[Public]

AMD Management Console User Guide



Publication #	Version: **15.0**
Issue Date:	**October 2026**

DISCLAIMER

Advanced Micro Devices

The contents of this document are provided in connection with Advanced Micro Devices, Inc. (‘AMD’) products.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED ‘AS IS’ AND AMD MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS PUBLICATION AND RESERVES THE RIGHT TO MAKE CHANGES TO SPECIFICATIONS AND PRODUCT DESCRIPTIONS AT ANY TIME WITHOUT NOTICE.

The information contained herein may be of a preliminary or advance nature and is subject to change without notice. No license, whether express, implied, arising by estoppel or otherwise, to any intellectual property rights is granted by this publication.

EXCEPT AS SET FORTH IN AMD’S STANDARD TERMS AND CONDITIONS OF SALE, AMD ASSUMES NO LIABILITY WHATSOEVER, AND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT.

AMD’s products are not designated, intended, authorized or warranted for use as components in systems intended for surgical implant in the body, or in other applications intended to support or sustain life, or in any other application in which the failure of AMD’s products could create a situation where personal injury, death, or severe property or environmental damage may occur. AMD reserves the right to discontinue or make changes to its products at any time without notice.

Trademarks

AMD, the AMD Arrow logo, and combinations thereof are trademarks of Advanced Micro Devices, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Other names are for informational purposes only and may be trademarks of their respective owners.

Copyright © 2013 - 2022 Advanced Micro Devices, Inc. All rights reserved.

Contents

Abbreviations **5**

Chapter 1 Introduction **6**

1.1 Architecture Overview 7

1.2 System Requirements 8

1.3 Prerequisites 8

1.4 AMC Installation Steps 8

Chapter 2 Configure AMC **15**

2.1 Authentication 16

2.2 Intune 18

2.3 About 19

Chapter 3 Layout of AMC UI **21**

Chapter 4 How to Manage Clients from AMC **23**

4.1 Discovery 23

4.2 Power 24

4.2.1 Power Operation on a Single System 26

4.2.2 Power Operation on a Group of Systems 28

4.2.3 Power Operation on a System or Group of Systems 29

4.3 Boot 31

4.4 Text Redirection 33

4.5 USB Redirection 34

4.5.1 USB Redirection on a Single System 34

4.5.2 USB Redirection on a Group of Systems 37

4.5.3 USB Redirection on a System or Group of Systems 38

4.6 KVM Redirection 39

4.7 Alerts Subscription/Un-Subscription 42

4.8 Health 43

4.9 Properties of the System 44

4.10 Inventory 45

4.11 Alert Reception 45
4.12 Log Entry Profile 46
4.13 Boot to Text Image 47
4.13.1 Sample Use Cases 48
4.14 Firmware Upgrade 50
4.15 Boot to BIOS (KVM Profile) 50
4.16 Opaque Management Data 52
4.17 Unown 53
4.18 Disk Wipe 55
4.19 Remote Access 55
4.20 Add Groups 58
4.21 Delete Groups 58
4.22 Rename Groups 59
4.23 Add system to selected group 59
4.24 Delete system 60
Chapter 5 Appendix 61
5.1 Troubleshooting issues: 61
5.2 Configuring Microsoft Entra ID App Registration for Intune Sync 66

Abbreviations

- **DASH** (**D**esktop and Mobile **A**rchitecture for **S**ystem **H**ardware): It is the DMTF Commercial Client management standard produced by the DMTF DMWG. It specifies the transport, management protocol (WS-Man) and DMTF CIM profiles used to manage desktop/mobile PC. A 'Dash Capable System' is a computer system which conforms to the DMTF DASH standard.
- **DMTF** (**D**istributed **M**anagement **T**ask **F**orce): It is an industry organization which develops system management standards such as DASH and WS-Management.
- **MC**: **M**anagement **C**ontroller.
- **DASH MC**: The MC that implements the external DASH protocol stack. It interfaces with other platform components (BIOS, SB, IMDs, etc.) to get needed information or control the platform.
- **Out-of-band management**: This defines the management tasks that are performed independent of the power or OS state on the managed client or system.
- **Managed System or Managed Node**: It is a DASH capable system i.e. a computer system which conforms to the DMTF DASH standard.

[Public]

Chapter 1 Introduction

This document describes features and usage of current version of AMC (AMD Management Console). AMC allows the IT Admin to remotely manage client computer systems which support the DMTF DASH standard.

Refer the document ‘AMC ReleaseNotes.pdf’ in the ‘docs’ folder of AMC installation.

AMC can manage DASH capable systems in a small business environment.

[Public]

1.1 Architecture Overview

Referring Figure 1, AMC consists of two major Layers. The first one is the AMC User Interface (AMC UI) and the other is the AMC Service. The AMC UI layer is a lightweight layer and relies entirely on the AMC Service.

Figure 1 shows an architectural overview of the AMC.

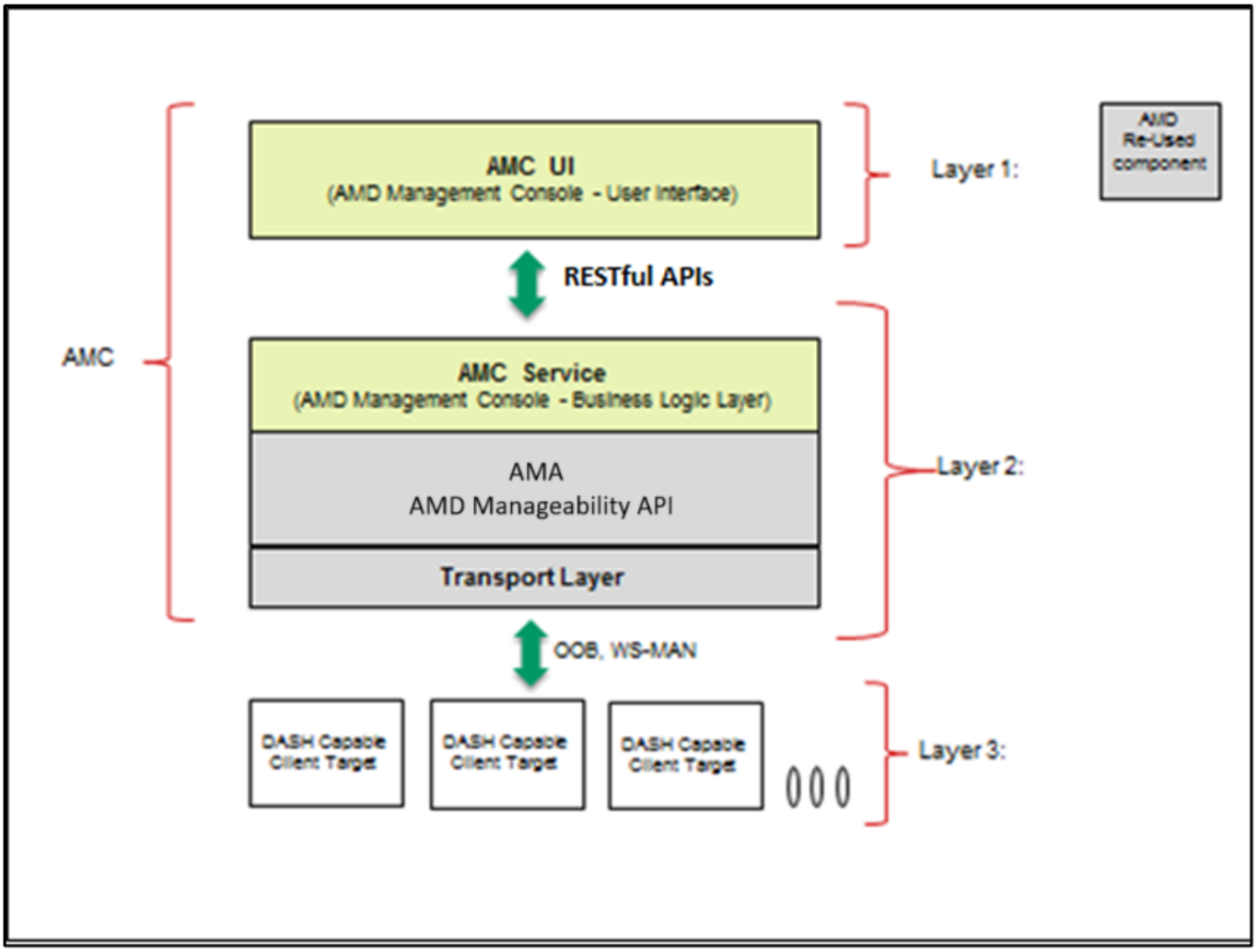


Figure 1: AMC High Level Architectural Overview.

[Public]

1.2 System Requirements

Supported Operating Systems

Listed below are the supported operating systems to install and use AMC:

- Windows 11
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Memory and Disk Space requirements

AMC requires a minimum of 1 GB Disk space and 4 GB RAM for normal functioning.

1.3 Prerequisites

DASH capable client desktops and notebooks (client targets) should be DASH enabled/configured to be managed from AMC. Kindly refer to the client system vendor's tool chain to configure the system.

Note: 'AMD Provisioning Console (APC)', an AMD tool can be used for configuration. Refer the release notes of APC for configuration/provisioning procedure for AIM-T based systems.

1.4 AMC Installation Steps

Once a system to be installed is identified with all the requirements as specified in *section 1.2*, use the 'AMC-setup-<version>-AMD.exe' to install AMC.

Note: If you have installed old AMC revision in your system, you first have to uninstall that version before installing AMC 3.2.

1. Double click on the 'AMC-setup-<version>-AMD.exe' windows installer file.
2. Prerequisites required for AMC installation will appear as shown in Figure 2. Click on Install will install all the prerequisites listed in this section.
   - Read and accept License before installing each of the prerequisite.

[Public]

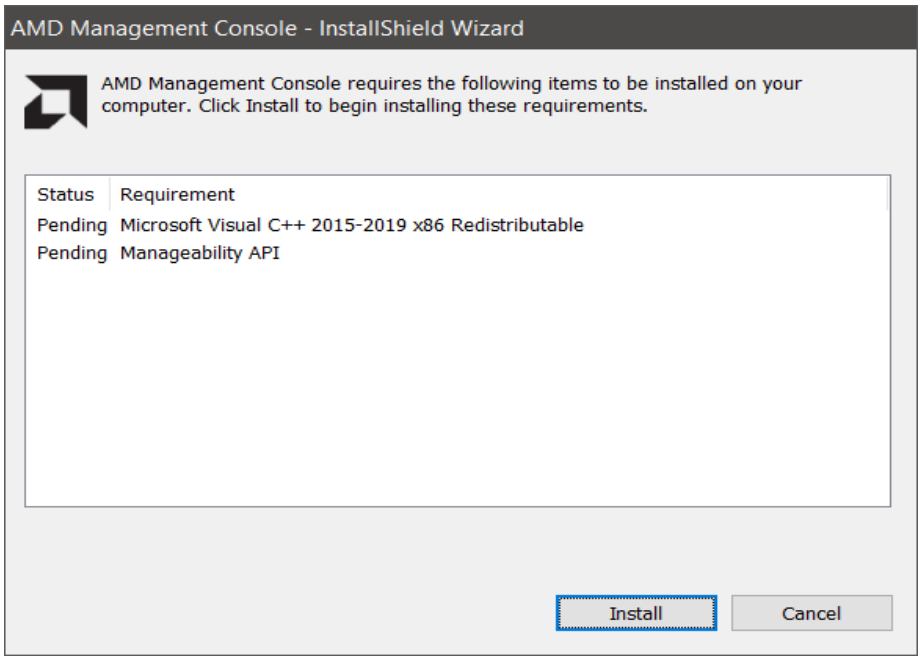
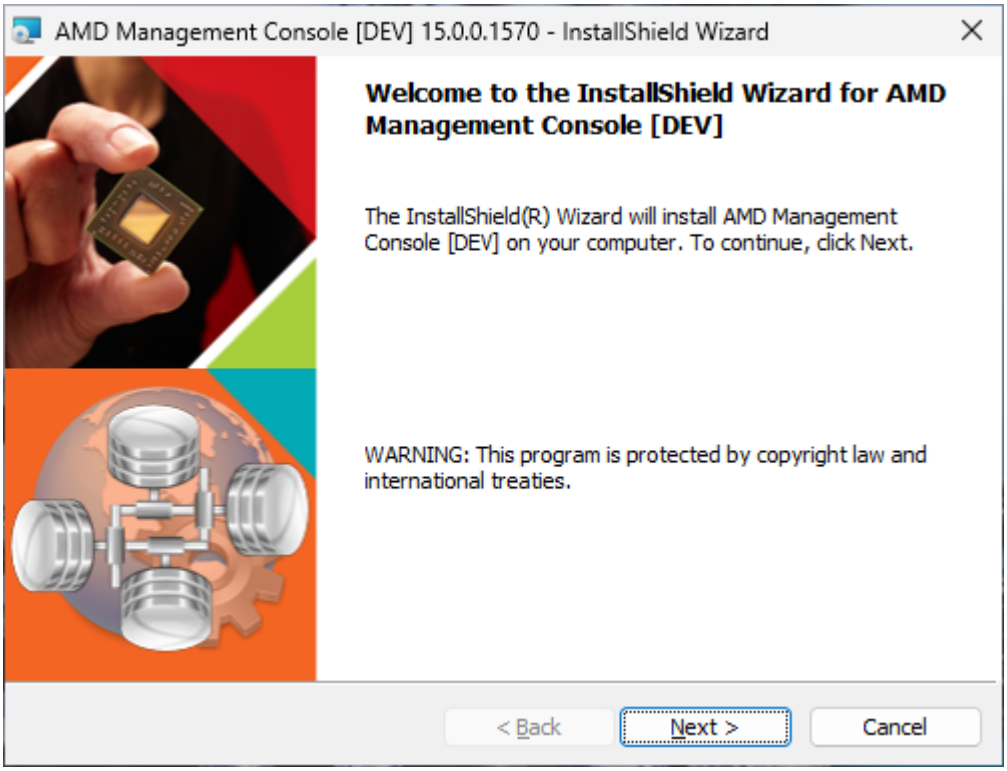


Figure 2: AMC Prerequisites Installation Dialog

3. After Prerequisites are installed, AMC setup wizard will appear as shown in Figure 3, click on 'Next' to continue the installation.



[Public]

Figure 3: AMC Setup Dialog

4. The ‘License Agreement’ dialog appears as shown in Figure 4.
5. Read the License Agreement carefully and select ‘I accept the terms in the license agreement’ radio button to accept the license terms and then click on the ‘Next’ to continue.
6. The ‘release notes’ dialog appears as shown in Figure 5, read the information and then click next to continue.
7. The ‘Destination Folder’ dialog appears as shown in Figure 6. Default destination folder can be changed by clicking the ‘Change’ button. Once done, click ‘Next’ to continue.

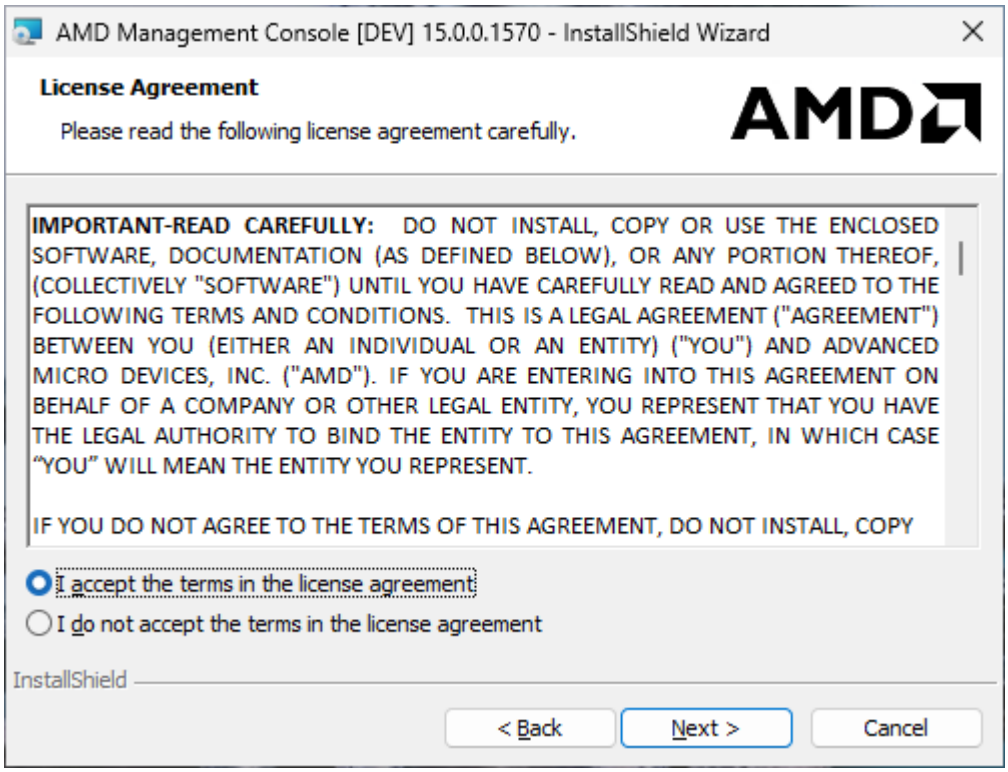


Figure 4: License Agreement Dialog

[Public]

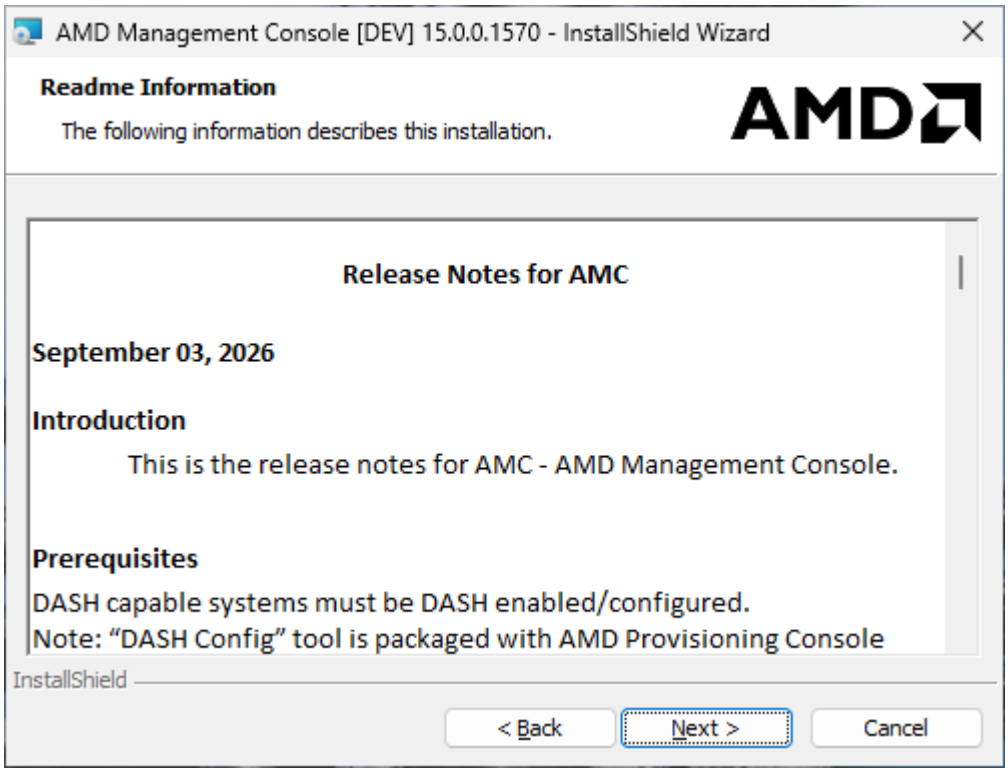


Figure 5: Release Notes Information

[Public]

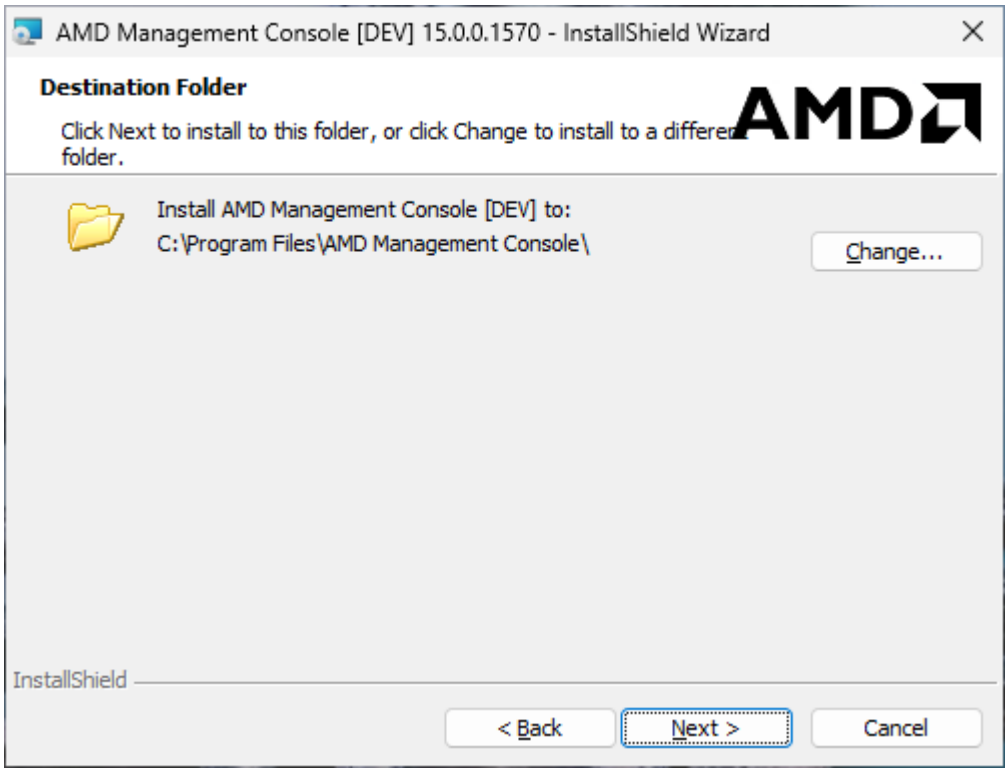


Figure 6: Destination Folder Dialog

[Public]

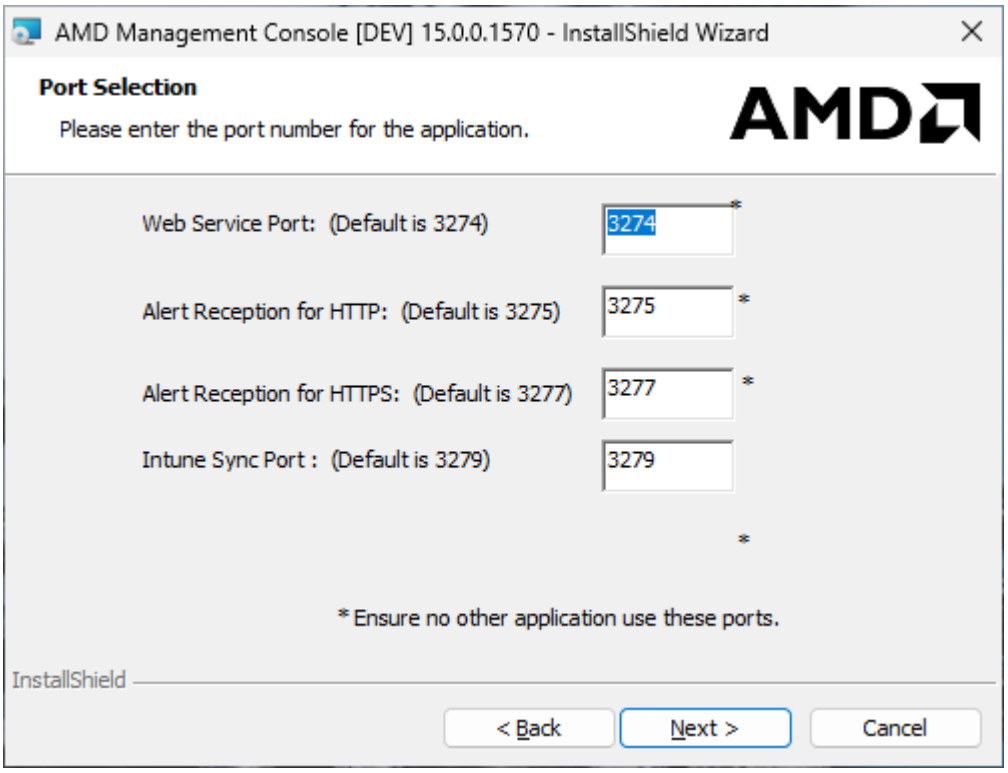


Figure 7: AMC Port Selection Dialog

8. The ‘AMC Port Configuration’ dialog appears as shown in Figure 7.
   a. The Web Service port (Default 3274) is used by AMC for creating a web service. The default AMC Service port is 3274. It is recommended not to change the AMC Service port unless the specified port is already in use by a different application.
   b. The Alert Reception ports are used by AMC Alert Service to receive alerts from the managed nodes (targets). The default Alert Reception for HTTP port is 3275 and for HTTPS is 3277. It is recommended not to change the Alert reception ports unless the specified port is already in use by a different application.

   Change the ports to the desired value if necessary and click ‘Next’ to continue installation.

9. The ‘Ready to Install the Program’ dialog appears as shown in Figure 8. Click on ‘Install’ to install the program.
10. The ‘Installation complete’ dialog appears as shown in Figure 9. Click ‘Finish’ to complete the installation.

