JakinID

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

Installation Quick Guide

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 examples. Please follow each section carefully to ensure a successful deployment.

1. System Requirements

1.1 Hardware Requirements

Component	Specification
CPU Processor	Core i5 2.5 GHz or faster (64-bit)
Memory	16.0 GB or higher
Hard Disk Space	50.0 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 Browser	• 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

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

Install the following for back-end on-prem AMS database configuration:

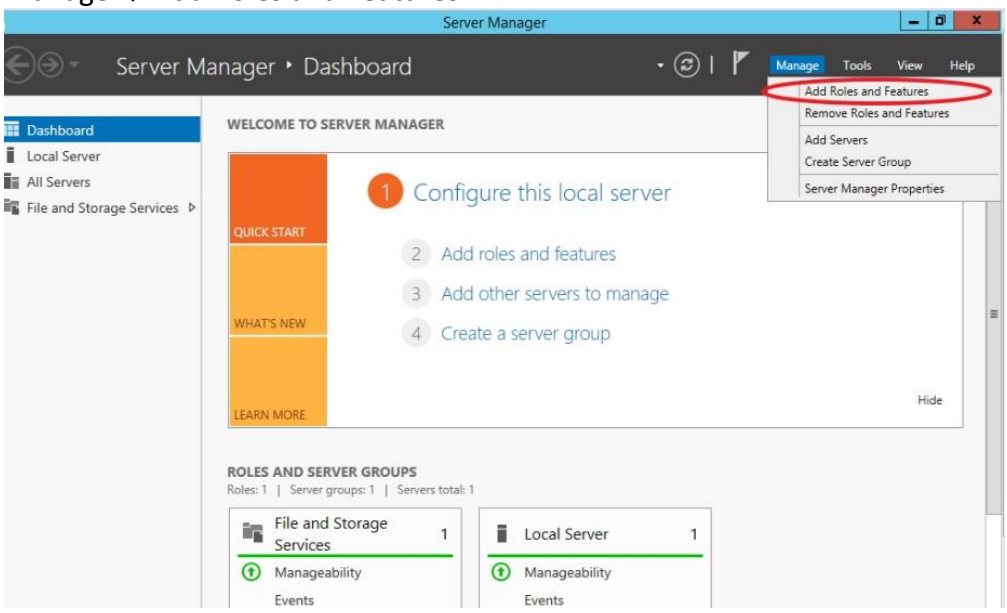
- MS SQL Server Express 2019 or above
- MS SQL Management Studio

3. IIS Web Server Configuration

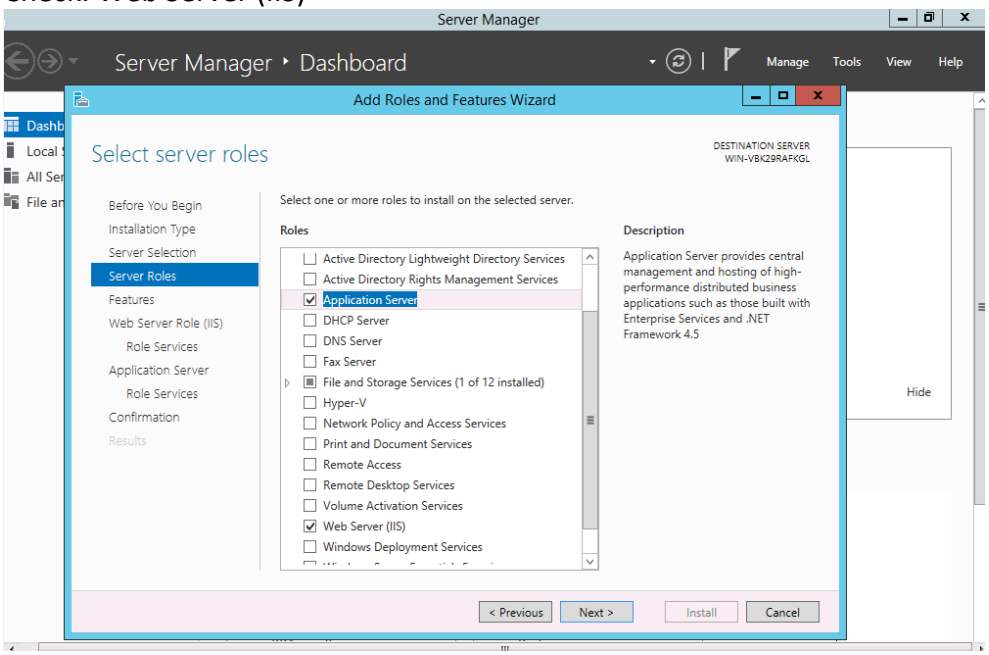
CRITICAL: IIS web server features and sub-features must be enabled before running setup.exe

