AIM-T User Guide - Windows

Publication #	**57880**	Revision:	**5.3**
Issue Date:	**February 2026**		

Advanced Micro Devices

© 2026 Advanced Micro Devices, Inc. All rights reserved.

The information contained herein is for informational purposes only, and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD's products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale. Any unauthorized copying, alteration, distribution, transmission, performance, display or other use of this material is prohibited.

Trademarks

AMD, the AMD Arrow logo, AMD AllDay, AMD Virtualization, AMD-V, PowerPlay, Vari-Bright, and combinations thereof are trademarks of Advanced Micro Devices, Inc. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

Linux is a registered trademark of Linus Torvalds.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the US and/or other countries.

PCIe is a registered trademark of PCI-Special Interest Group (PCI-SIG).

Qualcomm trademark of Qualcomm Incorporated, registered in the United States and other countries.

Realtek is a trademark of Realtek Semiconductor Corporation.

USB Type-C® and USB-C® are registered trademarks of USB Implementers Forum.

Reverse engineering or disassembly is prohibited.

USE OF THIS PRODUCT IN ANY MANNER THAT COMPLIES WITH THE MPEG ACTUAL OR DE FACTO VIDEO AND/OR AUDIO STANDARDS IS EXPRESSLY PROHIBITED WITHOUT ALL NECESSARY LICENSES UNDER APPLICABLE PATENTS. SUCH LICENSES MAY BE ACQUIRED FROM VARIOUS THIRD PARTIES INCLUDING, BUT NOT LIMITED TO, IN THE MPEG PATENT PORTFOLIO, WHICH LICENSE IS AVAILABLE FROM MPEG LA, L.L.C., 6312 S. FIDDLERS GREEN CIRCLE, SUITE 400E, GREENWOOD VILLAGE, COLORADO 80111.

Contents

List of Figures

List of Tables

Revision History

Date	Revision	Description
February 2026	5.3	• Updated Troubleshooting sections: 5.1.6, 5.2.5, and 5.2.6
December 2025	5.2	• Updated section 2.2.7 Remote Disk Wipe with a note for diskinfo command. • Edits to Section 2.2.9.3.2 WinRE KVM BSOD not supported on platforms without EC. • New Section 3.1.1 Network Ports requirement for AIM-T • Updated section 3.5.2 dash wake from sleep. • Updated Section 5.1.4 KVM update for multiple monitors. • Updated Appendix A, details for enabling AD in APC.
October 2025	5.1	• KVM Boot to WinRE (Windows Recovery Environment) • Update Troubleshooting section 5.1.5 missing alert event and section 5.2.4 terminating TCR session. • Updated Section 2.2.7 with a note for dike wipe operation. • Section 3.5.1, AMS installation • Update 2.2.7, Note Added at the end of section
September 2025	5.0	• Update section 5.1.3. • Updated Section J.2 with new APC image and Certs path • Update tools download link to (www.amd.com/DASH) • QCOM WLAN is not supported from AIM-T 5.0. • Section 3.2.1 Pre-Boot Wi-Fi needs to be disabled for AIM-T 2.1 and earlier releases. • Documented AIM-T 5.0 features • Updated the DASH profile Specification version • Added new section: Enable auto EAP TLS Certificate generation and Signing Feature Added installation details for Windows OS in Appendix J
November 2024	4.6	Updated section 3.1.
October 2024	4.5	Documented AIM-T 4.5 features.
April 2024	3.1	Added information about adding Wi-Fi access point profile.
February 2024	3.0	A few general edits and updates.
September 2023	2.2	Added a note in Appendix E.
April 2023	2.1	One minor edit in Chapter 1.
March 2023	2.0	• Updated figures in Appendix A. • Added Appendix I. • Incorporated changes from the technical review.
September 2022	1.0	Initial version.

Acronyms and Abbreviations

Table 1. Acronyms and Abbreviations

Term	Definition
ACMS	AMD Cloud Manageability Service
AIM-T	AMD Integrated Management Technology
AMD	Advanced Micro Devices
AMS	AIM-T Manageability Service
AP	Access Point
APC	AMD Provisioning Console
BIOS	Basic Input/Output System
DASH	Desktop and Mobile Architecture for System Hardware
DMTF	Distributed Management Task Force
IP	Internet Protocol
IT	Information Technology
KVM	Keyboard Video and Mouse
LAN	Local Area Network (aka Ethernet)
NIC	Network Interface Controller
OEM	Original Equipment Manufacturer
OS	Operating System (such as Microsoft® Windows® and Linux®)
SoC	System on a Chip
UI	User Interface
WLAN	Wireless Local Area Network (aka Wi-Fi)
VNC	Virtual Network Computing
EAP-TLS	Extensible Authentication Protocol–Transport Layer Security
WinRE	Windows Recovery Environment
OEM	Original Equipment Manufacturer
EC	Embedded Controller

Chapter 1 Introduction

This document specifies how users (typically, an IT administrator) manage systems remotely in an enterprise environment using AMD's AIM-T solution on both wired and wireless networks. AIM-T is a hardware and software solution that enables AMD-based commercial platforms to provide secure and remote management capability. This is achieved by integrating a dedicated core in AMD's Client SoC (starting from AMD Ryzen^{TM} PRO 6000 Series Processors) along with all the supporting SoC/platform level hardware, firmware, software applications and interfaces. With the help of special WLAN and LAN modules, AIM-T can manage a remote system through a Wi-Fi or ethernet connection.

For support, contact *dashsupport@amd.com*.

Chapter 2 AIM-T Capabilities and Features

2.1 Supported DASH Profiles

AMD's Manageability solution is continuously evolving technology, adding new features with every release. AIM-T 4.5 is our latest release. This section lists supported DASH profiles and describes other manageability features.

Table 2. List of Supported Profiles

No	Release	Profile Specification	Profile Description
1	AIM-T 1.0	DSP1058	Base Desktop and Mobile Profile
2		DSP1033	Profile Registration Profile
3		DSP0226	WS-Management Specification
4		DSP0227	WS-Management CIM Binding Specification
5		DSP0230	WS-CIM Mapping Specification
6		DSP1029	OS Status Profile
7		DSP1011	Physical Asset Profile
8		DSP1022	CPU Profile
9		DSP1026	System Memory Profile
10		DSP1014	Ethernet Port Profile
11		DSP1037	DHCP Client Profile
12		DSP1038	DNS Client Profile
13		DSP1035	Host LAN Network Port Profile
14		DSP1036	IP Interface Profile
15		DSP1027	Power State Management Profile
16		DSP1075	PCI Device Profile
17		DSP1034	Simple Identity Management Profile
18		DSP1116	IP Configuration Profile
19		DSP1018	Service Processor Profile
20		DSP1023	Software Inventory Profile
21		DSP1017	SSH Service Profile
22		DSP1039	Role Based Authorization Profile
23		DSP1061	BIOS Management Profile
24		DSP1012	Boot Control Profile
25		DSP1013	Fan Profile

No	Release	Profile Specification	Profile Description
26		DSP1009	Sensors Profile
27		DSP1010	Record Log Profile
28		DSP1054	Indications Profile
29		DSP1076	KVM Redirection
30		DSP1030	Battery Profile
31		DSP1025	Software Update Profile
32	AIM-T 2.0	DSP1024	Text Console Redirection Profile
33		DSP1108	Physical Computer and System View Profile
		DSP1012	Enhancement to Boot Control Profile - Boot Devices support, Boot Order Change/Set Next
		DSP1034	User Add/Delete support, Role Change/Assign (Enhancement to Simple Identity Management Profile).
34	AIM-T 3.0	DSP1015	Power Supply Profile
35	AIM-T 4.0	Custom Feature	Office/Home network Detection
		Custom Feature	KVM Consent (user consent for allowing KVM)
		DSP0226	Mutual Authentication
		Custom Feature	Wi-Fi Sync
36	AIM-T 4.5	DSP1070	Opaque Management Data Profile
		Custom Feature	Web UI for MPM
		Custom Feature	Disk Profile (Disk Info)
		Custom Feature	Active Directory based authentication
37	AIM-T 5.0	Custom Feature	Remote Disk Wipe
		Enhancement	OS-KVM now supports Higher Resolution up-to 4K [3840x2160]
		Enhancement	Support Cloud wake from x86 NRC with MediaTek and RealtekWLAN.
		Custom Feature	Automatic renewal of EAP TLS Certificate
38	AIM-T 5.1	Custom Feature	KVM Boot to WinRE (Windows Recovery Environment)

Table 3. Supported DASH version based on AIM-T Releases.

AIM-T Version	DASH Version
1.0	1.3
2.0	1.3
3.0	1.3
4.0	1.3
4.5	1.3
5.0	1.4
5.1	1.4

2.2 Custom Profile and Features

2.2.1 Mutual Authentication (MA)

MA is a 2-way authentication, where-in both the target (AIMT system) and DASH CLI host identify and verify themselves using TLS Certificate. DMTF (Distributed Management Task Force) supports multiple authentication mechanisms, one such mechanisms is to support mutual TLS (Mutual Authentication) used as below:

Sample DASHCLI command:

Dashcli.exe -h <hostname> -u <username> -P <password> -cert "<Mutual_Authentication_Certificate_File_ >" enumerate computersystem.

Note:

- *MA feature needs to be enabled, and TLS certification generated during provisioning package creation using APC tool.*
- *Client Certificate and Private Key should be available while sending DASH command. Both can be appended to the same file and sent as part of –cert DASHCLI command.*
- *For addition details, see:* https://www.dmtf.org/sites/default/files/standards/documents/DSP0226_1.2.0.pdf, *Section: C.3.7)*

2.2.2 KVM Consent

KVM consent, aka ensuring user consent for allowing KVM when in OS, gives users of managed system the option to allow or deny KVM access to their systems when a remote IT-admin initiates a KVM session.

Note:

1) *KVM consent feature must be enabled in the provisioning package (with APC tool). If not enabled, consent is deemed to be given.*

2) *Consent is not applicable in locked screen, this is to allow IT admin to login to the system even when the screen is locked and employee is not present to give consent.*

2.2.3 Active Directory (AD) Based Authentication

AD uses Kerberos, a network authentication protocol to provide user login and authentication services (credential validation username/password) to Organize and Manage user accounts, User Groups, and enables only authorized users access to managed systems.

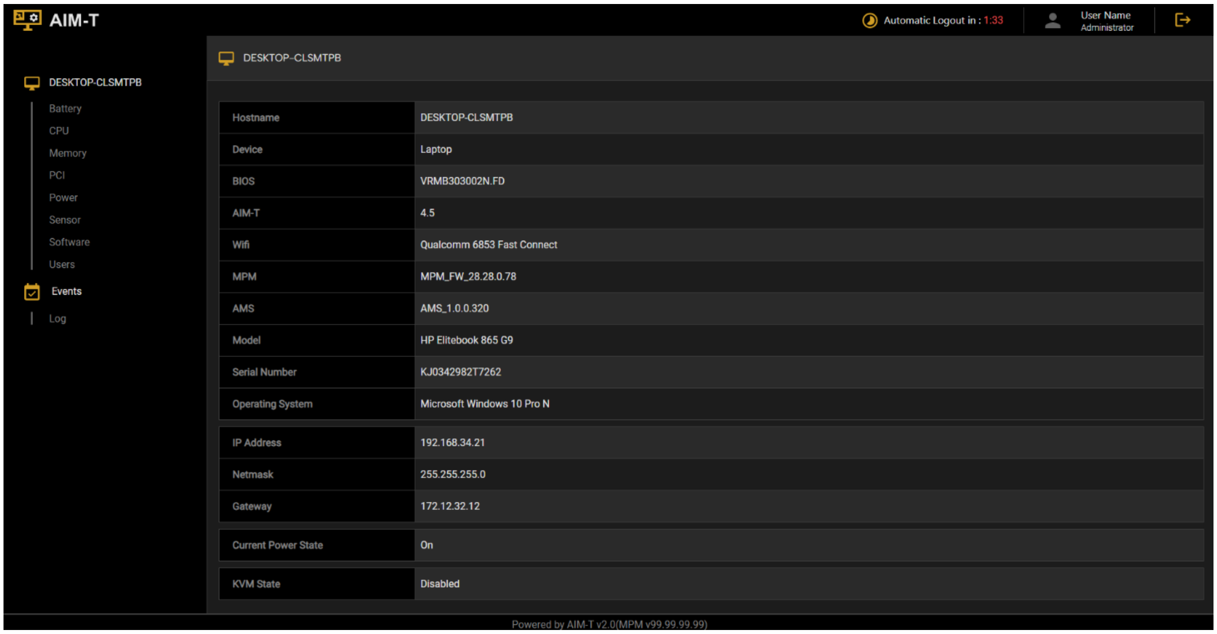
With AD, DASH commands can use Active Directory credentials to authenticate and manage remote systems.

Note: *AD feature needs to be enabled in provisioning package, for more details refer APC user Guide.*

Note: For successful authentication, AD Server and managed system time should be in sync and time difference of up-to 300 seconds [5 minutes] is acceptable for authentication.

2.2.4 Web User Interface

This functionality enables IT admins to view supported dash profiles and manage a single node system via a web interface. WEBUI feature must be enabled in the provisioning package and can be launched in compatible browsers by typing: *https:\\HostName_OR_IP:664*



Hostname	DESKTOP-CLSMTPB
Device	Laptop
BIOS	VRMB303002N.FD
AIM-T	4.5
Wifi	Qualcomm 6853 Fast Connect
MPM	MPM_FW_28.28.0.78
AMS	AMS_1.0.0.320
Model	HP Elitebook 865 G9
Serial Number	KJ0342982T7262
Operating System	Microsoft Windows 10 Pro N
IP Address	192.168.34.21
Netmask	255.255.255.0
Gateway	172.12.32.12
Current Power State	On
KVM State	Disabled

Figure 1. AIM-T WebUI Landing Page

Note: *We recommend Chrome and Microsoft Edge web browsers.*

2.2.5 Cloud Manageability

IT administrators can use this feature to manage enterprise systems even when those systems are outside the enterprise network thus overcoming any requirements for the host and managed systems to be a part of the same network or domain.

With AIM-T 5.1 release, Cloud Manageability feature is now enhanced to manage systems even if they are in Hibernate or Shutdown states [S4/S5 states. This is currently supported on systems having MediaTek and Realtek WLAN interface.

Note: *This feature must be enabled and configured during provisioning package creation using the APC tool and the ACMS software deployed. For more information see Appendix I.*

Note: Cloud manageability is not supported on Desktop platforms

2.2.6 Wi-Fi Sync and Office/Home Network Detection

This is a smart feature which auto detects network changes of managed systems and allows IT admins to continue to manage systems when they move outside the enterprise network and connect to home or public access points even if these networks were not provisioned.

Note:

This feature requires cloud Manageability to be enabled during provisioning package creation using the APC tool and the ACMS software deployed. For more information see Appendix I.

Enterprise network access details must be configured in the provisioning package. Up to eight additional most-recently connected (public, non-enterprise) access points' details are auto saved, if not provisioned.

2.2.7 Remote Disk Wipe

Remote disk wipe is a new feature which enables cryptographic erase/wipe of a storage disk connected to one or more managed nodes by an IT administrator using AMD provided DASH tools such as DASH CLI,ensuring that all data present on the remote system's hard drive will be erased permanently before its reprovisioned to be assigned to a different user or recycled Usage:

1. Enumerate disks to identify disk information in the system

```
dashcli.exe -h <hostname>   -C -S https -p 664  -u <username> -P <password> enumerate diskinfo
```

Command results will show disk information for each disk present in the system such as, Disk ID, Disk Serial Number, Disk Capacity.

Note: The *enumerate diskinfo* command does not show OS disk partition information.

2. Issue Disk Wipe Request “WipeDrive” utilizing above info

dashcli.exe -h <hostname> -C -S https -p 664 -u <username> -P <password> -t diskinfo[0] wipedisk enable

3. Power cycle the target system

dashcli.exe -h <hostname> -C -S https -p 664 -u <username> -P <password> -t computersystem[0] power cycle

***Note**: Target system needs to be restarted within 110 seconds of issuing the “Wipedisk” command. Else, Disk Wipe request gets deactivated and returns to original state.*

4. Disk Wipe Results
    a. Admin can refer to the result by querying Record Log and Log Entry commands for some of the below event IDs.
        i. 3000: Disk Wipe Started
        ii. 3001: Disk Wipe performed successfully.
        iii. 3002: Disk Wipe could not be performed due to an error.
5. Deactivating Disk Wipe Request
    a. Once Disk Wipe request has been activated using the above mentioned commands, for any reason, if the wipe operation needs to be aborted before power cycling the target, administrator can use below DASH command to achieve the same.

       dashcli.exe -h <hostname> -C -S https -p 664 -u <username> -P <password> -t diskinfo[0] wipedisk disable

***Note**: The types of disks supported is determined by OEM BIOS. By default, AMD reference design supports self-encrypted NVME SSD devices that are connected internal to the platform and do not support external devices. Wipe functionality is currently unsupported for disks with passwords enabled.*

***Note**: Data once erased using this feature cannot be recovered.*

Note: *After the Disk Wipe is successful, the target will remain in BIOS mode and in a manageable state. The target continues to be in Managed mode for every boot until the OS is installed. However, if OS installation is un-successful for whatever reason, the system may be in an unmanageable state, and it is advised to shutdown the system so that it can be managed again.*

2.2.8 Auto EAP TLS Certificate Generation and Signing Feature

Managed systems use EAP TLS certificates to establish secure connections with the enterprise wireless network. Since these certificates have a validity period, target managed systems have this feature to automatically renew certificates before they expire. For more information to enable and use this refer *section 3.7* below.

Note: *Available with AIM-T 5.0 release onwards.*

2.2.9 KVM boot to WinRE (Windows Recovery Environment)

KVM in WinRE / safe mode screens can be used to troubleshoot issues like BSOD [Blue Screen of Death] that can cause repeated system reboots. For e.g. BSOD resulting from events like the CrowdStrike blue Friday. In such cases IT administrators will be able to remotely enter KVM and

- Boot the computer to recovery environment.
- Navigate to the directory or location of the faulty driver/application.
- Delete the files or uninstall the problematic driver/application.
- Restart and return to normal Windows mode.

Note: *WinRE KVM is supported only on the wireless interface.*

Note: *AMS 5.1 is required. The standalone installer sets up all required files for AIM-T in Windows Recovery Environment and un-installing AMS removes all WinRE extensions. In case of AMS Microsoft store app, AMD chipset driver package must be installed.*

2.2.9.1 AMS 5.1 Installation

The AMS 5.1 installer will automatically add all necessary changes for supporting WinRE. These exact changes are also performed by the silent installer option.

Chipset Installer supporting AIM-T 5.1 adds the AMS-MailboxDrv driver to the recovery image. Installing AMS-MailboxDrv updates the recovery environment settings in accordance with Microsoft’s recommendations.

During the AMS installation process, if BitLocker is enabled, AMS installer will pause BitLocker temporarily, modify the recovery image with the above changes and then resume the BitLocker. This process may take a few minutes to complete.

Note: *The End User acknowledges and accepts the consequences of the foregoing operation and shall be responsible for ensuring their system is returned to the original configuration.*

Note: *For BitLocker functionality, it is recommended to enable BitLocker first and then install AMS. If BitLocker is enabled after AMS installation, then manual activation (reagentc /enable) of Windows Recovery Environment is needed.*

2.2.9.2 Starting KVM in WinRE

To launch KVM in WinRE, a new DASH command, '***startwinrekvm'***, has been introduced in DASHCLI 8.0 to facilitate WinRE KVM support.

For example, execute the following command:

`dashcli.exe -h <HostName> -S https -p 664 -u <username> -P <password> -cert "C:\Program Files\DASH CLI 8.0\certs\MutualAuthCert.pem" -t kvmredirection[0] startwinrekvm`

2.2.9.3 Uses cases for WinRE KVM

2.2.9.3.1 Starting WinRE session from Windows Desktop

1. Execute DASHCLI command *startwinrekvm and wait for system to reboot.*

2. Once the system reboots and viewer connects back it shows BIOS setup screen, use continue option to enter recovery mode.

2.2.9.3.2 From BSOD screen or from WinRE screen

1. Manually shutdown the system by pressing the power button, wait for system to shutdown and then execute DASH command *startwinrekvm*, system will wakeup now and KVM viewer should connect in BIOS KVM mode and finally to recovery mode.

Note: On certain systems, triggering a Blue Screen of Death (BSOD) results in a complete system hang accompanied by a black screen. This case will not be supported in WinRE KVM.

Note: On systems without an Embedded Controller (EC), typically desktops and workstations, WinRE KVM is not supported in the event of a BSOD.

2.2.9.3.3 Entering Safe mode

1. In Windows Recovery Environment, go to the “Choose an option” screen.

2. Select Troubleshoot > Advanced options > Startup Settings.

3. Click Restart and select a Safe Mode option.

4. The Safe Mode screen will appear in the KVM Viewer.

Note: *AMS Tray Icon won’t be visible in safe mode environment if AMS is installed from MSIX package as the safe mode environment disallows MSIX applications with foreground (UI) component.*

2.2.9.3.4 Ending the WinRE session

Closing the KVM Viewer ends the WinRE KVM session and reboots the platform to Windows OS.

2.2.9.3.5 Supported options during WinRE session

The following table shows the various actions the user can select from WinRE screen.

Table 3. Options for WinRE session

Action/Option chosen	Expected Behavior
Continue	The system reboots and shows BIOS setup in viewer. **Caution:** *After the system reboots and displays the BIOS setup screen, please terminate the KVM session by closing the viewer. Proceeding with the BIOS setup by selecting 'Continue' may cause the system to enter an unmanageable state.*
Turn Off	System shutdowns and is manageable.
Close Viewer	Ends KVM session and reboot the system to windows.
All other options: Troubleshoot/use a device	Continues in KVM session. **Note:** *User must close viewer to end WinRE KVM session, choosing any other option will make the system un-manageable.*

Note: *If there is network disconnection during WinRE KVM session, viewer will try to re-connect back to target until a timeout of 180 seconds, after timeout target will boot to OS and be in a manageable state.*

The following table shows the various supported options the user can choose from viewer window when in setup screen of recovery environment.

Table 4. Options in Setup screen of Recovery Environment

Key Press/Action	Expected Behavior
F4 - Safe Mode without Networking	System goes to safe mode and screen visible in viewer
F5 – Safe Mode with Networking	The system will boot to safe mode with networking.
F6 – Safe Mode with command prompt	System goes to safe mode with command prompt screen.

F10 or 0 for more options	Viewer shows WinRE startup settings screen
“OS shutdown” through power button / DASH command	System shutdowns and is manageable.
Reboot through DASH command	Continues in KVM session. The viewer will reconnect back after reboot and shows BIOS menu.
No keyboard input for 60 sec	System shutdowns and is manageable

Note: *User is advised to carefully choose options/function key press when in KVM session as choosing any other option or un-supported function key press will result in the system becoming un-manageable. It is also advised that user does not choose any option which makes the system boot to OS directly as this will make the system un-manageable.*

Chapter 3 Enabling AIM-T on Wireless and Wired Systems

3.1 Prerequisites

A laptop or desktop system with OEM's brand which supports AIM-T and Wired DASH functions. AIM-T requires the following compatible hardware modules:

- Wireless Network:
  - Qualcomm WCN6856, Wi-Fi 6E NFA725A, Wi-Fi 7 NCM825, NCM835.
  - MediaTek RZ616 and RZ717/MT 7925
  - Realtek WLAN - 8852CE – Wi-Fi 6 and Realtek WLAN - 8922AE – Wi-Fi 7

  Note: B*eginning with the AIM-T 5.0 release, WLAN modules from Qualcomm are not supported.*

Wired Network: Realtek, RTK8111EPP, RTK8111EPV, RTL8111FP, RTL8125AP, RTL8125BP

Table 5. Software Requirement for Wireless AIM-T

Application	Min. Version	Description
DASHCLI	8.0	A Command Line Interface tool to be installed on host (IT's system) for sending DASH commands to the target-client (AIM-T enabled system). This tool is available for both Windows and Linux OS Host systems.
AMD Provisioning Console (APC)	5.0	A Windows application which can be installed on any host (WIN OS based system) or even on target client (AIM-T system), This tool's User Interface allows us to configure and generate a package with "provisioning data". This package/data should then be provisioned on target-client. Refer to the APC guide for detailed information. For provisioning, refer to *Appendix A*.
AMS	5.1	A Windows application runs as a service on client systems. By default, this is pre-installed by OEMs on client systems before shipment. If it is not installed by default, it can also be downloaded from the Microsoft Store. The complete AMS package is available under Downloads section of the AMD portal (*www.amd.com/DASH*) For detailed instructions, refer to the APC guide.

Table 6. Software Requirement for Wired DASH

Note: *For all features to work, it is recommended to always install and use the latest versions of tools available at* ***www.amd.com/DASH.***

In addition, for wired DASH:

Application	Min. Version	Description
Realtek Ethernet Controller All-In-One Windows Driver	1.0.11.1	You should install it on AIM-T system for receiving DASH commands.

You can download:

- DASH CLI, Provisioning Console, and AMS from the AMD portal (*www.amd.com/DASH*).
- Realtek AIO package from Realtek or OEM support websites.

