



AIM-T User Guide - Windows

Publication #	57880	Revision:	4.5
Issue Date:	October 2024		

© 2024 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.

Broadcom is a registered trademark of Broadcom Corporation.

Linux is a registered trademark of Linus Torvalds.

Marvell is a registered trademark of Marvell Technology Group Ltd.

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

Contents	3
List of Figures.....	6
List of Tables	8
Revision History	9
Acronyms and Abbreviations	10
Chapter 1 Introduction.....	11
Chapter 2 AIM-T Capabilities and Features.....	12
2.1 Supported DASH Profiles.....	12
2.2 Custom Profile and Features.....	13
2.2.1 Mutual Authentication (MA)	13
2.2.2 KVM Consent	14
2.2.3 Active Directory (AD) Based Authentication.....	14
2.2.4 Web User Interface	14
2.2.5 Cloud Manageability.....	15
2.2.6 Wi-Fi Sync and Office/Home Network Detection.....	15
Chapter 3 Enabling AIM-T on Wireless and Wired Systems.....	16
3.1 Prerequisites.....	16
3.2 BIOS Menu Settings	17
3.3 Provisioning Console for Wireless AIM-T.....	18
3.3.1 Provisioning	19
3.3.2 Re-Provisioning	19
3.3.3 Un-Provisioning.....	19
3.4 DASHCLI	19
3.5 AIM-T Manageability Service (AMS)	21
3.5.1 Wake from Sleep.....	23
3.6 Realtek Ethernet Controller All-in-One Windows Driver	23
Chapter 4 User Scenario.....	25
4.1 AIM-T in OS.....	25
4.1.1 Prerequisites	25
4.1.2 Expected Behavior	25

4.1.3	Graceful Shutdown.....	25
4.2	AIM-T in Shutdown Mode.....	25
4.2.1	Prerequisites	25
4.2.2	Expected Behavior	26
4.2.3	Pressing Power Button	26
4.2.4	Detaching Power Adaptor	26
Chapter 5	Troubleshooting.....	27
5.1	On AIM-T DASH System.....	27
5.1.1	AMS Status is Off	27
5.1.2	Red AMS UI Tray	27
5.2	On Console (DASH CLI) System	28
5.2.1	KVM Command Response.....	28
5.2.2	Unresponsive AIM-T System.....	29
5.2.3	Distorted Display or Black Screen While Connecting KVM.....	30
Appendix A	Configuring Provisioning Data	32
Appendix B	Re-Provisioning	40
Appendix C	Un-Provisioning	42
Appendix D	Supported DASH Commands	43
Appendix E	Using KVM	45
Appendix F	Flashing RTK NIC Firmware	47
Appendix G	Supported Wired DASH Profiles.....	48
Appendix H	Supported DASH Profiles in AIM-T	49
Appendix I	Updating BIOS Capsule.....	53
I.1	Setting up a Download Server.....	53
I.2	Preparing a Valid Capsule.....	54
I.3	Reforming the Capsule.....	55
I.4	DASH Command for Capsule Update	55
Appendix J	AMD Cloud Manageability Service.....	56
J.1	Requirements.....	56
J.2	Installation and Setup	56
J.2.1	Installation	58
J.2.2	Configuration	59

J.2.3 DASH CLI Configuration.....59

J.2.4 AIM-T Managed System Configuration.....59

J.3 Testing the Setup59

Appendix K Adding Wi-Fi Access Point Profile.....61

K.1 Radius Server and Certificates.....68

K.1.1 Bring up FreeRadius Server.....68

K.1.2 Generate Certificates.....68

K.1.3 Copy Server Certificates69

K.1.4 Start FreeRadius Server69

List of Figures

Figure 1. AIM-T Options	18
Figure 2. AIM-T Advanced Options	18
Figure 3. DASHCLI	21
Figure 4. Installing AMS	21
Figure 5. AMS Icon	22
Figure 6. AIM-T Status	22
Figure 7. Realtek UI	23
Figure 8. DASH Client	24
Figure 9. AIM-T System Processor Info	24
Figure 10. AMS Status is Off	27
Figure 11. AMS UI Tray Issues	28
Figure 12. Start AMS Service	28
Figure 13. DASH CLI – KVM Output	29
Figure 14. Unresponsive AIM-T System	29
Figure 15. Responsive AIM-T system	30
Figure 16. Distorted Display or Black Screen While Connecting KVM	30
Figure 17. Profile Location	32
Figure 18. Contact Information	33
Figure 19. Crypto store	33
Figure 20. Adding Users	34
Figure 21. Adding Wi-Fi Access Point	34
Figure 22. Secure Port	35
Figure 23. TLS Certificate	35
Figure 24. KVM Key	36
Figure 25. DASH Profiles	37
Figure 26. Alerts	37
Figure 27. Summary	38
Figure 28. Result	38
Figure 29. Provisioning Command	39
Figure 30. Select Crypto Key	40

Figure 31. Copy Crypto Key	41
Figure 32. Re-provisioning Command	41
Figure 33. AMD KVM Viewer.....	46
Figure 34. Firmware Flash Status	47
Figure 35. AMC - Port Selection	54
Figure 36. Testing AMC	54
Figure 37. Valid Capsule	55
Figure 38. Capsule Update.....	55
Figure 39. APC PageThe generated files are present at the following path:	57
Figure 40. WPA2-PSK Security	62
Figure 41. WPA3-SAE Security	62
Figure 42. WPA2 Enterprise security: EAP TLS	63
Figure 43. WPA2 Enterprise security: EAP TTLS	64
Figure 44. WPA2 Enterprise security: EAP PEAP	64
Figure 45. WPA3 Enterprise security: EAP TLS	65
Figure 46. WPA3 Enterprise security: EAP TLS Additional Settings	65
Figure 47. WPA3 Enterprise security: EAP TTLS	66
Figure 48. WPA3 Enterprise security: EAP TTLS Additional Settings	66
Figure 49. WPA3 Enterprise security: EAP PEAP Settings.....	67
Figure 50. WPA3 Enterprise security: EAP PEAP Additional Settings.....	67

List of Tables

Table 1. Acronyms and Abbreviations.....	10
Table 2. List of Supported Profiles	12
Table 3. Software Requirement for Wireless AIM-T	16
Table 4. Software Requirement for Wired DASH	17
Table 5. Common DASH Commands	43
Table 6. Supported Wired DASH Profiles	48

Revision History

Date	Revision	Description
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	<ul style="list-style-type: none">• 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

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™ 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-T1.0	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-T2.0	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-T3.0	DSP1015	Power Supply Profile
35	AIM-T4.0	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-T4.5	DSP1070	Opaque Management Data Profile
		Custom Feature	Web UI for MPM
		Custom Feature	Disk Profile (Disk Info)
		Custom Feature	Active Directory based authentication

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: *KVM consent feature must be enabled in the provisioning package (with APC tool). If not enabled, consent is deemed to be given. Active Directory (AD) based authentication.*

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.*

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`

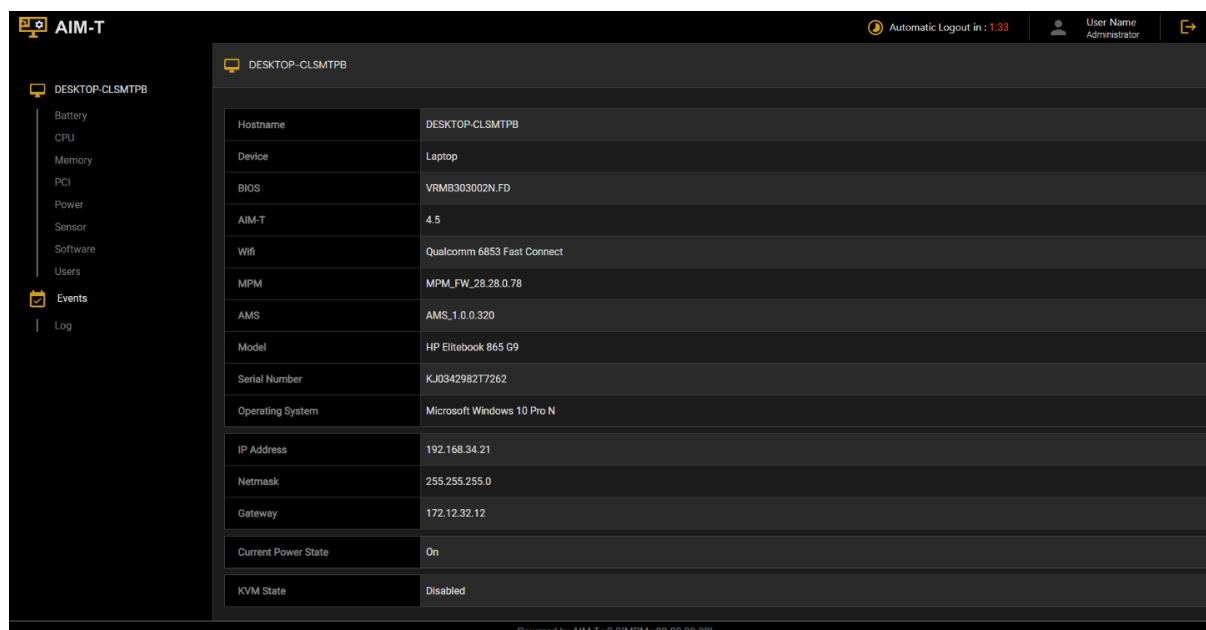


Figure 1. AIM-T WebUI Landing Page

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.

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.

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.

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/MT 7922 and RZ717/MT 7925.
- Wired Network: Realtek, RTK8111EPP, RTK8111EPV, RTL8111FP, RTL8125AP, RTL8125BP

Note: WLAN Adapter Drivers should be enabled for AMS service to start.

Table 3. Software Requirement for Wireless AIM-T

Application	Min. Version	Description
DASHCLI	5.0	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)	2.0	A windows application, 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 APC guide for detailed information. Add appendix section A
AMS	4.0	A windows application running as a service on client systems. By default, this is pre-installed by OEMs on client systems before shipment. If not installed by default, It can also be downloaded from Microsoft Store (). and the complete AMS package is available under downloads section of the AMD portal (w.amd.com/DASH). For detailed instructions refer APC guide

Table 4. Software Requirement for Wired DASH

In Addition to above:

Application	Min. Version	Description
Realtek Ethernet Controller All-In-One Windows Driver	1.0.11.1	You should install in 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.

3.2 BIOS Menu Settings

To enable AIM-T on intended systems, we have to select and enable appropriate options in 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:

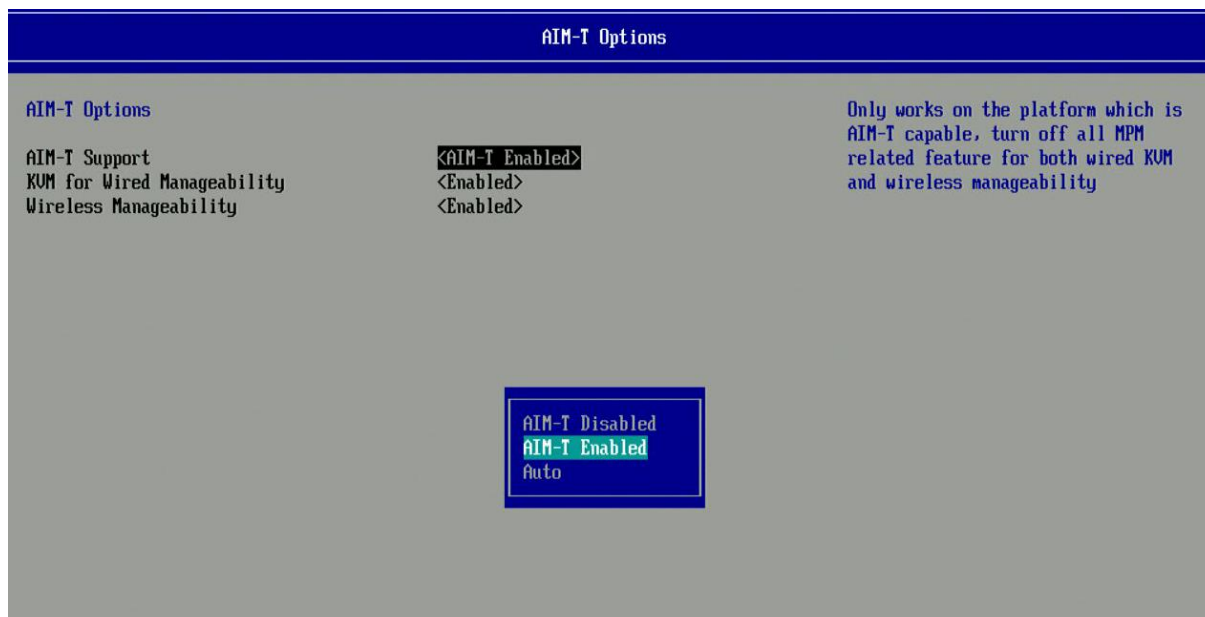


Figure 1. AIM-T Options



Figure 2. 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.

