

SaaS Access Manager Suite User Manual

The Ultimate SaaS Solution for Managing
All ACTatek Devices



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

Copyright 2010-2020 Jakin Technology Limited. All rights reserved.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without prior written permission of Jakin Technology Limited.

JakinID is a registered trademark of Jakin Technology Limited.

All trademarks, registered trademarks, and service marks are the property of the respective owners.

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:

Revision History	2
JakinID Access Manager Suite User Manual	4
Contents:	6
Chapter 1: Overview	10
1.1 SaaS AMS Introduction	10
1.2 System Requirements.....	11
1.3 Microsoft .Net Framework Requirements	11
Chapter 2: Configuring SaaS Access Manager Suite	12
2.1 Accessing AMS	12
2.2 Activate AMS	12
2.3 Log into AMS.....	13
2.4 Setup Database In AMS	13
2.4.1 Setup SQL Database Server	14
2.4.2 Setup Oracle Database.....	15
2.5 Server Setup In AMS.....	16
2.6 Add New AMS Domain	17
2.6 Add New AMS Login Accounts	17
2.7 Assign Permission To AMS Login Accounts	18
2.8 Login to AMS as Domain User.	18
Chapter 3: Configuring ACTA Series of Products	19
3.1 Accessing the ACTA Web Interface.....	19
.....	19
3.2 View Device Information	19

3.3 Enable Access Manager Mode	19
3.4 Register Acta Series of Products to SaaS AMS.....	20
3.5 Assigning Time Zones to Acta Series of Products.....	24
Chapter 4: Access Manager Suite Functionalities.....	25
4.1 Auto User Synchronization	25
4.2 Add Users.....	25
4.3 View/Edit User	26
4.4 Bulk Edit Users	26
4.5 Add/Edit/Delete Departments.....	27
4.6 Add/Edit/Delete Access Group	28
4.7 Add Access Right	28
4.8 View/Edit Access Right	30
4.9 Edit Triggers	30
4.10 Trigger Schedule Setup	30
4.11 Holiday Setup.....	31
4.12 Door Open Schedule.....	31
4.13 Bell Schedule.....	32
4.14 View Event Logs	32
4.15 Add Manual Event Logs	33
4.16 View/Delete Manual Event Logs	33
4.17 View Terminal List	33
4.18 Copy Terminal User	33
4.19 Copy Group Access Right	34
4.20 Copy Trigger	34
4.21 Department Association	34

4.22 Data Import.....	34
Chapter 5: Access Manager Workforce Management	36
5.1 Reports	36
5.2 Lunch In/Out	37
5.3 Access Manager Suite Work force Management Shift Manager – Access Application.....	38
5.3.1 Create New Shifts	38
5.3.2 View/Edit Shifts.....	39
5.3.3 Assign Shifts to Employees.....	40
5.3.4 Reporting	41
Chapter 6: Access Manager Suite Workforce Management and Access Control Advance Features	43
6.1 APB Requirements.....	43
6.2 Auto In/Out	43
6.3 Anti-Passback.....	44
6.4 User Message.....	45
6.5 Send Email	45
Chapter 7: Backup AMS Database.....	48
7.1 Database Backup.....	49
Appendix A. Site/Location Feature	51
Appendix B. Late IN Early OUT Notification (Email SMS)	54
Appendix C. Configure Access Manager Crowd Control Occupancy Limit and Notification.	57
Appendix D. Open Door by Terminals.	60
Appendix E. Visitor Registration	60
Appendix F. Anti-Pass Back Group.	63
Appendix: G. Health Risk Assessment.	66
Appendix: H. Time Off Management.....	68

Appendix: I. Payroll Management.....69

Appendix: J. Facial Finger Print Self-Enrollment.....70

Appendix: K. AMS Enhance security settings.....71

Appendix: L. Events Log to File Setting.....72

Chapter 1: Overview

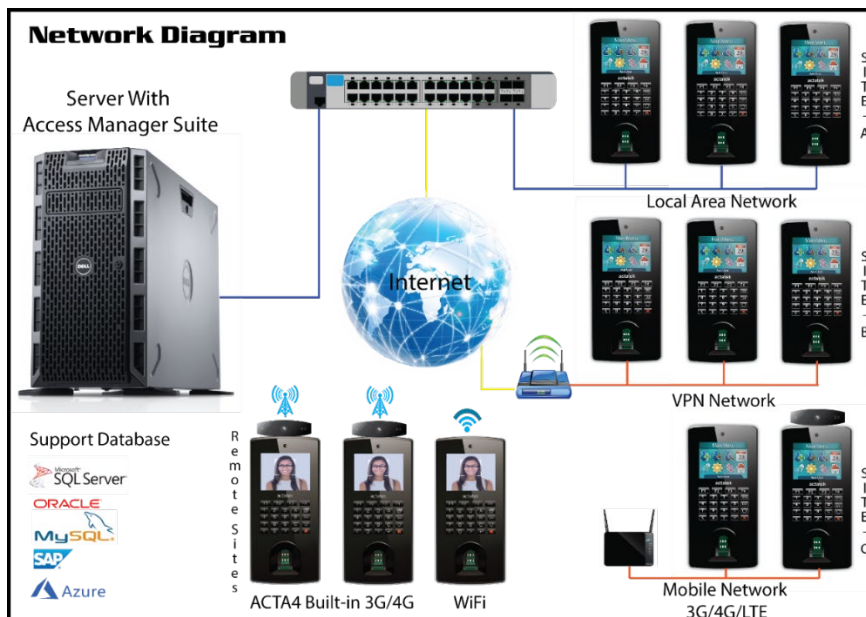
1.1 SaaS AMS Introduction

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 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 or 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

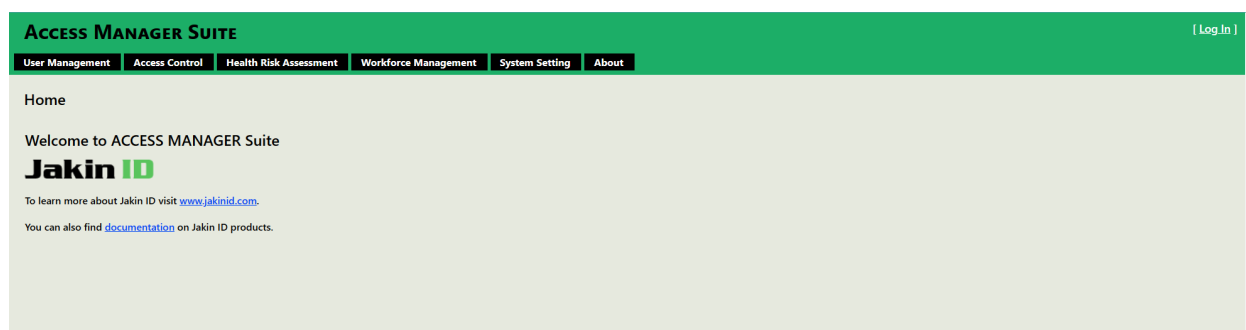
To download Microsoft .Net Framework, follow the link: <http://www.microsoft.com/net/downloads>

Chapter 2: Configuring SaaS Access Manager Suite

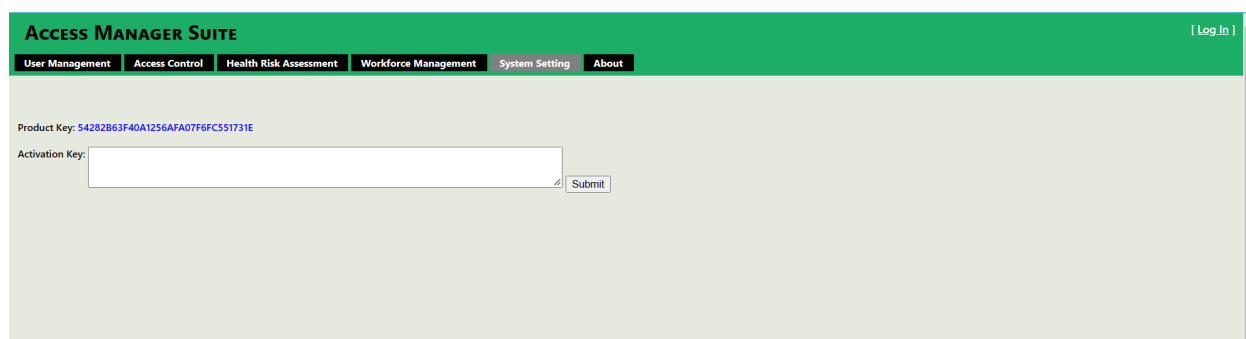
2.1 Accessing AMS

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

ACCESS MANAGER SUITE [Log In]

User Management Access Control Health Risk Assessment Workforce Management System Setting About

Log In
Please enter your Login ID and Password.

Account Information

Login ID: Admin

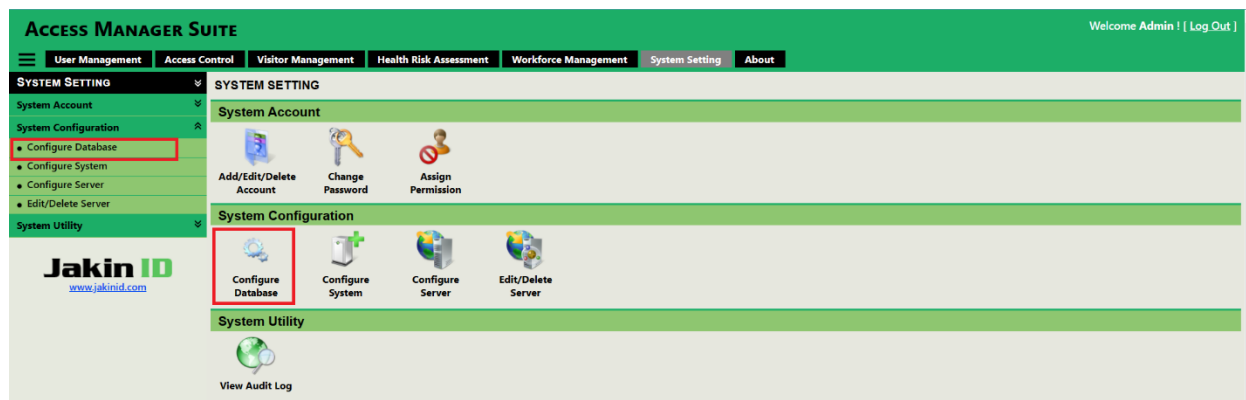
Password: •

☒ Keep me logged in

Log In

2.4 Setup Database In AMS

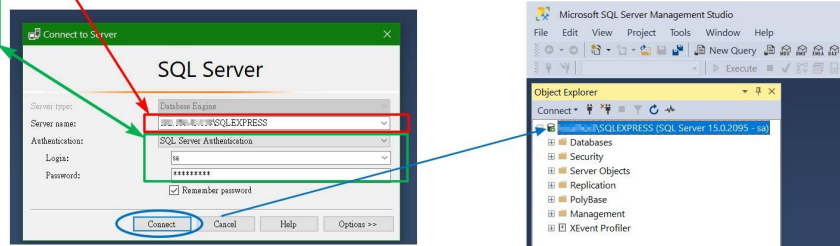
Once you've logged in as an administrator, go to **Control Panel** and then **Database Configuration**.