3.1.1 Network Ports Requirement for AIM-T

To ensure proper functionality of AIM-T, the following network ports must be open and accessible within the infrastructure:

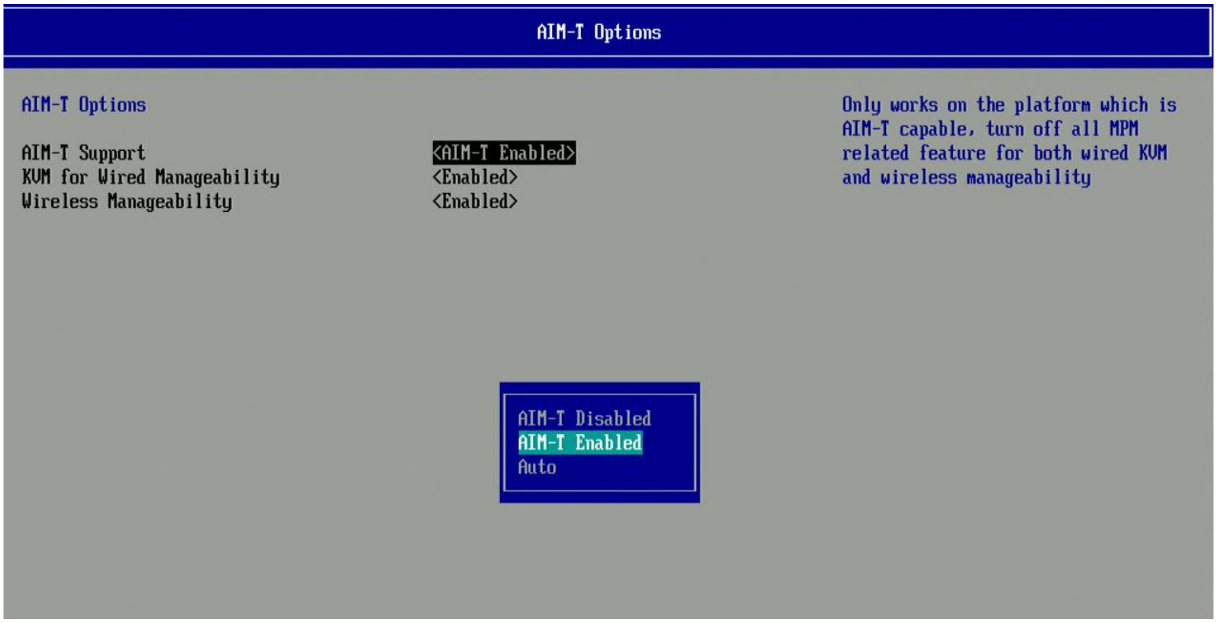
- **Port 664 (DMTF Manageability)**
  Required for Distributed Management Task Force (DMTF) DASH protocols that enable system manageability and monitoring.

- **Port 22 (SSH for KVM)**
  Required for secure shell (SSH) access to secure KVM traffic enabling remote console access.

3.2 BIOS Menu Settings

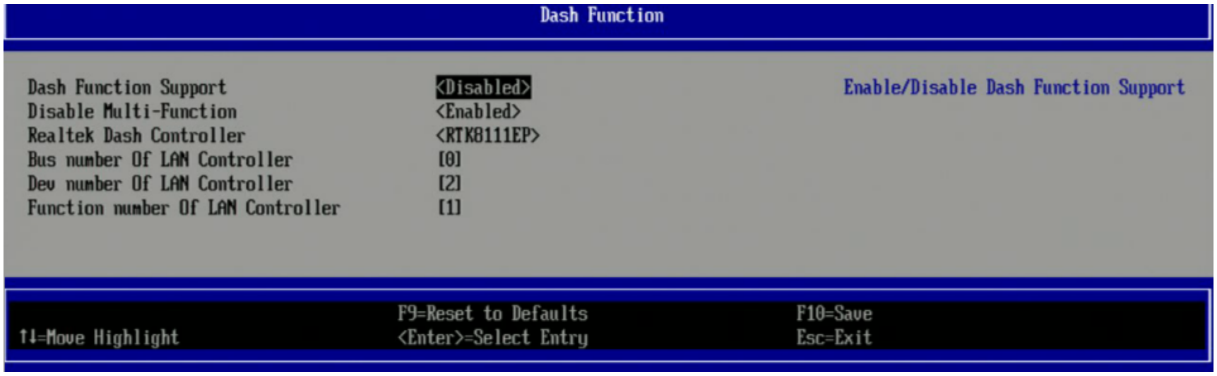
To enable AIM-T on intended systems, you must select and enable appropriate options in the BIOS Setup page, which are typically disabled by default on a fresh BIOS flash.

The following is an example showing AMD’s standard UI for enabling AIM-T and wired DASH in BIOS-Setup Menu:



```
                              AIM-T Options

AIM-T Options                                             Only works on the platform which is
                                                          AIM-T capable, turn off all MPM
AIM-T Support                    <AIM-T Enabled>          related feature for both wired KVM
KVM for Wired Manageability      <Enabled>                and wireless manageability
Wireless Manageability           <Enabled>

                                   AIM-T Disabled
                                   AIM-T Enabled
                                   Auto
```

Figure 2. AIM-T Options



```
                              Dash Function

 Dash Function Support            <Disabled>              Enable/Disable Dash Function Support
 Disable Multi-Function           <Enabled>
 Realtek Dash Controller          <RTK8111EP>
 Bus number Of LAN Controller     [0]
 Dev number Of LAN Controller     [2]
 Function number Of LAN Controller [1]

                             F9=Reset to Defaults        F10=Save
↑↓=Move Highlight            <Enter>=Select Entry        Esc=Exit
```

Figure 3. AIM-T Advanced Options

Note: *OEMs having their own BIOSes will usually find AIM-T Enable/Disable options under different sub-menus in the BIOS setup page; you can find this information from the OEM's BIOS manual.*

3.2.1 Pre-Boot Wi-Fi option

For AIM-T 2.1 and earlier releases, it is recommended to disable Pre-Boot Wi-Fi/Wireless as it may interfere with BIOS KVM functionality.

3.3 Provisioning Console for Wireless AIM-T

Download link: *https://developer.amd.com/tools-for-dmtf-dash/ www.amd.com/DASH*

- AMD Provisioning Console (on the website)

- *AMD_DASH_CLI_Setup_x.y.z.wwww* (for DASH CLI build 4.0.0.1632, the setup file will be *AMD_DASH_CLI_Setup_4.0.0.1632*).

3.3.1 Provisioning

For security purposes, most of the DASH commands require username/password. These usernames and passwords must be provisioned on the client (AIM-T system). When a client receives a DASH command, the AIM-T solution checks whether the username/password with DASH command matches the provisioned settings. Only authorized DASH commands will be processed.

For configuring provisioning data and to provision it on the AIM-T system, refer to Appendix A.

Note: *Backup the crypto key folders in the following location for re-provisioning: C:\Users\XXX\Documents\AMD Provisioning Console\Cryptostore*

3.3.2 Re-Provisioning

AMD supports re-provisioning and un-provisioning capabilities. Re-provisioning can be used when a user (IT administrator) wants to change the provisioned username/password or Wi-Fi AP's setting. The user can create a new package with the original crypto key and perform provisioning process again to overwrite the original settings on the AIM-T system. For steps to create a provisioning package and re-provision an AIM-T system, refer to Appendix D.

Note: *It is important that you back-up the crypto key safely as it cannot be retrieved if it is lost.*

3.3.3 Un-Provisioning

Un-provisioning can be used when a user (IT administrator) wants to wipe out the provisioning data in the AIM-T system. The user can trigger un-provisioning by sending a special DASH command with the username/password provisioned on the AIM-T system. In a case where a user has lost the original crypto key but wants to change username/password or Wi-Fi AP's setting, the user can un-provision the old provisioning data and follow section 3.3.1 to create a new crypto key and provision a new configuration. For steps to un-provision an AIM-T system, refer to Appendix C.

Note: *The un-provisioning process will wipe out the provisioned username/password. You must redo the provisioning to make DASH functional again.*

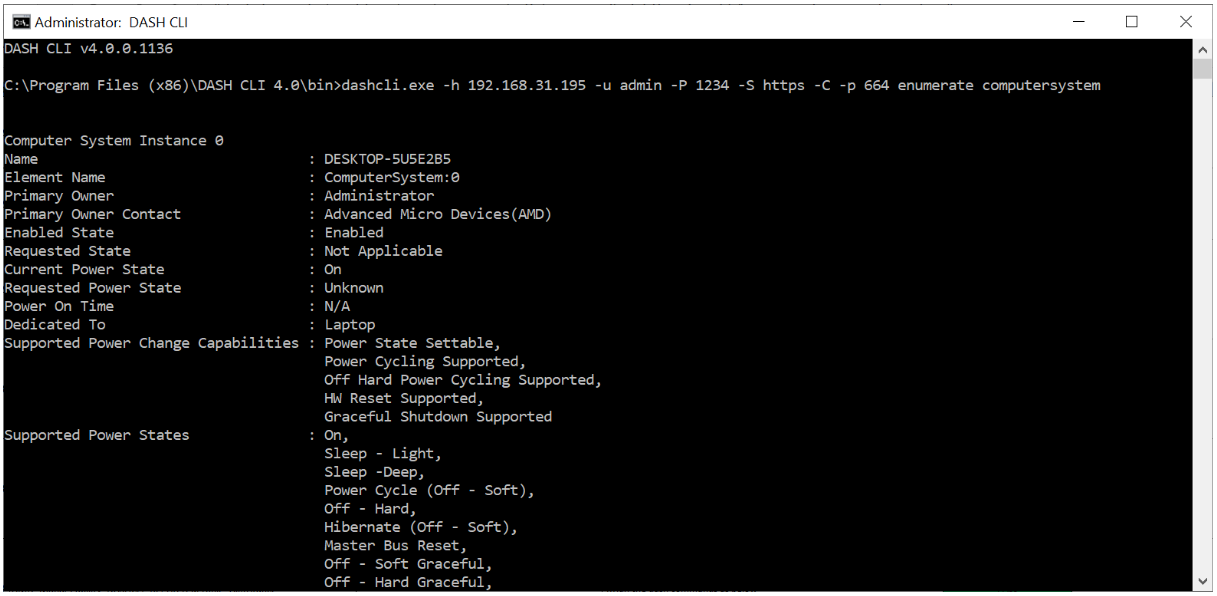
3.4 DASHCLI

Download link: *www.amd.com/DASH*

DASHCLI is a command line tool running on host (IT's system) for sending DASH commands to client (AIM-T system). For security purposes, most of the DASH commands require username/password OR MA. After launching DASHCLI, you can enter DASH commands such as the following:

```
dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate
computersystem
```

Here is a screenshot of the DASHCLI:



```
DASH CLI v4.0.0.1136

C:\Program Files (x86)\DASH CLI 4.0\bin>dashcli.exe -h 192.168.31.195 -u admin -P 1234 -S https -C -p 664 enumerate computersystem


Computer System Instance 0
Name                                 : DESKTOP-5U5E2B5
Element Name                         : ComputerSystem:0
Primary Owner                        : Administrator
Primary Owner Contact                : Advanced Micro Devices(AMD)
Enabled State                        : Enabled
Requested State                      : Not Applicable
Current Power State                  : On
Requested Power State                : Unknown
Power On Time                        : N/A
Dedicated To                         : Laptop
Supported Power Change Capabilities  : Power State Settable,
                                       Power Cycling Supported,
                                       Off Hard Power Cycling Supported,
                                       HW Reset Supported,
                                       Graceful Shutdown Supported
Supported Power States               : On,
                                       Sleep - Light,
                                       Sleep -Deep,
                                       Power Cycle (Off - Soft),
                                       Off - Hard,
                                       Hibernate (Off - Soft),
                                       Master Bus Reset,
                                       Off - Soft Graceful,
                                       Off - Hard Graceful,
```

Figure 4. DASHCLI

For more DASH commands, see Appendix F.

3.5 AIM-T Manageability Service (AMS)

AIM-T Manageability Service (AMS) is the Windows component of the solution and supports Wireless Manageability on the AIM-T system.

If an OEM enables the AIM-T feature from the factory, AMS should already be installed. For AIM-T capable systems not having AIM-T enabled from the factory, you can download and install AMS from Microsoft Store (*https://apps.microsoft.com/store/detail/9PM4WBSLVZTG*):

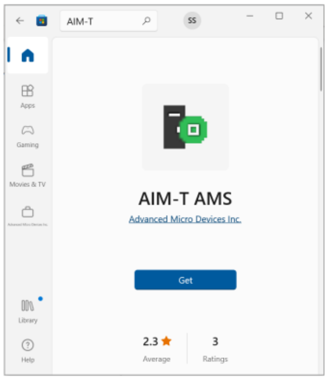


Figure 5. Installing AMS

By default, AMS should be installed on OEM's AIM-T capable products. AMS is auto launched when system boots to OS with Wi-Fi connection. AMS is available in hidden icons; you can double-click the icon to launch it:

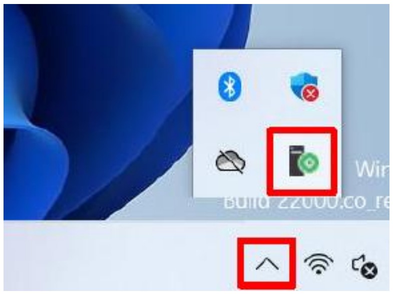
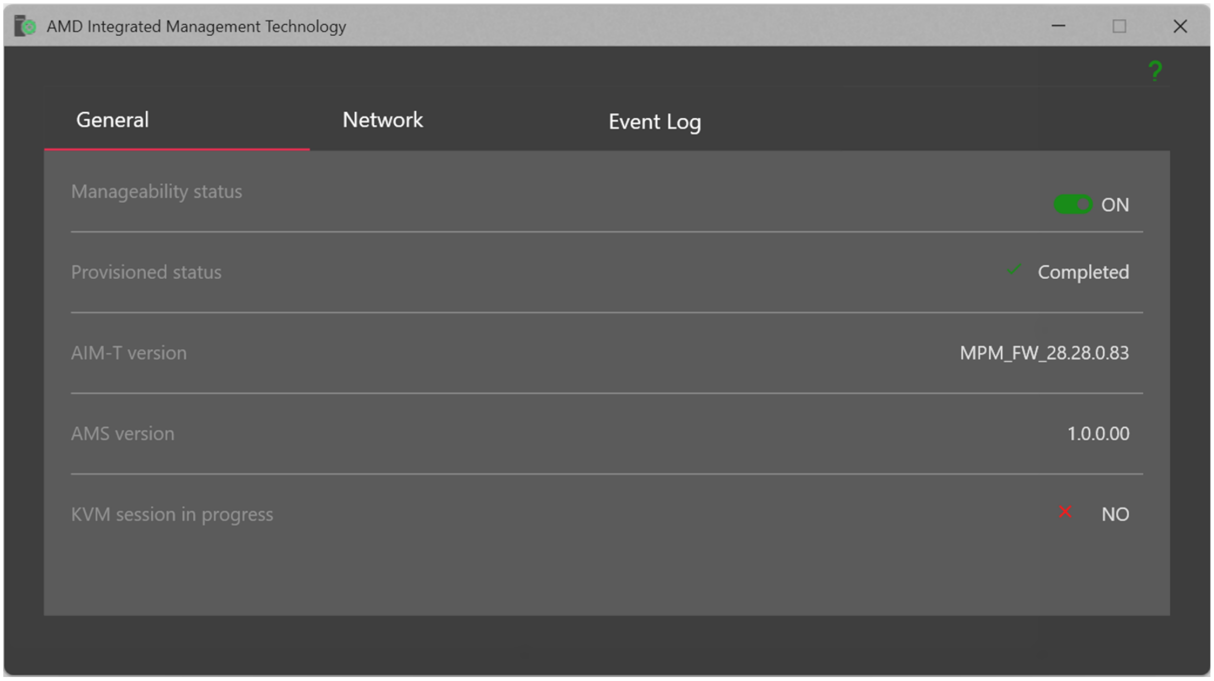


Figure 6. AMS Icon

You can check the AIM-T status in the AMS UI. If AIM-T is enabled in BIOS, the system is provisioned, and Wi-Fi is connected to Wi-Fi AP; the AMS should look as follows:


AMD Integrated Management Technology

General | Network | Event Log

Manageability status	ON
Provisioned status	✓ Completed
AIM-T version	MPM_FW_28.28.0.83
AMS version	1.0.0.00
KVM session in progress	✕ NO

Figure 7. AIM-T Status

AMS UI will be hidden if you log in to Windows with a standard user account. AMS may not be visible in **Apps & features** for a standard user, but it will not affect the DASH commands. The AIM-T system with a standard user account can still receive DASH commands from host. Contrarily, if a client user logs in with an administrator account, he/she can see AMS UI and AIM-T status.

3.5.1 AMS installation

AMS is distributed in 2 packages:

1. All in one installer (exe): A standalone installer that adds its dependencies in the following order:

    a. Add Mailbox Driver in Device Manager

    b. Add AMS Service in Windows Service Manager and start service

    c. Install tray UI and appear on Windows tray

    Once installation is successful, it will appear on the Control Panel. To upgrade, download and run the latest version of AMS. To uninstall, you can find AIM-T Manageability Service in the Control Panel and choose the Uninstall option OR run the setup again and choose the Uninstall option.

    For Silent Installation & Uninstallation

    - Installation: *<Package> /S /v/qn*
    - Uninstallation: *<Package> /X /S /v/qn*

2. MSIX package from Microsoft store: Contains AMS Service available as AIM-T App in MS Store.
   Download the AIM-T app from: *https://www.microsoft.com/store/apps/9PM4WBSLVZTG*

Note: *You must also install the AMS Mailbox driver which is part of AMD Chipset Drivers. Chipset drivers can be downloaded from* https://www.amd.com/en/support/download/drivers.html *by choosing the applicable platform.*

Once installation is successful, it is advised to wait at least a minute for post installation steps to be completed. AMS will appear in the "Apps & features" OR "Installed Apps" options, which usually varies/depends on Windows OS versions.

You will find app upgrades on the Microsoft Store app. To auto upgrade to the latest available version, ensure you have enabled the automatic update feature in the OS.

To uninstall, navigate to "Apps & Features"/"Installed Apps" and choose the appropriate option.

3.5.2 Wake from Sleep

AMS can wake up from sleep to respond to DASH queries with the help of S0i3 filter driver which is packaged along with AMS standalone installer. For MS Store based installer, the supporting filter driver should be installed via Chipset installer corresponding to the platform on which the driver is required to be installed.

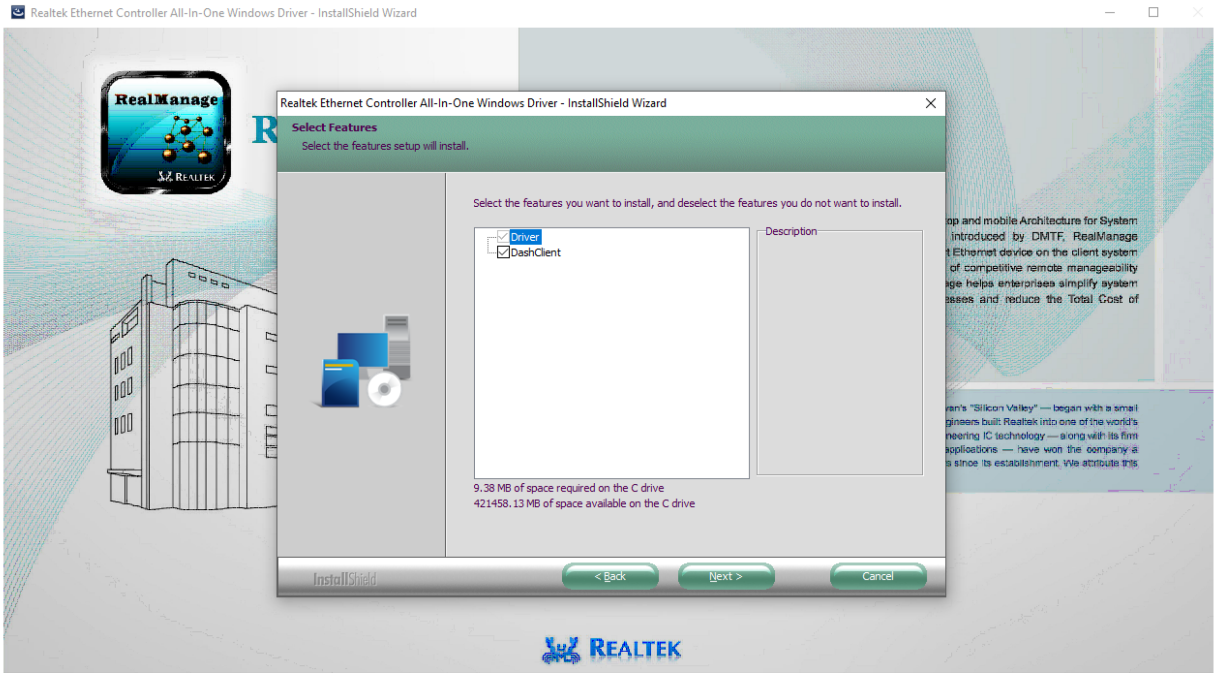
Note: *Wake from sleep is not supported in the S0i3 filter driver over cloud. So, a DASH packet coming over ACMS does not respond back to the client over cloud.*

Note: *Wake from sleep (S0i3) for DASH commands is not supported in DC mode (system on-battery and AC power supply not connected to system).*

3.6 Realtek Ethernet Controller All-in-One Windows Driver

Contact OEM to get the installation package and detailed information.

You should install Realtek Ethernet Controller All-in-One Windows Driver on client (AIM-T system) to make the system ready for DASH commands. Once the package is installed, you can check the DASH status and firmware version of NIC with Realtek service UI as follows:



Realtek Ethernet Controller All-In-One Windows Driver - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☑ Driver
☑ DashClient

Description

9.38 MB of space required on the C drive
421458.13 MB of space available on the C drive

op and mobile Architecture for System introduced by DMTF, RealManage t Ethernet device on the client system of competitive remote manageability ge helps enterprises simplify system esses and reduce the Total Cost of

van's "Silicon Valley" — began with a small gineers built Realtek into one of the world's neering IC technology — along with its firm applications — have won the company a s since its establishment. We attribute this

Figure 8. Realtek UI

You can find the execution file and launch Realtek UI in the default directory:

C:\Program Files (x86)\Realtek\Realtek Windows NIC Driver\RtDashService\RtDashUI

DASH client shows the current DASH status and FW version on the AIM-T system:

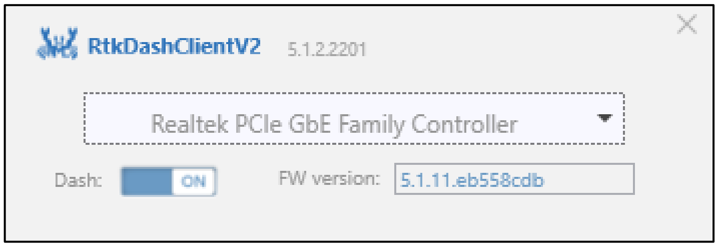
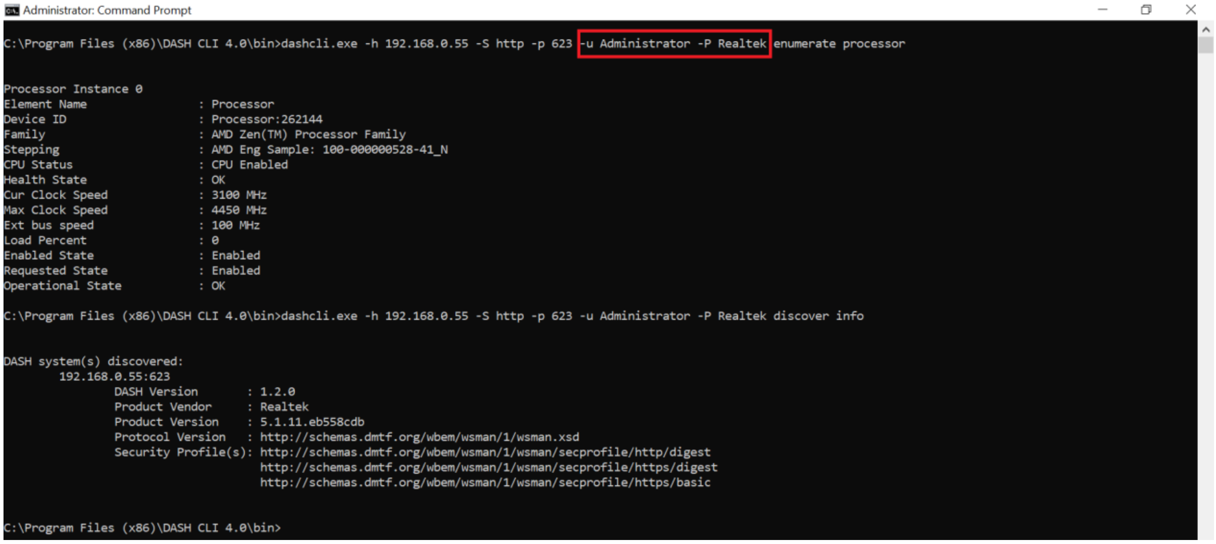


Figure 9. DASH Client

After the driver installation is complete, you can trigger DASH commands to retrieve information from the AIM-T system. The following is an example showing how to send a DASH command to get AIM-T system's processor info:



```
C:\Program Files (x86)\DASH CLI 4.0\bin>dashcli.exe -h 192.168.0.55 -S http -p 623 -u Administrator -P Realtek enumerate processor


Processor Instance 0
Element Name                : Processor
Device ID                   : Processor:262144
Family                      : AMD Zen(TM) Processor Family
Stepping                    : AMD Eng Sample: 100-000000528-41_N
CPU Status                  : CPU Enabled
Health State                : OK
Cur Clock Speed             : 3100 MHz
Max Clock Speed             : 4450 MHz
Ext bus speed               : 100 MHz
Load Percent                : 0
Enabled State               : Enabled
Requested State             : Enabled
Operational State           : OK

C:\Program Files (x86)\DASH CLI 4.0\bin>dashcli.exe -h 192.168.0.55 -S http -p 623 -u Administrator -P Realtek discover info


DASH system(s) discovered:
        192.168.0.55:623
                DASH Version       : 1.2.0
                Product Vendor     : Realtek
                Product Version    : 5.1.11.eb558cdb
                Protocol Version   : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
                Security Profile(s): http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/http/digest
                                     http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/digest
                                     http://schemas.dmtf.org/wbem/wsman/1/wsman/secprofile/https/basic


C:\Program Files (x86)\DASH CLI 4.0\bin>
```

Figure 10. AIM-T System Processor Info

Note: *The default credential for Realtek NIC is **Administrator** and **Realtek**. To learn how to change username and password for wired DASH by flashing Realtek NIC firmware, refer to Appendix F.*

3.7 Enable auto EAP TLS Certificate Generation and Signing Feature

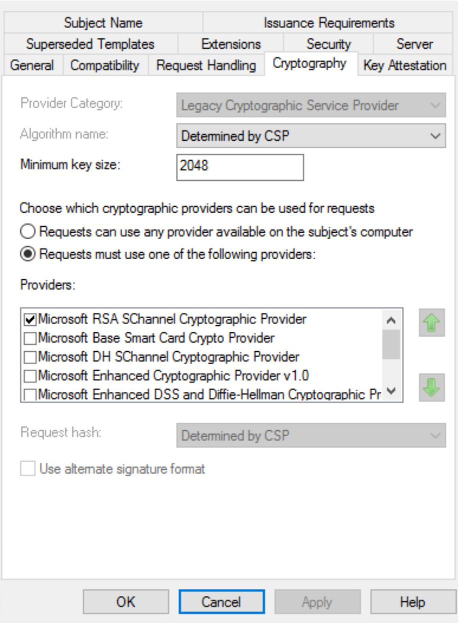
Managed systems use EAP TLS certificates to establish secure connections with the enterprise wireless network. These systems automatically renew their certificates before they expire.