[Public]

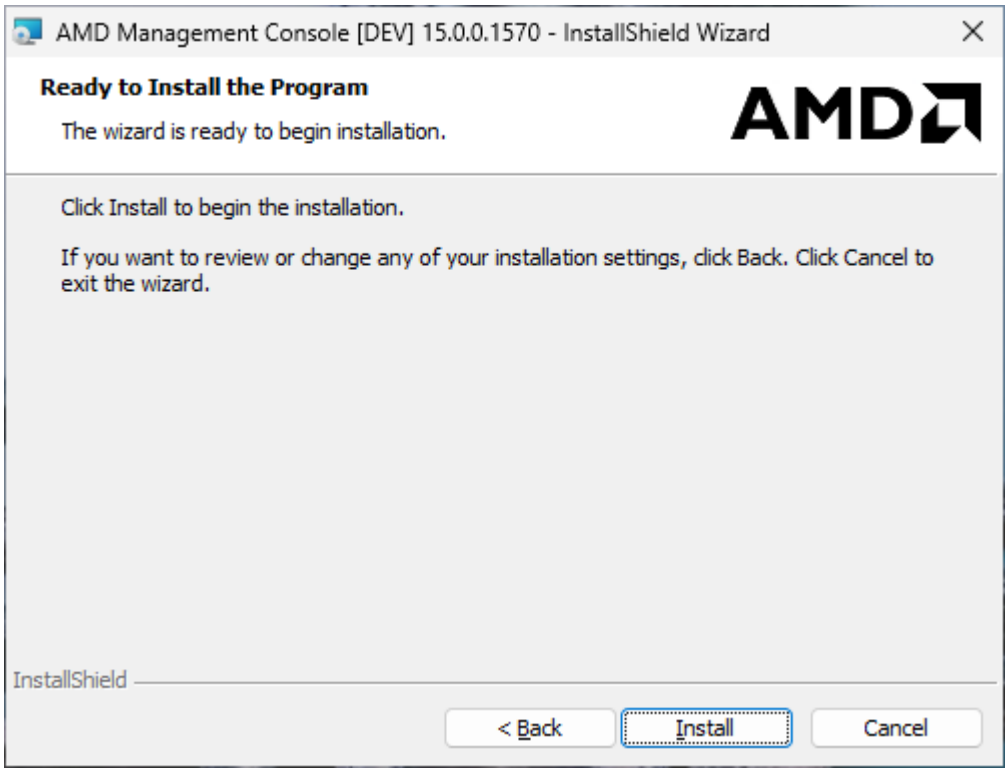


Figure 8: Ready to Install the Program Dialog

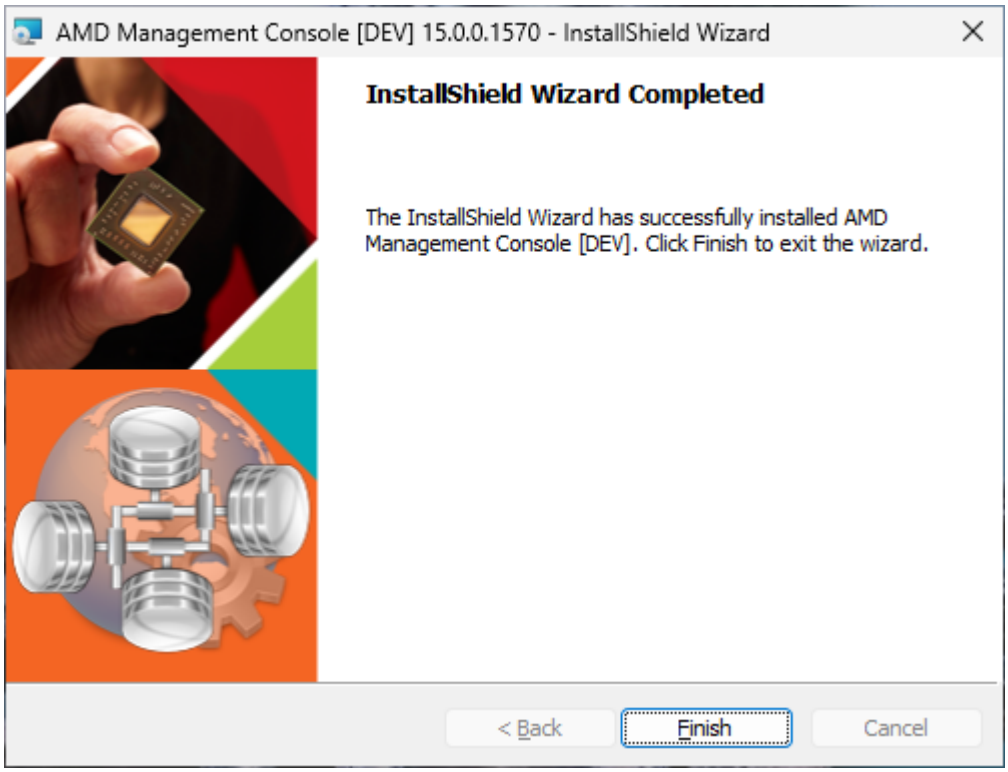


Figure 9: Installation Completion Dialog

[Public]

Chapter 2 Configure AMC

The configuration screen to configure AMC appears in two ways.

1. When UI is launched for the first time after installation, a dialog box will appear as shown in Figure 10. Click OK to get to the AMC Configuration screen.

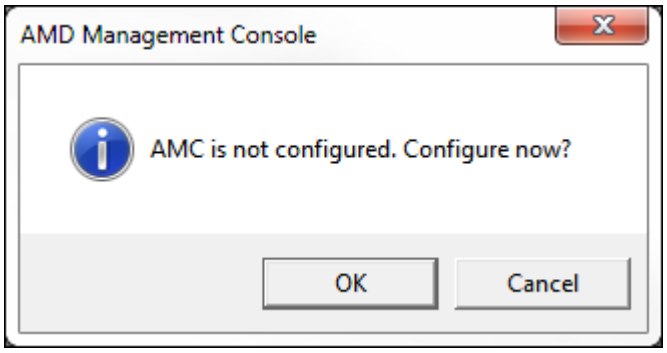


Figure 10: Configure AMC

2. After launching the UI, go to 'CONFIGURATION' tab and click on 'Settings' ribbon icon to get to the AMC Configuration Screen. Kindly refer to Figure 11 below.

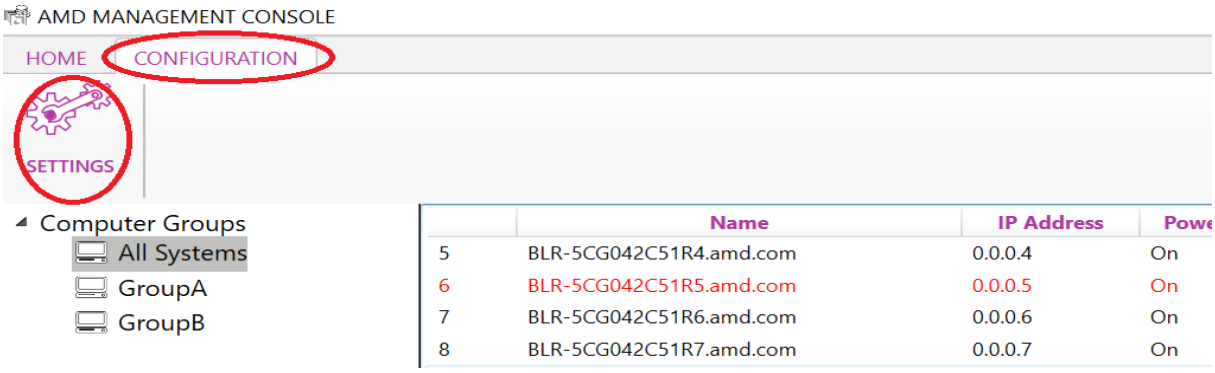


Figure 11: Configure AMC

The AMC configuration screen captures information such as authentication and connection details. AMC will use this information to connect and communicate with the managed computer systems.

[Public]

2.1 Authentication

AMC has support for up to five authentication entries. Each entry has an authentication identifier, scheme and corresponding credentials which must be provided. AMC has support for two types of authentication schemes, Digest and Active Directory respectively. IT administrator must provide at least one authentication entry (Auth Identifier, Scheme, Username and Password). AMC will use one of three entries in sequential order to authenticate itself to manage the target. Once a target is authenticated with a specific entry, the target is associated with that authentication entry. If AMC at a later stage is not able to manage the said system with the associated authentication entry, and if more than one authentication entry is available, AMC will try to utilize the other entries to authenticate itself with the said target. If this succeeds, the association is modified or else removed. Note that between authentication entries, the authentication identifier is unique. Specifically, there cannot be two entries with same authentication identifier. It is expected that the computer systems should be provisioned with one of the three authentication entries provided in AMC. Provisioning the managed system is beyond the scope of AMC. IT Admin should use the respective vendor tools to provision the managed computer system.

In Figure 12-A, the IT administrator has provided two authentication entries. First, with Digest Authentication Scheme with credentials and the second, with Active directory authentication scheme with credentials.

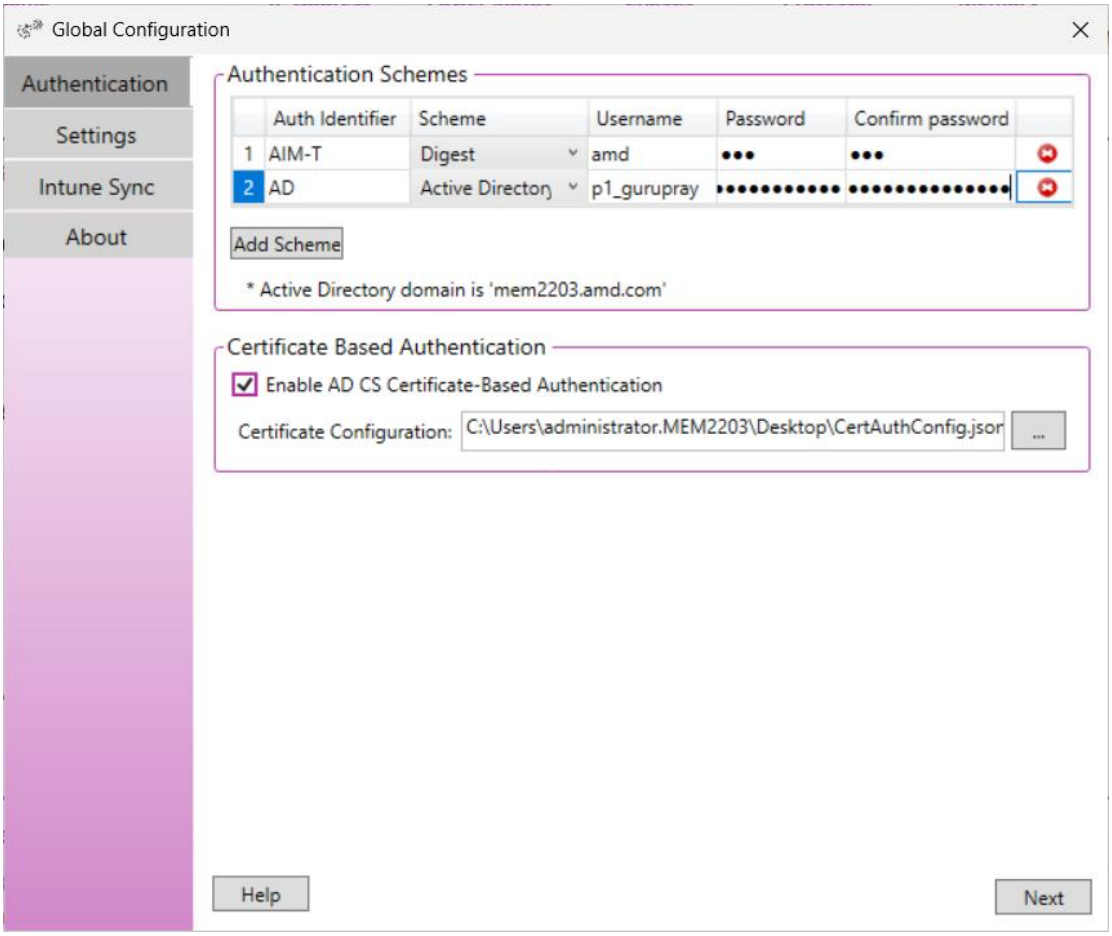


Figure 12-A: Authentication Screen

[Public]

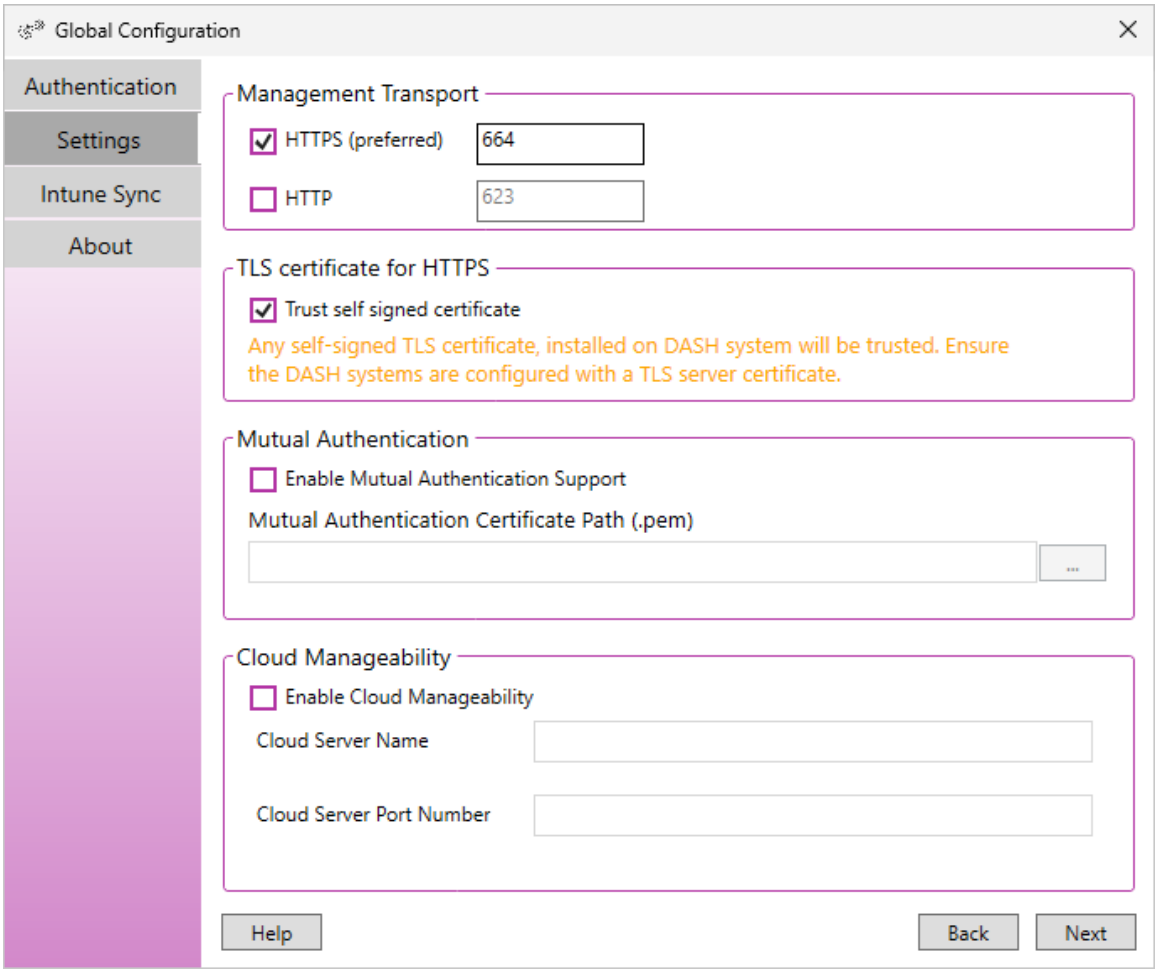


Figure 12-B: Configuration -> Settings

AMC can communicate with the managed DASH computer systems on either HTTP or HTTPS transport. The default port for HTTP is 623 and HTTPS is 664. This transport and port selection is used by AMC for managing all DASH computer systems. Trust self-signed certificate option allows administrators to ignore self-signed TLS certificates used for HTTPS while performing DASH operations.

AMC supports communicating managed targets through AMC Cloud Manageability Service [ACMS], user can enable ACMS support and provide ACMS server name, port details through which AMC can communicate to managed node via ACMS server. All ACMS certificates to be copied to installation folder under certs folder

AMC supports Mutual authentication through which both Managed node and AMC Console will be mutual authenticated to trust each other. User can enable Mutual authentication support as shown in Figure 12-B. Once Mutual Authentication is enabled a Mutual authentication certificate path (.pem) to be provided through which AMC Console and Managed node will be mutually authenticated. Figure 12-B shows the connectivity detail. For the changes to take effect, the IT Admin should click first on ‘Validate’ and then click on ‘Save’.

[Public]

Note: To delete an already entered authentication scheme, please select the option "not-used" and save the entry**.**

2.1.1 Certificate Based Authentication

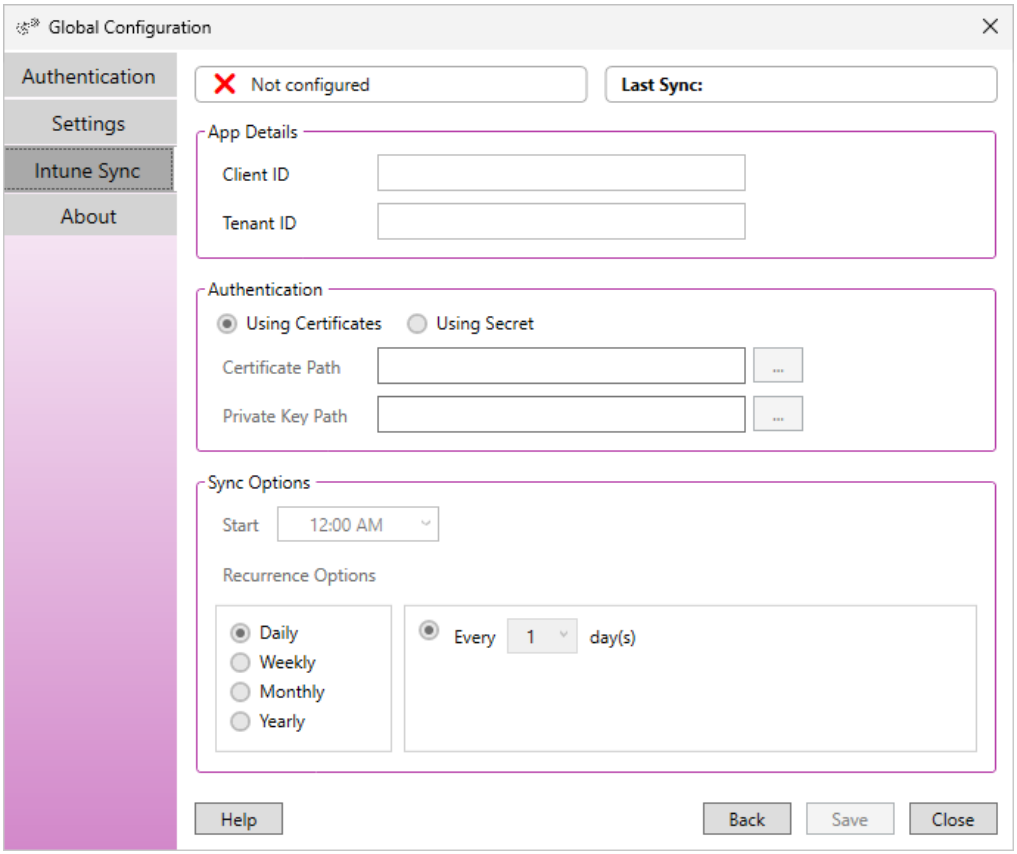
AMC supports certificate based authentication for enhanced security. When the " **Enable AD CS Certificate-Based Authentication**" checkbox is selected under the **Certificate Based Authentication** section on the Authentication tab, a browse panel becomes visible as shown in Figure 12 to choose the config file required for enrolling DASH Authentication certificate (CertAuthConfig.json).

2.2 Intune

The **Intune Sync** feature enables AMC to automatically import and manage devices from **Microsoft Intune**. To configure Intune Sync, an application must first be registered in **Microsoft Azure Active Directory (Azure AD)**, and the required authentication details such as **Tenant ID**, **Client ID**, and an authentication method (either a **Client Secret** or **Certificate**) must be provided in AMC. Once the connection is established, administrators can configure the synchronization schedule, such as daily or periodic sync intervals.

During each synchronization cycle, AMC retrieves the managed device inventory from Microsoft Intune and automatically initiates **DASH discovery** for the synced devices. This allows devices discovered through Intune to be onboarded and managed within AMC without requiring manual discovery. Intune Sync helps streamline device management by ensuring that newly enrolled or updated Intune devices are automatically reflected in the AMC inventory.

[Public]



Note:

Refer Appendix 5.2 Configuring Microsoft Entra ID App Registration for Intune Sync

2.3 About

The about tab displays the name of the application, the version information, web service (machine name where the web service runs), web port (port to which the UI Console connects to AMC Service) and alert port (port on which the AMC Service receives alerts from managed systems) as in Figure 13.

[Public]

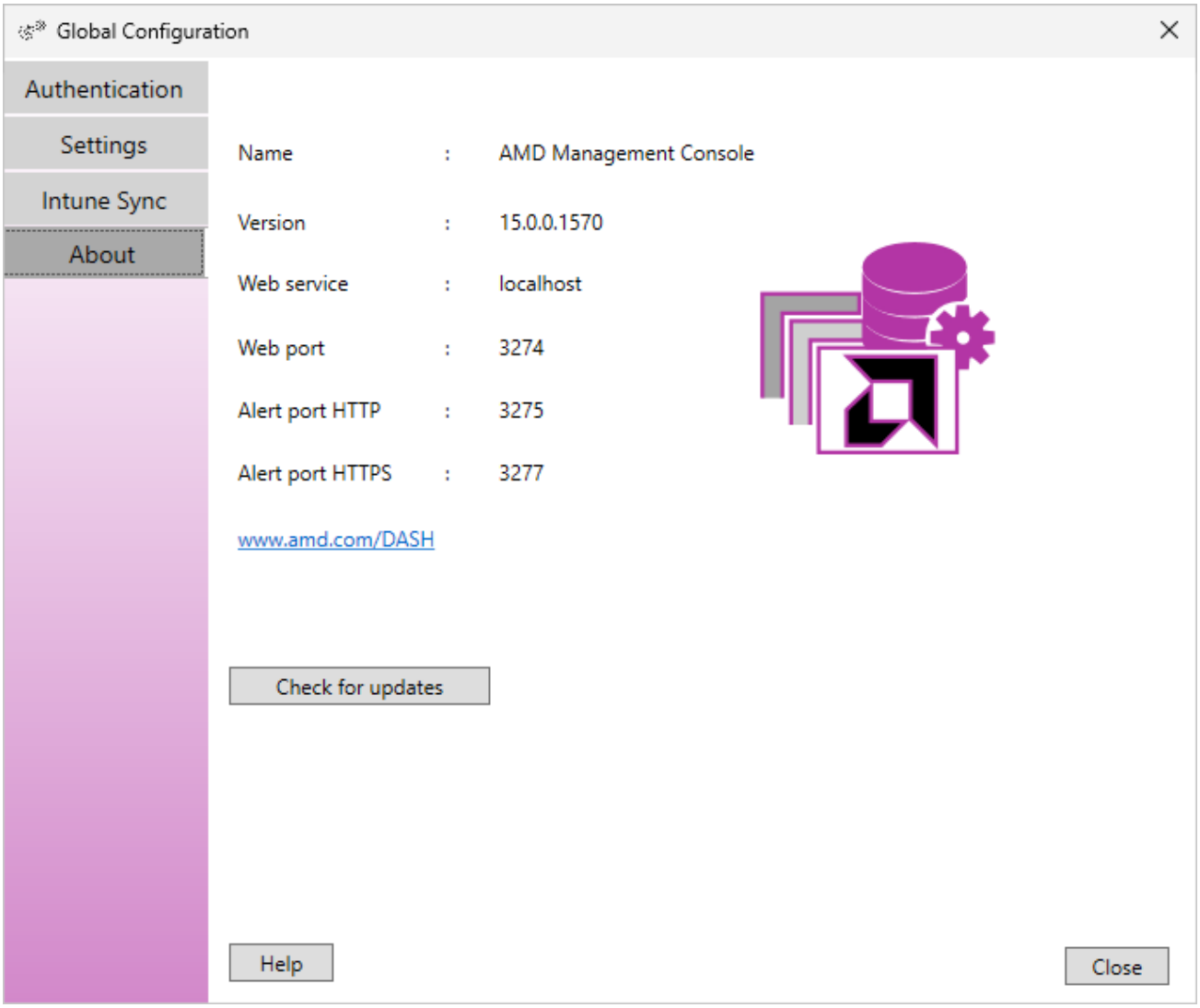


Figure 13: About Screen

Note: AMC About screen provides an option to check for latest AMC updates. When user click on 'Check for updates' button, AMC will check whether any updates are available. Updates available will be shown as a pop-up along with a tray icon.

[Public]

Chapter 3 Layout of AMC UI

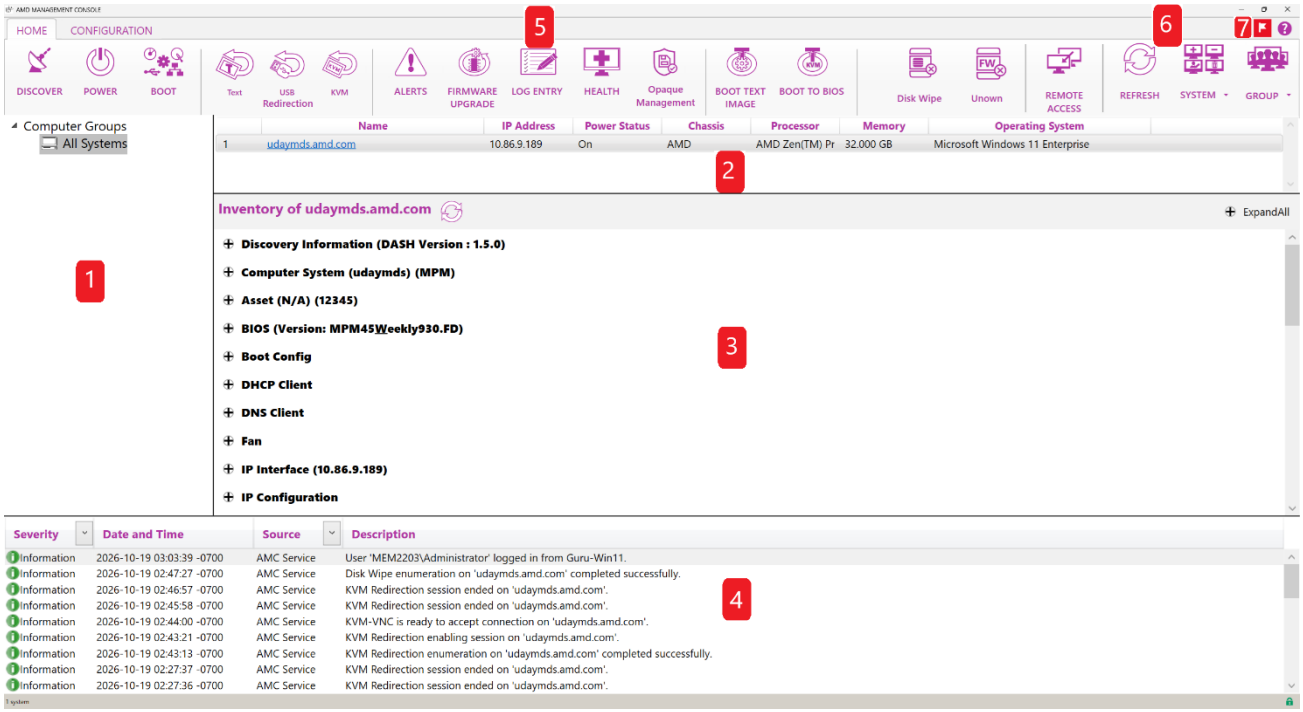


Figure 14: AMC UI Layout

Managed Computer Groups

In Figure 14, the area marked 1, lists all the Computer Groups created in AMC. By default AMC creates a Computer Group called ‘All Systems’. This group cannot be deleted. After every discovery activity, all the DASH capable systems will be listed under this default Group. New groups can be added to the computer groups list by right clicking on the Computer Group and selecting ‘Add Group’ or by clicking on the ‘Add’ menu item under Group Ribbon icon near the item marked 6. Groups can be deleted by right clicking the relevant group and selecting ‘Delete Group’ or by selecting the ‘Delete’ menu item under Group Ribbon icon near the item marked 6. Group names can be renamed by right clicking the relevant group and selecting ‘Rename Group’ or by selecting the ‘Rename’ menu item under Group Ribbon icon near the item marked 6. To add systems to any group thus created, right click on the Group to which systems are to be added and click on ‘Add systems’ menu item and select the systems from the new screen. Click on Ok to accomplish the task. There is one more way to add systems to a specific group. Select a system or a group of systems from the area mentioned 2. Click on ‘Add to Group’ menu item under System Ribbon icon, this will result in a screen showing the available groups to which the user wants to move the system/systems already selected. After making the selection, click ok to complete the task.