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 it 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

ACCESS MANAGER SUITE Welcome Admin ! [[Log Out](#)]

[Home](#) [Access Manager](#) [Visitor Registration](#) [Access Application](#) [Control Panel](#) [About](#)

CONTROL PANEL

- System Account
- System Configuration
 - Configure Database
 - Configure System
 - Configure Server
 - Edit/Delete Server
- System Utility

CONFIGURE DATABASE

- There is no terminal settings for current server[169.254.53.209], please go to [System Configuration - Server Setup] to setup

Access Manager Database

Database Type:

Database Server Address: **Host**

Database Server Instance: **Service Name**

User Name: **User ID**

User Password: **Password**

*Default port will be used if left blank

Port:

DATABASE SETUP SUMMARY

- Checking existence of database: [AMSCrowdControl20200614CleanDB4]
- Using database server: DESKTOP-99RD5D0\SQLXPRESS2017
- Database does not exist
- Creating database...
- Database is created successfully

2.5 Server Setup In AMS

ACCESS MANAGER SUITE Welcome Admin ! | Log Out |

SYSTEM SETTING

- System Account
- System Configuration
 - Configure Database
 - Configure System
 - Configure Server
 - Edit/Delete Server
- System Utility

CONFIGURE SERVER

Terminal [Access Server] Settings

Terminal Group
Sales Outlet

Server IP Address Detected IP Address: [192.168.56.1]([192.168.1.18])
192.168.56.1

Date / Time Settings

Time Zone
(GMT -08:00:00) Pacific Time (US & Canada)

☐ Enable SNTP Server
Type SNTP Server Here

Body Temperature Monitoring

High Body Temperature Threshold (°C)
37.50 e.g. 37.50

Event Log Settings

Agent Server IP Address
192.168.56.1

Agent Server IP Address Port
80

Magic String

End Point URL
/AccessServer/AgentService.asmx

Setup

Copyright © 2010 - 2020 Jakin Technology Limited. All Rights Reserved.

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.

ACCESS MANAGER SUITE Welcome Admin ! | Log Out |

SYSTEM SETTING

- System Account
- System Configuration
 - Configure Database
 - Configure System
 - Configure Server
 - Edit/Delete Server
- System Utility

CONFIGURE SERVER

Terminal [Access Server] Settings

Terminal Group
Sales Outlet

Server IP Address Detected IP Address: [192.168.56.1]([192.168.1.18])
192.168.56.1

Date / Time Settings

Terminal group[Sales Outlet] is added successfully

Jakin ID
www.jakinid.com

2.6 Add New AMS Domain

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

ACCESS MANAGEMENT SUITE Welcome Admin! [Log Out]

ACCESS MANAGER ADD / EDIT / DELETE DOMAIN

Domain Name: Description:

Product Key: 26BBBA6E3A77E90E27E563C7129F50D

ID	Domain Name	Description	Action
1	JakinIDRmd	JakinIDRmd	Edit Delete
2	JakinIDCA	JakinIDCA	Edit Delete
4	TSheetsCA	TSheetsCA	Edit Delete
8	SLO	SLO	Edit Delete
9	Test	Test	Edit Delete
10	Canberra	Canberra	Edit Delete
13	TWN	TWN	Edit Delete
14	LTPDEMO	Lufthansa Technik Phils demo	Edit Delete
15	parka	parka	Edit Delete
17	DHL Qatar	Qatar Regional Office	Edit Delete
18	OTCDEMO	OTC demo	Edit Delete
19	HKO	HKO	Edit Delete
20	HKO2	HKO2	Edit Delete
21	HKO3ACTA4	HKO3ACTA4	Edit Delete
24	El Sewedy	El Sewedy	Edit Delete

Copyright © 2010 - 2020 Jakin Technology Limited. All Rights Reserved.

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**.

ACCESS MANAGER SUITE Welcome Admin! [Log Out]

SYSTEM SETTING ADD / EDIT / DELETE ACCOUNT

Account Information

Login ID: Name: Password: Department:

☐ Administrator ☒ Active

Register

Login ID	Name	Password	Department	Administrator	Active	Action
A999	Administrators	***	All Departments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete
Admin	Demo	***	All Departments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete
HR	HR	***	All Departments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete
IT	IT	***	All Departments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete
Nancy	Nancy Adam	***	All Departments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete
Payroll	Payroll	***	All Departments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete
Test	Test	***	All Departments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete

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.

The screenshot shows the 'ACCESS MANAGER SUITE' interface. The top navigation bar includes 'Home', 'Access Manager', 'Visitor Registration', 'Access Application', 'Control Panel', and 'About'. The 'Control Panel' is selected, and the 'Assign Permission' section is active. A table lists users: Admin, HR, and QA. The 'HR' user is selected, and the 'Permission Details' for 'Login ID: HR' are shown. The 'Access Manager' tab is active, displaying a list of permissions with checkboxes to allow or deny access. The 'Apply' button is at the bottom right.

Permission Name	Allow
User	
Add User	<input checked="" type="checkbox"/>
View/Edit User	<input checked="" type="checkbox"/>
Bulk Edit User	<input checked="" type="checkbox"/>
Department	
Add/Edit/Delete Department	<input checked="" type="checkbox"/>
Groups & Access Rights	
Add/Edit/Delete Access Group	<input checked="" type="checkbox"/>
Add Access Right	<input checked="" type="checkbox"/>
View/Edit Access Right	<input checked="" type="checkbox"/>
Triggers & Holidays	
Edit Trigger	<input checked="" type="checkbox"/>
Configure Trigger Schedule	<input checked="" type="checkbox"/>
Configure Holiday	<input checked="" type="checkbox"/>
Visitor Manager	
Register Visitor	<input checked="" type="checkbox"/>
View/Edit Visitor	<input checked="" type="checkbox"/>
Door & Bell Schedule	

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

The screenshot shows the 'ACCESS MANAGEMENT SUITE' login page. The top navigation bar includes 'User Management', 'Access Control', 'Health Risk Assessment', 'Workforce Management', 'System Setting', and 'About'. The 'LOG IN' section is active, and the user is prompted to enter their Login ID and Password. The 'Domain Name' is set to 'JakinIDCA'. The 'Log In' button is at the bottom right.

LOG IN
Please enter your Login ID and Password.

Account Information

Login ID: Admin

Password: •

Domain Name: JakinIDCA

☐ Keep me logged in

Log In

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.

ACTatek Web Interface > Terminal Setup

- view User List
- Add New User
- Departments
- User Messages

Access Control

- Access Groups
- Triggers
- Holidays Setting

Terminal Settings

- Terminal Setup**
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule

Miscellaneous

Terminal Mode ☐ Stand Alone ☒ Access Manager

Job Code ☒ Disable ☐ Enable

Door Strike 1 Option ☐ Disable ☒ Access Granted ☐ Emergency

Relay Delay 8 sec (1-20)

☐ Disable

☒ Door Strike 1 Clone

☐ Access Denied

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](http://IP ADDRESS OF AMS:80/AccessServer/AccessService.asmx)

Example: [http:// 192.168.0.14:80/AccessServer/AccessService.asmx](http://192.168.0.14:80/AccessServer/AccessService.asmx)

ACTatek The worldwide leader in Web based technologies.

Terminal

- Log Off
- Terminal Status
- Add Record

User Administration

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages
- Admin Setting

Access Control

ACCESS Client Setup

Connection Type Lan

Access Client

Device Status Unregistered

Server Status Offline or unreachable...

Endpoint URL http://192.168.1.10/AccessServer/AccessService.asmx

Interval(Seconds) 10

Domain Name Enable ☒

Domain Name

Set

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

ACTatek The worldwide leader in Web based technologies.

Terminal <ul style="list-style-type: none"> Log Off Terminal Status Add Record User Administration <ul style="list-style-type: none"> Attendance Report Daily Report View Event Log Add Event Log View User List Add New User Departments User Messages Admin Setting Access Control <ul style="list-style-type: none"> Access Groups 	<h3>ACCESS Client Setup</h3> <p>[Save settings successfully...]</p> <table> <tr> <td>Connection Type</td> <td>Lan</td> </tr> <tr> <td>Access Client</td> <td></td> </tr> <tr> <td>Device Status</td> <td>Unregistered</td> </tr> <tr> <td>Server Status</td> <td>Online</td> </tr> <tr> <td>Endpoint URL</td> <td>http://192.168.1.90/AccessServer/AccessService.asmx</td> </tr> <tr> <td>Interval(Seconds)</td> <td>10</td> </tr> <tr> <td>Domain Name Enable</td> <td><input type="checkbox"/></td> </tr> </table> <p> <input type="button" value="Set"/> <input type="button" value="Register"/> </p>	Connection Type	Lan	Access Client		Device Status	Unregistered	Server Status	Online	Endpoint URL	http://192.168.1.90/AccessServer/AccessService.asmx	Interval(Seconds)	10	Domain Name Enable	<input type="checkbox"/>
Connection Type	Lan														
Access Client															
Device Status	Unregistered														
Server Status	Online														
Endpoint URL	http://192.168.1.90/AccessServer/AccessService.asmx														
Interval(Seconds)	10														
Domain Name Enable	<input type="checkbox"/>														

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.

