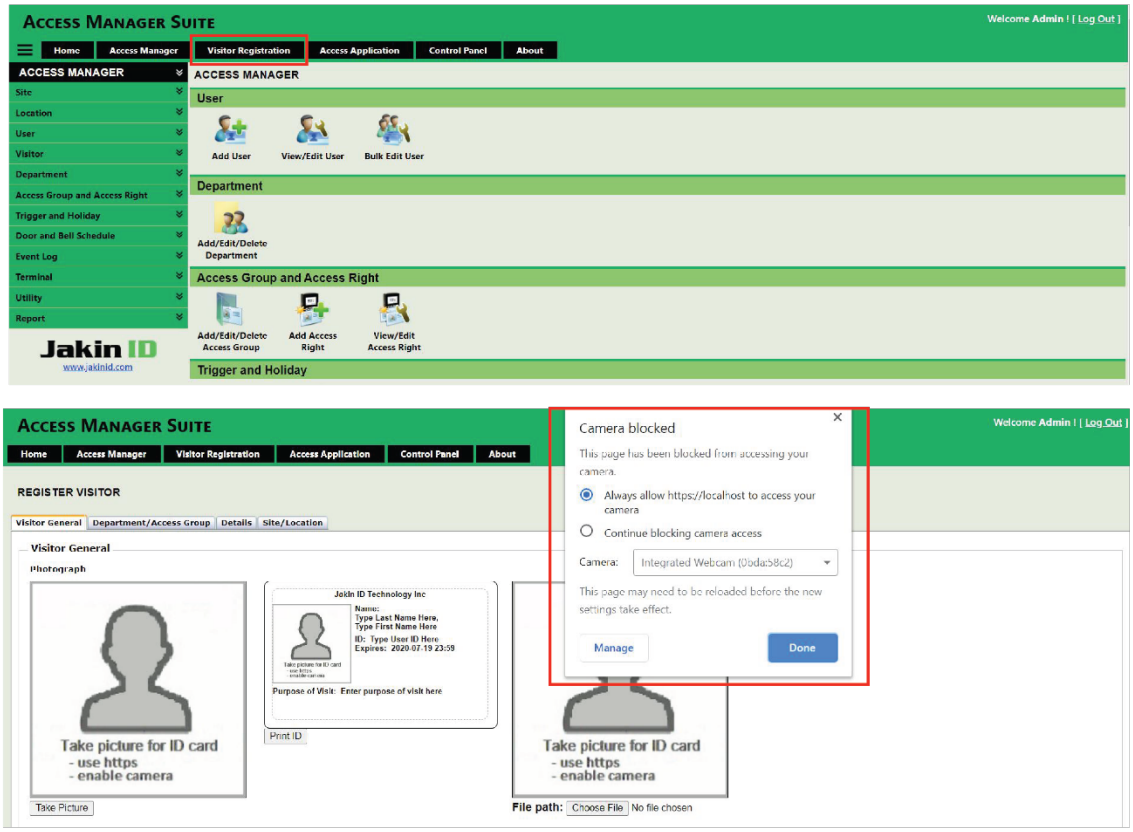
the automated visitor management system allows to prints the relevant type of badge for visitors or contractors by using any Card Printers.

steps to register new visitor and print ID card for visitors via Zebra ID card printer.

1. Make sure the PC or laptop is connected with the web camera, and also the ID card printer ready. (Mobile devices also can use to register the new visitors example: - Mobile phones, Tablets and etc...)

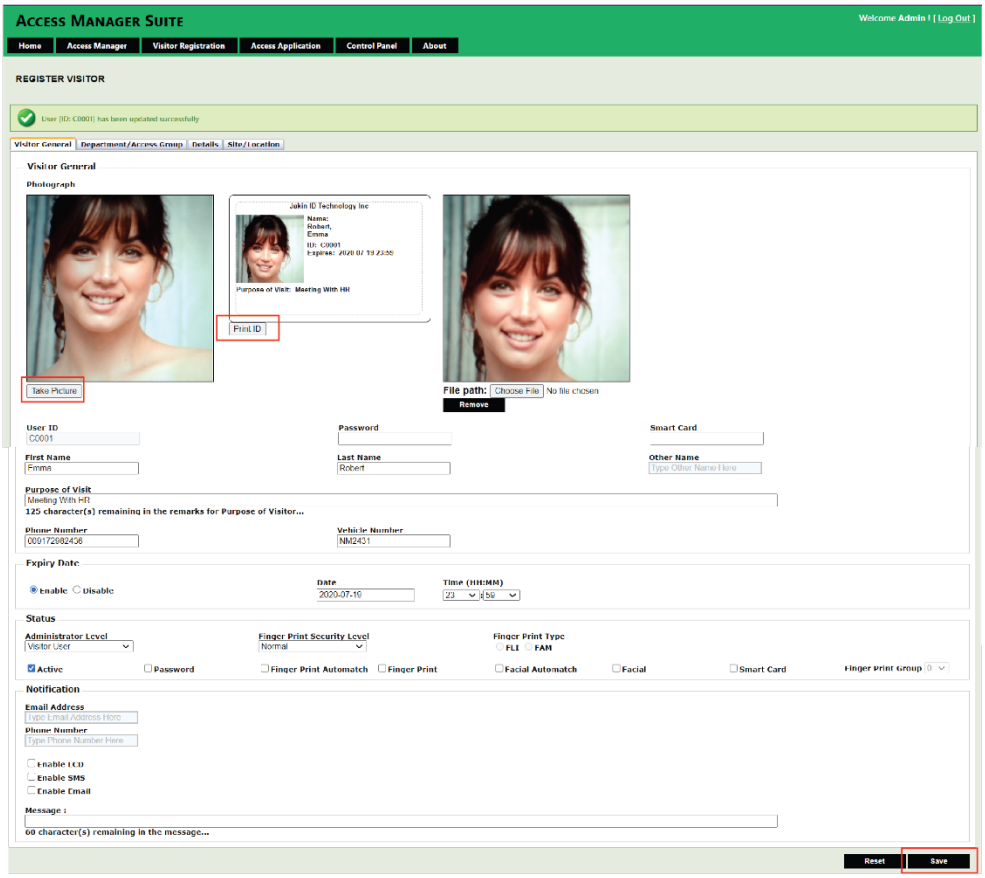
2.Open Chrome browser, and then Login to AMS's "Visitor Registration page. (*Please ignore Chrome's SSL alert message, and continue to browse the URL.)

