



# AMPS

# User Guide

## AMD Management Plugin for SCCM

**Issue Date:** November 2025

## **Disclaimer**

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. AMD reserves the right to make changes to the specifications and product descriptions at any point of time without prior 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 to use as components in systems intended for surgical implant in the body, 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**

Copyright © 2007 - 2024 Advanced Micro Devices, Inc. All rights reserved.

# Table of Contents

<b>TABLE OF CONTENTS</b>	<b>3</b>
<b>TABLE OF FIGURES</b>	<b>6</b>
<b>NOTATIONS USED</b>	<b>11</b>
<b>REVISION HISTORY</b>	<b>12</b>
<b>CHAPTER 1 INTRODUCTION</b>	<b>13</b>
1.1 ARCHITECTURE OVERVIEW	13
1.2 PREREQUISITES AND SYSTEM REQUIREMENTS	15
1.3 INSTALLING AND UN-INSTALLING AMPS	16
1.3.1 <i>AMPS deployment in CAS</i>	16
1.3.2 <i>Installing/Upgrading AMPS</i>	16
1.3.3 <i>Uninstalling AMPS</i>	16
1.4 USING THE AMPS FEATURES	17
1.4.1 <i>Accessing the DASH Configuration node</i>	18
1.4.2 <i>Accessing the DASH Scheduled Tasks node</i>	20
1.4.3 <i>Accessing the All DASH Capable Systems node</i>	21
1.4.4 <i>Accessing the All DASH Managed Systems node</i>	22
1.4.5 <i>Accessing the All DASH Unmanaged Systems node</i>	23
1.5 LOGGING IN AMPS	23
<b>CHAPTER 2 CONFIGURING DASH IN MEM</b>	<b>25</b>
2.1 AUTHENTICATION	27
2.2 DASH MANAGEMENT PORTS AND TRANSPORT	27
2.3 ALERTS EVENT PORT	28
2.4 CONFIGURATION MANAGER SETTINGS	28
2.4.1 <i>DASH Wakeup during Package Deployment</i>	28
2.4.2 <i>Auto Discovery of DASH Devices</i>	29
2.5 TLS CERTIFICATE FOR HTTPS	29
2.6 DASH CAPABLE CHECK	29
2.7 CLOUD MANAGEABILITY	30
2.8 MUTUAL AUTHENTICATION	30
2.9 CONFIGURATION IN CAS	30
2.10 INFORMATION ABOUT THE AMPS PLUGIN	30
<b>CHAPTER 3 PERFORMING DASH OPERATIONS</b>	<b>32</b>
3.1 DISCOVERY	32
3.1.1 <i>Discovering a Collection</i>	32
3.1.2 <i>Discovering a Device</i>	35
3.2 POWER CONTROL	37
3.2.1 <i>Power Control on Collection</i>	37
3.2.2 <i>Power Control on Device</i>	41
3.2.3 <i>Power States</i>	43
3.2.4 <i>Scheduled Power Control</i>	44
3.3 BOOT CONTROL	45
3.4 TEXT REDIRECTION	47
3.5 USB REDIRECTION	50
3.5.1 <i>Connecting USB Redirection</i>	51
3.5.2 <i>Disconnecting USB Redirection</i>	52

3.6	SUBSCRIBING/UN-SUBSCRIBING ALERTS	53
3.6.1	<i>Subscribing Alerts</i>	55
3.6.2	<i>Un-Subscribing Alerts</i>	56
3.6.3	<i>Receiving Alerts</i>	57
3.7	INVENTORY	58
3.7.1	<i>Inventory Collection</i>	58
3.7.2	<i>Viewing the DASH Inventory or Resource Explorer</i>	59
3.8	LOG ENTRY	95
3.9	BOOT TO TEXT IMAGE	97
3.9.1	<i>Sample Use Cases</i>	101
3.10	FIRMWARE UPDATE	103
3.10.1	<i>Firmware Update on Collection</i>	103
3.10.2	<i>Firmware Update on Device</i>	106
3.11	BOOT TO BIOS (KVM PROFILE)	108
3.11.1	<i>Boot to BIOS on Device</i>	108
3.12	KVM REDIRECTION	110
3.13	OPAQUE MANAGEMENT DATA	113
3.14	UNOWN	114
3.15	DISK WIPE	115
3.16	TROUBLESHOOTING	117
3.16.1	<i>Troubleshooting DASH issues</i>	117
3.16.2	<i>Troubleshooting KVM issues</i>	121
<b>CHAPTER 4</b>	<b>ROLE-BASED ADMINISTRATION</b>	<b>123</b>
4.1	SECURITY ROLE	123
4.1.1	<i>Full Administrator Security Role</i>	123
4.1.2	<i>Operations Administrator Security Role</i>	124
4.1.3	<i>Remote Tools Operator Security Role</i>	125
4.2	CONFIGURATION IN MEM FOR AMPS	126
4.2.1	<i>Overview of collections in MEM</i>	126
4.2.2	<i>Overview of collection object's security in MEM</i>	127
4.2.3	<i>MEM collection security rights</i>	128
4.2.4	<i>Security rights defined for DASH tasks</i>	129
4.2.4.1	Collection class/instance	129
4.2.4.2	Read operations	129
4.2.4.3	Modify operations	129
4.2.5	<i>Security rights for DASH operations</i>	129
4.2.6	<i>Security rights defined for DASH settings</i>	132
4.2.6.1	Read	133
4.2.6.2	Modify	133
4.2.7	<i>Configuration of AMPS</i>	134
4.2.7.1	Steps	134
4.2.8	<i>Security Scope</i>	134
4.2.8.1	Collection	135
4.3	CASE STUDY	135
4.3.1	<i>Business scenario</i>	135
4.3.2	<i>Solution Description</i>	135
4.4	ERROR MESSAGES	143
<b>CHAPTER 5</b>	<b>DASH SCHEDULED TASKS</b>	<b>147</b>
5.1	SCHEDULE DASH TASKS	147
5.1.1	<i>Recurrence Patterns</i>	148
5.1.1.1	One time Recurrence Pattern	148
5.1.1.2	Weekly Recurrence Pattern	149

5.1.1.3	Monthly Recurrence Pattern	150
5.1.1.4	Custom Recurrence Pattern	151
5.2	DASH SCHEDULED TASKS	152
<b>CHAPTER 6</b>	<b>CREATING USER ACTION REPORT FOR AMPS</b>	<b>156</b>
6.1	PREREQUISITES	156
6.2	OPENING SSRS FROM MEM	157
6.3	DELETE DEFAULT DATASETS AND PROPERTIES	162
6.4	ADDING NEW DATASETS	163
6.4.1	<i>DASHUserActionLogs</i>	163
6.4.2	<i>Users</i>	167
6.5	SETTING PARAMETER PROPERTIES	168
6.5.1	<i>Login</i>	168
6.5.2	<i>Severity</i>	171
6.5.3	<i>DateRange</i>	172
6.6	ARRANGING THE VALUES IN THE REPORT	173
6.7	RENAMING THE REPORTS HEADINGS	178
6.8	RUNNING REPORT IN MEM	179
6.9	RUNNING REPORT IN SSRS	185
<b>CHAPTER 7</b>	<b>DASH REPORTS</b>	<b>188</b>
7.1	DASH DIAGNOSTIC REPORT	188
7.2	DASH WAKE ON LAN STATUS REPORT	189
7.3	DASH MANAGED SYSTEMS REPORT	190
7.4	DASH UNMANAGED SYSTEMS REPORT	190
7.5	DASH NON DASH SYSTEMS REPORT	191
7.6	DASH UNDISCOVERED SYSTEMS REPORT	191
7.7	DASH MEMORY REPORT	192
<b>CHAPTER 8</b>	<b>AMPS STATUS MONITORING</b>	<b>193</b>
8.1	ALL AMPS STATUS MESSAGES	193
<b>CHAPTER 9</b>	<b>APPENDIX</b>	<b>195</b>
9.1	PROVISIONING	195
9.2	USING SELF-SIGNED CERTIFICATES FOR HTTPS COMMUNICATION	195
9.3	DISCUSSION FORUM LINK	195
9.4	ACTIVE DIRECTORY CONFIGURATION DOCUMENTS	195
9.5	DASH SUPPORT EMAIL	195

# Table of Figures

Figure 1.1: AMPS Architecture Overview	14
Figure 1.2: Control Panel AMPS Uninstallation	17
Figure 1.3: Removing AMPS using AMPS installer	17
Figure 1.4: Configure MEM for DASH operations	19
Figure 1.5: DASH Scheduled Tasks Node	20
Figure 1.6: All DASH Capable Systems Node	21
Figure 1.7: All DASH Managed Systems Node	22
Figure 1.8: All DASH Unmanaged Systems Node	23
Figure 1.9: Folder path of AMPS logs	24
Figure 10: DASH Configuration Screen	26
Figure 11: Authentication Schemes Section	27
Figure 12: Management Ports and Transport Section	27
Figure 13: Alerts Event Port Section	28
Figure 14: Configuration Manager Settings Section	28
Figure 15: DASH Wakeup Section	29
Figure 16: DASH Auto Discover Section	29
Figure 17: TLS certificate for HTTPS Section	29
Figure 18: AMPS DASH Capable check	30
Figure 19: AMD Cloud manageability settings	30
Figure 20: Immediate Discovery Schedule on Collection	34
Figure 21: Schedule Discovery on Collection	34
Figure 22: Discovery Result	35
Figure 23: DASH Discovery on a Device	36
Figure 24: Result of Discovery on Device	37
Figure 25: Power Control on Collection	38
Figure 26: Immediate Power Control on Collection	39
Figure 27: Scheduled Power Control on Collection	40
Figure 28: Power Control on Device	41
Figure 29: Power Control on Device	42
Figure 30: Scheduled Power Control	45
Figure 31: DASH Boot Control on Device	46
Figure 32: Boot Control on Device	47
Figure 33: Text Redirection on device	48
Figure 34: Text Redirection	49
Figure 35: USB Redirection on Device	50
Figure 36: USB Redirection	51
Figure 37: USB Redirection Connect	52
Figure 38: USB Redirection Disconnect	53
Figure 39: Alerts on device	54
Figure 40: Alerts	55

Figure 41: Alerts Subscription	56
Figure 42: Alerts Un-Subscription	57
Figure 43: Alerts Reception	57
Figure 44: Inventory on device	59
Figure 45: Inventory	59
Figure 46: DASH Inventory shown in Resource Explorer	60
Figure 47: DASH 'Alert Destination' Profile Properties	61
Figure 48: DASH 'Battery' Profile Inventory	62
Figure 49: DASH 'BIOS' Profile Inventory	63
Figure 50: DASH 'Boot Config' Profile Inventory	64
Figure 51: DASH 'Computer System' Profile Inventory	65
Figure 52: DASH 'DHCP Client' Profile Inventory	66
Figure 53: DASH 'DNS Client' Profile Inventory	67
Figure 54: DASH 'Ethernet Port' Profile Inventory	68
Figure 55: DASH 'Filter Collection' Profile Properties	69
Figure 56: DASH 'Identity' Properties	70
Figure 57: DASH 'Indication Filter' Profile Properties	71
Figure 58: DASH 'Indication Subscription' Profile Properties	72
Figure 59: DASH 'Indicator LED' Profile Properties	73
Figure 60: DASH 'IP Configuration' Profile Properties	74
Figure 61: DASH 'IP Interface' Profile Properties	75
Figure 62: DASH 'KVM Redirection' Profile Properties	76
Figure 63: DASH 'Media Redirection' Profile Properties	77
Figure 64: DASH 'Memory' Profile Properties	78
Figure 65: DASH 'Network Port' Properties	79
Figure 66: DASH 'Opaque Management Data' Profile Properties	80
Figure 67: DASH 'Operating System' Profile Properties	81
Figure 68: DASH 'PCI Device' Profile Properties	82
Figure 69: DASH 'Physical Asset' Profile Properties	83
Figure 70: DASH 'Physical Computer System View' Profile Properties	84
Figure 71: DASH 'Platform Watchdog Service' Profile Properties	85
Figure 72: DASH 'Power Supply' Profile Properties	86
Figure 73: DASH 'Processor' Profile Properties	87
Figure 74: DASH 'Record Log' Profile Properties	88
Figure 75: DASH 'Registered Profile' Profile Properties	89
Figure 76: DASH 'Role' Profile Properties	90
Figure 77: DASH 'Software' Profile Properties	91
Figure 78: DASH 'Text Redirection' Profile Properties	92
Figure 79: DASH 'USB Redirection' Profile Properties	93
Figure 80: DASH 'User' Profile Properties	94
Figure 81: DASH Hardware History	94
Figure 82: Viewing the Log Entry of a device	95

