

On-premises Access Manager Suite (on-prem AMS)

Quick installation Guide

Version 4.0

Overview

This guide provides comprehensive instructions for installing and configuring the on-premises Access Manager Suite (on-prem AMS) software on Windows Server operating systems for example. Please follow each section carefully to ensure successful deployment.

1. System Requirements

1.1 Hardware Requirements

Component	Specification
CPU Processor	Core Ultra 5 250K Plus/ Ryzen 7 9700X or faster (64-bit)
Memory	16.0 GB or higher
SSD Hard Disk Space	100.0 GB or higher
Network Controller	100 Mbps or higher

1.2 Software Requirements

Component	Requirements
Operating System	- Windows 11 Professional (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	• Microsoft SQL Server 2012 or above • Microsoft SQL Server 2014 or above • Microsoft SQL Server 2016 or above • Microsoft SQL Server 2019 or above • Microsoft Azure SQL Server • MySQL 8.0.44 or above • Oracle 11g or above
Microsoft .NET Framework	• 3.5.1, 4.0, 4.7 & 4.8
Supported Web Browsers	• Microsoft Edge 108.0 or higher • Firefox 3.5 or higher • Chrome 6.0 or higher • Safari 5.0 or higher

2. Pre-Installation Requirements

CRITICAL: The following components must be installed before running the AMS setup.exe installer:

2.1 Required .NET Framework versions (if not previously installed) for Windows OS

1. **.NET Framework 4.7.2** - From the unzipped on-prem AMS installation folder, run the following installer: \DotNetFX472\Net472-kb4054530-x86-x64-allos-enu.exe
2. **.NET Framework 4.8** - From the unzipped on-prem AMS installation folder, run the following installer: \DotNet48\NDP48-x86-x64-AllOS-ENU.exe

2.2 Install SQL Server Compact Edition, which is required for storing on-prem AMS configuration and license information.

Install both 32-bit and 64-bit versions from the unzipped on-prem AMS installation folder

- SSCERuntime-ENU.msi (32-bit)
- SSCERuntime-ENU-x64.msi (64-bit)

2.3 MS SQL Server Express & Management Studio

Download and install the following for back-end on-prem AMS database configuration for example:

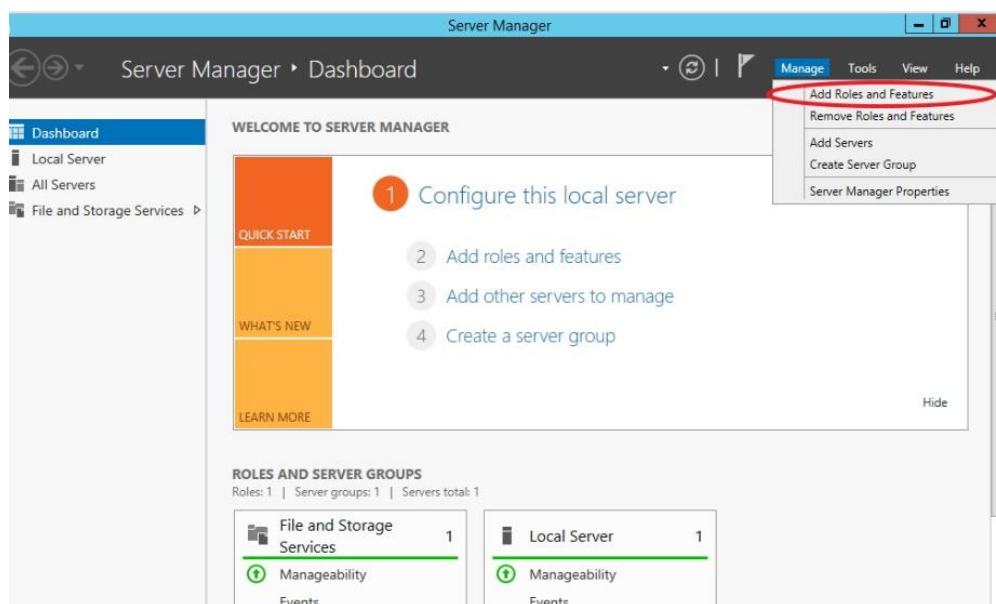
- Microsoft® SQL Server® 2022 Express or above
- Microsoft® SQL Server Management Studio

3. IIS Web Server Configuration

CRITICAL: IIS web server features and sub-features must be enabled before running setup.exe

