Quick Administrator's Guide to On-Premise AMS Software Installation & Mobile App Integration

Introduction

The JakinID Silver Quick Administrator's Guide is designed to provide a step-by-step process for the installation, configuration, and integration of the AMS (Access Manager Suite) software with the JakinID Silver Mobile App and ACTAtek devices. This guide covers the complete setup, from initial system requirements and AMS software installation to mobile app integration and device configuration.

The instructions include pre-installation requirements, new installations, upgrade steps for existing systems, and best practices for post-installation configurations.

AMS Pre-installation Requirements:

Hardware Requirements:

- CPU: Intel Core i5 1.20 GHz or faster (64-bit)
- Memory: 8 GB or higher
- Hard Disk: 500 GB or higher. Use SSD, NVMe for fast performance (AMS software only consumes approximately 150 MB)
- Network Controller: 100 Mbps or higher

Software Requirements:

- Operating System:
  - Windows 10/11 Professional (64-bit)
  - Windows Server 2012 or above (64-bit)
- Database:
  - Microsoft SQL Server (2012, 2014, 2016, 2019, 2022), Microsoft Azure SQL,AWS.
- .Net Framework:
  - .Net 4.8

Pre-installation Checklist:

1. Ensure MS SQL Server is installed and configured:
2. Ensure MS IIS features and sub-features are installed.
3. Disable firewall or configure it to allow port 80 and 443 for data transfer.

Access Manager Suite (AMS) Software Installation Visual Guide (jakinid.com)
Access Manager Suite (AMS) Software Installation & User Manual (jakinid.com)

Download the AMS Installation Package:

- Contact **support@actatek.com** to obtain the latest AMS version.

AMS Installation Guide for New AMS setup:

1. **Run AMS Installer**:
   - Download the latest AMS installation package.
   - Run setup.exe from the package to begin the installation.
2. **AMS Activation**:
   - After installation, the AMS login page will appear. Provide your AMS Product Key to generate an Activation Key and unlock the login page (Default login: admin, password: 1).
3. **Database Configuration**:
   - Navigate to **Control Panel > Database Configuration**.
   - Enter your SQL Server information:
     - **Database Type**: SQL Server
     - **Server Address**: <PC Name/IP>\SQLEXPRESS
     - **Database Name:** <Your Database Name>
     - **User**: sa
     - **Password**: <Your SQL Password>
   - Click **Setup** to create the AMS database.
4. **Server Setup**:
   - Navigate to **Server Setup** in the AMS Control Panel.
   - Enter the server information:
     - **Terminal Group**: AMS
     - **Time Zone**: GMT +8 (Singapore)
     - **Agent Server IP Address:**<https://AMS SERVER IP/ NAME>
     - **Agent Server port:** 443 (HTTPS port)
     - **Magic String**: 1234
   - Click **Setup** to finalize the server setup.

AMS Upgrade Guide for Existing AMS:

1. **Backup the AMS Database:** Backup AMS database is crucial to ensure data integrity and availability in case of system failures, data corruption, or other unforeseen events.
2. **Uninstall the existing &Run new AMS Installer**:
    - Download the latest AMS installation package.
    - Uninstall the existing AMS
    - Run setup.exe from the package to begin the installation.
3. **AMS Activation**:
    - After installation, the AMS login page will appear. Provide your AMS Product Key and **''About''** Tab screenshot to generate an Activation Key and unlock the login page (Default login: admin, password: 1).
4. **Database Configuration**:
    - Navigate to **Control Panel > Database Configuration**.
    - Enter your SQL Server information:
        - **Database Type**: SQL Server
        - **Server Address**: <PC Name/IP>\SQLEXPRESS
        - **Database Name:** <Your Database Name>
        - **User**: sa
        - **Password**: <Your SQL Password>
    - Click ''**Setup'' to** re-intiate the AMS connection to existing database.
    - Click **''Upgrade''** to upgrade the AMS database schema to latest version that required for the latest features su as JakinID Silver App

---

AMS Post-installation Configuration:

Granting IIS Access to AMS Folders:

1. Go to the root folder location (e.g., **C:\ProgramData\Actatek**).
2. Locate the **AccessManager** folder and right-click it, then select **Properties**.
3. Navigate to the **Security** tab and add the **IIS_IUSRS** account.
4. Ensure that the **IIS_IUSRS** account has full permissions to **C:\inetpub\wwwroot\AccessManage**, then click **Apply** and **OK**.
5. Repeat the same process for these folders:
    - **C:\inetpub\wwwroot\AccessManager\Images**
    - **C:\inetpub\wwwroot\AccessManager\SilverApp**
6. Lastly, restart IIS for the changes to take effect.

AMS Post-installation Configuration for Mobile App:

DNS Registration:

Register a DNS name for the SaaS AMS server (e.g., ams.resellerdomain.com) to provide easy access for users, customers, and devices to the AMS web application.

Enable HTTPS and Port 443:

install an SSL/TLS certificate from a trusted provider (e.g., Let's Encrypt, DigiCert) to secure communication between AMS, ACTAtek devices, and mobile app users, ensuring encrypted data transmission.

ACTAtek Device Configuration and User Enrollment for new AMS:

Login to ACTAtek Device Web UI:

1) Set up the **Terminal Clock** for correct date and time.
2) Enable **Access Manager Mode** from the **Terminal Setup** section.

Register Device with AMS:

1) Enter the **Endpoint URL** in **Access Client Setup**: http://<AMS PC IP Address>/AccessServer/AccessService.asmx
2) Click **Set** and then **Register** to register the device with AMS.

Bulk User Import and Enrollment:

1) Use the **AMS Import Data Utility** to import employee data from an Excel sheet for bulk user account creation (e.g., first name, last name).
2) After importing users, use the **AMS Remote Enrollment Feature** to add user credentials such as face, fingerprint (FP), or smart card (SM) for complete user credential creation.

Alternatively, you can manually enroll users using the ACTAtek device's graphical interface, where you can add credentials like face, FP, SM, and more.

Mobile App (Silver) Connection to AMS:

To connect the JakinID Silver Mobile App with the AMS, users can follow one of two methods:

Silver App Server Link:

- Admins can share the AMS home page URL with end users via email, WhatsApp, and other communication platforms. Users can then open the AMS home page on their mobile phones, where the Silver App is installed, using any web browser.
- By clicking the Silver App Server Link, the mobile application will automatically connect to the AMS server.

QR Code Method:

- After the admin logs into the SaaS AMS portal, they can download and share the QR code displayed on the AMS home page. This QR code contains the initial connection information needed to connect the mobile app.
- Users can then download and scan this QR code using their Silver Mobile App, which will automatically connect the app to the correct SaaS AMS domain.

Manual Entry Method:

- Alternatively, users can manually enter the SaaS AMS server address and domain name in the Silver Mobile App's settings. This allows the app to connect to the correct domain if the QR code method is not used.

Both methods ensure a seamless and secure connection between the mobile app and the SaaS AMS domain for real-time access and management.

Additional Security Considerations:

- Ensure all AMS and ACTAtek device communications are secured via HTTPS.
- Use strong, complex passwords for AMS admin and user accounts.
- Regularly update SSL certificates to maintain secure communication channels.
- Keep AMS and device firmware up to date for the latest security patches.