3.3 Provisioning Console for Wireless AIM-T

Download link: <https://developer.amd.com/tools-for-dmtf-dash/>

- AMD Provisioning Console (on the website)
- `AMD_DASH_CLI_Setup_x.y.z.www` (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 match 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. User must redo the provisioning to make DASH functional again.

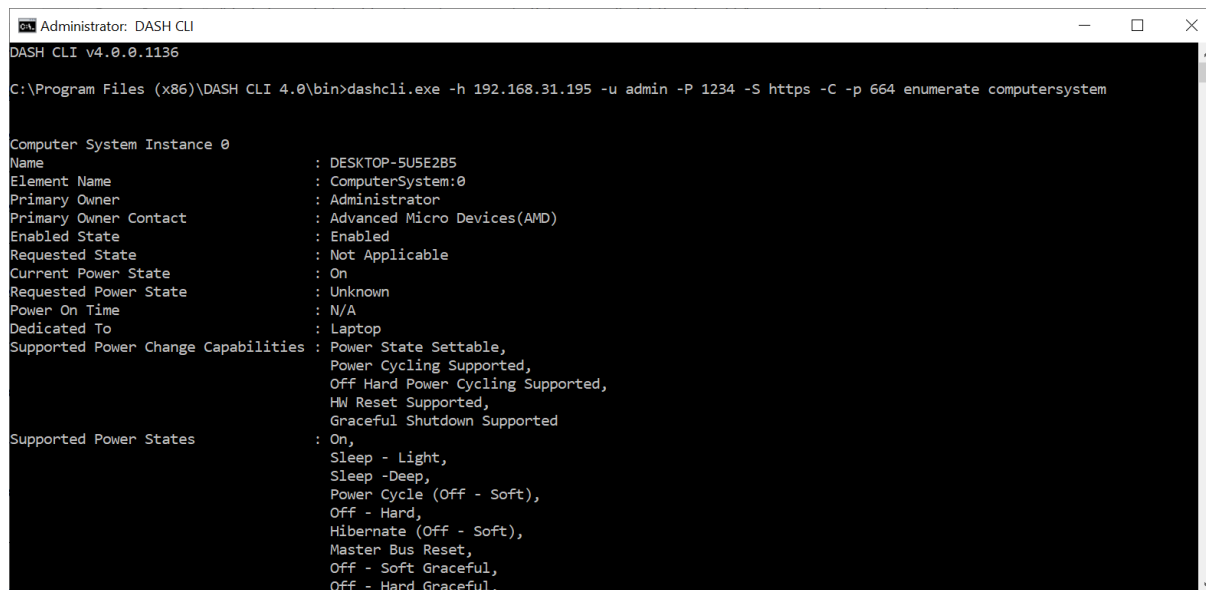
3.4 DASHCLI

Download link: <https://developer.amd.com/tools-for-dmtf-dash/>

DASHCLI is a command line tool running on host (IT's system) for sending DASH commands to client (AIM-T system). For security purpose, most of the DASH commands require username/password OR MA based 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:



```
Administrator: DASH CLI
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 3. DASHCLI

For more DASH commands, see Appendix F.

3.5 AIM-T Manageability Service (AMS)

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>):

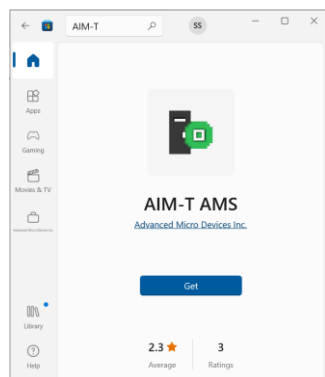


Figure 4. Installing AMS

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:

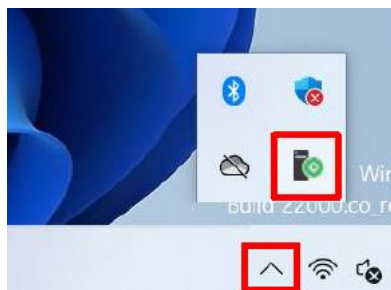


Figure 5. AMS Icon

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:

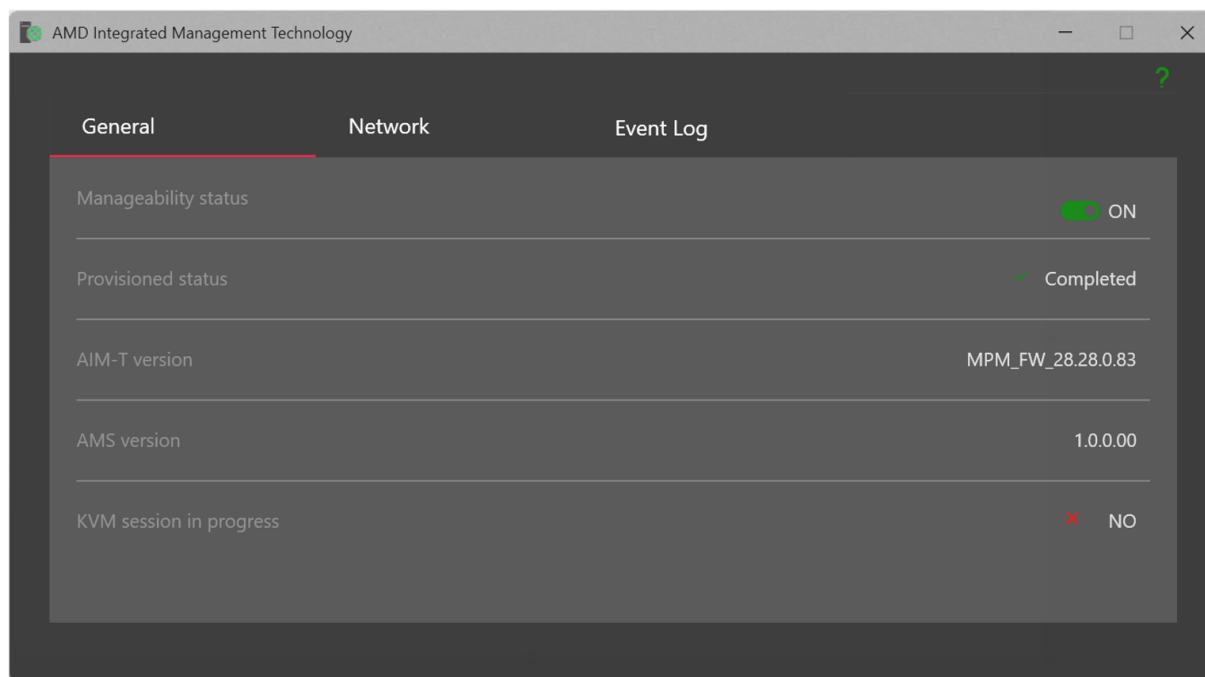


Figure 6. AIM-T Status

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 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: In AIM-T 4.0, 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.

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:

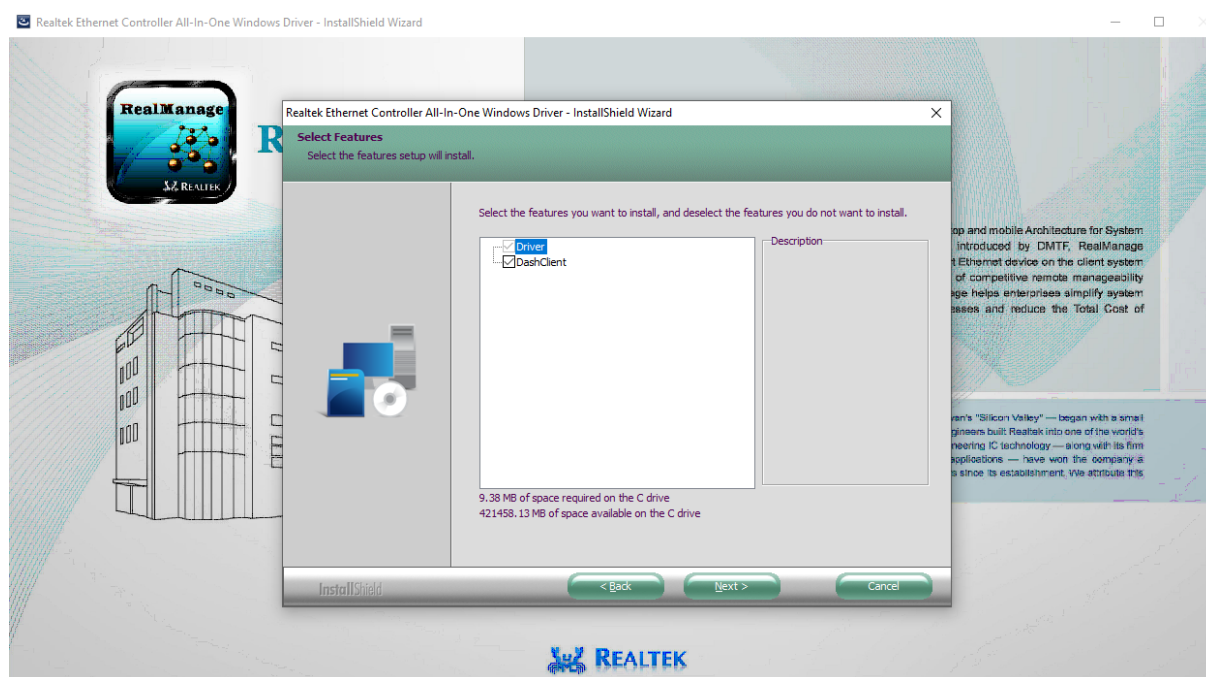


Figure 7. Realtek UI

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 8. 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:

```
Administrator: Command Prompt
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 9. 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.