Managed Systems

In Figure 14, the area marked 2, lists all the managed DASH capable computer systems for a particular group selected in area marked 1. If the group selected in area 1 is changed, the respective managed targets of that

[Public]

group get listed in area 2. The systems which are listed here are color coded. The systems with black color inform that the right authentication credential is available with AMC to manage it. The systems with red color inform the user that AMC does not have the right credentials to manage the system.

Inventory

In Figure 14, the area marked 3 is where all the inventory information of a single managed computer system gets listed. The computer system for which the inventory gets listed is based on the selection of the system made from the list in area 2. The asset and inventory information displayed here are identity of the system, physical assets, processor, system memory, Ethernet port, BIOS, OS and System Software.

Activity Log and Alerts

In Figure 14, the area marked 4 is where all the activity and alerts are listed. When an IT Admin initiates an operation, the operations progress is shown in this area. This area also lists the alerts which are received from the managed computer systems. IT Admin can apply filters for information required to be seen in area 4. In the source column, selecting ‘Managed Systems’ will show only the alerts from Managed systems, selecting ‘AMC Service’ will show only activity initiated by the IT Admin as tracked by AMC Service and its progress. Selecting ‘Show All’ will show all the messages (both from AMC service and Managed systems). IT Admin can also apply filters for the Severity column; user can select one of ‘Show All’, ‘Information’, ‘Warning’, ‘Error’, ‘Error and Warning’ and the respective severity items only will be displayed in area 4.

Manage DASH Clients from AMC

In Figure 14, the area marked 5 is where all the ribbon icons are present. Clicking on them will initiate a management operation, either with a single managed computer system or group of computer systems. The same operation can also be performed by right clicking in the area 1 (Group) or in the area 2 (System). The management operations that can be initiated in this release are Discovery of manageable systems, Power monitoring and control, Boot monitoring and control, Text Redirection, USB Redirection, Alert subscription/un-subscription, Health monitoring.

AMC Group or System activity

In Figure 14, the area marked 6 is where all the ribbon icons with menu items are available. Using these icons, IT Admin can create new groups, delete existing groups, add a system to a group, remove a system from a group or delete a system from AMC. To refresh the information in areas 2 and 3, the refresh ribbon icon can be used.

AMC Auto Updates

The Auto Update ribbon appears in AMC whenever a newer software version is available for installation. When displayed, users can click the ribbon to view update details, verify the available version, and initiate the update process. AMC automatically checks for eligible updates and provides a streamlined experience for keeping the application up to date with the latest features, enhancements, and fixes. After the update is installed, AMC may prompt for a restart to complete the upgrade process.

[Public]

Chapter 4 How to Manage Clients from AMC

To Manage Clients from AMC, initially manageable systems have to be discovered. Then a set of tasks or operations can be performed against the manageable systems discovered.

4.1 Discovery

Note: Before performing a discovery operation, make sure that the authentication details are correct, refer *'Authentication'*.

Discovery is the process of adding systems to AMC for management. Only systems that have hardware which supports DMTF management specification can be discovered by AMC. On successful discovery, the system is added to 'All Systems' group and inventory is performed on that system. The systems thus added will be of black in color, if AMC was able to authenticate itself successfully using one of the authentication entries provided in the *'Authentication'* screen. The systems thus added will be of red in color, if AMC was not able to authenticate itself successfully using any of the authentication entries provided through AMC. Through discovery, AMC determines if a system supports DASH and which specific capabilities or features are accessible.

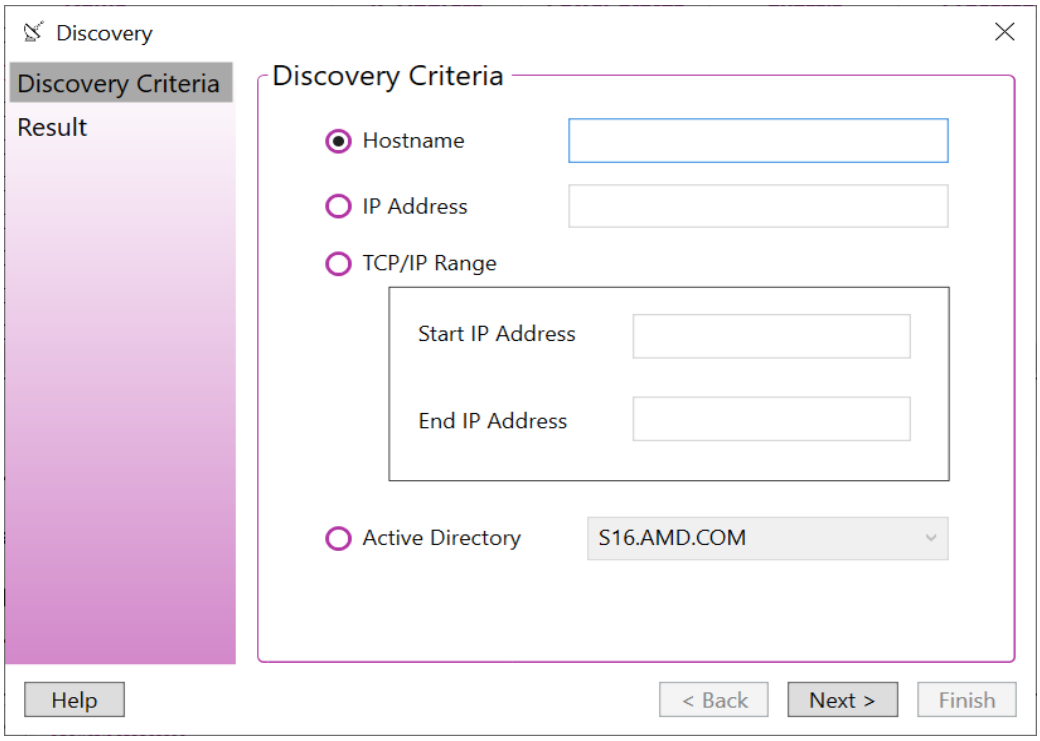


Figure 15: Discovery

[Public]

Four different modes of discovery are supported by AMC

1. **Hostname:** Any system name can be provided for discovery. AMC will query the system and find out if that system is manageable or not. For hostname discovery to work correctly, ensure the DNS settings are correct and working. This method is useful for finding out if a single system is manageable or not.
   Note: Hostname should be configured based on Microsoft standard specifications set for specifying the hostname of a windows system.

2. **IP Address:** Any valid IP address can be provided for discovery. AMC will query that address and find out if that system is manageable or not. This method is useful for finding out if a single system is manageable or not.

3. **IP Subnet:** A range of IP address can be provided for discovery. AMC will scan each IP address in that range and find out if the system with that IP address is manageable by AMC or not. This method is one of the bulk discovery mechanisms, where large numbers of systems can be discovered.

4. **Active Directory:** If the system on which AMC is installed is part of an active directory domain, then discovery is initiated on all the systems which are a part of that domain. Each system in that domain is determined if it is manageable by AMC or not. This method is one of the bulk discovery mechanisms, where a large number of systems can be discovered.

Note: Discovery requests are queued. If a user chooses active directory discovery and then tries to do any of the other types of discovery, then that discovery will be done after the completion of active directory discovery.

4.2 Power

AMC can monitor (current state of the system) and manage (transition the system to a new required power state) the power state of a computer system remotely. Below is the list of all possible power states, a computer system can support.

Power State	State Number	Friendly Name	Description	Corresponding ACPI State
Power On	2	On/Power On	Initiate the transition of the system to full on state.	G0/S0
Sleep – Light	3	Sleeping Lightly/Sleep Light	Initiate the transition of the system to standby or sleep state.	G1/S1 or G1/S2
Sleep – Deep	4	Sleeping/Sleep	Initiate the transition of the system to standby or sleep state.	G1/S3

[Public]

Power State	State Number	Friendly Name	Description	Corresponding ACPI State
Power Cycle (Off Soft)	5	Immediate Power Reset	Transition the system to off state in which the system consumes a minimal amount of power, followed by a transition to on state.	G2/S5 then G0/S0
Power Off – Hard	6	N/A	Initiate the transition of the system to power off state, in which the power consumption is zero except for the real-time clock.	G3
Hibernate	7	Hibernating/Hibernate	Transition the system to hibernation state. – write system context to non-volatile storage, power off the system and devices.	G1/S4
Power Off – Soft	8	Off/Immediate Power Off	Initiate the transition of the system to off state, in which the system consumes a minimal amount of power.	G2/S5
Power Cycle (Off Hard)	9	N/A	Transition the system to power off state, in which the power consumption is zero except for the real-time clock, followed by a transition to on state.	G3 to G0/S0
Master Bus Reset	10	Immediate Warm Reset	Perform hardware reset on the system.	
Diagnostic Interrupt (NMI)	11	Immediate Diagnostic Interrupt	Assert an NMI on the system.	
Power Off - Soft Graceful	12	Off/Shutdown	Perform an orderly transition to power off state, in which the system consumes a minimal amount of power.	G2/S5
Power Off - Hard Graceful	13	N/A	Perform an orderly transition to power off state, in which the power consumption is zero except for the real-time clock.	G3

[Public]

Power State	State Number	Friendly Name	Description	Corresponding ACPI State
Master Bus Reset Graceful	14	Warm Restart	Perform an orderly shutdown of the system followed by hardware reset.	
Power Cycle (Off – Soft Graceful)	15	Restart	Perform an orderly transition of the system to power off state, in which the system consumes a minimal amount of power, followed by a transition to on state.	G2/S5 to G0/S0
Power Cycle (Off - Hard Graceful)	16	N/A	Perform an orderly transition of the system to power off state, in which the power consumption is zero except for the real-time clock, followed by a transition to on state.	G3 to G0/S0

All of the above power state transitions cannot be requested remotely. The subset of the above list will be visible to the user based on the said computer system's capabilities. From AMC, the power state transitions can be requested for a single system or a group of systems.

4.2.1 Power Operation on a Single System

1. Click on any managed computer groups.
2. Right click on the specific system on which the power operation is to be performed.
3. Select 'Power' from the menu. You will get the power screen.
4. The Power Screen will show:
    a. The 'system name' against which you are going to perform the power operation.
    b. The 'current power state' of the system.
    c. The list of power states which the system can accept from its current state is shown in the 'select power state to apply' drop down list.
5. When any option in 'select power state to apply' drop down list is selected, an explanation of the power state is displayed.
6. To start the transition of the system to the new power state, click on 'Apply'.
7. The result of the operation will be shown and the user can close the power screen by clicking on 'Finish'.

[Public]

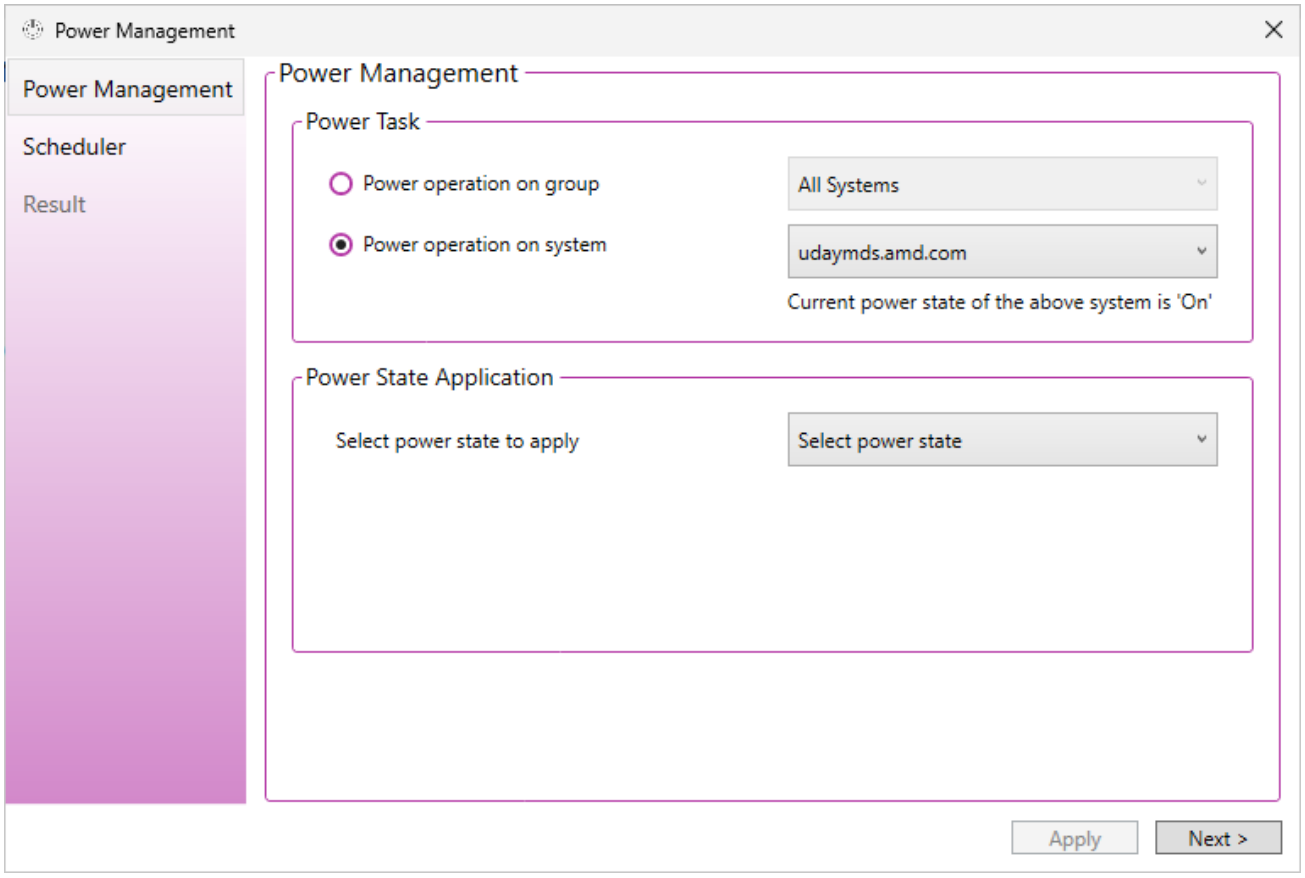
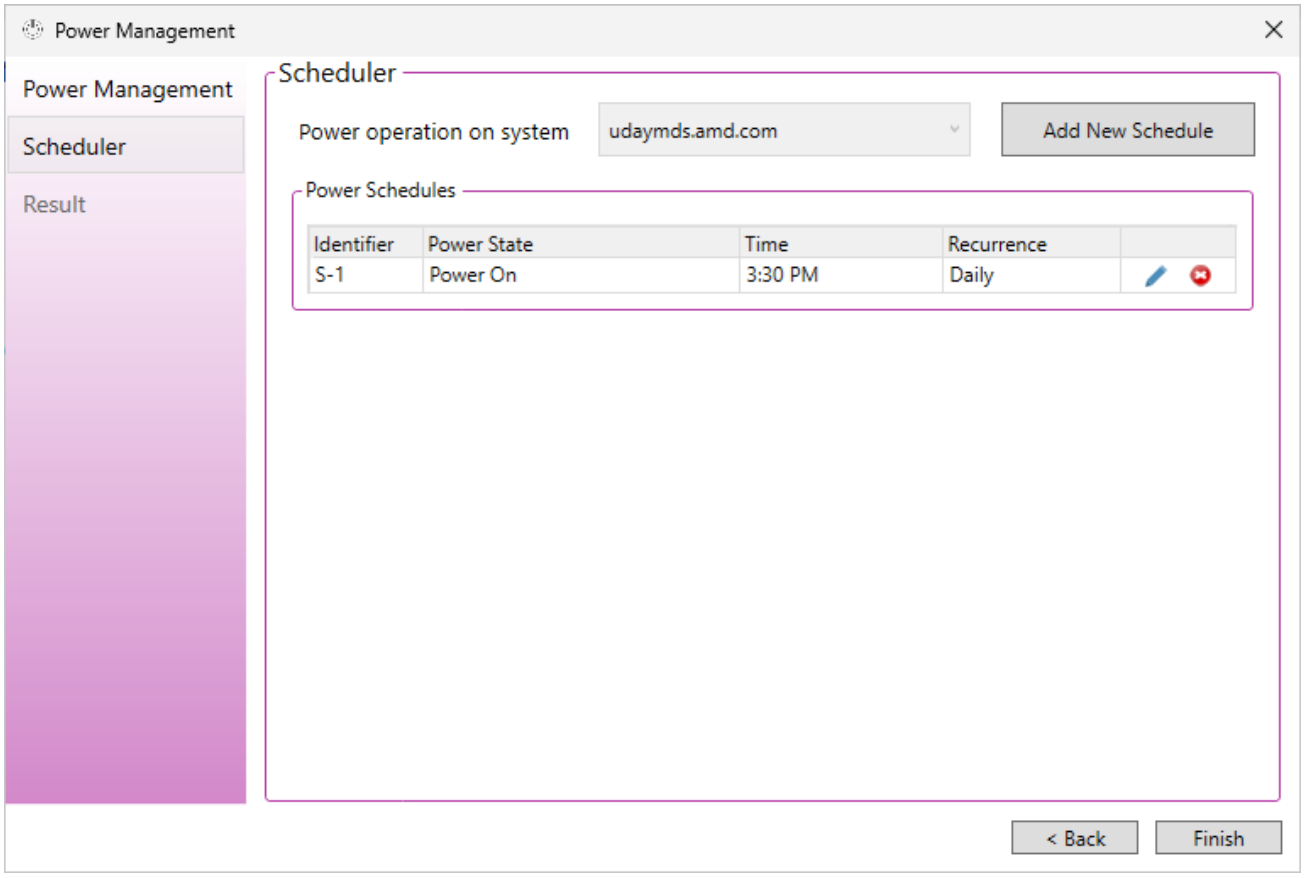


Figure 16: Power operation on a single computer system

Power scheduler

The Power Scheduler feature allows administrators to automate DASH power operations on managed systems by scheduling a desired power state at a specific time. Users can select a target device, choose the required power operation (such as Power On), and define the execution time in the scheduler. Once configured, Managed device would automatically apply the selected power operation daily at the scheduled time, eliminating the need for manual intervention and helping ensure systems maintain the desired operational state according to organizational requirements.

[Public]



4.2.2 Power Operation on a Group of Systems

1. Right click on the group against which you want to perform the power operation.
2. Select ‘Power’ from the menu to get the power screen.
3. The Power Screen will show:
    a. The ‘Group Name’ against which you are going to perform the power operation.
    b. The list of power states which all the systems in that group can accept is shown in the ‘select power state to apply’ drop down list.
4. On selecting any option in ‘select power state to apply’ drop down list, an explanation of the selected power state is displayed.
5. Click ‘Apply’ to start transition of all the systems in the group to the new power state.
6. The result screen will show that the power operation on the group has been initiated.

Close the power screen by clicking ‘Finish’. The group tasks are background tasks, and the progress of the task can be tracked at the ‘Activity Log’ area.

[Public]

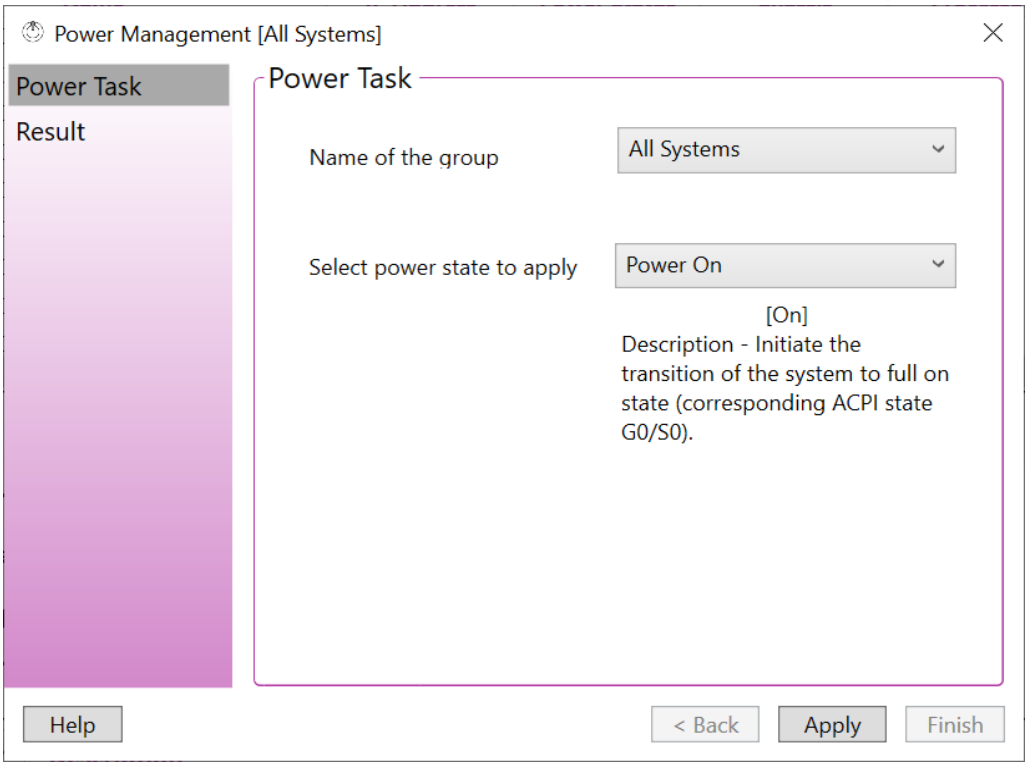


Figure 17: Power operation on a group of computer systems

4.2.3 Power Operation on a System or Group of Systems

1. Click on ‘Power’ icon in the ribbon area to get the power screen.
2. The Power Screen initiated this way will give the option to the user either to:
    a. Perform the power operation of any system in the drop down list. The default system selected would be the system which had the focus before clicking the ‘Power’ icon, but the system can be changed by the user.
    b. Perform the power operation of any group in the drop down list. The default group selected would be the group against which the focus was there before clicking on the ‘Power’ icon, but the group can be changed to a group for which a user wishes to perform the power operation.

    Select one of the above options. Note, if you select the power operation for the system then the current power state of the system selected from the drop down is informed below the drop down.
3. On selecting any option in ‘select power state to apply’ drop down list, an explanation of the selected power state is displayed.
4. Click on ‘Apply’ to start the transition of the system(s) to a new power state.
5. The result of the operation will be shown and the user can close the power screen by clicking on ‘Finish’.

[Public]

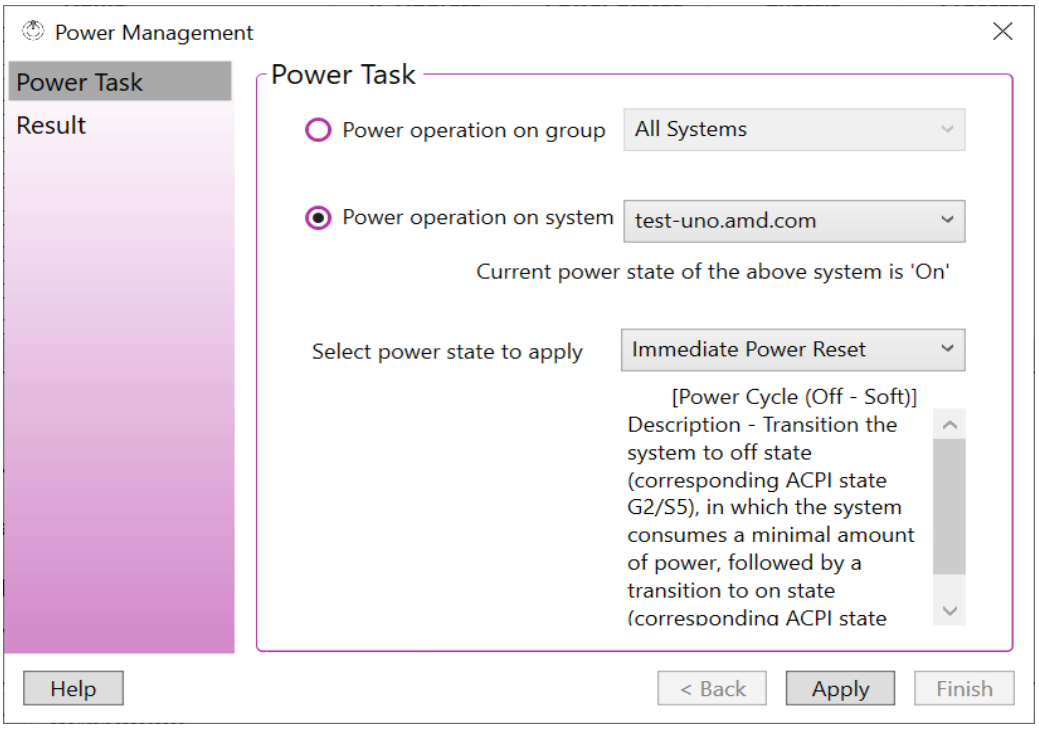


Figure 18: Power operation on either single or group of systems

[Public]

4.3 Boot

A boot configuration consists of a boot order, which specifies the order of boot devices. The boot order is used during booting.

A computer system can have one or more boot configurations. If there are more than one boot configuration for a computer system, the settings data (will it be used for next boot? will it be used only for next boot? or will it not be used for next boot?) associated with the boot configurations, is used to determine which boot-configurations and boot order should be followed during next boot process.

AMC's Boot task shows all the boot configurations available for the system being managed. For each boot configuration, it shows the current boot order and allows the user to modify the boot order if required. This version of AMC only informs the present value of the setting data (will it be used for next boot, will it be used only for next boot, will it not be used for next boot) but does not allow the user to modify this.