The following components must be set up and configured for the automatic renewal of EAP TLS certificates on managed systems (such as those in an enterprise environment).

3.7.1 Active Directory Configuration

To configure the Active Directory:

1. Make sure the ADCS (Active Directory Certificate Service) is running in Active Directory.
2. Create a computer certificate template for AIM-T EAP TLS feature.
3. Make sure the following settings are enabled:
    a. On the Cryptography tab, provide minimum key size as 2048 bits as AIM-T supports RSA 2048 bit key only.



Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

○ Requests can use any provider available on the subject's computer

● Requests must use one of the following providers:

Providers:

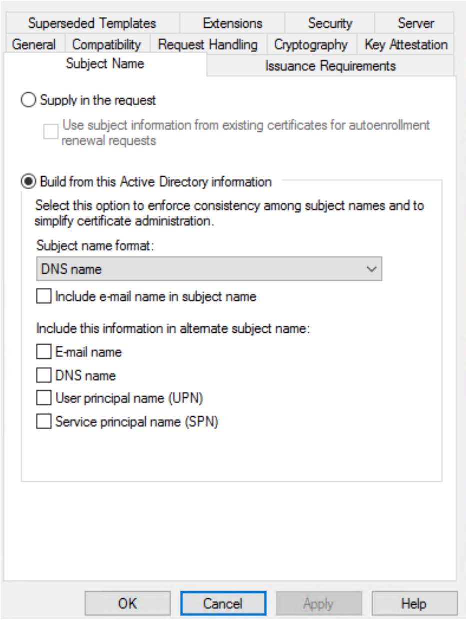
☑ Microsoft RSA SChannel Cryptographic Provider
□ Microsoft Base Smart Card Crypto Provider
□ Microsoft DH SChannel Cryptographic Provider
□ Microsoft Enhanced Cryptographic Provider v1.0
□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr

Request hash: Determined by CSP

□ Use alternate signature format

Figure 11. Cryptography Tab

b. On the Subject Name tab, choose the “Build from this active Directory information” option and select “Subject name format” as “DNS name”. This option is recommended by Microsoft for security reasons. It means that, when ADCS issues a certificate to a host machine that has requested it, ADCS includes the hostname of that machine build from Active Directory in the CN (common name) of the certificate



○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

DNS name

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

Figure 12. Subject Name Tab

c. On the Security tab, add “Domain Computers” group to enroll for certificate and remove Authenticated users from Enroll permission. This enables ADCS to allow certificate requests from all computers that are members of the domain.

3.7.2 Radius Server Configuration

During the EAP TLS connection process, the identity field is utilized for Active Directory authentication prior to establishing the TLS connection. The managed system will transmit its identity in the following format:

Identity string format: host/{system hostname with FQDN}

Example: host/systemName.xyz.com

Note that if the identity string being used for EAP TLS authentication is not suitable for your Active Directory authentication requirements then add or modify an identity rule accordingly.

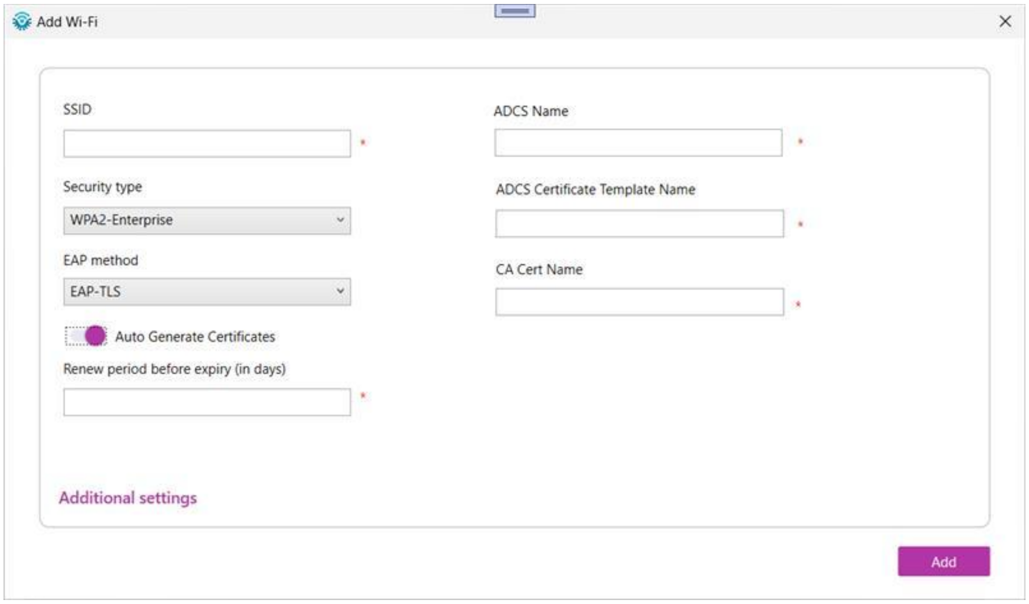
3.7.3 APC Configuration

1) Go to the **Network & Wi-Fi** menu and select the **Wi-Fi** tab.

2) Click on the **"Add Wi-Fi"** button and choose the security type **"WPA2-Enterprise"** or **"WPA3-Enterprise".**

3) Once selected, the window will expand to display more input fields. Choose the **EAP method** as **EAP-TLS.**

4) Click on the toggle button for **"Auto-generate certificates"** This action will expand the window with new fields, as shown in the figure below.


Add Wi-Fi
SSID
Security type
EAP method
Auto Generate Certificates
Renew period before expiry (in days)
ADCS Name
ADCS Certificate Template Name
CA Cert Name
Additional settings
Add

Security type: WPA2-Enterprise

EAP method: EAP-TLS

Figure 13. Auto EAP TLS Configuration

5) Fill in the appropriate fields as explained in the following table.

Table 7. EAP TLS Parameters

Field Name	Description
SSID	Enter name of WiFi Access Point.
ADCS Name	Enter the hostname of the Active Directory Server System with the FQDN.
ADCS Template Name	Enter the certificate template name that has been configured for Wireless NAC.
CA Cert Name	Enter the EAP TLS certificate issuer name. Specify the name of the CA that issued the EAP TLS certificate. This is

	typically the common name (CN) of the issuing CA.
Renew period before expiry (in days)	Enter the desired Auto Renew Period in days. It is important to ensure that this renew period is shorter than the overall certificate validity period. e.g, If the "Renew period before expiry" is set to 30 days and the certificate validity is 90 days, the system will initiate the certificate renewal process after 60 days (90-30 = 60) to complete certificate renewal in 90 days. i.e. 30 days before expiry.

Note:

1. On the managed system, at the first boot to Windows OS, after the system is provisioned, an EAP TLS certificate will be generated if system is connected to the enterprise network.
2. **Auto renewal of certificate:** When EAP TLS certificate approaches its expiration date, the system will initiate the renewal process either at the next system boot or upon a network UP/DOWN event.
3. If in case certificate expires, [when managed system is offline during renewal period] then system will initiate the certificate renewal process as soon as it is connected back to enterprise network.
4. If this feature is enabled, then there is no need to add manual WiFi profiles as described in **Appendix K Adding Wi-Fi Access Point Profile**.

Chapter 4 User Scenario

4.1 AIM-T in OS

4.1.1 Prerequisites

- Client (AIM-T system) has AMS installed and provisioned
- Host (IT admin's console system) has DASHCLI installed
- Host can ping client's IP

4.1.2 Expected Behavior

When a client user is working on an AIM-T system, an enterprise IT can send DASH commands (Appendix D) to the client and fetch system's software and hardware information back silently. Some DASH commands can force the AIM-T system to shut down or reboot. In that case, the client user will observe system graceful shutdown, hard shutdown, or reboot without any notification. Also, the enterprise IT can force an AIM-T system to do BIOS capsule update with a special DASH command and process (Appendix I).

Moreover, the IT can request the client to establish a KVM (0) session. In OS, IT can start an OS KVM in which a VNC viewer will pop-up immediately and show AIM-T system's screen. The other option is that IT sends a BIOS KVM command through DASH to request the AIM-T system restart and enter BIOS setup menu. When the client enters BIOS menu, the VNC viewer on host system should display the same screen.

Note: *A user can terminate KVM session by closing VNC viewer. The safe way to shut down an AIM-T system is to close the VNC viewer and send a DASH command to shut the AIM-T system down (Appendix D).*

4.1.3 Graceful Shutdown

After a user triggers graceful shutdown in OS power menu on a AIM-T system having a power adaptor attached, the system will shut down and restart AIM-T. Thirty seconds later, the system will have AIM-T capability to process DASH commands and KVM session request. For more information, refer to section 4.2.

4.2 AIM-T in Shutdown Mode

4.2.1 Prerequisites

- AIM-T function needs to be enabled in BIOS setup menu on the AIM-T system
- The AIM-T system must be AIM-T provisioned
- Power adaptor must be attached

4.2.2 Expected Behavior

When AIM-T is working in shutdown mode on a AIM-T system, there is no display. However, the power LED may blink and fan spin occasionally depending on the OEM's design and Wi-Fi AP's behavior. Normally, when a client user shuts the system down through OS, the power LED and fan should turn off for 3~6 seconds and automatically turn on for 30~40 seconds. Then, the power LED and fan turn off again. After that, a host (IT's system) can send DASH commands (Appendix D) to the AIM-T system which will wake up with power LED on, fan spinning, and it will take 60 seconds to be prepared for the incoming DASH commands. Some DASH commands can force the AIM-T systems boot to OS. When there is no more DASH command in the queue for 3 minutes, the system will shutdown. Same as AIM-T in OS mode, AIM-T supports KVM function in shutdown mode. The KVM (0) session request sent from IT will trigger the system restart and establish a KVM connection.

4.2.3 Pressing Power Button

In the shutdown mode, regardless of power LED is on or off, a client user can boot the system to OS by pressing a power button.

Note: *When the power LED turns on, an AIM-T system may not be ready for handling the power button event for the first 30 seconds. User should press the power button after 30 seconds of power LED turning on.*

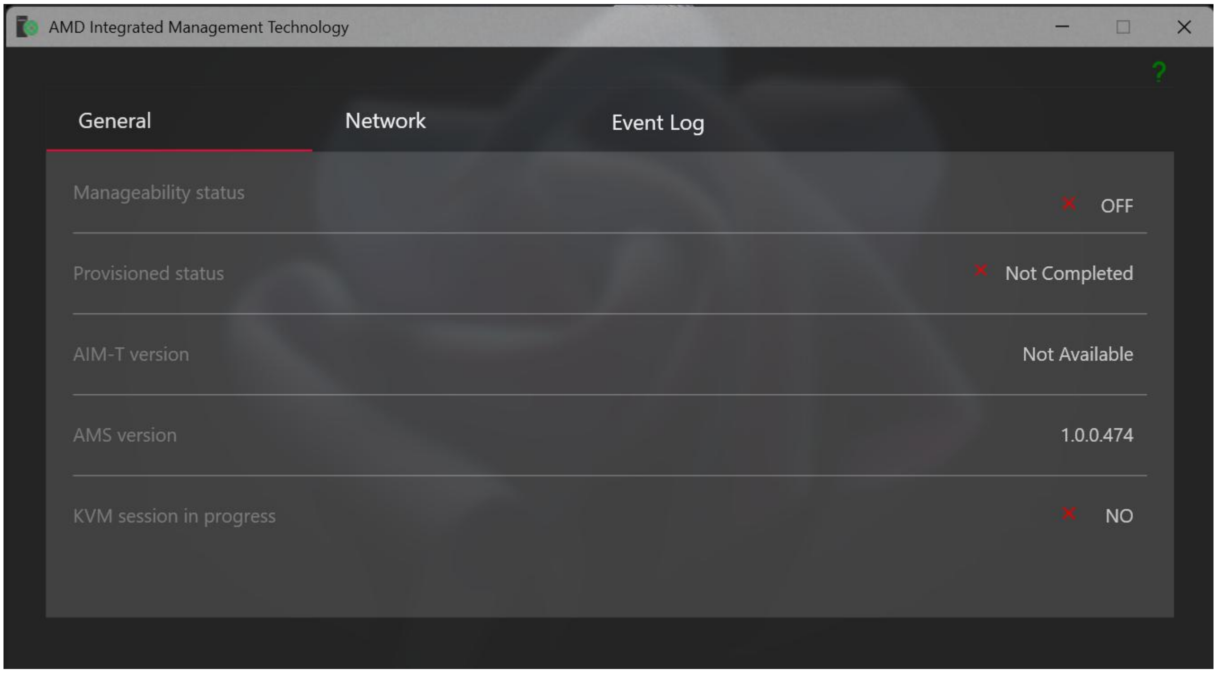
4.2.4 Detaching Power Adaptor

Power adaptor attachment is one of the requirements for AIM-T in shutdown mode. Removing power adaptor will force the system turn AIM-T off during shutdown mode.

Chapter 5 Troubleshooting

5.1 On AIM-T DASH System

5.1.1 AMS Status is Off



Manageability status ✗ OFF

Provisioned status ✗ Not Completed

AIM-T version Not Available

AMS version 1.0.0.474

KVM session in progress ✗ NO

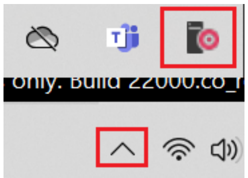
Figure 14. AMS Status is Off

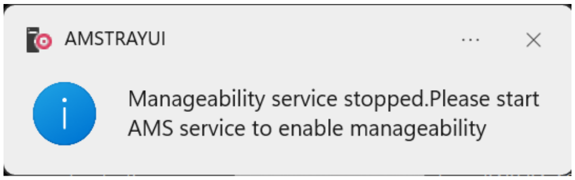
If the **Manageability status** is OFF in the AMS UI tray, user can check the following to recover it:

- AIM-T is ON in the BIOS menu
- Device Manager > System > AMS-MailboxDrv works properly
- Launch services to ensure that AMS is running

5.1.2 Red AMS UI Tray

In some cases, the AMS tray icon will turn red as AMS may not start:



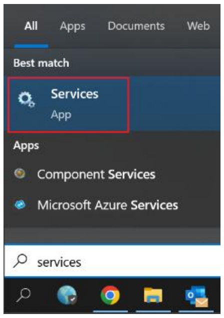


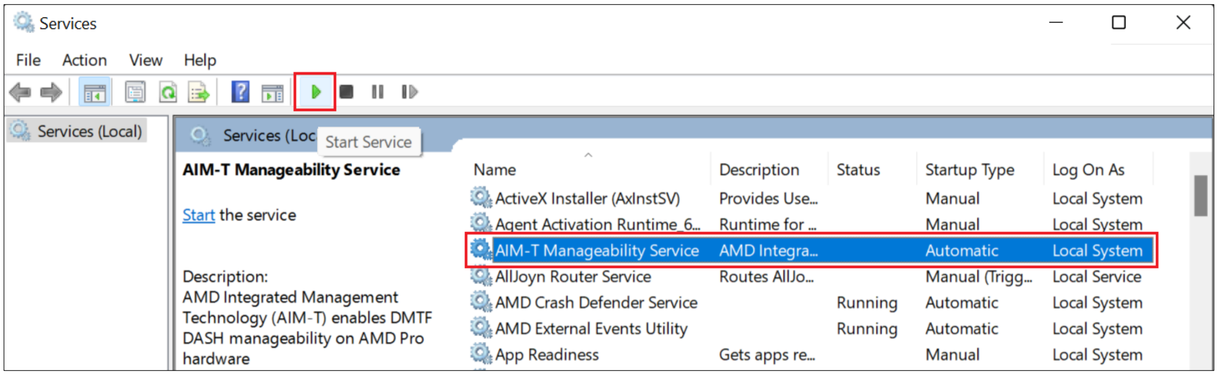
Manageability service stopped.Please start AMS service to enable manageability

Figure 15. AMS UI Tray Issues

You can re-launch AMS to recover it.

Also, you can search for **Services** and start the service as follows:





AIM-T Manageability Service

Start the service

Description:
AMD Integrated Management Technology (AIM-T) enables DMTF DASH manageability on AMD Pro hardware

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Use...		Manual	Local System
Agent Activation Runtime_6...	Runtime for ...		Manual	Local System
AIM-T Manageability Service	AMD Integra...		Automatic	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigg...	Local Service
AMD Crash Defender Service		Running	Automatic	Local System
AMD External Events Utility		Running	Automatic	Local System
App Readiness	Gets apps re...		Manual	Local System

Figure 16. Start AMS Service

5.1.3 KVM consent after target wakes up from S0i3

Upon resuming from the S0i3 state, the KVM session with KVM consent will function only if the target system was either already in a "locked-screen" state or returned directly to the Desktop without requiring a sign-in (with the sign-in option set to "never").

5.1.4 KVM with Higher Resolution [AIM-T 5.0 onwards]

Higher Resolution KVM (in OS) is supported from AIM-T 5.0 release onwards on compatible platforms.

1. The max resolution supported is 4K 3840x2160.
2. Resolution in BIOS KVM will remain as 1024x768.
3. In case of multiple displays connected to target, the attached Display which is marked as primary will be selected for redirection. Key and mouse movement will work only for primary display screen and secondary external display will remain ON. For releases earlier than AIM-T 5.0, the secondary external display will be turned off/disabled by graphics driver when KVM is launched.

4. KVM is not supported if no monitor is attached to the target.
5. Display configuration change during KVM is not supported.

5.1.5 Missing Alerts and Indication subscription

If the IT admin has subscribed to alerts from a system, this system can send alerts only if it is online/connected to a network. As alerts are real time events, you may lose the alerts if the system is disconnected from the network.

5.1.6 Display Flickers after closing KVM session

In target systems running AIM-T 4.5 or earlier versions, terminating an OS KVM session by closing the KVM viewer may cause the display to flicker briefly, showing a momentary black screen. This is expected behavior and not a cause for concern. However, this behavior is not observed in AIM-T 5.0 or later versions.

5.2 On Console (DASH CLI) System

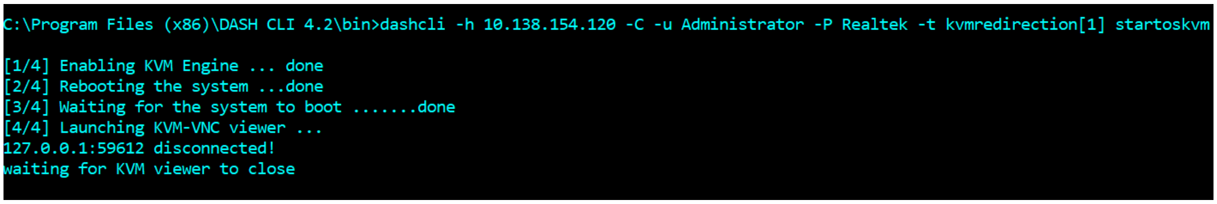
5.2.1 KVM Command Response

Both OS KVM and BIOS KVM require a KVMSSHKey which is in a provisioning package generated by the user (refer to Appendix A) and should be saved in:

C:\Program Files (x86)\DASH CLI x.y\certs\

For example: For DASH CLI 4.0, the path is C:\Program Files (x86)\DASH CLI 4.0\certs\

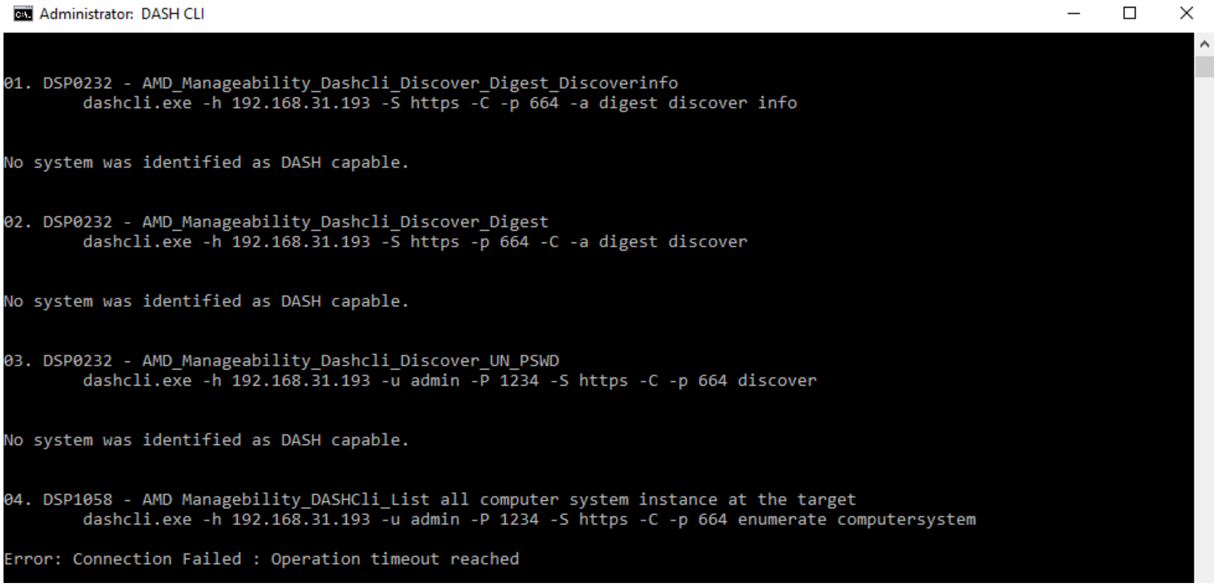
The folder *certs* is set as an administrator folder which may be controlled by an enterprise IT policy.



```
C:\Program Files (x86)\DASH CLI 4.2\bin>dashcli -h 10.138.154.120 -C -u Administrator -P Realtek -t kvmredirection[1] startoskvm

[1/4] Enabling KVM Engine ... done
[2/4] Rebooting the system ...done
[3/4] Waiting for the system to boot .......done
[4/4] Launching KVM-VNC viewer ...
127.0.0.1:59612 disconnected!
waiting for KVM viewer to close
```

Figure 17. DASH CLI – KVM Output

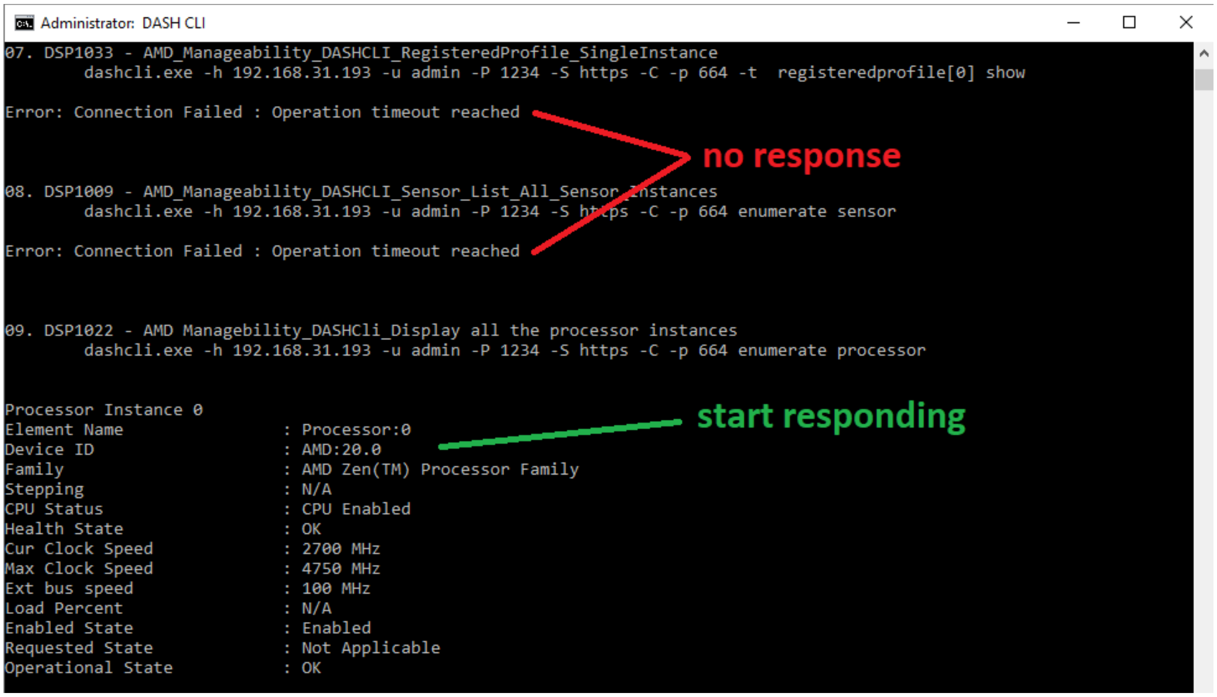
5.2.2 Unresponsive AIM-T System



```
01. DSP0232 - AMD_Manageability_Dashcli_Discover_Digest_Discoverinfo
        dashcli.exe -h 192.168.31.193 -S https -C -p 664 -a digest discover info


No system was identified as DASH capable.


02. DSP0232 - AMD_Manageability_Dashcli_Discover_Digest
        dashcli.exe -h 192.168.31.193 -S https -p 664 -C -a digest discover


No system was identified as DASH capable.


03. DSP0232 - AMD_Manageability_Dashcli_Discover_UN_PSWD
        dashcli.exe -h 192.168.31.193 -u admin -P 1234 -S https -C -p 664 discover


No system was identified as DASH capable.


04. DSP1058 - AMD Managebility_DASHCli_List all computer system instance at the target
        dashcli.exe -h 192.168.31.193 -u admin -P 1234 -S https -C -p 664 enumerate computersystem

Error: Connection Failed : Operation timeout reached
```

Figure 18. Unresponsive AIM-T System

When an AIM-T system is in the shutdown mode, the console cannot get any DASH response immediately. You should wake the AIM-T system up by sending a DASH command. Then, the AIM-T system will take 1~1.5 minute to be ready for handling DASH commands. You can keep sending DASH commands to ensure that the AIM-T system is ready.



```
07. DSP1033 - AMD_Manageability_DASHCLI_RegisteredProfile_SingleInstance
        dashcli.exe -h 192.168.31.193 -u admin -P 1234 -S https -C -p 664 -t  registeredprofile[0] show

Error: Connection Failed : Operation timeout reached


08. DSP1009 - AMD_Manageability_DASHCLI_Sensor_List_All_Sensor_Instances
        dashcli.exe -h 192.168.31.193 -u admin -P 1234 -S https -C -p 664 enumerate sensor

Error: Connection Failed : Operation timeout reached



09. DSP1022 - AMD Managebility_DASHCli_Display all the processor instances
        dashcli.exe -h 192.168.31.193 -u admin -P 1234 -S https -C -p 664 enumerate processor


Processor Instance 0
Element Name                 : Processor:0
Device ID                    : AMD:20.0
Family                       : AMD Zen(TM) Processor Family
Stepping                     : N/A
CPU Status                   : CPU Enabled
Health State                 : OK
Cur Clock Speed              : 2700 MHz
Max Clock Speed              : 4750 MHz
Ext bus speed                : 100 MHz
Load Percent                 : N/A
Enabled State                : Enabled
Requested State              : Not Applicable
Operational State            : OK
```

Figure 19. Responsive AIM-T system

Other reasons for an AIM-T system being unresponsive can be the AIM-T system is not connected to the same network domain or it is not configured properly. To fix the AIM-T system, refer to section 5.1.