Figure 83: Log Entry-----	96
Figure 84: Status Message Details-----	97
Figure 85: Boot Text Image on device-----	98
Figure 86: Boot Text Image-----	99
Figure 87: Boot Text Image after adding URL-----	100
Figure 88: Boot Text Image after booted to URL-----	101
Figure 89: Selecting DOS Image-----	102
Figure 90: Firmware Update on Collection-----	103
Figure 91: Immediate Firmware Update on Collection-----	104
Figure 92: Scheduled Firmware Update on Collection-----	105
Figure 93: Firmware Update on Device-----	106
Figure 94: Firmware Update on Device-----	107
Figure 95: Boot to BIOS on Device-----	108
Figure 96: Boot to BIOS-----	109
Figure 97: BIOS Screen in VNC Viewer-----	110
Figure 98: KVM Redirection on Device-----	111
Figure 99: KVM Redirection On Device-----	112
Figure 100: Windows Screen in RtkDASH Viewer-----	113
Figure 101: Role Based Administration mechanism in MEM-----	123
Figure 102: Selecting Full Administrator role-----	124
Figure 103: Selecting Operations Administrator role-----	125
Figure 104: Selecting Remote Tools Operator role-----	126
Figure 105: User Collection-----	128
Figure 106: Device Collection-----	128
Figure 107: Security rights for DASH operation-----	131
Figure 108: Security permissions for different roles for a collection.-----	132
Figure 109: Security rights user collection and access mapping-----	133
Figure 110: Opening the DASH Configuration window.-----	134
Figure 111: Creating user group in "Active Directory Users and Computers" Application-----	136
Figure 112: Adding Users in "Active Directory Users and Computers" application-----	137
Figure 113: Adding Users to Administrative Users-----	138
Figure 114: Adding "Call Center Admins" to "Administrative Users"-----	139
Figure 115: Creating 4 user collections in "Administrative Users"-----	139
Figure 116: Creating "Device Collection" for Device Management-----	140
Figure 117: Adding Roles to Call Center Admins-----	141
Figure 118: Assigning Call Center Device Collection to Call Center Administrator Users-----	141
Figure 119: Choose the Call Center Systems from Device Collections-----	142
Figure 120: Summary of 4 Accounts and Collection mapping and security Roles assigned-----	143
Figure 121: Collection Error-----	144
Figure 122: Device Error-----	145
Figure 123: DASH Configuration Error-----	146
Figure 124: DASH Task Scheduler-----	148



Figure 125: DASH Task Scheduler One Time	149
Figure 126: DASH Task Scheduler Weekly	150
Figure 127: DASH Task Scheduler Monthly	151
Figure 128: DASH Task Scheduler Custom	152
Figure 129: DASH Scheduled Tasks Node	153
Figure 130: DASH Scheduled Tasks	154
Figure 131: DASH Scheduled Task Details	155
Figure 132: Reporting services point role	156
Figure 133: Opening Report Manager Link	157
Figure 134: SQL Server Reporting Services	157
Figure 135: Adding new folder to SSRS	158
Figure 136: New Folder prompt with Name field	158
Figure 137: Create Report option	159
Figure 138: Adding Report Name and Path	160
Figure 139: Create Reports Wizard completed successfully	161
Figure 140: Microsoft Report Builder utility	162
Figure 141: Deleting Datasets	162
Figure 142: Adding Datasets	163
Figure 143: Setting values to DASH User Action Logs	166
Figure 144: Updated Datasets and Parameters	167
Figure 145: Creating Users dataset	168
Figure 146: Editing Parameter Properties	169
Figure 147: Editing Available Values	170
Figure 148: Setting Available Values to Login Parameter	171
Figure 149: Setting Available Properties to Severity parameter	172
Figure 150: Setting Available Values to Date Range parameter	173
Figure 151: Table or Matrix option in Report Builder	174
Figure 152: Choosing the DASH User Action Logs Dataset	175
Figure 153: Setting Row Groups and Values	176
Figure 154: Choosing count property to Computer Name Value	177
Figure 155: De-selecting "Show subtotals and grand totals" option	178
Figure 156: Renaming the headers in the report	178
Figure 157: Save menu option in File menu	179
Figure 158: Running the report in MEM	180
Figure 159: DASH User Action Report window	181
Figure 160: Choosing Severity	182
Figure 161: Choosing Users	183
Figure 162: Choosing Date Range	184
Figure 163: DASH User Action Report with values	185
Figure 164: Running Report in SSRS from MEM	185
Figure 165: DASH User Action Report in SSRS	186
Figure 166: Viewing Report in SSRS	187



Figure 167: DASH Reports in SSRS----- 188

Figure 168: Diagnostic Report----- 189

Figure 169: DASH Wake on LAN Status Report ----- 190

Figure 170: DASH Managed Systems Report----- 190

Figure 171: DASH Unmanaged Systems Report ----- 191

Figure 172: DASH Non DASH Systems Report ----- 191

Figure 173: DASH Undiscovered Systems Report ----- 192

Figure 174: DASH Memory Inventory Report ----- 192

Figure 175: All AMPS Status Messages Queries ----- 193

Figure 176: Select Date and Time for AMPS Status Messages ----- 194

Figure 177: All AMPS Status Messages ----- 194

## Notations Used

Term	Description
Out-of-band management	Out of band (OOB) management tasks are those performed independent of the power or OS state on the managed client or system.
DASH	Desktop Mobile Architecture for System Hardware (DASH), is a client management standard produced by the Distributed Management Task Force (DMTF). DASH specifies the transport, management protocol (WS-Man), and DMTF CIM profiles used to manage desktop and mobile PCs. DASH defines a set of interoperability standards for managing, monitoring, and controlling PCs, regardless of system power state (on, off, stand-by) or OS capability.
DASH-capable system	A DASH-capable system is a computer system that conforms to the DMTF DASH standard.
Management controller	Management controller enables OOB platform management capabilities with technologies such as DASH.
DASH management controller	The DASH management controller implements the DASH protocol stack. It interfaces with other platform components (BIOS, SB, IMDs, etc.) to get needed information or control the platform.
MEM Administrator Console or MEM console	This is the GUI interface of MEM Site Server used for managing MEM servers. MEM console is also called the configuration manager console.
Windows Management Instrumentation	WMI is the infrastructure for management data and operations on Windows-based OSes. It provides an interface through which instrumented components provide information and notification. WMI is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF).
SQL Server Reporting Service	SSRS is a server-based report generating software system from Microsoft.

## Revision History

Date	Revision	Description
November 15 2025	2.7	Content for 8.0 Release
Aug 01 2024	2.6	Content for 7.1 Release
May 30, 2024	2.5	Content for 7.0 Release
June 27,2023	2.4	Content for 6.1 Release
February 09,2023	2.3	Content for 6.0 Release
October 13, 2020	2.2	Content for 5.5 Release
August 01, 2020	2.1	Content for 5.0 Release
January 17, 2020	2.0	Content for 4.5 Release
September 12, 2018	1.9	Content for 4.2 Release
June 17, 2018	1.8	Content for 4.1 Release
November 02, 2017	1.7	Content for 4.0 Release
September 01, 2016	1.6	Content for 3.5 Release
February 04, 2016	1.5	Content for 3.0 Release
October 26, 2015	1.4	Content for 2.5 Release
June 10, 2015	1.3	Content for 2.3 Release
February 23, 2015	1.2	Content for 2.2 Release
September 23, 2014	1.1	Content for 2.1 Release
August 08, 2014	1.0	Content for 2.0 Release
July 25, 2014	0.8	Contents for beta
July 05, 2014	0.5	First draft

# Chapter 1 Introduction

---

This document describes features and usages of the AMPS - AMD Management plugin for System Center Configuration Manager (SCCM). AMPS supports SCCM versions 2211/2303/2309/2403 which are installed on Windows server versions 2016 and above.

The AMPS is a plugin for MEM. It allows MEM administrators to remotely manage client systems that support the DMTF DASH standard irrespective of the state of the clients OS.

The plugin supports the DASH 1.0, 1.1 and 1.2 capabilities, including:

- Discovery (Manual and Auto).
- Authentication (Digest and Active Directory).
- Inventory.
- Remote Power Control (On/Off).
- Wake on DASH.
- Boot Control.
- Text redirection.
- USB redirection.
- KVM Redirection
- Log Entry
- Alert subscription and reception.
- Scheduled Power Control on a collection.
- Boot Text Image
- Boot To BIOS
- Disk Wipe
- Unown

## 1.1 Architecture Overview

The architectural overview of the AMPS is illustrated in Figure 1.1 Note all items in yellow DASH UI (DASH Console extensions), DASH Provider, DASH Proxy and DASH SDK are the components of AMPS.

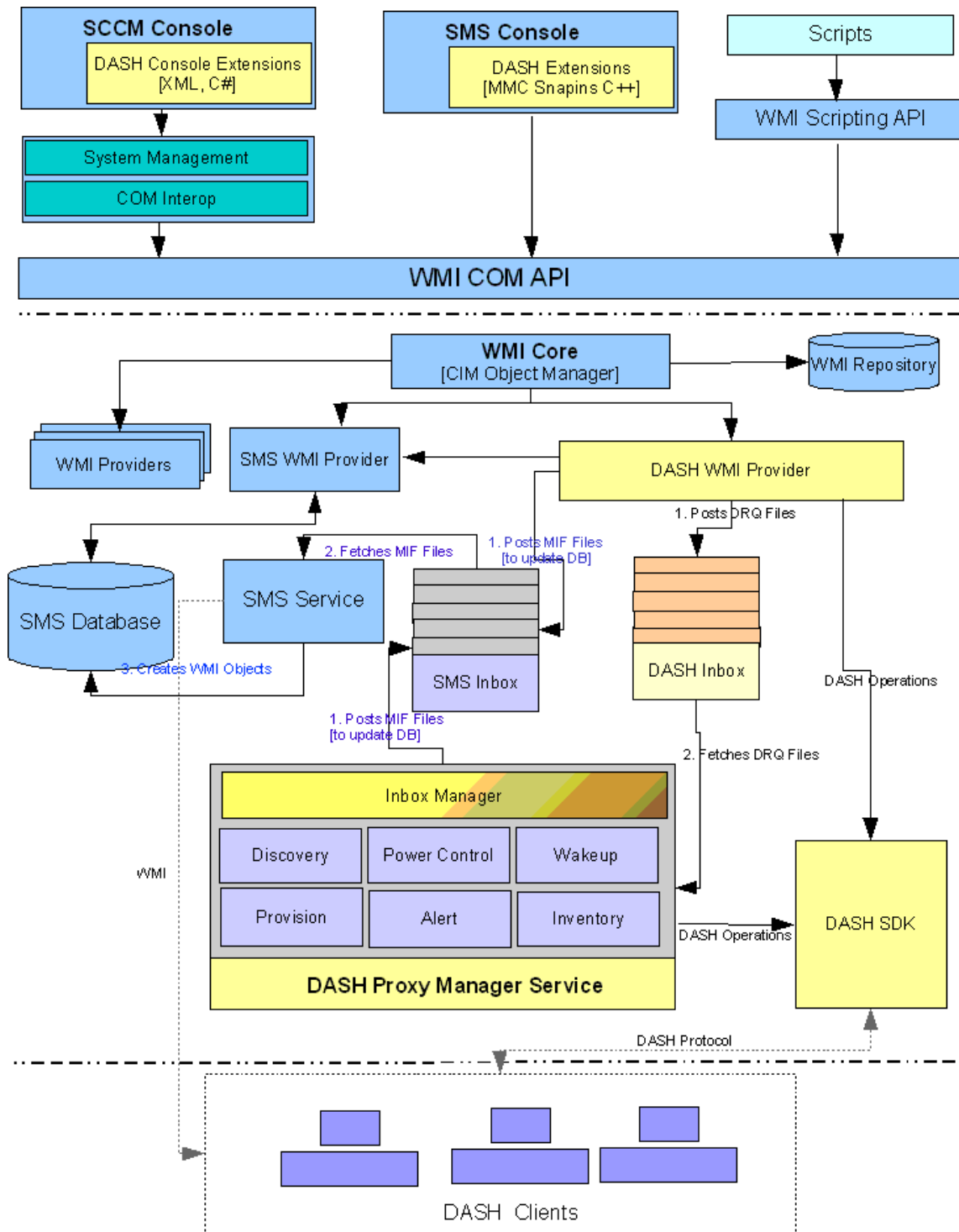


Figure 1.1: AMPS Architecture Overview

## 1.2 Prerequisites and System Requirements

The prerequisites to install AMPS are:

- Supported Microsoft Endpoint Configuration Manager must be installed.
- The Site server must be configured.