Terminal <ul style="list-style-type: none"> Log Off Terminal Status Add Record User Administration <ul style="list-style-type: none"> Attendance Report Daily Report View Event Log Add Event Log View User List Add New User Departments User Messages Admin Setting Access Control <ul style="list-style-type: none"> Access Groups Triggers 	<h3>ACCESS Client Setup</h3> <p>[Save settings successfully...]</p> <table> <tr> <td>Connection Type</td> <td>Lan</td> </tr> <tr> <td>Access Client</td> <td></td> </tr> <tr> <td>Device Status</td> <td>Unregistered</td> </tr> <tr> <td>Server Status</td> <td>Online</td> </tr> <tr> <td>Endpoint URL</td> <td>http://192.168.1.10/AccessServer/AccessService.asmx</td> </tr> <tr> <td>Interval(Seconds)</td> <td>10</td> </tr> <tr> <td>Domain Name Enable</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Domain Name</td> <td>Client A</td> </tr> </table> <p> <input type="button" value="Set"/> <input type="button" value="Register"/> </p> <div style="border: 1px solid blue; padding: 2px; width: fit-content; margin-top: 5px;">Client A</div>	Connection Type	Lan	Access Client		Device Status	Unregistered	Server Status	Online	Endpoint URL	http://192.168.1.10/AccessServer/AccessService.asmx	Interval(Seconds)	10	Domain Name Enable	<input checked="" type="checkbox"/>	Domain Name	Client A
Connection Type	Lan																
Access Client																	
Device Status	Unregistered																
Server Status	Online																
Endpoint URL	http://192.168.1.10/AccessServer/AccessService.asmx																
Interval(Seconds)	10																
Domain Name Enable	<input checked="" type="checkbox"/>																
Domain Name	Client A																

Copyright © 2012

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

Terminal <ul style="list-style-type: none"> Log Off Terminal Status Add Record User Administration <ul style="list-style-type: none"> Attendance Report Daily Report View Event Log Add Event Log View User List Add New User Departments User Messages Admin Setting Access Control	<h3>Device Registration</h3> <p>Synchronization in progress</p> <p>Please DO NOT power off the ACTatek device!</p> <p style="text-align: center;">starting slave device registration...</p> <p style="text-align: center;">Progress</p> <div style="border: 1px solid orange; width: 200px; height: 15px; margin: 10px auto;"></div>
---	--

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.

ACTatek The worldwide leader in Web based technologies.

The screenshot displays the 'ACCESS Client Setup' web interface. On the left is a navigation menu with categories: 'Terminal' (Log Off, Terminal Status, Add Record), 'User Administration' (Attendance Report, Daily Report, View Event Log, Add Event Log, View User List, Add New User, Departments, User Messages, Admin Setting), and 'Access Control' (Access Groups). The main content area shows the 'ACCESS Client Setup' page with a red message: '[slave device registration succeeded...]'. Below this, the configuration details are listed: Connection Type (Lan), Access Client (highlighted), Device Status (Registered), Server Status (Online), Endpoint URL (http://192.168.1.90/AccessServer/AccessService.asmx), Interval(Seconds) (10), and Domain Name Enable (unchecked). At the bottom of the configuration section are 'Set' and 'Unregister' buttons.

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

TERMINAL LIST

System Information

Number of registered terminals: 3 Refresh

Export

File Format:
 Export

Search Option

Terminal Serial Number <input type="text"/>	Terminal Name <input type="text"/>	Terminal IP <input type="text"/>	<input checked="" type="checkbox"/> Partial Terminal Name, Serial Number, IP
Department <input type="text" value="-- All --"/>	Department Name <input type="text"/>	Department Description <input type="text"/>	<input checked="" type="checkbox"/> Partial Department Name, Description

Search

Terminal List

Page Size:

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	
00111DB007f2	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.

ACCESS MANAGER SUITE Welcome Admin! [Log Out]

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

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 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	
00111DB00072	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	

Terminal Details

Pending Synchronization Request(s): 0

Terminal Settings

ID: 00111DB00008 Name: Lift Access Reader

SN: 00111DB00008 No Timezone

Group: AMSHostPC (GMT -12:00:00) Eniwetok, Kwajalein

Model: A-100K-FSM-C-WI (GMT -11:00:00) MidwayIsland, Somosa

(GMT -10:00:00) Hawaii

(GMT -09:00:00) Alaska

(GMT -08:00:00) Pacific Time (US & Canada)

(GMT -08:00:00) Tijuana, Baja California

(GMT -07:00:00) Mexican Standard Time; Chihuahua, La Paz, Mazatlan

(GMT -07:00:00) Mountain Standard Time (US & Canada)

(GMT -07:00:00) Arizona

(GMT -06:00:00) Central Standard Time (US & Canada)

(GMT -06:00:00) Mexico City, Tegucigalpa

(GMT -06:00:00) Saskatchewan

(GMT -06:00:00) Central America

(GMT -05:00:00) Eastern Standard Time (US & Canada)

(GMT -05:00:00) Eastern Standard Time, Indiana (East)

(GMT -05:00:00) Bogota, Lima, Quito

(GMT -04:00:00) Atlantic Standard Time (Canada)

(GMT -04:30:00) Caracas, La Pa

(GMT -04:00:00) Santiago

Timezone: (GMT +05:30:00) Bombay, Calcutta, Madras, New Delhi

High Body Temperature Threshold °C, e.g. 37.50: 37.50

Terminal Access IP : Port: 192.168.1.121 : 80

Resynchronize User Update to Terminal Update

Refresh Close

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.



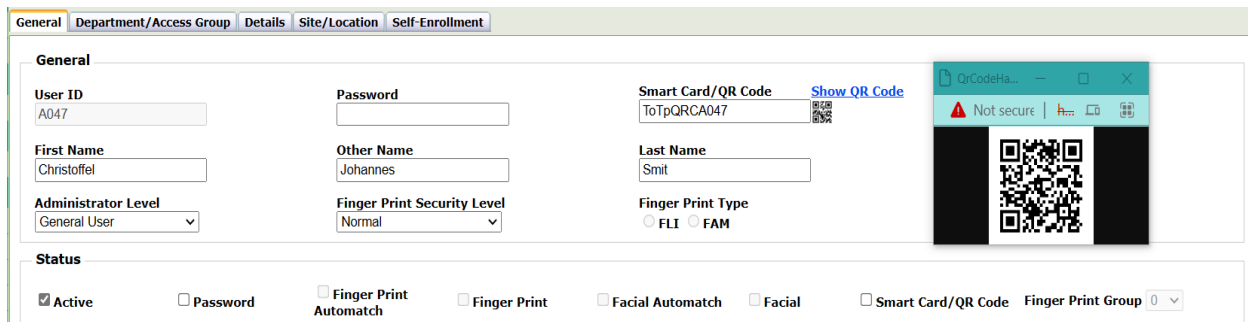
Anti-Passback Setting

Type: Update

Trigger: Update

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.



General | Department/Access Group | Details | Site/Location | Self-Enrollment

General

User ID: Password:

Smart Card/QR Code: [Show QR Code](#)

First Name: Other Name: Last Name:

Administrator Level: Finger Print Security Level:

Finger Print Type: ☐ FLI ☐ FAM

Status

☒ Active ☐ Password ☐ Finger Print Automatch ☐ Finger Print ☐ Facial Automatch ☐ Facial ☐ Smart Card/QR Code Finger Print Group:

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

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

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

ACCESS MANAGER **BULK EDIT USER**

Site Location User

Department Access Group User ID

Access Method Facial Finger Print Smart Card Password

The searching process may take a while...

Refresh

User ID	Last Name	First Name	Active	Facial	Facial Automatch	Finger Print	Finger Print Automatch	Smart Card	Password	Finger Print Security Level
AB007	Face	Test								Normal
6666										Normal
83000018	الهيلى	ابراهيم								Normal
83000030	النعيمى	خليفة								Normal
83000034	الهجرى	موزة								Normal
83000037	الكبرى	سعد								Normal
83000040	الشيخ	حسن								Normal
83000041	العمادى	على								Low
83000042	الجهنى	اسماء								Low
83000044	اليوسف	عبدالله								Normal
83000046	التميمى	مرىم								Normal
83000047	السوى	خليفة								Normal
83000048	الغنى	احمد								Normal
83000049	جوهري	سلطان								Low
83000050	المريشى	على								Normal
83000051	الجمد	ابراهيم								Normal

Finger Print Security Level **Set**

Active Status **Set**

Facial Status **Set**

Facial Automatch Status **Set**

Finger Print Status **Set**

Finger Print Automatch Status **Set**

Smart Card Status **Set**

Password Status **Set**

Department **Set**

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.

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

ACCESS MANAGER **ADD / EDIT / DELETE DEPARTMENT**

Add Department

Department Name Description Parent Department

Type Department Name Here Type Description Here -- Head --

Add

Collapse Department List

Department Name	Description	Parent Department	Actions
EMERGENCY	Emergency Group	-- Head --	Edit
General	General	-- Head --	Edit
Admin	Administrator	-- Head --	Edit Delete
Engineer	Engineering	-- Head --	Edit Delete
H.R.	Human Resources	-- Head --	Edit Delete
Marketing	Marketing	-- Head --	Edit Delete
Production	Production	-- Head --	Edit Delete
Sales	Sales	-- Head --	Edit Delete

Department Organization

Departments

- ☐ [-2-EMERGENCY_Emergency Group]
- ☐ [0-General_General]
- ☐ [1-Admin_Administrator]
- ☐ [2-Engineer_Engineering]
- ☐ [3-H_R_Human Resources]
- ☐ [4-Marketing_Marketing]
- ☐ [5-Production_Production]
- ☐ [6-Sales_Sales]

Update **Delete**

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.

ADD ACCESS RIGHT

Access Right Information

Access Right Name

HR

Department | Access Group

H.R. | General Staff

Terminal Name | SN

A4 Master 2024 | 00111DB000B9

Quick Access:

☒ Enable
 ☐ Disable

Add

Access Right Time Schedule

Existing Access Right Schedule:

<-- Please select -->

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.

ADD ACCESS RIGHT

Access Right Information

Access Right Name

Main Entrance

Department | Access Group

H.R. | General Staff

Terminal Name | SN

ACTA3 Slave 1 | 00111DA04B26

Quick Access:

☒ Enable ☐ Disable

Add

Access Right Time Schedule

Existing Access Right Schedule: <-- Please select -->

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MON																								
TUE																								
WED																								
THU																								
FRI																								
SAT																								
SUN																								

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.

Access Right Time Schedule

Existing Access Right Schedule: <-- Please select -->

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MON																								
TUE																								
WED																								
THU																								
FRI																								
SAT																								
SUN																								
Holiday																								

Remarks: To setup Late In, Early Out Notification time, select day of week checkbox and click on the time-table to set start and end time.

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**.

ACCESS MANAGER	EDIT TRIGGER				
Site	Search Options				
Location	Terminal Name SN				
User	A4 Exit 02 00111DB00009				
Visitor	Search				
Department	Terminal ID	Trigger	Trigger Name	Status	Actions
Access Group and Access Right	00111DB00009	IN	IN	Enabled	Edit
Trigger and Holiday	00111DB00009	OUT	OUT	Enabled	Edit
• Edit Trigger	00111DB00009	F1	Lunch IN	Enabled	Update Cancel
• Configure Trigger Schedule	00111DB00009	F2	F2	Please Select...	Edit
• Configure Holiday	00111DB00009	F3	F3	Enabled	Edit
Door and Bell Schedule	00111DB00009	F4	F4	Enabled	Edit
	00111DB00009	F5	F5	Enabled	Edit
	00111DB00009	F6	F6	Disabled	Edit
	00111DB00009	F7	F7	Enabled	Edit
	00111DB00009	F8	F8	Enabled	Edit

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 Manager. 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.