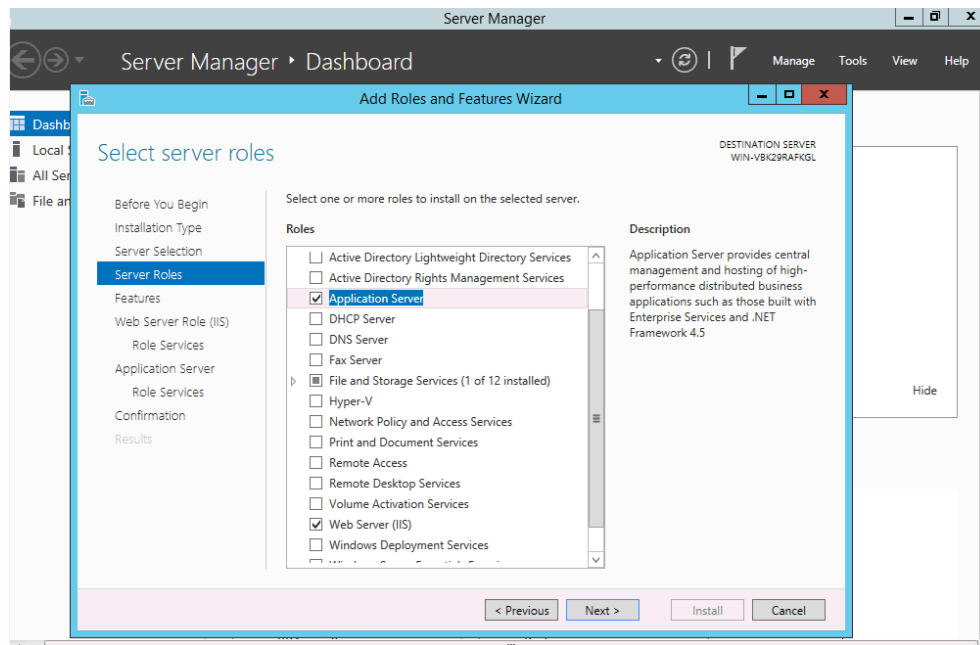
3.1 Installing IIS Roles and Features

3. **Open Server Manager** and click
 - Manage → Add Roles and Features



4. Select Server Roles

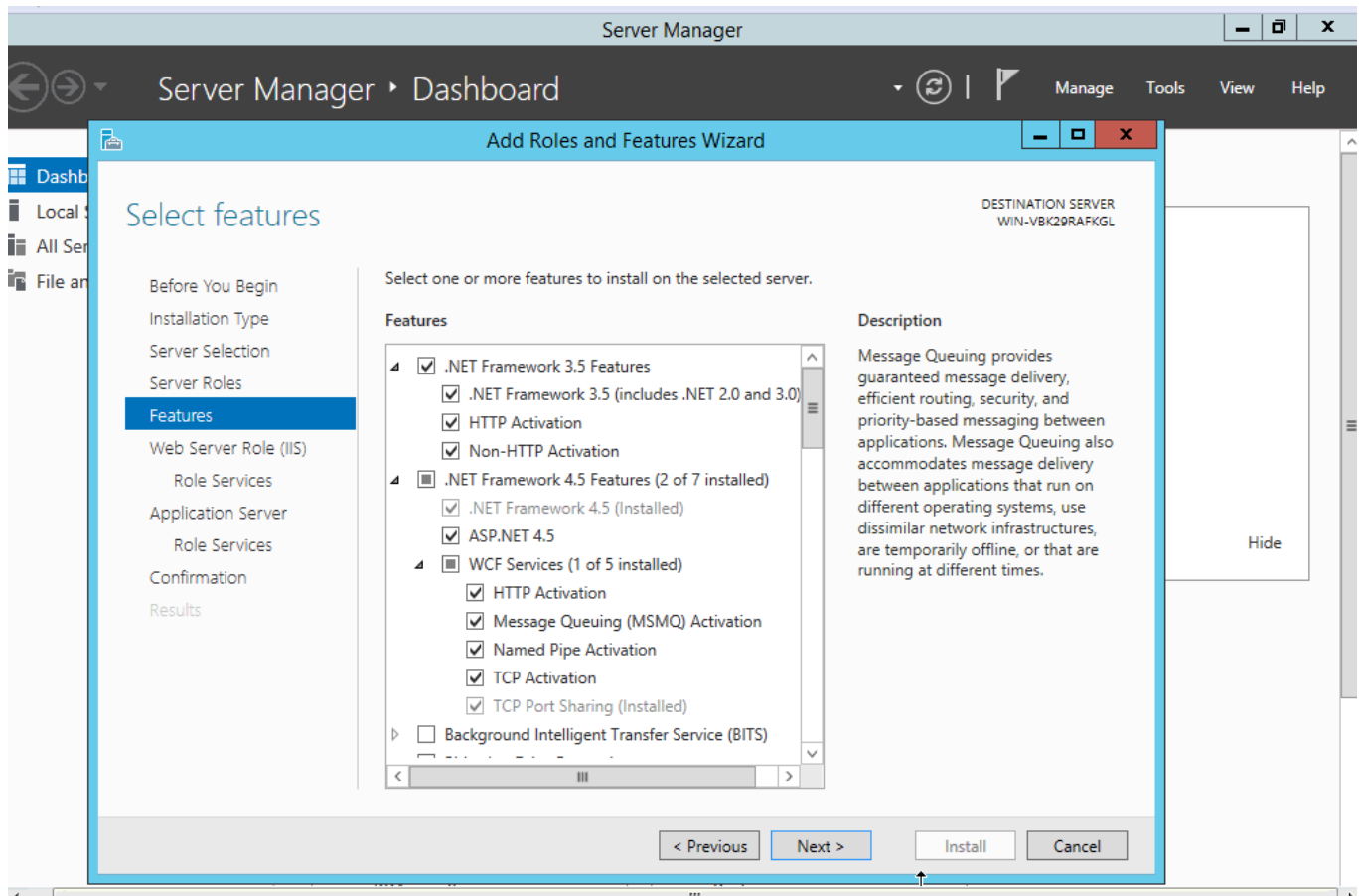
- Check: Application Server
- Check: Web Server (IIS)



5. Configure Features - Select the following:

- .NET Framework 3.5 Features
- .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- HTTP Activation
- Non-HTTP Activation
- .NET Framework 4.5 Features
- .NET Framework 4.5 (Installed)
- ASP.NET 4.5
- WCF Services
- HTTP Activation
- Message Queuing (MSMQ) Activation

- Named Pipe Activation
- TCP Activation



3.2 Web Server Role Services

Under Web Server (IIS) → Role Services, enable the following:

- **Common HTTP Features**
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - HTTP Redirection
 - WebDAV Publishing

