## Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.2</td>
<td>2013/11/13</td>
<td>Added Upgrading AMS procedures in Section 7</td>
<td>Michael</td>
</tr>
<tr>
<td>1.0.1</td>
<td>2013/08/26</td>
<td>Added Access Apps Shift Manager</td>
<td>Michael</td>
</tr>
<tr>
<td>1.0.0</td>
<td>2013/08/02</td>
<td>Official Initial Release</td>
<td>Michael</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Offices:

Asia and the Rest of the World:

ACTAtek 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):

ACTAtek Technology Inc.
Suite 230, 10691 Shellbridge Way
Richmond, BC V6X 2W8
Canada

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

Europe, Middle East & Africa:

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

Phone: (44) 121 411 2288
Fax: (44) 121 411 2299
Sales: (44) 121 288 9923
E-mail: sales-eu@actatek.com (Sales Enquiries)
Singapore & Malaysia:

ACTAtek Pte Ltd
18, Boon Lay Way, #09-96/97/98
TradeHub 21, 609966
Singapore

Phone: (65) 6515 4520
Fax: (65) 6515 4521
E-mail: sales-asean@actatek.com (Sales Enquiries)

Thailand

ACTATek (THAILAND) Co. Ltd.
378 Soi Laphrao 101 Yaek Soi 12
Laphrao Road Klong Jan
Bangkapi Bangkok 10240
Thailand

Phone: (662) 378 1072
Fax: (662) 378 1072
E-mail: sales-asean@actatek.com (Sales Enquiries)

India, Sri Lanka, & Mauritius

ACTAtek Technology Pvt Ltd.
Room 206, 9/2, 1st Floor, East Patal Nagar,
New Delhi 110008
India

Phone: (91) 9899987333
E-mail: sales-india@actatek.com (Sales Enquiries)
Contents:

Chapter 1: Overview .................................................................................................................. 9
  1.1 Introduction ......................................................................................................................... 9
  1.2 Network Diagram .............................................................................................................. 9
  1.3 System Requirements......................................................................................................... 10
  1.4 Microsoft .Net Framework Requirements ......................................................................... 10

Chapter 2: Configuring Access Manager Suite ......................................................................... 11
  2.1 Accessing AMS .................................................................................................................. 11
  2.2 Activate AMS ..................................................................................................................... 11
  2.3 Log Into AMS .................................................................................................................... 12
  2.4 Setup Database In AMS .................................................................................................... 12
  2.5 Server Setup In AMS ......................................................................................................... 14
  2.6 Add New AMS Login Accounts ...................................................................................... 15
  2.7 Assign Permission To AMS Login Accounts ..................................................................... 15

Chapter 3: Configuring ACTAtek Terminals ............................................................................. 16
  3.1 Accessing the ACTAtek Web Interface ............................................................................... 16
  3.2 View Device Information .................................................................................................. 16
  3.3 Enable Access Manager Mode ........................................................................................ 17
  3.4 Register ACTAtek to AMS ............................................................................................... 17

Chapter 4: Access Manager Suite Functionalities ...................................................................... 20
  4.1 Auto User Synchronization .............................................................................................. 20
  4.2 Add Users ......................................................................................................................... 20
  4.3 View/Edit User .................................................................................................................. 21
  4.4 Bulk Changes On Users ................................................................................................... 21
  4.5 Add/Edit/Delete Departments ........................................................................................ 22
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.6 Add/Edit/Delete Access Group</td>
<td>22</td>
</tr>
<tr>
<td>4.7 Add Access Right</td>
<td>23</td>
</tr>
<tr>
<td>4.8 View/Edit Access Right</td>
<td>24</td>
</tr>
<tr>
<td>4.9 Edit Triggers</td>
<td>25</td>
</tr>
<tr>
<td>4.10 Trigger Schedule Setup</td>
<td>25</td>
</tr>
<tr>
<td>4.11 Holiday Setup</td>
<td>25</td>
</tr>
<tr>
<td>4.12 Door Open Schedule</td>
<td>26</td>
</tr>
<tr>
<td>4.13 Bell Schedule</td>
<td>26</td>
</tr>
<tr>
<td>4.14 View Event Logs</td>
<td>27</td>
</tr>
<tr>
<td>4.15 Add Manual Event Logs</td>
<td>27</td>
</tr>
<tr>
<td>4.16 View/Delete Manual Event Logs</td>
<td>28</td>
</tr>
<tr>
<td>4.17 View Terminal List</td>
<td>28</td>
</tr>
<tr>
<td>4.18 Copy Terminal User</td>
<td>28</td>
</tr>
<tr>
<td>4.19 Copy Group Access Right</td>
<td>29</td>
</tr>
<tr>
<td>4.20 Copy Trigger</td>
<td>29</td>
</tr>
<tr>
<td>4.21 Department Association</td>
<td>29</td>
</tr>
<tr>
<td>4.22 Data Import</td>
<td>29</td>
</tr>
<tr>
<td>4.23 Reports</td>
<td>30</td>
</tr>
<tr>
<td>Chapter 5: Access Manager Suite Advance Features</td>
<td>32</td>
</tr>
<tr>
<td>5.1 APB Requirements</td>
<td>32</td>
</tr>
<tr>
<td>5.2 Auto In/Out</td>
<td>32</td>
</tr>
<tr>
<td>5.3 Anti-Passback</td>
<td>33</td>
</tr>
<tr>
<td>5.4 Lunch In/Out</td>
<td>33</td>
</tr>
<tr>
<td>Chapter 6: Access Apps</td>
<td>35</td>
</tr>
<tr>
<td>6.1 Shift Manager</td>
<td>35</td>
</tr>
</tbody>
</table>
6.1.1 Create New Shifts ................................................................. 35
6.1.2 View/Edit Shifts ............................................................... 36
6.1.3 Assign Shifts to Employees ............................................. 36
6.1.4 Reporting ............................................................... 37