3. Make click allow to connect the camera



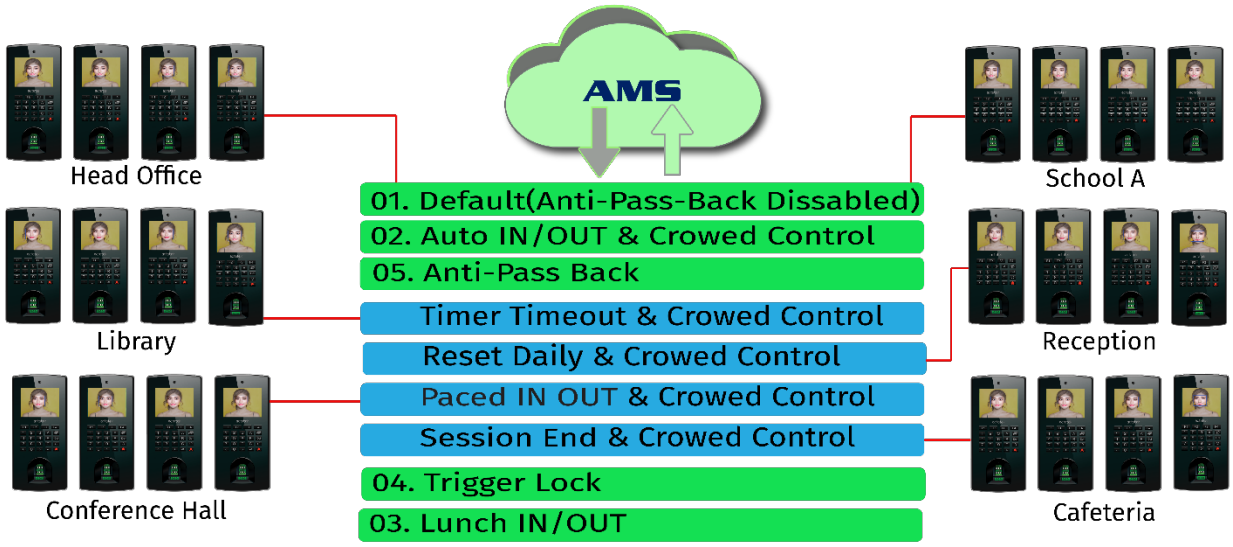
4. Capture or uplod the vistor image and Enter the Vsitor details such as ID,Name and etc. Once done Click Save button to add the vistor in to the system.

5.Click on Print ID button to print the visitor card by any ID card Printer Exampe:-Zebra, Magic Card


ACCESS MANAGER SUITE
Welcome Admin ! [Log Out]
Home
Access Manager
Visitor Registration
Access Application
Control Panel
About
REGISTER VISITOR
User [ID: C0001] has been updated successfully
Visitor General
Department/Access Group
Details
Site/Location
Visitor General
Photograph
Jakin ID Technology Inc
Name:
Robert,
Emma
ID: C0001
Purpose of Visit: Meeting With HR
Print ID
Take Picture
File path:
Choose File
No file chosen
Remove
User ID
C0001
Password
Smart Card
First Name
Emma
Last Name
Robert
Other Name
Type Other Name Here
Purpose of Visit
Meeting With HR
125 character(s) remaining in the remarks for Purpose of Visitor...
Phone Number
00917282436
Vehicle Number
NM2431
Expiry Date
Enable
Disable
Date
2020-07-10
Time (HH:MM)
23
59
Status
Administrator Level
Visitor User
Finger Print Security Level
Normal
Finger Print Type
FLI
FAM
Active
Password
Finger Print Automatch
Finger Print
Facial Automatch
Facial
Smart Card
Finger Print Group
Notification
Email Address
Type Email Address Here
Phone Number
Type Phone Number Here
Enable LCD
Enable SMS
Enable Email
Message :
60 character(s) remaining in the message...
Reset
Save

Appendix F. Anti-Pass Back Group.