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

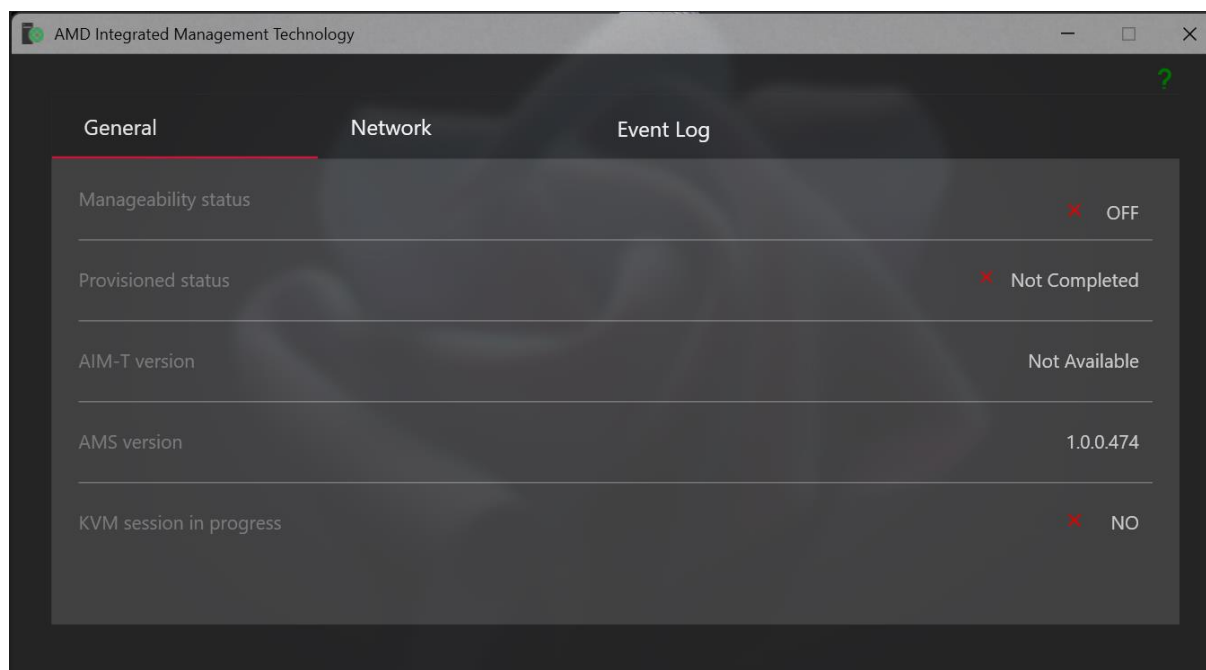


Figure 10. AMS Status is Off

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:

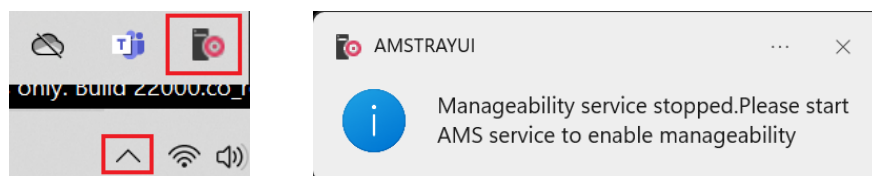


Figure 11. AMS UI Tray Issues

You can re-launch AMS to recover it.

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

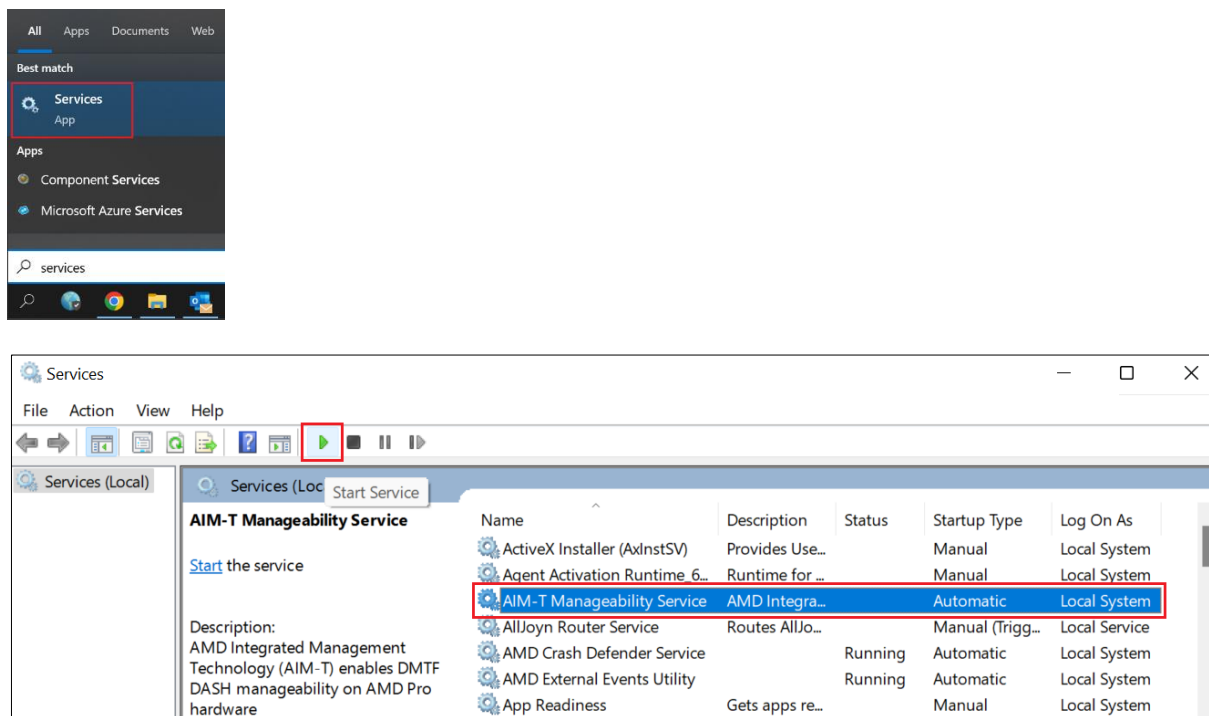


Figure 12. Start AMS Service

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

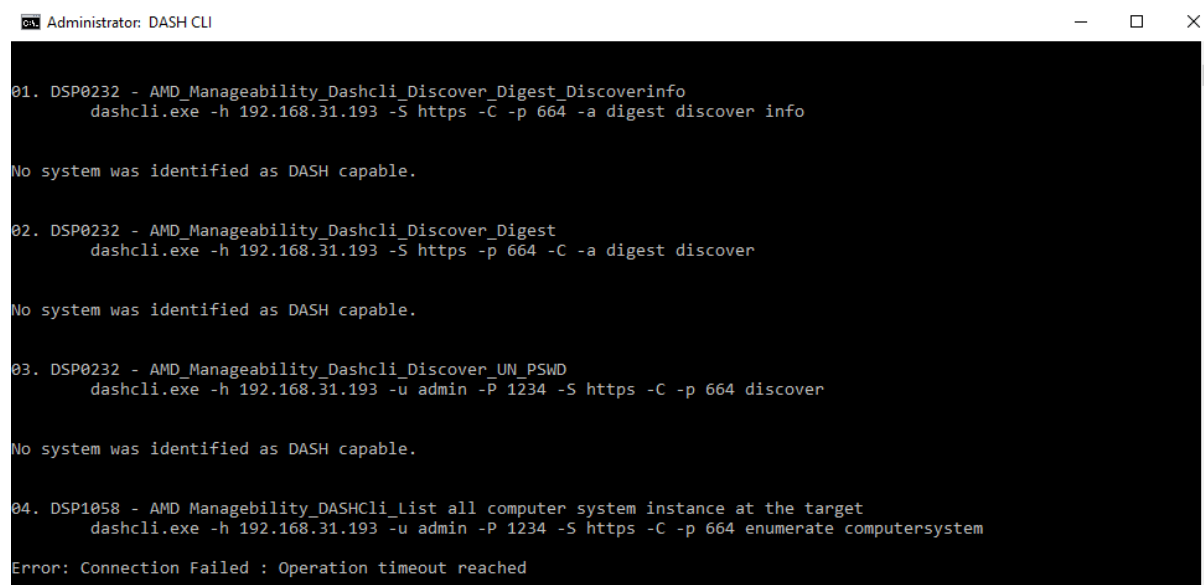
The folder *certs* is set as an administrator folder which may be controlled by an enterprise IT policy.

```
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 13. DASH CLI – KVM Output

5.2.2 Unresponsive AIM-T System



```
Administrator: DASH CLI

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

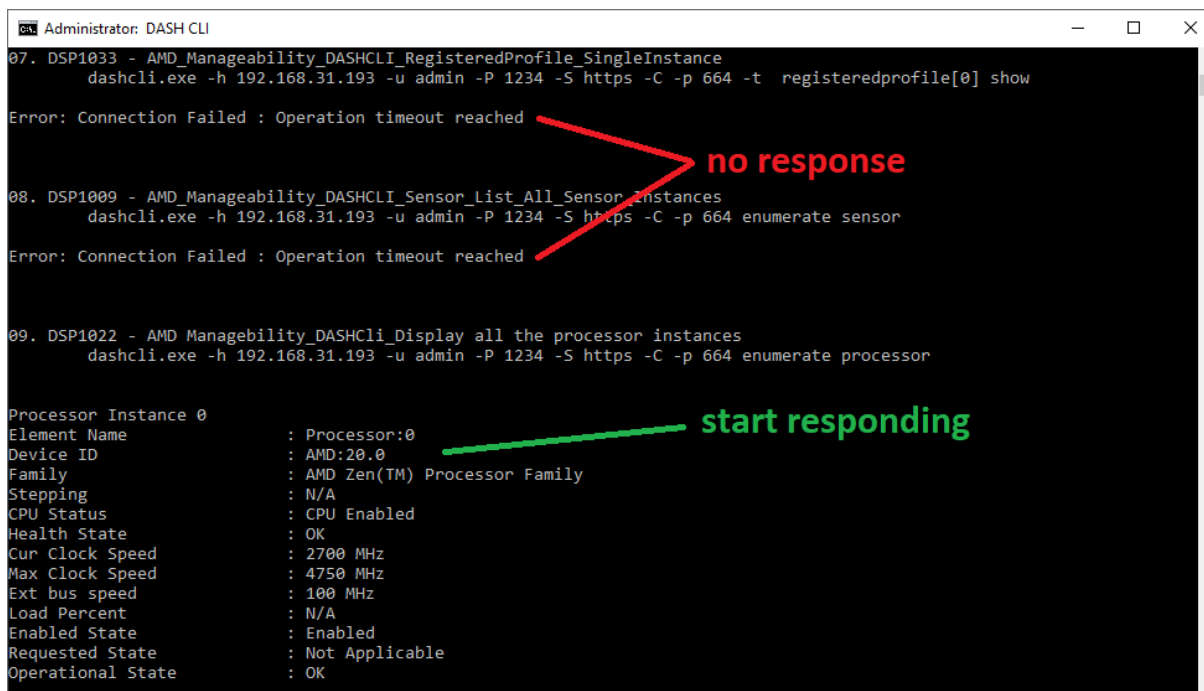
No system was identified as DASH capable.