- **Health and Diagnostics**

- HTTP Logging
- Custom Logging
- Logging Tools
- ODBC Logging
- Request Monitor

- **Performance**

- Static Content Compression
- Dynamic Content Compression

- **Security**

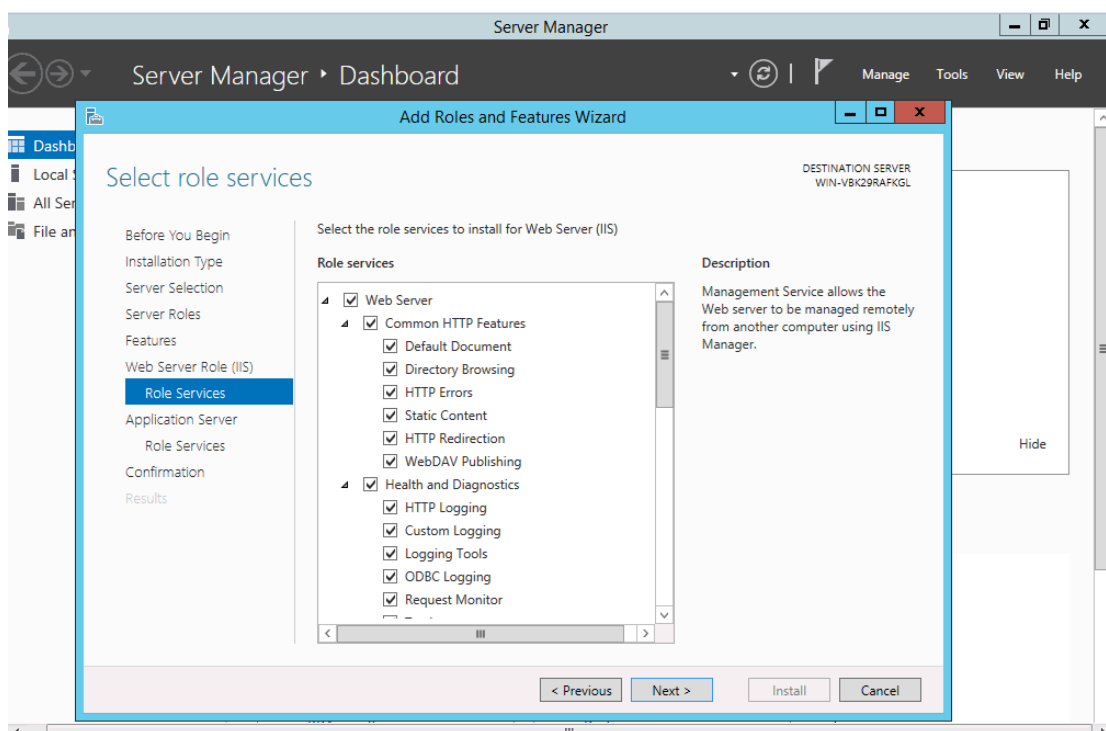
- Request Filtering
- Basic Authentication
- Centralized SSL Certificate Support
- Client Certificate Mapping Authentication
- Digest Authentication
- IIS Client Certificate Mapping Authentication
- IP and Domain Restrictions
- URL Authorization
- Windows Authentication

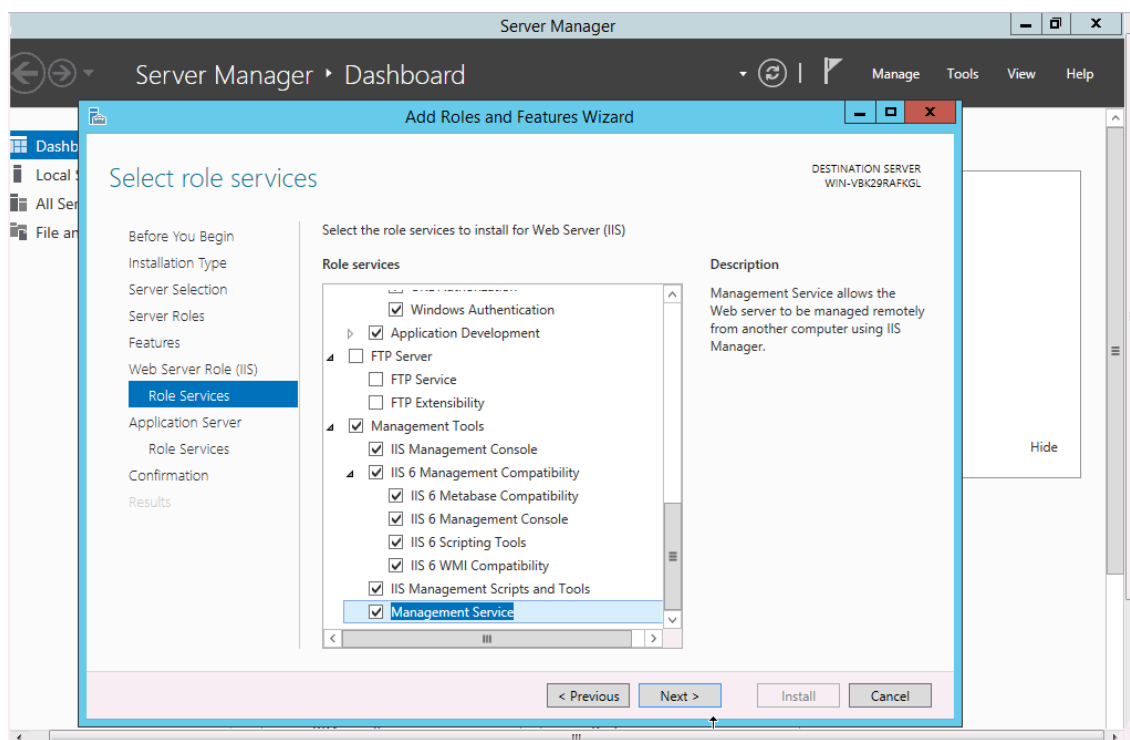
- **Application Development**

- .NET Framework 4.5
 - Application Development
- 

- **Management Tools**

- IIS Management Console
- IIS 6 Management Compatibility
- IIS 6 Metabase Compatibility
- IIS 6 Management Console
- IIS 6 Scripting Tools
- IIS 6 WMI Compatibility
- IIS Management Scripts and Tools
- Management Service