For information on the hardware and software requirements, refer to the following web location:  
<https://docs.microsoft.com/en-in/sccm/core/plan-design/configs/supported-configurations>

## 1.3 Installing and Un-installing AMPS

You can deploy AMPS in three possible scenarios.

- **AMPS with MEM Console and Standalone Site Server:** In this scenario, the MEM Site server and the console are on the same system. Install AMPS on this system that has both the Site server and console.
- **AMPS with MEM Console:** In this scenario, the MEM site server and MEM console are on two different systems. Therefore, you need to install AMPS twice, once on the site server system and once on the MEM console system. First, complete installation of plugin on the site server and then install the plugin on the console system. Plugin software automatically guides and lets you install only the required components on each system (site server and console).
- **AMPS with CAS (Central Administration Site):** Here, the IT infrastructure will have CAS and one or more primary sites, along with optional secondary sites. Details of AMPS installation in CAS is described in the section '[AMPS deployment in CAS](#)'.

### 1.3.1 AMPS deployment in CAS

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

1. Ensure previous versions of AMPS (if any) are uninstalled from all primary site servers and CAS site system.
2. Install AMPS first on CAS system.
3. After the installation is complete on CAS system, install AMPS on all primary site server systems which manage DASH capable systems.
4. It is not required to install AMPS on secondary site server systems.

Similarly, uninstall of AMPS in CAS infrastructure must be done in this order:

1. AMPS must be uninstalled from all primary site servers.
2. Finally, AMPS must be uninstalled from CAS.

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

### 1.3.2 Installing/Upgrading AMPS

To install/upgrade the DASH plug-in for both the above scenarios,

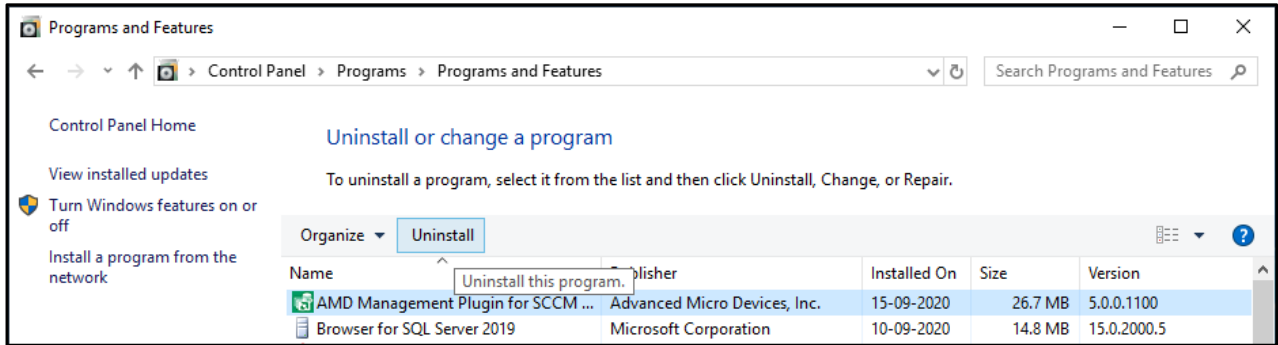
1. Use the *AMPS-<version>-AMD.exe* installer.
2. Follow the steps in the Install wizard to complete installation.

### 1.3.3 Uninstalling AMPS

To uninstall AMPS, perform the following steps:

1. In **Control Panel**, click **Programs and Features**.
2. Double-click the **AMD Management Plugin for SCCM** program to uninstall.

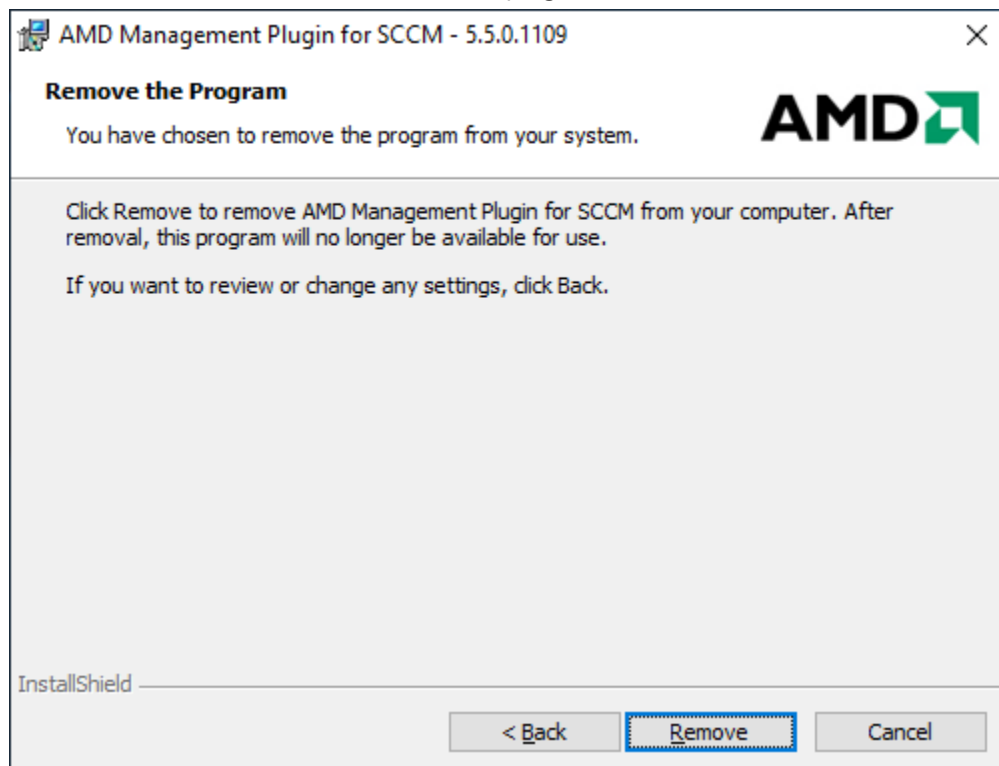




**Figure 1.2: Control Panel AMPS Uninstallation**

Alternatively,

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



**Figure 1.3: Removing AMPS using AMPS installer**

## 1.4 Using the AMPS Features

AMPS extends the MEM Administrator console to support out-of-band management using DASH.

AMPS provides the following features:

- Configure MEM for DASH operations.
- Perform DASH operations on DASH-capable systems.

The AMPS installation creates the following nodes to provide the above features.

- Configuration node called **DASH Configuration**. This node contains the screen to capture the configuration information for DASH.
- Configuration node called **DASH Scheduled Tasks**. This node contains the screen to view all the scheduled DASH tasks
- Collection node called **All DASH Capable Systems**. This collection node contains all the devices which are DASH capable.
- Collection node called **All DASH Managed Systems**. This collection node contains all the devices which are DASH capable and provisioned with working credentials.
- Collection node called **All DASH Unmanaged Systems**. This collection node contains all the devices which are DASH capable but not provisioned correctly.

**Note:** If you are installing the plugin to an MEM console, first install it to the primary site.

### 1.4.1 Accessing the DASH Configuration node

To configure MEM for DASH operations, perform the following steps:

1. In the **Microsoft Endpoint Configuration Manager** window, click **Administration**.
2. Expand the **Overview** node, then click the **DASH Management** node, and select **DASH Configuration**.
3. Click the properties ribbon icon.  
The DASH configuration screen is displayed. For details on configuration, refer to **Chapter 2**.