04. DSP1058 - AMD_Manageability_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 14. 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.



```
Administrator: DASH CLI
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_Manageability_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 15. 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

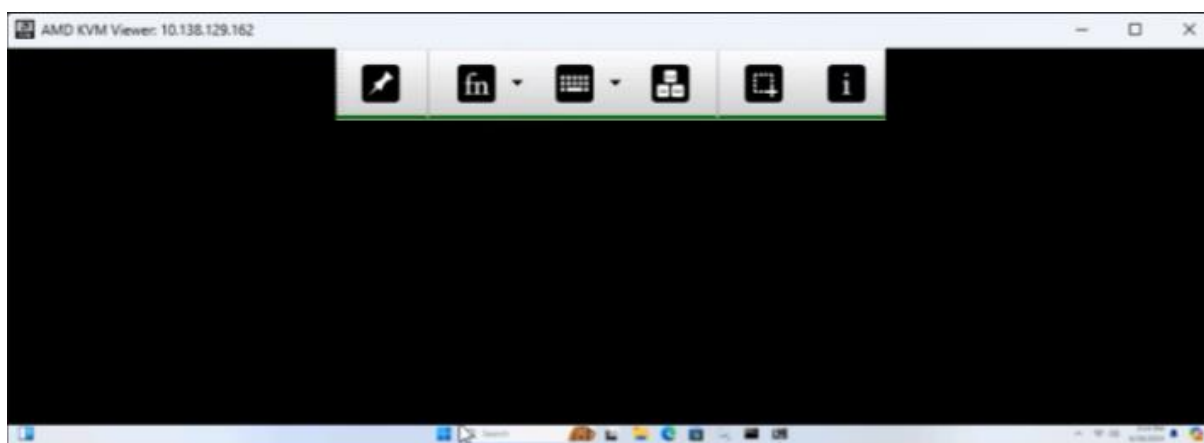


Figure 16. Distorted Display or Black Screen While Connecting KVM

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:

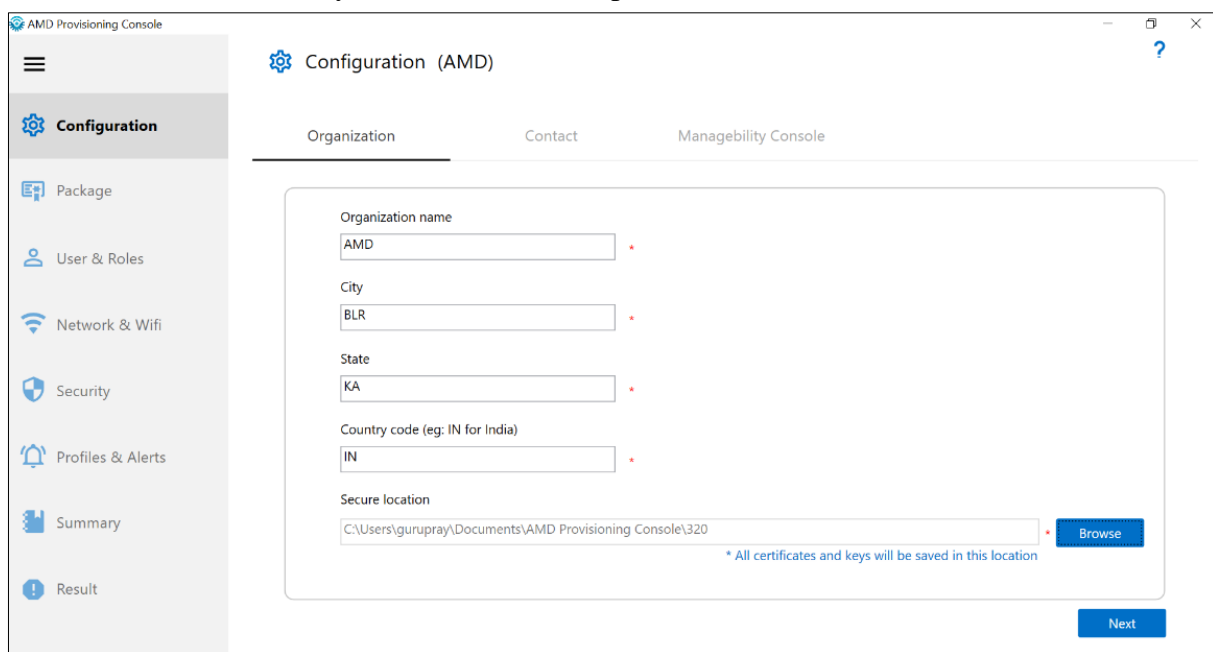
```
dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t  
computersystem[0] power cycle
```

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.

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-1.0.0.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:



The screenshot shows the AMD Provisioning Console Configuration window. The left sidebar contains a menu with the following items: Configuration (selected), Package, User & Roles, Network & Wifi, Security, Profiles & Alerts, Summary, and Result. The main area is titled 'Configuration (AMD)' and has three tabs: Organization (selected), Contact, and Manageability Console. The Organization tab contains the following fields:

- Organization name: AMD
- City: BLR
- State: KA
- Country code (eg: IN for India): IN
- Secure location: C:\Users\gurupray\Documents\AMD Provisioning Console\320

Each field has a red asterisk indicating it is required. A 'Browse' button is next to the Secure location field. A note below the Secure location field states: '* All certificates and keys will be saved in this location'. A 'Next' button is at the bottom right of the main area.

Figure 17. Profile Location

5. Fill in the contact information:

AMD Provisioning Console

Configuration (AMD)