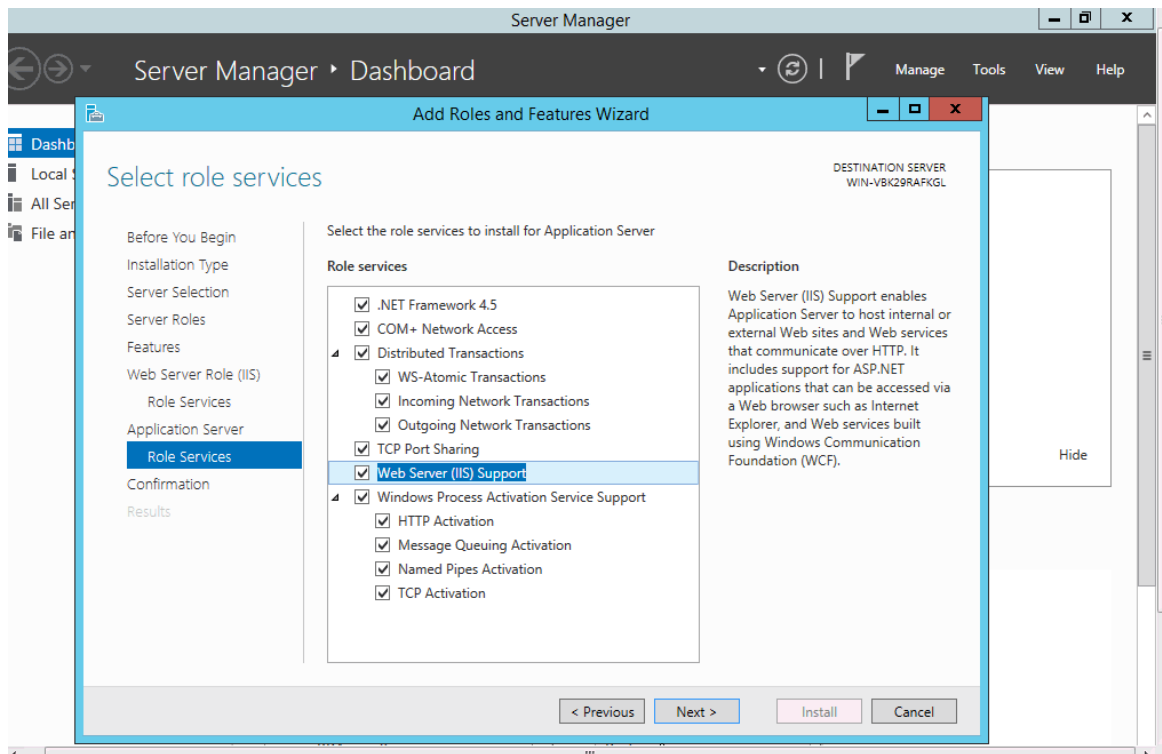


3.3 Application Server Role Services

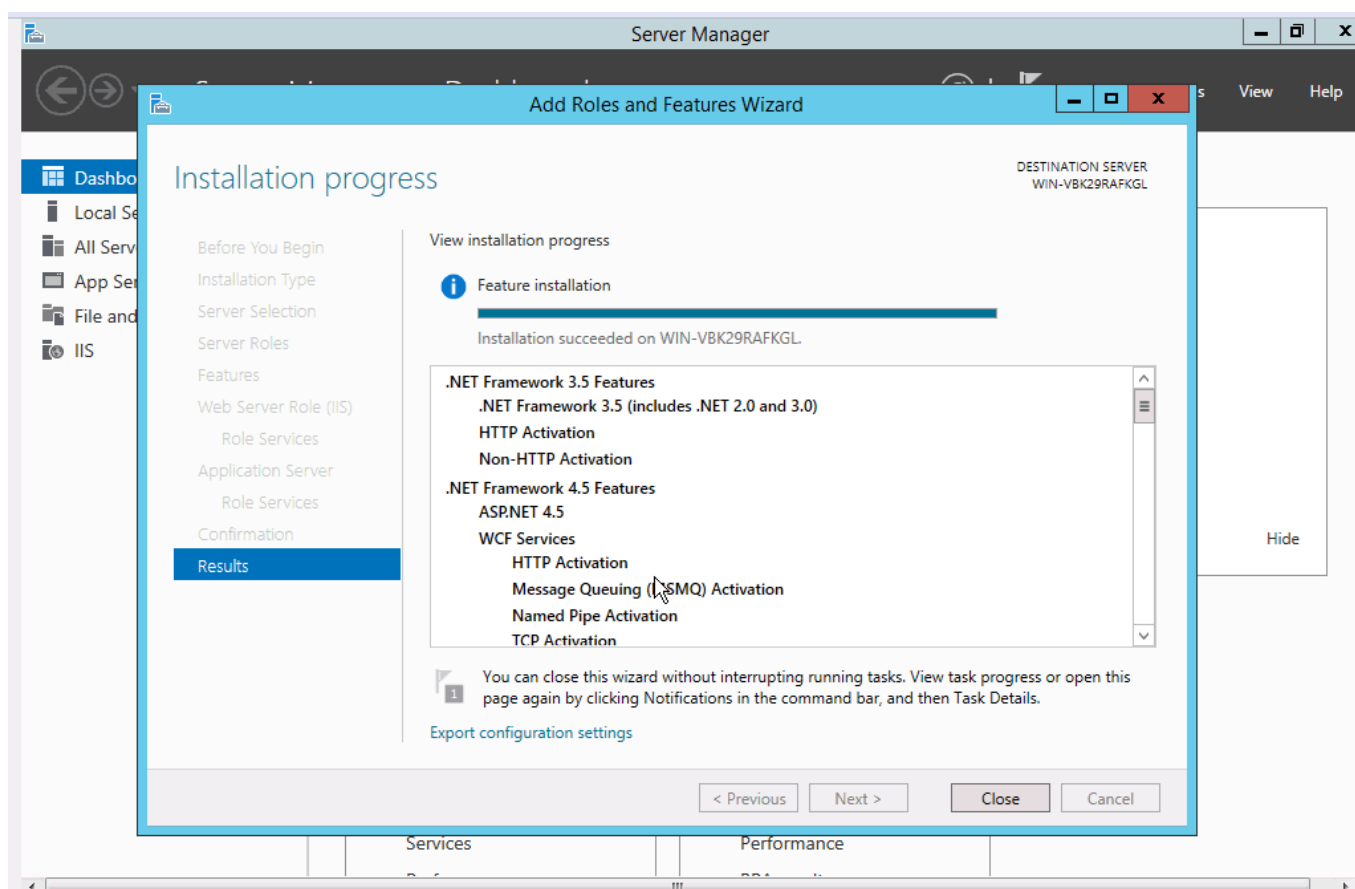
Under Application Server → Role Services, enable:

- .NET Framework 4.5
- COM+ Network Access
- Distributed Transactions
 - WS-Atomic Transactions
 - Incoming Network Transactions
 - Outgoing Network Transactions
- TCP Port Sharing
- Web Server (IIS) Support
- Windows Process Activation Service Support
 - HTTP Activation
 - Message Queuing Activation

- Named Pipes Activation
- TCP Activation



6. Click **Install** and wait for the installation to complete



4. Firewall Configuration

Ensure the following ports are open in Windows Firewall to allow inbound and outbound access to the on-prem AMS:

- **Port 80 (HTTP)** - Required for web access
- **Port 443 (HTTPS)** - Required if HTTPS support is needed

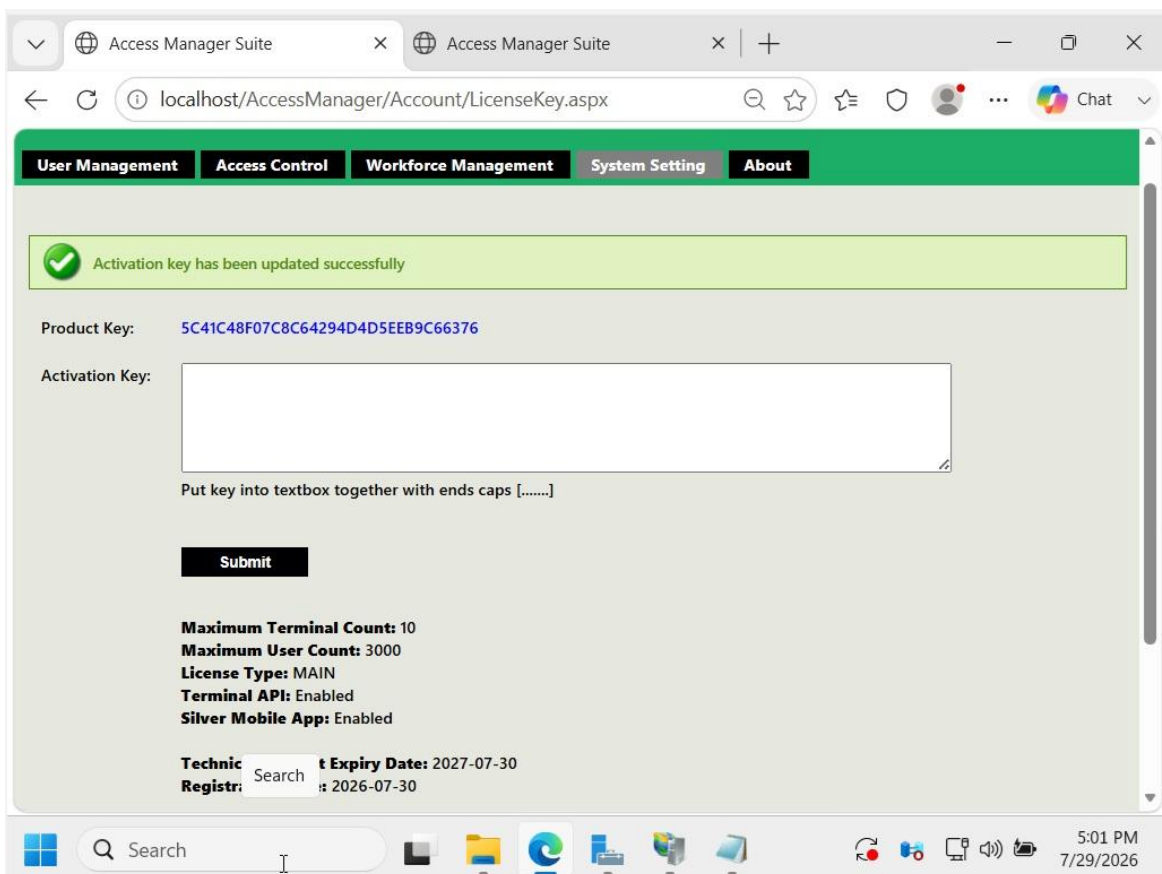
Important: Verify that Windows Firewall or third-party antivirus software (Norton, McAfee, ESET) does not block these default IIS web server ports.