**Figure 1.4** illustrates these steps.

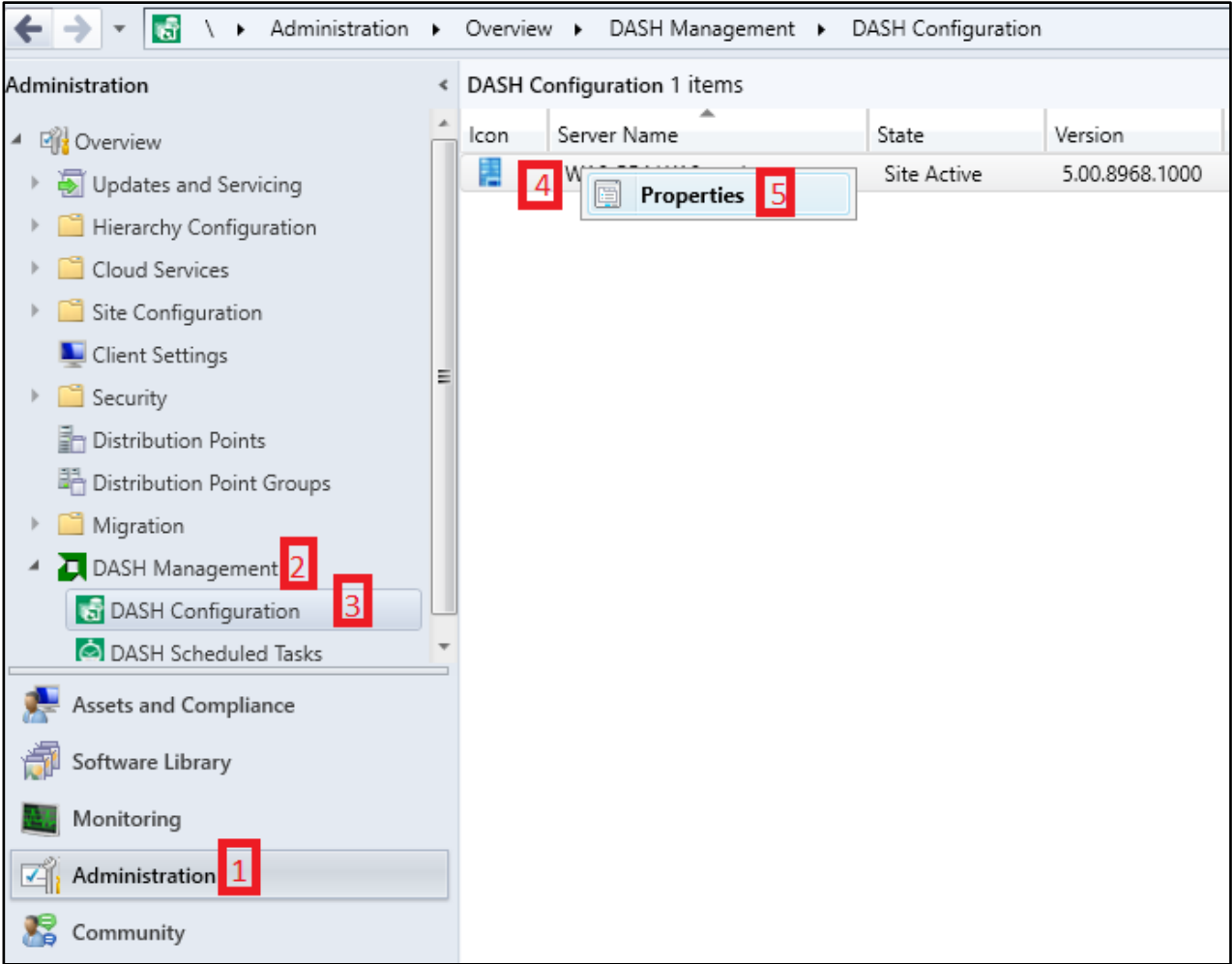
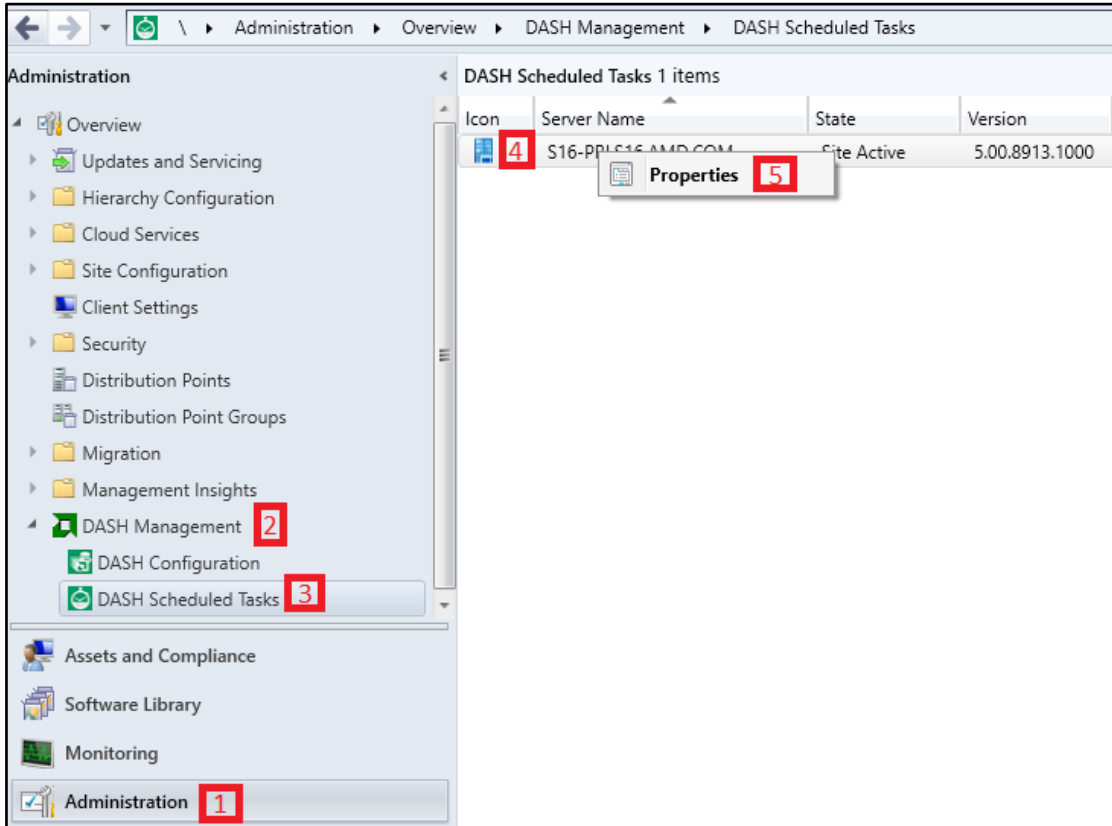


Figure 1.4: Configure MEM for DASH operations

## 1.4.2 Accessing the DASH Scheduled Tasks node

To access the **DASH Scheduled Tasks** node, perform the following steps :

1. In the **Microsoft Endpoint Configuration Manager** window, click **Administration**.
2. Expand the **Overview** node, then click the **DASH Management** node, and select **DASH Scheduled Tasks**.
3. Click the properties ribbon icon.  
The DASH configuration screen is displayed. For details on configuration, refer to **Chapter 2**.  
Figure 1.5 illustrates these steps.



**Figure 1.5: DASH Scheduled Tasks Node**

### 1.4.3 Accessing the All DASH Capable Systems node

To perform DASH operations on DASH capable systems, access the **All DASH Capable Systems** node as follows:

1. In the **Microsoft Endpoint Configuration Manager** window, click **Assets and Compliance**.
2. Expand the **Overview** node and click **Device Collections**.
3. Click the **All DASH Capable Systems** collections node.  
All the systems on which you can perform the DASH operations are displayed.

For details on performing the DASH operations, refer to Figure 1.6 illustrates the steps mentioned above.

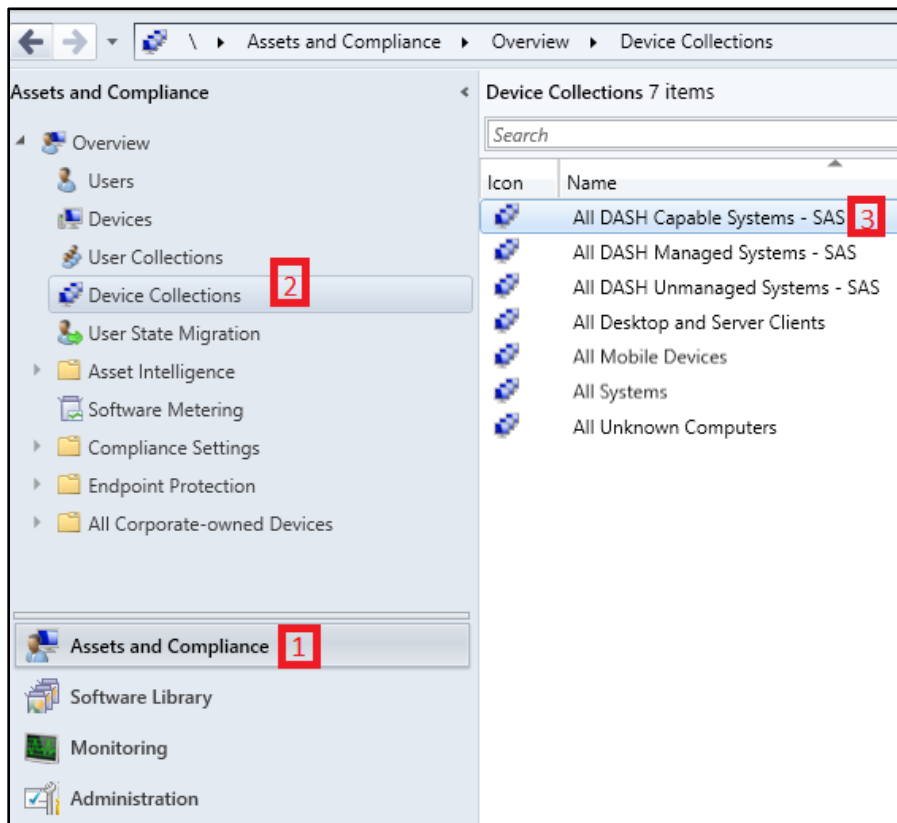


Figure 1.6: All DASH Capable Systems Node

#### 1.4.4 Accessing the All DASH Managed Systems node

To perform DASH operations on the DASH Managed systems, access the **All DASH Managed Systems** node as follows:

1. In the **Microsoft Endpoint Configuration Manager** window, click **Assets and Compliance**.
2. Expand the **Overview** node and click **Device Collections**.
3. Click the **All DASH Managed Systems** collections node.

For details on performing the DASH operations, refer to Figure 1.7 illustrates the steps mentioned above.

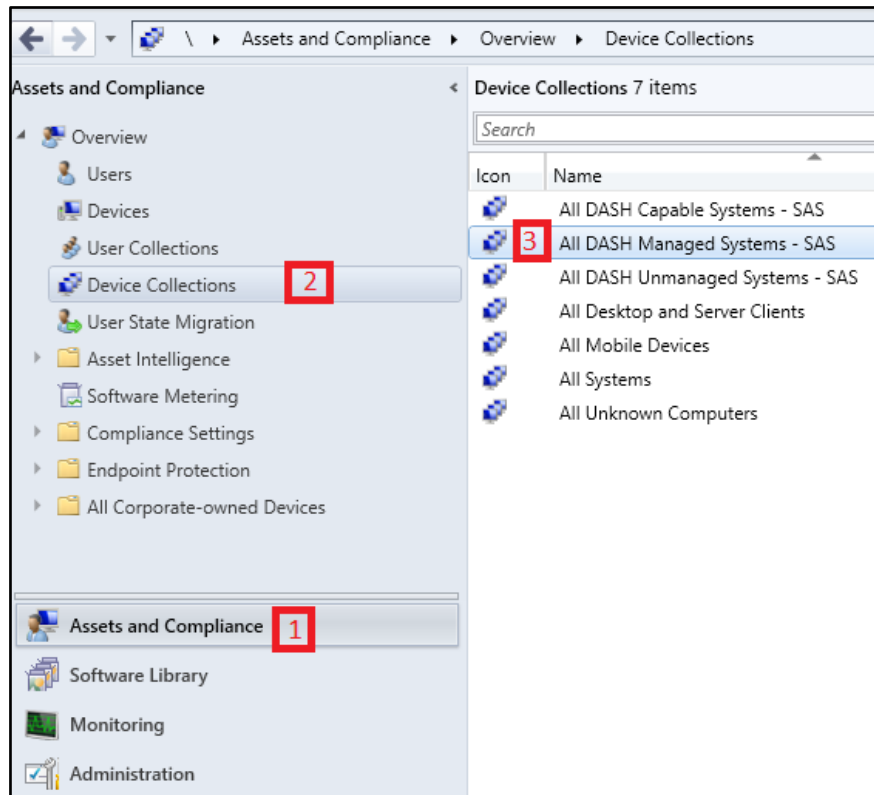


Figure 1.7: All DASH Managed Systems Node

### 1.4.5 Accessing the All DASH Unmanaged Systems node

To perform DASH operations on the DASH Managed systems access the **All DASH Unmanaged Systems** node as follows:

1. In the **Microsoft Endpoint Configuration Manager** window, click **Assets and Compliance**.
2. Expand the **Overview** node and click **Device Collections**.
3. Click the **All DASH Unmanaged Systems** collections node.

For details on performing the DASH operations, refer to Figure 1.8 illustrates the steps mentioned above.

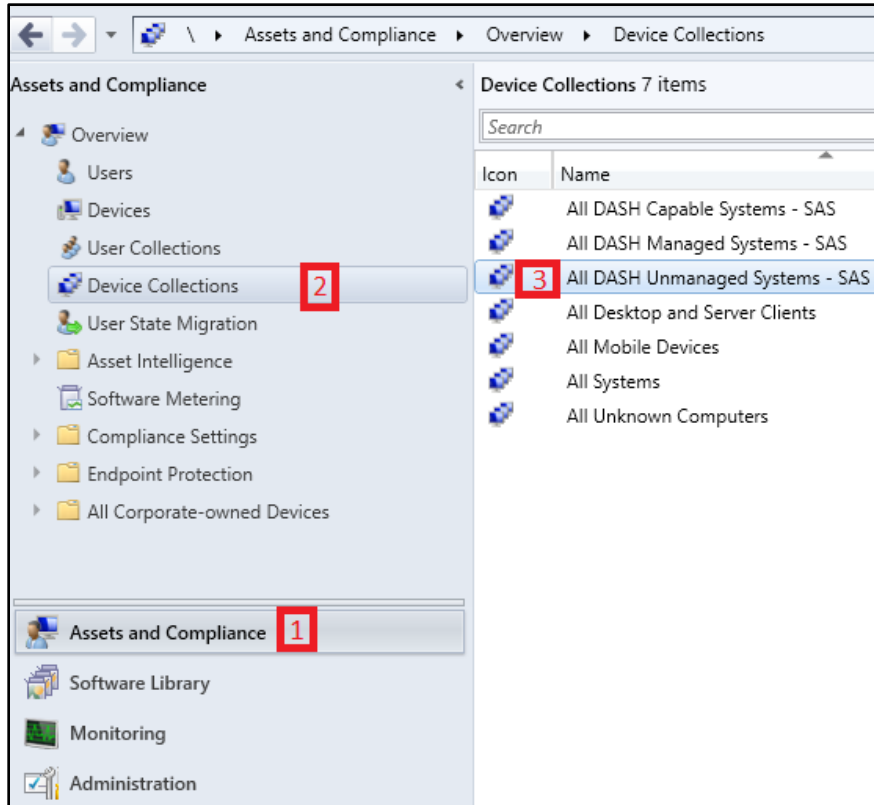


Figure 1.8: All DASH Unmanaged Systems Node

## 1.5 Logging in AMPS

AMPS logs are return to the folder "C:\ProgramData\AMD Management Plugin for SCCM" on AMPS installed systems as shown in Figure 1.9.