5.2.3 Distorted Display or Black Screen While Connecting KVM

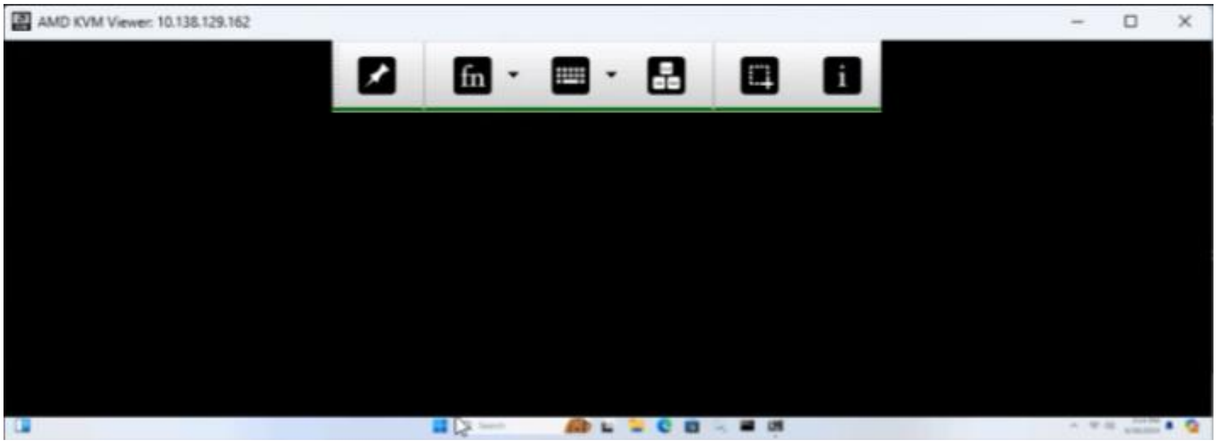


Figure 20. Distorted Display or Black Screen While Connecting KVM

When a host system initiates a KVM session with an AIM-T system, the host user (enterprise IT admin) may witness a distorted VNC viewer. Most of the time, this problem happens when the client was in the shutdown mode and was woken up by a KVM request. This problem can be recovered by rebooting the AIM-T system. When a host user witnesses the issue, he/she can launch a new DASHCLI console (do not close the old one) and send a power cycle DASH command to the client:

dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t computersystem[0] power cycle

This command can reboot the AIM-T system. Then, the host user will see the client's BIOS menu with a clear display on the VNC viewer in a few minutes.

5.2.4 Terminating TCR Session

For OEMs which support text BIOS, when TCR session is ongoing, if you choose to boot from BIOS setup to BIOS window, the system will reboot and stay in BIOS. However, putty session will not reconnect and system will be temporarily unmanageable. The system becomes manageable only after it boots to OS after a timeout of 3 minutes.

To terminate the TCR session, close the Putty viewer window.

5.2.5 WebUI page not loading fully or not showing all details

When systems are tested in a closed network environment without internet access, certain Web UI features may not appear or function properly. For example, the automatic logout timer might be missing, and the "Expand All" button may not operate as intended. This is because many web applications depend on external libraries, APIs, or services that require internet connectivity. Without access to these resources, features may be incomplete or malfunction.

To resolve these issues, it is recommended that the browser be connected to the internet, allowing it to access these resources online.

5.2.6 DASH discover and discover commands return error via ACMS service

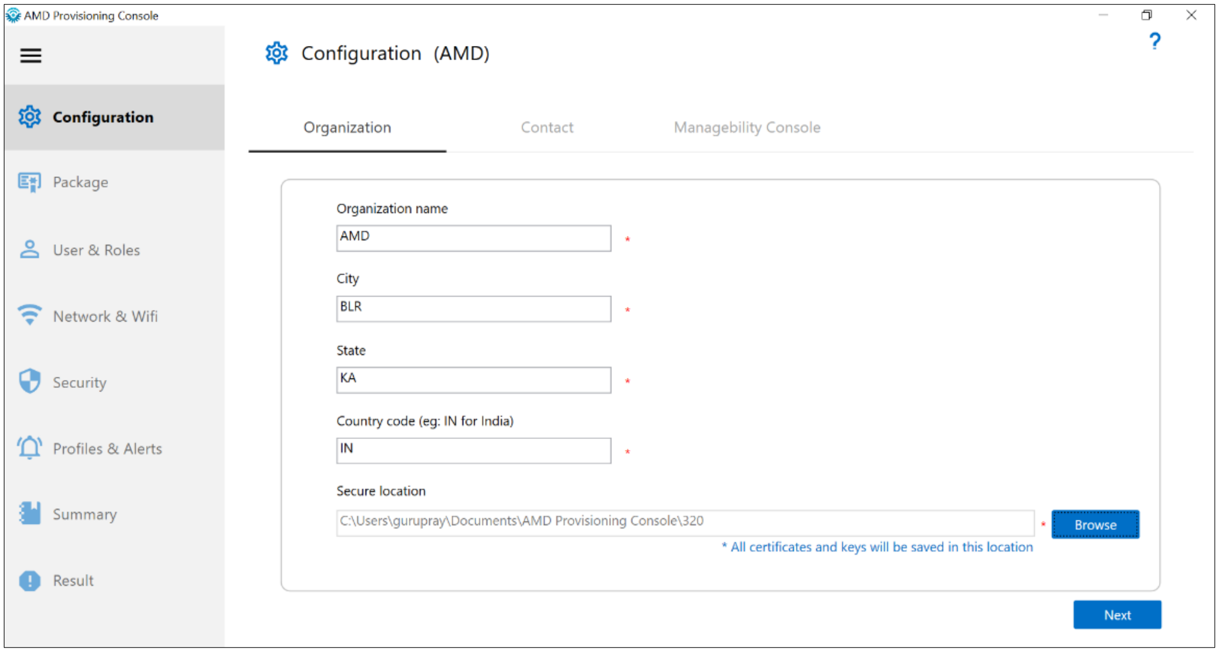
If the DASH commands "*discover*" and "*discover info*" return the error "*No system was identified as DASH capable*" when executed via the ACMS service, it is recommended that you retry the commands with an increased timeout by using the -T <seconds> argument in the DASHCLI. An example with increased timeout of 60 seconds:

dashcli.exe -r <acms_host> -h <hostname> -u <username> -P <password> -rp 5050 -C -p 664 -T 60 discover

Appendix A Configuring Provisioning Data

Complete the following steps to configure the provisioning data:

1. On host (IT’s system), install AMD Provisioning Console tool using the executable file (for example, *Provisioning_Console_setup-5.0.0.xxx-AMD.exe*).
2. Launch AMD Provisioning Console.
3. Fill in the organization information.
4. Select the location where you want to store the profiles:



Organization name: AMD *

City: BLR *

State: KA *

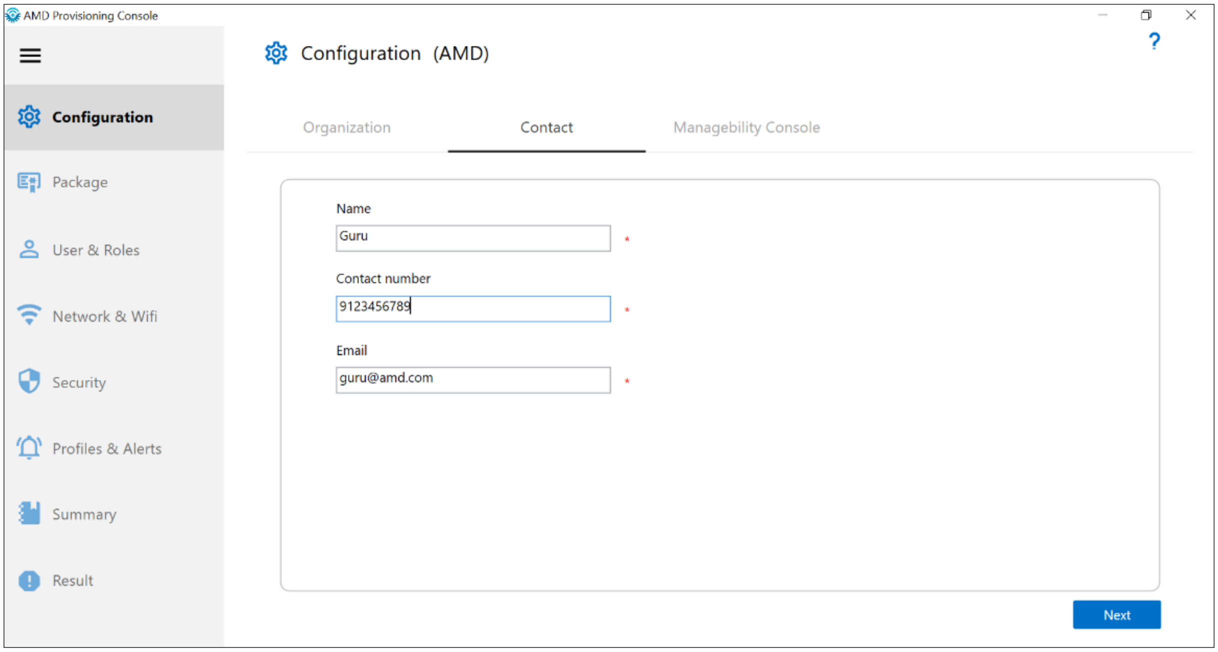
Country code (eg: IN for India): IN *

Secure location: C:\Users\gurupray\Documents\AMD Provisioning Console\320 *

* All certificates and keys will be saved in this location

Figure 21. Profile Location

5. Fill in the contact information:



Name: Guru *

Contact number: 9123456789 *

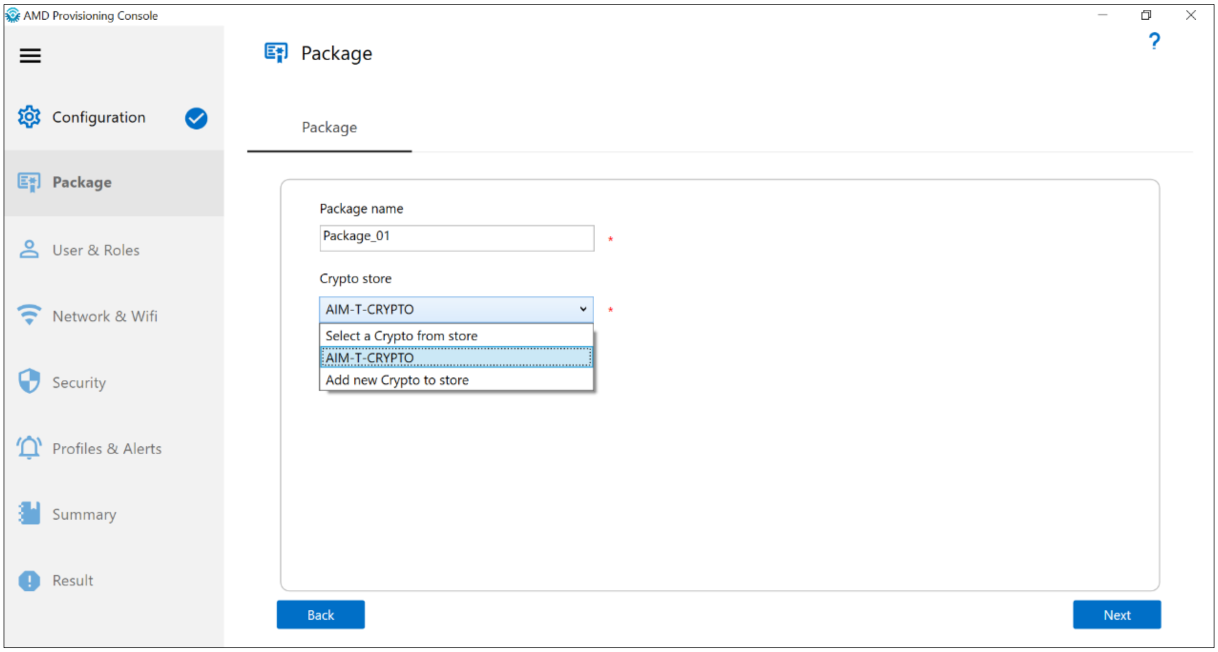
Email: guru@amd.com *

Figure 22. Contact Information

6. Provide a **Package name**.

   It will be a part of the provisioning package's folder name.

7. Create a new Crypto and select it from the **Crypto store** drop-down:

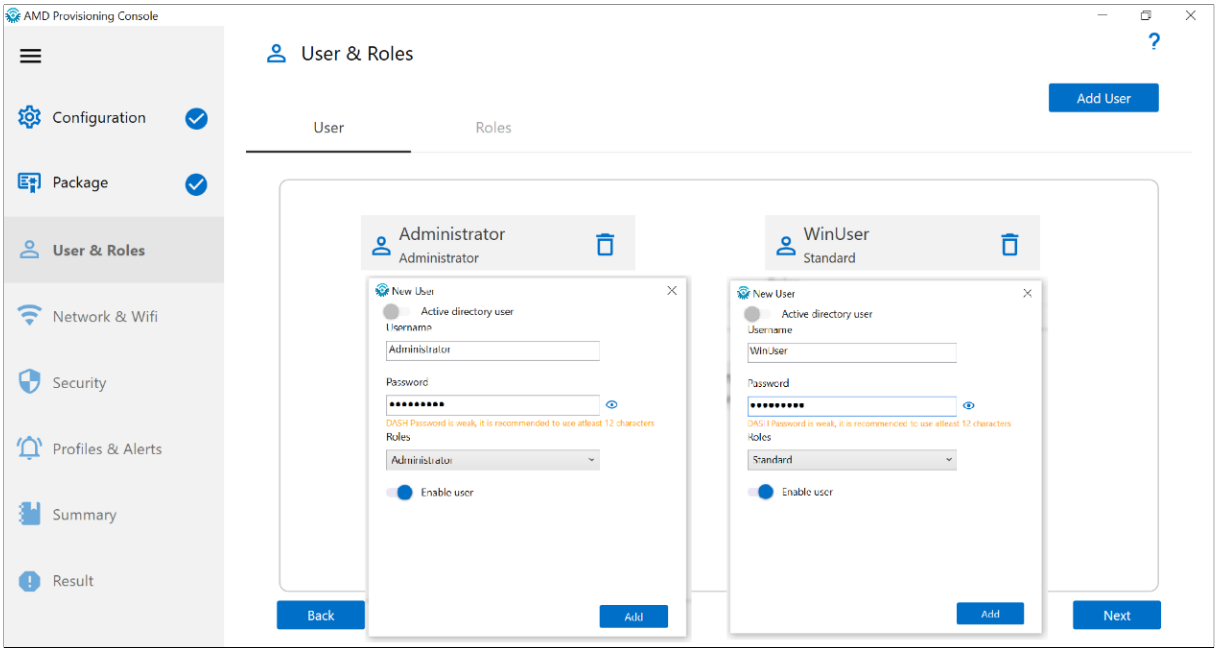


Package name: Package_01 *

Crypto store: AIM-T-CRYPTO *

Figure 23. Crypto store

8. Add two users (one standard and one admin) without changing the **Roles** configuration:



Administrator
Administrator

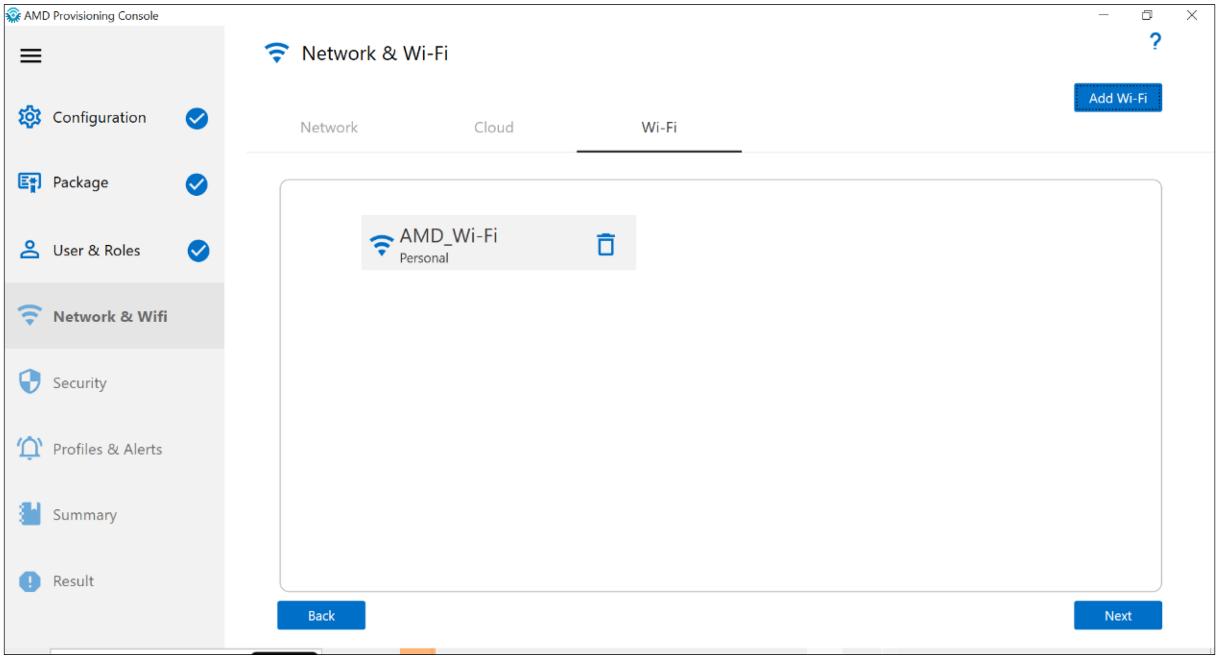
WinUser
Standard

New User
○ Active directory user
Username: Administrator
Password: ••••••••••
DASH Password is weak, it is recommended to use atleast 12 characters
Roles: Administrator
● Enable user

New User
○ Active directory user
Username: WinUser
Password: ••••••••••
DASH Password is weak, it is recommended to use atleast 12 characters
Roles: Standard
● Enable user

Figure 24. Adding Users

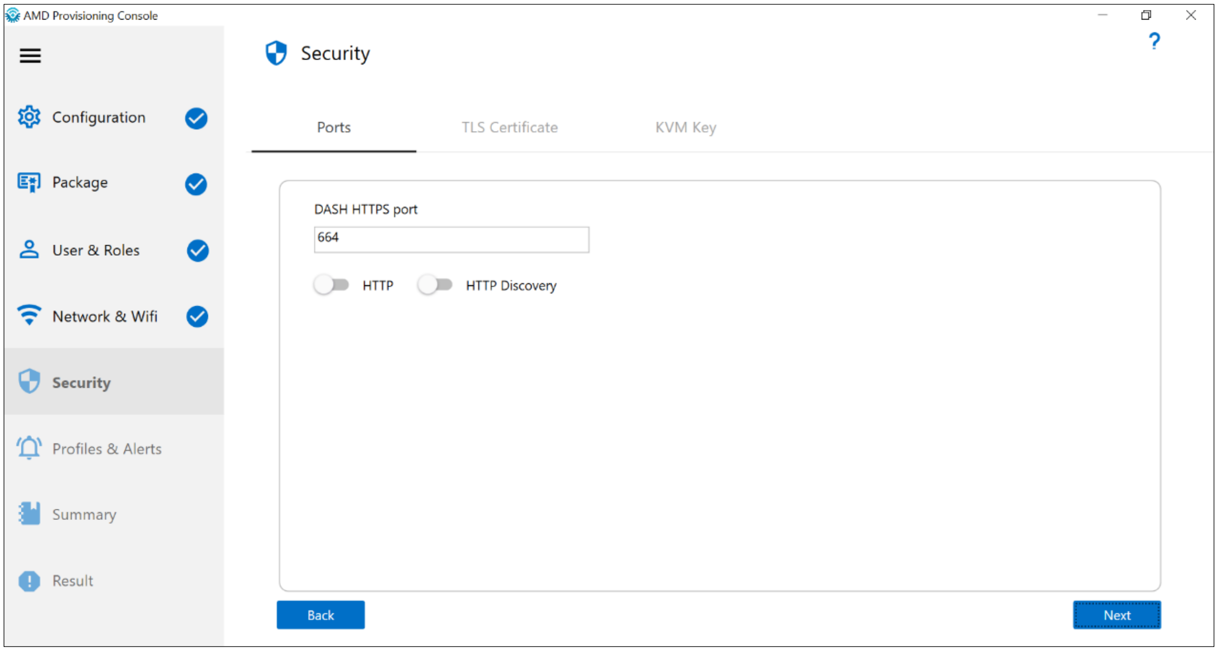
9. Add one or up to 5 Wi-Fi access point profiles. This setting is required for AIM-T in the System Shutdown mode. See *Appendix J* for details.