Organization Contact Manageability Console

Name
Guru

Contact number
9123456789

Email
guru@amd.com

Next

Figure 18. 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:

AMD Provisioning Console

Package

Package

Package name
Package_01

Crypto store
AIM-T-CRYPTO

Select a Crypto from store
AIM-T-CRYPTO
Add new Crypto to store

Back Next

Figure 19. Crypto store

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

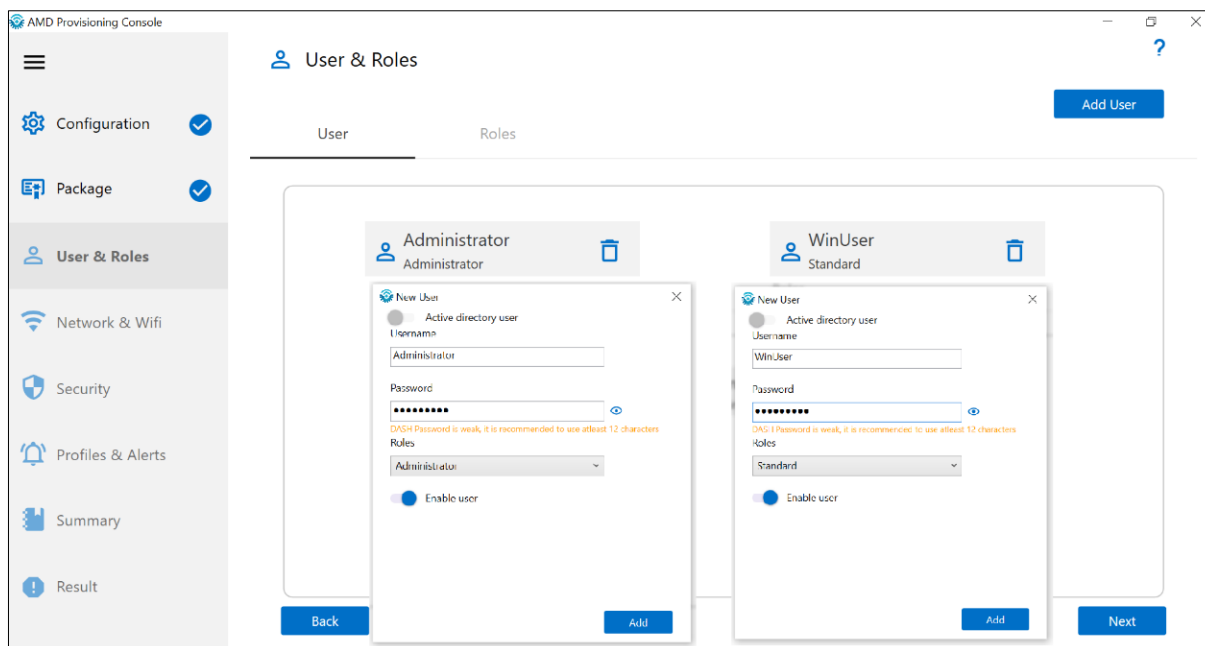


Figure 20. Adding Users

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.

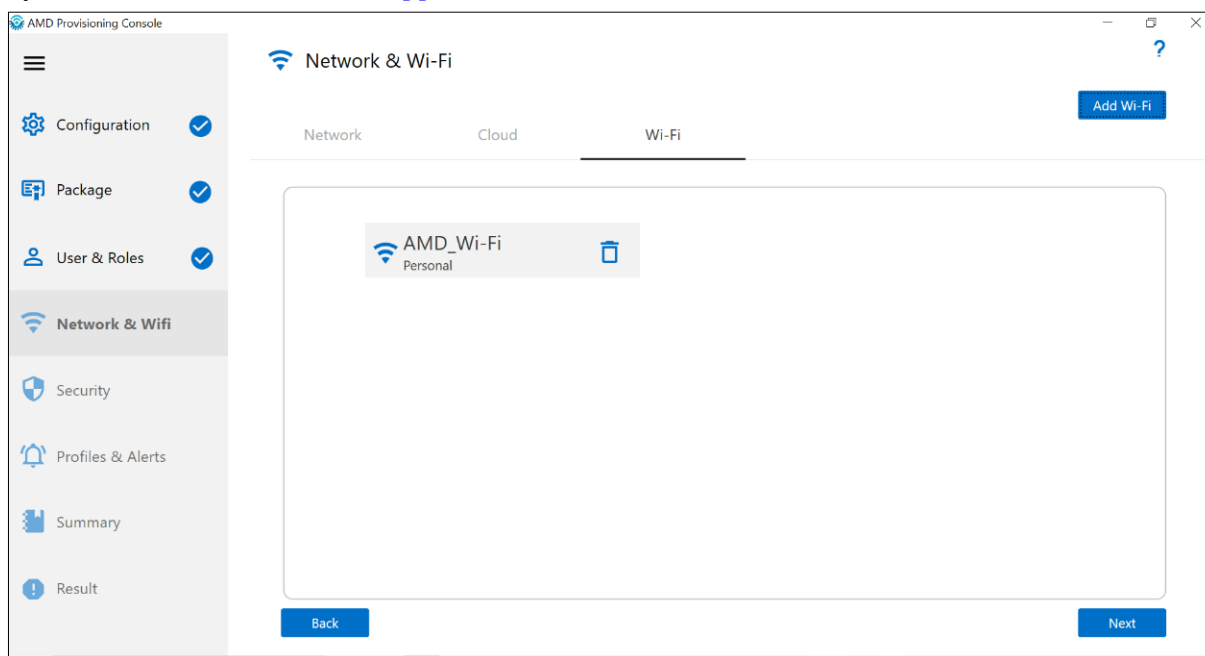
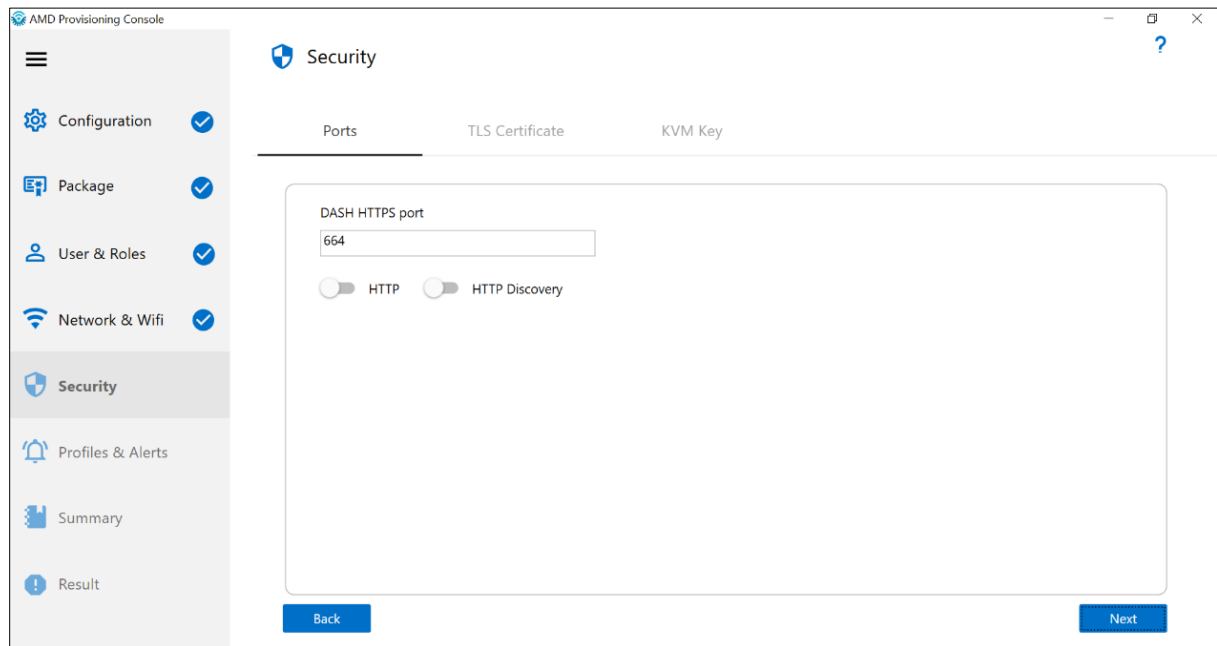
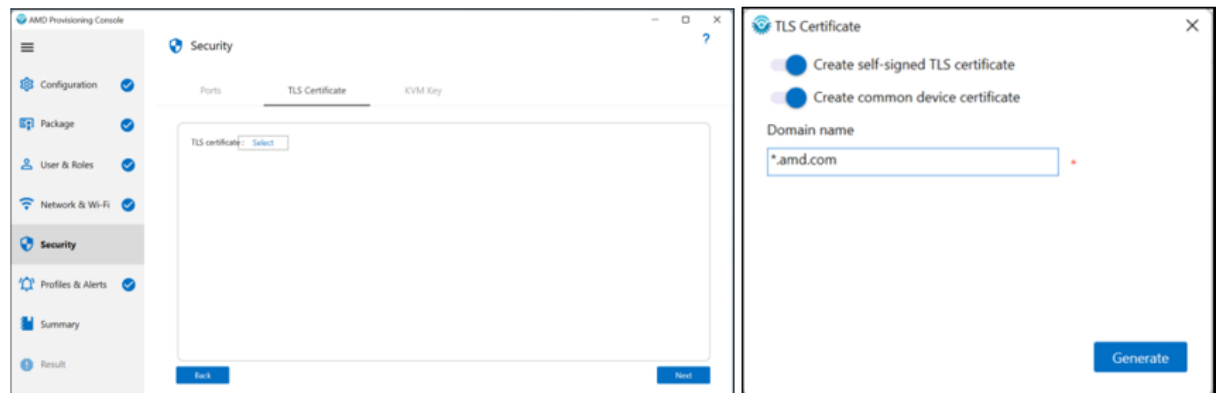


Figure 21. Adding Wi-Fi Access Point

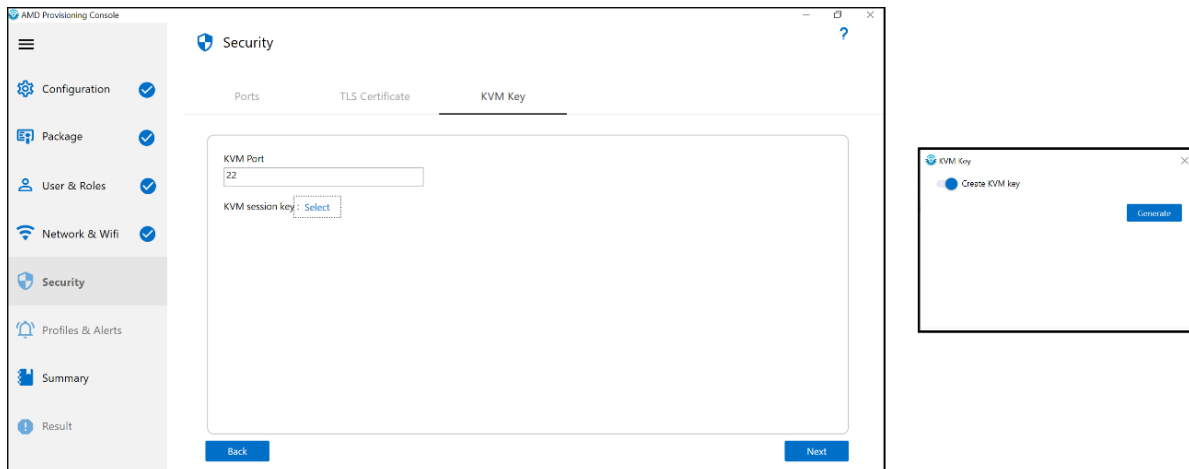
10. Use the default port number (664) for **Secure port**:

**Figure 22. Secure Port**

11. Generate a TLS certificate:

**Figure 23. TLS Certificate**

12. Generate a KVM key:

**Figure 24. KVM Key**

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

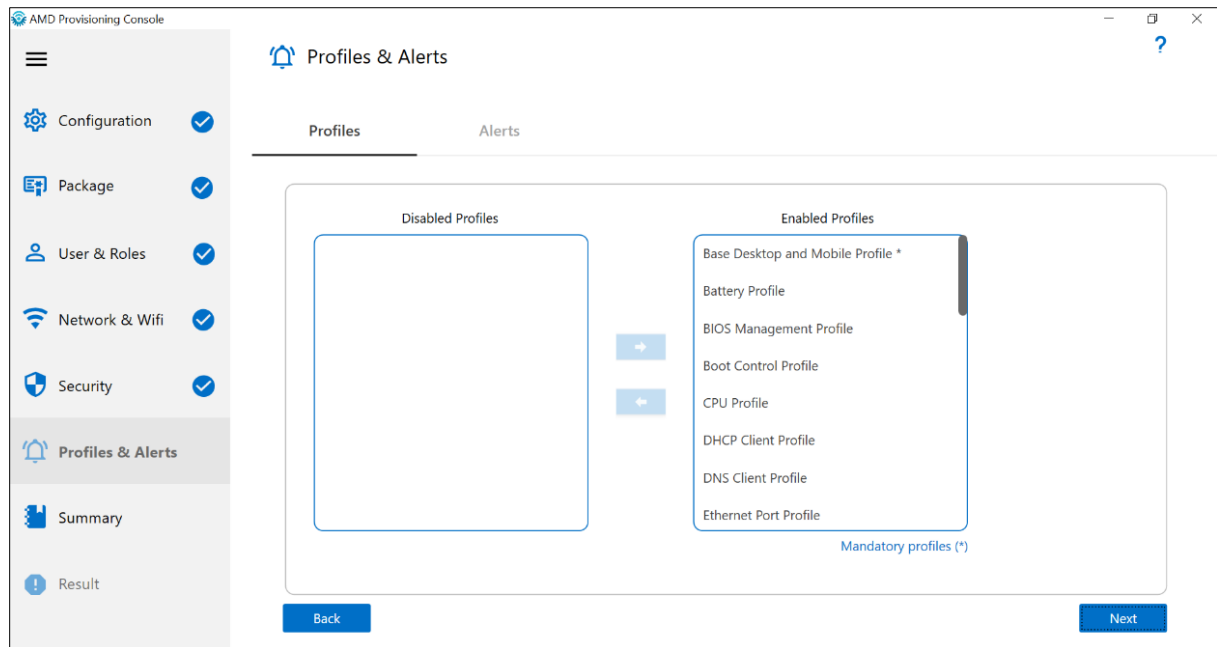


Figure 25. DASH Profiles

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

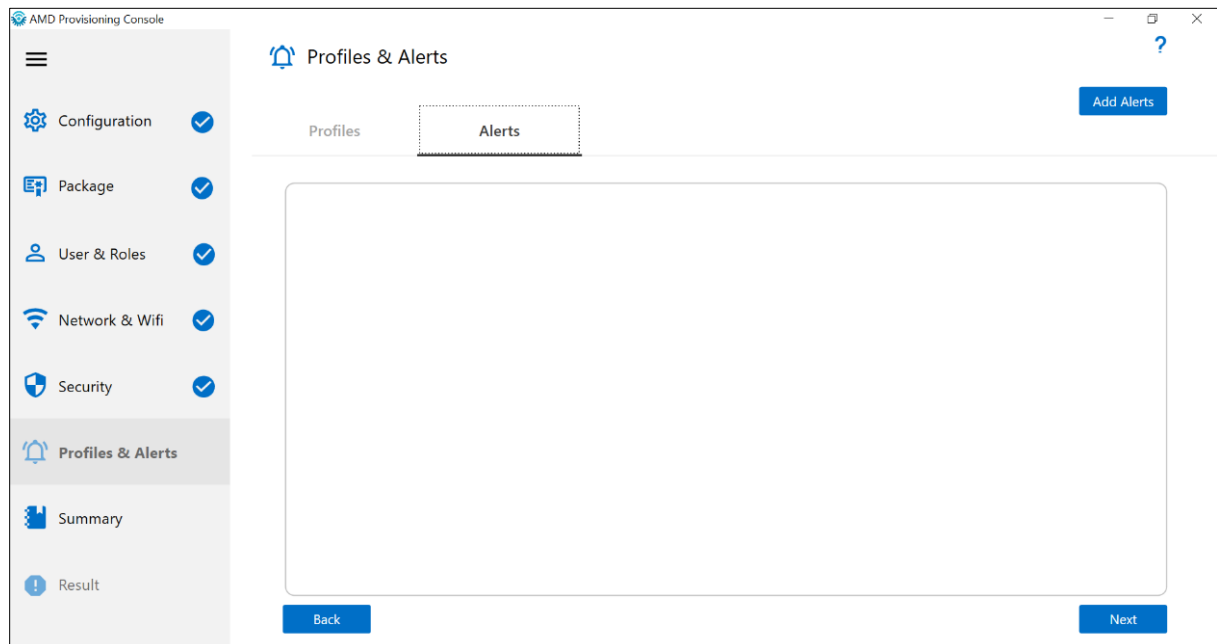


Figure 26. Alerts

15. Click the **Submit** button:

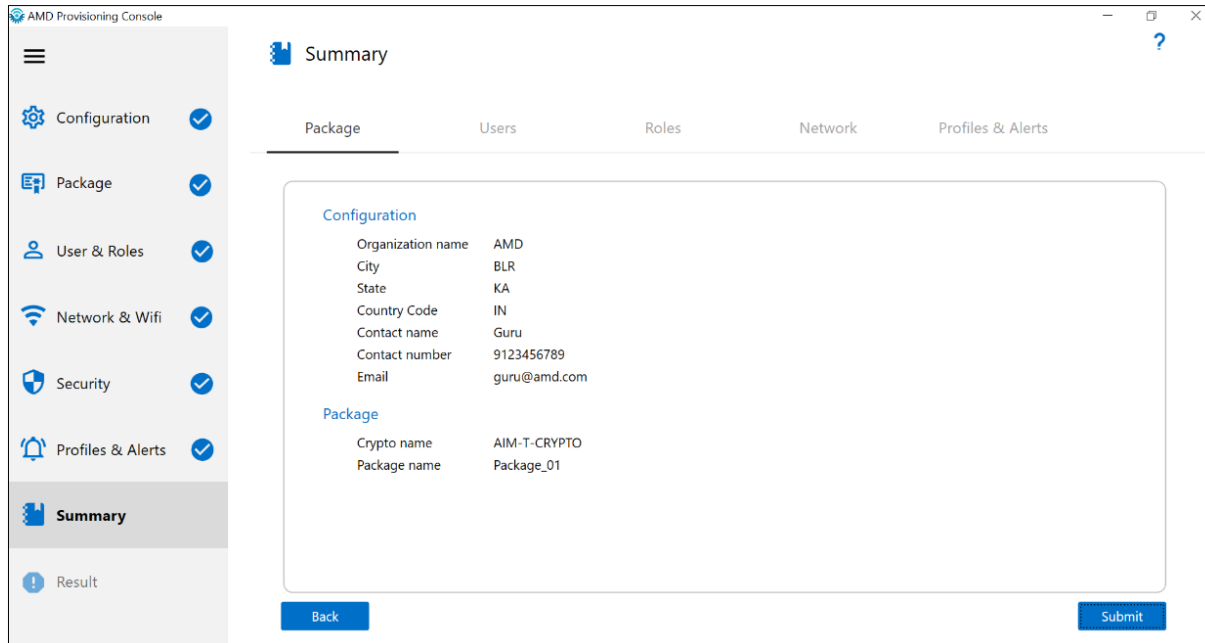


Figure 27. Summary

The *Result* pane is displayed:

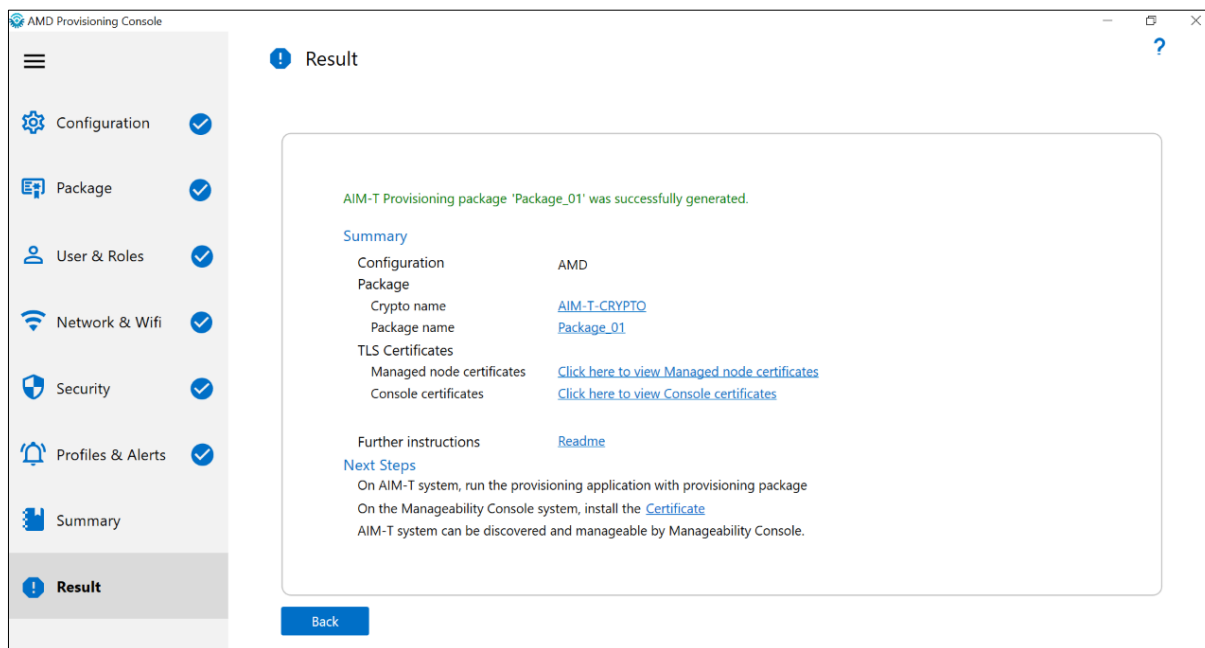


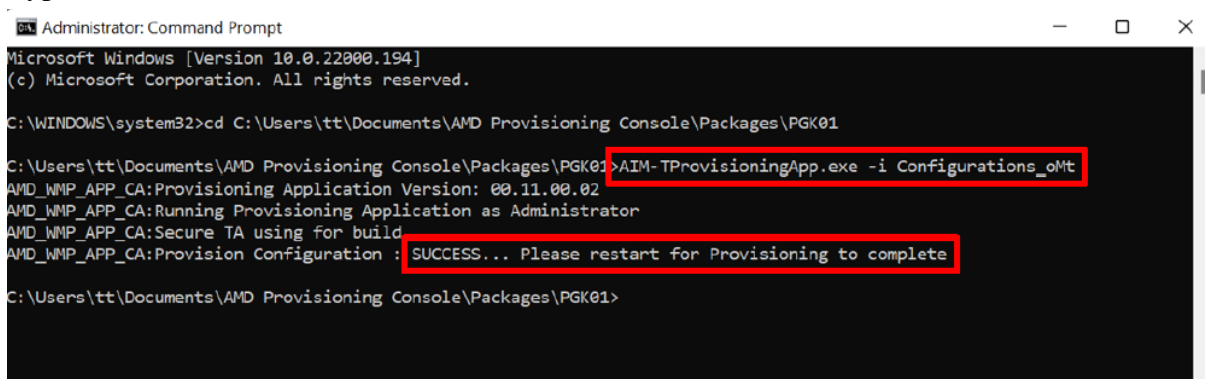
Figure 28. Result

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 29. Provisioning Command

19. If you generated a KVM key in Step 12, copy the KVMSSHKey from the provisioning package (`<package path>\consolecertificates\KVMSSHKey`) to `C:\Program Files (x86)\DASH CLI x.y\certs\` on host.

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:

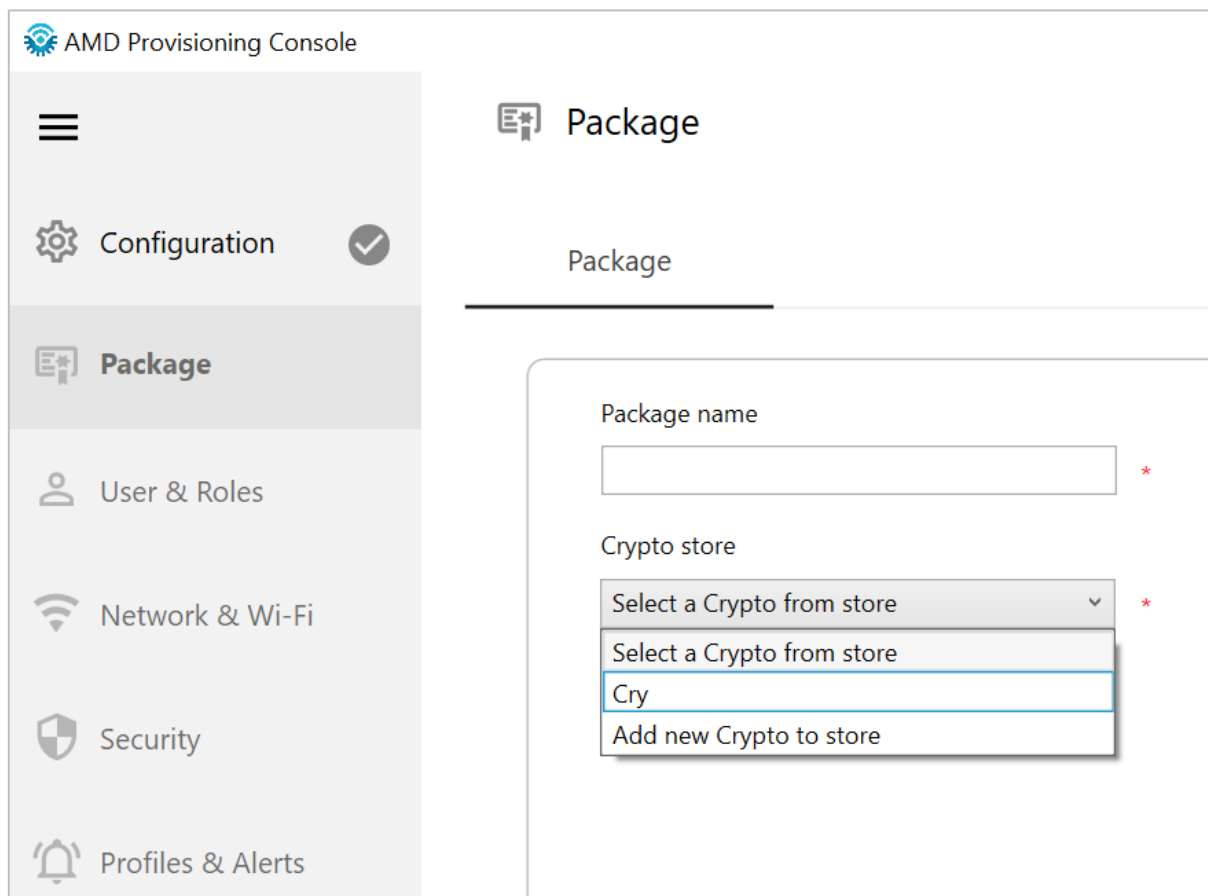


Figure 30. Select Crypto Key