5. On-prem AMS Installation

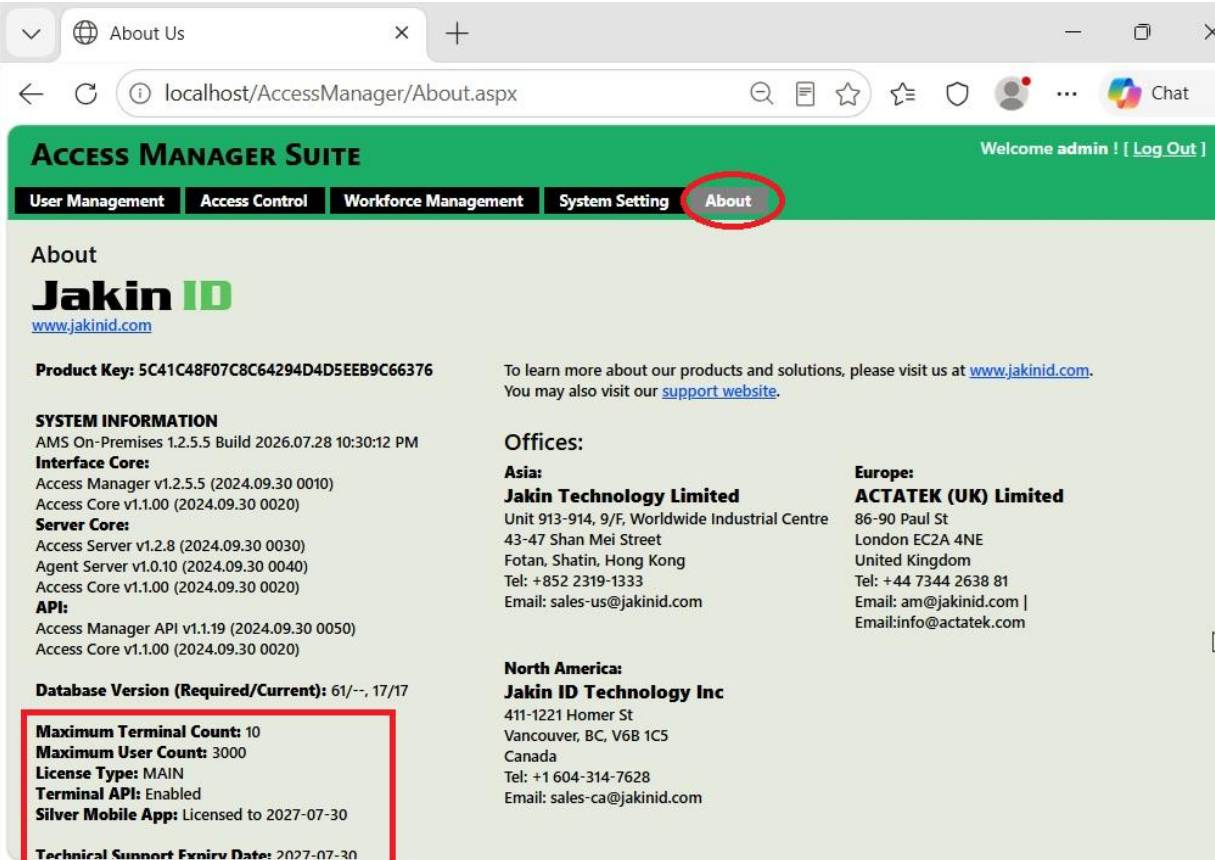
7. **Verify Prerequisites:** Confirm all components from Section 2 are installed
8. **Verify IIS Configuration:** Confirm all IIS features from Section 3 are enabled
 - **Run AMS Installer:** Locate and double-click **setup.exe** from the on-prem AMS installation package
9. **Follow Installation Wizard:** Complete all prompts in the installation wizard
10. **Open AMS Login Page**

Open the AMS login page at: <http://localhost/AccessManager/>

Enter the AMS key and click the 'Submit' button.

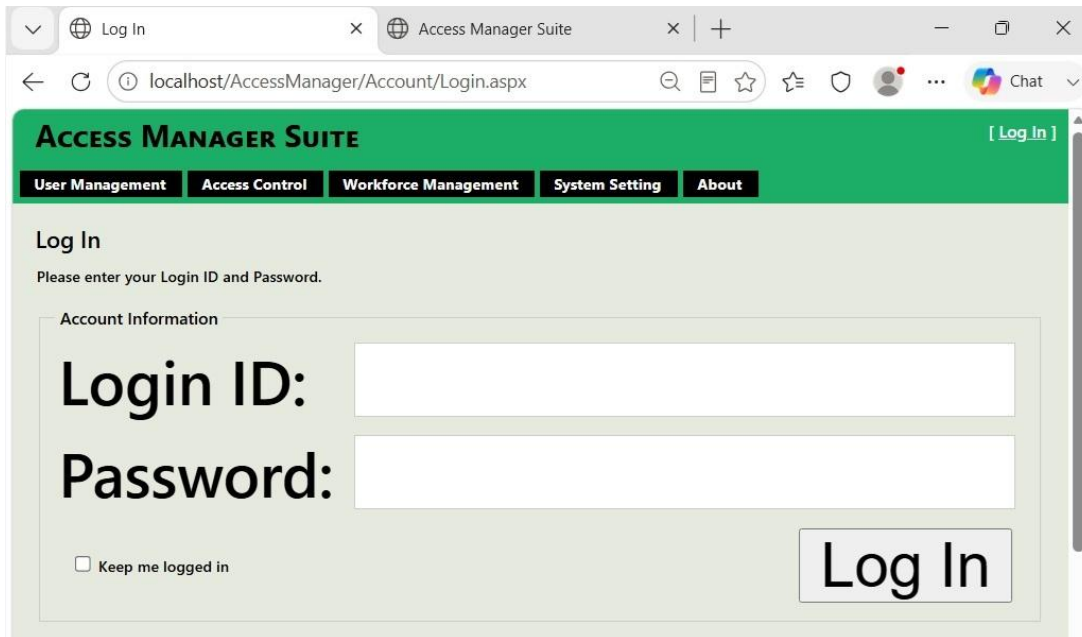


Note: You can open the AMS About page to view the AMS Product Key, the activation license information, and the technical support expiry date.