This PC > Local Disk (C:) > ProgramData > AMD Management Plugin for SCCM			
Name	Date modified	Type	Size
AlertService.log	23-10-2020 19:39	LOG File	782 KB
AMPSUI-Administrator.log	23-10-2020 19:27	LOG File	189 KB
AMPSUI-AppAdmin.log	17-09-2020 14:30	LOG File	1 KB
AMPSUI-AppAuthor.log	17-09-2020 14:25	LOG File	2 KB
AMPSUI-AppMan.log	17-09-2020 14:13	LOG File	2 KB
AMPSUI-AssetMan.log	17-09-2020 13:51	LOG File	10 KB
AMPSUI-CompSetMan.log	17-09-2020 13:58	LOG File	10 KB
AMPSUI-EPMan.log	17-09-2020 15:29	LOG File	1 KB
AMPSUI-Ganesh.log	15-09-2020 19:36	LOG File	9 KB
AMPSUI-InfraMan.log	17-09-2020 15:16	LOG File	2 KB
AMPSUI-OpAdmin.log	17-09-2020 17:44	LOG File	28 KB
AMPSUI-OpMan.log	17-09-2020 14:32	LOG File	1 KB
AMPSUI-ReadOnly.log	17-09-2020 13:43	LOG File	11 KB
AMPSUI-RemoteTools.log	15-09-2020 19:50	LOG File	8 KB
AMPSUI-SecAdmin.log	17-09-2020 15:26	LOG File	1 KB
AMPSUI-swupdman.log	17-09-2020 15:19	LOG File	1 KB
DASHDeploy.log	23-10-2020 12:23	LOG File	551 KB
DASHService.log	23-10-2020 19:27	LOG File	6,603 KB

Figure 1.9: Folder path of AMPS logs



## Chapter 2      Configuring DASH in MEM


---

The DASH Configuration node allows you to configure for Authentication, Management Port, Management Transport, and DASH Wake-Up.

The DASH Configuration window can be modified only by a user with “Full Administrator” role.

**Important:** Before performing any DASH operation on the client device, configure DASH with correct Authentication, Management Port and Management Transport.

To access the DASH Configuration properties, refer to the **1.4.1** section. The screen in Figure 10 appears.


DASH Configuration
×

### Authentication Schemes

	Auth Identifier	Scheme	Username	Password	Confirm Password
1	AMD	Digest	Administrator	*****	*****
2		<Not Used>			
3		<Not Used>			

### Management Port and Transport

☒ HTTPS (preffered)

☐ HTTP

### Alerts

Event Port : 8080

### Configuration Manager Settings

☒ DASH Wakeup - Use DASH to wakeup a collection of devices during power management and package deployment

☒ DASH Auto Discover - Enable automatic DASH discovery of newly found devices by site server

### TLS certificate for HTTPS

☒ Trust self signed certificate

\* Any self-signed TLS certificate, installed on DASH system will be trusted. Ensure the DASH systems are configured with a TLS server certificate.

### DASH Capable check

☒ Skip the DASH capability check in the menu

Improves performance in certain configurations. Enable only if required

### Cloud Manageability

☐ Enable Cloud Manageability

Server Name: 
 Port:

### Mutual Authentication

☐ Enable Mutual Authentication Support

Certificate (.pem)  Browse

About
Help

Validate
Close

**Figure 10: DASH Configuration Screen**

Note: See section 0 for configuring in CAS infrastructure.

## 2.1 Authentication

AMPS supports up-to 3 authentication entries. Each authentication entry has an authentication identifier, scheme and corresponding credentials. Provide the identifier and credentials while making the authentication entries. AMPS has support for two types of authentication schemes, Digest and Active Directory.

To manage a DASH capable device, the IT administrator needs to provide at-least one valid authentication entry (Identifier, Scheme, Username, and Password). To manage the target, AMPS uses the three entries in sequential order to authenticate itself.

Authentication Schemes

	Auth Identifier	Scheme	Username	Password	Confirm Password
1	Realtek	Digest	Administrator	*****	*****
2	Broadcom	Digest	Administrator	*****	*****
3		<Not Used>			

Figure 11: Authentication Schemes Section

Notes:

- Among the authentication entries, Identifier is unique.
- You cannot have two entries with same identifier.
- You need to configure one of the 3 authentication entries to all the DASH computer systems that AMPS is going to manage.
- Configuring the managed system is beyond the scope of AMPS. The IT administrator needs to use the respective vendor tools to configure the managed computer system.
- To make the changes effective, click on the **Save** button.

## 2.2 DASH Management Ports and Transport

AMPS can communicate with the managed DASH computer systems either on HTTP or HTTPS. User has an option to choose either of the ports or both.

Management Port and Transport

☒ HTTPS (preferred) 664

☒ HTTP 623

Figure 12: Management Ports and Transport Section

Notes:

- The default port for HTTP is 623 and HTTPS is 664.
- The managed ports must match with all managed systems.
- This transport and port selection is used for all the managed DASH computer systems.
- The connectivity details selection is illustrated in Figure 10
- You can make changes to the existing settings.

- To make the changes effective, click on the **Save** button.

## 2.3 Alerts Event Port

AMPS receive alerts from the managed devices for which it subscribes to. The port it should receive alerts should be configured during the installation process of AMPS. The port number entered during installation is visible in the configuration screen against Event Port as shown in Figure 13.



**Figure 13: Alerts Event Port Section**

## 2.4 Configuration Manager Settings

The plugin provides some features that are closely integrated to the MEM functioning. They are:

- DASH Wakeup during package deployment.
- DASH Auto Discovery.

These features are explained in this section.



**Figure 14: Configuration Manager Settings Section**

### 2.4.1 DASH Wakeup during Package Deployment

The DASH Wakeup functionality enables MEM users to utilize secure DASH commands in addition to Wake On LAN (WOL) packets to power up systems.

Wake On LAN (WOL) is an unauthenticated broadcast packet which MEM sends to the collection of devices before a software deployment activity is performed by MEM.

This WOL packet is not guaranteed to Wake all the devices in the collection. Therefore, to authenticate and successfully turn on all the devices part of the collection, before deploying a software, you can use the DASH power on operation provided by the AMPS. .

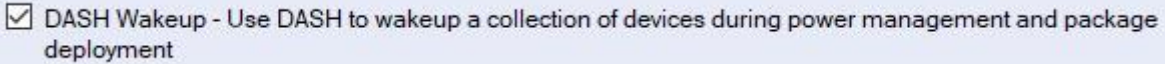
To support the DASH Wakeup feature, perform the following steps:

**Important:** Ensure that a working authentication scheme is saved as explained in the Authentication section.

- In the **DASH Configuration** screen Figure 15 Select the **DASH Wakeup** during Package Deployment check box, if already not selected.

- Ensure to enable the Wake On LAN option and a valid future schedule is associated when creating the software deployment package for a device collection.

If all the above three steps are performed, then DASH power on commands are sent to the device collection before the deployment of the said package.



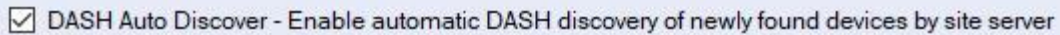
**Figure 15: DASH Wakeup Section**

## 2.4.2 Auto Discovery of DASH Devices

**Discovery** section explains how DASH devices can be discovered for the devices that were part of the MEM before the plugin was installed.

After AMPS installation, if a new device is added to MEM to be managed, the added device is checked for DASH support automatically, if the **DASH Auto Discover** check box is selected.

For more information, refer to Figure 16 Selecting the DASH auto discover checkbox removes the need to do the manual Discovery at a later stage.



**Figure 16: DASH Auto Discover Section**

## 2.5 TLS certificate for HTTPS

Trust self signed certificate option allows administrators to ignore self signed TLS certificates used for HTTPS while performing DASH operations.



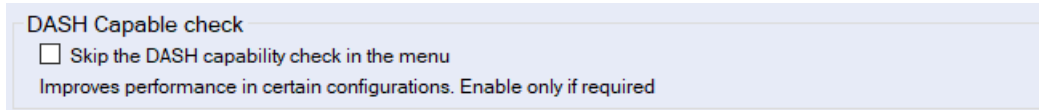
**Figure 17: TLS certificate for HTTPS Section**

## 2.6 DASH Capable check

AMPS validates the selected system if its DASH capable before enabling DASH operations on the system, so SCCM operations will also be blocked until AMPS verifies. If user wants to perform any non DASH operations user will need to wait until AMPS validation is complete. This option helps user to skip the waiting time which AMPS takes to validate DASH capability.

If this option is checked, AMPS will not validate if the user selected system is DASH capable and enables all the DASH operations on the selected system. This option will be helpful only incase user wants to do any non DASH operations.

If this option is not checked, AMPS will perform the DASH capability check before enabling DASH operations on the selected system. By default this option will be unchecked as shown in Figure 18.

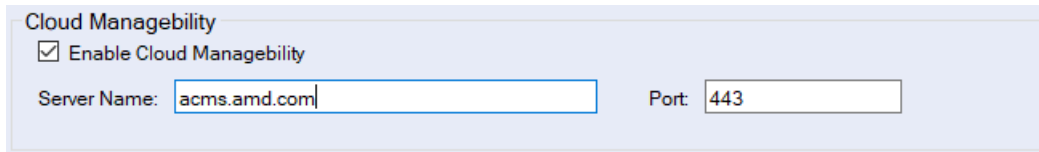


**Figure 18: AMPS DASH Capable check**

## 2.7 Cloud Manageability

AMPS supports Cloud manageability, user can enable this option and provide Cloud server name and Cloud port details so that AMPS can perform DASH operations through Cloud server.

Once this option is enabled all DASH traffic will be routed through Cloud server.

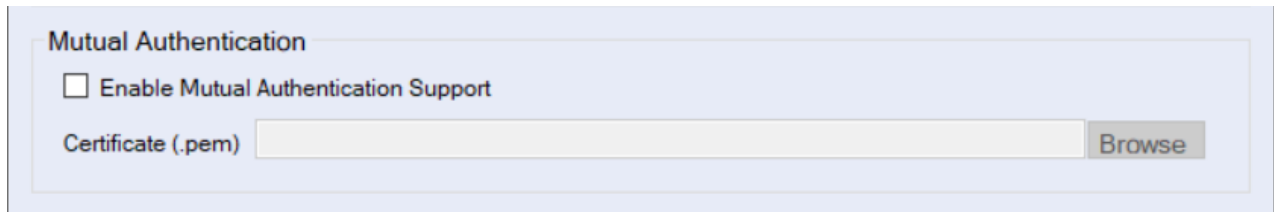


**Figure 19: AMD Cloud manageability settings**

## 2.8 Mutual Authentication

AMPS supports Mutual Authentication, user can enable this option and provide Mutual Authentication certificate path, so that AMPS can perform DASH operations on systems which has Mutual Authentication enabled. Only .pem files are supported for Mutual Authentication..

Once this option is enabled all DASH traffic will be routed through Cloud server.



**Figure 20: Mutual Authentication settings**

## 2.9 Configuration in CAS

In CAS infrastructure, it is required to configure settings for any one primary site server. The same DASH Configuration settings are used by all other primary site servers for communication with DASH capable systems.