ACCESS MANAGER		DOOR OPEN SCHEDULE																																																																																																																																																																																																																																		
Site	⌵	Select Terminal																																																																																																																																																																																																																																		
Location	⌵	Terminal Name SN <input type="text" value="A4 Exit 02 00111DB00009"/>																																																																																																																																																																																																																																		
User	⌵	Door Open Schedule																																																																																																																																																																																																																																		
Visitor	⌵	Time Schedule																																																																																																																																																																																																																																		
Department	⌵	Existing Door Open Schedule: <input type="text" value="Please Select -->"/>																																																																																																																																																																																																																																		
Access Group and Access Right	⌵	<table border="1"> <thead> <tr> <th>Day</th> <th>00</th><th>01</th><th>02</th><th>03</th><th>04</th><th>05</th><th>06</th><th>07</th><th>08</th><th>09</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th> </tr> </thead> <tbody> <tr> <td>Sun</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>•</td><td>•</td><td>•</td><td>•</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Mon</td> <td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td> </tr> <tr> <td>Tue</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>•</td><td>•</td><td>•</td><td>•</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Wed</td> <td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Thu</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>•</td><td>•</td><td>•</td><td>•</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Fri</td> <td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Sat</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>•</td><td>•</td><td>•</td><td>•</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td>Hol</td> <td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td>•</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </tbody> </table>		Day	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Sun									•	•	•	•													Mon	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	Tue									•	•	•	•													Wed	•	•	•	•	•	•	•	•	•	•	•	•													Thu									•	•	•	•													Fri	•	•	•	•	•	•	•	•	•	•	•	•													Sat									•	•	•	•													Hol	•	•	•	•	•	•	•	•	•	•	•	•												
Day	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23																																																																																																																																																																																																												
Sun									•	•	•	•																																																																																																																																																																																																																								
Mon	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•																																																																																																																																																																																																												
Tue									•	•	•	•																																																																																																																																																																																																																								
Wed	•	•	•	•	•	•	•	•	•	•	•	•																																																																																																																																																																																																																								
Thu									•	•	•	•																																																																																																																																																																																																																								
Fri	•	•	•	•	•	•	•	•	•	•	•	•																																																																																																																																																																																																																								
Sat									•	•	•	•																																																																																																																																																																																																																								
Hol	•	•	•	•	•	•	•	•	•	•	•	•																																																																																																																																																																																																																								
Door and Bell Schedule	⌵																																																																																																																																																																																																																																			
• Configure Door Schedule																																																																																																																																																																																																																																				
• Configure Bell Schedule																																																																																																																																																																																																																																				
Event Log	⌵																																																																																																																																																																																																																																			
Terminal	⌵																																																																																																																																																																																																																																			
Utility	⌵																																																																																																																																																																																																																																			

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.

ACCESS MANAGER

- Site
- Location
- User
- Visitor
- Department
- Access Group and Access Right
- Trigger and Holiday
- Door and Bell Schedule
- Event Log**
- View Event Log
- Add Manual Event Log
- View/Delete Manual Event Log
- Terminal

EVENT LOG

Event Log Status

Number of Event Logs in system: 138

Search Option

First Name

Type First Name Here

Last Name

Type Last Name Here

User ID

Type User ID Here

☐ Partial

Period

<-- Please select -->

OR

Start Date

End Date

Terminal Name | SN

<-- All -->

Department

<-- All -->

Event

<-- All -->

Access Method

<-- All -->

☒

Export

Search

Event Log								
Number of Event Logs: 138								
Timestamp	UserID	First Name	Last Name	Department	Event	Access Method	Terminal SN	Terminal
2020-06-21 9:03:31 PM	A999			General	CASE-IS-OPENED	Remote Door	00111DA04B26	ACTA3 Slave 1
2020-06-21 9:03:30 PM	A999			General	CASE-IS-CLOSED	Remote Door	00111DA04B26	ACTA3 Slave 1
2020-06-21 6:43:17 PM	AB007	Test	Face	General	OUT	Facial	00111DB00009	A4 Exit 02
2020-06-21 6:43:09 PM	AB007	Test	Face	General	IN	Facial	00111DB00009	A4 Exit 02
2020-06-21 5:37:30 PM	AB007	Test	Face	General	OUT	Facial	00111DB000BA	ACTA4 Entrance
2020-06-21 5:37:25 PM	AB007	Test	Face	General	IN	Facial	00111DB000BA	ACTA4 Entrance
2020-06-19 10:05:56 AM	AB007	Test	Face	General	OUT	Facial	00111DB00009	A4 Exit 02
2020-06-19 10:03:02 AM	AB007	Test	Face	General	IN	Facial	00111DB00009	A4 Exit 02
2020-06-19 9:38:29 AM	AB007	Test	Face	General	OUT	Facial	00111DB000BA	ACTA4 Entrance
2020-06-19 9:28:37 AM	AB007	Test	Face	General	IN	Facial	00111DB00009	A4 Exit 02

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.

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

TERMINAL LIST

System Information

Number of registered terminals: 3

Export

File Format: TXT

Search Option

Terminal Serial Number

Terminal Name

Terminal IP

☐ Partial Terminal Name, Serial Number, IP

Department

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	192.168.1.121-443	jakinid_4_00.2247	157/100000	2022-12-19 09:35:01 AM	Online	Details	
00111DB00009	Craftaria-A	A-100K-FA-FSM-WI	192.168.1.146	192.168.1.101-443	jakinid_4_00.2247	157/100000	2022-12-19 09:35:01 AM	Online	Details	
00111DB00072	Main Entrance - B	ACTA3-50K-FLI	192.168.1.131	192.168.1.131-443	actatek_3_06.2240	157/50000	2022-12-19 09:35:10 AM	Online	Details	

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.

Access Manager > Utilities > Data Import > Load CSV File								
P20 fx								
	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.

ACCESS MANAGER Site Location User Visitor Department Access Group and Access Right Trigger and Holiday Door and Bell Schedule Event Log Terminal Utility • Import Data Report	DATA IMPORT		
	CSV Option Data Mapping Setting Log		
	Mapping Option <input type="checkbox"/> Auto Generate User ID --Prefix-- Type Start Number Here		
	Data Mapping <div> <div>User ID <-- Please select --></div> <div>Password <-- Please select --></div> <div>First Name <-- Please select --></div> <div>Other Name <-- Please select --></div> <div>Card SN <-- Please select --></div> <div>Last Name <-- Please select --></div> </div>		

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.

Control Panel > System Configuration > APB Setting

Access Manager APB Setting

APB Setting: LUNCH IN/OUT

Lunch OUT: 12:00

Lunch IN: 13:00

Update

Reset All

IN

Update

Access Manager > Triggers & Holidays > Edit Triggers

Search Options

Terminal Name / SN
 ACTAtek / 00111DA04B19

[Search](#)

Terminal ID	Trigger	Trigger Name	Status	Actions
00111DA04B19	IN	IN	Enabled	Edit
00111DA04B19	OUT	OUT	Enabled	Edit
00111DA04B19	F1	LunchOUT	Enabled	Edit
00111DA04B19	F2	LunchIN	Enabled	Edit

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.

Access Apps > Shift Manager > Create Shift

Save **New**



Shift Details **Time Rounding**



Shift Name

Description



Shift Schedule


☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat ☐ Sun ☐ Hol

Start Time  Grace Period 

End Time  Grace Period 

Break Schedule

Start Time  End Time 

Break Length :  ☒ Enable Break

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.

Access Apps > Shift Manager > Edit Shift

View/Edit Shifts

Shifts

Refresh Update

	ID	Shift Name	Start Time	Shift End	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Hol	
Edit	1	Morning	07:00	16:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Delete

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**.

Access Apps > Shift Manager > Assign Employees Shifts

User ID First Name Last Name Shift Department

User List:

User ID	First Name	Last Name	Shift	Department
A999				
B11		James		

Filter

Shift

Shift User ID

Load Shift

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**.

Access Apps > Shift Manager > Assign Employees Shifts

Filter

User ID	First Name	Last Name	
A999			
B11		James	
B12	Mike		
B13			
B14			
C11			
C15			
C14			
1234	admin		
1325	admin		
2115	admin		

Shift

Morning

Load Shift

Assign Employee

Add >

Add All >>>

< Remove

<<< Remove All

Commit

Shift	User ID ▲
1	B11
1	B12
1	B13

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.

Access Apps > Shift Manager > View Report

Create Shift

Edit Shift

Employees

Assign Employee Shifts

Reporting

View Report

From: <M/d/yyyy> 15

To: <M/d/yyyy> 15

User ID:

Shift:

Load Report Data

Apply Grace Rounding

Apply Time Rounding

Generate Report

Export Report

User ID	First Name	Last Name	Shift Name	Day	Date
B12			Morning	Mon	2013-08-26
B11			Morning	Mon	2013-08-26
A999			Morning	Mon	2013-08-26
B13			Morning	Mon	2013-08-26

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.

Access Apps > Shift Manager > View Report

Report

☐ Apply Grace Rounding
☐ Apply Time Rounding

Generate Report Export Report

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

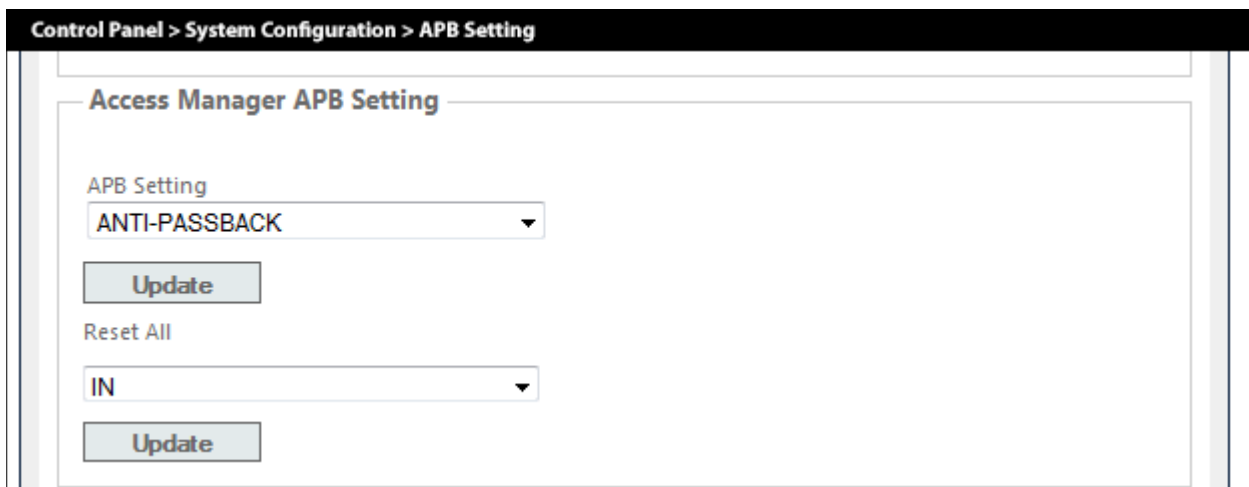
The **Auto In/Out** feature allows the ACTATEK terminal to use server-side authentication to automatically determine the IN or OUT status of a user during authentication and records a preceding punch event based on the user's previous event. To enable this feature, go into the **Control Panel** tab and 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.