Introduce new "APB Group" to have different APB settings. With new APB Groups, AMS can concurrently set to Disable APB for one APB Group A, Anti-Pass back for another APB Group B, AUTO IN/OUT for another APB Group C etc. Undefined APB Group for certain Departments/Terminals may follow System-wide default APB settings



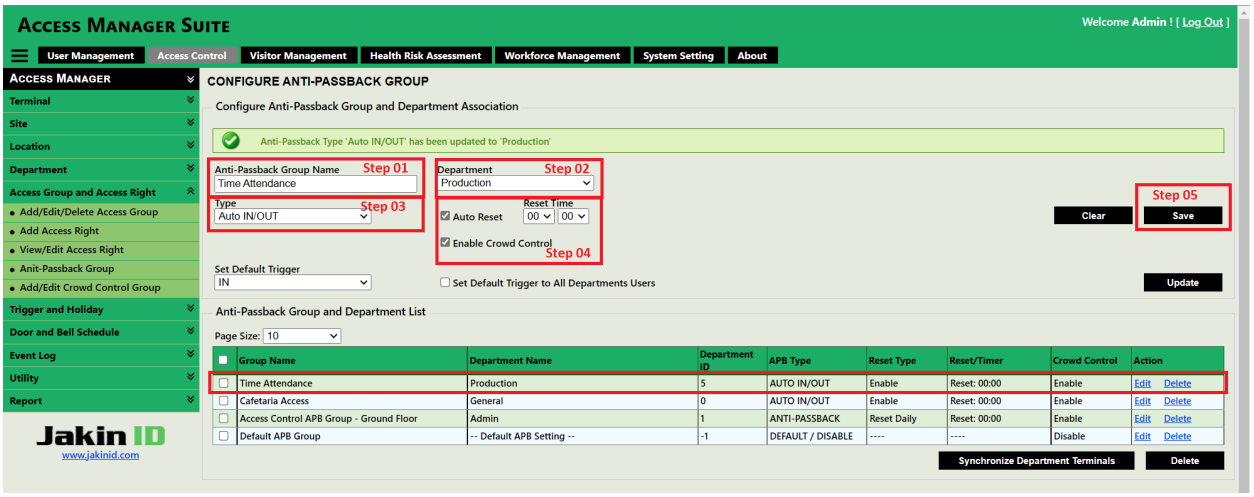
The APB advance features will require the Access Manager Suite Server to reside on the same local area network as the ACTAtek terminals for the best possible outcome. Authentication is determined by the status of the users from the Access Manager Suite Server when working with multiple ACTAtek terminals therefore a low latency network is required.

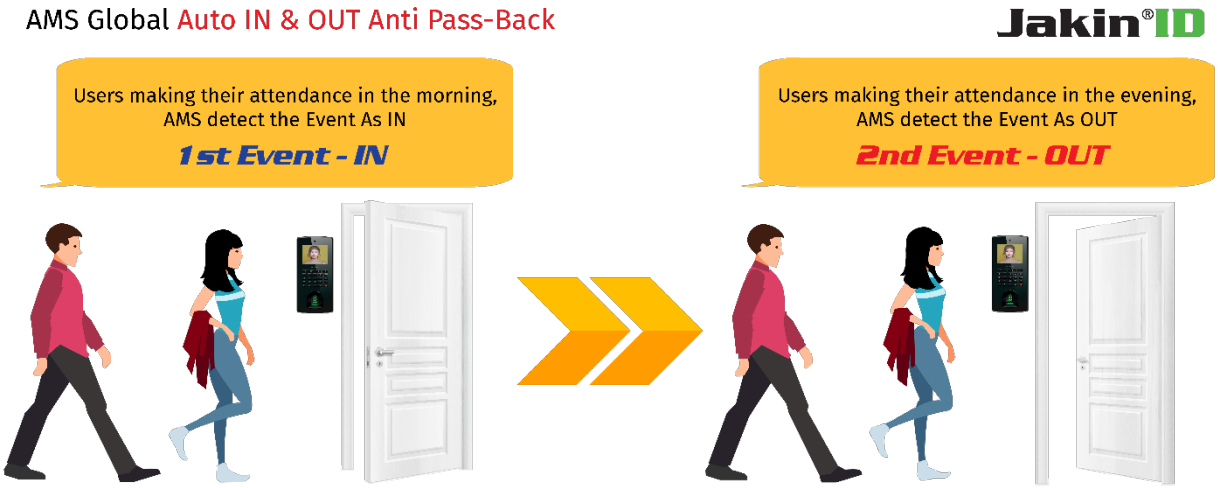
In any event where the Access Manager Suite Server goes offline or the ACTAtek terminal loses communication with AMS server, the ACTAtek terminal will not be able to request a server-side authentication and instead record an ID UNKNOWN event record while the ACTAtek terminal screen shows ID Reserved AMS Offline during the punch.

Auto In/Out

The **Auto In/Out** feature allows the ACTATEK terminal to use server-side authentication to automatically determine the IN or OUT status of a user during authentication and records a preceding punch event based on the user's previous event. To enable this feature, go into the **Access Control** tab and then **Anti-Passback Group**. Create new **APB settings by assign a group name and selecting the particular**

department >> Change from **DEFAULT** to **AUTO IN/OUT** and press **Update** button to save. The ACTATEK particular department associated terminals will now only show **AUTO** on the LCD screen.





The AMS Auto In/Out feature allows the ACTA3 terminal to use AMS server side authentication to automatically determine the IN or OUT status of a user during authentication and records a preceding punch event based on the user's previous event.

Anti-Passback

Anti-pass back- is a security measure that aims to prevent consecutive entries for one access event, or prevent multiple people from using the same access credentials It can stop users from entering the area by using the same access event example IN for specific time period. such that the user must proceed with **IN** event and then forced to use **OUT** event and not **IN** again.