Note: It must take few minutes for the configuration settings to propagate in CAS infrastructure. If the settings are not updated, check if replication status is good in Monitoring\Overview\Site Hierarchy section in Console.

## 2.10 Information about the AMPS Plugin

To know about the AMPS plugin version number and URL for other DASH related tools from AMD:

- In the Configuration screen, click the **About** button.  
The **About** screen appears as illustrated in Figure

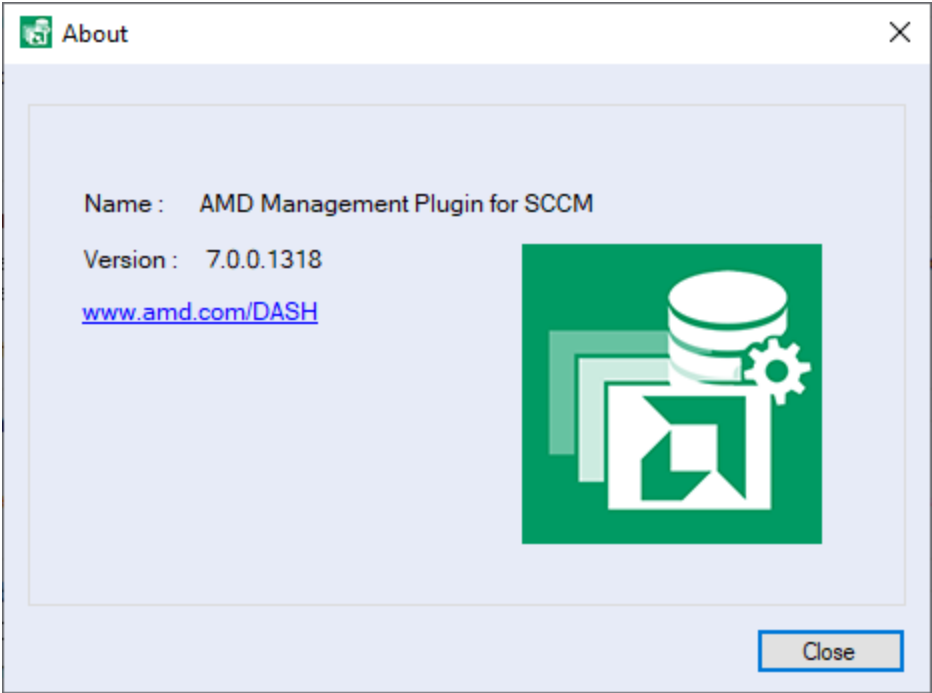


Figure 21: About Screen

## Chapter 3 Performing DASH Operations

---

The AMPS installation creates a collection node called **All DASH Capable Systems**. This collection contains all the devices which are DASH capable.

For information on how to access the **All DASH Capable Systems** node, refer to the section 1.4.3

The following DASH operations can be performed on devices under DASH capable devices:

- Discovery.
- Power Control.
- Boot Control.
- Text Redirection.
- USB Redirection.
- Alerts.
- Inventory.
- Log Entry.
- Boot to Text Image
- Firmware Update
- Boot to BIOS(KVM Profile)
- KVM Redirection

### 3.1 Discovery

The AMPS supports the DASH discovery of DASH capable systems within a collection or the discovery of an individual client device.

#### 3.1.1 Discovering a Collection

The AMPS Discover feature allows you to automatically discover the DASH capable systems within a collection.

To discover DASH capable client systems in a collection, perform the following steps:

1. Expand the **Assets and Compliance** node.
2. Click **Device Collections**.  
In the right pane, list of all the collections appears.
3. Right-click the collection in which you want to discover all the DASH capable systems.  
The shortcut menu appears.
4. In the shortcut menu, Point to **DASH** and then click **Discover**.

Discovery of the DASH capable client systems in **All Systems** Collections is illustrated in Figure



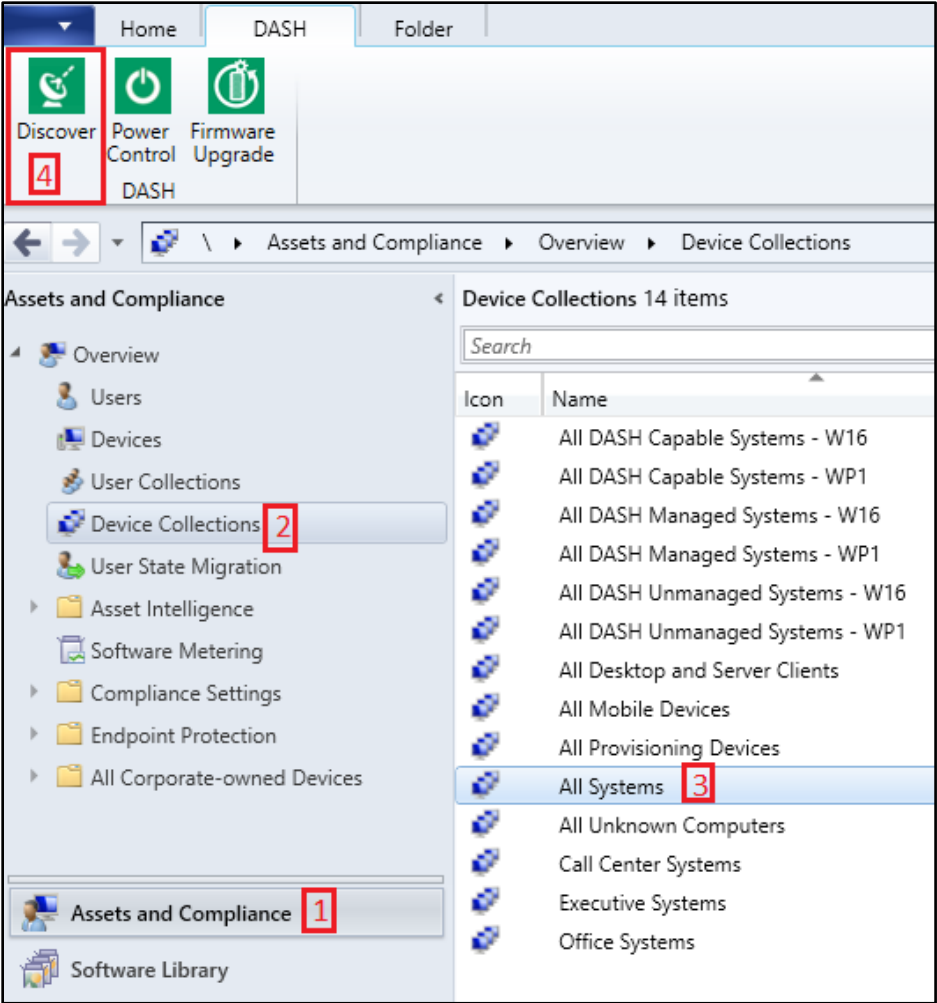


Figure 22 DASH Collection Node

The **Discover Collection** dialog box appears as shown in Figure 20 & Figure 21.

- 5. To discover DASH capable systems in the collections, click the **Apply** button.

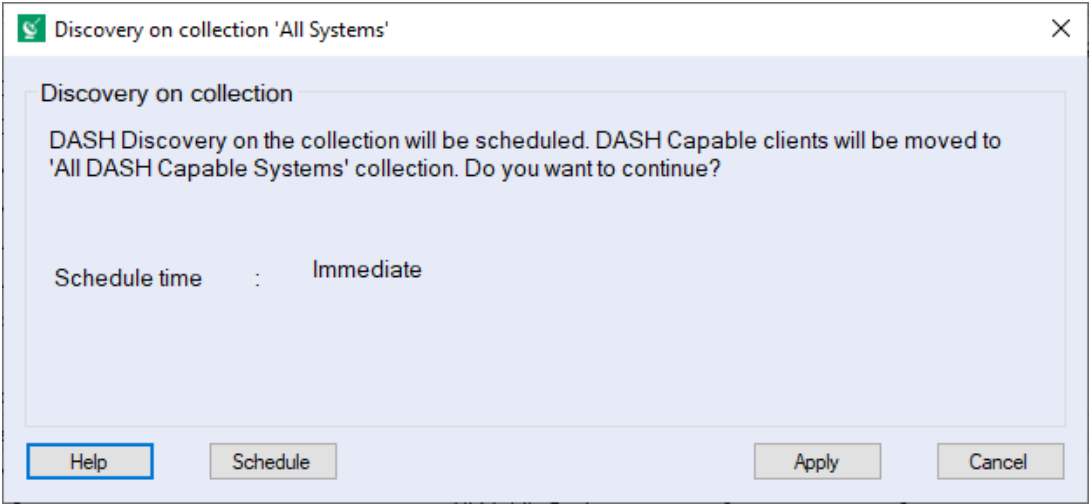


Figure 20: Immediate Discovery Schedule on Collection

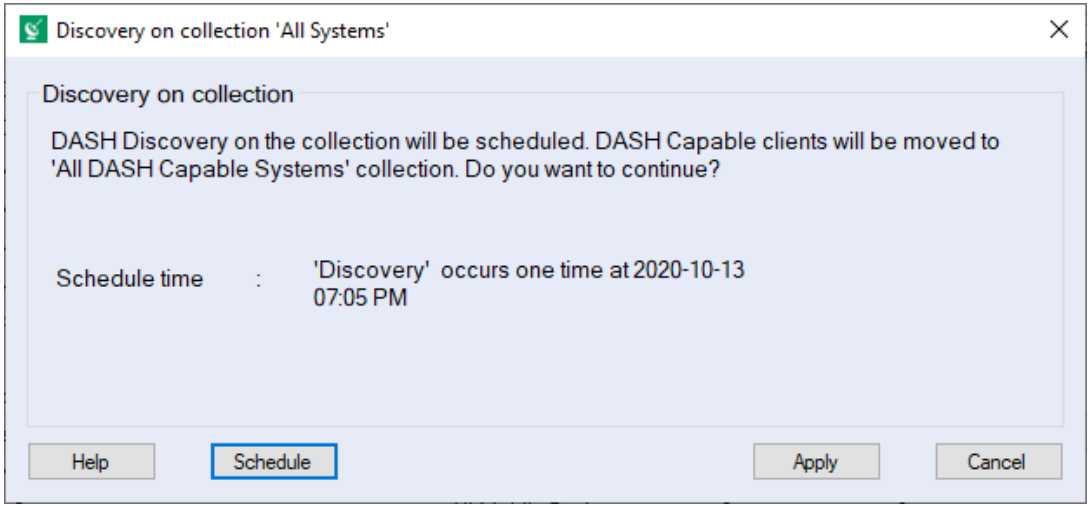
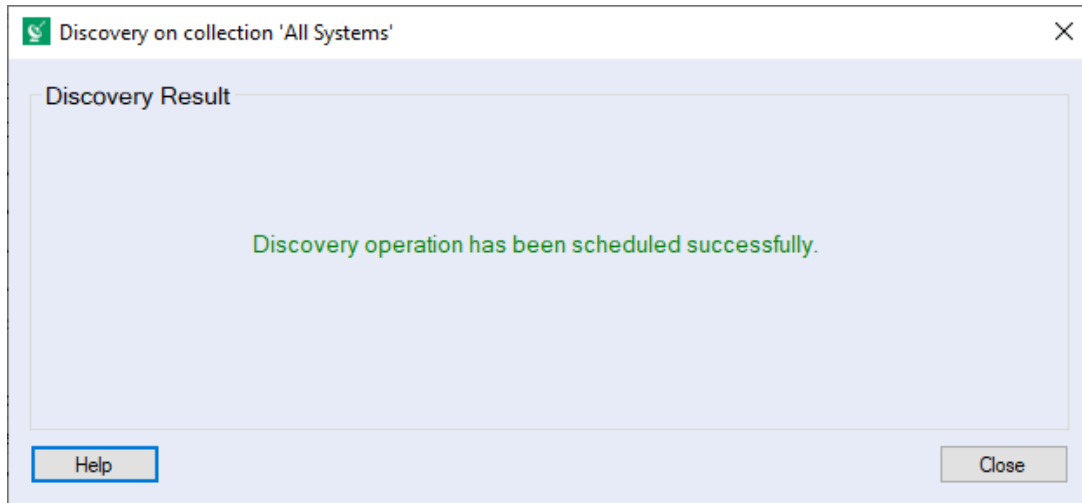


Figure 21: Schedule Discovery on Collection

The systems that are DASH capable are now moved to the **All DASH Capable Systems** collection.