AMD_Wi-Fi
Personal

Figure 25. Adding Wi-Fi Access Point

10. Use the default port number (664) for **Secure port**:



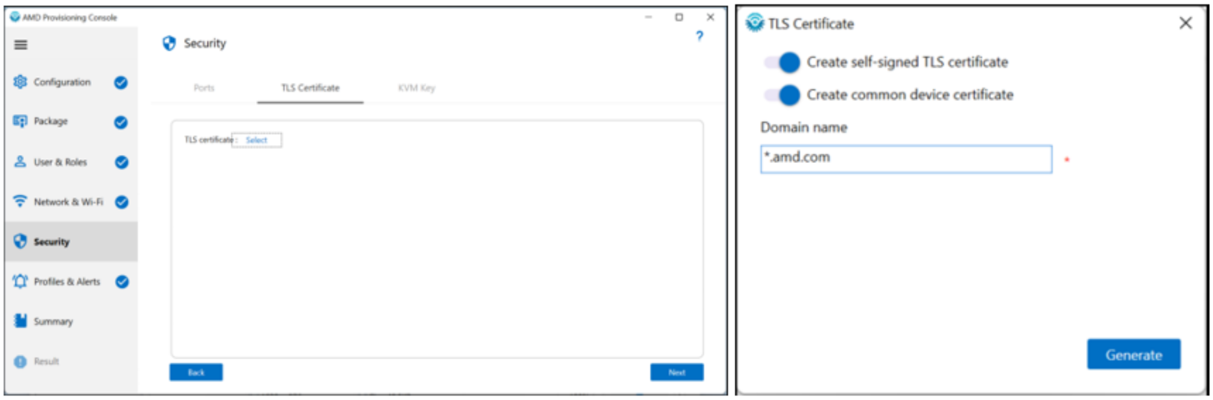
DASH HTTPS port: 664

HTTP

HTTP Discovery

Figure 26. Secure Port

11. Generate a TLS certificate:



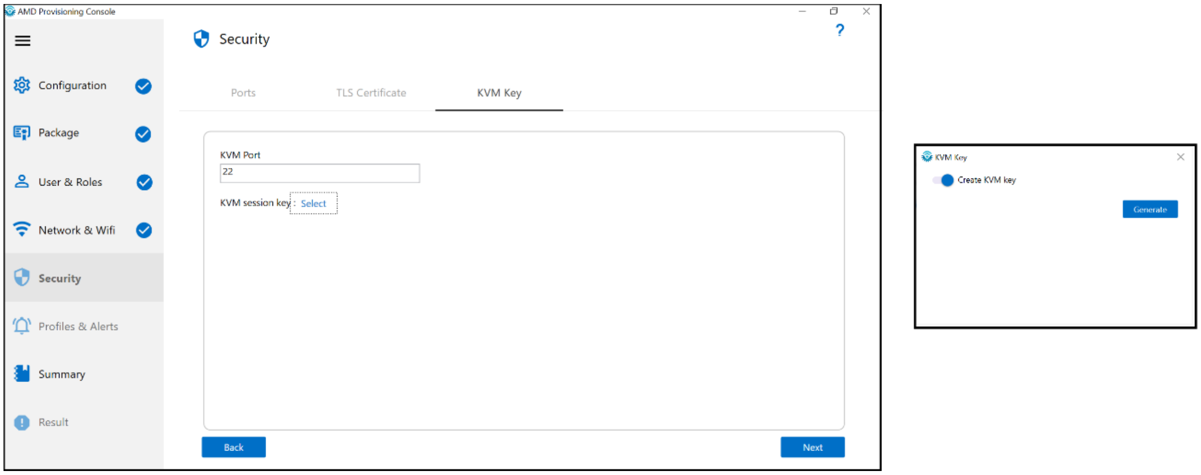
Create self-signed TLS certificate

Create common device certificate

Domain name: *.amd.com *

Figure 27. TLS Certificate

12. Generate a KVM key:

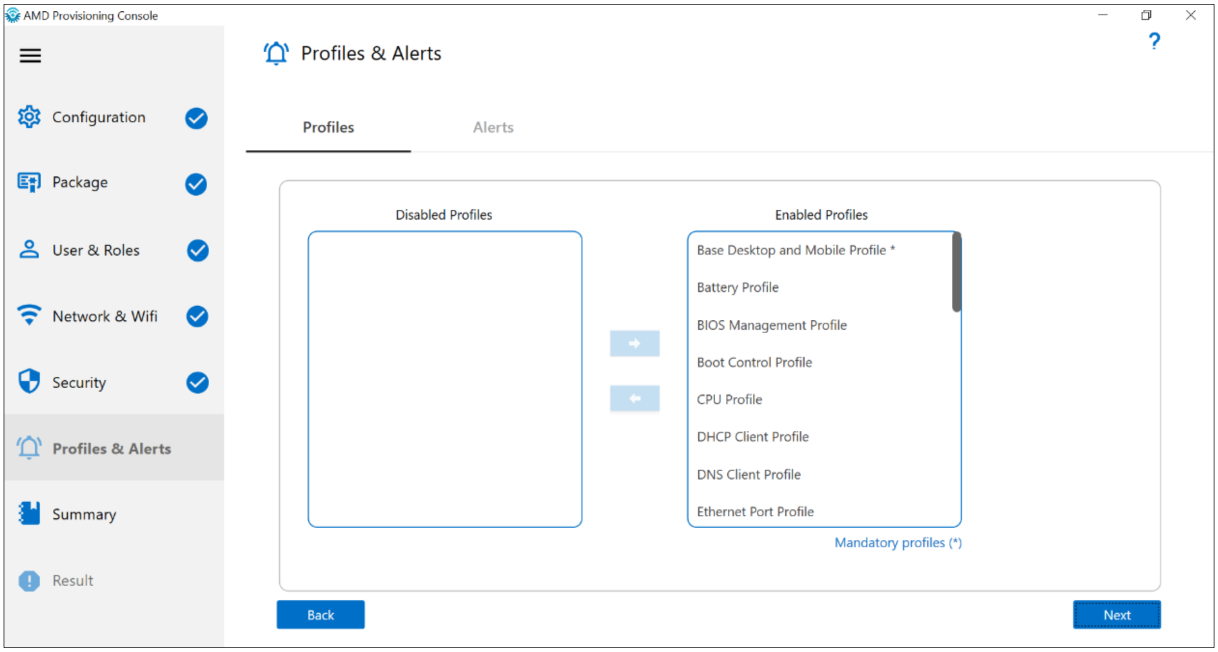


KVM Port
22

KVM session key : Select

Figure 28. KVM Key

13. All supported DASH profiles enabled by default. You can disable profiles that are not required.



Disabled Profiles

Enabled Profiles

Base Desktop and Mobile Profile *
Battery Profile
BIOS Management Profile
Boot Control Profile
CPU Profile
DHCP Client Profile
DNS Client Profile
Ethernet Port Profile

Mandatory profiles (*)

Figure 29. DASH Profiles

14. Alerts are not required. You can skip this step.

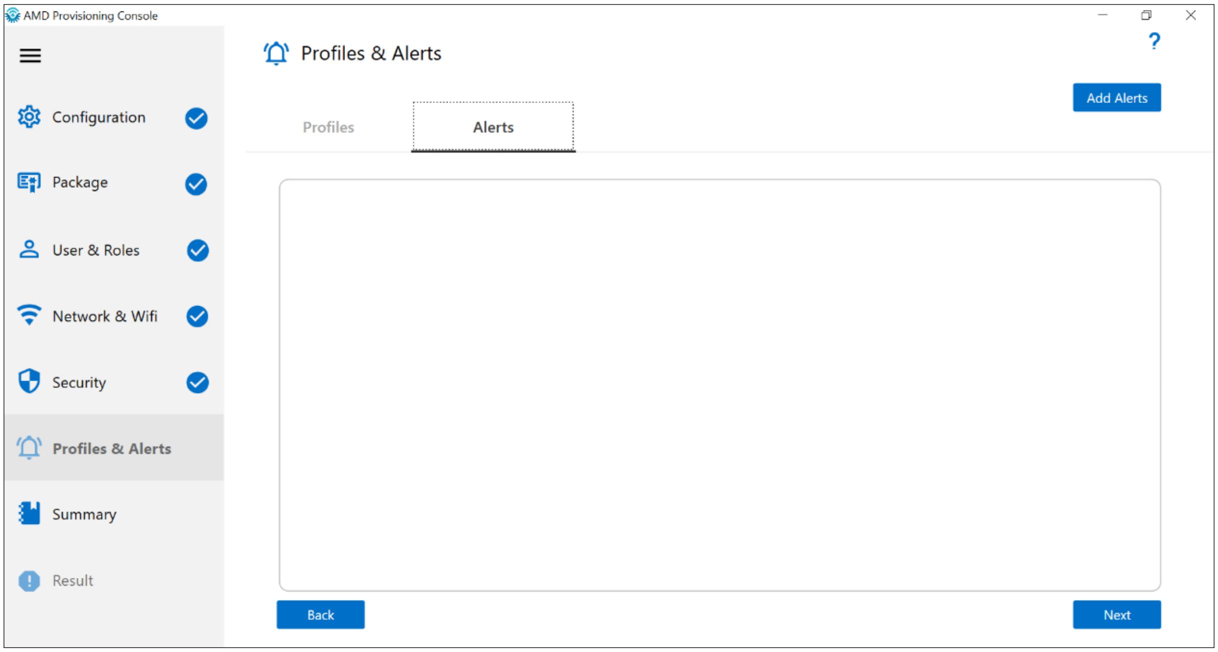
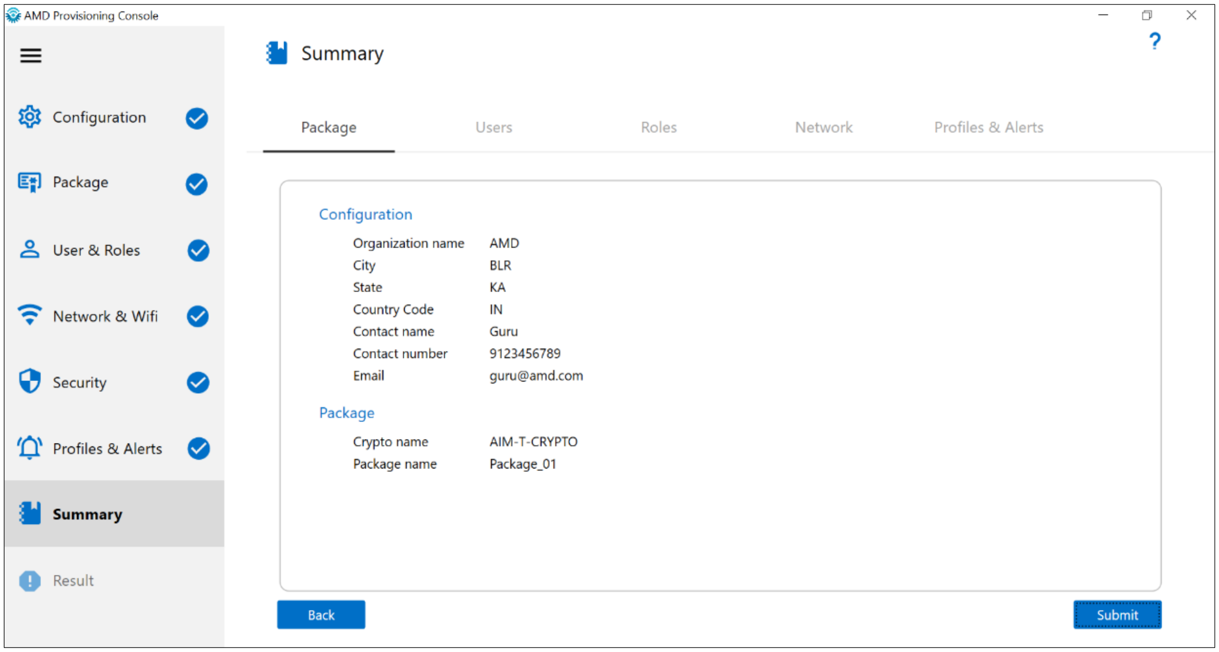


Figure 30. Alerts

15. Click the **Submit** button:



Configuration

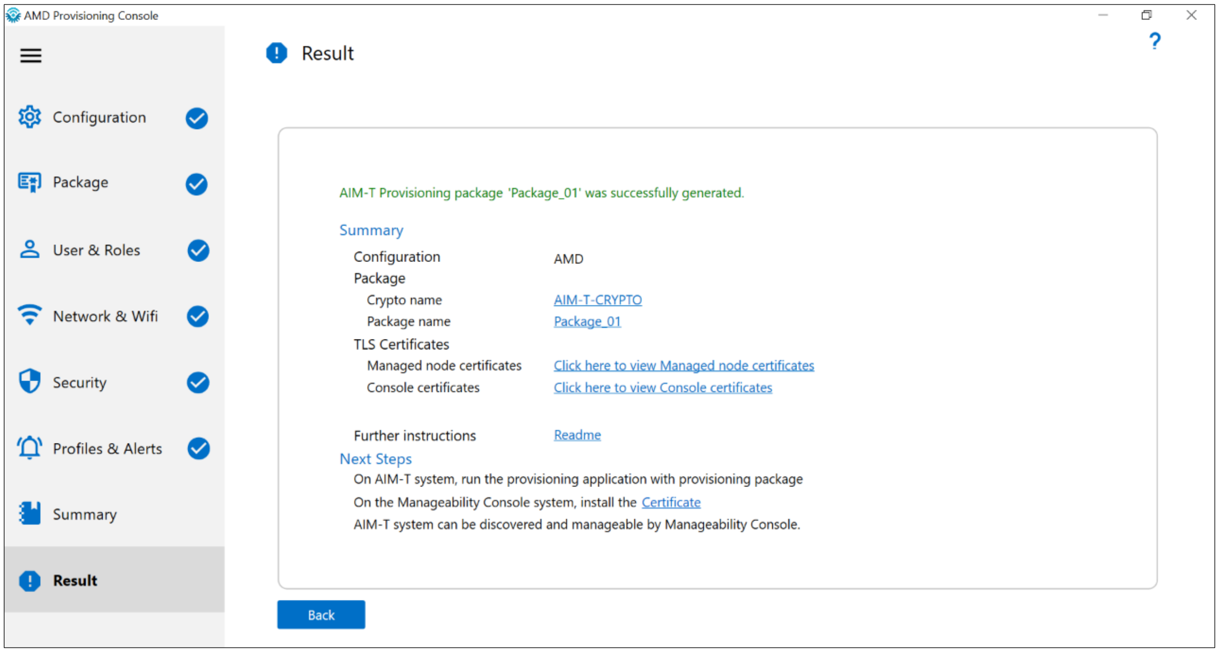
Organization name	AMD
City	BLR
State	KA
Country Code	IN
Contact name	Guru
Contact number	9123456789
Email	guru@amd.com

Package

Crypto name	AIM-T-CRYPTO
Package name	Package_01

Figure 31. Summary

The *Result* pane is displayed:



AIM-T Provisioning package 'Package_01' was successfully generated.

Summary

Configuration	AMD
Package	
Crypto name	AIM-T-CRYPTO
Package name	Package_01
TLS Certificates	
Managed node certificates	Click here to view Managed node certificates
Console certificates	Click here to view Console certificates
Further instructions	Readme

Next Steps

On AIM-T system, run the provisioning application with provisioning package

On the Manageability Console system, install the Certificate

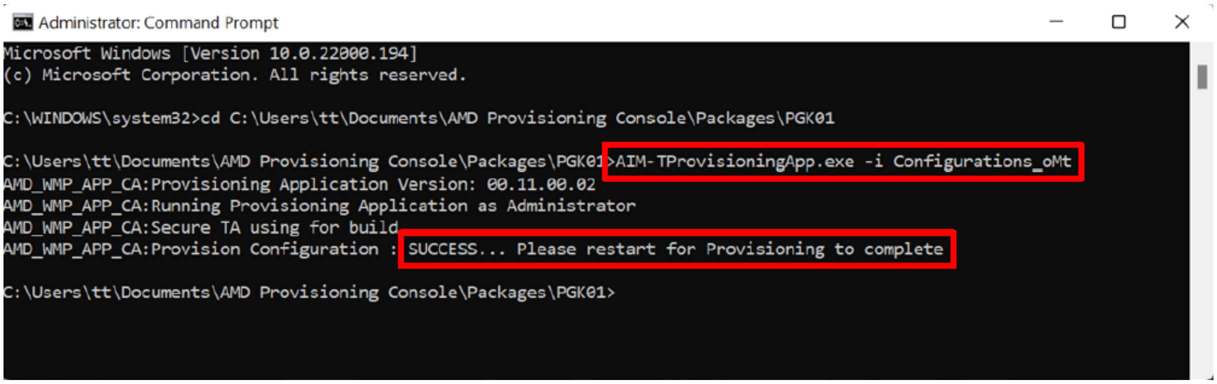
AIM-T system can be discovered and manageable by Manageability Console.

Figure 32. Result

The provisioning package is generated.

16. Copy the provisioning package (saved in the directory set in Step 4) to client (AIM-T system).
17. On the client, launch a prompt command as an administrator and go to the package location.

18. Type the command `AIM-TProvisioningApp.exe -i XXXX_oMt`:



```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.22000.194]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\tt\Documents\AMD Provisioning Console\Packages\PGK01

C:\Users\tt\Documents\AMD Provisioning Console\Packages\PGK01>AIM-TProvisioningApp.exe -i Configurations_oMt
AMD_WMP_APP_CA:Provisioning Application Version: 00.11.00.02
AMD_WMP_APP_CA:Running Provisioning Application as Administrator
AMD_WMP_APP_CA:Secure TA using for build
AMD_WMP_APP_CA:Provision Configuration : SUCCESS... Please restart for Provisioning to complete

C:\Users\tt\Documents\AMD Provisioning Console\Packages\PGK01>
```

Figure 33. Provisioning Command

19. If you generated a KVM key in Step12, copy the KVMSSHKey from the provisioning package (*<package path>\consolecertificates\KVMSSHKey*) to *C:\Program Files (x86)\DASH CLI x.y\certs\* on host.

20. Enable Active Directory (AD) feature during provisioning.

To add an Active directory user, toggle the **Active directory user** option and provide the following details.

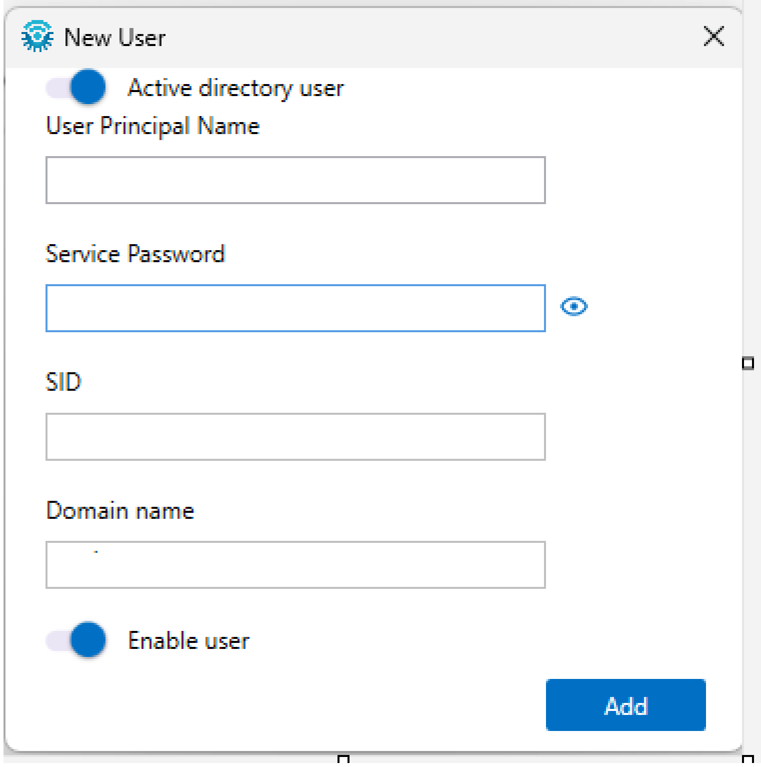


Figure 34. Add AD user

- **User Principal Name**: The AD service account through which AIM-T connects to Active directory for validating the credentials. Provide the username configured in AD.

- **Service Password**: AD service account password through which AIM-T connects to Active directory for validating the credentials.

- **SID (Security Identifier)**: Object SID of the user group through which user will be authorized.

  Provide the ID of user group created (e.g. In AD group configured by IT admin in their organization, right click on Group >Properties > Object SID)

- **Domain name**: Domain name to which AIM-T should connect for AD credential validations.

- **Enable user**: Enable or disable the user.

Appendix B Re-Provisioning

Complete the following steps to re-provision:

1. Ensure that provisioning is done on the AIM-T system.
2. Launch *AMD Provisioning Console*.
3. Select the crypto key provisioned on the AIM-T system:

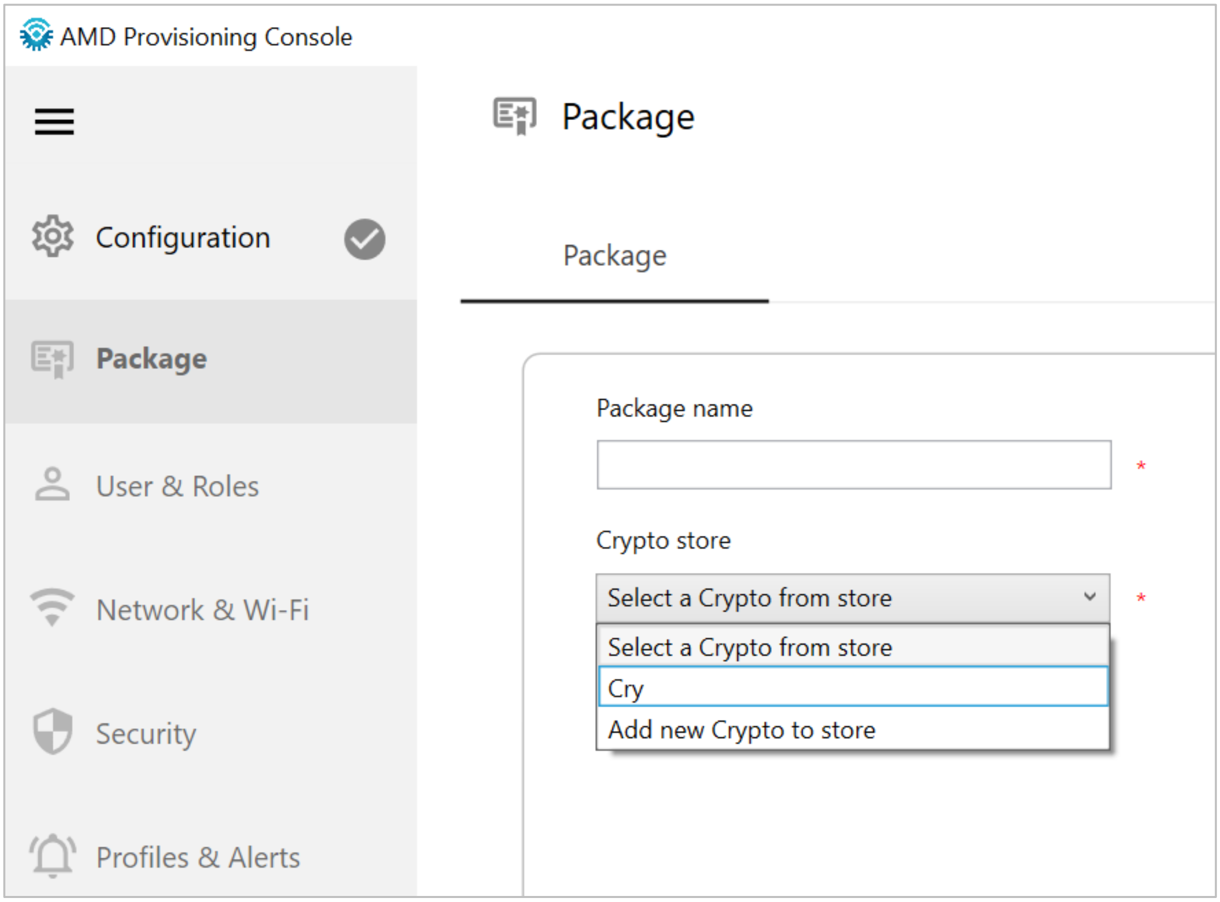


Figure 35. Select Crypto Key

4. If you cannot see the original crypto key in Step 3 but you do have a copy of the key, copy it to *Documents\AMD Provisioning Console\Cryptostore*.

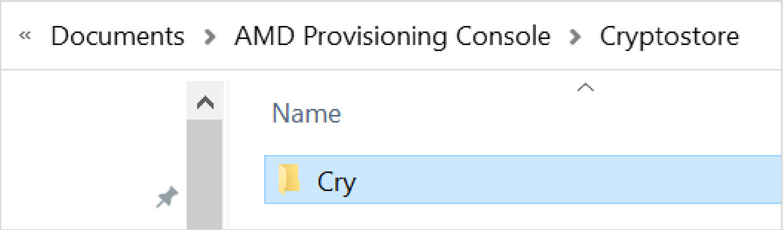
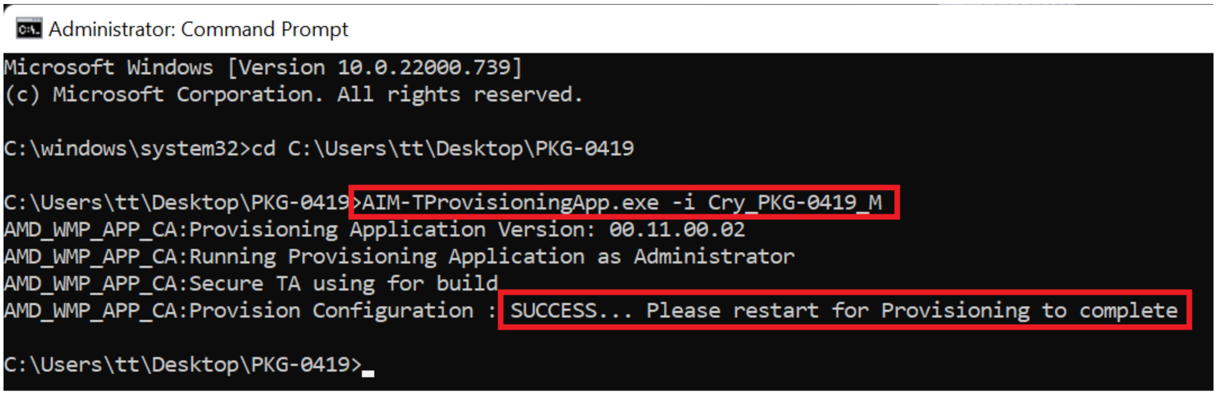


Figure 36. Copy Crypto Key

5. Repeat steps 2 and 3.

6. Refer to Appendix A and generate a provisioning package with a new username/password or new Wi-Fi AP's setting.
7. Execute the command:
   `AIM-TProvisioningApp.exe -i XXXX_M`



```
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>cd C:\Users\tt\Desktop\PKG-0419

C:\Users\tt\Desktop\PKG-0419>AIM-TProvisioningApp.exe -i Cry_PKG-0419_M
AMD_WMP_APP_CA:Provisioning Application Version: 00.11.00.02
AMD_WMP_APP_CA:Running Provisioning Application as Administrator
AMD_WMP_APP_CA:Secure TA using for build
AMD_WMP_APP_CA:Provision Configuration : SUCCESS... Please restart for Provisioning to complete

C:\Users\tt\Desktop\PKG-0419>
```

Figure 37. Re-provisioning Command

8. If you re-generate a new KVM key, complete step 19 in Appendix A to copy the KVMSSHKey to DASHCLI's *cert* folder.

Appendix C Un-Provisioning

Complete the following steps to un-provision:

1. Ensure that the AIM-T system has enabled AIM-T and is provisioned. You can send some DASH commands in Appendix D to ensure that DASH is working with its username/password.
2. Execute the following command:

```
dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -p 664 unown
```

Appendix D Supported DASH Commands

Some of the supported commands for a DASH capable system are as follows:

Note: *Adding -v 1 option will provide detailed logs.*

Table 8. Common DASH Commands

Commands	Description
`dashcli.exe -h <ipaddress> -S https -C -p 664 -a digest discover info`	Display discovery information with Digest authentication
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate computersystem`	Enumerate all the computer system profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate registeredprofile`	Enumerate all the registered profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate sensor`	Enumerate sensor details
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate processor`	Enumerate all the processor profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate dhcpclient`	Enumerate all the DHCP client profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate dnsclient`	Enumerate all the DNS client profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate ethernetport`	Enumerate all the ethernet port profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate networkport`	Enumerate all the network port profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate ipinterface`	Enumerate all the IP interface profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate ipconfiguration`	Enumerate all the IP configuration profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate operatingsystem`	Enumerate all the OS profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate asset`	Enumerate all the asset profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate memory`	Enumerate all the memory profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate pcidevice`	Enumerate all the PCI device instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate ssh`	Enumerate all the SSH profile instances
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate recordlog`	Enumerate all the records information

Commands	Description
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate battery`	Enumerate the battery info
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t computersystem[#instance] power status`	Display current power status of the AIM-T system
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t computersystem[#instance] power shutdown`	Power shutdown the AIM-T system
`dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t computersystem[#instance] power cycle`	Power cycle the AIM-T system