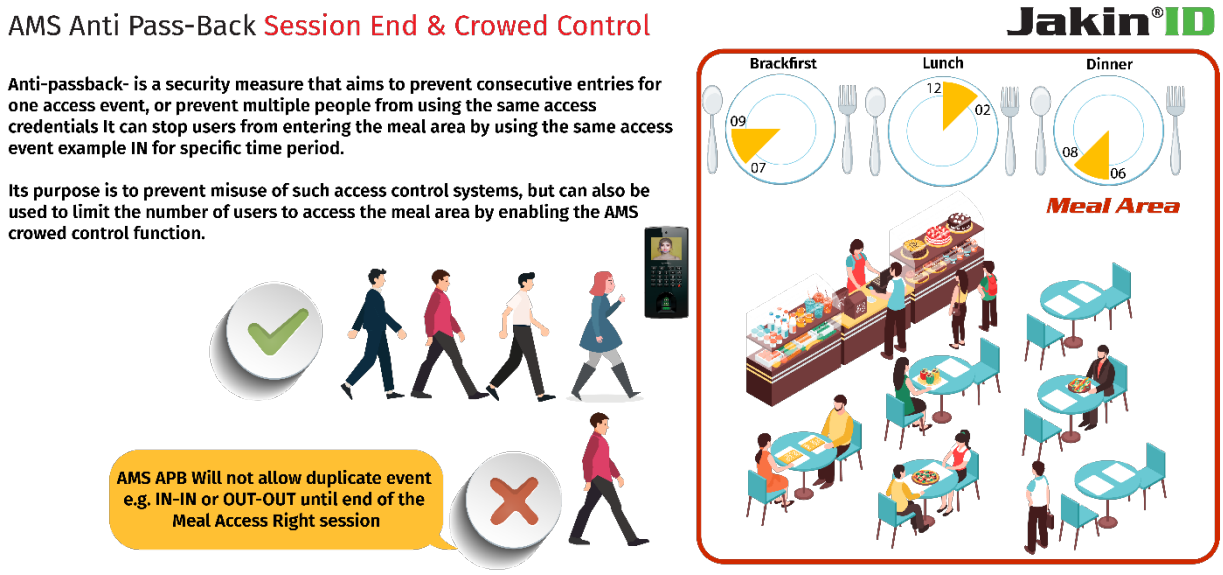
Its purpose is to prevent misuse of such access control systems, but can also be used to limit the number of users to access the area, room, floor by enabling the AMS crowed control function.

The **Anti-Passback** feature allows the ACTAtek terminal to use server-side authentication to automatically determine the IN or OUT status of a user during authentication and records a preceding punch event based on the user's previous event. example scenario where Anti-Passback would be used is to ensure that the user enters through the first door with ACTA3 terminal set on IN and then exit using the second door with ACTA3 terminal set on OUT.

To enable this feature, go into the **Control Panel** tab and then **System Configuration**. Change **APB setting** to **ANTI-PASSBACK** and press **Update** button to save. To use this feature, only triggers **IN** and **OUT** will be affected by Anti-Passback.

To enable this feature, go into the **Access Control** tab and then **Anti-Passback Group**. Create new **APB settings by assign a group name and selecting the particular department >> Change** from **DEFAULT** to **Anti-Passback** and press **Update** button to save. The ACTATEK particular department associated. terminals will now use server-side authentication to automatically determine the IN or OUT status of a user during authentication. To use this feature, only triggers **IN** and **OUT** will be affected by Anti-Passback.

- ✓ **Reset Daily - Reset Daily at the time configured to allow Passback**
- ✓ **Timer Timeout - Reset at Timer Timeout after previous event to allow Passback**
- ✓ **Session End - Reset at the End of Access Right time Session to allow Passback**
- ✓ **Paced IN OUT - No APB Reset, Timer Paced between IN/OUT events**



Lunch In/Out

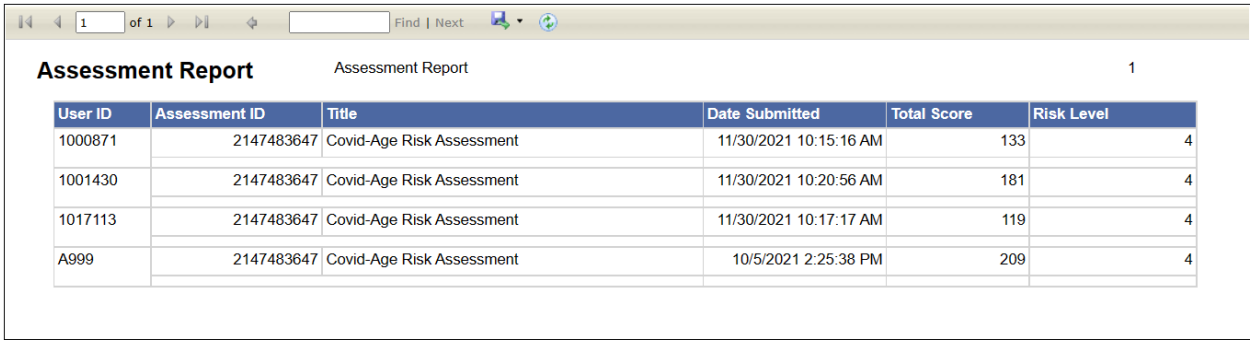
The **Lunch In/Out** feature is used when you would like to enforce a lunch time period so no users can punch in from break until the set time is reached. If they try to punch back in from break before the set time has reached, it will reject them on the ACTAtek terminals.