3.1 Installing IIS Roles and Features

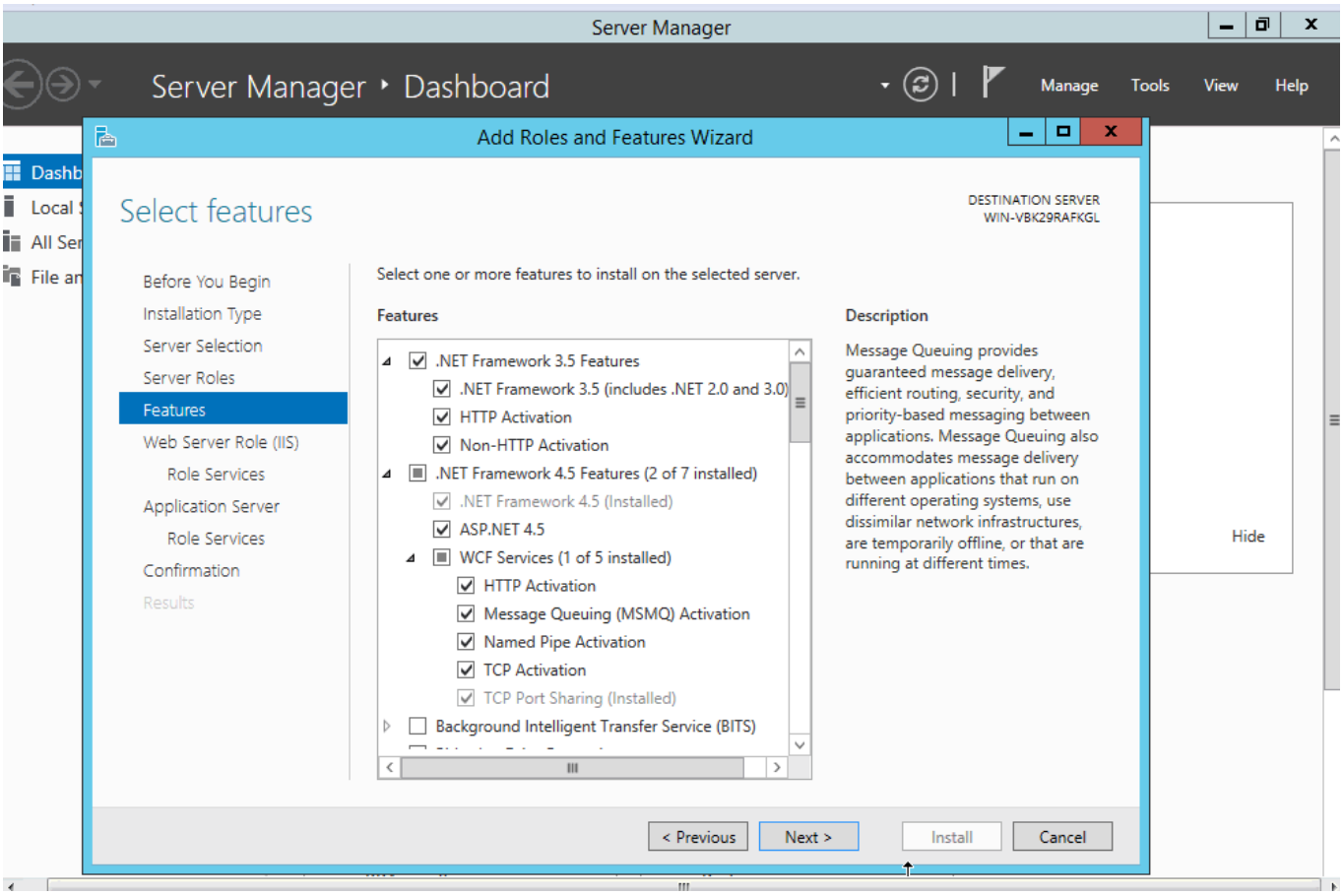
3. **Open Server Manager** and click
    - Manage → Add Roles and Features