Chapter 7: Upgrading AMS Software ........................................ 39
7.1 Database Backup ............................................................... 39
7.2 Upgrading AMS from 1.0.1.x to 1.2.3.x ................................ 41
7.3 Upgrading AMS from 1.2.3.x to 1.2.3.x ................................ 45
Chapter 1: Overview

1.1 Introduction

Access Manager Suite (AMS) provides centralized web-based control and management to multiple ACTAtek terminal 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 ACTAtek system at all times, either on site or remotely. In addition, the AMS software gathers event log data from all ACTAtek terminals into a centralized database to simplify user redundant tasks. To enhance user management, AMS will facilitate all data synchronization of ACTAtek terminals 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 ACTAtek terminals on different networks, either public or private, can connect and communicate globally.

1.2 Network Diagram
1.3 System Requirements

<table>
<thead>
<tr>
<th><strong>Hardware Requirements</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Processor</td>
<td>Dual Core 2.0 GHz or faster (32-bit/64-bit)</td>
</tr>
<tr>
<td>Memory</td>
<td>4.0 GB or higher</td>
</tr>
<tr>
<td>Hard Disk Space</td>
<td>20.0 GB or higher</td>
</tr>
<tr>
<td>Network Controller</td>
<td>100 Mbps or higher</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Software Requirements</strong></th>
<th></th>
</tr>
</thead>
</table>
| Operating System          | Windows XP Professional (32-bit)  
Windows Vista Business (32-bit/64-bit) or above  
Windows 7 Professional (32-bit/64-bit) or above  
Windows 8 Professional (32-bit/64-bit) or above |
| Database Server Software Support | Microsoft SQL Server 2005  
Microsoft SQL Server 2008  
MySQL  
Oracle |
| Microsoft .Net Framework  | 2.0, 3.5, & 4.0 |
| Supported Web Browser     | Internet Explorer 7.0 or higher  
Firefox 3.5 or higher  
Chrome 6.0 of higher  
Safari 5.0 or higher |

1.4 Microsoft .Net Framework Requirements

<table>
<thead>
<tr>
<th>AMS Version:</th>
<th>.Net Version Requirement:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.40 to 1.2.3.x (Latest)</td>
<td>.Net 4.0</td>
</tr>
<tr>
<td>1.0.1.28 to 1.0.1.33</td>
<td>.Net 2.0/3.5</td>
</tr>
</tbody>
</table>

To download Microsoft .Net Framework, follow the link below:  
http://www.microsoft.com/net/downloads
Chapter 2: Configuring Access Manager Suite

2.1 Accessing AMS

<table>
<thead>
<tr>
<th>Method</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local computer access to AMS</td>
<td><a href="http://localhost/AccessManager/">http://localhost/AccessManager/</a></td>
</tr>
<tr>
<td>Network access to AMS</td>
<td><a href="http://IP">http://IP</a> ADDRESS OF SERVER/AccessManager/</td>
</tr>
</tbody>
</table>

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 this page. Contact ACTAtek support staff and provide the Product Key to them and in return, you should receive an Activation Key back.
2.3 Log Into AMS

<table>
<thead>
<tr>
<th>Administrator Default Login Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

2.4 Setup Database In AMS

Once you've logged in as an administrator, go to Control Panel and then Database Configuration.
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.
2.5 Server Setup In AMS

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

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

![Control Panel > System Accounts > Register/Edit/Delete Account](image)

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.