To enable this feature, go into the **Access Control** tab and then select **Anti-Passback**. Create new **APB settings by assign a group name and selecting the particular department >>** Change **APB setting** to **LUNCH IN/OUT** and press **Update** button to save. Set a **LUNCH OUT** time to allow LUNCHOUT trigger to be used when the user goes on their break. Set a **LUNCH IN** time to allow LUNCHIN trigger to be used after their break is over. The ACTAtek terminal will allow LUNCHIN trigger after the time has passed the set LUNCH IN time in AMS.

Next**, Edit Triggers** on an ACTAtek terminal through the AMS web interface.
Set F1 to "LunchOUT" and F2 to "LunchIN" **or** F3 to "LunchOUT" and F4 to "LunchIN."
Use **Copy Trigger** function and copy them over to all other registered ACTAtek terminals.

Appendix: G. Health Risk Assessment.

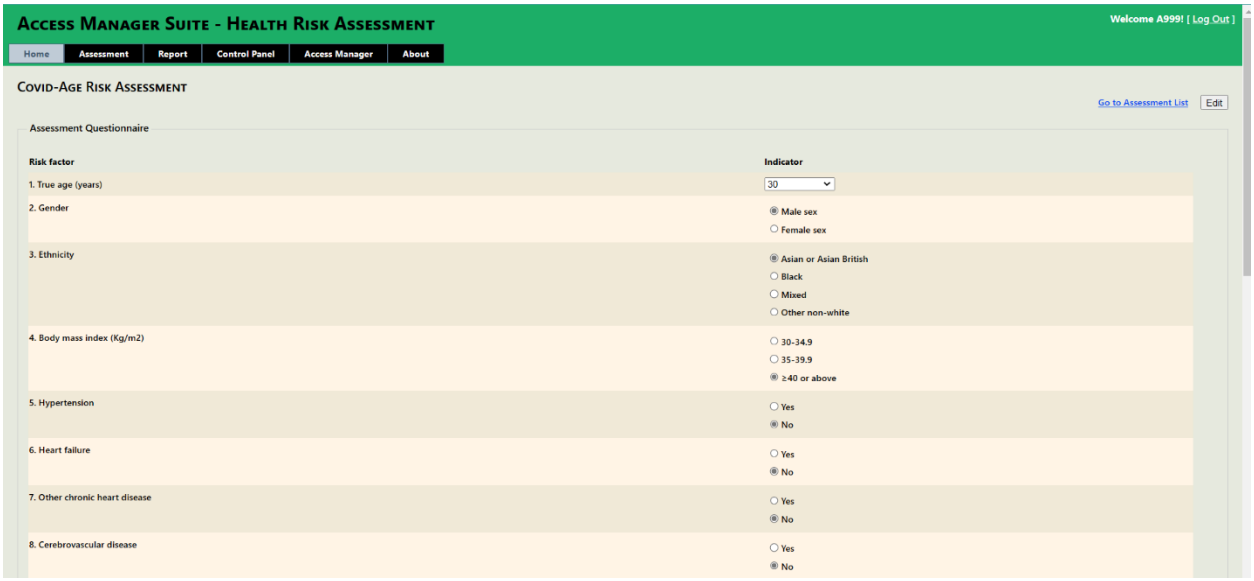
The AMS Health risk assessment (HRA) aggregate data is used by employers and wellness providers to understand the health risks of a population, to measure the impact of an employer-sponsored wellness program, and to improve the use of resources. The AMS default British Medical Association standards assessment for health appraisals and issues reports to customers who comply with these standards to determine the user's risk levels.



User ID	Assessment ID	Title	Date Submitted	Total Score	Risk Level
1000871	2147483647	Covid-Age Risk Assessment	11/30/2021 10:15:16 AM	133	4
1001430	2147483647	Covid-Age Risk Assessment	11/30/2021 10:20:56 AM	181	4
1017113	2147483647	Covid-Age Risk Assessment	11/30/2021 10:17:17 AM	119	4
A999	2147483647	Covid-Age Risk Assessment	10/5/2021 2:25:38 PM	209	4

The AMS health risk assessment includes a questionnaire, an assessment of health status, and personalized feedback about actions that can be taken to reduce risks, maintain health, and prevent disease. AMS health risk assessment questionnaire is usually completed online using a PC, tablet, or

smart phone. After Users submitted their answers, the HR manager can separate Users into different risk group based on their risk level so as to prevent cross spread of Covid especially to the high-risk groups



The health risk assessment also can include questions in the following example areas:

Demographic characteristics – age, gender
Lifestyle behaviors – exercise, eating habits, alcohol and tobacco use
Emotional health – mood, stress, life events
Physical health – weight, blood pressure, cholesterol levels
Current and previous health conditions

Quick setup steps:

1.Login to MS SQL management studio software to restore the 'AMS_Assessment_SampleDB.bak' file into SQL server.

http://www.actatek.com/Downloads/support/ams/ams_health_assessment.zip

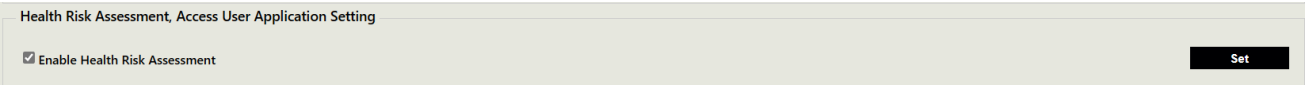
2. Edit the 'Web.config' file located at ' C:\inetpub\wwwroot\AccessManager\HealthRiskAssessment\ ' ,and change the below 2 db connection strings ,and save the file.

