

Release Notes

AMD Management Plugin for SCCM v6.1

July 17, 2023

Introduction

This release notes is applicable to AMD Management Plugin for SCCM (AMPS). This version is targeted towards System Center Configuration Manager version 1910. The AMPS extends the Configuration Manager to support out-of-band management of client devices using DMTF's DASH initiative.

System requirements

Please check Microsoft documentation on installing Configuration Manager server and Configuration Manager Console. AMPS must be installed after Configuration Manager server, console are installed and configured.

AMPS Deployment Scenarios

You can deploy AMPS in three possible scenarios.

- **AMPS with SCCM Console and Standalone Site Server:** In this scenario, the SCCM Site server and the SCCM console are on the same system.
AMPS must be installed on this system containing both the Site server and console.
- **AMPS with SCCM Console:** In this scenario, the SCCM Site server and SCCM console are on two different systems.
Therefore, AMPS must be separately installed on the site server system and on the SCCM console system.
The plugin must first be installed on the site server and later on the console system. The plugin software automatically guides you to install only the required components on the site server and on the console.
- **AMPS with CAS (Central Administration Site):** In this scenario, the IT infrastructure contains the CAS and one or more primary

sites, along with optional secondary sites.

In CAS infrastructure, AMPS software must be installed in this order:

- Ensure that previous versions of AMPS (if any) are uninstalled from all the primary site servers and the CAS site system.
- Install AMPS first on the CAS system.
- After the installation on the CAS system is complete, install AMPS on all the primary site server systems that manage the DASH capable systems.
- You need not install AMPS on secondary site server systems.

Similarly, AMPS software must be uninstalled in this order:

- Un-install AMPS from all the primary site servers.
- Finally, un-install AMPS from CAS.

Note: Upgrade can be done in any order. Ensure that, post the upgrade, the versions of AMPS on the CAS, the primary Site servers, and the Administrative console are the same.

Installing and Un-installing AMPS

Installing/Upgrading AMPS

To install or upgrade the DASH plug-in for all the above-mentioned AMPS Deployment Scenarios, perform the following steps:

- Run the AMPS-*<version>*-AMD.exe installer.
- Follow the steps in the Install wizard to complete the installation.

Uninstalling AMPS

To uninstall AMPS, perform the following steps:

- In **Control Panel**, click **Programs** and then click **Programs and Features**.
- To uninstall AMPS, double-click the **AMD Management Plugin for SCCM** program, and select **Uninstall**.

Alternatively,

- Run the AMPS-<version>-AMD.exe installer.
- Click the **Remove** button to uninstall the plugin.

Integration points of AMPS in Configuration Manager Console

- 'All DASH Capable Systems', 'All DASH Managed Systems' and 'All DASH Unmanaged Systems' custom collections are created.
- The DASH Configuration screen can be found at:
Administration | Overview | DASH Management | DASH Configuration | Properties.

New features supported in AMPS v6.1

- Improvement in switching Device/Device Collections in some SCCM configurations (via 'skipping DASH capability check in menu' option in DASH Configuration).
- Bug fixes for KVM stability.

New features supported in AMPS v6.0

- Support for AIM-T 1.0, 2.0
- Fix for multiple bugs and performance improvement.

Note:

TLS Certificates for DASH HTTPS communication and KVM key for KVM feature have to be generated using AMD Provisioning Console (APC).
For AMPS,

1. ConsoleRootCertificate.crt – This is a Root CA certificate for communicating with DASH system. Import this certificate into Windows Certificate store (via "Manage Computer Certificates" application)
2. KVM SSH Key – This key is used for KVM session for AIM-T systems. This key has to be copied to "C:\Program Files (x86)\AMD Management Plugin for SCCM\certs" folder.

New features supported in AMPS v5.5

- Added DASH Capabilities to "Operations Administrator" role

- Added Discovery Schedule to Device Collection DASH options
- Added DASH Profile Inventory
- Appended site code to Default AMPS device collection for fresh installation
- Added a new report "DASH Memory Report"
- Updated User Guide
 - Added DASH User Action Report creation section
 - Updated Security Rights based authorization section
- DASHConfig 2.0 is packaged
- Renamed reports
 - 'Wake on DASH Status Report' to 'DASH Wake on LAN Status Report'
 - 'Non-DASH Systems Report' to 'DASH Non DASH Systems Report'
 - 'Undiscovered Systems Report' to 'DASH Undiscovered Systems Report'
- Fix for multiple bugs and performance improvement

New features supported in AMPS v5.0

- Added support for Realtek F Series KVM
- Support for 'Next Single Use Boot' configuration in Boot Control Profile
- Fix for multiple bugs and performance improvement

New features supported in AMPS v4.5

- Option provided to trust or reject self-signed TLS certificates for HTTPS DASH communication.
- DASHConfigRT is packaged with AMPS to configure Realtek based DASH systems.
- Following packages were updated (CIM Schema-2.52, Putty-0.73).
- Japanese Language support has been added.
- Support version 1910 of SCCM (Microsoft Endpoint Manager - MEM)
- Support Windows Server 2019
- Added support for Marvell 10GbE Ethernet (Shared mode only)

New features supported in AMPS v4.2

- Case-sensitivity for Authentication Identifier and Username columns is introduced in Configuration screen

- Performance enhancements by fetching the exact credentials for target systems in devices collections use case
- Support for Wake on LAN Functionality.
- Displaying Last-Wake-On-LAN time in WOL Reports.
- Auto Discovery and DASH WakeUp feature is enhanced.
- Integrity check for authentication table is added.