The screenshot shows the 'Access Manager > View/Edit User > Edit > User Message' interface. It features a 'User Message' section with two input fields: 'Email Address' (containing 'Type Email Address Here') and 'Handphone Number' (containing 'Type Handphone Number He'). Below these are three checkboxes: 'Enable LCD' (checked), 'Enable SMS' (unchecked), and 'Enable Email' (unchecked). A 'Message :' label is followed by a text area containing 'Please pay your monthly rent by the end of the month.' and a character count 'You have 7 characters remaining for your message..'

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.

The screenshot shows the 'Control Panel > System Configuration > Email Setting' interface. It features an 'Email Setting' section with a checked 'Enable Email' checkbox. Below are four input fields: 'Email server' (smtp.gmail.com), 'Port' (25), 'User' (example@actatek.com), and 'Password' (masked with dots). A 'Set' button is located at the bottom right.

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.

Control Panel > System Configuration > Email Setting

Email Setting

Email setting saved

Email server: smtp.gmail.com

Port: 25

User: example@actatek.com

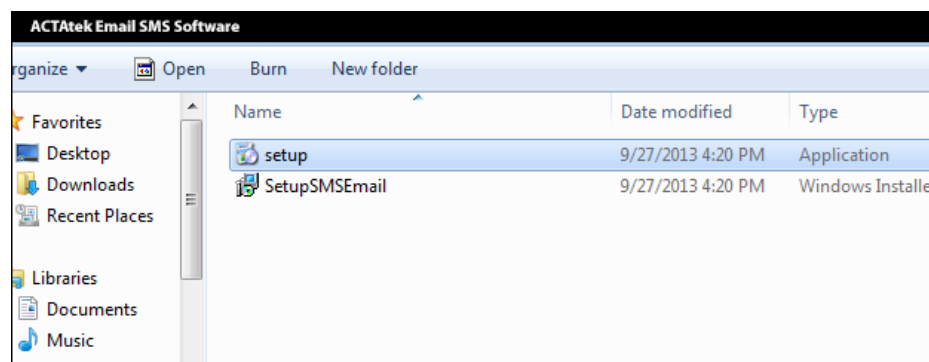
Password: ●●●●●●●●

Set

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.

The screenshot shows the 'Access Manager > View/Edit User > Edit > Email User Message' interface. It features a 'User Message' section with two input fields: 'Email Address' (containing 'james@gmail.com') and 'Handphone Number' (with a placeholder 'Type Handphone Number Here'). Below these are three checkboxes: 'Enable LCD' (unchecked), 'Enable SMS' (unchecked), and 'Enable Email' (checked). A 'Message :' field contains the text 'Meeting tomorrow at 9:00AM. Do not be late.' and a character count indicates 'You have 17 characters remaining for your message..'. At the bottom, there is an 'Expiry Date' field.

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: Handphone Number:

☐ 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

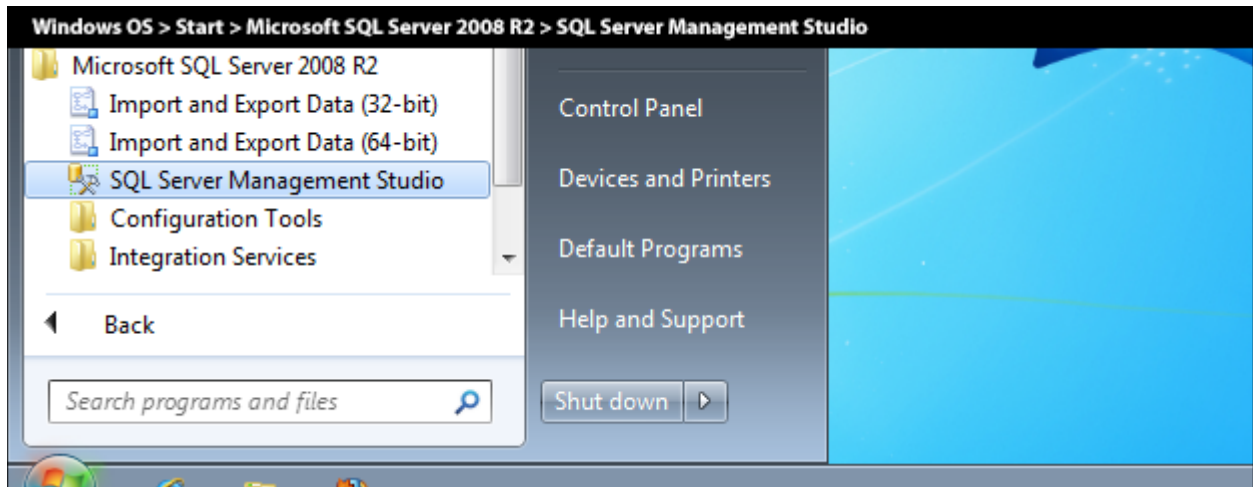
 **actatektest@gmail.com**
to threed94

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:

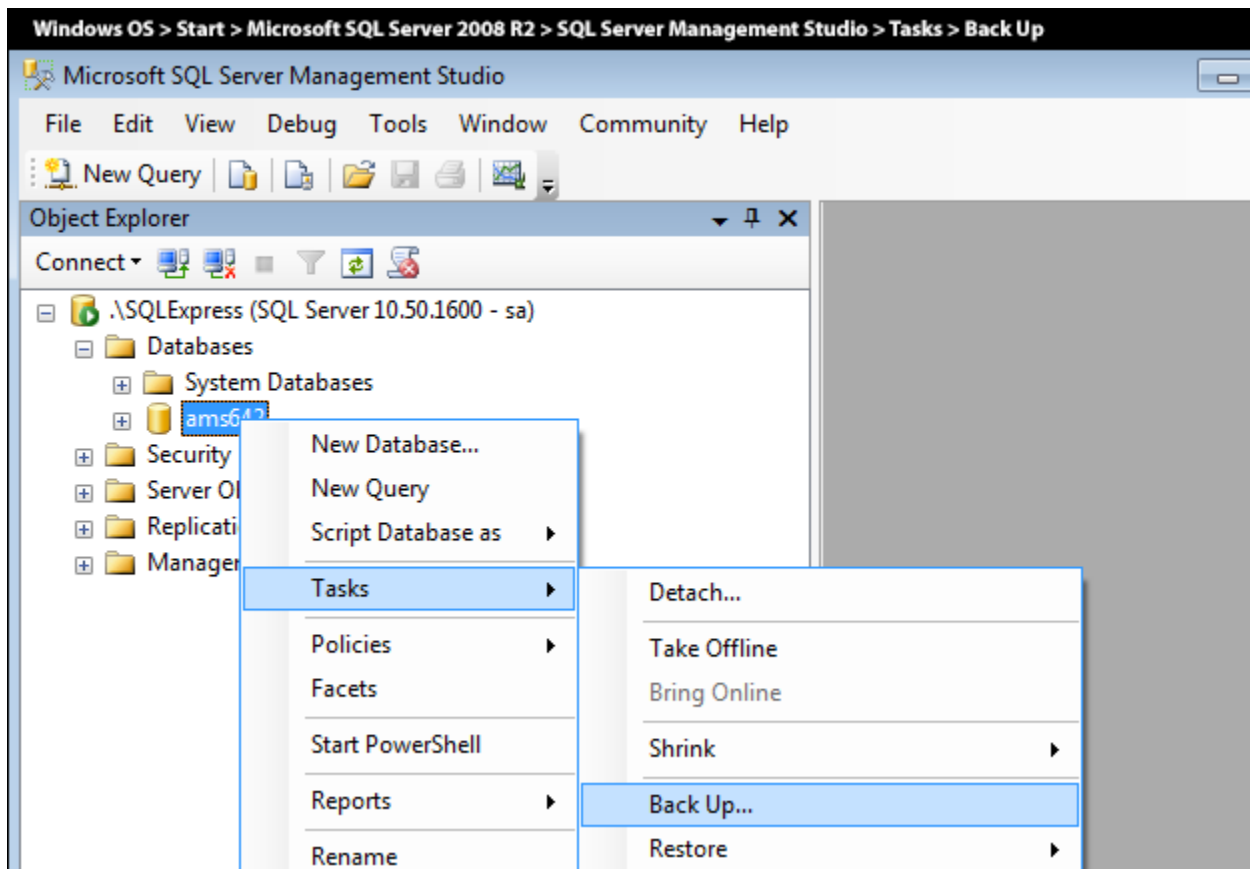
[Local Access] .\SQLExpress

or

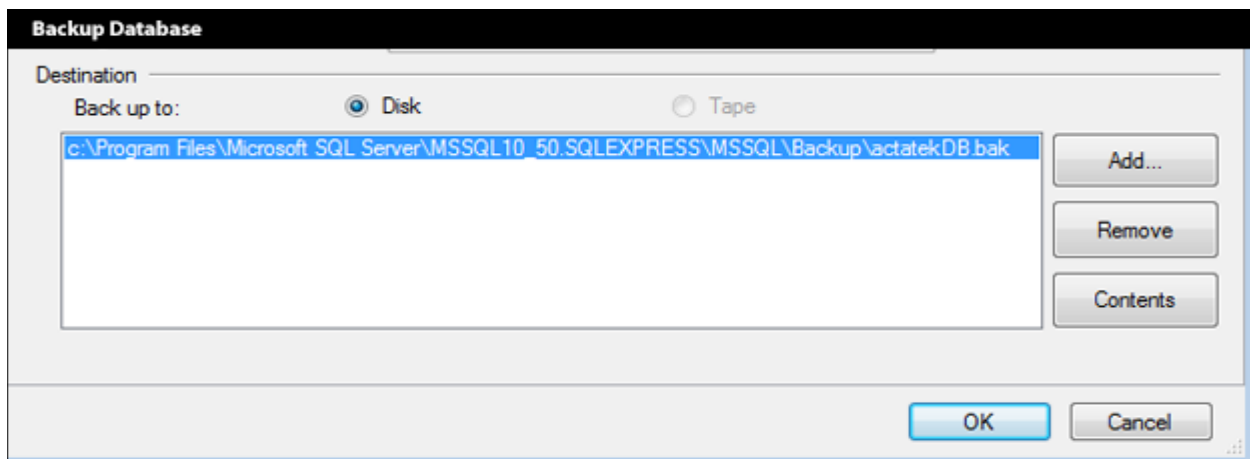
[Network Access] **IP ADDRESS OF SQL SERVER**\SQLExpress



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.