To perform the Boot task follow these steps in AMC:

1. Select the system on which Boot task has to be performed.
2. Either right click on the system and select 'Boot' menu item or click on the ribbon icon 'Boot'.
3. The Boot Screen appears and displays:
   a. Drop down list with all the boot configurations available for the system.
   b. Settings information for the selected boot configuration from the drop down list.
      Setting information would be one of the following:
      i. This boot configuration will be used during next boot.
      ii. This boot configuration will not be used during next boot.
      iii. This boot configuration will be used only for next boot
   c. The current boot order for the selected boot configuration from the drop down list.
4. Select the required boot configuration from the 'Name' drop down list.
5. Check on 'Change boot order' check box if the boot order needs to be changed.
6. Move the Boot Devices to the 'New boot order' list box in the order required.
7. User can change Default boot configuration by clicking checkbox and can change Next boot configuration with Next boot only configuration.
   Note: There is no need to move all the Boot devices from current boot order to the new boot order list box. If only partial devices are moved, then the actual boot order set would be with the devices set in the New order followed by other devices available in the current boot order and Next boot configuration/Next boot only configuration are not mandatory.
8. Click on 'Next' Button to have the new boot order take effect. The result screen will show the result, e.g. 'boot order was successfully changed'.
9. Close the power screen by clicking 'Close'.

[Public]

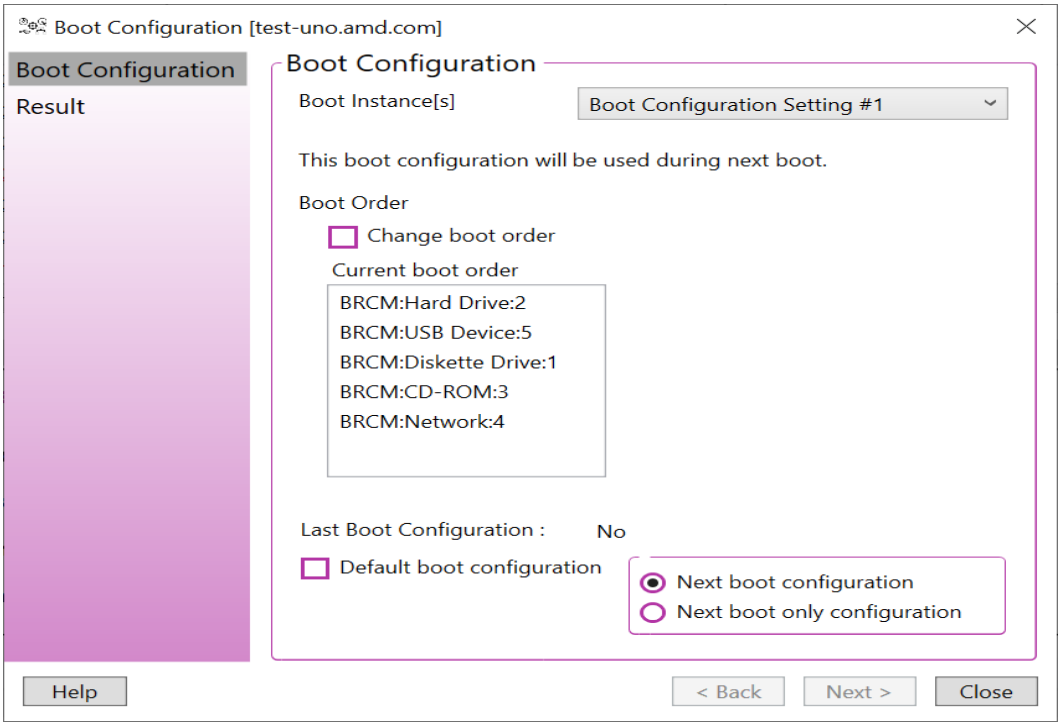


Figure 19: Boot Configuration

[Public]

4.4 Text Redirection

Text redirection provides BIOS-assisted console and keyboard redirection to a remote computer system terminal. Boot progress, BIOS setup screen, command line OS or command line diagnostic program screens are redirected to the remote terminal. AMC has a terminal screen by which IT Admin can see the console text of the managed system. The managed system can be instructed to redirect its console text to the terminal console using either Telnet or SSH launched by AMC. To perform the same follow these steps in AMC:

1. Select the system from which the text has to be redirected.
2. Either right click on the system and select 'Text Redirection' menu item or click on the text portion of ribbon icon 'Redirection'.
3. The Text Redirection Screen appears and shows:
    a. Drop down list with available protocols for text redirection, SSH and Telnet respectively. Default selection is SSH, it can be switched to Telnet if required.
    b. The Name of the Service that runs on the system to redirect the text.
    c. The port through which the text will be redirected.
    d. The information/status – e.g. Support for OTP (one time password) is stated.
4. Select the required protocol from the 'select protocol' drop down list.
5. Click on Connect.
6. If the connection is successful, the text redirection screen will close and the terminal console Screen will appear.
   Note:
    - If OTP is supported, the terminal console will connect automatically to the system.
    - If OTP is not supported, credentials will have to be entered in the terminal console. On successful authentication, text activity on the system will be redirected to the terminal console.
7. Close the terminal screen if text redirection is no more required from the said system.

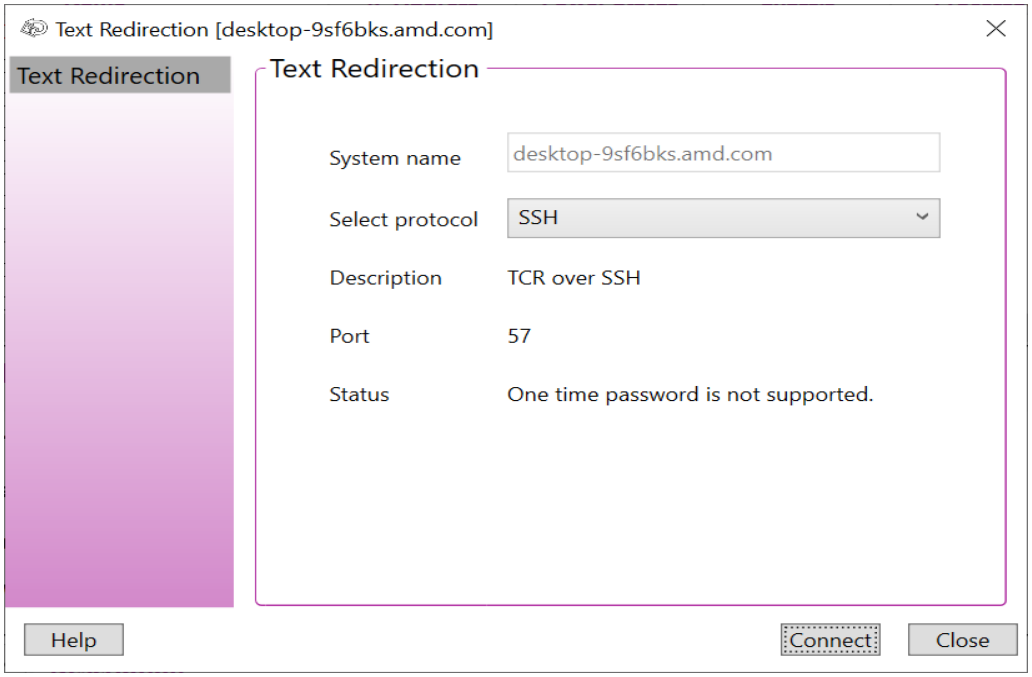


Figure 20: Text Redirection

[Public]

To view and manage the BIOS remotely from AMC:

1. Select a system for which you want to view and manage the BIOS.
2. Perform the steps 2 to 6 listed above to have the terminal console active to receive the redirected text from the system.
3. Click on Power icon and select ‘graceful power cycle’ option in the available power states. Click ‘Apply’ to change the power state.

The terminal screen launched by AMC will receive the boot screen remotely and user can interact with the remote system using the keystrokes from the AMC system.

4.5 USB Redirection

USB Redirection provides a ‘virtual’ USB device which reads data from a remote image file. This allows BIOS to boot from a remote image.

USB Redirection can be used to boot the managed systems to an image file such as .iso. The ISO Image file must be available as http web URL.

IT Admin can initiate an action to attach the managed systems USB to a remote URL. This operation can be performed against a single system or on a group of systems.

AMC has its own ISO webserver. Root folder is C:/AMC-ISO. ISOs can be placed in the mentioned folder and http:<ip of AMC console machine>:3274/<iso placed in AMC-ISO> can be used as USB URL.
e.g. *http://10.10.10.2:3274/dos.iso*

4.5.1 USB Redirection on a Single System

1. Click on any managed computer group.
2. Right-click the target system on which the USB Redirection operation is to be performed.
3. Select USB Redirection from the context menu. If the managed system supports USB Redirection, the USB Redirection window is displayed.
4. Configure the USB Redirection settings based on the supported redirection mode.

Wired USB Redirection
Below are the parameters required to start USB redirection on a Wired platform,

- Redirection url - Enter a valid URL manually which AMC can use it to create a Virtual USB drive on the selected Managed device.
- Select a previously configured ISO image or URL from the available list.

Initiate the redirection by clicking Connect.

Note:

AMC validates only the URL format. The availability and accessibility of the specified resource must be ensured by the administrator.

[Public]

Wireless USB Redirection
For systems supporting Wireless USB Redirection, AMC supports both OS USBR and BIOS USBR modes.

The USB Redirection window displays:

- Name - Hostname of the managed device.
- USB Redirection Name - USB redirection profile configured on the target system.
- Element Name - Unique USB redirection instance identifier.
- Connection Mode - Current redirection mode.
- Enabled State - Current operational state.
- USBR Type:
    - OS USBR - Redirects USB media while the operating system is running.
    - BIOS USBR - Redirects USB media during BIOS environments, this option would be used for installing Windows on the selected Managed device.

The administrator can choose one of the following media sources:

1. USB Device
   Redirect an already mounted ISO device or a physical USB storage device connected to the AMC host system. Select the required device from the USB Device drop-down list.

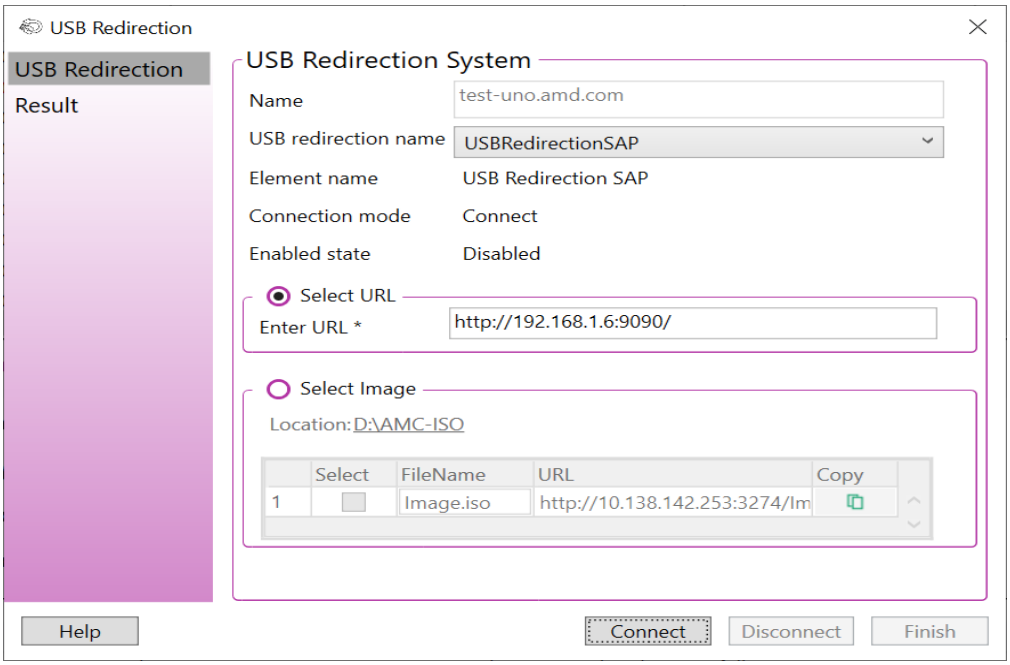
2. Select Image (*.iso)
   Browse and select an ISO image file.
   AMC mounts the selected ISO image on the AMC host system and redirects the mounted media to the managed endpoint.

Additional settings:
SSH Key - Specify the SSH private key used to establish secure communication required for Wireless USB Redirection operations.

Once all required details are chosen, Connect button would be enabled, so user can click Connect to initiate USB Redirection.
To terminate an existing session, click Disconnect.
Click Finish to close the USB Redirection window.

Note: Successful USB Redirection depends on platform support, network connectivity, valid credentials, and accessibility of the selected USB device, ISO image, or URL.

[Public]



USB Redirection on a Wired platform

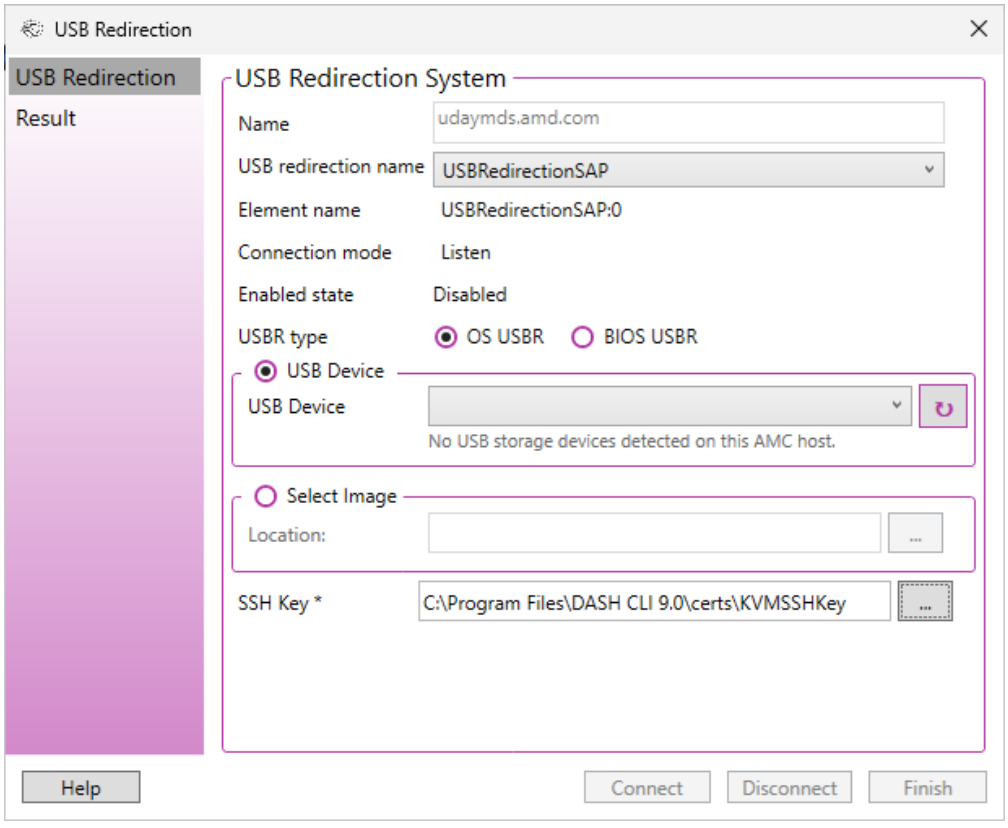


Figure 21: USB Redirection on a Wireless platform

[Public]

4.5.2 USB Redirection on a Group of Systems

1. Right click on the group against which the USB redirection operation is to be performed.
2. Select 'USB Redirection' from the menu. USB Redirection screen will be displayed.
3. The USB Redirection Screen will allow:
   a. To select the group for whose system's AMC is going to attach the remote URL. The user can change the group against which the USB Redirection operation is to be performed.
   b. To enter a new valid URL that can be attached to the USB of the systems in the selected Group or select URL from next grid which already mapped based on folder.

   A template and example in the right format is shown below the URL entry. AMC only validates the URL format. The existence of the URL and accessibility of the URL by the managed target has to be ensured by the user and outside the scope of AMC.
4. User can either:
   a. Click 'Connect', the entered URL would be attached to the USB of the systems in the selected group.
      Or
   b. Click 'Disconnect', to detach the URL for the USB of the systems in the selected group.
5. The result screen will show that the requested group operation was initiated. Close the power screen by clicking on 'Finish'. Note that all group tasks are background tasks, and at the 'Activity Log' area its progress can be tracked.

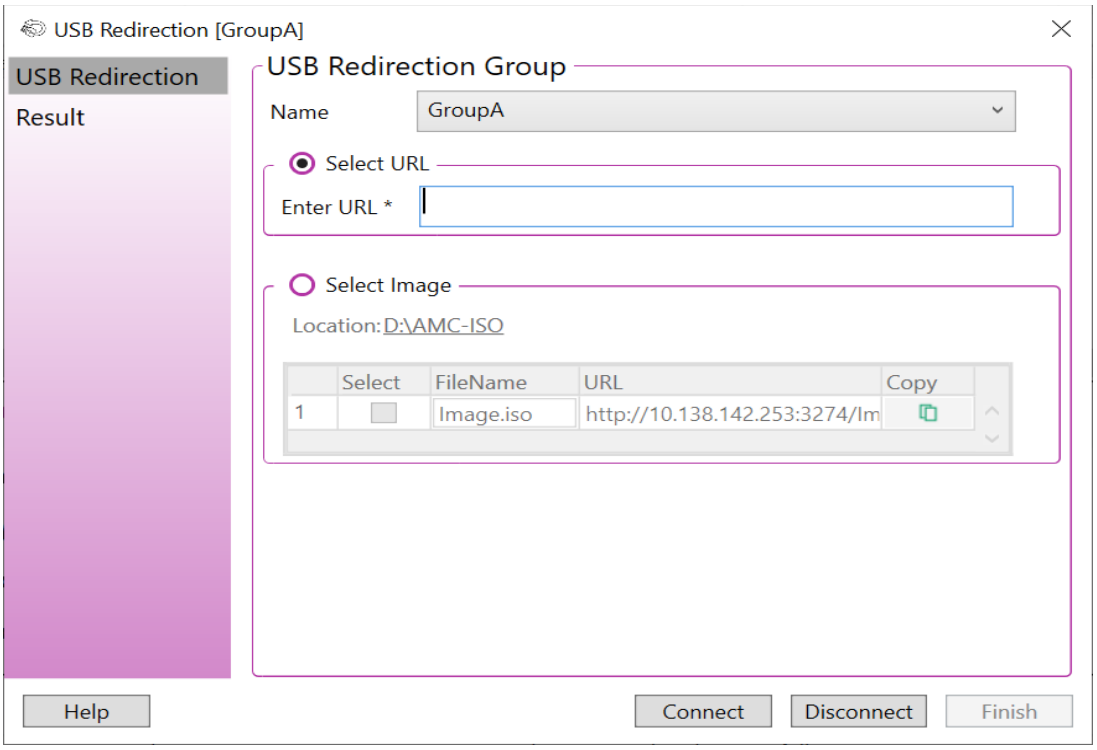


Figure 22: USB Redirection on a group of systems

[Public]

4.5.3 USB Redirection on a System or Group of Systems

1. Click on USB ‘Redirection’ icon in the ribbon area. A USB redirection screen will appear.
2. The USB Redirection Screen initiated in the above way will give the option to the user either to:
   a. Perform the USB redirection operation of the system which had the focus before clicking the USB ‘Redirection’ icon
   b. Or, Perform the USB redirection operation for any group in the drop down list. The default group selected would be the group against which the focus was there before clicking on the USB ‘Redirection’ icon, but user can change the group against which he wishes to perform the USB redirection operation.
3. System is selected if:
   a. The USB of the system selected is already attached to the remote URL then the attached URL will be shown, and the option to either modify through ‘Modify’ check box or disconnect by clicking ‘Disconnect’ is available to the user.
   b. The USB of the selected system is not attached. The user can replace/update any existing URL or enter a new valid URL and click on ‘Connect’.
4. If Group is selected, the user can choose from either of the below:
   a. Click ‘Connect’, so the entered URL would be attached to the USB of the systems in the selected group.
   b. Or. Click ‘Disconnect’, to detach the URL for the USB of the systems in the selected group.
5. The result of the operation will be shown and the user can close the USB Redirection screen by clicking on ‘Finish’.

A template and example in the right format is shown below the URL entry. AMC only validates the URL format. The existence of the URL and accessibility of the URL by the managed target has to be ensured by the user and outside the scope of AMC.

[Public]

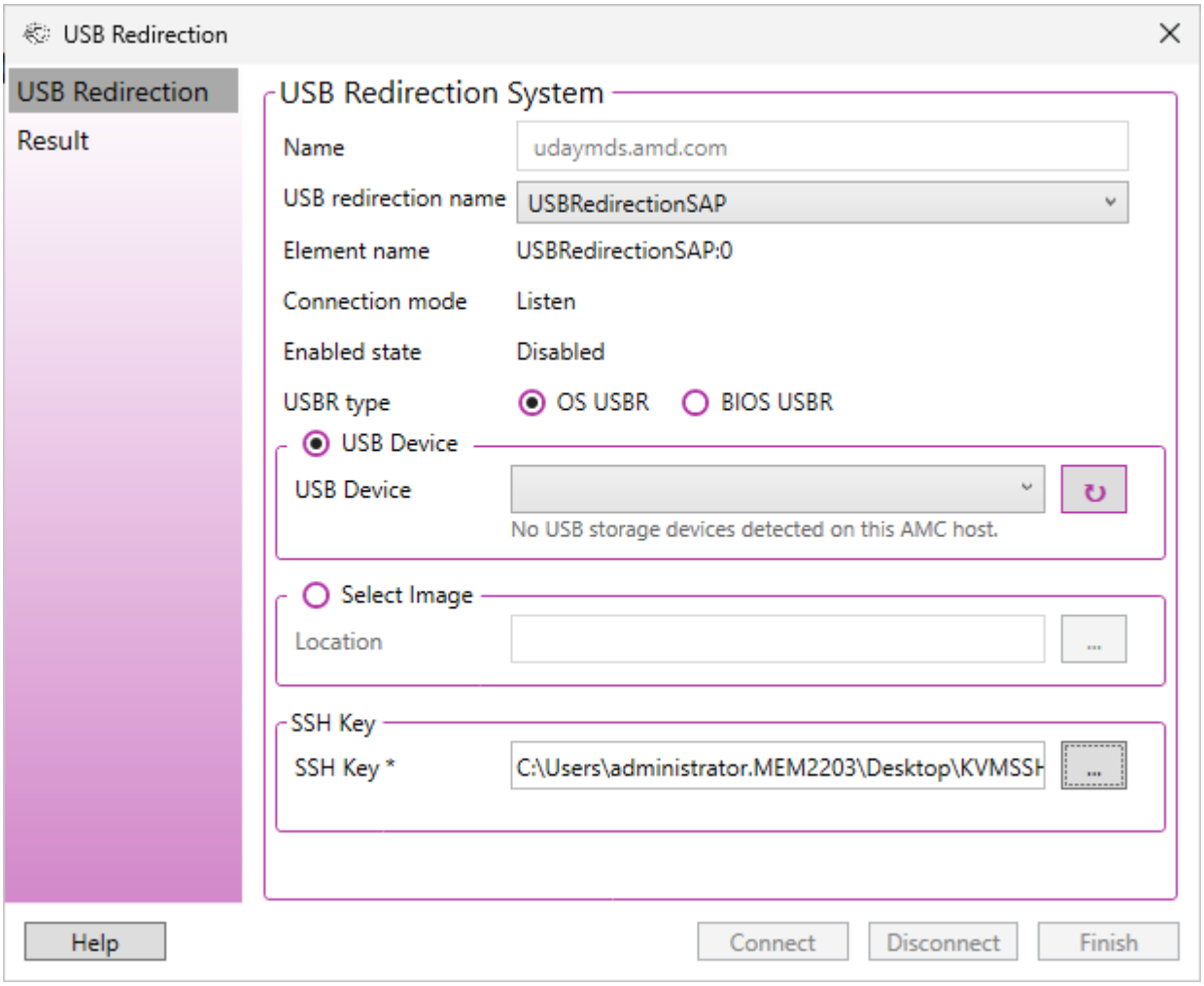


Figure 23: USB Redirection on a single or group of systems

4.6 KVM Redirection

KVM Redirection implements the DMTF DASH KVM profile and provides the workflow where user can boot the managed system to the OS screen and remotely connect to the Target OS screen via the VNC viewer. User can switch to BIOS screen by manually rebooting the target to BIOS.

Through the VNC viewer, the user can access the OS/BIOS screen and interact with mouse & keyboard.

1. Select the system for which KVM is to be initiated.
2. Either right click on the system or select ‘KVM Redirection’ menu item or click on the ribbon icon ‘KVM.

When the user starts the KVM workflow by clicking the Start button, the following tasks are initiated:

1. KVM enable command is sent to the managed system.
2. Once Managed system is ready with the VNC server, VNC viewer is launched.

[Public]

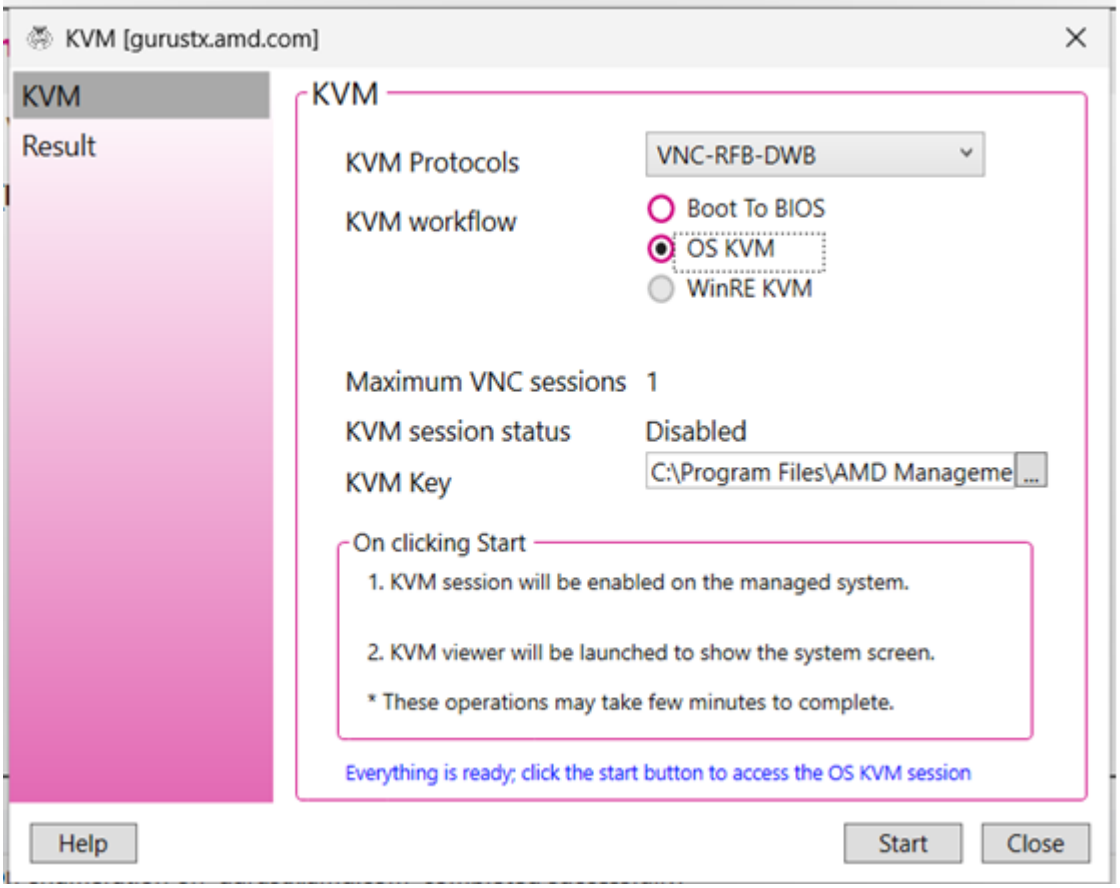


Figure 24: KVM Redirection

Figure below shows the OS screen of Target system:

[Public]


AMD KVM Viewer: 10.86.13.162
fn
Ctrl
Alt
Del
AMD Ryzen 5 36
AMD
RYZE

[Public]

Figure 25: VNC viewer showing OS Screen of DASH Target

4.7 Alerts Subscription/Un-Subscription

AMC can subscribe to alerts generated by the managed systems. The types of alerts are platform, boot-progress and lifecycle events. These events include temperature alerts, fan failure, chassis intrusion, ProcHot, ThermTrip, and BIOS boot failure. AMC shows:

i. List of available alerts that the managed system can send.
ii. List of alerts that the managed system is already subscribed to.