`dashcli -h dash-system -p 664 -S https -C  -u <username> -P <password> software[0] install  <URL for Capsule>`
`Example:  dashcli -h 192.168.0.176 -S https -C -p 664   -u admin -P amd@123 -t software[0] install http://192.168.0.211:3274/Capsule.zip`
	Update the Software BIOS through Capsule update

***Note**: For a full list of supported DASH commands please refer DASH CLI user guide packaged with DASH CLI installation.*

Appendix E Using KVM

When an OEM device supports KVM function, a host (IT's system) can use DASHCLI `startkvm` command to initiate a KVM session to the AIM-T system:

```
dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t
kvmredirection[0] startkvm
```

Complete the following steps to establish a KVM session:

1. Enable AIM-T and KVM function on AIM-T system's BIOS setup menu.
2. Ensure that the AIM-T system has been AIM-T provisioned (Appendix A).
3. Place a copy of KVMSSHKey in *C:\Program Files (x86)\DASH CLI 4.0\certs\,* where you execute DASHCLI commands on host (Appendix A).
4. Boot AIM-T system to OS.
5. Run one of the following DASH commands on the host:

   ```
   dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t
   kvmredirection[0] startkvm
   ```

   or

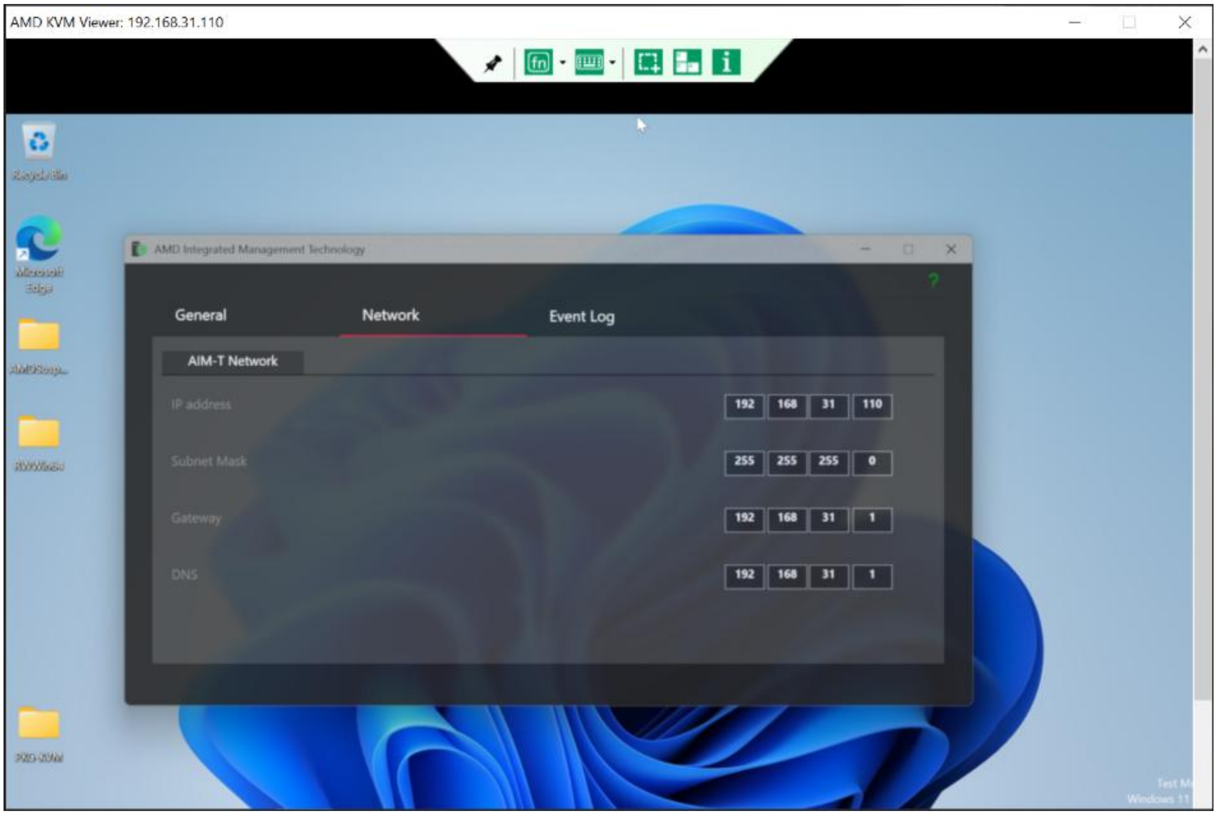
   ```
   dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t
   kvmredirection[0] startoskvm
   ```

   For more information, refer to Figure 17. DASH CLI – KVM Output.

6. If the step 3 was executed correctly, a VNC viewer will be launched on host.
7. If the graphics driver installed on the AIM-T system supports instant KVM, go to step 8 for OS KVM. Otherwise, the system will auto-reboot and go to step 10 for BIOS KVM.

Note: *Ctrl + Alt + Del combination requires DASH CLI 7.0 or higher. Otherwise, Ctrl key is known to cause issues.*

8. Host can see the client's screen on VNC viewer called OS KVM:



AMD KVM Viewer: 192.168.31.110

AMD Integrated Management Technology

General | Network | Event Log

AIM-T Network

IP address 192 168 31 110

Subnet Mask 255 255 255 0

Gateway 192 168 31 1

DNS 192 168 31 1

Figure 38. AMD KVM Viewer

9. To trigger the BIOS KVM, configure the VNC viewer to restart the client in Windows power option.
10. After reboot, the AIM-T system will stop at F1/F2 window. The same screen is displayed on the VNC viewer. F1 is selected by default; it is to continue to OS and F2 is to boot to BIOS.

    Note: *OEM may change the definition of F1/F2 or replace it with other keys.*

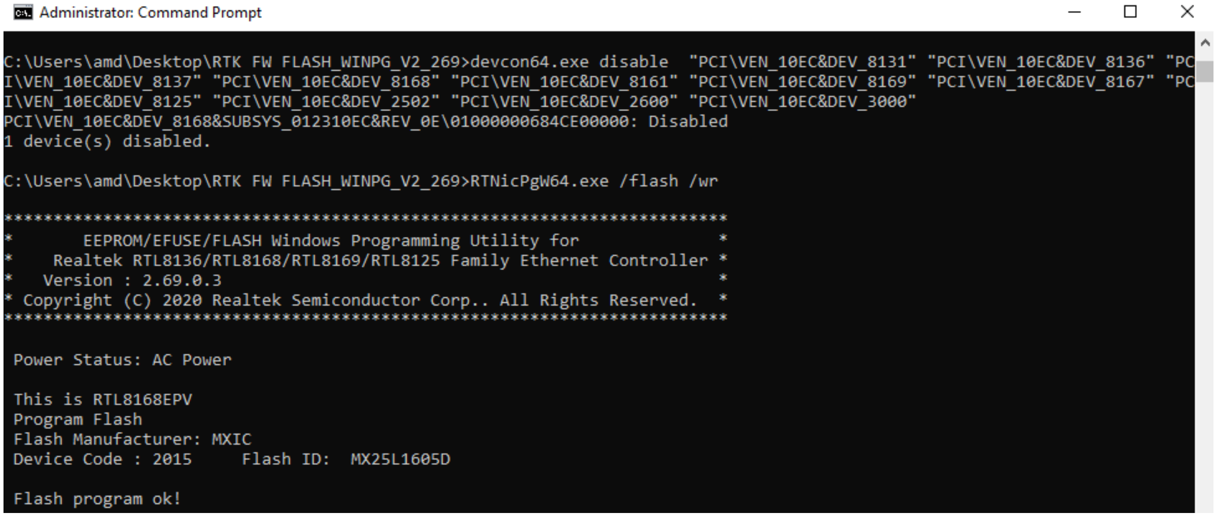
11. Based on the F1/F2 configuration in the previous step, press F1 on the VNC Viewer. The AIM-T system will boot to OS and OS KVM will be established.
    If you press F2, the client will boot to BIOS setup menu (BIOS KVM).
12. Ensure that BIOS menu navigation is possible using keyboard and mouse from the VNC viewer.
13. If required, modify the BIOS settings using VNC viewer and save them.
14. The AIM-T system should auto-reboot while exiting the BIOS setup menu. Check if the changes made in the previous step are reflected correctly.
15. Close the VNC viewer to finish the KVM session and select **Yes** to reboot the AIM-T system again.

    Note: *If you select* ***No****, the AIM-T system will not restart.*

Appendix F Flashing RTK NIC Firmware

Contact OEM for more information on getting the flash tool with the bin file.

You can use the command line interface with the related bin file (68EPSPIB.bin) to flash Realtek NIC's firmware and Config file (68EPSPI.CFG) to run *WINPG64.bat*. The following figure shows the firmware flashed successfully:



```
C:\Users\amd\Desktop\RTK FW FLASH_WINPG_V2_269>devcon64.exe disable  "PCI\VEN_10EC&DEV_8131" "PCI\VEN_10EC&DEV_8136" "PC
I\VEN_10EC&DEV_8137" "PCI\VEN_10EC&DEV_8168" "PCI\VEN_10EC&DEV_8161" "PCI\VEN_10EC&DEV_8169" "PCI\VEN_10EC&DEV_8167" "PC
I\VEN_10EC&DEV_8125" "PCI\VEN_10EC&DEV_2502" "PCI\VEN_10EC&DEV_2600" "PCI\VEN_10EC&DEV_3000"
PCI\VEN_10EC&DEV_8168&SUBSYS_012310EC&REV_0E\01000000684CE00000: Disabled
1 device(s) disabled.

C:\Users\amd\Desktop\RTK FW FLASH_WINPG_V2_269>RTNicPgW64.exe /flash /wr

*************************************************************************
*       EEPROM/EFUSE/FLASH Windows Programming Utility for              *
*    Realtek RTL8136/RTL8168/RTL8169/RTL8125 Family Ethernet Controller *
*   Version : 2.69.0.3                                                  *
* Copyright (C) 2020 Realtek Semiconductor Corp.. All Rights Reserved.  *
*************************************************************************

 Power Status: AC Power

 This is RTL8168EPV
 Program Flash
 Flash Manufacturer: MXIC
 Device Code : 2015     Flash ID:  MX25L1605D

 Flash program ok!
```

Figure 39. Firmware Flash Status

Appendix G Supported Wired DASH Profiles

Table 9. Supported Wired DASH Profiles

Profiles	Requirement
Base Desktop and Mobile	Mandatory
Profile Registration	Mandatory
Role Based Authorization	Mandatory
Simple Identity Management	Mandatory
BIOS Management	Optional
Boot Control	Optional
CPU	Optional
DHCP	Optional
Fan	Optional
Indications	Optional
IP Interface	Optional
KVM Redirection	Optional
OS Status	Optional
Physical Asset	Optional
Power State Management	Optional
Power Supply	Optional
Record Log	Optional
Sensor	Optional
Battery	Optional
Software Inventory	Optional
Software Update	Optional
System Memory	Optional
Text Console redirection	Optional
USB Redirection	Optional

Appendix H Supported DASH Profiles in AIM-T

DMTF DASH Specification - *https://www.dmtf.org/standards/dash*

See 2.1 Supported DASH Profiles for a list of all supported DASH profiles release-wise.

AMD PRO Manageability Features	Corresponding Profiles
Asset Inventory - HW/SW	DSP1011 DSP1022 DSP1013 DSP1075 DSP1030 DSP1029 DSP1026 DSP1015 DSP1009 DSP1061 DSP1023
Remote Power Control / DASH Power Control	DSP1027
Boot Control	DSP1012
Platform Alerts	DSP1010 DSP1054
HTTPS Secure Transport & WS-Management	DSP0226 DSP0232
Standardized Discovery	DSP0232
User Administration	DSP1034 DSP1039 We do support DASH user and not host OS credentials.
IPv4 (out-of-band)	Supported
Text Console Redirection	DSP1024 DSP1017

AMD PRO Manageability Features	Corresponding Profiles
BIOS Management	DSP1061
PLDM/MCTP interfaces for Health monitoring (fan speed, temp, etc.)	DSP0240 We do use PLDM. We do not need MCTP as MPM also as part of platform and we are using custom PLDM.
OS Status (Out of band)	DSP1029
“Graceful”"/ “Soft” Shutdown	DSP1027
Management Firmware Update - Remotely	DSP1025
AMD KVM Redirection	DSP1076 DSP1017
Network Information	DSP1088 DSP1014 DSP1035 DSP1036 DSP1037 DSP1038 DSP1116

AMD PRO Manageability Features	Corresponding Profiles	AIM-T Version
Asset Inventory - HW/SW	DSP1011 DSP1022 DSP1013 DSP1075 DSP1030 DSP1029 DSP1026 DSP1015 DSP1009 DSP1061 DSP1023	
Remote Power Control / DASH Power Control	DSP1027	
Boot Control	DSP1012	
Platform Alerts	DSP1010 DSP1054	
HTTPS Secure Transport & WS-Management	DSP0226 DSP0232	
Standardized Discovery	DSP0232	
User Administration	DSP1034 DSP1039 We do support DASH user and not host OS credentials.	
IPv4 (out-of-band)	Supported	
Text Console Redirection	DSP1024 DSP1017	
BIOS Management	DSP1061	

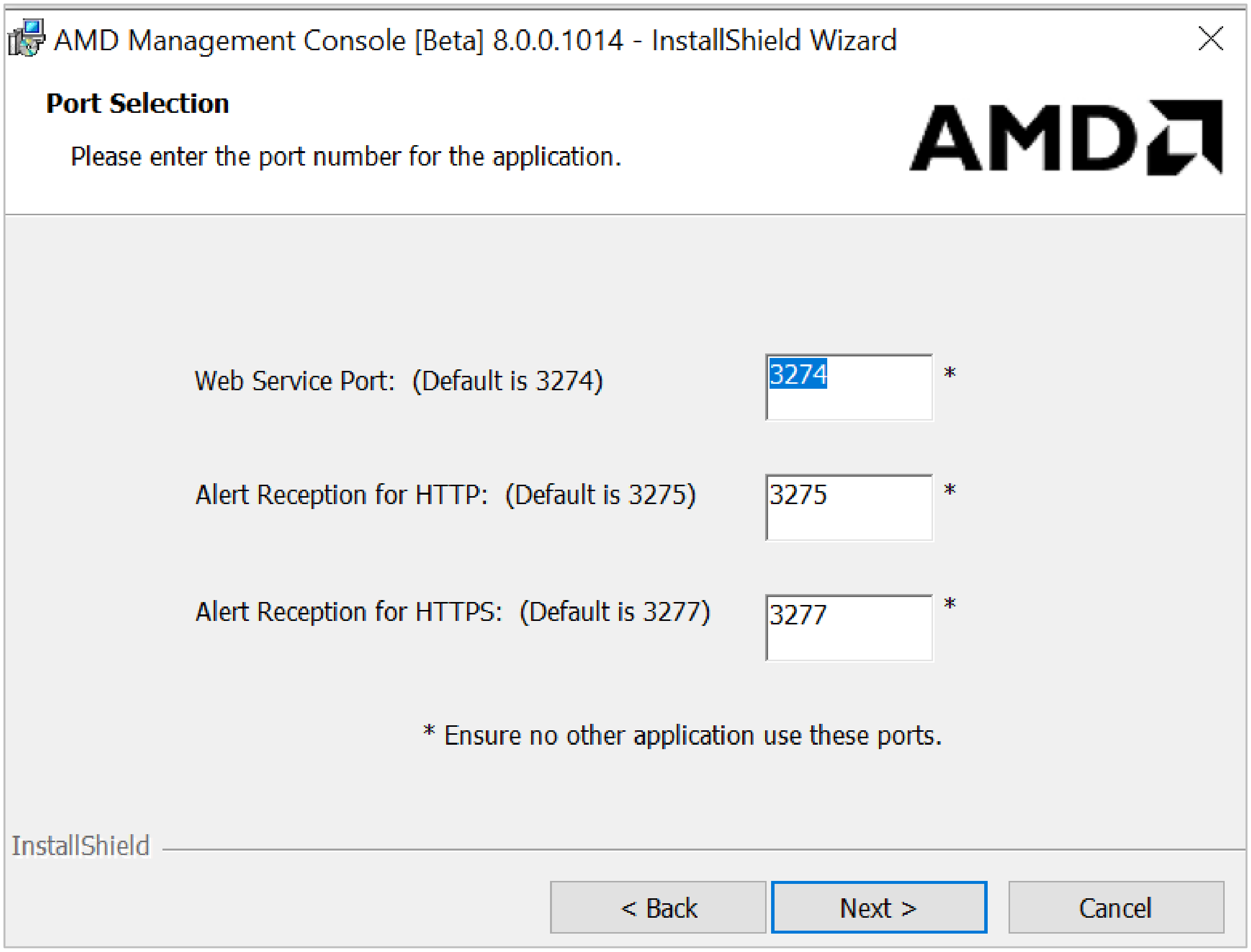
AMD PRO Manageability Features	Corresponding Profiles	AIM-T Version
PLDM/MCTP interfaces for Health monitoring (fan speed, temp, etc.)	DSP0240 We do use PLDM. We do not need MCTP as MPM also as part of platform and we are using custom PLDM.	
OS Status (Out of band)	DSP1029	
“Graceful”/“Soft” Shutdown	DSP1027	
Management Firmware Update - Remotely	DSP1025	
AMD KVM Redirection	DSP1076 DSP1017	
Network Information	DSP1088 DSP1014 DSP1035 DSP1036 DSP1037 DSP1038 DSP1116	

Appendix I Updating BIOS Capsule

An enterprise IT admin is allowed to force a AIM-T system for performing a BIOS capsule update with DASH commands. However, the IT must setup a download server for AIM-T systems to download the latest valid capsule that can be recognized and installed by Windows OS. The AMS installed on AIM-T systems utilizes an inbox app *PnPutil.exe* in OS to install a BIOS capsule. DASH commands can ask a AIM-T system to download the capsule and then AMS will run *PnPutil.exe* to install the capsule.

I.1 Setting up a Download Server

AMD provides the tool AMD Management Console (AMC- *www.amd.com/DASH*) to send DASH commands with a user-friendly interface. When installing AMC, the installer will simulate a virtual webserver with the network port 3274 (by default) and create a folder "*C:\AMC-ISO*" to act as the download space.



AMD Management Console [Beta] 8.0.0.1014 - InstallShield Wizard

Port Selection

Please enter the port number for the application.

Web Service Port: (Default is 3274) 3274 *

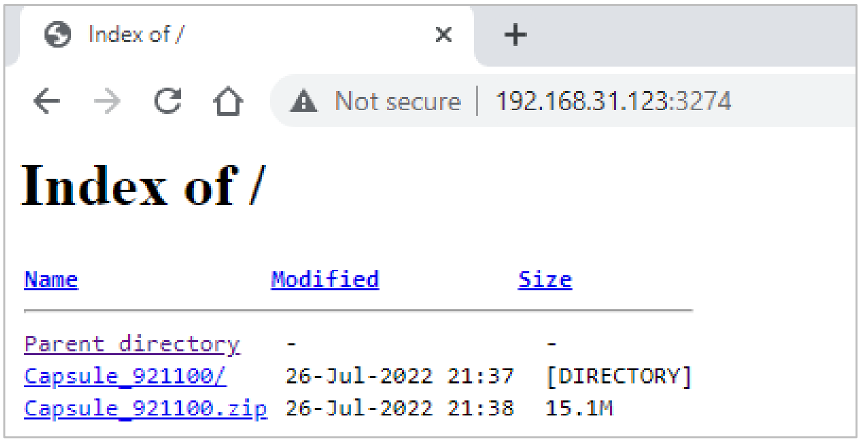
Alert Reception for HTTP: (Default is 3275) 3275 *

Alert Reception for HTTPS: (Default is 3277) 3277 *

* Ensure no other application use these ports.

Figure 40. AMC - Port Selection

After AMC is installed, you can place any file in the folder *C:\AMC-ISO* and type-in: http:<ip of AMC console machine>:3274 in the web browser to test it:



Index of /

```
Name                Modified            Size

Parent directory    -                   -
Capsule_921100/     26-Jul-2022 21:37   [DIRECTORY]
Capsule_921100.zip  26-Jul-2022 21:38   15.1M
```

Figure 41. Testing AMC

Note: *The network port 3274 may be blocked by the firewall, an IT admin must give permission to allow the traffic through this port.*

I.2 Preparing a Valid Capsule

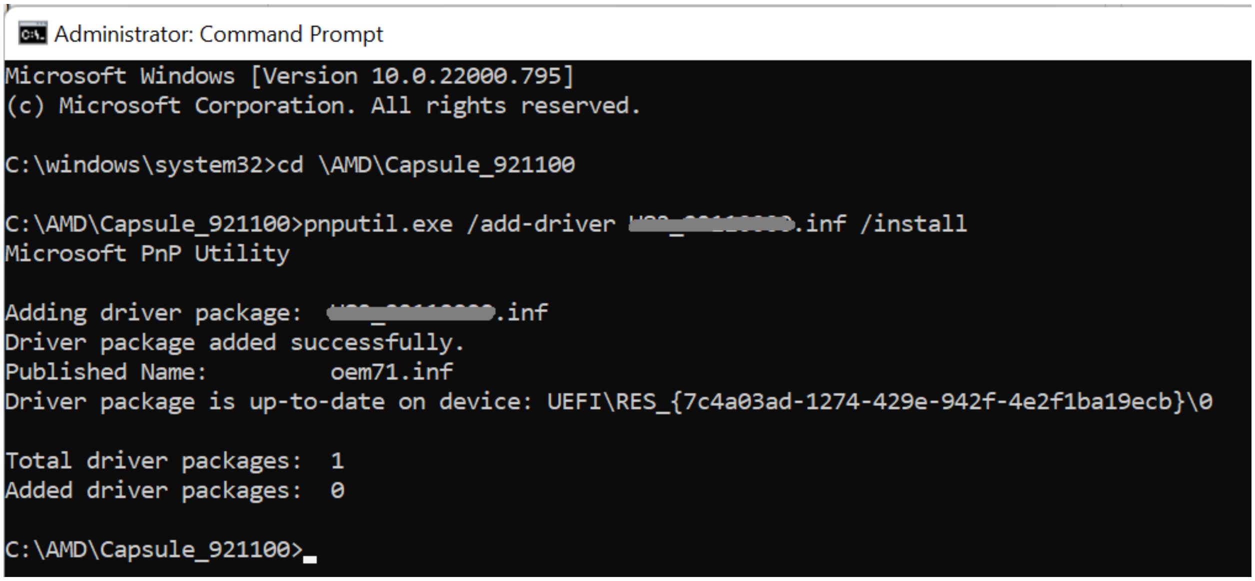
An enterprise IT should be able to download a BIOS capsule from the OEM's website (or other channels). A valid capsule includes:

- *.bin* or *.cap* file – the new firmware
- *.cer* file – the certificate
- *.cat* file – the driver catalog
- *.inf* file – the driver information

You can launch a command prompt as admin and execute the following command to trigger the capsule installation:

```
PnPutil.exe /add-driver xxx.inf /install
```

If the installation is successful, it means the capsule is valid:



```
Microsoft Windows [Version 10.0.22000.795]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>cd \AMD\Capsule_921100

C:\AMD\Capsule_921100>pnputil.exe /add-driver [redacted].inf /install
Microsoft PnP Utility

Adding driver package:  [redacted].inf
Driver package added successfully.
Published Name:         oem71.inf
Driver package is up-to-date on device: UEFI\RES_{7c4a03ad-1274-429e-942f-4e2f1ba19ecb}\0

Total driver packages:  1
Added driver packages:  0

C:\AMD\Capsule_921100>_
```

Figure 42. Valid Capsule

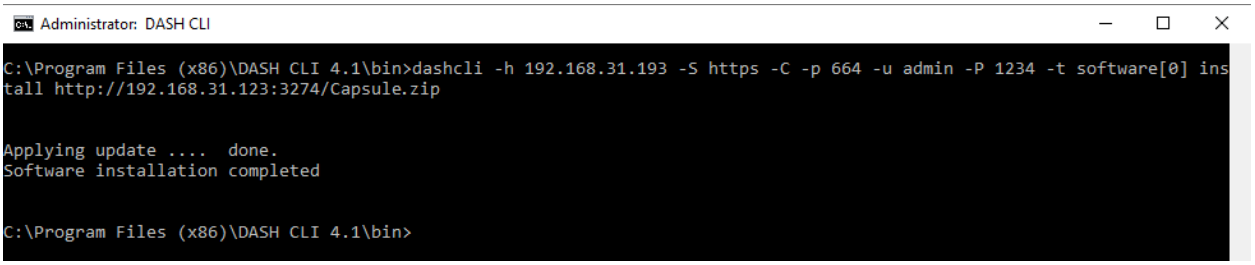
I.3 Reforming the Capsule

After verifying the content of a BIOS capsule, reform the capsule to an AMS readable format as follows:

1. Create a folder **Capsule**.
2. Copy all the files from the valid capsule and paste them to the new folder *\Capsule*.
3. Zip *\Capsule* into *capsule.zip.*
4. Put *capsule.zip* in *C:\AMC-ISO.*

I.4 DASH Command for Capsule Update

```
dashcli -h <ipaddress> -p 664 -S https -C -u <username> -P <password> software[0] install
<URL for Capsule>
```



```
C:\Program Files (x86)\DASH CLI 4.1\bin>dashcli -h 192.168.31.193 -S https -C -p 664 -u admin -P 1234 -t software[0] ins
tall http://192.168.31.123:3274/Capsule.zip


Applying update ....  done.
Software installation completed


C:\Program Files (x86)\DASH CLI 4.1\bin>
```

Figure 43. Capsule Update

Appendix J AMD Cloud Manageability Service

AMD Manageability solution enables the IT administrators to effectively manage enterprise systems when the system is powered on/off.

AMD Cloud Manageability Service (ACMS) is a software product within AMD Manageability that enables the IT administrators to manage enterprise systems even when those systems are outside the enterprise network. A limitation in current DASH implementation is that both IT admin and DASH node must be on the same network or routable domain. ACMS circumvents this limitation by introducing a publicly running daemon that will facilitate IT admins to manage a DASH node from their homes (public network).

J.1 Requirements

You can get the ACMS software from the downloads section of the AMD portal (*https://www.amd.com/DASH*).