**Figure 22: Discovery Result**

this is the window shown when user clicks on "Apply" button.

### 3.1.2 Discovering a Device

This feature enables you to discover a single DASH capable system.

To discover an individual DASH capable system, perform the following steps:

1. Expand the **Assets and Compliance** node.
2. Expand the **Devices** node and click **All Systems**.
3. In the right pane, right-click the device for which you want to discover DASH. The shortcut menu appears.
4. In the shortcut menu, point to **DASH** and then click **Discover**.

The Discover a Device procedure is illustrated in Figure 23.

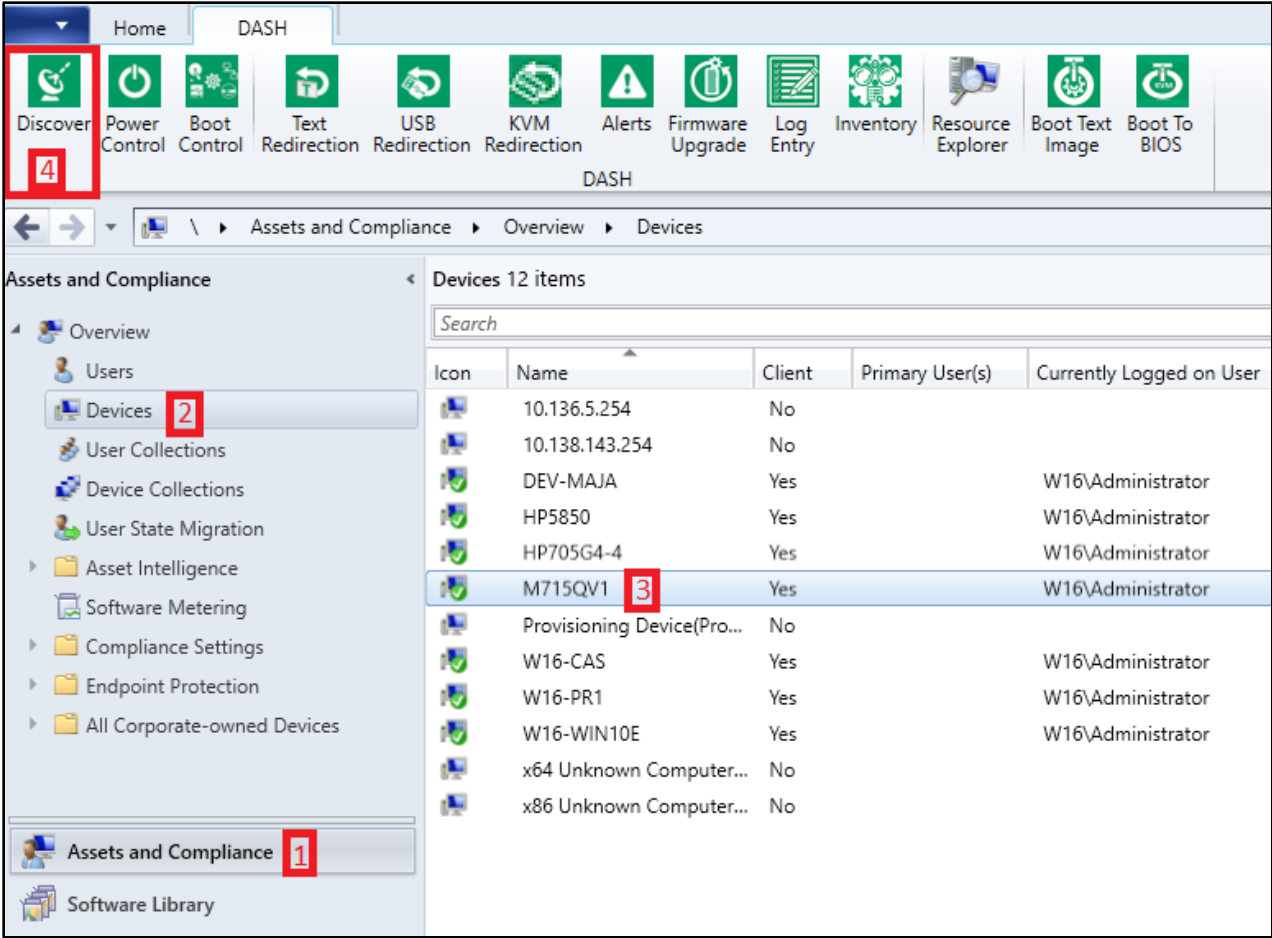
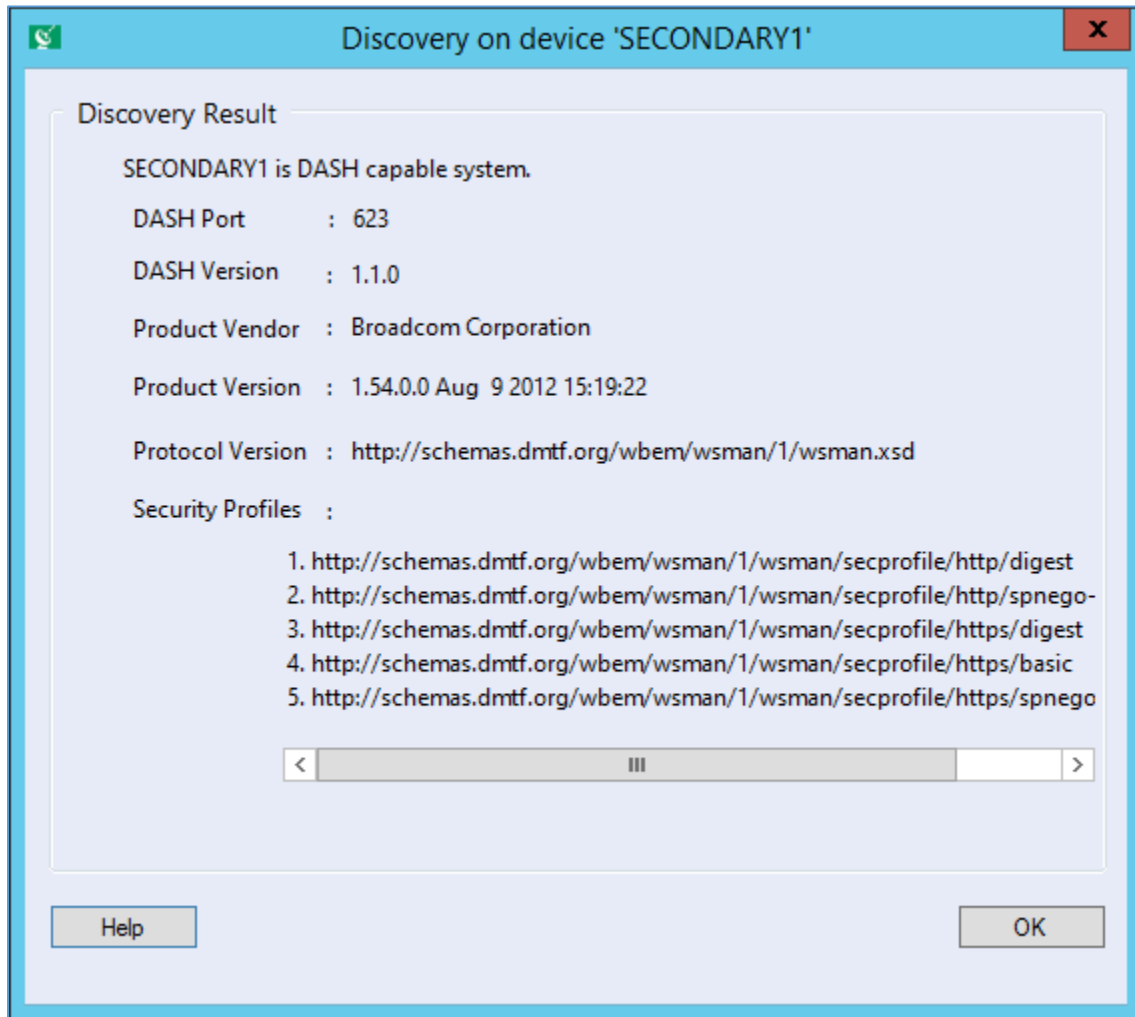


Figure 23: DASH Discovery on a Device

The **Discovery Result** dialog box appears as shown in Figure 24.



**Figure 24: Result of Discovery on Device**

5. In the **Discovery Results** dialog box, click the **OK** button.

The system that are DASH capable are now moved to the **All DASH Capable Systems** collection.

## 3.2 Power Control

This feature allows you to control the power state of a DASH-capable client system or group of systems, including power on, power off, power reset, and power cycle.

### 3.2.1 Power Control on Collection

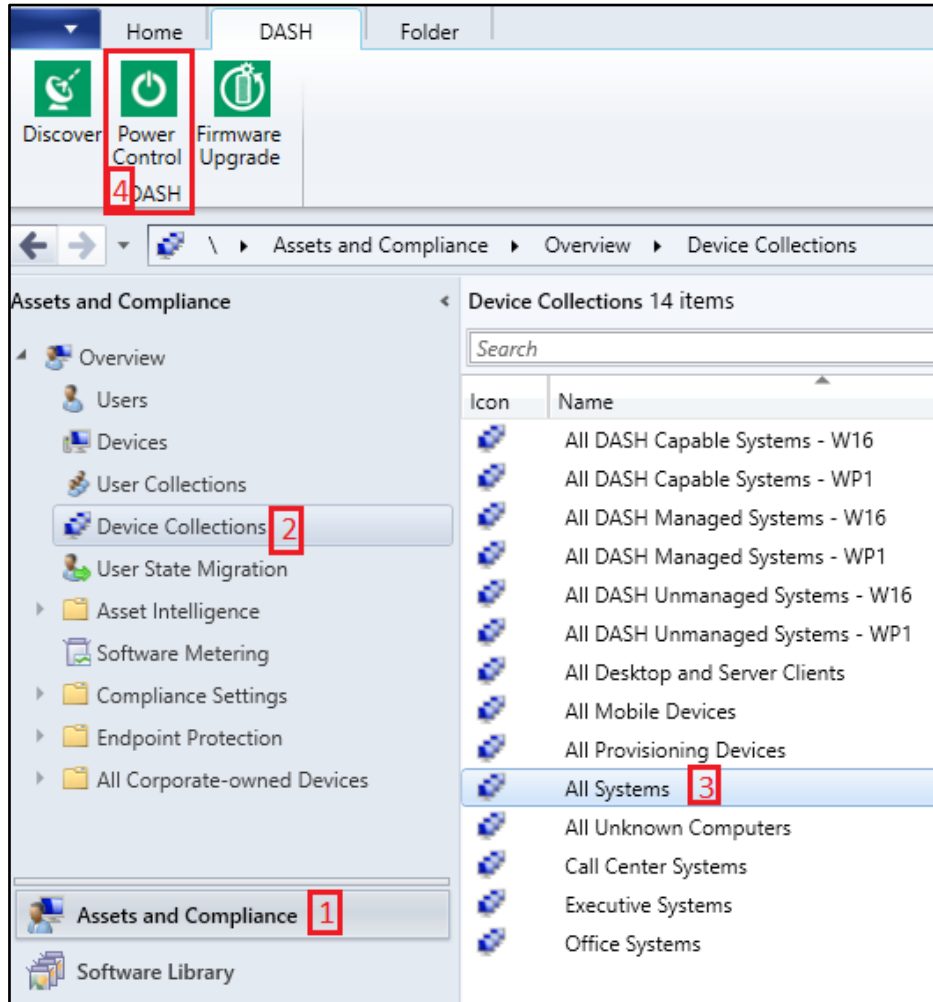
AMPS allows you to control the power state of a group of systems in a given collection.