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

[User Management](#)
[Access Control](#)
[Visitor Management](#)
[Health Risk Assessment](#)
[Workforce Management](#)
[System Setting](#)
[About](#)

ACCESS MANAGER ▾ **ADD / EDIT / DELETE SITE**

Terminal ▾

Site ▾

• Add/Edit/Delete Site

Location ▾

Department ▾

Access Group and Access Right ▾

Trigger and Holiday ▾

Door and Bell Schedule ▾

Event Log ▾

Utility ▾

Report ▾

Site [KSA] has been added successfully

Add Site

Site Name Description

*Site name cannot be empty

Add

Site Name	Description	Action
Canada	Office	Edit Delete
USA	Office	Edit Delete
KSA	Office	Edit Delete

Jakin ID
www.jakinid.com

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.

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

[Home](#)
[Access Manager](#)
[Access Application](#)
[Control Panel](#)
[About](#)

ACCESS MANAGER ▾ **ADD / EDIT / DELETE LOCATION**

Site ▾

• Add/Edit/Delete Site

Location ▾

• Add/Edit/Delete Location

User ▾

Department ▾

Access Group and Access Right ▾

Trigger and Holiday ▾

Door and Bell Schedule ▾

Event Log ▾

Terminal ▾

Utility ▾

Location [Liver Pool] has been added successfully

Add Location

Location Name Description

Add

Location Name	Description	Action
New York	Branch	Edit Delete
London	Branch	Edit Delete
Los Angeles	Branch	Edit Delete
Liver Pool	Branch	Edit Delete

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.

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

Home Access Manager Access Application Control Panel About

ACCESS MANAGER

Site

Location Site has been associated with the specified location successfully

User

Department Site and Location Association

Access Group and Access Right Site Name | Description: UK | Office Location Name | Description: Associate

Trigger and Holiday Page Size

Door and Bell Schedule Page Size: 10 Refresh

Event Log

Terminal Site and Location List

ID	Site Name	Location ID	Location Name	Delete
1	USA	2	Los Angeles	Delete
2	USA	0	New York	Delete
3	USA	3	Liver Pool	Delete
4	UK	1	London	Delete

- View Terminal
- Open Door by Terminal
- Copy Terminal User
- Copy Terminal Access Right
- Copy Terminal Trigger
- Associate Location
- Associate Terminal
- Associate Department

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.

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

Home Access Manager Access Application Control Panel About

ACCESS MANAGER

Site

Location Location has been associated with the specified terminal successfully

User

Department Location and Terminal Association

Access Group and Access Right Location Name | Description: London | Branch Terminal Name | SN: ACTA4 Entrance | 00111DB000BA Associate

Trigger and Holiday Page Size

Door and Bell Schedule Page Size: 10 Refresh

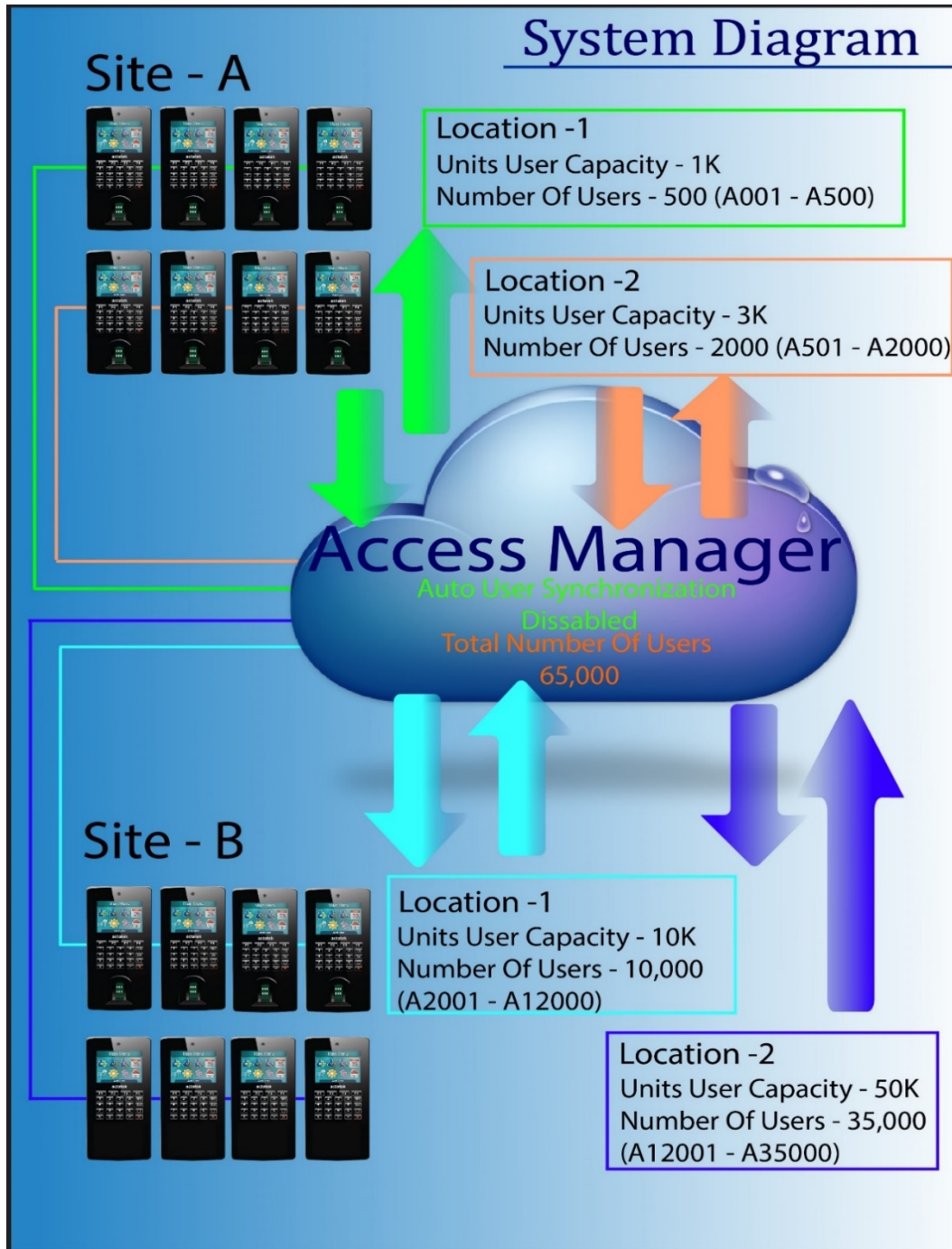
Event Log

Terminal Location and Terminal List

ID	Location Name	Terminal ID	Terminal Name	Delete
1	Liver Pool	00111DB000B9	A4 Master	Delete
2	London	00111DA04826	ACTA3 Slave 1	Delete

- View Terminal
- Open Door by Terminal
- Copy Terminal User
- Copy Terminal Access Right
- Copy Terminal Trigger
- Associate Location
- Associate Terminal
- Associate Department

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.

ACCESS MANAGER SUITE Welcome Admin | [Log Out]

Home Access Manager Access Application Control Panel About

ACCESS MANAGER

ADD ACCESS RIGHT

Access Right Information

Access Right Name: [Type Right Name Here] Department: [Access Group]

Terminal Name / SN: [Please select -->] Quick Access: ☒ Enable ☐ Disable

Access Right Time Schedule

Existing Access Right Schedule: [Please select -->]

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MON																								
TUE																								
WED																								
THU																								
FRI																								
SAT																								
SUN																								
Holiday																								

Remarks: To setup Late In, Early Out Notification time, select day of week checkbox and click on the time-table to set start and end time.

Day & Time

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Holiday ☐ Daily

From: [00] : [00] To: [00] : [29] Set: [Please select -->]

Modify Time

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.

ACCESS MANAGER SUITE

Welcome Admin | [Log Out]

ACCESS MANAGER

ADD ACCESS RIGHT

Access Right Information

Access Right Name: Department / Access Group: DCM / 06 / 16 / 05 Door 05

Late IN Early Out Notification: Terminal Name / SN: Atashah Independent Primary - Girls Quick Access: ☒ Enable ☐ Disable

Access Right Time Schedule

Existing Access Right Schedule: Please select

MON 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23

TUE

WED

THU

FRI

SAT

SUN

Holiday

Access Right Time Range Set in Green

Late IN and Early OUT set in Orange

Item note: to setup Late In, Early Out Notification time, select day of week checkbox and click on the time table to set start and end time.

Day & Time

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Holiday ☒ Daily

From: 00 To: 17 Set: Enable

Late In, Early Out Notification

Settings to Enable alert for Manager and User

Send to: ☐ Manager ☐ User

Send to: ☐ Manager ☐ User

Append message to User's Phone SMS and Email message if User's Notification has been configured.

Check box to send to user but also need to set SMS, Email on edit user screen

This is read-only text fields show up to indicate the time range of Late IN and Early OUT notification settings

Monday: ("Monday_08:59"ON;"Monday_16:58"OFF)

Tuesday: ("Tuesday_08:59"ON;"Tuesday_16:58"OFF)

Wednesday: ("Wednesday_08:59"ON;"Wednesday_16:58"OFF)

Thursday: ("Thursday_08:59"ON;"Thursday_16:58"OFF)

Friday: ("Friday_08:59"ON;"Friday_16:58"OFF)

Saturday: ("Saturday_08:59"ON;"Saturday_16:58"OFF)

Sunday: ("Sunday_08:59"ON;"Sunday_16:58"OFF)

Holiday: ("Holiday_08:59"ON;"Holiday_16:58"OFF)

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

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

Home **Access Manager** **Visitor Registration** **Access Application** **Control Panel** **About**

CONTROL PANEL

- System Account**
 - Add/Edit/Delete Account
 - Change Password
 - Assign Permission
- System Configuration**
 - Configure Database
 - Configure System
 - Configure Server
 - Edit/Delete Server
- System Utility**
 - View Audit Log

Jakin ID
www.jakinid.com

CONFIGURE SYSTEM

System Update

Product Key: A26C3CB197FD72BE9767C2CD24FD2E27
Activation Key: **Submit**

Access Manager Server Setting

Automatic Synchronization: **Update**

Anti-Passback Setting

Type: **AutoReset** ☒ **Enable Crowd Control** **Update**

DEFAULT **Update**

AUTO IN/OUT

ANTI-PASSBACK **Update**

LUNCH IN/OUT

TRIGGER LOCK

SMS Setting

☐ Enable SMS

SMS server address: **Set**

Username:

Password:

Email Setting

☐ Enable Email

Email server address:

Email server port:

Username:

Password: **Set**

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 15 minutes 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.