Note:Please change the texts in red color based on customer SQL db server settings.

```
  <connectionStrings>

    <add name="AMS_ConnetionString" connectionString="Data
Source=localhost\SQLEXPRESS;Initial Catalog=AMSDB;User ID=sa;Password=123456" />

    <add name="ASSM_ConnetionString" connectionString="Data
Source=localhost\SQLEXPRESS;Initial Catalog=AMS_Assessment;User
ID=sa;Password=123456" />

  </connectionStrings>
```

3.Once done, Login to AMS as the admin User and **enable** Health Risk Assessment, Access User Application Setting from the AMS **Configure System** Page.

localhost/AccessManager/Account/SystemUpdate.aspx



4. Now the Admin can see the Health Risk Assessment module from the AMS UI.

Appendix: H. Time Off Management

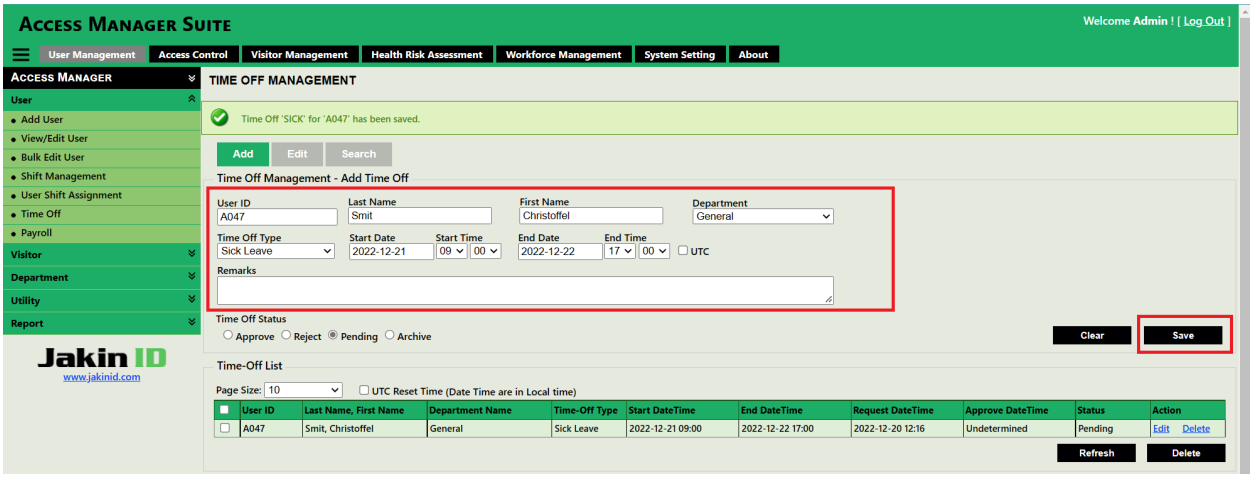
Time-off management is the process of managing time-off requests such as Vacation, sick leave and Others leave through a series of policies, guidelines, and rules that are specific to your business.

The automated time off management to reduce the time spent on paper forms and approvals. Managing employee time off requests by AMS could be any easier and more user friendly.

The time off manager allows your employees to request leaves of absence, add comments, and sent them to the manager for approval.

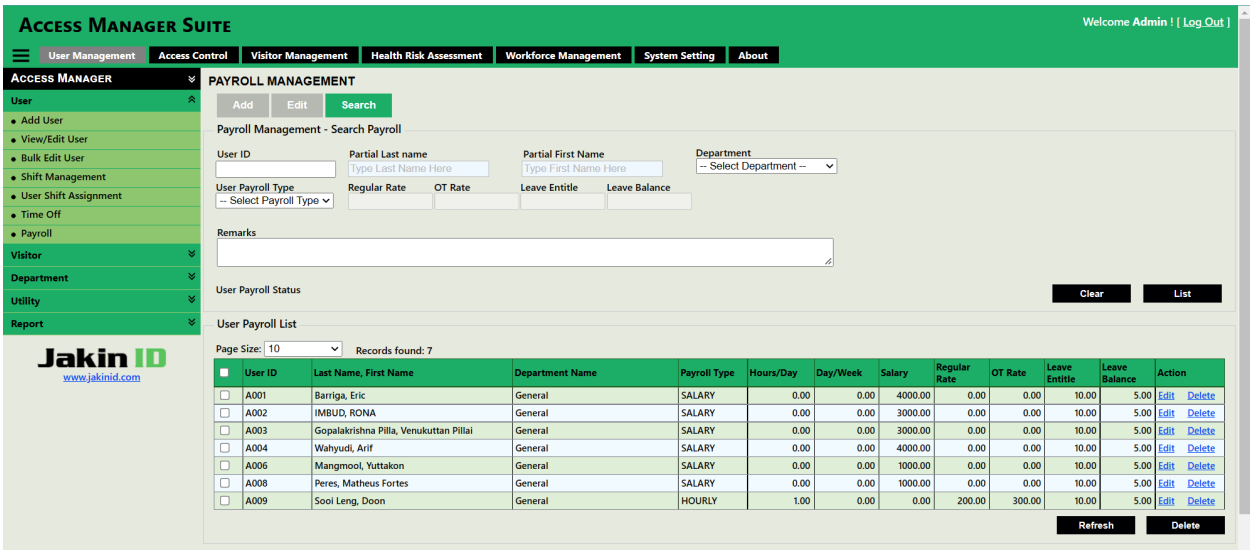
To create a new time off request, User need brows the AMS to go into the **User Management** tab and then enter the user ID, select **a type of vacation** and select the Time Of period. Once done, press **Save**

button to finish the Time Off request. The users also can use the ACTAtek mobile App to request their time off.