IT Admin can use AMC to modify the subscribed list.

1. Select the system for which alerts has to be monitored /managed.
2. Either right click on the system and select 'Alerts' menu item or click on the ribbon icon 'Alerts'.
3. The Alert Screen will be displayed
   a. Available filters as a list box in the left. This is a list of events that this system is capable of sending.
   b. Subscribed filters as a list box in the right. This is a list of events for which the Subscription is already in place.
4. For Subscribing, select any item in the 'Available filters' list and Click on the → arrow to move the item to the 'Subscribed filters' list.
5. For Un-Subscribing, select any item in the 'Subscribed filters' list and Click on the ← arrow to move the item to the 'Available filters' list.
6. Once all the changes are done, click 'Apply'. On occurrence of an event for which subscription exists, the managed system will send an alert to AMC which will be displayed as mentioned *here*.
7. The result of the operation will be shown and the user can close the Alert Subscription/Un-Subscription screen by clicking on 'Close'.

[Public]

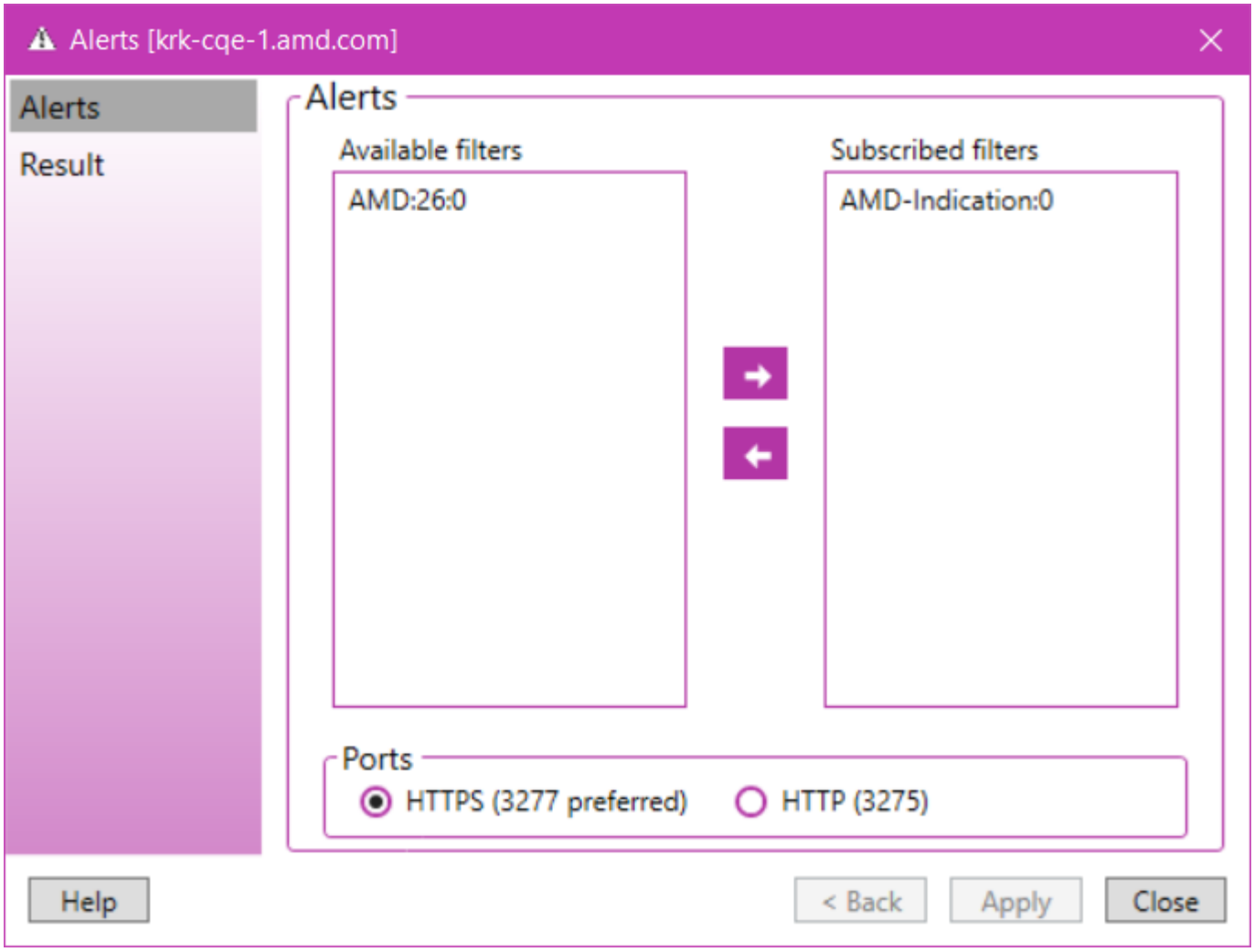


Figure 26: Alert Subscription / Un-Subscription

4.8 Health

AMC shows the health of a managed computer systems by way of displaying sensor information.
The sensors shown are temperature and fan.
To monitor the health of system:

1. Select the system for which the health has to be monitored.
2. Either right click on the system and select ‘Health’ menu item or click on the ribbon icon ‘Health’.
3. The Health screen will show a tree view of all the sensors and fans in the system in each node. Each node in the high level view will contain:
    a. The Name of the sensor or fan.
    b. The present health state of the sensor in braces.
4. If the present state is not normal, then to know more details expand the tree and view the present reading etc.
5. To see details of all sensors click on the ‘Expand All’ icon.
6. To close the health screen click on OK.

[Public]

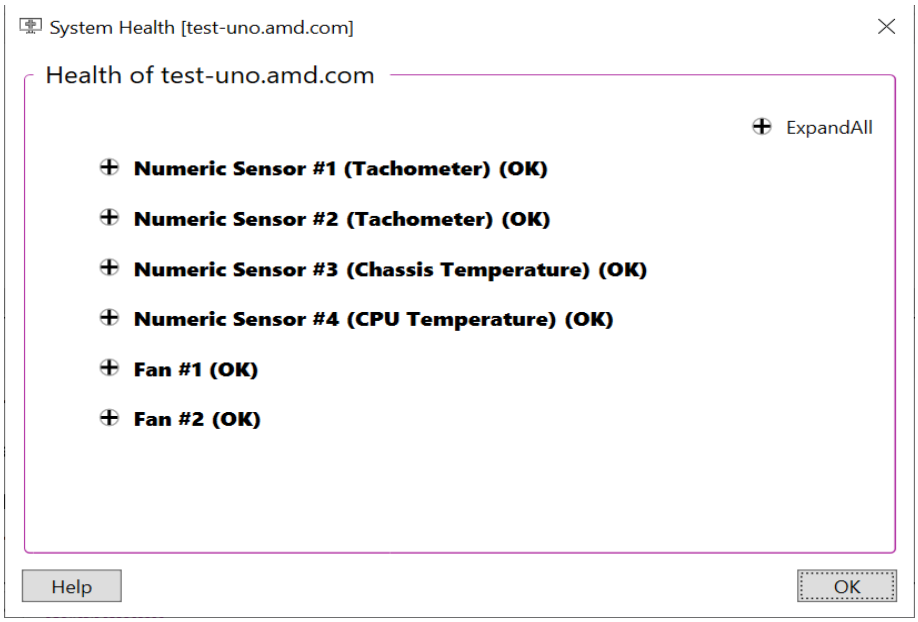


Figure 27: Health of a Computer System

4.9 Properties of the System

AMC supports global configuration, with three authentication entries and choice for management transport and management port. AMC provides a screen through which user can infer the configuration that is being used for a particular target in question.

1. Select the system for which the properties has to be viewed.
2. Right click on the system and select ‘properties’ menu item.
3. The Properties screen will show up as in Figure 28.
4. To close the properties screen click on OK.

[Public]

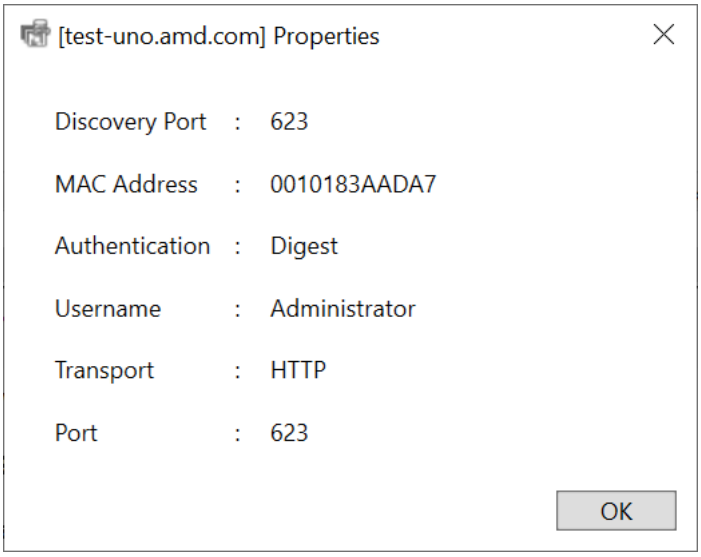


Figure 28: System Properties Screen

4.10 Inventory

Refer *here*.

4.11 Alert Reception

AMC is capable of receiving the alerts when an alert-able event is triggered in the managed system. In AMC, alerts are subscribed / unsubscribed as mentioned in the *Alerts Subscription/Un-Subscription* section. The received alerts are displayed as mentioned in the *Activity Log & Alerts* section.

[Public]

4.12 Log Entry Profile

The managed DASH systems are capable of maintaining log files such as for example, a log file for all events that are generated.

AMC can read log files maintained by the managed DASH computer system, if available. Users can navigate the log screen using the provided controls.

1. Select the system for which the Log Entries has to be viewed.
2. Either right click on the system and select 'Log Entry' menu item or click on the ribbon icon 'Log Entry.
3. The Log Entry screen displays the latest 20 log entries. The navigation buttons on the screen allow users to view all the log entries for the selected device.
4. When the user double clicks on a log entry, a separate popup window is launched which displays log entry in detail.
5. The navigation buttons on the screen are **Previous** and **Next** which navigate to the older and newer log entries in the Log Entry, and updates the fields in the pop up screen.

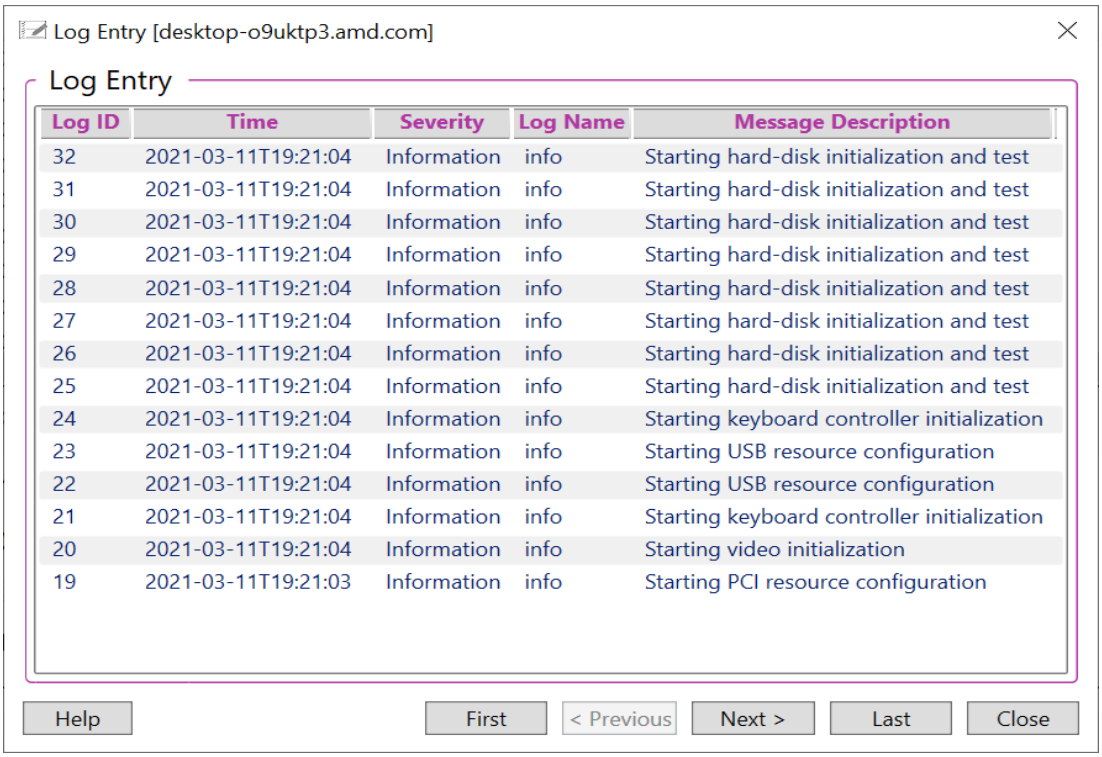


Figure 29: Record Log

[Public]

4.13 Boot to Text Image

Boot Text Image feature provides an environment where user can boot the managed system to a user defined text based remote image (e.g. .iso image).

The screen allows the user to specify the remote image (.iso) file in the web URL format.

1. Select the system for which Boot to text image has to be initiated.
2. Either right click on the system and select 'Boot to text image' menu item or click on the ribbon icon 'Boot to text image'.

When the user start deploying text image by clicking the Start button, the following tasks are initiated:

1. A SSH session with the remote managed system is established to provide an environment to control and monitor the managed system. Note that this environment is text only environment, so text only screens are visible.
2. The ISO image specified in the URL is attached as an image in USB device or select Image from File Explorer.
3. Boot order of the managed system is changed to 'USB' device as first Boot device.
4. Power reset is performed on the managed system.
5. The managed system boots to the URL image and the boot process can be seen in the SSH terminal session.

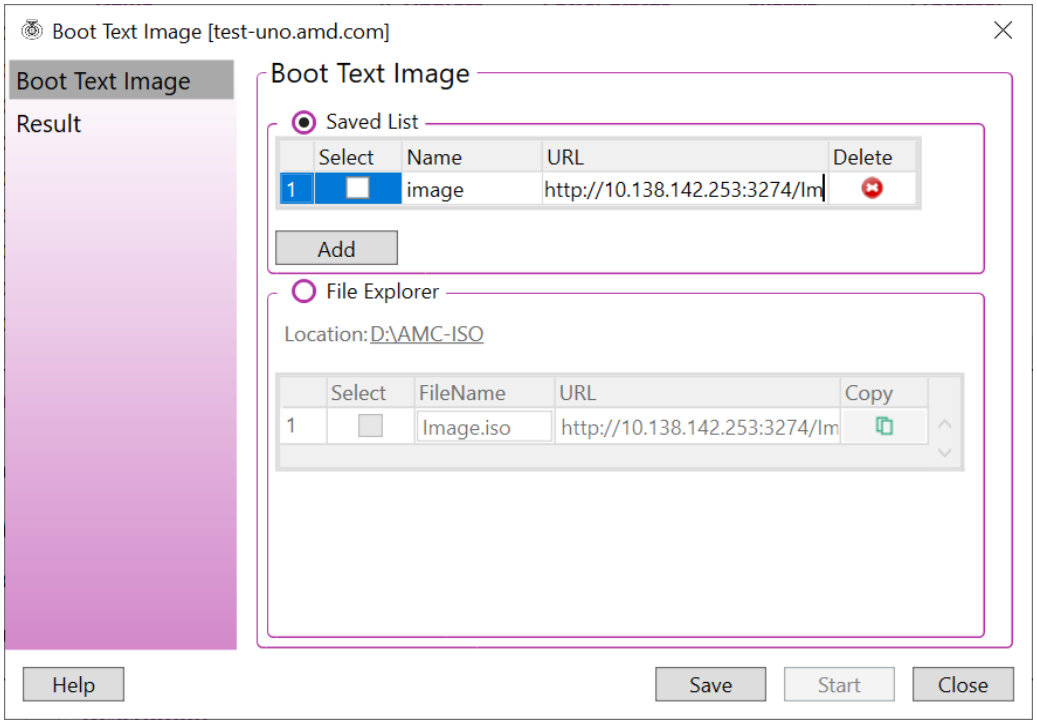


Figure 30: Boot Text Image

Note: After successfully booting to a remote image file, the boot order of that particular remote system will be changed to '*USB*' as first boot device. So, after the terminal session is completed, perform these steps on the DASH system to bring it back to original state:

- Disconnect USB using USB Redirection screen

[Public]

- Change boot order to original state

In the Boot Text Image screen,

- Grid shows list of URLs with Name associated with a Select checkbox to select a URL that user intends to boot the managed system to. User can use the Delete button to delete the URL.
- User can click on Add (+) button to add new URL to list.
- User has to click the Save button to save the list of URLs.
- User has to click on the Start button to initiate deploy to text image task.

Note:

- Clicking 'Start' button won't save the list. URL list has to be saved by clicking 'Save' button.
- If an URL is already connected, that URL is shown as checked in the URLs list.
- User can save up to 10 URLs in the list.

Figure below shows the remote console after booting to the DOS image:

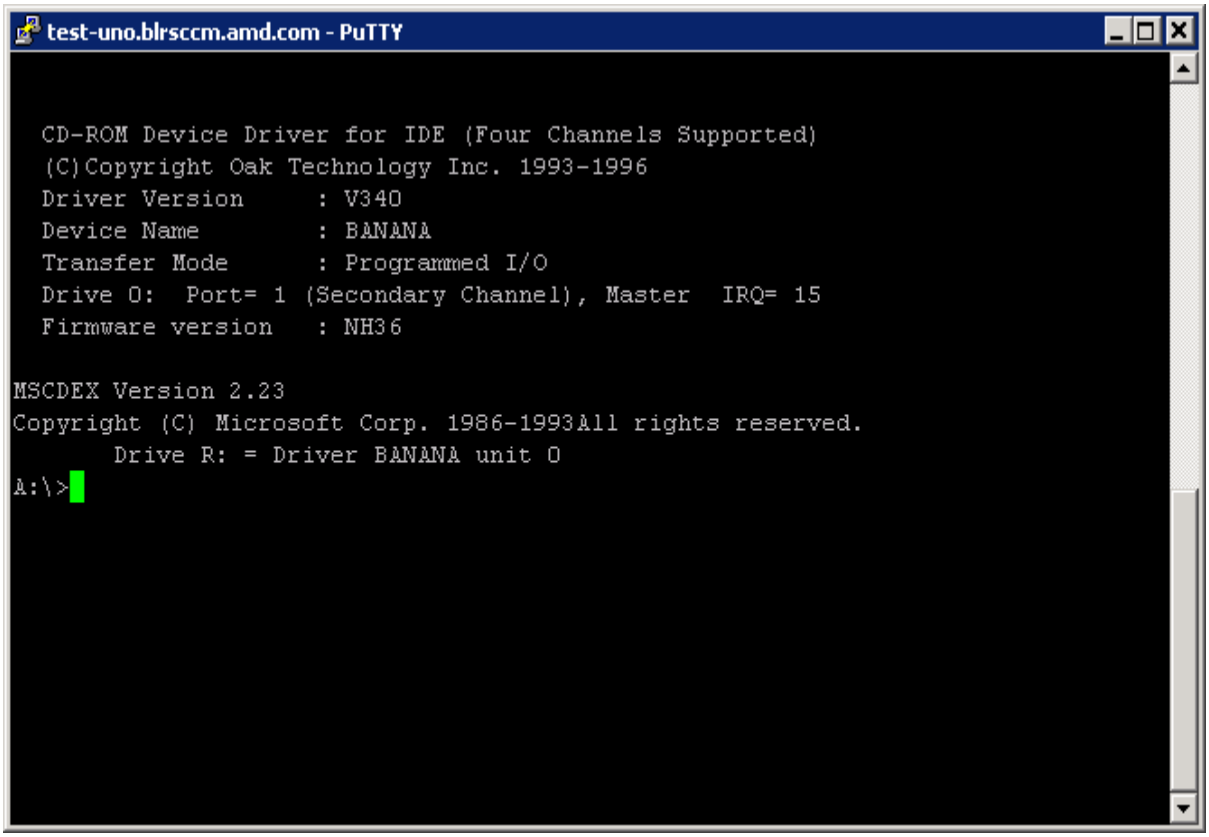


Figure 31: DOS Image

4.13.1 Sample Use Cases

DISCLAIMER: *The use cases shared here are for representation purpose only and do not form a part of any agreement or legal binding on part of company. Shown views are not a part of the actual deliverables. The product and technology displayed if any, or referred to is for representation only and AMD does not guarantee the use of all of them. Consult your own technology advisor with respect to your situation. In no event shall*

[Public]

AMD be liable for any direct, indirect, special, incidental, or consequential damages arising out of the use of the information herein. Test these applications in a controlled environment before trying on production.

Case 1: Hiren's multipurpose Boot CD

Hiren's BootCD is a boot disk utility which is packaged with various tools to run diagnostic and monitoring tests to troubleshoot PC. Utilities such as disk partition tools, recovery tools, network tools, backup tools, testing tools, system information tools can found in the package.

Download link: *http://www.hirensbootcd.org/download/*

When you download, file will be in *zip* format. Extract the zip file into a folder using any third party softwares like *7-zip* or *WinRAR*. Then create the image as *.iso* using tools such as *MagicISO* or *UltraISO*.

Hiren's multipurpose Boot CD is deployed via 'Boot Text Image' and below is the boot screen after it has deployed. From this screen various tools can be selected and run on the remote system.

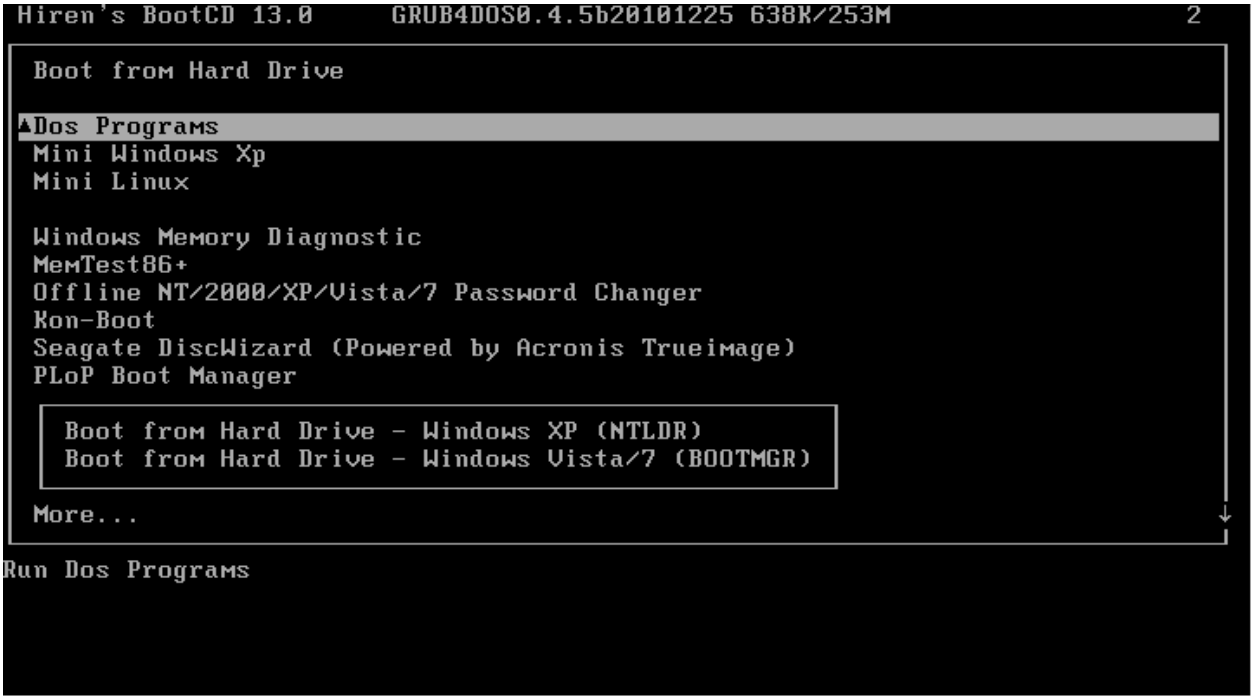


Figure 32: Boot to Dos Image

[Public]

4.14 Firmware Upgrade

This feature allows you to update the firmware on selected devices Firmware Update on Device.

AMC allows you to update the firmware for any device.

1. Select the system for which firmware update has to be initiated.
2. Either right click on the system and select ‘Firmware Upgrade’ menu item or click on the ribbon icon ‘Firmware Upgrade’.
3. From the Software Module drop-down list, select the required Software module.
4. To update the firmware of the collection of devices, select the checkbox next to the managed system you wish to update, and click on the Apply button to initiate Firmware update on the device.
5. To delete a URL, click the Delete button next to the device URL.
6. To add a new firmware URL to the list, click the Add (+) button or select URL from File Explorer.
7. After you are done adding or removing devices, click the Save button to save the list of Firmware URLs.