11. Log in to AMS Click the **Login** link at the top right, and enter the default AMS login credentials:

- **Login ID:** admin
- **Password:** 1



The screenshot shows a web browser window with two tabs: 'Log In' and 'Access Manager Suite'. The address bar shows the URL 'localhost/AccessManager/Account/Login.aspx'. The page has a green header with the text 'ACCESS MANAGER SUITE' and a '[Log In]' link on the right. Below the header is a navigation bar with five buttons: 'User Management', 'Access Control', 'Workforce Management', 'System Setting', and 'About'. The main content area is titled 'Log In' and contains the instruction 'Please enter your Login ID and Password.' Below this is a section titled 'Account Information' with two input fields: 'Login ID:' and 'Password:'. There is a checkbox labeled 'Keep me logged in' and a 'Log In' button.

Log In

Access Manager Suite [Log In]

User Management Access Control Workforce Management System Setting About

Log In

Please enter your Login ID and Password.

Account Information

Login ID:

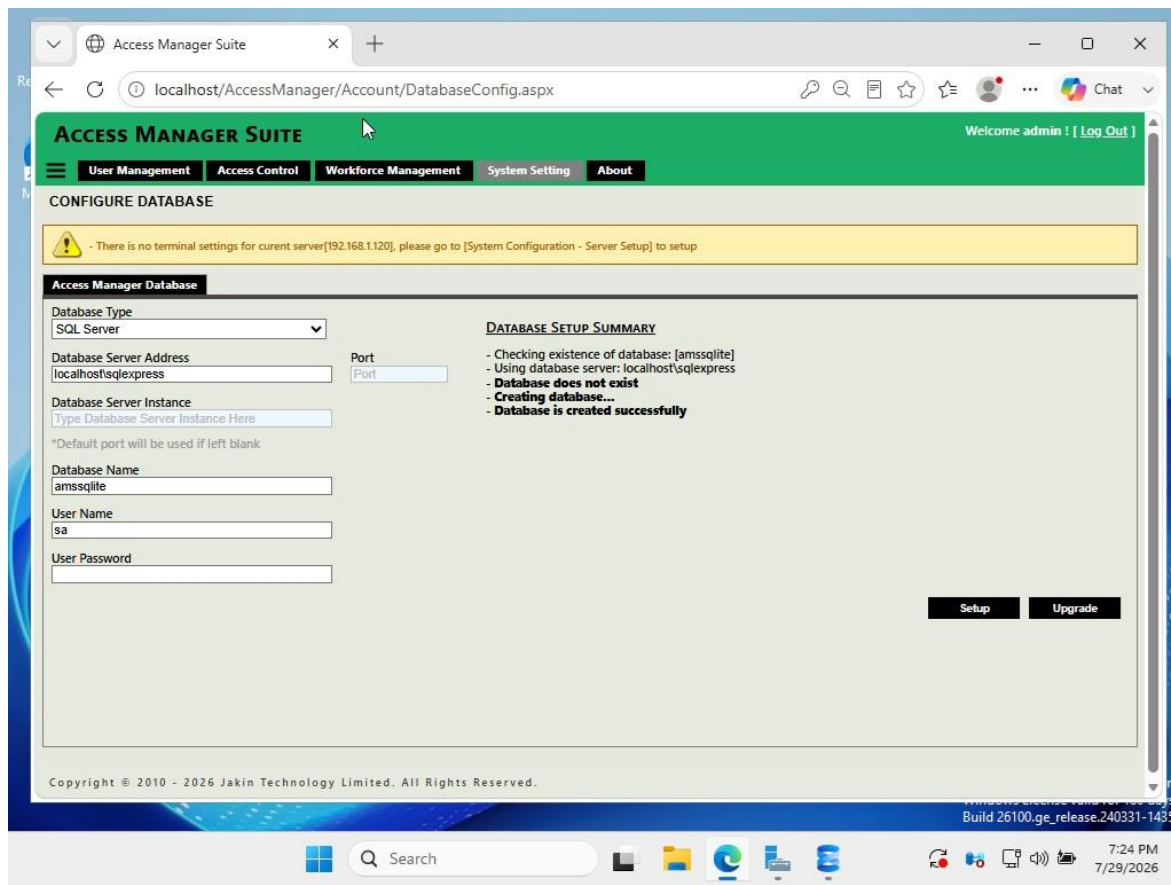
Password:

☐ Keep me logged in

Log In

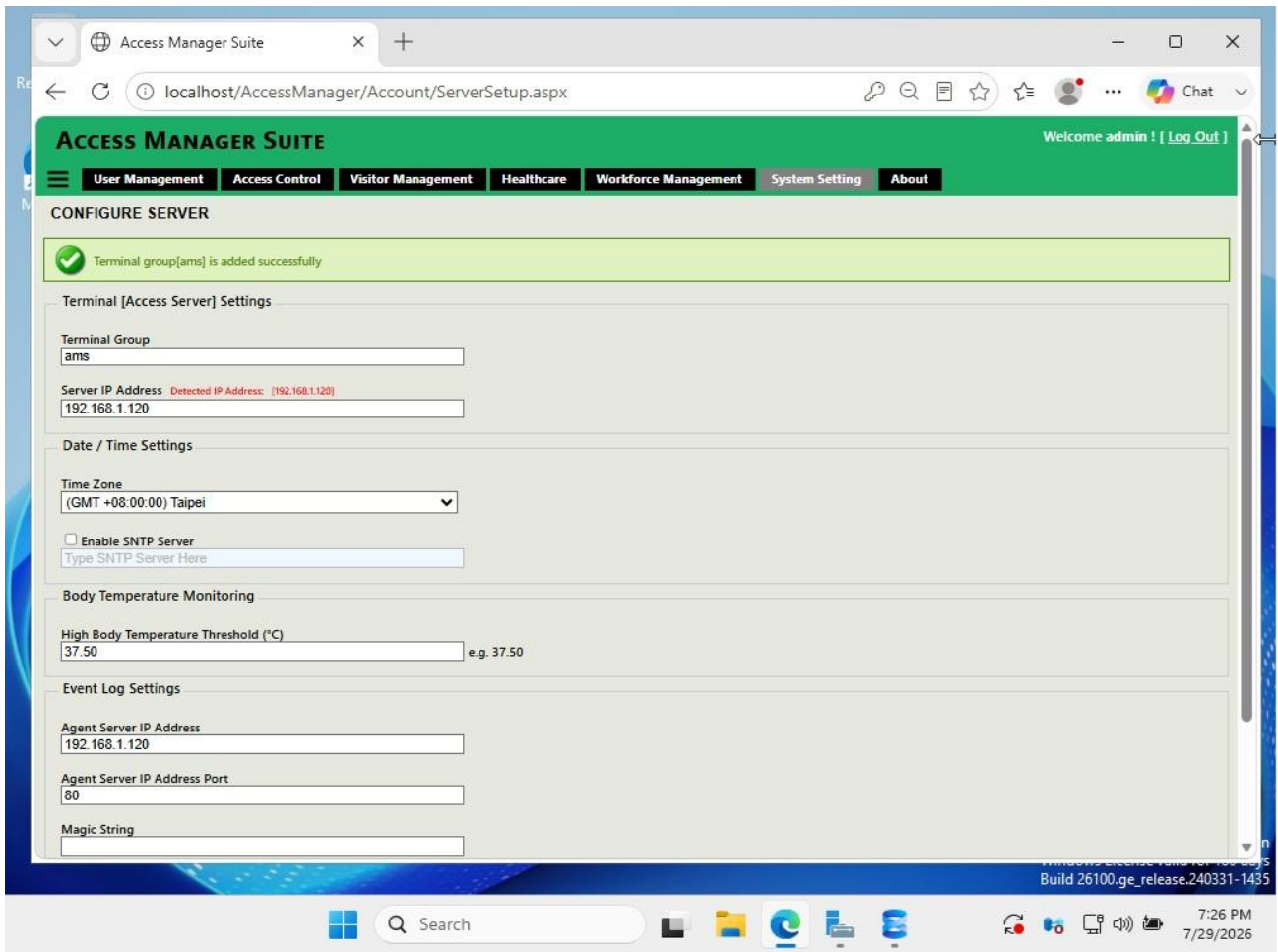
11. Configure Database Connection:

When prompted, configure the connection to your **MS SQL Server** database, and click the '**Setup**' button. AMS will automatically create the database and its tables, making them ready for use.



12. Configure Server Settings

Enter the **Terminal Group Name** (e.g., ams), verify the **AMS Server IP**, change the **Time Zone** settings, and enter the **Magic String** (e.g., 1). Finally, click the **Submit** button to save the server settings.



6. Post-Installation Configuration

6.1 Set Folder Permissions

After installation is completed, run the permission configuration script as Administrator:

13. Navigate to the unzipped on-prem AMS installation folder
14. Right-click on below file.
 - **AMS_Set_Folder_Permission.bat**



15. Select

- **Run as Administrator**

This script configures permissions to the AMS program data folders. Please follow the instructions displayed in the command prompt window to finish the operations.

6.2 Create AMS Temp Folder

Create a folder named **temp** under drive C, for example: C:\temp

7. ACTatek Device Configuration and Registration

Important Safety Notice: During device system backup or registration, the device will be temporarily out of service under system maintenance mode. **Please keep the door left open if this is for access control installation.**

7.1 Pre-Registration Steps

16. **Perform System Backup:** Complete device system backup before device registration with on-prem AMS.

Note: When registering a second (slave) or subsequent device with AMS, all existing device data will be deleted.

17. **Verify Terminal Clock:** Ensure the device's Terminal Clock settings are correctly configured, and the date/time is up-to-date
- 

18. **Configure IP Settings:** Verify the device's IP settings are correct so it can communicate with the on-prem AMS server

7.2 On-prem AMS Endpoint Configuration

Configure the on-prem AMS Endpoint URL on each device:

19. Navigate to the device's **[Access Client Setup]** page

20. Enter the on-prem AMS Endpoint URL:

`http://[AMS_Server_IP or domain name]/AccessServer/AccessService.asmx`

Replace **[AMS_Server_IP]** or **[domain name]** with your actual on-prem AMS server IP address or domain name

21. Click **[Set]** and **[Register]** button to start the device registration with on-prem AMS. Wait for the device registration process to be finished.

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
- Payroll Info

Access Control

- Access Groups
- Triggers
- Holidays Setting

Terminal Settings

- Terminal Setup
- WiFi Setup
- Authentication/Log Setup
- Terminal List
- Access Client Setup

ACCESS Client Setup

[master device registration succeeded...]

Connection Type	Lan
Access Client	
Device Status	Registered
Server Status	Online
Endpoint URL	http://192.168.1.120/AccessServer/AccessService.asmx
Interval(Seconds)	10
Domain Name Enable	☐
AMS host offline network test	☒

Last AMS host offline network test log

Error getting AMS URL test network log

8. Common Troubleshooting

8.1 Installation Failures

Issue: Setup.exe fails to install

Solution:

- Verify all .NET Framework versions are installed (Section 2.1)
- Ensure IIS is fully configured (Section 3)
- Check Windows Event Viewer for detailed error messages

8.2 Web Access Issues

Issue: Cannot access AMS web interface

Solution:

- Verify ports 80 and 443 are open in Windows Firewall
- Check antivirus software is not blocking IIS
- Verify IIS is running in Services (services.msc)

8.3 Device Communication Issues

Issue: Devices cannot communicate with on-prem AMS server

Solution:

- Verify device IP settings and network connectivity
- Confirm AMS Endpoint URL is correctly configured on devices
- Check firewall allows communication from device IP addresses
- Verify folder permissions were set correctly (Section 6.1)