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*.

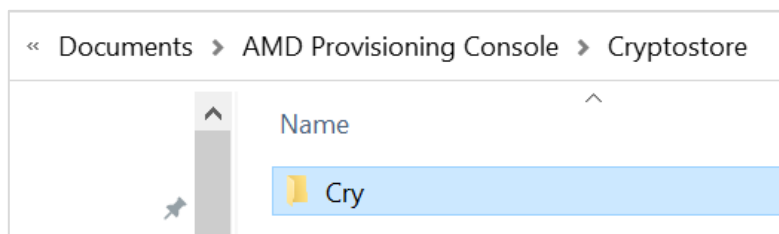
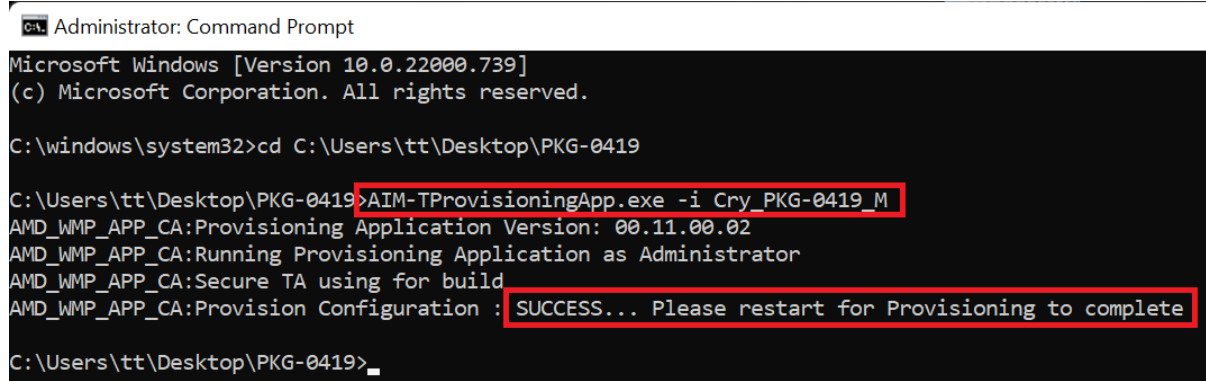


Figure 31. Copy Crypto Key

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
```



```
Administrator: Command Prompt
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 32. 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 5. 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
<code>dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 enumerate battery</code>	Enumerate the battery info
<code>dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t computersystem[#instance] power status</code>	Display current power status of the AIM-T system
<code>dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t computersystem[#instance] power shutdown</code>	Power shutdown the AIM-T system
<code>dashcli.exe -h <ipaddress> -u <username> -P <password> -S https -C -p 664 -t computersystem[#instance] power cycle</code>	Power cycle the AIM-T system
<code>dashcli -h dash-system -p 664 -S https -C -u <username> -P <password> software[0] install <URL for Capsule></code> Example: <code>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</code>	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 13. 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:

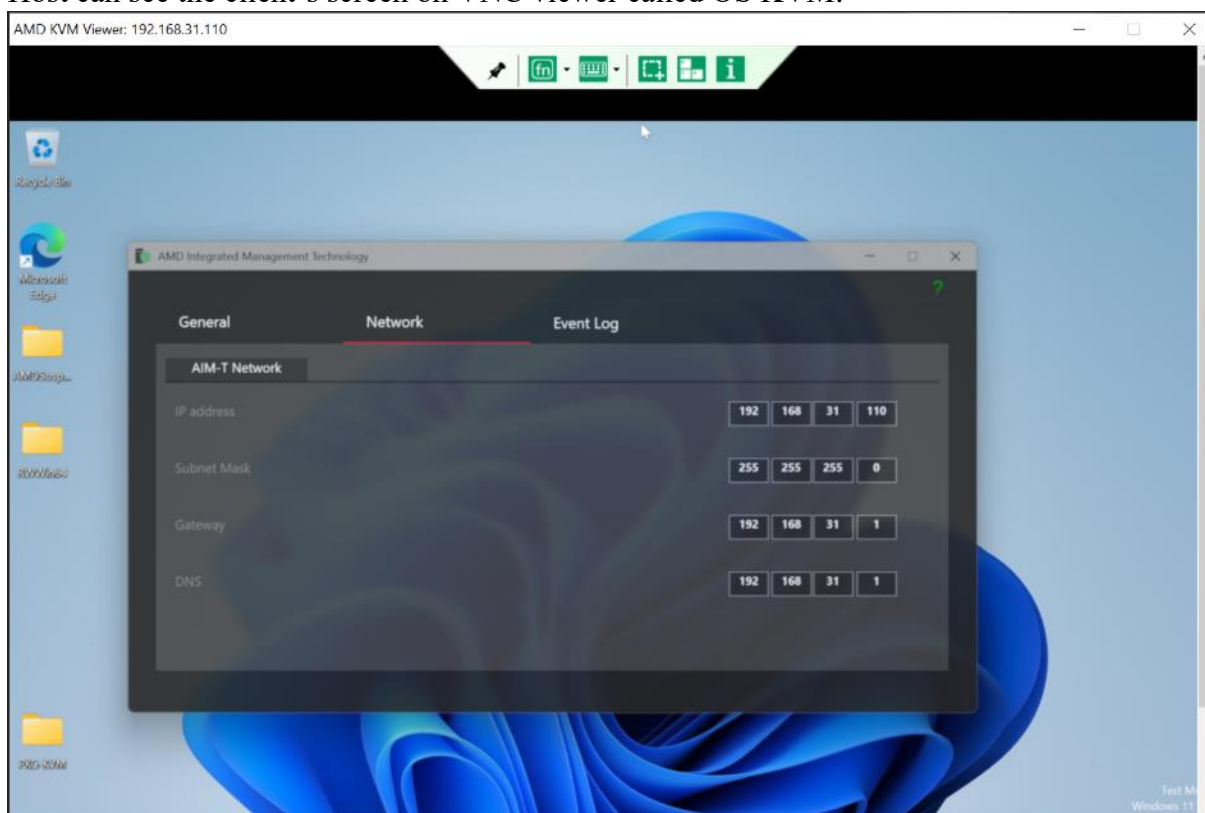


Figure 33. AMD KVM Viewer

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.

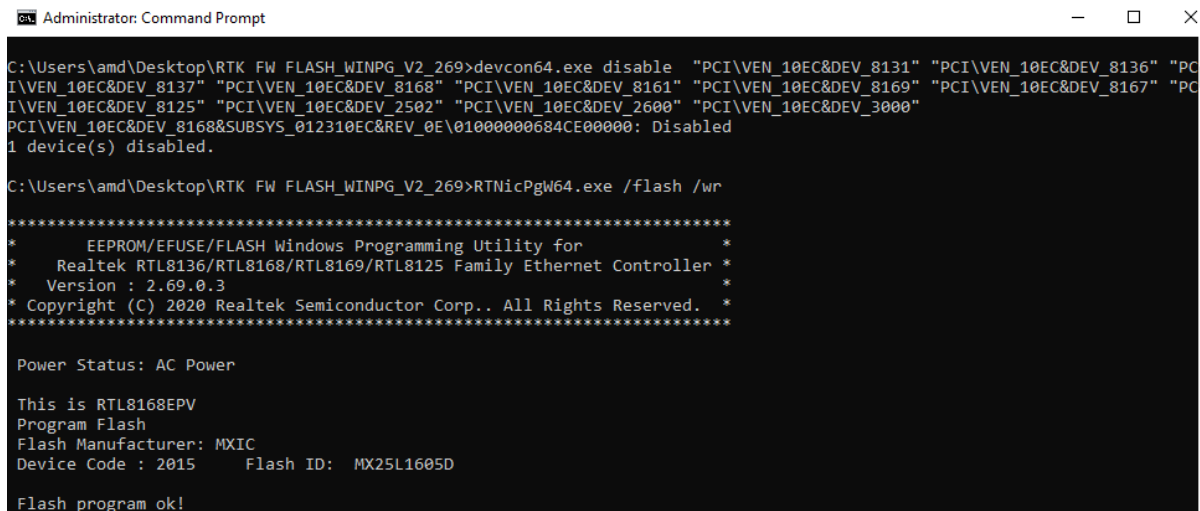
11. Based on the F1/F2 configuration in the previous step, press F1 on the VNC Viewer. The AIM-T system will boot to OS and OS KVM will be established.
If you press F2, the client will boot to BIOS setup menu (BIOS KVM).
12. Ensure that BIOS menu navigation is possible using keyboard and mouse from the 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:



```
Administrator: Command Prompt

C:\Users\amd\Desktop\RTK FW FLASH_WINPG_V2_269>devcon64.exe disable "PCI\VEN_10EC&DEV_8131" "PCI\VEN_10EC&DEV_8136" "PCI\VEN_10EC&DEV_8137" "PCI\VEN_10EC&DEV_8168" "PCI\VEN_10EC&DEV_8161" "PCI\VEN_10EC&DEV_8169" "PCI\VEN_10EC&DEV_8167" "PCI\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 34. Firmware Flash Status

Appendix G Supported Wired DASH Profiles

Table 6. 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 - <https://developer.amd.com/tools-for-dmtf-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.

AMD

Web Service Port: (Default is 3274) *

Alert Reception for HTTP: (Default is 3275) *

Alert Reception for HTTPS: (Default is 3277) *

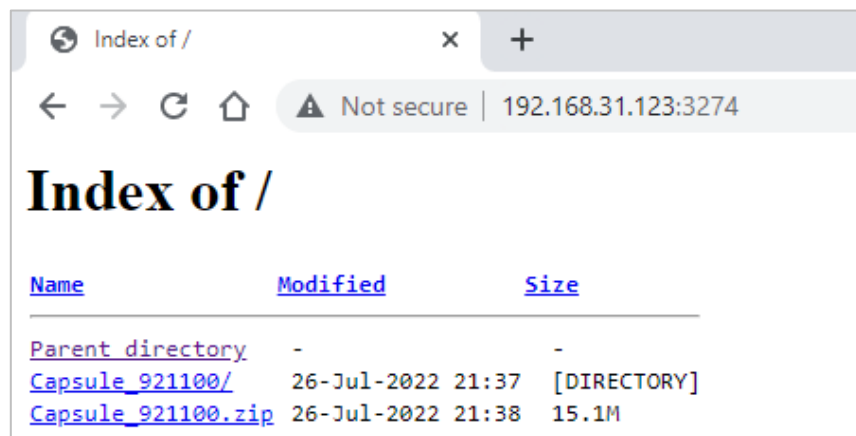
* Ensure no other application use these ports.

InstallShield

< Back Next > Cancel

Figure 35. 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:

**Figure 36. 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

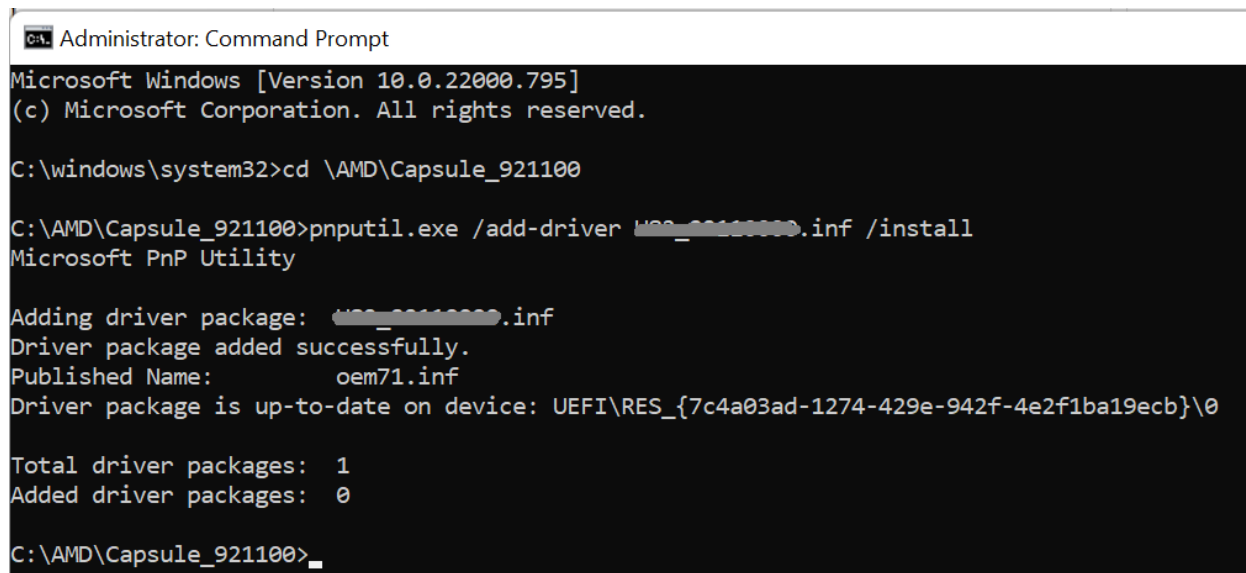
An enterprise IT should be able to download a BIOS capsule from the OEM's website (or other channels). A valid capsule includes:

- `.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:



```

Administrator: Command Prompt
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 OEM71.inf /install
Microsoft PnP Utility

Adding driver package: OEM71.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 37. Valid Capsule

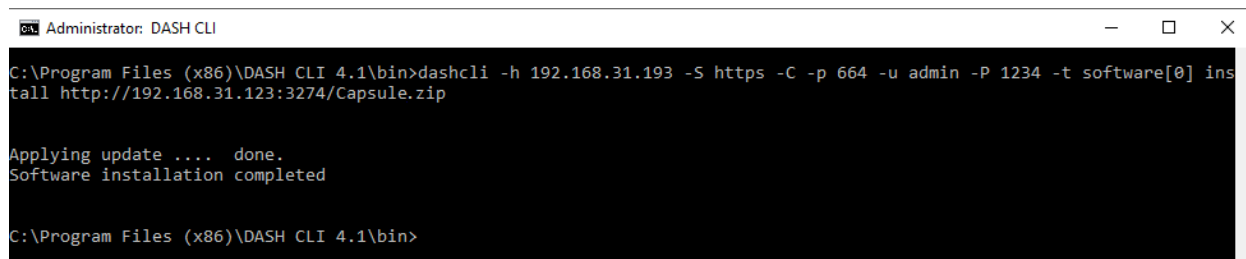
I.3 Reforming the Capsule

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>
```



```

Administrator: DASH CLI
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 38. 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:
 - Linux® system capable of running Ubuntu® 20.04 LTS
 - Public IP
- On public clouds, it can be achieved by spawning Ubuntu 20.04 Virtual Machine (VM) in public subnet. 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®. 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:

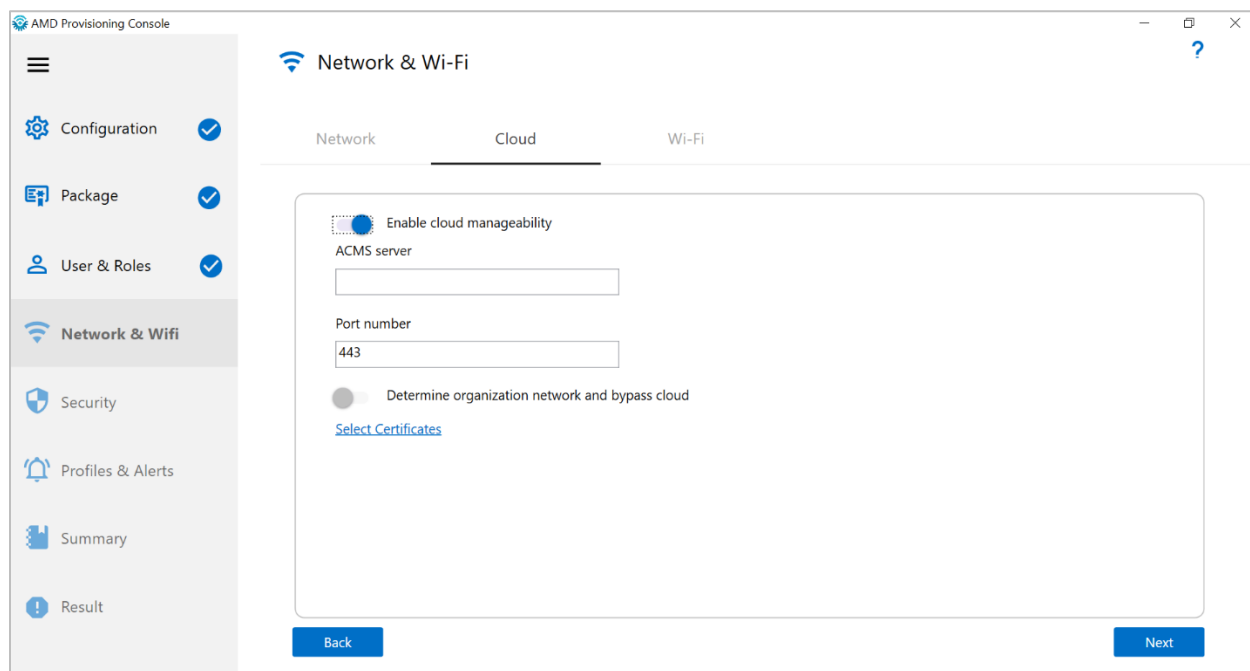


Figure 39. APC PageThe generated files are present at the following path:

\$(SecurePath)\AMD Provisioning Console\Packages\\$(PackageName)\Cloud

\$(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*
- Console
 - *acmscert.pem*
 - *consolecert.pem*
- AIM-T
 - *nodecert.pem*
 - *nodekey.pem*
 - *acmscert.pem*

J.2.1 Installation

Complete the following steps to install ACMS:

1. On Ubuntu 20.04, 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 acms
● 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
```