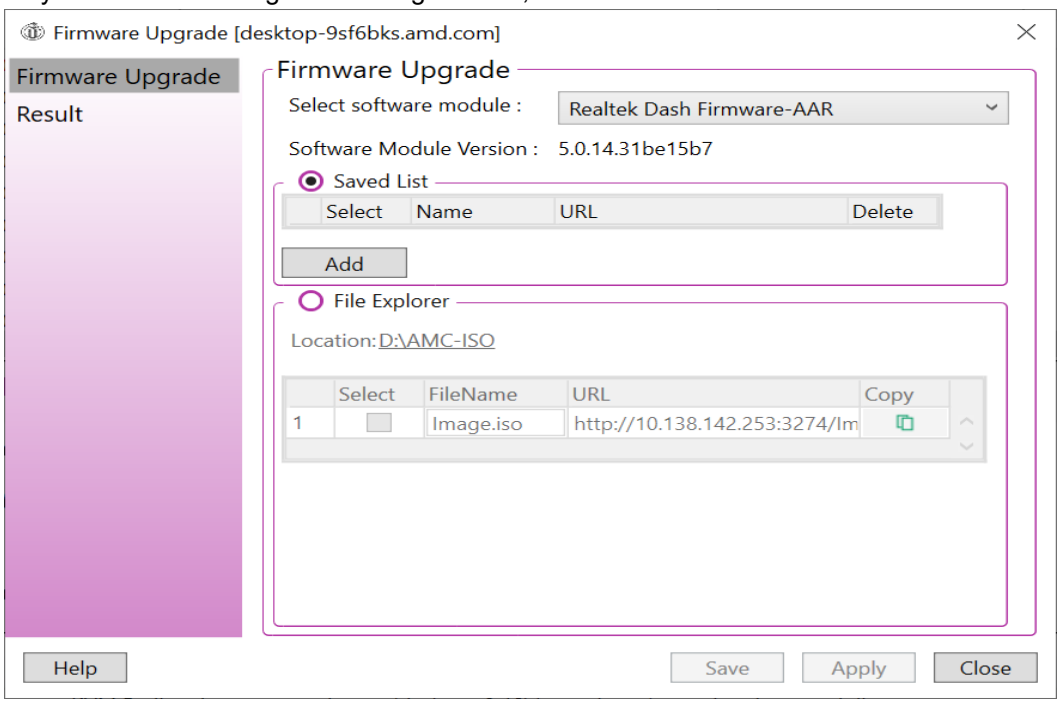


Figure 33: Firmware Upgrade

Note:

- Clicking **Apply** button won’t save the list. To save the URL list, click the **Save** button.
- Up to 10 Firmware URLs can be saved in the list.

4.15 Boot to BIOS (KVM Profile)

Boot to BIOS implements the DMTF DASH KVM profile and provides the workflow where user can boot the managed system to the BIOS setup screen, and remotely connect to the BIOS screen via the VNC viewer.

Through the VNC viewer, the user can access the BIOS screen and interact with mouse & keyboard.

3. Select the system for which Boot to BIOS has to be initiated.

[Public]

4. Either right click on the system or select ‘Boot to BIOS’ menu item or click on the ribbon icon ‘Boot to BIOS image’.

When the user starts the Boot to BIOS workflow by clicking the Start button, the following tasks are initiated:

3. KVM enable command is sent to the managed system.
4. The managed system is rebooted.
5. After the managed system boots to BIOS setup screen and once the VNC server is ready, VNC viewer is launched.

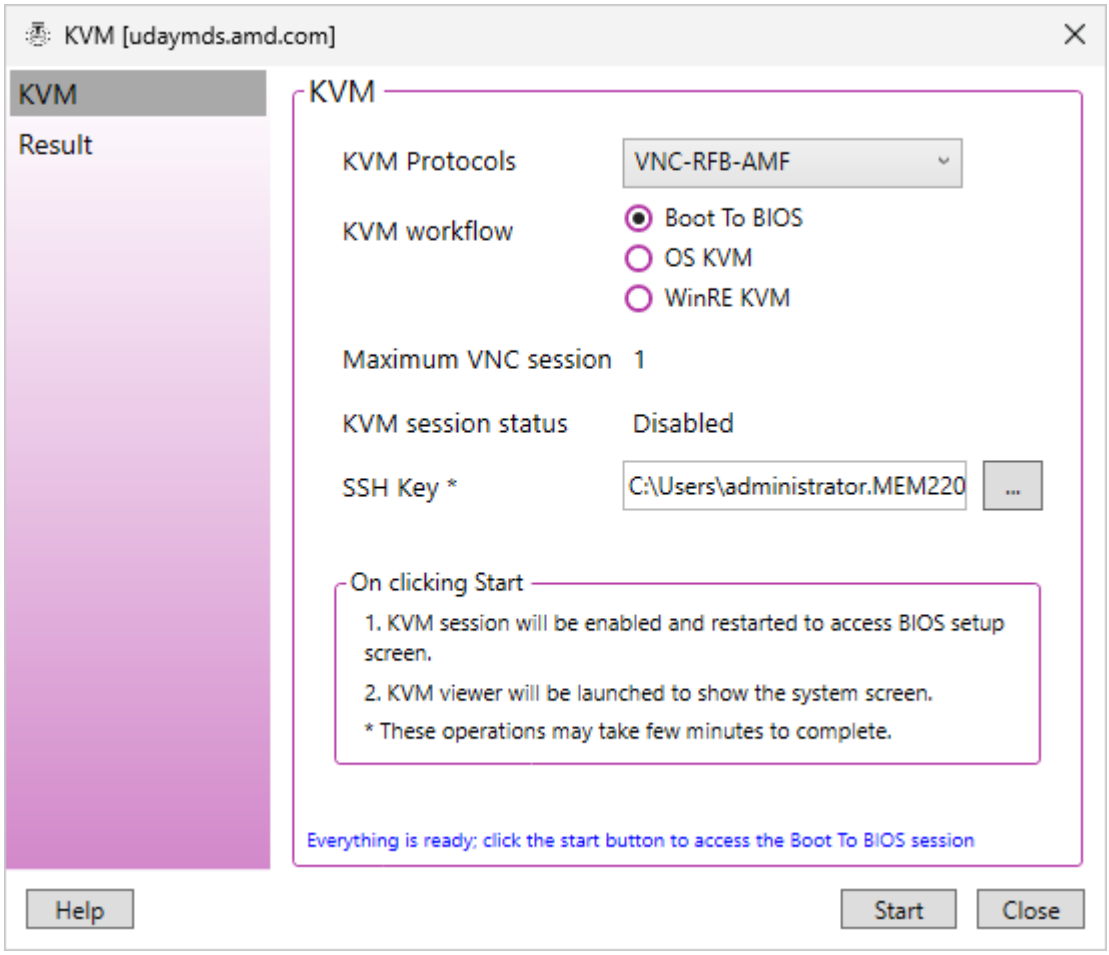


Figure 34: Boot to BIOS

Note

- Connecting to VNC server might take some time, since the managed system has to be rebooted.
- When the VNC Viewer is closed, the managed system is rebooted.

[Public]

Figure below shows the BIOS setup screen:

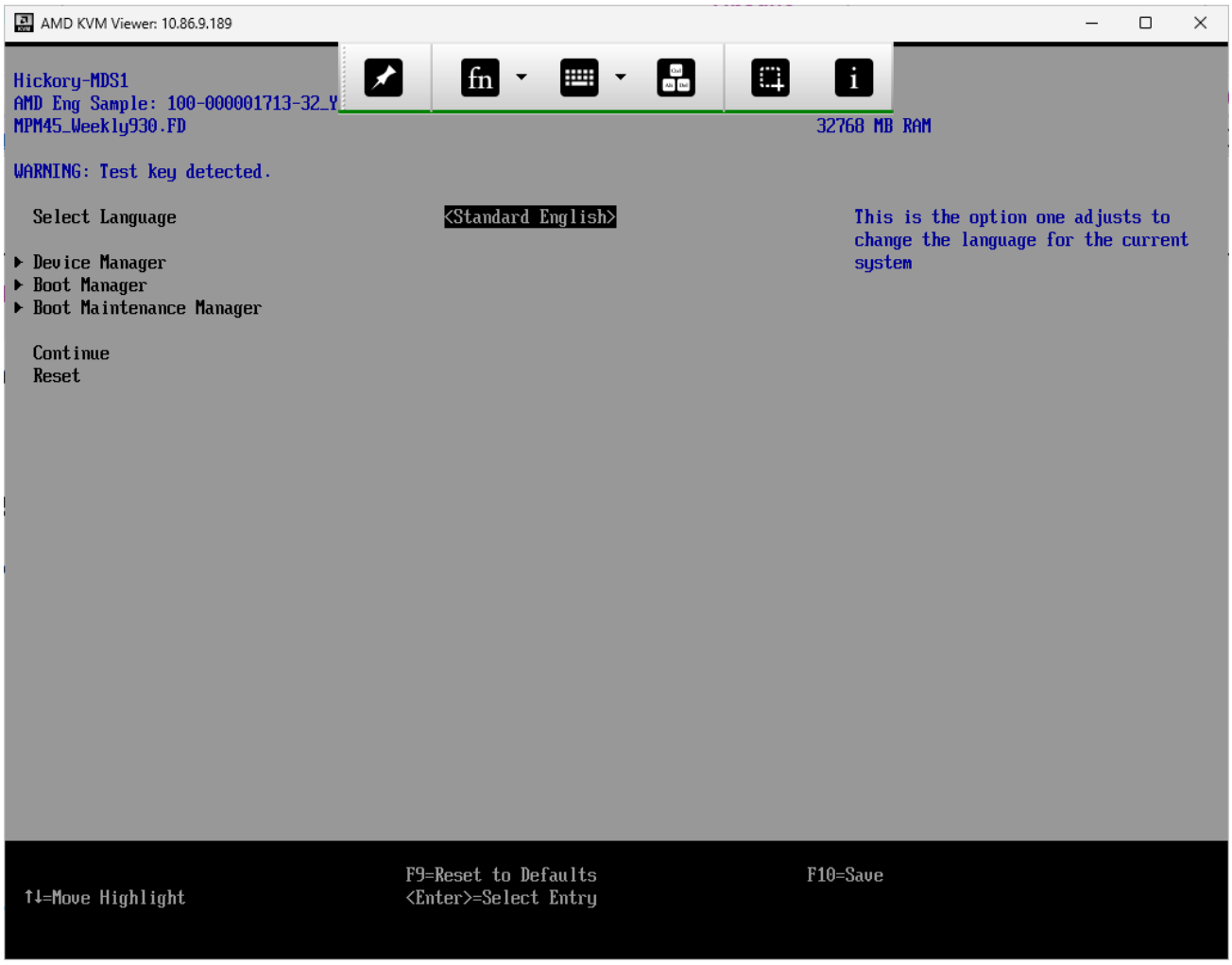


Figure 35: BIOS Setup Screen

4.16 Opaque Management Data

Opaque Management Data extends the management capability of referencing profiles by adding the capabilities to create, manage, use and delete the opaque management data objects. User can create an opaque management data object and store required text in it persistently. User can specify the Element name, Text/Data to be stored and limit of data that it can hold as shown in the below screenshot.

[Public]

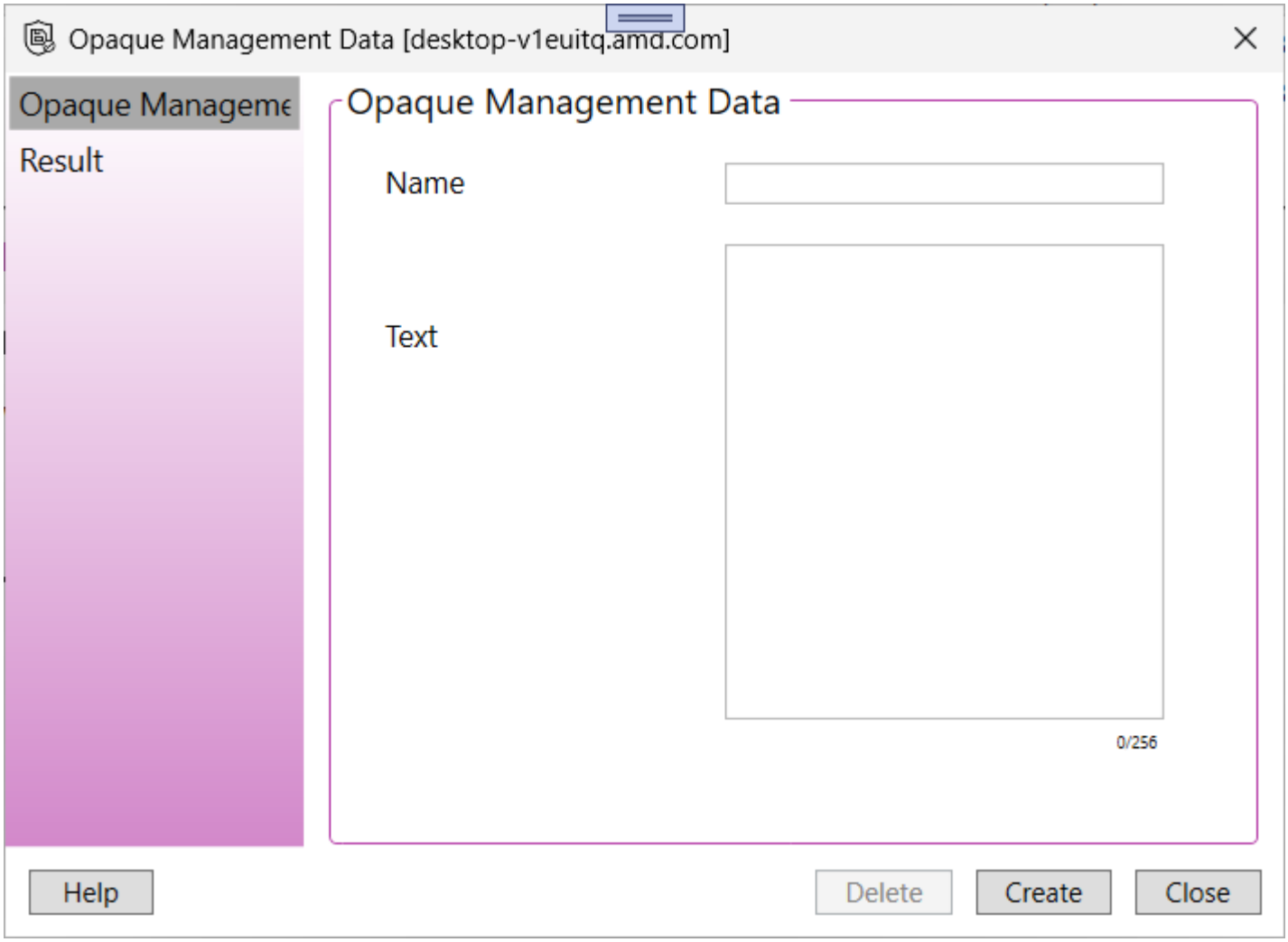


Figure 36: Opaque Management Data

4.17 Unown

AMC supports unowning a device by deleting all the provisioning data on a Managed system. System will become unmanageable through DASH after performing this operation.

[Public]

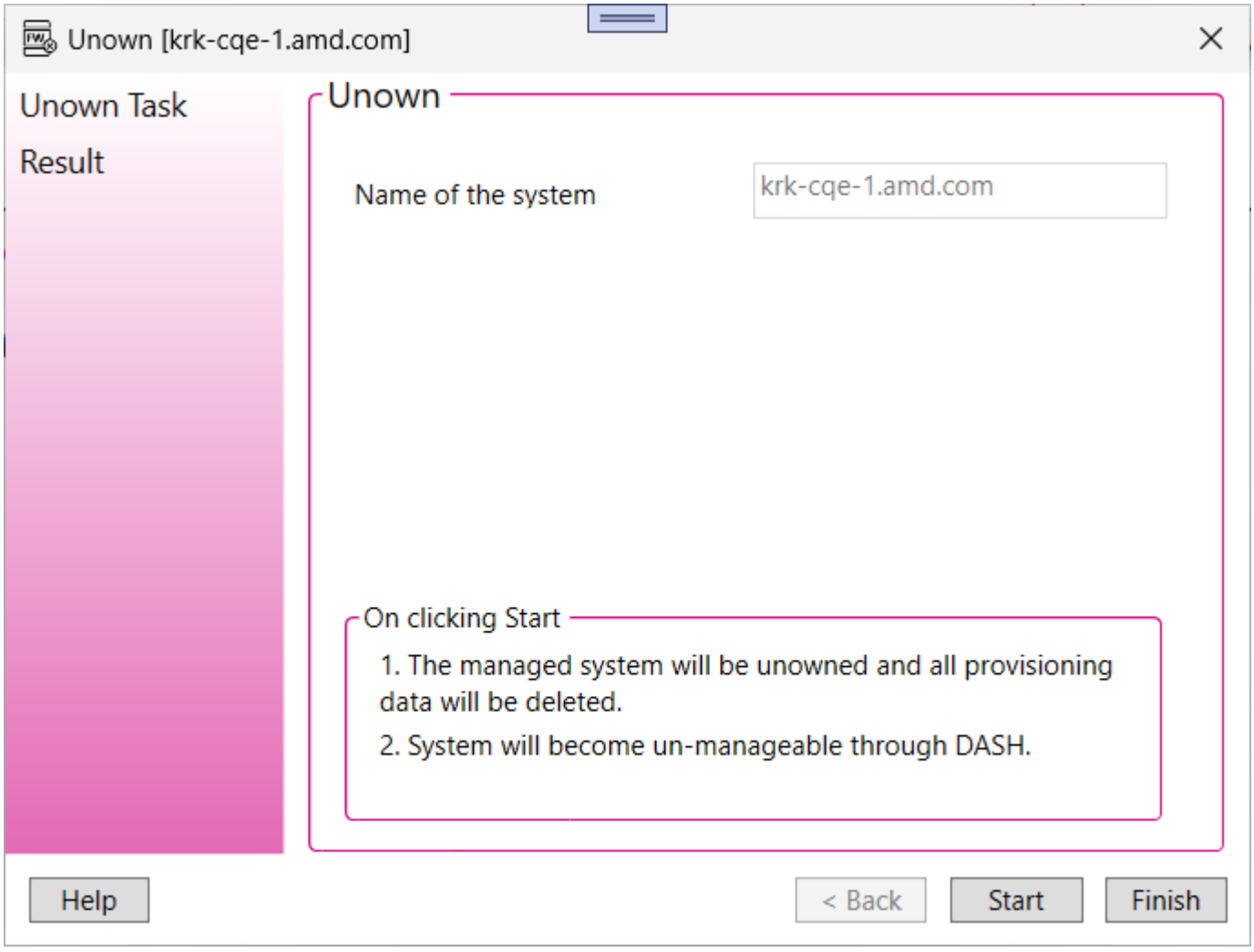


Figure 37: Unown

Note: Target system needs to be restart to complete the unown operation.

[Public]

4.18 Disk Wipe

AMC supports Disk Wipe by deleting all the contents of the selected disk.

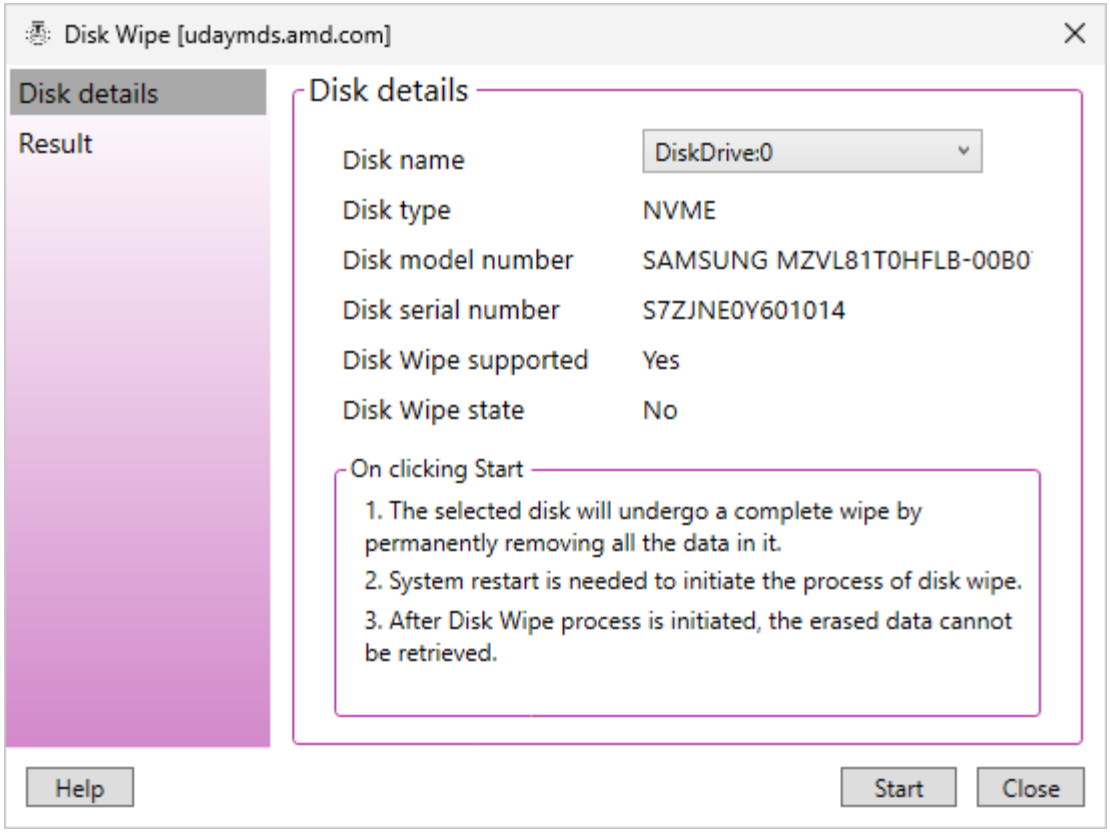


Figure 38: Disk Wipe

Note:

1. Warning: Following a disk wipe, if an operating system was previously installed on the disk, the system will be unable to boot into the operating system. It will be necessary to reinstall the OS.
2. Disk Wipe is supported only in AIM-T supported system with version 5.0 and above.
3. Power restart is needed to initiate Disk Wipe after enabling Disk Wipe.
4. This feature is typically utilized during the process of system decommissioning.

4.19 Remote Access

Remote Access feature provides support for launching of In band KVM and Remote Desktop tools.

To use In band KVM feature, ensure the relevant Windows driver package released by the network interface provider is installed on the DASH system.

Through the VNC viewer, the user can access the Target screen and interact with mouse & keyboard.

1. Select the system for which Remote Access has to be initiated.
2. Click on the ribbon icon Remote Access to initiate the process.

[Public]

When the user starts the Remote Access workflow by clicking the Start button, the following tasks are initiated:

In-Band KVM

1. Once Clicked on Start Target Screen will open once the VNC server is ready, VNC viewer is launched.

Disclaimer: In band KVM feature is supported by respective ethernet network interface provider. For Realtek based DASH systems, contact nicfae@realtek.com

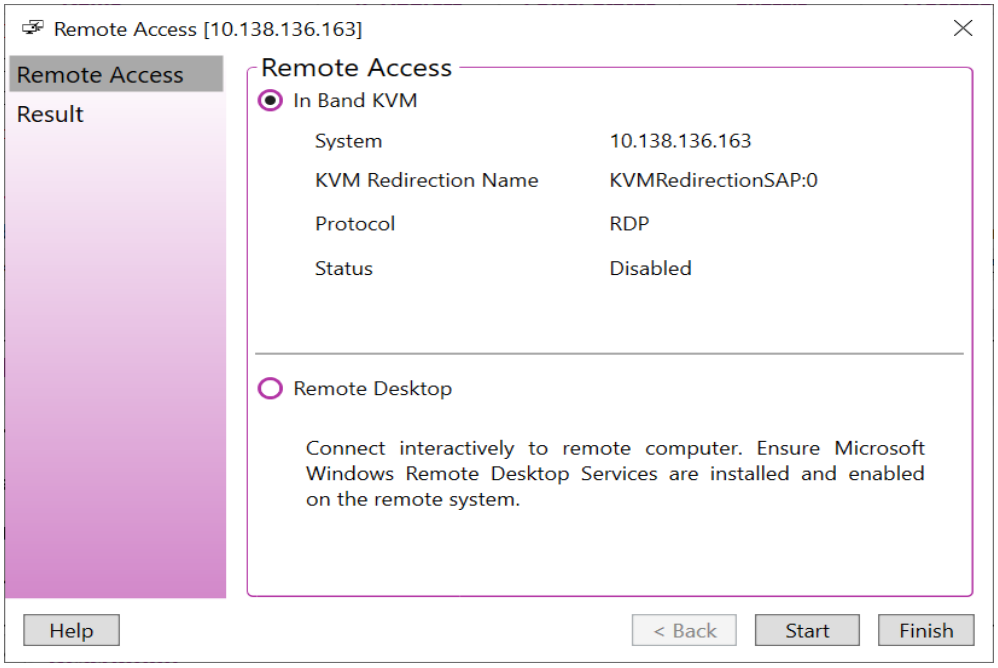


Figure 39: Remote Access In Band KVM Selected

Remote Desktop

1. Once Clicked on Start Target Screen will open once when Remote Desktop is launched.

Remote Desktop enables the user to remotely log into the DASH system, which has the Windows terminal services server. The user is presented the desktop interface (or application GUI) of the remote system, as if it were accessed locally. The user might require regular Windows username/password for connecting to the remote system, For more details, visit the Remote Desktop link: *https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access*.