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

Home Access Manager Visitor Registration Access Application Control Panel About

ACCESS MANAGER

ADD / EDIT CROWD CONTROL GROUP

Add Search

Add Crowd Control Group

Crowd Control Group Name Remarks

Enable ☒ Occupancy Limit

Occupancy Level to send Notification Notification Interval

SMS Phone Email

Add

Group ID	Group Name	Remarks	Enable	Limit	Notification Occupancy	Notification Interval	Terminals Attached	Action
1	IT Department	Control	Enable	10	5	30 minutes	0	Edit Delete
2	Meeting Room	Test	Enable	30	7	15 minutes	2	Edit Delete

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.

ACCESS MANAGER SUITE Welcome Admin | [Log Out]

Home **Access Manager** **Access Application** **Control Panel** **About**

ACCESS MANAGER **OPEN DOOR BY TERMINAL**

System Information

Location: Number of registered terminals: 3 Clear All Status Refresh

User: Search Option

Department: Terminal Name Terminal Serial Number Terminal IP ☒ Partial Terminal Name, Serial Number, IP

Access Group and Access Right: Department Department Name Department Description ☒ Partial Department Name, Description

Trigger and Holiday: <-- All --> Search

Door and Bell Schedule: Access User Authentication

Event Log: Access User ID Password

Terminal: Authenticate with Access User ID. Password as on destination terminals to open door.

☒ Skip Offline terminals when select all

Terminals List Page Size: 10

<input checked="" type="checkbox"/>	Serial Number	Name	Model	URL Link	Firmware Version	Registered User	Last Update	Current Status	Action	Request Status
<input checked="" type="checkbox"/>	0011DA04B26	ACTA3 Slave 1	ACTA3-1K-FU-SM-C	192.168.1.47	actatek_3.06.1927	132/1000	7/7/2020 9:52:56 AM	Online	Open Door Details	Opened 7/7/2020 4:07:34 PM
<input checked="" type="checkbox"/>	0011DB00089	AI Master	ACTA4-50K-FAC3-FU-SM-C	192.168.1.122	jakiniid_4.00.2024	132/50000	7/7/2020 9:52:20 AM	Online	Open Door Details	Opened 7/7/2020 4:07:35 PM
<input checked="" type="checkbox"/>	0011DB0008A	ACTA4 Entrance	ACTA4-5K-FAC3-FU-C	192.168.1.100	jakiniid_4.00.2024	132/5000	7/7/2020 9:51:22 AM	Online	Open Door Details	Opened 7/7/2020 4:07:36 PM

Remark: Click on Refresh button to update Request Status later.

Open Door

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

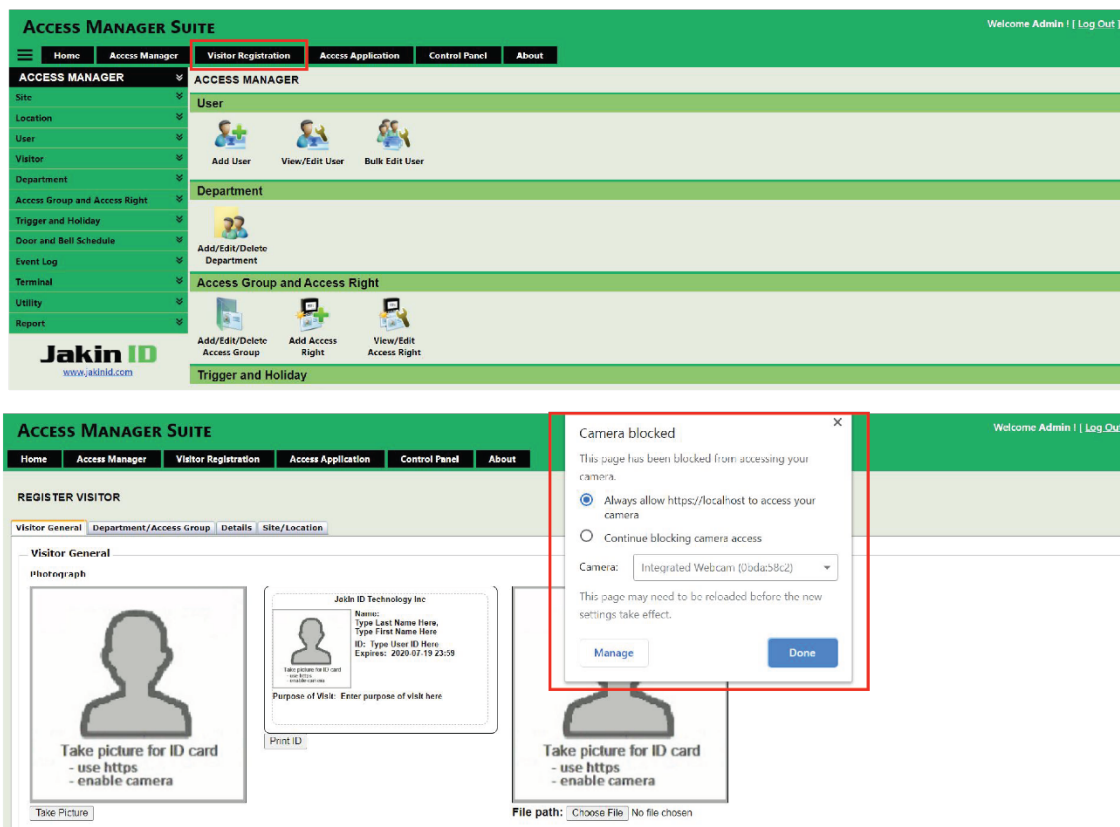
Appendix E. Visitor Registration

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 Vistor 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

Take Picture

First ID

File path: Choose File No file chosen

Remove

Jakin ID Technology Inc

First Name

Robert

ID: C0001

Expires: 2020-07-19 23:59

Purpose of Visit: Meeting With HR

First ID

User ID

C0001

First Name

Emma

Purpose of Visit

Meeting With HR

125 character(s) remaining in the remarks for Purpose of Visitor...

Phone Number

000172982436

Vehicle Number

NH2431

Expiry Date

enable

Disable

Date

2020-07-16

Time (HHMM)

23:59

Status

Administrator Level

Visitor User

Finger Print Security Level

Normal

Finger Print Type

FLE FAN

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 ICD

enable SMS

enable Email

Message

60 character(s) remaining in the message...

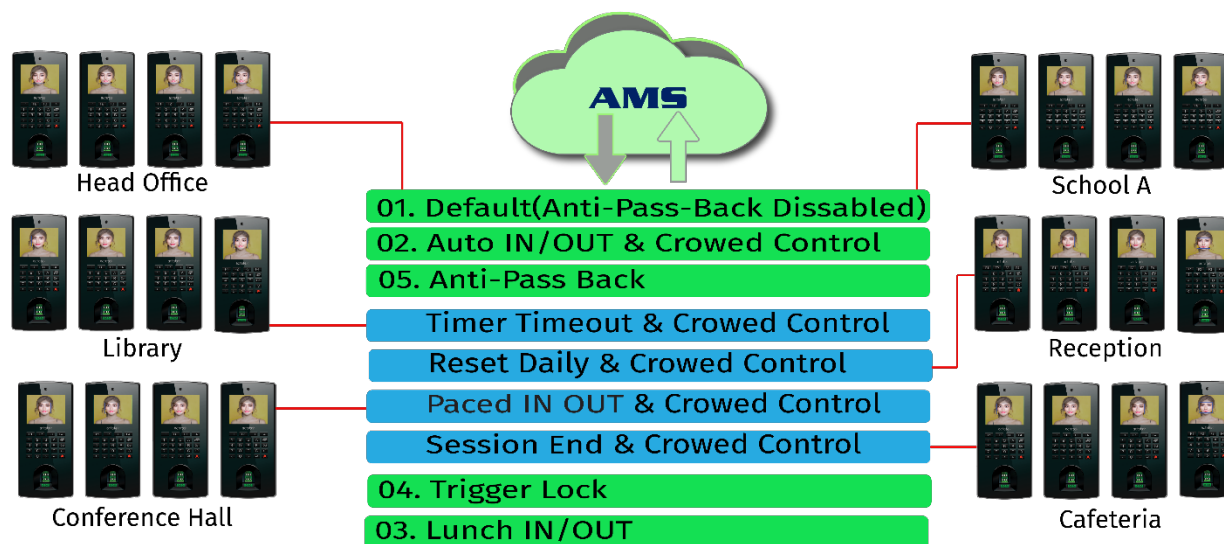
Reset

Save

Access Manager Suite User Manual - Page 62

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.

ACCESS MANAGER SUITE Welcome Admin ! [Log Out]

CONFIGURE ANTI-PASSBACK GROUP
Configure Anti-Passback Group and Department Association

Anti-Passback Type 'Auto IN/OUT' has been updated to 'Production'

Step 01: Anti-Passback Group Name: Time Attendance
Step 02: Department: Production
Step 03: Type: Auto IN/OUT
Step 04: Auto Reset: 00:00, Enable Crowd Control: ☒
Step 05: Save

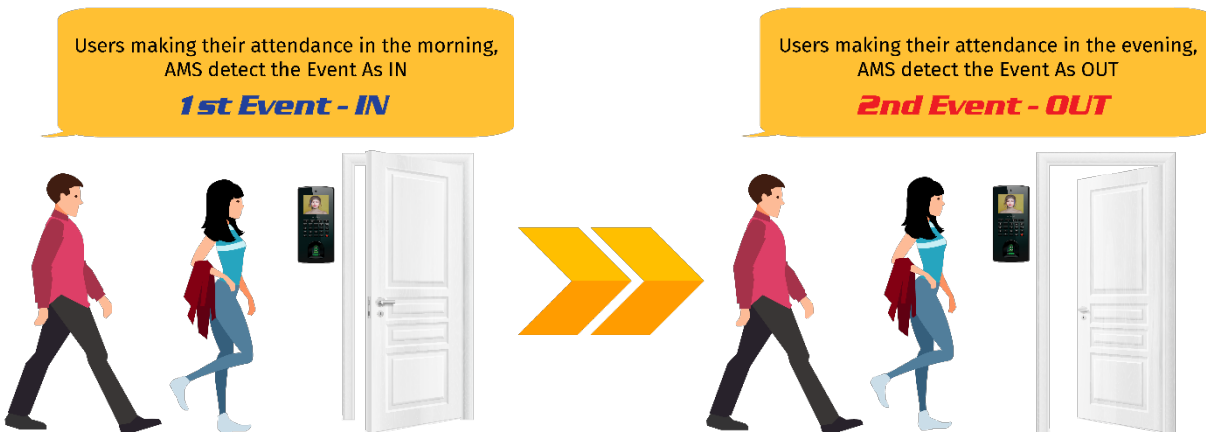
Set Default Trigger: IN
Set Default Trigger to All Departments Users: ☐

Anti-Passback Group and Department List

Group Name	Department Name	Department ID	APB Type	Reset Type	Reset/Timer	Crowd Control	Action
<input type="checkbox"/> Time Attendance	Production	5	AUTO IN/OUT	Enable	Reset: 00:00	Enable	Edit Delete
<input type="checkbox"/> Cafeteria Access	General	0	AUTO IN/OUT	Enable	Reset: 00:00	Enable	Edit Delete
<input type="checkbox"/> Access Control APB Group - Ground Floor	Admin	1	ANTI-PASSBACK	Reset Daily	Reset: 00:00	Enable	Edit Delete
<input type="checkbox"/> Default APB Group	-- Default APB Setting --	-1	DEFAULT / DISABLE	----	----	Disable	Edit Delete

Synchronize Department Terminals Delete

AMS Global Auto IN & OUT Anti Pass-Back



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 crowd 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.