![Control Panel > System Accounts > Assign Permission](image)
Chapter 3: Configuring ACTAtek Terminals

3.1 Accessing the ACTAtek Web Interface

<table>
<thead>
<tr>
<th>Super Administrator Default Login Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>

By entering the IP address of the ACTAtek 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's 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.

![Terminal Setup Screenshot]

3.4 Register ACTAtek to 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. Press the Set button to test the Endpoint URL.

Endpoint URL:

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

### 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.

Press the **Register** button to register this ACTAtek terminal to Access Manager.

The ACTAtek terminal that is the first to register to AMS with a clean database will push all its user data from the ACTAtek terminal into the AMS database. All following ACTAtek terminals that will be registering to AMS will have its user data replaced by the downloaded copy from the AMS database during registration.
When the ACTAtek terminal has finished the registration process, a successfully message as indicated below would appear.

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

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 more characters long. For fingerprint and smart card enrollments, this will have to be accomplished on any of the registered ACTAtek terminals by providing the associated User ID to the fingerprint or smart card enrollment process.
In the status field, ensure **Active** is checked to enable this new user in the system. You may also wish to check **Password** if this user can enter through PIN method otherwise leave it unchecked if you do not wish to let this user authenticate through PIN method.

Additional settings which you may choose to set for any new user are: department & groups, user information, user expiry date, and user 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.

#### 4.4 Bulk Changes On Users

Bulk changes on 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, fingerprint, automatch, password, and smart card. Additionally, adjustable user settings apply to fingerprint quality, departments, and groups. For each change, press the **Set** button to save the changes to the queue. When all the changes are made, press the **Commit** button to permanently make the changes to the selected users. The registered ACTAtek terminals will now enter **System Maintenance Mode** while these changes are being made.
4.5 Add/Edit/Delete Departments

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

4.6 Add/Edit/Delete Access Group

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

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

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

In the Day & Time field, the administrator defines the restrictions and the rules in terms of a schedule. By default, the schedule has all time and days of the week disabled which can be referenced below by the light grey dots.
After making setting changes to the Day & Time field, press the Modify Time button to review the changes made. The filled black dots are set for enabled while the light grey dots are set for disabled.

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

Press the Add button to add this access right to Access Manager. Notice that this access right only affects a single ACTAtek terminal therefore to have this access right 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 system.
4.9 Edit Triggers

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

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

4.10 Trigger Schedule Setup

Based on a schedule, the administrator can choose enable or disable triggers. To setup this functionality, select an ACTAtek terminal from the drop down list. In the Day & Time field, select a trigger ID, time frame, date, and specify either enabled or disabled. To save this schedule, press Modified Time button and the changes will now reflect on the trigger schedule field. When ready, press the Setup button to make the final changes. By default, the trigger schedule settings are on disabled and affect no days of the week unless checked.

4.11 Holiday Setup

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

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

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

4.13 Bell Schedule

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

Administrators can view event logs that have been collected from the ACTAtek terminals in real time. Additionally, the administrator may choose to use the search option to search for specific events and export the results in a CSV file. The View EventLog 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 > Event Logs > View Event Logs]

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.

![Access Manager > Event Logs > View Event Logs > Search Results]
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, and sync information.

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 to associate newly registered user to specific departments. To accomplish this, predefine an ACTAtek terminal from the terminal list and select a department and press the Associate button to add this association. Now all newly added users on this terminal will automatically be associated to the specified department.

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.

<table>
<thead>
<tr>
<th>Access Manager &gt; Utilities &gt; Data Import &gt; Load CSV File</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>C1000</td>
</tr>
<tr>
<td>C2000</td>
</tr>
</tbody>
</table>
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.

![Data Mapping](image)

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

### 4.23 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.
Chapter 5: Access Manager Suite Advance Features

5.1 APB Requirements

<table>
<thead>
<tr>
<th>Software &amp; Firmware</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Manager Suite</td>
<td>1.2.3.64 or newer</td>
</tr>
<tr>
<td>Actatek 3 Firmware</td>
<td>3.06.1302 or newer</td>
</tr>
</tbody>
</table>

The 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.

5.2 Auto In/Out

The **Auto In/Out** feature allows the ACTAtek terminal to auto determine the IN or OUT status of an user during authentication and records the punch event accordingly. 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.

![Control Panel > System Configuration > APB Setting](image)

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 you reset all with **IN** status, Auto In/Out system will determine the next punch as an **OUT** event for all the users.
5.3 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**.

![Control Panel > System Configuration > APB Setting]

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.