[Public]

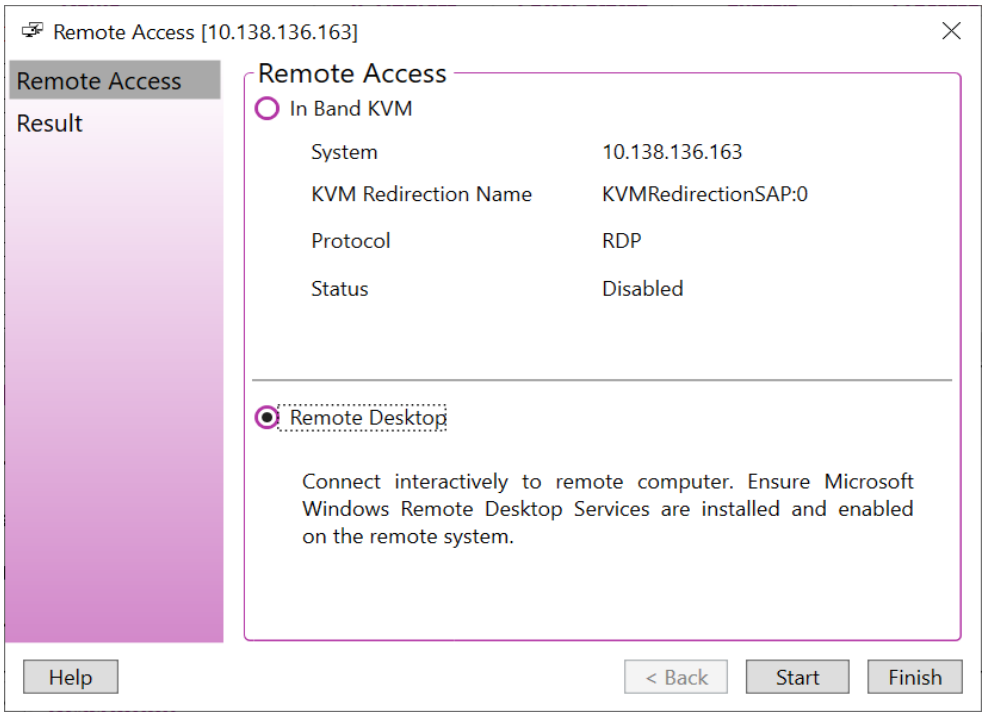


Figure 40: Remote Access Remote Desktop Selected

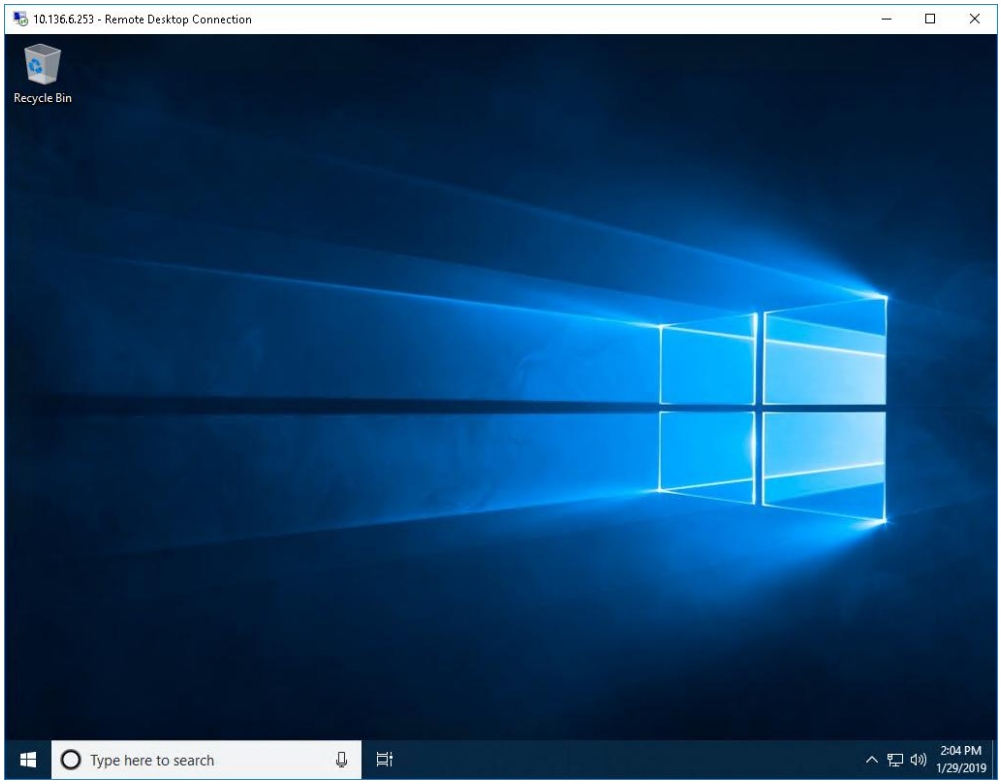


Figure 41: Microsoft Remote Desktop

[Public]

4.20 Add Groups

This feature allows you to create a system Groups.
AMC allows you to create a Groups and you can maintain each system in separate groups.

1. Select the 'GROUP' icon in the right-hand side from the main window. Or right click on Computer Groups and then select Add Groups
2. Once clicked on 'GROUP' icon/Computer Groups select add from the drop-down list or Add Groups from Computer Groups.
3. Now in the 'ADD-Group' window enter the group name and then click on OK.

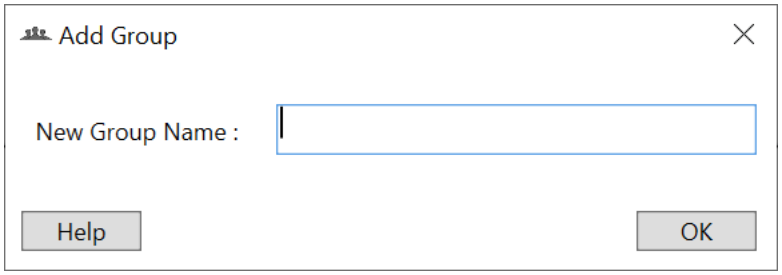


Figure 42: Add Group

4.21 Delete Groups

This feature allows you to delete a system Group

1. Select the 'GROUP' icon in the right-hand side from the main window then select delete option. Or right click on Computer Groups and then select Delete Group.

2. A confirmation window is prompted to the user

3. Once confirmed, the selected Group will be deleted from the Group list which is shown under Computer Groups.

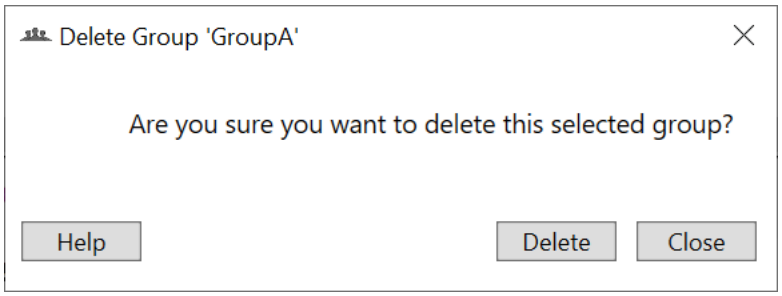


Figure 43: Delete Group

[Public]

4.22 Rename Groups

This feature allows you to rename a system Group.

1. Select the 'GROUP' icon in the right-hand side from the main window then select rename option. Or right click on Computer Groups and then select rename Group.

2. Enter the Group name to modify and click on OK.

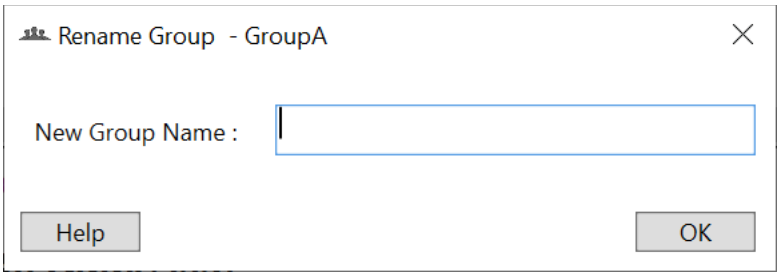


Figure 44: Rename Group

4.23 Add system to selected group

This feature allows you to add a system to selected group.

1. Right click on selected target in the list and select option 'Add to Group'.

2. This window shows all available groups.

3. In this we can select groups to which the system needs to be added and click on OK.

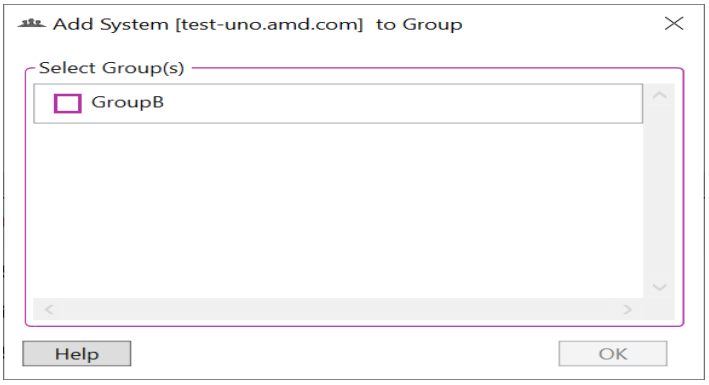


Figure 45: Add system to selected Group

[Public]

4.24 Delete system

This feature allows you to delete single or multiple systems.

1. Right click on the target in the list and select option 'Delete system'.
2. Selected target will be deleted upon clicking 'Delete'.

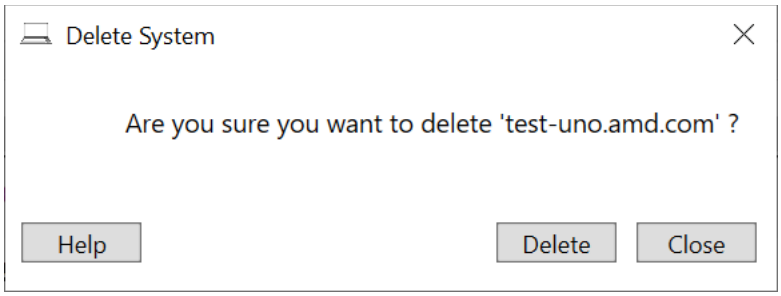


Figure 46: Add system to selected Group

[Public]

Chapter 5 Appendix

5.1 Troubleshooting issues:

Screen	Error	Description	Remediation
Configuration	The domain user name or password is incorrect.	After save the credentials service return with error code 4103	Check Domain username and password correctly.
Discover	Discovery failed.	May be target is not available	Target is invalid or may be not available in this movement
	System is not DASH capable.	May be not DASH enabled target or need to check target credentials in settings page	May be not DASH enabled target or need to check target credentials in settings page
Power	Power task on the system failed.	On scheduling power states if service return 0 showing this message	While doing power operation based on selected power state failed please retry again or please check your credentials once again
	Power task on the group failed.	On scheduling power states on group if service return other than 0 showing this message	Supported power status not available in selected group of target machines or please check your credentials once again(eg: power OFF, power ON, Sleep, Hibernate etc.)
	No power state available.	There is no supported power states are available	Supported power status not available in selected target machine(eg: power OFF, power ON, Sleep, Hibernate etc.)

[Public]

	Unauthorized. Verify authentication credentials or port configuration.	There was null power instance from service	Please check the credentials
Boot Config	No boot configuration instances found.	There is null response in the service output for the boot instances .	Boot configuration instances are not found in selected target, please verify the target once
	Changed Boot order had failed.	Once change boot order response from service stating that error code >0	Changing boot order on selected target is failed please retry again
	Default configuration failed.	Once change Default configuration response from service stating that error code >0	Changing default configuration on selected target is failed please retry again
	Object reference not set to an instance of object	In the implementation of boot config if no devices are added this error is seen	When Boot Config profile has not devices listed. The NIC vendor has not added Devices in Boot config.
	Next configuration failed.	Once change Next configuration response from service stating that error code >0	Changing next configuration on selected target is failed please retry again
Text Redirection	End the existing session and try again.	If No of putty sessions more than 0	Please close the current Putty window.
	Verify if the system supports Text Redirection and try again.	On load event if service return error code >0	Text Redirection not supported by selected target or please verify your credentials once
	Text redirection failed. Verify if the system supports text redirection and try again.	Text redirection has 0 instances	When there are no instances in text redirection. This message is seen. If the platform claims support for Text redirection, at least one instance needs to be supported. Please contact the NIC vendor for a fix to this issue
	No text redirection instance found.	If 0 result found in service response text instance count	Text Redirection not enabled on the

[Public]

			selected target machine
USB Redirection	Verify if the system supports USB Redirection and try again.	On load event if service return error code >0	Selected target not supports USB Redirection or please verify your credentials once
	No USB Redirection instance found.	there is null USB instance found in the service response or if RedirectionSAPName is null	USB Redirection not enabled on the selected target
	Already USB Redirected, either Modify or Disconnect.	USB Redirection mode in enabled state	USB Redirection already enabled in the selected target you may disconnect it or you can modify it.
	No USB Redirection instance found.	service returns error code = 6504	USB Redirection not enabled on the selected target
	Verify if URL exists.	service returns error code other than 6504	May be Entered URL doesn't exist check again
	Text redirection failed. Verify if the system supports text redirection and try again.	USB redirection has 0 instances	When there are no instances in USB redirection. This message is seen. If the platform claims support for USB redirection, at least one instance needs to be supported. Please contact the NIC vendor for a fix to this issue
KVM Redirection	System does not support KVM redirection.	Response contains error code not equal to 0	KVM redirection not supported by selected target or please verify your credentials once
	Supported KVM Redirection Instance not found.	KVM instance count 0	KVM instance not found on the selected target please verify it once
	Unable to connect to AMC Service.	got error	Check your AMC service once, Go to services.msc and check these **AMCAlertservice, AMCDASHService, AMCWebservice**

[Public]

System Health	System Health information not found.	Inventory count is 0 or null response from the service	System health not supported on selected target or please verify your target once
Firmware Upgrade	Firmware Upgrade is not supported for this device.	If service response error code 0 when page loading	Firmware upgrade not supported on selected target or please verify your credentials once
	Firmware Upgrade task failed..	After initiating firmware upgrade if service response error code !=0	Firmware upgrade failed on selected target please retry again
Log Entry	Log Entry operation failed.	service response contains null value or error code >0 in log instance object	Log Entry not supported on selected target or please verify your credentials once
Alerts	No Indication filters were found.	service response indication instances are null or 0	Alerts are not supported on selected target or please verify your credentials once
	Subscribed filter list had failed.	service response error code > 0	Operation failed on subscribing alerts please retry once again
	Enumeration of subscribed indication failed	There is no support to subscribe to events	When the platform does not support any events for subscription this error can be seen.
Boot to Text	No BootToTextImage data found in the response	boot to text image response instance are null	Boot text image not supported on selected target or please verify your credentials once
Boot to BIOS	KVM redirection failed.	service response error code >0	KVM Redirection failed on selected target please verify your credentials once
	System does not support KVM redirection.	After applied boot to bios service response error code >0	Selected target doesn’t supports KVM Redirection please verify your target
	Supported KVM Redirection Instance not found.	if redirection protocol VNC-RFB not found in the service response	KVM Instance not found in the selected target

[Public]

	KVM Redirection enumeration failed	If KVM redirection is set as supported but has 0 instance, then this message is shown	Upon enumeration 0 instances are found. Check with NIC vendor if KVM support is added
Remote Access	Supported KVM Redirection Instance not found.	If KVM instances are not found in the service response	Please check target whether it supports In band KVM
	KVM Redirection enumeration failed	If KVM redirection is set as supported but has 0 instance, then this message is shown	Upon enumeration 0 instances are found. Check with NIC vendor if KVM support is added

KVM redirection prints out Error codes when faced with an issue. Here is a table to help resolve few historically encountered issues:

Serial Number	Error code	Friendly Name	Description
1	Error 20	Key Parse Failed	This error can be seen if some file related to installation has been modified. Issue can be resolved by reinstalling AMC
2	Error 21	Connection Failed	This error can be seen if the platform did not successfully connect to the remote system via SSH. Re attempting to connect may resolve issue. If issue persists, please contact platform vendors
3	Error 22	Host name not found	This error can be seen if the platform did not allow a socket connection with the client. This issue can occur if IP address changes in KVM session or if the KVM session is not enabled due to SSH failure. Please contact vendor if issue recurs.
4	Error 23	Connection Key failed	This error can be seen if the platform did not successfully connect to the SSH connection with the provided key for KVM 1.9 and above. When this error occurs, SSH connection with KVM 1.8 is then attempted for KVM Redirection

[Public]

5	Error 24	Not Supported	This error can be seen when KVM Redirection is not supported on the platform where it was launched
6	Error 25	Connection Forcibly Closed	This error can be seen if some activity in the platform forced it to close the connection

5.2 Configuring Microsoft Entra ID App Registration for Intune Sync

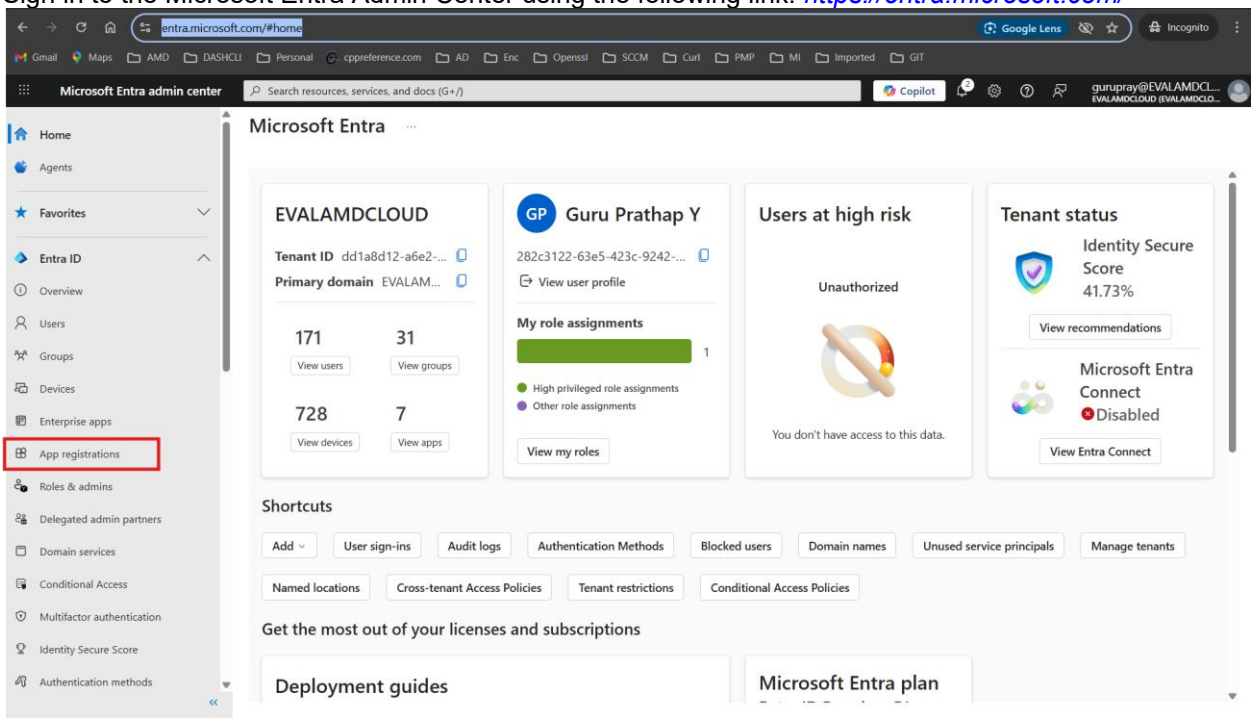
AMC integrates with Microsoft Intune through a Microsoft Entra ID application registration. The following steps describe how to create the application, configure the required permissions, and obtain the credentials needed to enable Intune Sync.

Prerequisites

- Microsoft Entra ID administrator access.
- Microsoft Intune subscription.
- Permission to grant Microsoft Graph API application permissions.

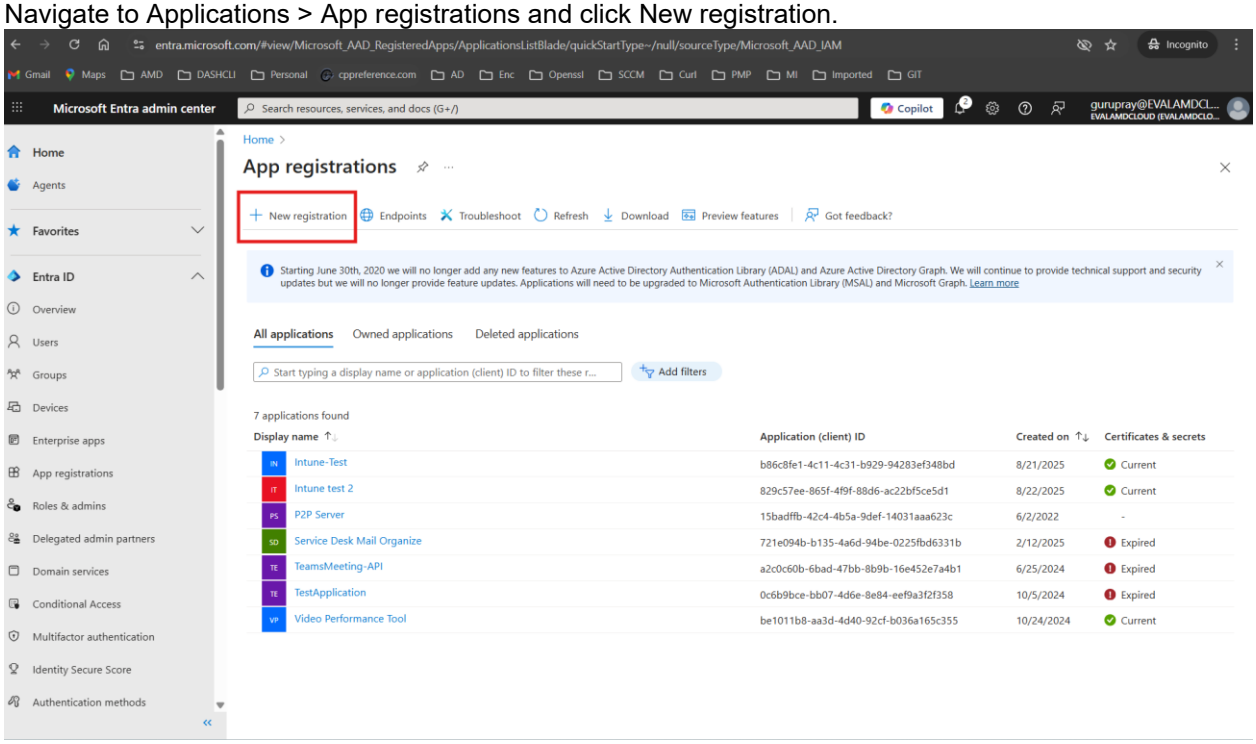
Steps:

1. Sign in to the Microsoft Entra Admin Center using the following link: *https://entra.microsoft.com/*

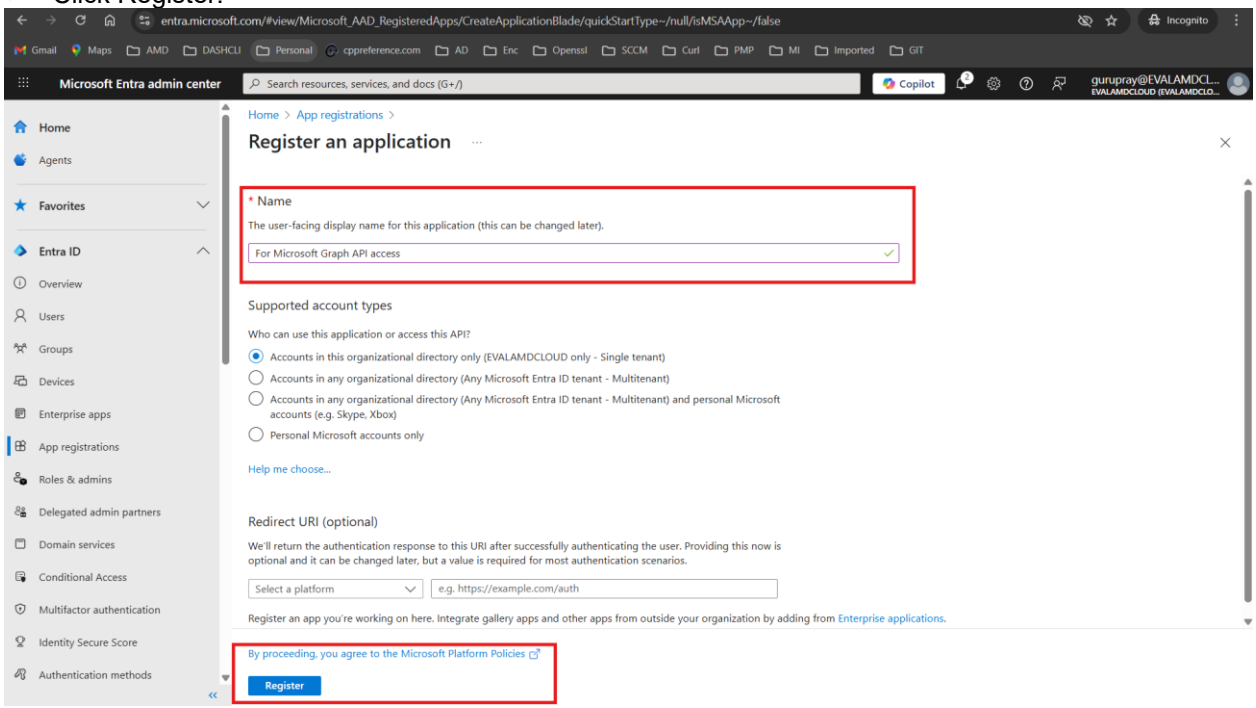


[Public]

2. Navigate to Applications > App registrations and click New registration.

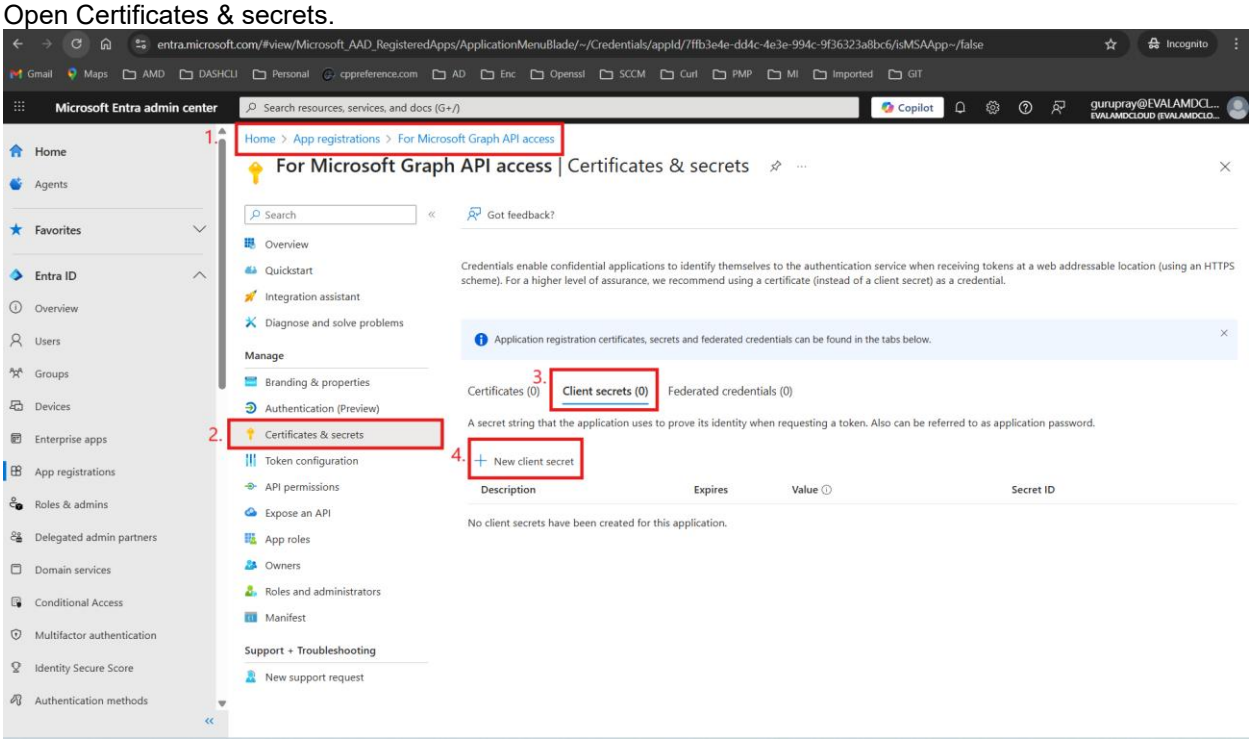


3. Enter the application details:
   - Name: Specify a name for the application.
   - Supported account types: Select the required account type for your organization.
   - Redirect URI: Configure only if required by your deployment.
   - Click Register.