- To run ACMS, it should be deployed on either
  - Linux® system capable of running Ubuntu® 24.04 LTS
  - Windows Server 2022

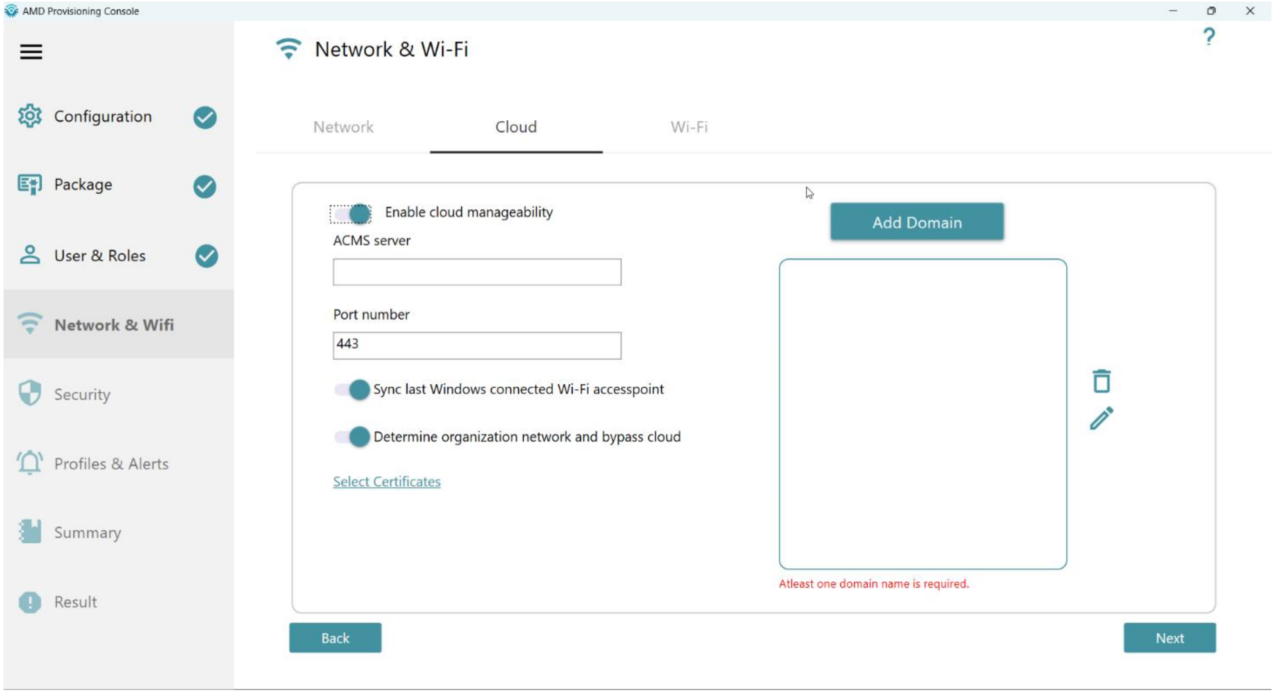
  Note: Sever must be hosted with a Public IP.
- On public clouds, it can be achieved by spawning Virtual Machine (VM) in public subnet or behind a load balancer. The recommended configuration for all the systems is 4-core x64 with at least 4 GB of RAM.
- AIM-T 2.0 and later supports AMD Cloud Manageability. Ensure that AMS 2.0 or later is installed on Windows® on the managed node. AIM-T system must be provisioned with cloud option enabled using AMD Provisioning Console.
- You can use DASH CLI to issue the manageability commands over cloud. DASH CLI 4.5 and later support AMD Cloud Manageability.
- AMD Provisioning Console (APC) is used to generate TLS certificates and to configure ACMS server hostname in managed systems. APC 2.0 and later have the cloud option.

J.2 Installation and Setup

Before installing the ACMS, create a provisioning package using APC to generate the required TLS certificates.

APC is used to generate certificate, key, and certificate authority for ACMS, DASH CLI, and AIM-T.

The following figure shows various options of the APC page:



Enable cloud manageability

ACMS server

Port number
443

Sync last Windows connected Wi-Fi accesspoint

Determine organization network and bypass cloud

Select Certificates

Atleast one domain name is required.

Figure 44. APC Page Screeshot

The generated files are present at the following path:

$(SecurePath)\AMD Provisioning Console\Packages\$(PackageName)\AIM-T\ACMS\

$(SecurePath) is the path provided to the APC tool, $(PackageName) is the package name provided by the user. The following three folders are present at this location:

- ACMS
  - *acmscert.pem*
  - *acmskey.pem*
  - *trustedclients.pem*
- DASHCLI

  – acmscert.pem
  – consolecert.pem

J.2.1 Installation

Complete the following steps to install ACMS:

1. On Ubuntu, install the package as follows:

```
$ sudo apt install ./acms_1.0.0.1099_amd64.deb
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'acms' instead of './acms_1.0.0.1099_amd64.deb'
The following NEW packages will be installed:
  acms
0 upgraded, 1 newly installed, 0 to remove and 62 not upgraded.
After this operation, 1,474 kB of additional disk space will be used.
Get:1 /home/amd/certs-work/acms_1.0.0.1099_amd64.deb acms amd64 1.0.0.1099 [417 kB]
Selecting previously unselected package acms.
(Reading database ... 254233 files and directories currently installed.)
Preparing to unpack .../acms_1.0.0.1099_amd64.deb ...
Unpacking acms (1.0.0.1099) ...
Setting up acms (1.0.0.1099) ...
```

2. Start ACMS:

```
$ sudo systemctl start acms
```

3. Verify that it is running on port 443:

```
$ systemctl status amcs
● acms.service - AMD Cloud Manageability Service
     Loaded: loaded (/lib/systemd/system/acms.service; enabled; vendor preset:
enabled)
     Active: active (running) since Tue 2023-01-31 13:51:22 IST; 2s ago
   Main PID: 485996 (acms)
      Tasks: 1 (limit: 9375)
     Memory: 756.0K
     CGroup: /system.slice/acms.service
             └─485996 /bin/acms --bind 0.0.0.0:443 --poll 60 --cert
/etc/acms/acmscert.pem --key /etc/acms/acmskey.pem --ca /etc/acms/trustedclients.pem

Jan 31 13:51:22 acms-host systemd[1]: Started AMD Cloud Manageability Service.
```

4. (Optional) Enable it to start automatically at boot time:

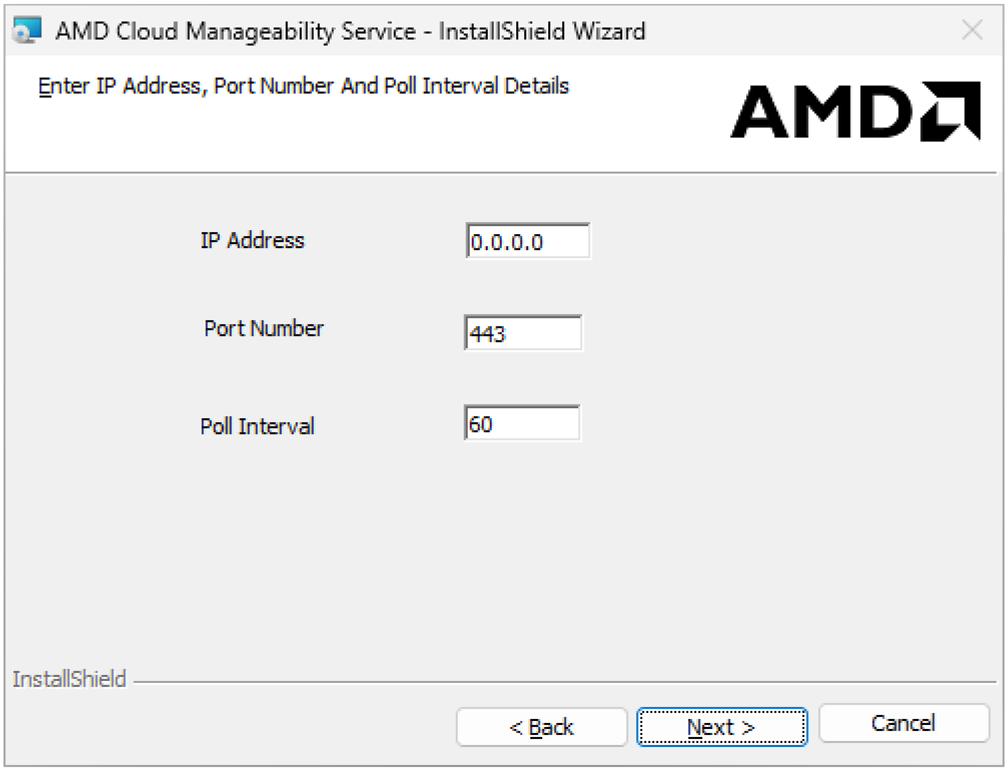
```
$ sudo systemctl enable acms
Created symlink /etc/systemd/system/multi-user.target.wants/acms.service →
/lib/systemd/system/acms.service.
```

5. Use `journalctl` to view the logs from ACMS and `-f` option for the live logs:

```
$ journalctl -fu acms
```

On Windows

1) Download the latest available installer and follow on-screen instructions.
    a. Use the default options or configure these options:



AMD Cloud Manageability Service - InstallShield Wizard

Enter IP Address, Port Number And Poll Interval Details

IP Address: 0.0.0.0

Port Number: 443

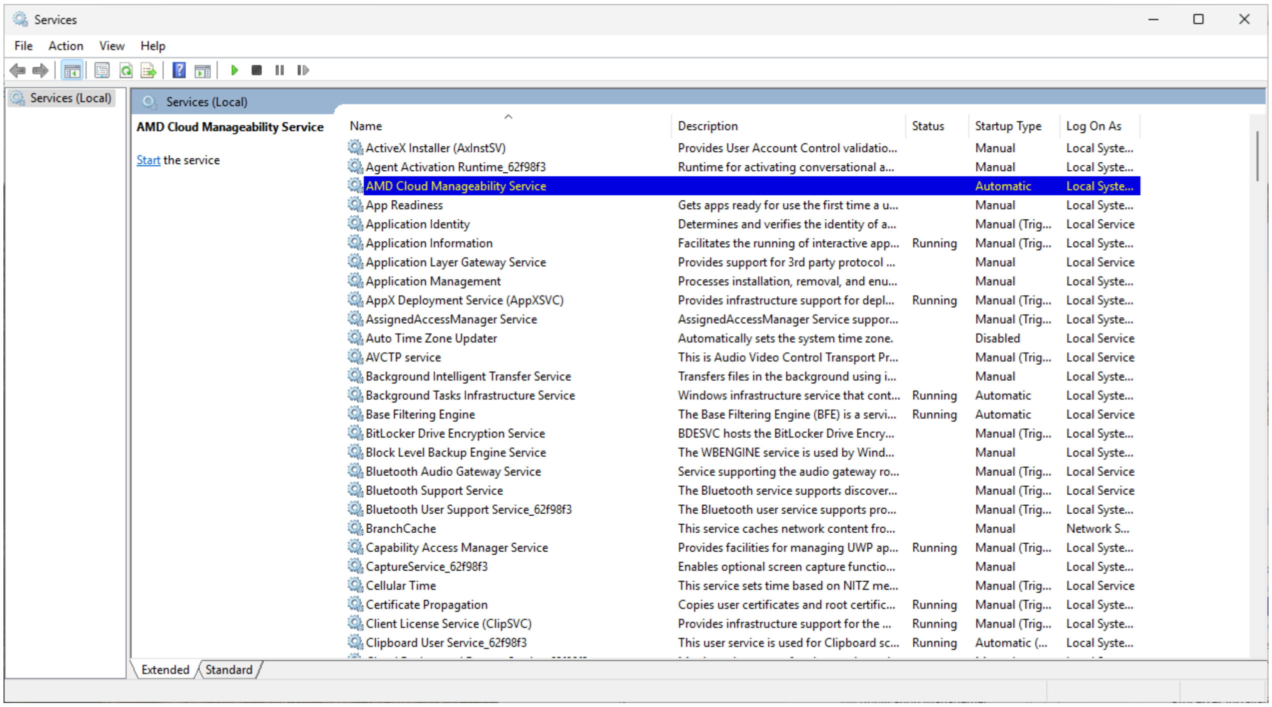
Poll Interval: 60

Figure 45. ACMS options during installations

Copy all 3 certificates created using APC tool, available at**: $(SecurePath)\AMD Provisioning Console\Packages\$(PackageName)\AIM-T\ACMS\** to the installation path: ***%ProgramFiles%\AMD\Cloud Manageability Service\Certs***

b. acmscert.pem
c. acmskey.pem
d. trustedclients.pem

2) After installation is complete, search for the service "***AMD Cloud Manageability Service***" in the services applet [services.msc] and start it.



AMD Cloud Manageability Service

Start the service

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides User Account Control validatio...		Manual	Local Syste...
Agent Activation Runtime_62f98f3	Runtime for activating conversational a...		Manual	Local Syste...
AMD Cloud Manageability Service			Automatic	Local Syste...
App Readiness	Gets apps ready for use the first time a u...		Manual	Local Syste...
Application Identity	Determines and verifies the identity of a...		Manual (Trig...	Local Service
Application Information	Facilitates the running of interactive app...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway Service	Provides support for 3rd party protocol ...		Manual	Local Service
Application Management	Processes installation, removal, and enu...		Manual	Local Syste...
AppX Deployment Service (AppXSVC)	Provides infrastructure support for depl...	Running	Manual (Trig...	Local Syste...
AssignedAccessManager Service	AssignedAccessManager Service suppor...		Manual (Trig...	Local Syste...
Auto Time Zone Updater	Automatically sets the system time zone.		Disabled	Local Service
AVCTP service	This is Audio Video Control Transport Pr...		Manual (Trig...	Local Service
Background Intelligent Transfer Service	Transfers files in the background using i...		Manual	Local Syste...
Background Tasks Infrastructure Service	Windows infrastructure service that cont...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Filtering Engine (BFE) is a servi...	Running	Automatic	Local Service
BitLocker Drive Encryption Service	BDESVC hosts the BitLocker Drive Encry...		Manual (Trig...	Local Syste...
Block Level Backup Engine Service	The WBENGINE service is used by Wind...		Manual	Local Syste...
Bluetooth Audio Gateway Service	Service supporting the audio gateway ro...		Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetooth service supports discover...		Manual (Trig...	Local Service
Bluetooth User Support Service_62f98f3	The Bluetooth user service supports pro...		Manual (Trig...	Local Syste...
BranchCache	This service caches network content fro...		Manual	Network S...
Capability Access Manager Service	Provides facilities for managing UWP ap...	Running	Manual (Trig...	Local Syste...
CaptureService_62f98f3	Enables optional screen capture functio...		Manual	Local Syste...
Cellular Time	This service sets time based on NITZ me...		Manual (Trig...	Local Service
Certificate Propagation	Copies user certificates and root certific...	Running	Manual (Trig...	Local Syste...
Client License Service (ClipSVC)	Provides infrastructure support for the ...	Running	Manual (Trig...	Local Syste...
Clipboard User Service_62f98f3	This user service is used for Clipboard sc...	Running	Automatic (...	Local Syste...

Figure 46. APC Page Screeshot ACMS service

J.2.2 Configuration

ACMS implements 2-way-TLS for securing itself against unauthorized access. Hence, only the clients with trusted certificate will be able to connect. The certificates, private key, and certificate authority files in PEM format respectively are expected at the following locations:

```
/etc/acms/amcscert.pem
/etc/acms/acmskey.pem
/etc/acms/trustedclients.pem
```

Copy them from the *Cloud\ACMS* folder in the APC package.

J.2.3 DASH CLI Configuration

DASH CLI uses the following certificates for authentication with ACMS:

```
%ProgramFiles(x86)%\DASH CLI 4.0\certs\consolecert.pem

%ProgramFiles(x86)%\DASH CLI 4.0\certs\acmscert.pem
```

Copy them from the *Cloud\Console* folder in the APC package.

J.2.4 AIM-T Managed System Configuration

Run the provisioning package on the system. Ensure that AIM-T provisioning package is generated with cloud option enabled.

J.3 Testing the Setup

Test the local setup without ACMS. ACMS must be first to start followed by AMI-T. On *dash-cli-win10* execute *dashcli.exe* as follows:

```
dashcli.exe -C -h aimt-host -u admin -P adminpass enumerate commputersystem
```

The output might resemble as follows:

```
Error: Connection Failed : Could not resolve host
```

The equivalent command using `-r` option is as follows:

```
dashcli.exe -r acms-host -C -h aimt-host -u admin -P adminpass enumerate computersystem
```

Observe the output, it will be identical to output displayed when connected directly:

```
Computer System Instance 0
Name                                : MS-WIN10
Element Name                        : Computer System:0
Primary Owner                       : AMD
Primary Owner Contact               : N/A
Enabled State                       : Enabled
Requested State                     : Not Applicable
Current Power State                 : On
Requested Power State               : Unknown
Power On Time                       : 2021/12/15 17:56:28
Dedicated To                        : Desktop
Supported Power Change Capabilities : Power State Settable,
                                      Power Cycling Supported,
                                      HW Reset Supported,
                                      Graceful Shutdown Supported
Supported Power States              : Sleep -Deep,
                                      Power Cycle (Off - Soft),
                                      Hibernate (Off - Soft),
                                      Off - Soft,
                                      Master Bus Reset,
                                      Off - Soft Graceful,
                                      Master Bus Reset Graceful,
                                      Power Cycle (Off - Soft Graceful)
Request Supported Power States      : Sleep -Deep,
                                      Power Cycle (Off - Soft),
                                      Hibernate (Off - Soft),
                                      Off - Soft,
                                      Master Bus Reset,
                                      Off - Soft Graceful,
                                      Master Bus Reset Graceful,
                                      Power Cycle (Off - Soft Graceful)
Available Requested Power States    : On,
                                      Off - Hard,
                                      Hibernate (Off - Soft),
                                      Off - Soft,
                                      Master Bus Reset
```

Observe the command above; the certificates and key PEM files paths were not specified. By default, DASH CLI reads the certificates and key from the *certs* folder in the installation location.

Appendix K Adding Wi-Fi Access Point Profile

An enterprise-based wireless profile can only contain credentials required for one EAP method.

Although Radius servers can support multiple EAP methods at the same time, to optimize on flash size and simplify implementations, AIM-T only supports one EAP method per profile.

However, if IT Admins want the solution to attempt multiple EAP methods, one profile must be used for each EAP method. The wireless connections on AIM-T supports only two enterprise profiles and three personal profiles.

The wireless profiles support WPA2 PSK, WPA2 Enterprise, and WPA3 SAE.

WPA PSK, WPA Enterprise, Open networks, and WPA3 OWE are not supported due to security concerns.

The wireless profiles support up to 4K certificates. 8K certificates maybe supported in the future if sufficient CPU processing capability and storage are available.

Certificates are supported in PEM format only.

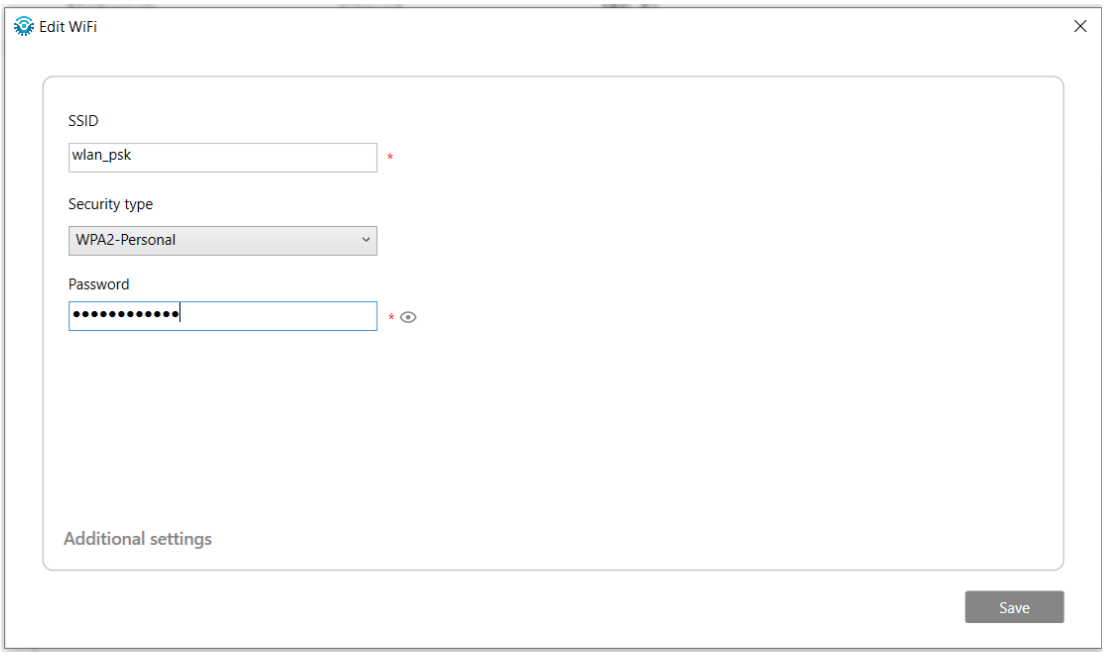
IT Admins must only use decrypted key for provisioning.

This following section provides instructions to add a Wi-fi profile to create a provisioning package.

To add a wi-fi profile:

1. On the AMD Provisioning Console, click **Network & Wi-Fi** from the left navigation pane.
2. Click the **Wi-Fi** tab and click the **Add Wi-Fi** button.
3. In the Add Wi-Fi window provide the following information:
    a. SSID: Enter the wireless network name configured in the access point.
    b. From the Security Type list, select one of four security methods:
        i. WPA2-Personal (Default)
        ii. WPA2-Enterprise
        iii. WPA3-SAE
        iv. WPA3-Enterprise

c. Enter the passphrase that is already shared with you to connect to the wireless network if you have chosen **WPA2-Personal** or **WPA3-SAE** options. Go to *step 10 – providing default port number for Secure port*.

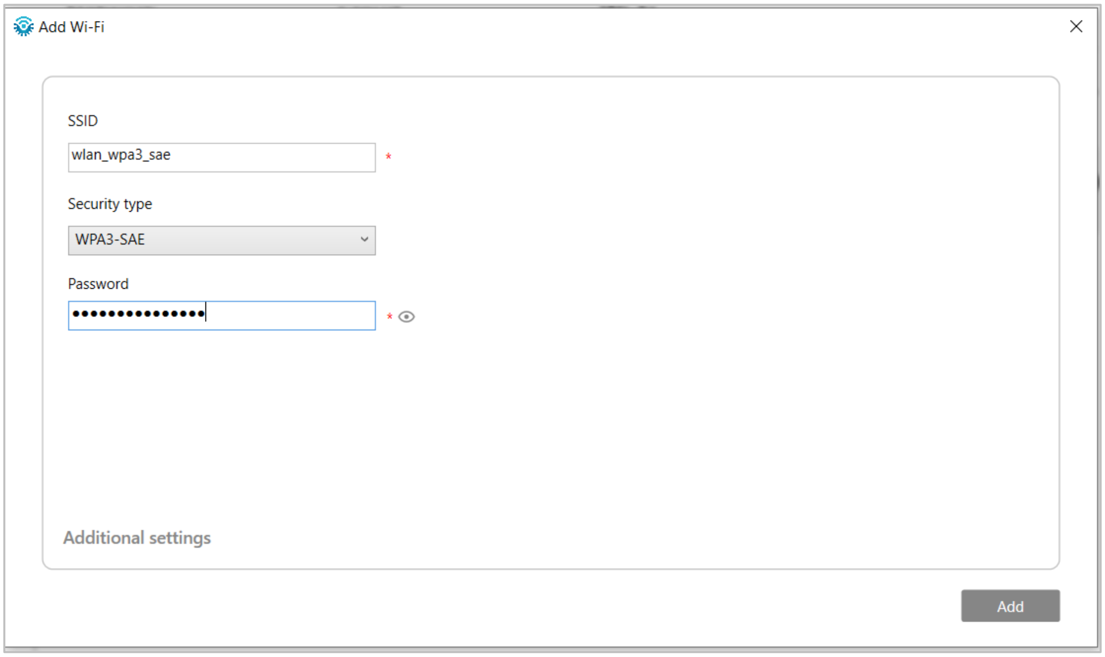

Edit WiFi

SSID: wlan_psk *

Security type: WPA2-Personal

Password: •••••••••••• *

Figure 47. WPA2-PSK Security


Add Wi-Fi

SSID: wlan_wpa3_sae *

Security type: WPA3-SAE

Password: ••••••••••••••• *

Figure 48. WPA3-SAE Security

d. If you have chosen the 8021x enterprise security options (WPA2-Enterprise or WPA3-Enterprise):

   i. Enter the **Username** and **Password**. The user identity and secret key will be used for user identification with the Radius server.