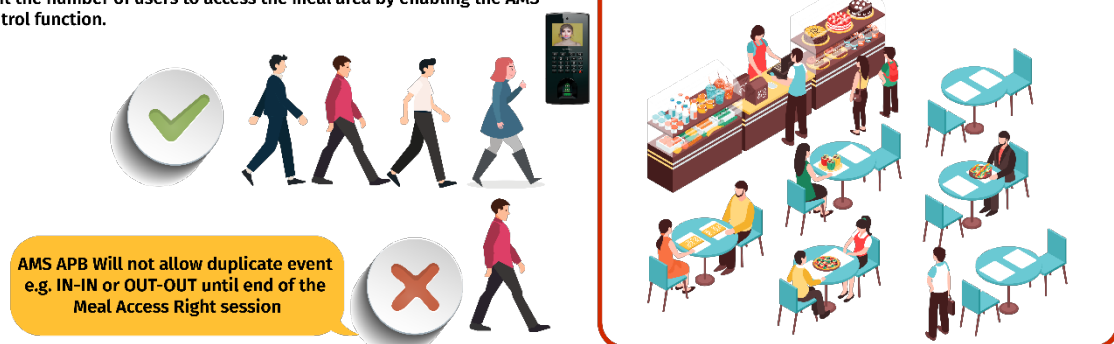
To enable this feature, go into the **Access Control** tab and then **Anti-Passback Group**. Create new **APB settings** by assign a group name and selecting the particular department >> Change from **DEFAULT** to **Anti-Passback** and press **Update** button to save. The ACTATEK particular department 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

AMS Anti Pass-Back Session End & Crowded Control

Anti-passback- 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 meal area by using the same access event example IN for specific time period.

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 meal area by enabling the AMS crowded control function.



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.

1 of 1					
Find Next					
Assessment Report					
Assessment Report					
1					
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

ACCESS MANAGER SUITE - HEALTH RISK ASSESSMENT

Welcome A9991 [Log Out]

Home Assessment Report Control Panel Access Manager About

COVID-AGE RISK ASSESSMENT

[Go to Assessment List](#) [Edit](#)

Assessment Questionnaire

Risk factor	Indicator
1. True age (years)	30
2. Gender	<input checked="" type="radio"/> Male sex <input type="radio"/> Female sex
3. Ethnicity	<input checked="" type="radio"/> Asian or Asian British <input type="radio"/> Black <input type="radio"/> Mixed <input type="radio"/> Other non-white
4. Body mass index (Kg/m ²)	<input type="radio"/> 30-34.9 <input type="radio"/> 35-39.9 <input checked="" type="radio"/> ≥40 or above
5. Hypertension	<input type="radio"/> Yes <input checked="" type="radio"/> No
6. Heart failure	<input type="radio"/> Yes <input checked="" type="radio"/> No
7. Other chronic heart disease	<input type="radio"/> Yes <input checked="" type="radio"/> No
8. Cerebrovascular disease	<input type="radio"/> Yes <input checked="" type="radio"/> No

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>
```

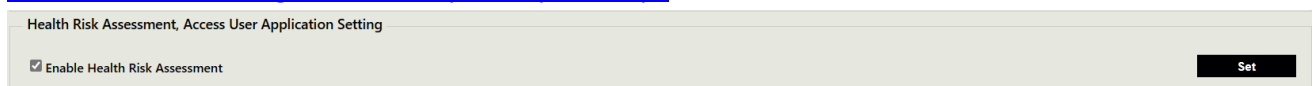
```
  <add name="AMS_ConnetionString" connectionString="Data
Source=localhost\SQLEXPRESS;Initial Catalog=AMSDB;User ID=sa;Password=123456" />
```

```
  <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>



Health Risk Assessment, Access User Application Setting

☒ Enable Health Risk Assessment

Set

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.

ACCESS MANAGER SUITE Welcome Admin ! | Log Out

ACCESS MANAGER

- User Management
- Access Control
- Visitor Management
- Health Risk Assessment
- Workforce Management
- System Setting
- About

TIME OFF MANAGEMENT

Time Off 'SICK' for 'A047' has been saved.

Add **Edit** **Search**

Time Off Management - Add Time Off

User ID: A047 Last Name: Smit First Name: Christoffel Department: General

Time Off Type: Sick Leave Start Date: 2022-12-21 Start Time: 09:00 End Date: 2022-12-22 End Time: 17:00 UTC: ☐

Remarks:

Time Off Status: ☐ Approve ☐ Reject ☒ Pending ☐ Archive

Clear **Save**

Time-Off List

Page Size: 10 ☐ UTC Reset Time (Date Time are in Local time)

User ID	Last Name, First Name	Department Name	Time-Off Type	Start DateTime	End DateTime	Request DateTime	Approve DateTime	Status	Action
<input type="checkbox"/> A047	Smit, Christoffel	General	Sick Leave	2022-12-21 09:00	2022-12-22 17:00	2022-12-20 12:16	Undetermined	Pending	Edit Delete

Refresh **Delete**

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**.

ACCESS MANAGER SUITE Welcome Admin ! | Log Out

ACCESS MANAGER

- User Management
- Access Control
- Visitor Management
- Health Risk Assessment
- Workforce Management
- System Setting
- About

PAYROLL MANAGEMENT

Add **Edit** **Search**

Payroll Management - Search Payroll

User ID: Partial Last name: Partial First Name: Department: -- Select Department --

User Payroll Type: Regular Rate: OT Rate: Leave Entitle: Leave Balance

Remarks:

User Payroll Status: **Clear** **List**

User Payroll List

Page Size: 10 Records found: 7

User ID	Last Name, First Name	Department Name	Payroll Type	Hours/Day	Day/Week	Salary	Regular Rate	OT Rate	Leave Entitle	Leave Balance	Action
<input type="checkbox"/> A001	Barriga, Eric	General	SALARY	0.00	0.00	4000.00	0.00	0.00	10.00	5.00	Edit Delete
<input type="checkbox"/> A002	IMBUD, RONA	General	SALARY	0.00	0.00	3000.00	0.00	0.00	10.00	5.00	Edit Delete
<input type="checkbox"/> A003	Gopalakrishna Pilla, Venukuttan Pillai	General	SALARY	0.00	0.00	3000.00	0.00	0.00	10.00	5.00	Edit Delete
<input type="checkbox"/> A004	Wahyudi, Arif	General	SALARY	0.00	0.00	4000.00	0.00	0.00	10.00	5.00	Edit Delete
<input type="checkbox"/> A005	Mangmool, Yuttakon	General	SALARY	0.00	0.00	1000.00	0.00	0.00	10.00	5.00	Edit Delete
<input type="checkbox"/> A008	Peres, Matheus Fortes	General	SALARY	0.00	0.00	1000.00	0.00	0.00	10.00	5.00	Edit Delete
<input type="checkbox"/> A009	Sool Leng, Doon	General	HOURLY	1.00	0.00	0.00	200.00	300.00	10.00	5.00	Edit Delete

Refresh **Delete**

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 private 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>

ID	Terminal ID	Terminal Name	Department	Action
4	00111DB00008	Dubai Sales Outlet A	General	Delete
2	00111DB00F72	HongKong Sales Outlet C	General	Delete

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

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

VIEW / EDIT USER

Export

File Format:

TXT

Export

Payroll Employee

Employee for user 'Ahmed, Sami (A11230)' is not on Payroll system

Create Payroll Employee

General
Department/Access Group
Details
Site/Location
Self-Enrollment
Trigger Lock Schedule

Self-Enrollment

User ID

A11230

Terminal ID

[00111DB000E3] ACTA4 Master

Access Method

Fingerprint Enrollment

Request Self-Enrollment

✓

Enrollment is queued ID:[62860] [ENROLL_FP]

Save

Cancel

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**

ACCESS MANAGER SUITE
Welcome admin ! [[Log Out](#)]

≡
User Management
Access Control
Visitor Management
Health Risk Assessment
Workforce Management

System Setting
About

CONFIGURE SYSTEM

System Update

Product Key: 7D0ED69D4874047C6FA40D3BFB043CF1

Activation Key:

Put key into textbox together with ends caps [.....]

[Submit](#)

Language

English (United States) [Update](#)

Enhance Security Settings

Enhance Security	Forward To Https	Login Maximum Retries	Timeout on Maximum Retries	
<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	3 v	1 hour v	Set

SMS Setting

☒ Enable SMS

SMS server address:

Username:

Password:

2
3
4
5
6
8
10

1 hour
2 hours
3 hours
4 hours
8 hours
12 hours
24 hours

[Set](#)

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.

Events Log to File Setting

☒ Enable Events Log to File

Events Log Directory e.g. C:\EventsLog

Log File Prefix e.g. Log_

Set

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

File Explorer view of C:\EventsLog:

Name	Date modified	Type	Size
DHL_28072022180000.log	7/28/2022 6:25 PM	Text Document	1 KB
DHL_28072022200000.log	7/28/2022 8:30 PM	Text Document	1 KB

Notepad view of DHL_28072022180000.log:

```

C400002307202220:07:0901
C400002307202221:12:0901
C400002307202221:14:3901
AC0092307202221:15:0001
AC0092307202221:16:4001
AC0092307202221:18:0001
  
```

Notepad status bar: Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8