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



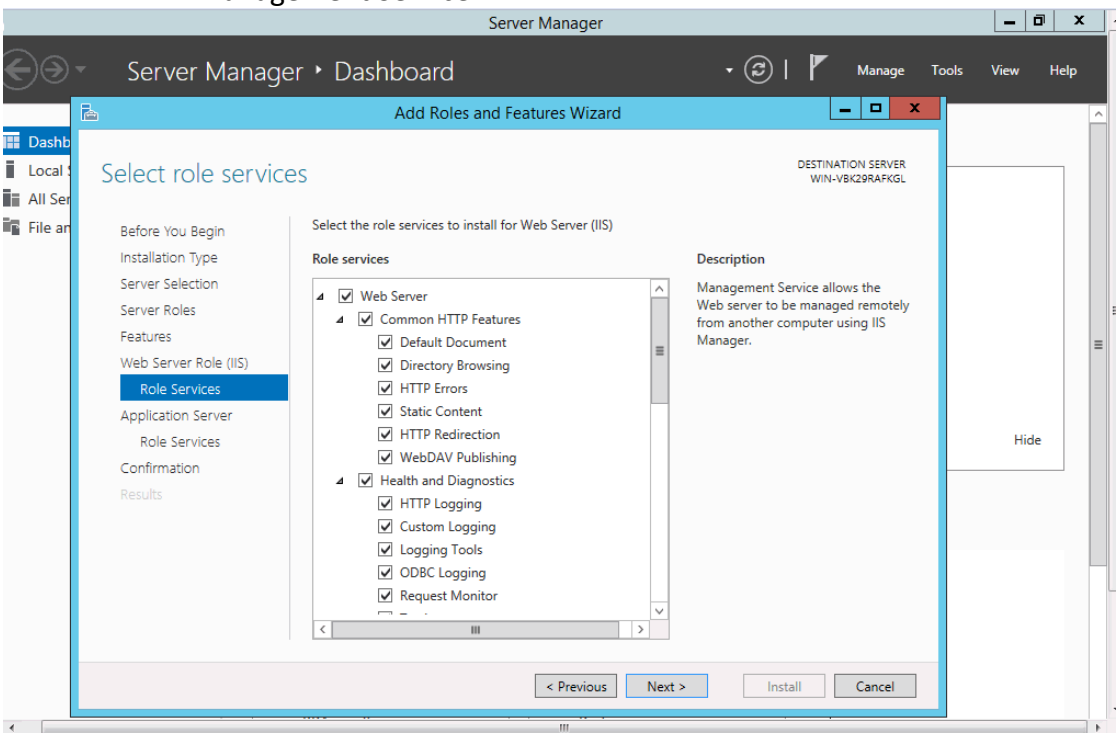
3.2 Web Server Role Services

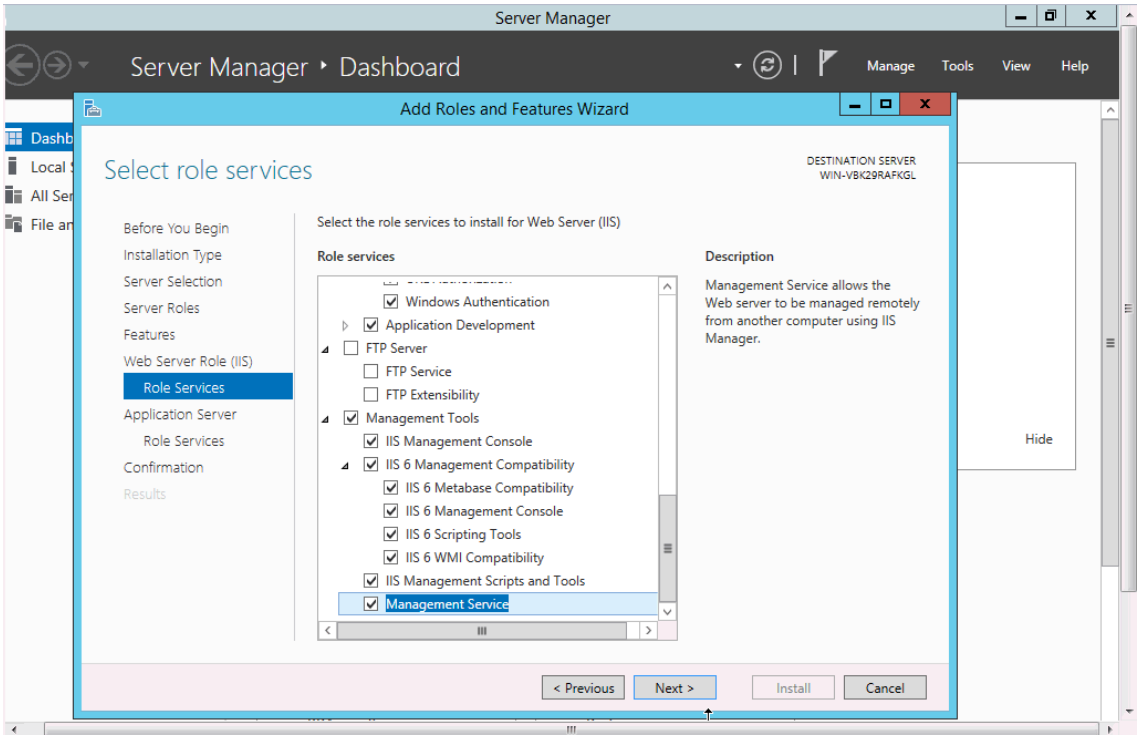
Under Web Server (IIS) → Role Services, enable the following:

- **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

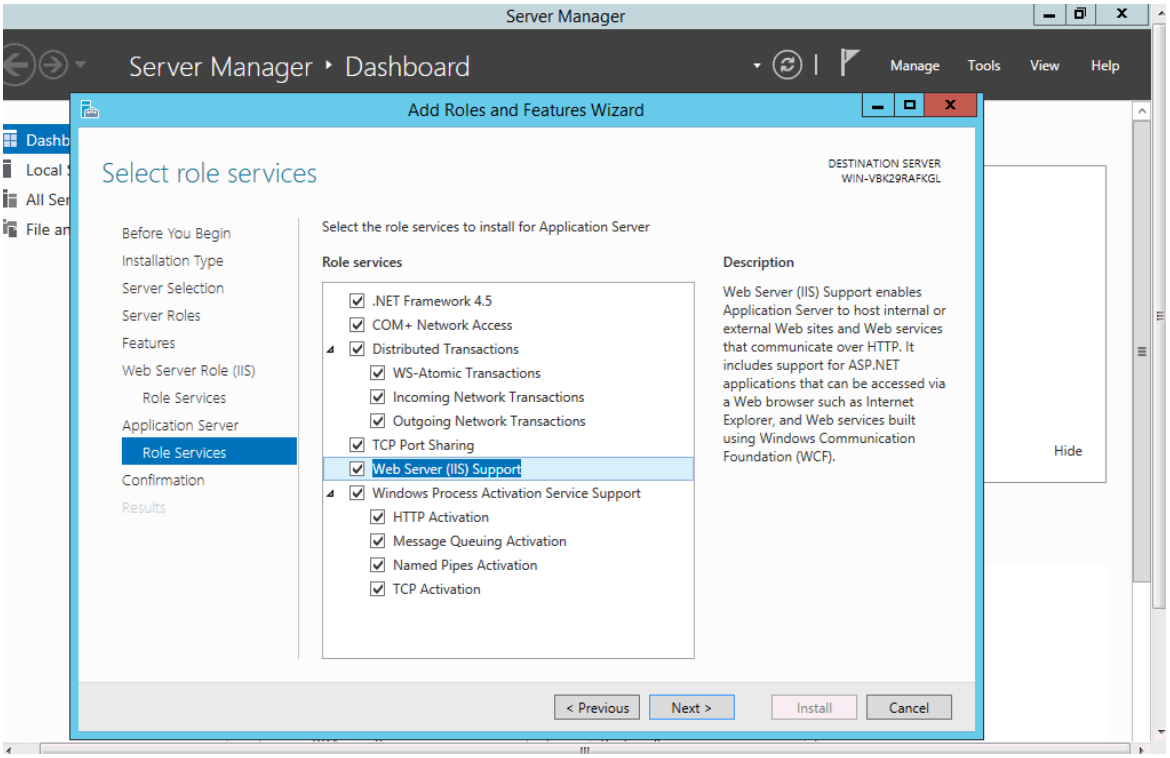




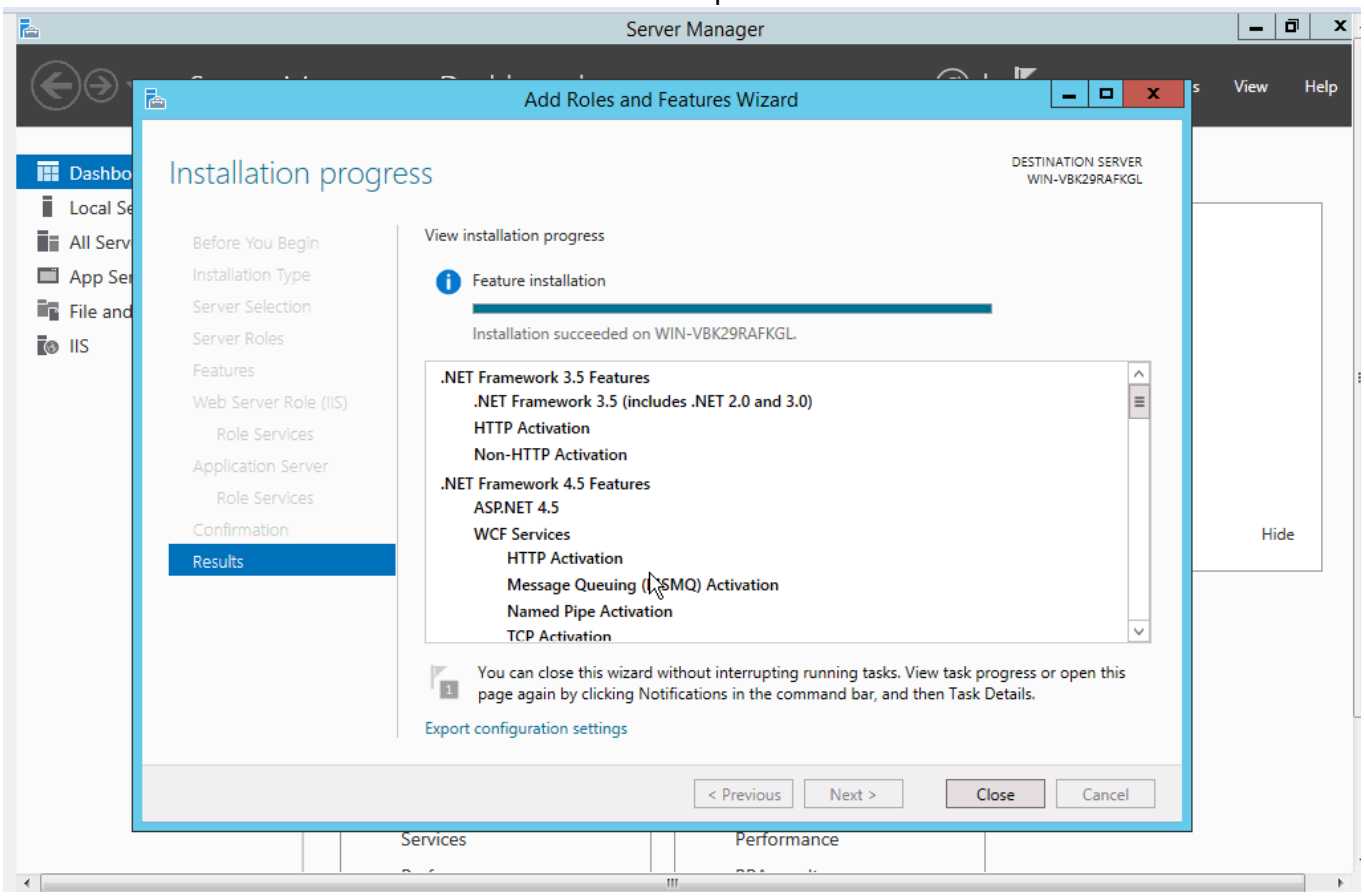
3.3 Application Server Role Services

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
9. **Run AMS Installer:** Locate and double-click
    - **setup.exe** from the on-prem AMS installation package
10. **Follow Installation Wizard:** Complete all prompts in the installation wizard
11. **Configure Database Connection:** When prompted, configure the connection to your MS SQL Server database using SQL Management Studio

6. Post-Installation Configuration

6.1 Set Folder Permissions

After installation completes, run the permission configuration script as Administrator:

12. Navigate to the unzipped on-prem AMS installation folder
13. Right-click
    - **AMS_Set_Folder_Permission.bat**
14. Select
    - **Run as Administrator**

This script configures permissions for the following folders:

- C:\inetpub\wwwroot\AccessManager\Images
- C:\inetpub\wwwroot\AccessManager\SilverApp
- C:\ProgramData\Actatek\AccessManager

7. ACTAtek Device Configuration

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

15. **Perform System Backup:** Complete device system backup before device registration with on-prem AMS
16. **Verify Terminal Clock:** Ensure the device's Terminal Clock settings are correctly configured and the date/time is up-to-date
17. **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:

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

18. Enter the on-prem AMS Endpoint URL:

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

19. Replace

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

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

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)