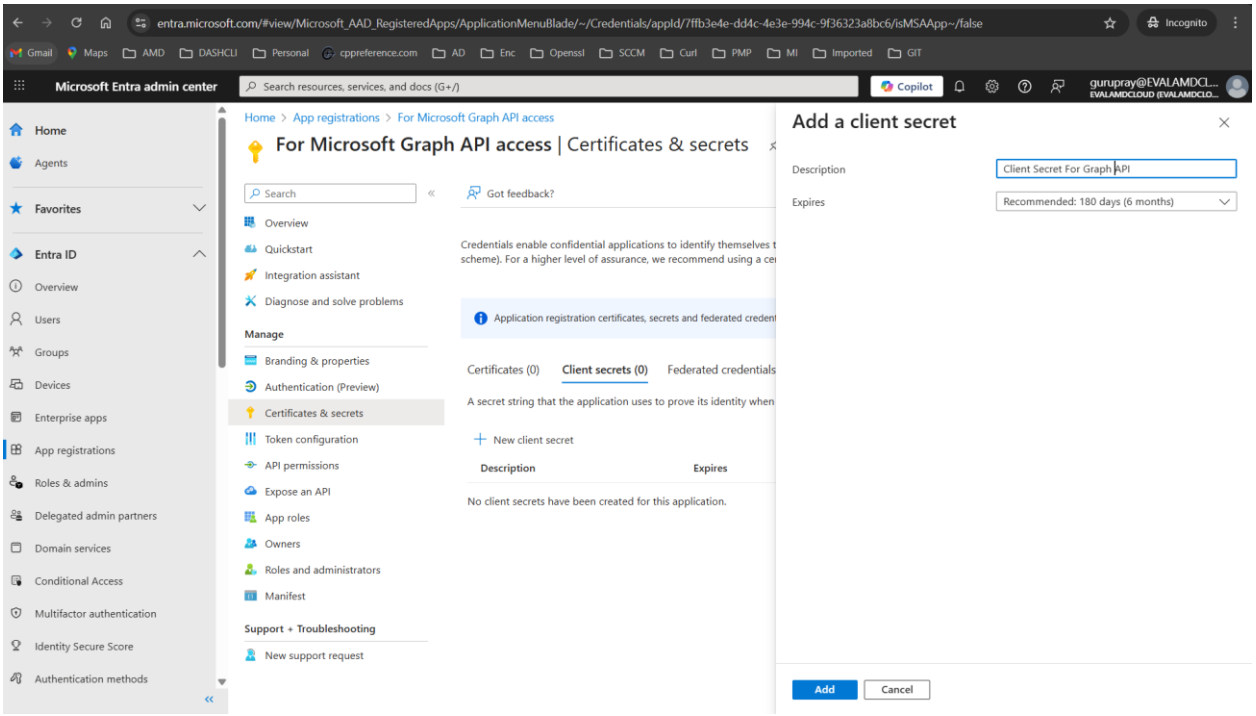


[Public]

4. Create a client secret:
   - Open Certificates & secrets.

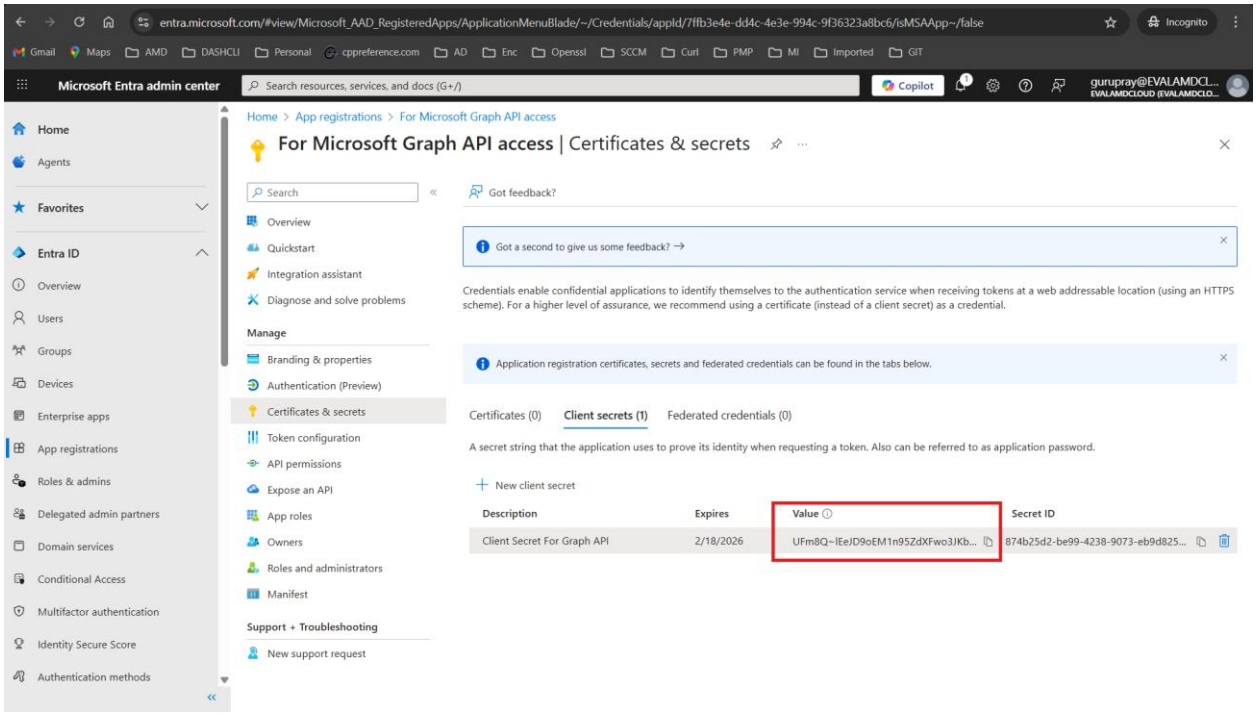


   - Click New client secret.

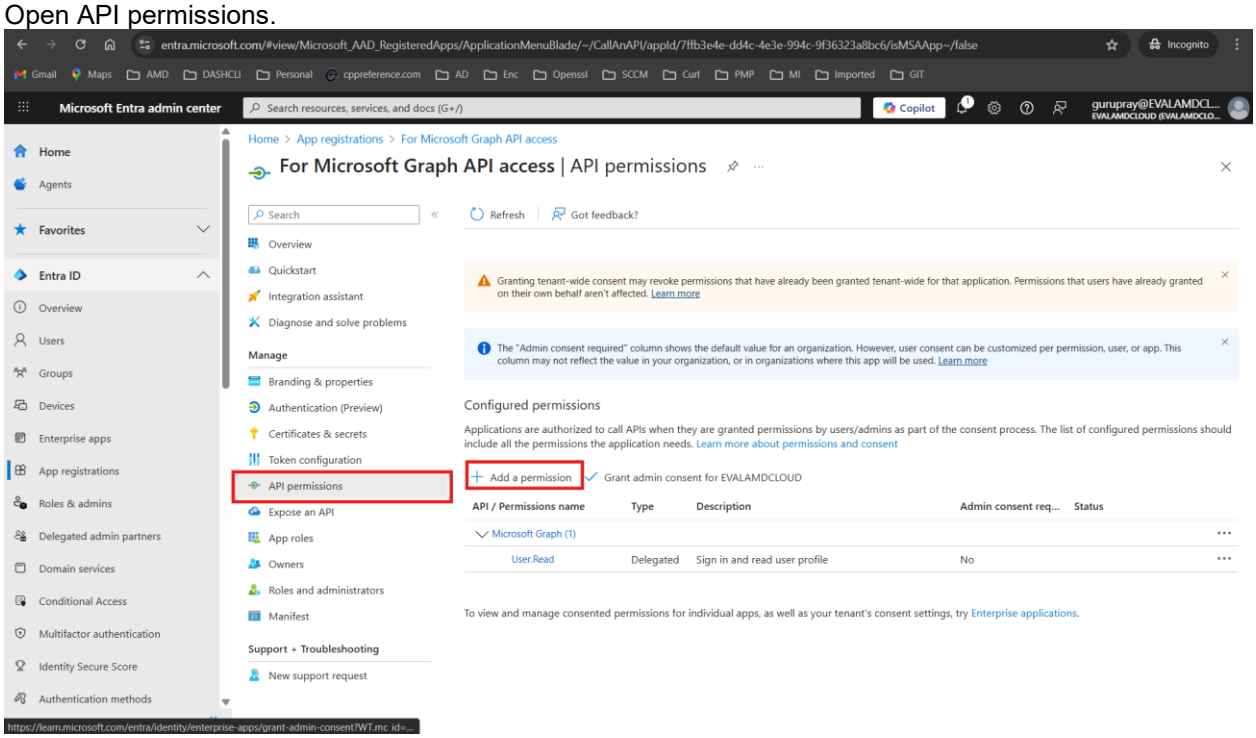


   - Provide a description and expiration period.
   - Click Add.
   - Copy and save the generated Secret Value.

[Public]

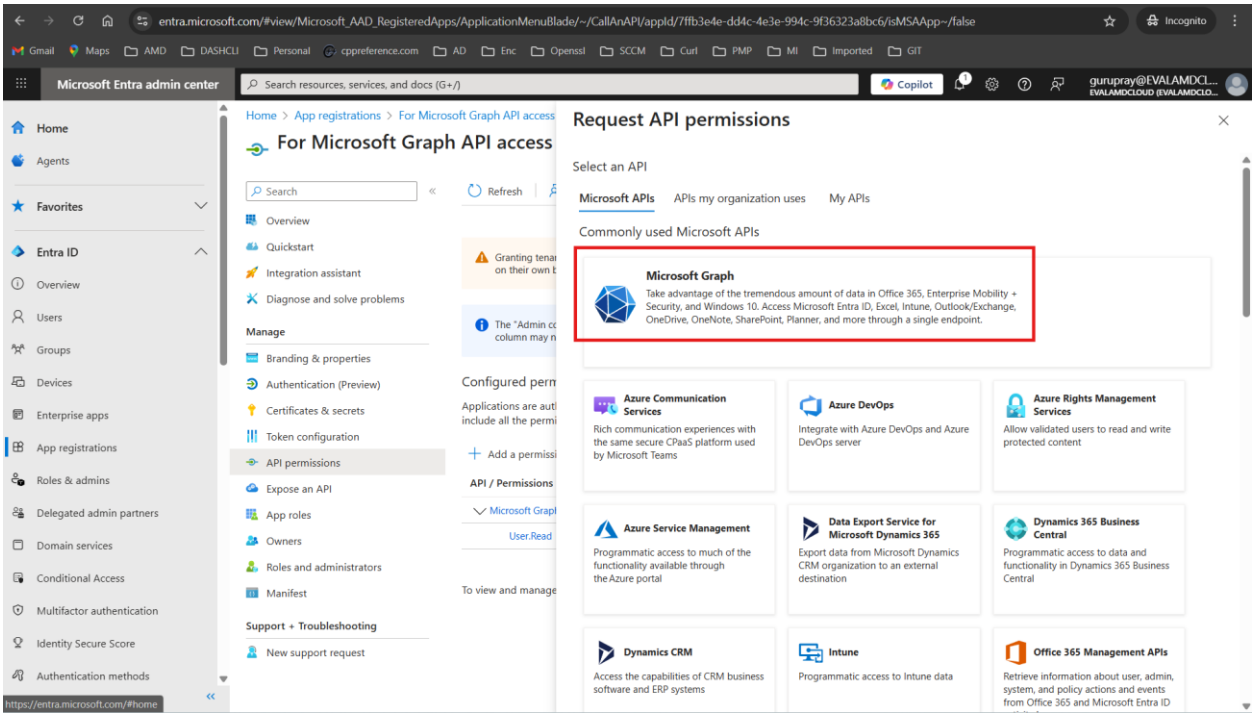


5. Configure Microsoft Graph API permissions:
   - Open API permissions.

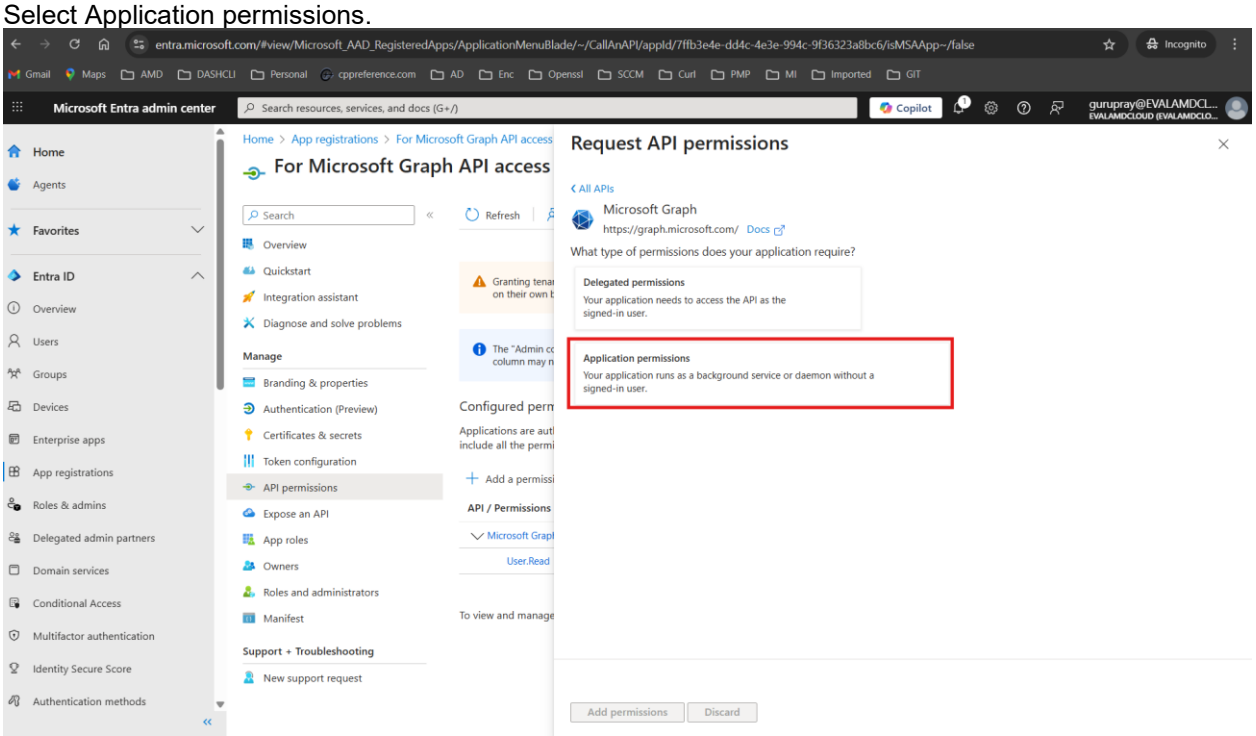


   - Click Add a permission.
   - Select Microsoft Graph.

[Public]

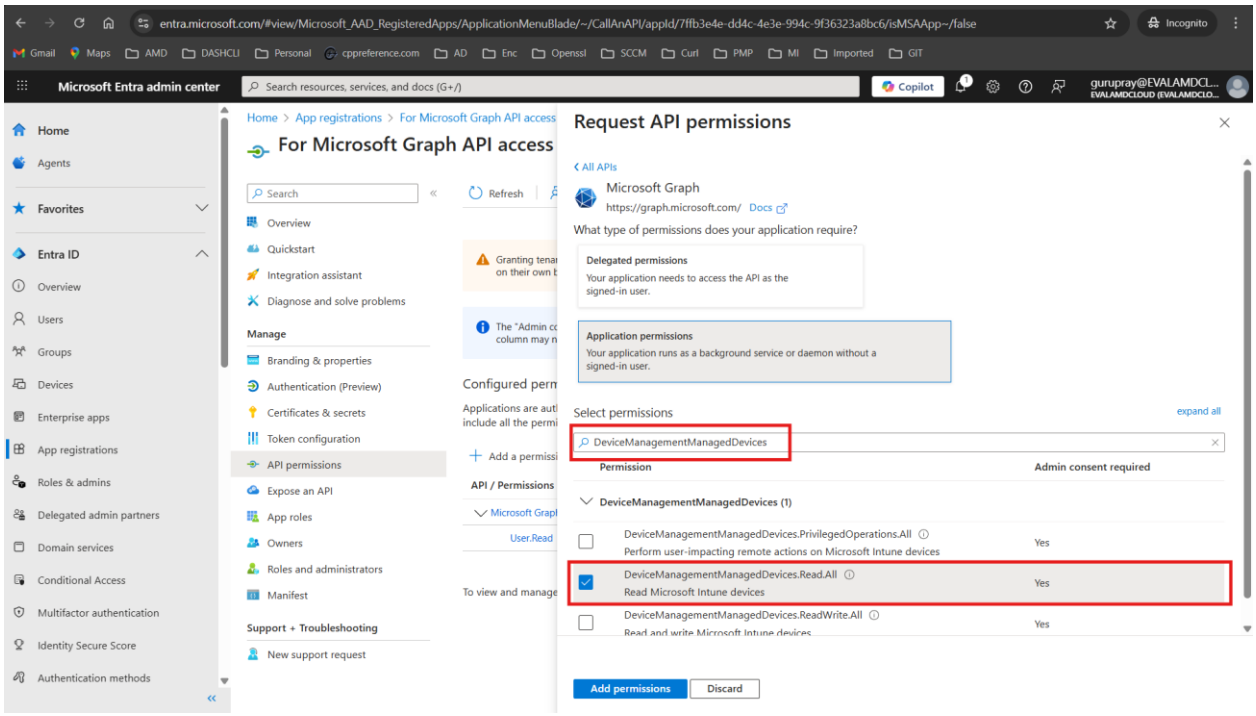


- Select Application permissions.



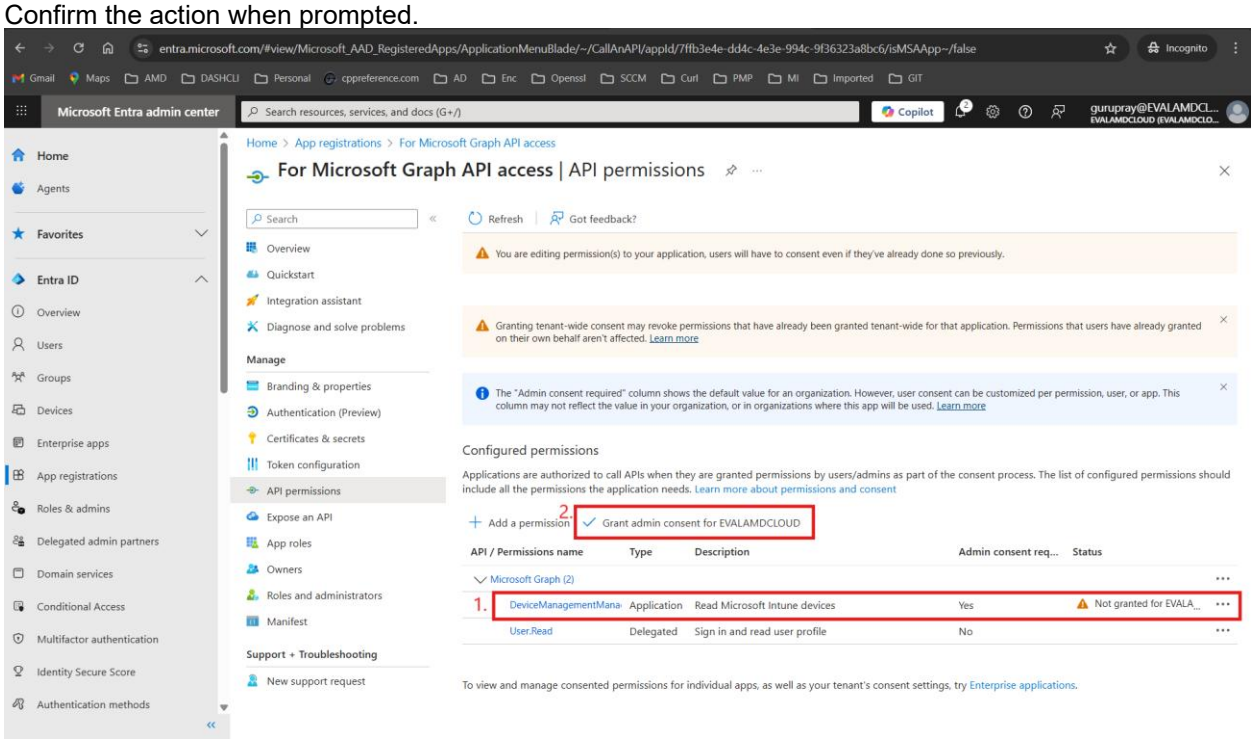
- Search for DeviceManagementManagedDevices.

[Public]



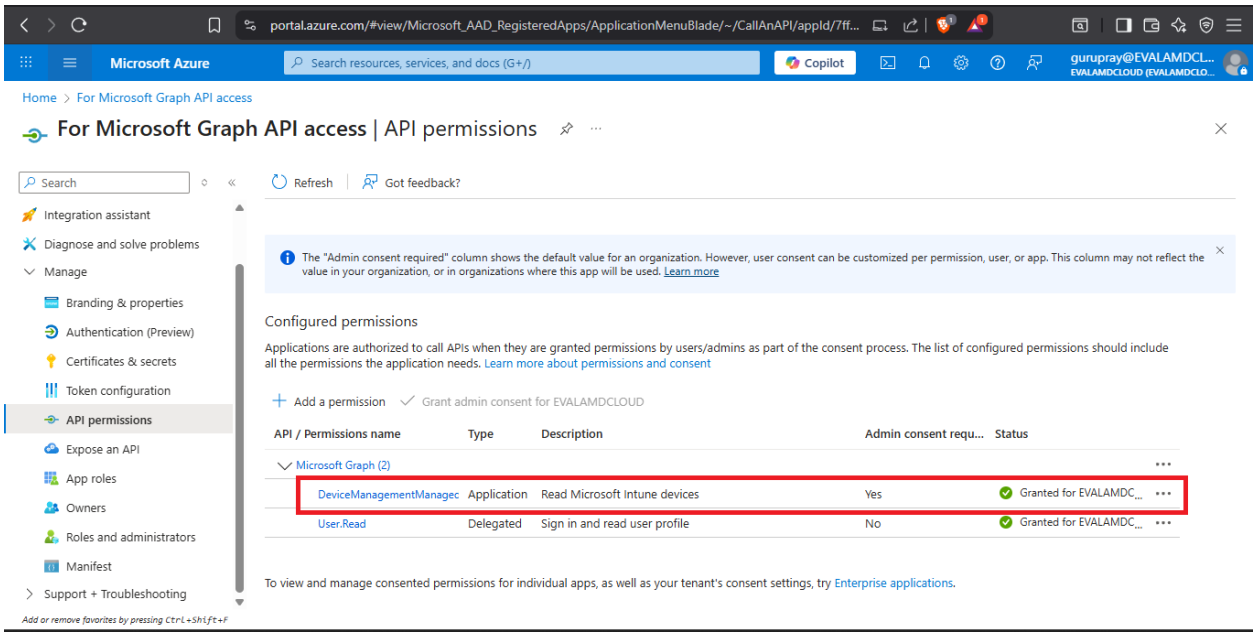
- Select DeviceManagementManagedDevices.Read.All.
- Click Add permissions.

6. Grant administrator consent:
   - Under API permissions, select Grant admin consent for <Tenant Name>.
   - Confirm the action when prompted.



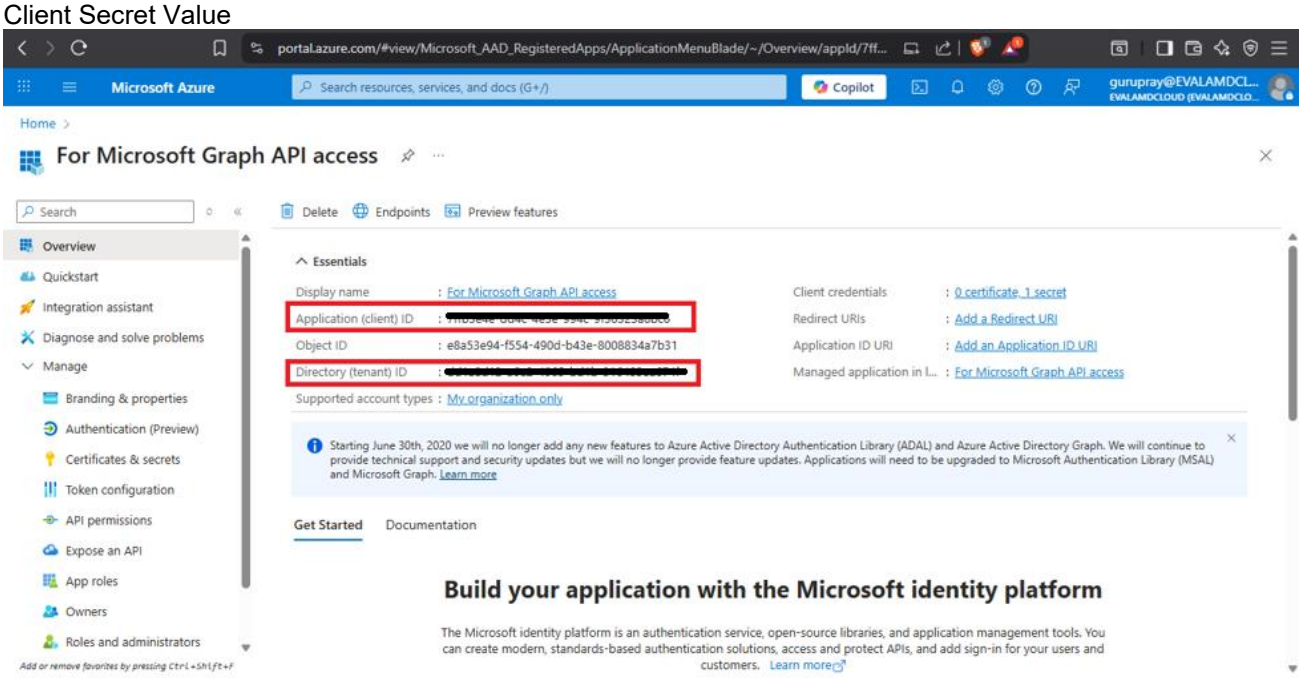
[Public]

7. Verify that the permission DeviceManagementManagedDevices.Read.All shows Granted for <Tenant Name>.



8. Obtain the required application details:

- Application (Client) ID
- Directory (Tenant) ID
- Client Secret Value



Note:
AMC uses these credentials to securely connect to Microsoft Intune and synchronize managed device information from the configured tenant.