5.4 Lunch In/Out

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

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

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

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

Use **Copy Trigger** function and copy them over to all remainder ACTAtek terminals.
When the user presses the F1 shortcut key on the ACTAtek terminal, it will bring them to the LunchOUT trigger and etc. When the user punches with trigger LunchOUT, it will signify to AMS that the user is on lunch break. When the user punches in with trigger LunchIN, it will be accepted if the punch was made after 13:00 as seen in the images above or else they will be rejected.
Chapter 6: Access Apps

6.1 Shift Manager

6.1.1 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.
6.1.2 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.

![View/Edit Shifts screenshot]

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.

6.1.3 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.

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

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

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

### 6.1.4 Reporting

Press the **View Report** button in the menu to generate report in **Shift Manager**. Shift Manager Reporting gives you the flexibility to filter by **User ID** and also by **Time**. By specifying a **User ID** and a **Time**, you can generate a user report for the week, or for 2 weeks, or for the month, and even for the year. By leaving the User ID field out, you can generate reports containing all employees. Daily reports can also be generated for auditing purpose.
For every changes made in the filter criteria, you will need to press **Load Data Report** button such that it will acquire the event data related to the filter from Access Manager.

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

**Grace Rounding** and **Time Rounding** options can be checked if they are applicable to the reporting as required. Press **Generate Report** button to update the report such that the rounding options are taken account for.
Chapter 7: Upgrading AMS Software

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.
7.2 Upgrading AMS from 1.0.1.x to 1.2.3.x

It is highly recommended to make a back up copy of the current AMS database before proceeding.

When upgrading your AMS from 1.0.1.x to 1.2.3.x, the first step is to stop your Internet Information Service (IIS). This will allow you to uninstall Access Manager Suite without complications since it is no longer running as a service.

Go to Window’s Control Panel and then Program and Features. In this list, select Access Manager Suite and press Uninstall. Follow the Windows Installer to remove AMS completely. When Access Manager Suite software is no longer on this list, you have successfully uninstalled AMS.

Download the latest version of AMS. Extract the compressed ZIP file that contains the installation files to the newest version of AMS. Open its folder and run setup.exe to continue with the installation process.
Follow the AMS installation wizard by pressing the **Next** button.

Once the AMS installation has completed, go back to Internet Information Services (IIS) window and go into **Application Pools**. Right click with your mouse on **AccessServer** as highlighted below and select
Advance Settings. Change .NET Framework Version from v2.0 to v4.0 and press the OK button to save the changes. Do the following to the DefaultAppPool so it is also using .NET Framework Version v4.0.
Now in the actions field for managing servers in IIS, press the **Start** action to start up IIS so AMS can run as a service and be accessible on your web browser.

If you receive the following error as shown above when trying to access the Access Manager web interface, this means you have not configured the .NET Framework to v4.0 correctly in IIS. Please revert back a couple of steps to find instructions on how to change .NET Framework from v2.0 to v4.0 for **AccessServer** and **DefaultAppPool** application pools in order for AMS to run properly.

If you have configured IIS correctly to use the .NET Framework v4.0, you should now be able to access the new version of AMS on your browser. By default, the URL to access AMS is:

- **[Local Access]** [http://localhost/AccessManager/](http://localhost/AccessManager/)
- **[Network Access]** [http://IP ADDRESS OF SERVER/AccessManager/](http://IP ADDRESS OF SERVER/AccessManager/)

Login to AMS and then go to **Control Panel** and then **Database Configuration**. Press the **Upgrade** button to let the database know that a new version of AMS has been installed. When completed, the current page should now produce a **Database Upgrade Summary** and let you know that the database has now
been upgraded to a newer revision. You have upgraded AMS successfully from 1.0.1.x to 1.2.3.x and you may now use AMS.

7.3 Upgrading AMS from 1.2.3.x to 1.2.3.x

It is highly recommended to make a back up copy of the current AMS database before proceeding.

When upgrading your AMS from 1.2.3.x to 1.2.3.x, the first step is to stop your Internet Information Service (IIS). This will allow you to uninstall Access Manager Suite.
Go to Window’s Control Panel and then Program and Features. In this list, select Access Manager Suite and press Uninstall.

Download the latest version of AMS and extract the compressed ZIP file that contains the installation files of AMS. Run setup.exe to continue with the installation process.
Follow the AMS installation wizard by pressing the **Next** button.

When AMS has finished installing, go to IIS and press the **Start** button to reinitiate web services.
Login to AMS and then go to Control Panel and then Database Configuration. Press the Upgrade button to let the database know that a new version of AMS has been installed. When completed, the current page should now produce a Database Upgrade Summary and let you know that the database has now been upgraded to a newer revision. You have upgraded AMS successfully from 1.2.3.x to 1.2.3.x and you may now use AMS.