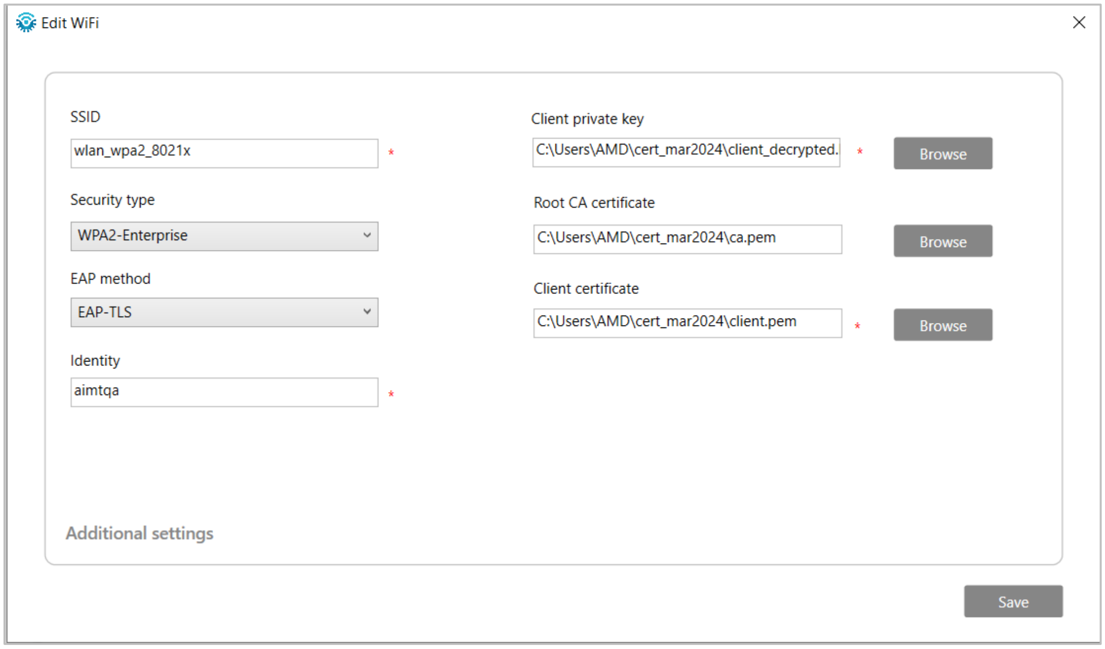
   ii. Select an EAP method to be used to authenticate with the Radius server. You have the following options to choose from:

      - TLS
      - TTLS
      - PEAP

e. Browse for and choose the Client private key. You must upload the decrypted Client private key (**client_decrypted.key**). The size of the Client private key must be less than 4K.

f. Browse for and choose the Root CA certificate (**ca.pem**). The Root CA certificate must be in the .pem format and its size must be less than 4K.

g. Browse for and choose the Client certificate (**client.pem**). The Client certificate must be in the .pem format and its size must be less than 4K.



Edit WiFi

SSID: wlan_wpa2_8021x *

Security type: WPA2-Enterprise

EAP method: EAP-TLS

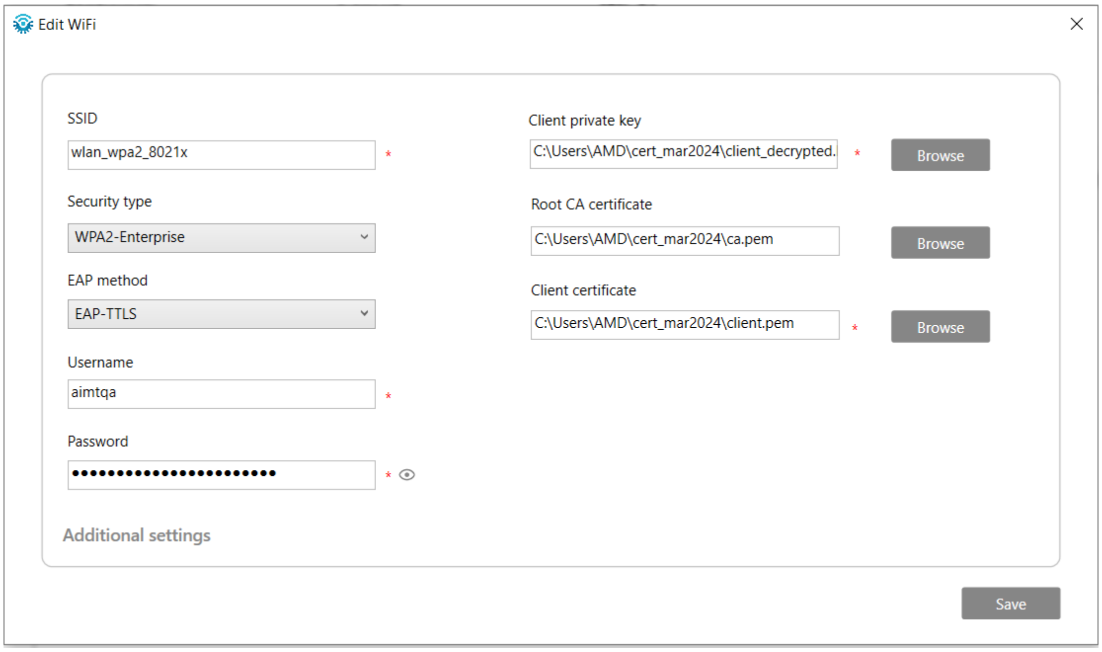
Identity: aimtqa *

Client private key: C:\Users\AMD\cert_mar2024\client_decrypted. *

Root CA certificate: C:\Users\AMD\cert_mar2024\ca.pem

Client certificate: C:\Users\AMD\cert_mar2024\client.pem *

Figure 49. WPA2 Enterprise security: EAP TLS



Edit WiFi

SSID: wlan_wpa2_8021x *

Security type: WPA2-Enterprise

EAP method: EAP-TTLS

Username: aimtqa *

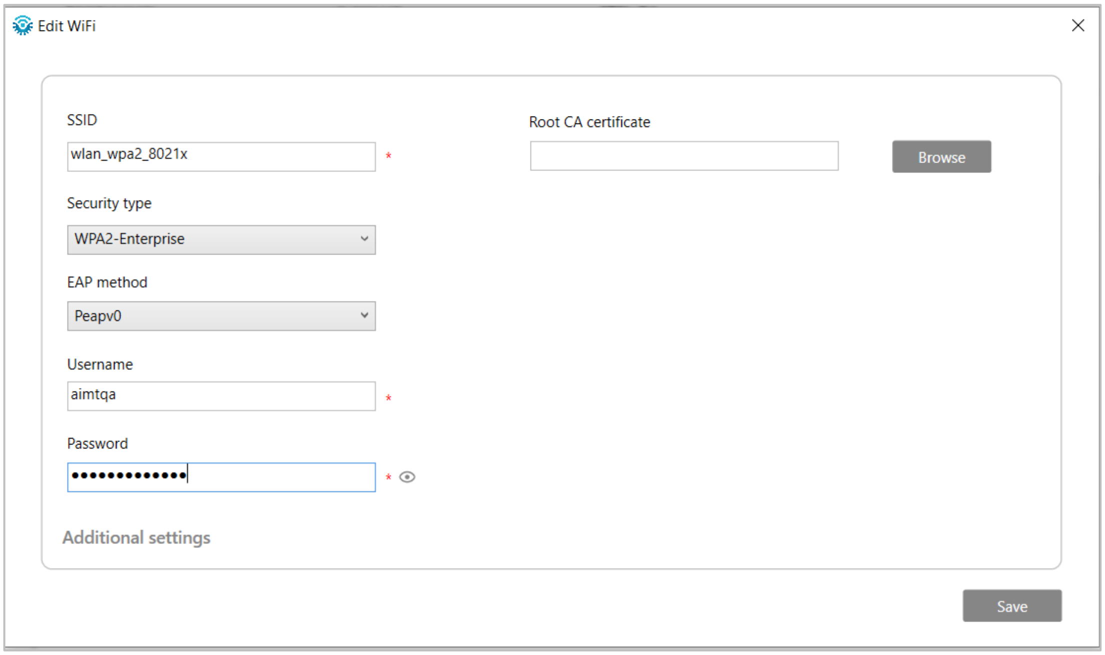
Password: •••••••••••••••••••••• *

Client private key: C:\Users\AMD\cert_mar2024\client_decrypted. *

Root CA certificate: C:\Users\AMD\cert_mar2024\ca.pem

Client certificate: C:\Users\AMD\cert_mar2024\client.pem *

Figure 50. WPA2 Enterprise security: EAP TTLS



Edit WiFi

SSID: wlan_wpa2_8021x *

Security type: WPA2-Enterprise

EAP method: Peapv0

Username: aimtqa *

Password: ••••••••••••• *

Root CA certificate:

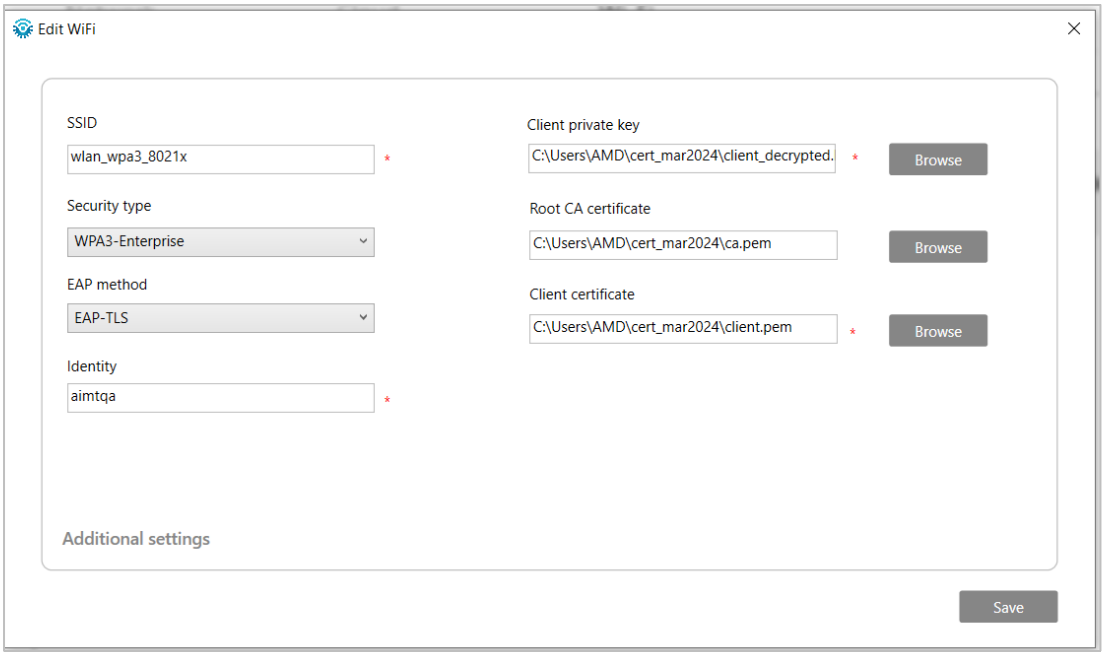
Figure 51. WPA2 Enterprise security: EAP PEAP

h. Go to *step 10 – providing default port number for Secure port*.

i. If you have chosen the WPA3-Enterprise option, select the:

   i. **Pairwise** and **Groupwise** options as **GCMP_256** for connecting to access point configured with WPA3 enterprise security (GCMP).

ii. **Pairwise** and **Groupwise** options as **GCMP_CCMP** for connecting to access point configured with WPA3 enterprise security (CCMP).



Edit WiFi

SSID: wlan_wpa3_8021x *

Security type: WPA3-Enterprise

EAP method: EAP-TLS

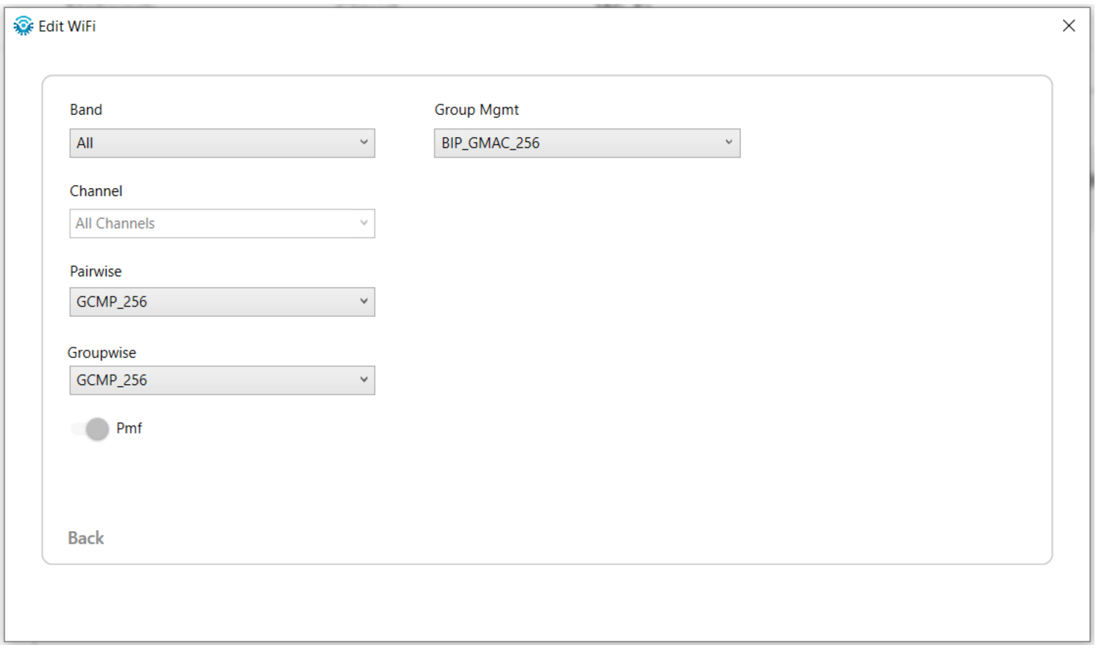
Identity: aimtqa *

Client private key: C:\Users\AMD\cert_mar2024\client_decrypted. *

Root CA certificate: C:\Users\AMD\cert_mar2024\ca.pem

Client certificate: C:\Users\AMD\cert_mar2024\client.pem *

Figure 52. WPA3 Enterprise security: EAP TLS



Edit WiFi

Band: All

Channel: All Channels

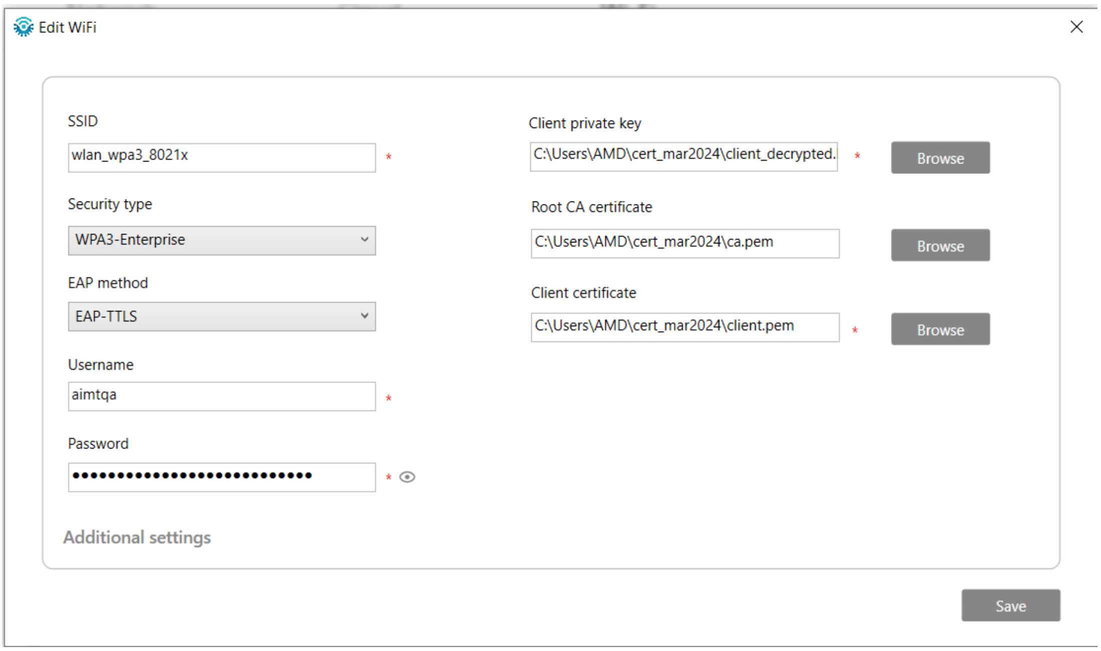
Pairwise: GCMP_256

Groupwise: GCMP_256

Pmf

Group Mgmt: BIP_GMAC_256

Figure 53. WPA3 Enterprise security: EAP TLS Additional Settings


Edit WiFi

SSID: wlan_wpa3_8021x *

Security type: WPA3-Enterprise

EAP method: EAP-TTLS

Username: aimtqa *

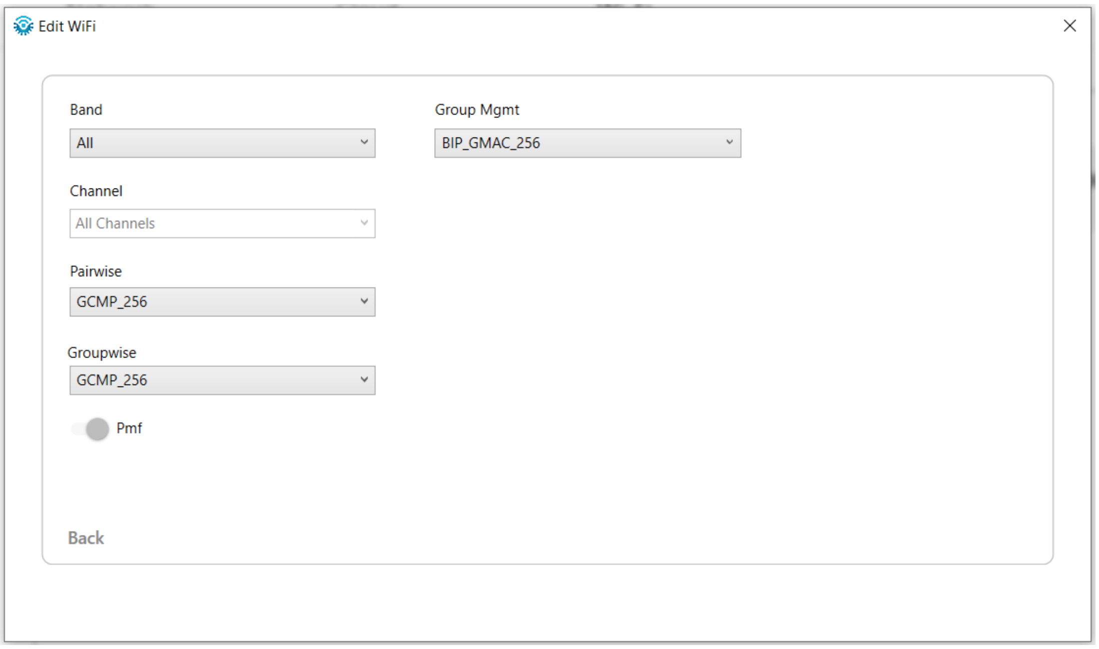
Password: •••••••••••••••••••••••••••• *

Client private key: C:\Users\AMD\cert_mar2024\client_decrypted. *

Root CA certificate: C:\Users\AMD\cert_mar2024\ca.pem

Client certificate: C:\Users\AMD\cert_mar2024\client.pem *

Figure 54. WPA3 Enterprise security: EAP TTLS


Edit WiFi

Band: All

Channel: All Channels

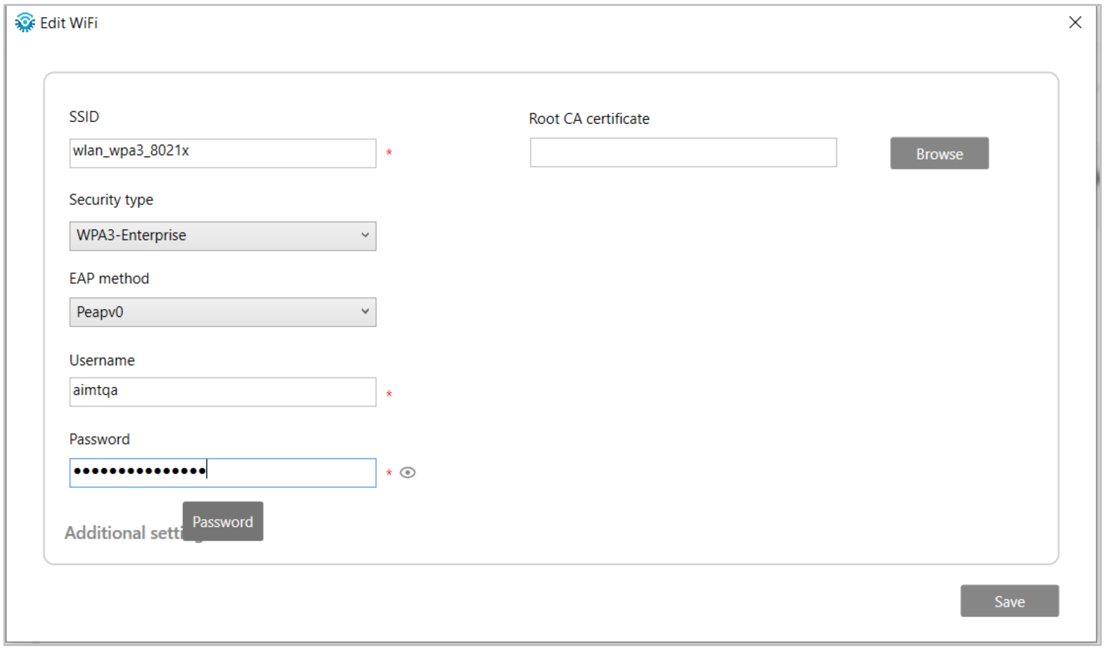
Pairwise: GCMP_256

Groupwise: GCMP_256

Pmf

Group Mgmt: BIP_GMAC_256

Figure 55. WPA3 Enterprise security: EAP TTLS Additional Settings



SSID: wlan_wpa3_8021x *

Root CA certificate:

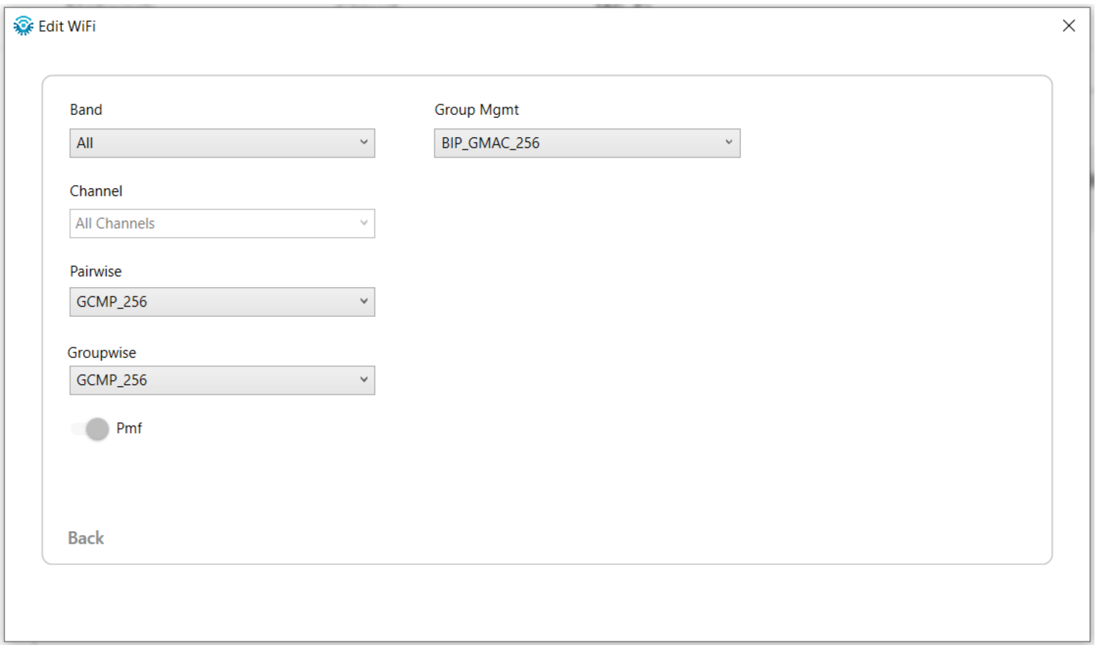
Security type: WPA3-Enterprise

EAP method: Peapv0

Username: aimtqa *

Password: ••••••••••••••• *

Figure 56. WPA3 Enterprise security: EAP PEAP Settings



Band: All

Group Mgmt: BIP_GMAC_256

Channel: All Channels

Pairwise: GCMP_256

Groupwise: GCMP_256

○ Pmf

Figure 57. WPA3 Enterprise security: EAP PEAP Additional Settings

j. Go to *step 10 – providing default port number for Secure port*.

K.1 Radius Server and Certificates

This section explains how to bring up FreeRadius server and generate server and client certificates.

K.1.1 Bring up FreeRadius Server

To bring up FreeRadius Server.

1. Bring up the Linux server with Ubuntu OS installed.
2. Install FreeRadius Server using the following commands.

```
apt update

apt-get install freeradius
```

K.1.2 Generate Certificates

Use the following openssl commands to generate server and client certificates:

# Generate self-signed root CA cert

```
openssl req -nodes -x509 -newkey rsa:4096 -keyout ca.key -out ca.crt -subj
"/C=IN/ST=KAR/L=BNLR/O=test/CN=`hostname -f`/emailAddress=test-root@test.com" -days
365
```

# Generate server cert to be signed

```
openssl req -nodes -newkey rsa:4096 -keyout server.key -out server.csr -subj
"/C=IN/ST=KAR/L=BNLR/O=test/CN=`hostname -f`/emailAddress=test-server@test.com" -days
365
```

# Sign the server cert

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out
server.crt
```

# Create server PEM file

```
cat server.crt > server.pem

openssl rsa -in server.key   -out  server_decrypted.key
```

# Generate client cert to be signed

```
openssl req -nodes -newkey rsa:4096 -keyout client.key -out client.csr -subj
"/C=IN/ST=KAR/L=BNLR/O=test/CN=`hostname -f`/emailAddress=test-client@test.com" -days
365
```

# Sign the client cert

```
openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -CAserial ca.srl -out
client.crt
```

# Create client PEM file

```
cat client.crt > client.pem

openssl rsa -in client.key   -out  client_decrypted.key

openssl x509 -in ca.crt -out ca.pem
```

K.1.3 Copy Server Certificates

Copy the server certificates to the FreeRadius Server certs path as mentioned here:

```
cp ca.pem /etc/freeradius/3.0/certs/ca.pem

cp server.pem /etc/freeradius/3.0/certs/server.pem

cp server_decrypted.key /etc/freeradius/3.0/certs/server_decrypted.key
```

K.1.4 Start FreeRadius Server

To start the FreeRadius Server on the Linux terminal, use the following command:

```
freeradius -XX // for debugging purpose.
```

OR

```
Service freeradius start
```

Upload the Client private key, CA certificates and Client certificates in the AMD Provisioning Console while *creating the Wi-Fi access point*.