Appendix: I. Payroll Management

Payroll Management lets AMS admin view, modify, and create detailed payroll information for their employees. It is composed of three general categories**: Hourly / Daily / Salary**.



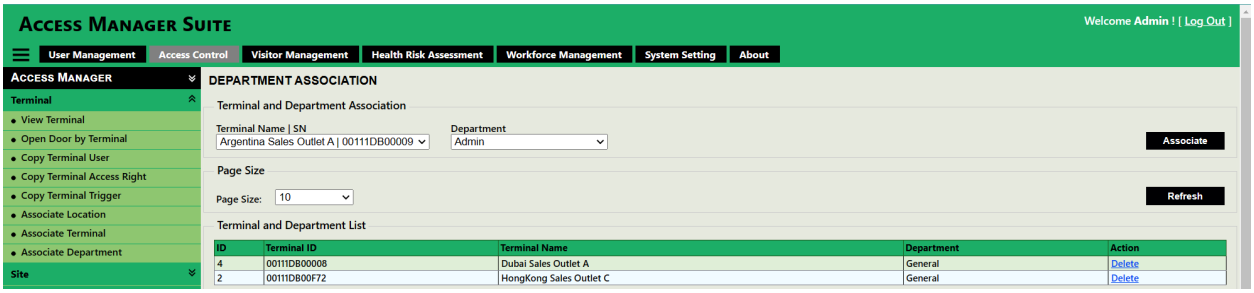
Appendix: J. Facial Finger Print Self-Enrollment

Accurately enrolling and verifying a person's identity is essential, and made all the easier through biometrics. Onboarding new users, visitors, Contractors, customers and employees is a critical function for many privet and government sectors.

AMS facial fingerprint enrollment function is saves time, improves convenience, and ensures a positive, simple user experience for employees. This can be use Whether your employee is migrating to face recognition from another access credential, a first-time enrollment, or simply bringing employees back to work in-person

In order to use the AMS Self Enrollment, feature the admin needs to make sure the ACTAtek device is associated with a particular department.

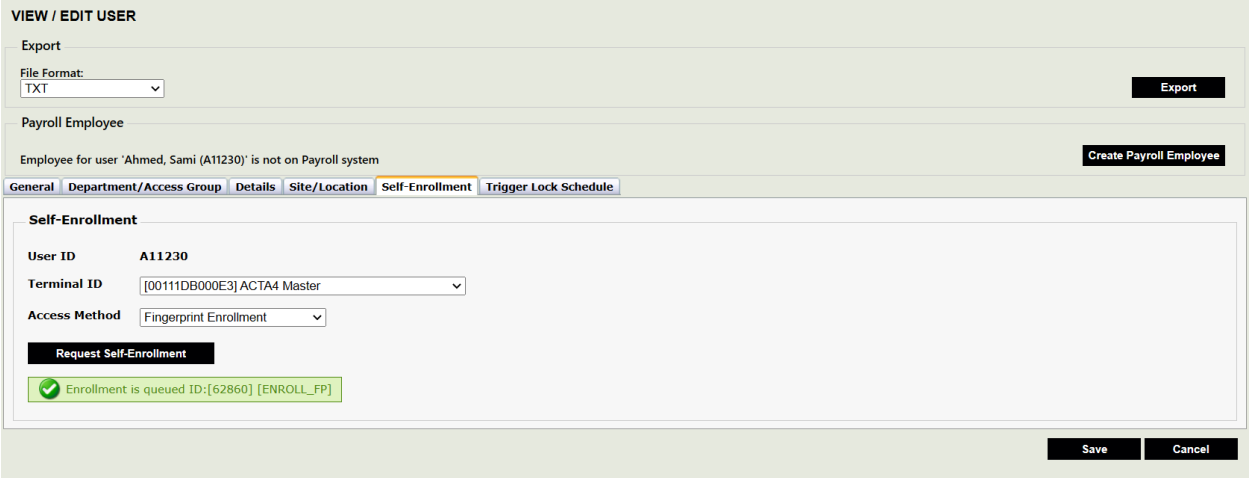
AMS Associate Department: -
https://localhost/AccessManager/ACTAtekAccessManager/frmTerminalDept.aspx



Then go to the **View/Edit** user and click on edit. Select the **self -enrollment** tab from edit user screen. Now the admin can select the **Terminal ID** and the **Access Method** and then select the **Request Self-Enrollment** to send out the Facial / Fingerprint enrollment request to remote location ACTAtek device where employee (user) working.

When the AMS hosted in privet/public cloud, The ACTATEK devices can receive the AMS face/fingerprint self-enrollment requests over internet.

https://localhost/AccessManager/UserManagement/frmEditUser.aspx



The employee When the AMS hosted in privet/public cloud, The ACTATEK devices can receive the AMS face/fingerprint self-enrollment requests over internet.