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/amscert.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\amscert.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 computersystem
```

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.

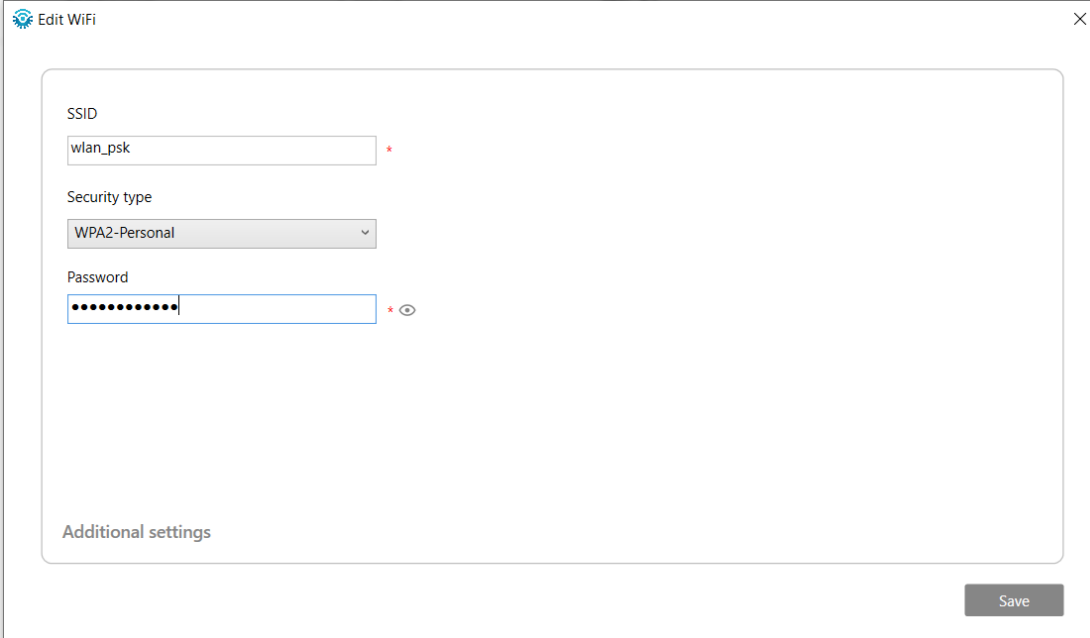
IT Admins must only use decrypted key for provisioning.

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

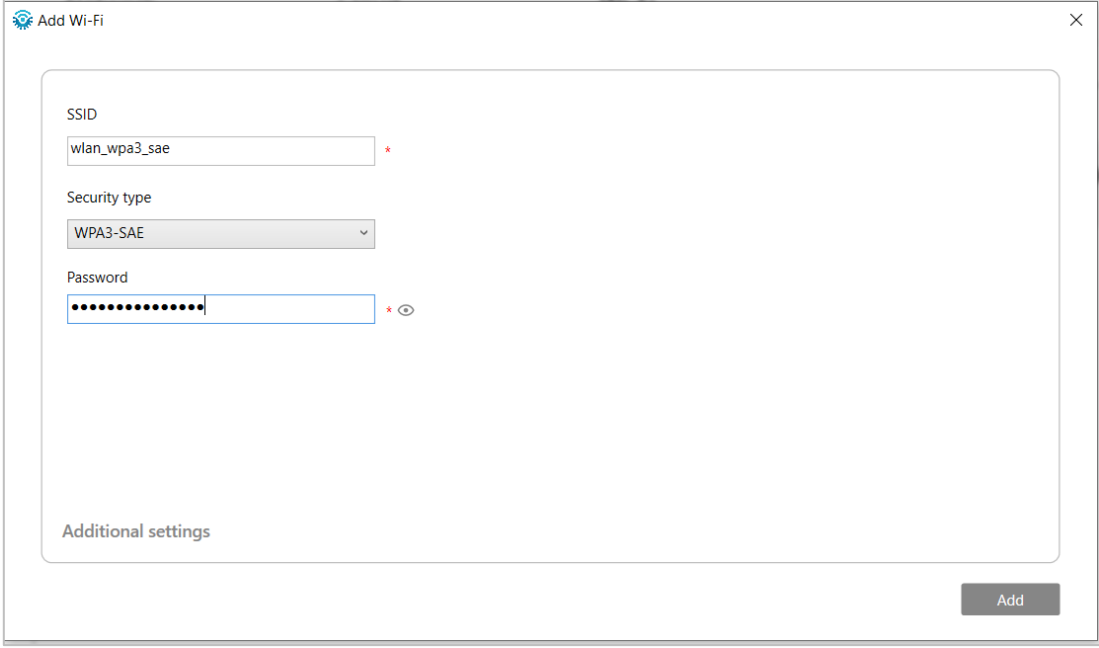
- c. Enter the passphrase that is already shared with you to connect to the wireless network if you have chosen **WPA2-Personal** or **WPA3-SAE** options. Go to [step 10 – providing default port number for Secure port](#).



The screenshot shows the 'Edit WiFi' window. It contains the following fields and controls:

- SSID:** A text input field containing 'wlan_psk' with a red asterisk to its right.
- Security type:** A dropdown menu currently set to 'WPA2-Personal'.
- Password:** A text input field filled with dots, with a red asterisk and an eye icon to its right.
- Additional settings:** A section header at the bottom of the main form area.
- Save:** A button located at the bottom right of the window.

Figure 40. WPA2-PSK Security



The screenshot shows the 'Add Wi-Fi' window. It contains the following fields and controls:

- SSID:** A text input field containing 'wlan_wpa3_sae' with a red asterisk to its right.
- Security type:** A dropdown menu currently set to 'WPA3-SAE'.
- Password:** A text input field filled with dots, with a red asterisk and an eye icon to its right.
- Additional settings:** A section header at the bottom of the main form area.
- Add:** A button located at the bottom right of the window.

Figure 41. 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.

The screenshot shows the 'Edit WiFi' window in Windows. The 'Security type' is set to 'WPA2-Enterprise'. The 'EAP method' is set to 'EAP-TLS'. The 'Identity' field contains 'aimtqa'. The 'Client private key' field contains 'C:\Users\AMD\cert_mar2024\client_decrypted.' with a 'Browse' button. The 'Root CA certificate' field contains 'C:\Users\AMD\cert_mar2024\ca.pem' with a 'Browse' button. The 'Client certificate' field contains 'C:\Users\AMD\cert_mar2024\client.pem' with a 'Browse' button. A 'Save' button is at the bottom right.

Figure 42. WPA2 Enterprise security: EAP TLS

Edit WiFi

SSID: wlan_wpa2_8021x *

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

Security type: WPA2-Enterprise

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

EAP method: EAP-TTLS

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

Username: aimtqa *

Password: *

Additional settings

Save

Figure 43. WPA2 Enterprise security: EAP TTLS

Edit WiFi

SSID: wlan_wpa2_8021x *

Root CA certificate: Browse

Security type: WPA2-Enterprise

EAP method: Peapv0

Username: aimtqa *

Password: *

Additional settings

Save

Figure 44. 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).

The screenshot shows the 'Edit WiFi' window in Windows. The 'Security type' is set to 'WPA3-Enterprise'. The 'EAP method' is set to 'EAP-TLS'. The 'Identity' field contains 'aimtqa'. The 'Client private key' field contains 'C:\Users\AMD\cert_mar2024\client_decrypted.' with a 'Browse' button. The 'Root CA certificate' field contains 'C:\Users\AMD\cert_mar2024\ca.pem' with a 'Browse' button. The 'Client certificate' field contains 'C:\Users\AMD\cert_mar2024\client.pem' with a 'Browse' button. There is a 'Save' button at the bottom right.

Figure 45. WPA3 Enterprise security: EAP TLS

The screenshot shows the 'Edit WiFi' window in Windows, specifically the 'Additional settings' section. The 'Band' is set to 'All'. The 'Group Mgmt' is set to 'BIP_GMAC_256'. The 'Channel' is set to 'All Channels'. The 'Pairwise' is set to 'GCMP_256'. The 'Groupwise' is set to 'GCMP_256'. There is a 'Pmf' toggle switch which is currently turned off. There is a 'Back' button at the bottom left.

Figure 46. WPA3 Enterprise security: EAP TLS Additional Settings

The screenshot shows the 'Edit WiFi' window with the following settings:

- SSID: wlan_wpa3_8021x
- Security type: WPA3-Enterprise
- EAP method: EAP-TTLS
- Username: aimtqa
- Password: [Redacted]
- 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

Additional settings are visible at the bottom, and a 'Save' button is located at the bottom right.

Figure 47. WPA3 Enterprise security: EAP TTLS

The screenshot shows the 'Edit WiFi' window with the following settings:

- Band: All
- Channel: All Channels
- Pairwise: GCMP_256
- Groupwise: GCMP_256
- Pmf: [Toggle]

Additional settings are visible at the bottom, and a 'Back' button is located at the bottom left.

Figure 48. WPA3 Enterprise security: EAP TTLS Additional Settings

Edit WiFi

SSID: wlan_wpa3_8021x *

Root CA certificate: Browse

Security type: WPA3-Enterprise

EAP method: Peapv0

Username: aimtqa *

Password: *

Additional settings: Password

Save

Figure 49. WPA3 Enterprise security: EAP PEAP Settings

Edit WiFi

Band: All

Group Mgmt: BIP_GMAC_256

Channel: All Channels

Pairwise: GCMP_256

Groupwise: GCMP_256

Pmf: ☐

Back

Figure 50. 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*.