New features supported in AMPS v4.1

- Authentication identifier introduced in Configuration screen
- Performance and network enhancements to KVM use case
- Support up to Configuration Manager update 1802, and clients Windows 10 update 1803.

New features supported in AMPS v4.0

- KVM Redirection support – Boot To BIOS screen workflow.
Note: Platform and DASH LoM must support KVM profile. The DASH LoM must be set to obtain IP address from DHCP server to use this feature.
- Support version 1706, 1702, 1610, 1606, 1602 & 1511 of SCCM
- Support Windows Server 2016 & Windows 10 OS
- Support DASH CIM Schema 2.48.0

New features supported in AMPS v3.6

- Option to enable/disable 'Auto DASH Discovery' and 'DASH WakeUp' in DASH Configuration screen.

New features supported in AMPS v3.5

Following reports are created and deployed:

- DASH Diagnostic Report
- Wake on DASH Status Report
- DASH Managed Systems Report
- DASH Unmanaged Systems Report
- Non DASH Systems Report
- Undiscovered Systems Report

New features supported in AMPS v3.0

- Firmware Upgrade on device and collection.
This feature enables the user to upgrade or downgrade the firmware of a device or a collection.
- The ability to schedule DASH tasks on a collection:
 - Power on collection.
 - Firmware upgrade on collection.
- A DASH Scheduled Tasks tab, which allows the user to view all the scheduled DASH tasks.
- "All AMPS Status Messages" Status Message Queries, which enables user to view all status messages related to AMPS.
- Three collections of DASH systems:
 - All DASH Capable Systems - contains all DASH systems.
 - All DASH Managed Systems - contains all manageable DASH systems, that is, DASH systems that are provisioned with working credentials.
 - All DASH Unmanaged Systems - contains all unmanageable DASH Systems which are not provisioned correctly.

Features supported in AMPS v2.5

- Boot text image feature – text-based ISO images can be remotely deployed.
- Performance enhancements to handle large number of devices in a collection.

Features supported in AMPS v2.3

- Role based administration is enabled for DASH tasks. User must have 'Remote Tools Operator' role and necessary scope on the collection to perform DASH tasks. 'Full Administrator' also has access.
- Support for Record Log profile.
- DASH Wakeup (replacement for Wake on LAN) supported for,
 - Power management in Collection
 - Application deployment

- Program deployment
- Task sequence deployment
- Software updates deployment
- Power on collection supports additional power states such as 'Hibernate', 'Sleep'.
- DASH Configuration is moved under |Administration|Overview|DASH Management node.
- DASH action performed by users is logged in Configuration Manager Status Message Viewer.
- AMPS supports DMTF DASH 1.2 profiles.

Features supported in AMPS v2.2

- Text Redirection.
- USB Redirection.
- Inventory.
- Alerts subscription, un-subscription and reception.
- Support for CAS installation with multiple primary sites.

Features supported in AMPS v2.1

- Support for digest & active directory authentication.
- Multiple authentication schemes, up to 3 accounts supported.
- Discovery available on per device & on per collection.
- Power control available on per device & on per collection.
- User friendly power state names displayed in power window, along with DASH standard names.
- Boot control available on per device.
- DASH Inventory available in Configuration Manager Resource Explorer.
- DASH Wakeup feature is supported. DASH Wakeup command is sent to all DASH Capable devices, when a package is deployed with 'Send wake-up packets' option.

Note

1) AMPS version on Configuration Manager Site server installation and

Configuration Manager Console-only installation must be same.

2) User guide is available in the download package (as Word document) and also integrated into DASH UI screens (in CHM format)

3) DASH Service log can be found on the Site Server in the location:
%ALLUSERSPROFILE%\AMD Management Plugin for
SCCM\DASHService.log. Maximum log size is 10MB. Log file is automatically rotated, and one previous log file is retained.

4) Refer Active Directory configuration document in the package for using active directory authentication scheme.

5) For users with non-administration permissions, to use AMPS, permission must be enabled on DASH WMI namespace:

- a) Go to Start|Run, enter WMIMgmt.msc and open the console.
- b) Go to the Properties of WMI Control
- c) Go to the Security Tab
- d) Select "Root\DASH" and open "Security"
- e) Ensure "Authenticated Users" has "Execute Methods", "Enable Account" and "Remote Enable" rights.

Validated configurations

Database: SQL Server 2019, SQL Server 2016, SQL Server 2014

Operating Systems	Configuration Manager/MEM Site System	Configuration Manager/MEM Console
Windows 2019 Server	√	√
Windows 2016 Server	√	√
Windows 2012 Server R2	√	√
Windows 10	-	√
Windows 11	-	√

√ = Supported