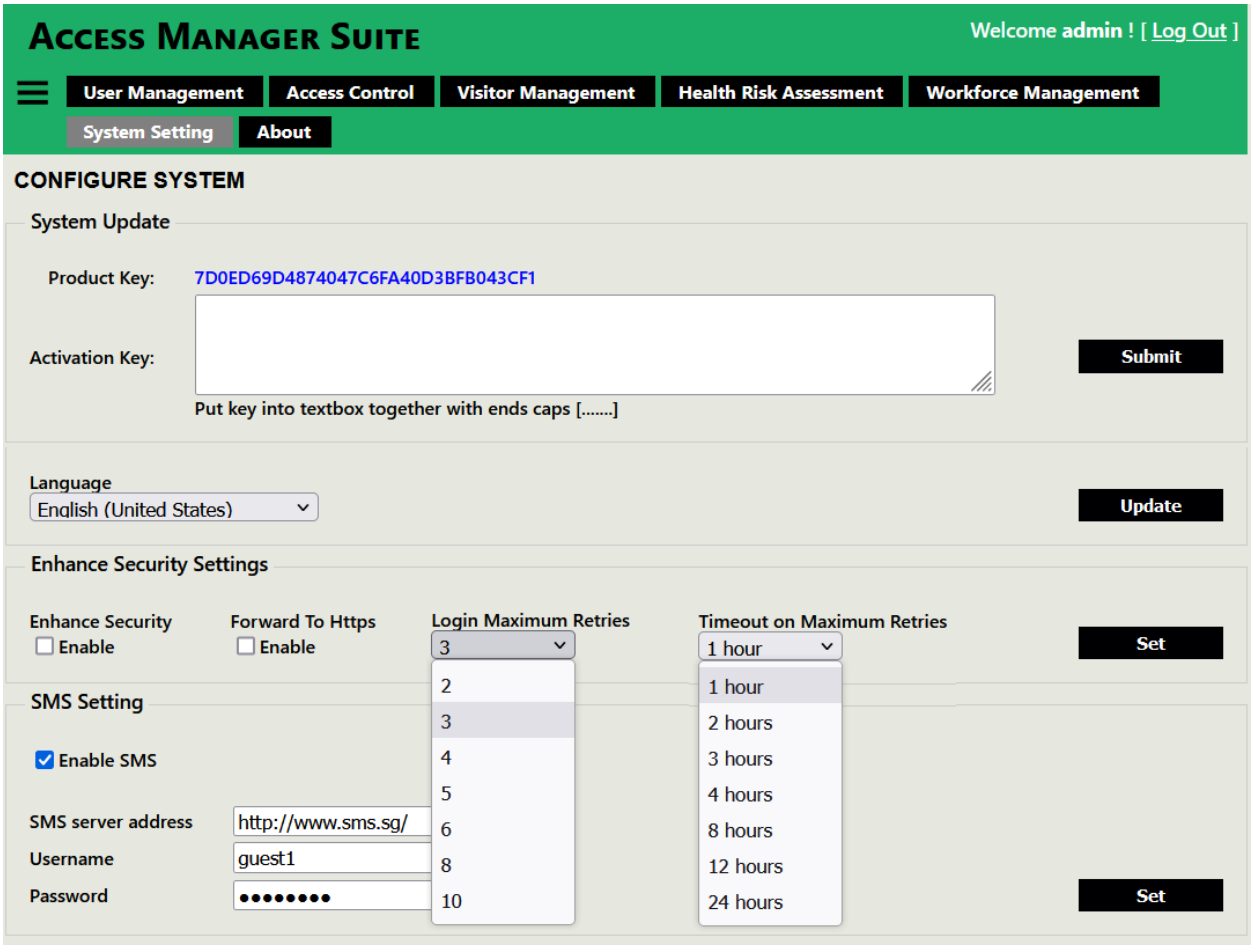
Remote face enrollment saves time, improves convenience, and ensures a positive, simple user experience for employees. Whether your company is migrating to face recognition from another access credential, a first-time installation, or simply bringing employees back to work in-person

Appendix: K. AMS Enhance security settings

Establishes AMS Enhance security settings that define how users browse the AMS via a Web browser.

Once enabled AMS Enhance Security Settings: -

- **Forward Http to Https automatically for all AMS UI requests**
- **Limit number of Login Failure retries**
- **Set Wait time in hours after reached Maximum Login Failure Retries**



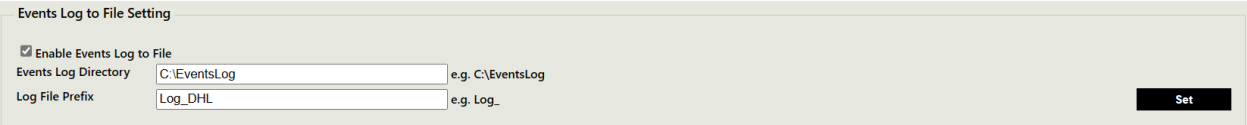
Appendix: L. Events Log to File Setting

Log management has become one of the biggest use cases for big data solutions and integrations. AMS now allow the customer to save the IN/OUT attendance events to a log file for further integrations.

To enable this feature, Please create a folder as ''**EventsLog**''to save the logs in the following path **C:\ drive** and the Directory for Events Log files and Log file prefix can be set at AMS System Configuration screen, at **Control Panel > Configure System** screen.

http://localhost/AccessManager/Account/SystemUpdate.aspx

NOTE:- Ensure the Events Log folder at drive C:/ is having full permissions to AMS IIS Users, administrators. Events Log to File configuration changes will not be effective until AMS server IIS is restarted.



Once the function has enabled, AMS Will write a single line of log per event in the file with following format **Example:- 0008312903202123:03:0002**

<6 Digit AMS Employee ID><ddMMyyyyhh:mm:ss><EventID> (IN=01, OUT=02)

Please refer to below Example log line per event