To control the power state of a collection node, perform the following steps:

1. Expand the **Assets and Compliance** node.

2. Expand the **Overview** node and click **Device Collections**.  
In the right pane, the list of all the available collections appears.
3. Right-click the collection for which you want to initiate power control.  
The shortcut menu appears.
4. In the shortcut menu, select **DASH** and then click **Power Control**.

Figure 25 illustrates the above steps.



**Figure 25: Power Control on Collection**

The **Power Control on Collection** dialog box appears, as shown in Figure 26 and Figure 27.

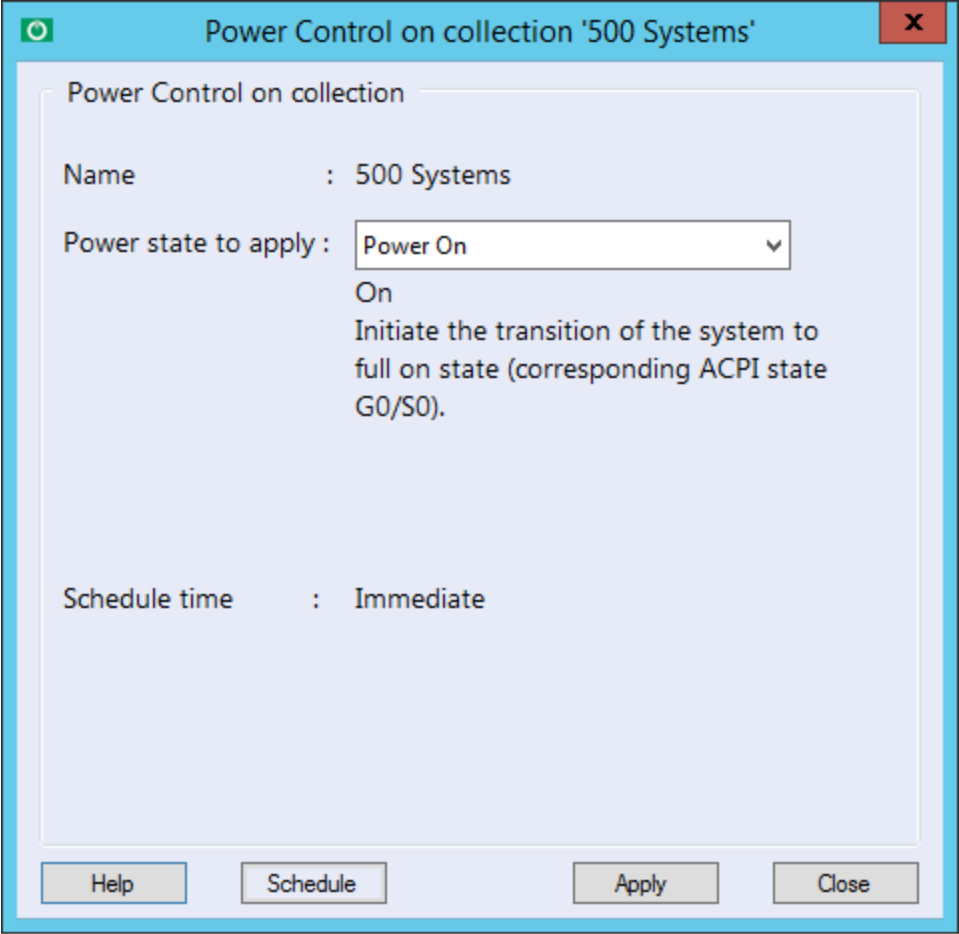
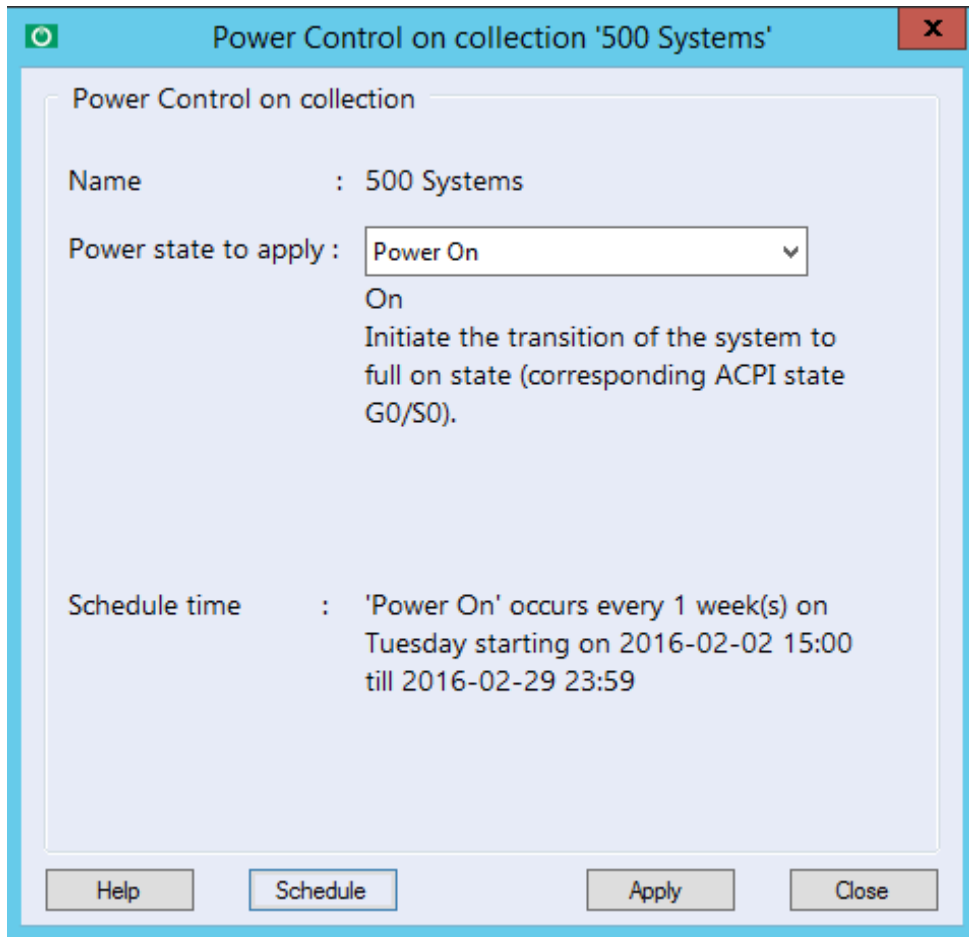


Figure 26: Immediate Power Control on Collection



**Figure 27: Scheduled Power Control on Collection**

5. In the **Power Control on Collection** dialog box, select a desired value from the **Power state to apply** drop-down list.

The following power state options are available:

- **Power On:** Initiates the transition of the system to the full ON state (corresponding ACPI state G0/S0).
- **Sleep:** Initiates the transition of the system to the standby or sleep state (G1/S3).
- **Hibernate:** Initiates the transition of the system to the hibernation state, writes system context to non-volatile storage, and powers off the system and devices (G1/S4).
- **Power Shutdown:** Initiates the transition of the system to the off state (corresponding ACPI state G2/S5), in which the system consumes a minimal amount of power.
- **Power Restart:** Initiates an orderly transition of the system to the power off state (corresponding ACPI state G2/S5), in which the system consumes a minimal amount of power, followed by a transition to the on state (corresponding ACPI state G0/S0).
- **Power Immediate Warm Reset:** Initiates a hardware reset of the system.

**Note:** The **Power Shutdown** and **Power Restart** functions depend on the capabilities of the managed device.

6. Schedule Time states the occurrence of the specified power task. It can be immediate (shown in Figure 26) or Scheduled (shown in Figure 27).
7. To apply the changes, click the **Apply** button.
8. To schedule a power task for collection, click the **Schedule** button.



### 3.2.2 Power Control on Device

AMPS allows you to control the power state of an individual DASH client. To control a DASH client's power state, perform the following steps:

- 1. Expand the **Assets and Compliance** node.
- 2. Expand the **Overview** node and click on **Devices**
- 3. In the right pane, right-click the device on which you want to apply power control. The shortcut menu appears.
- 4. In the shortcut menu, select **DASH** and then click **Power Control**.

Figure 28 illustrates the above procedure.

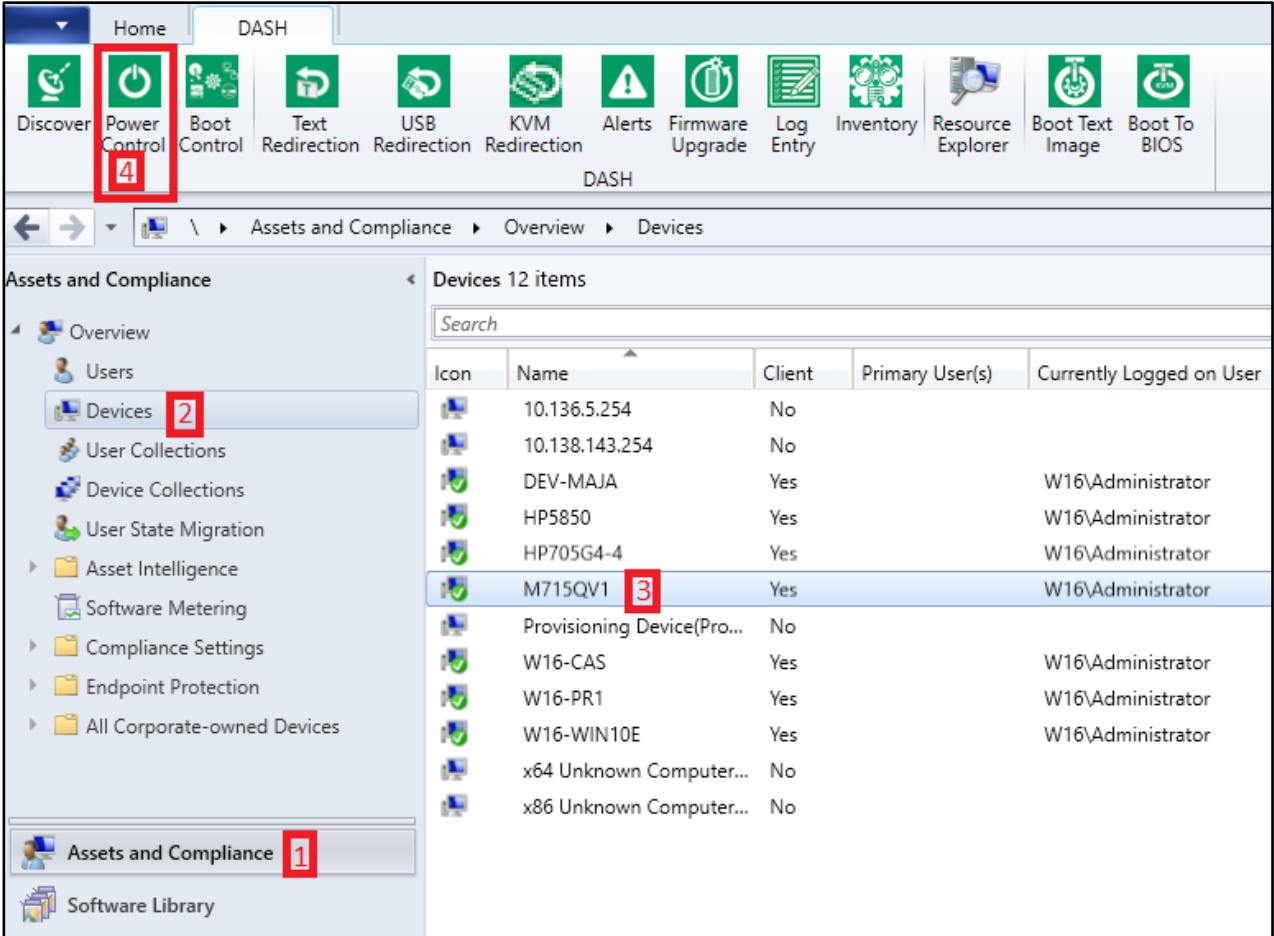
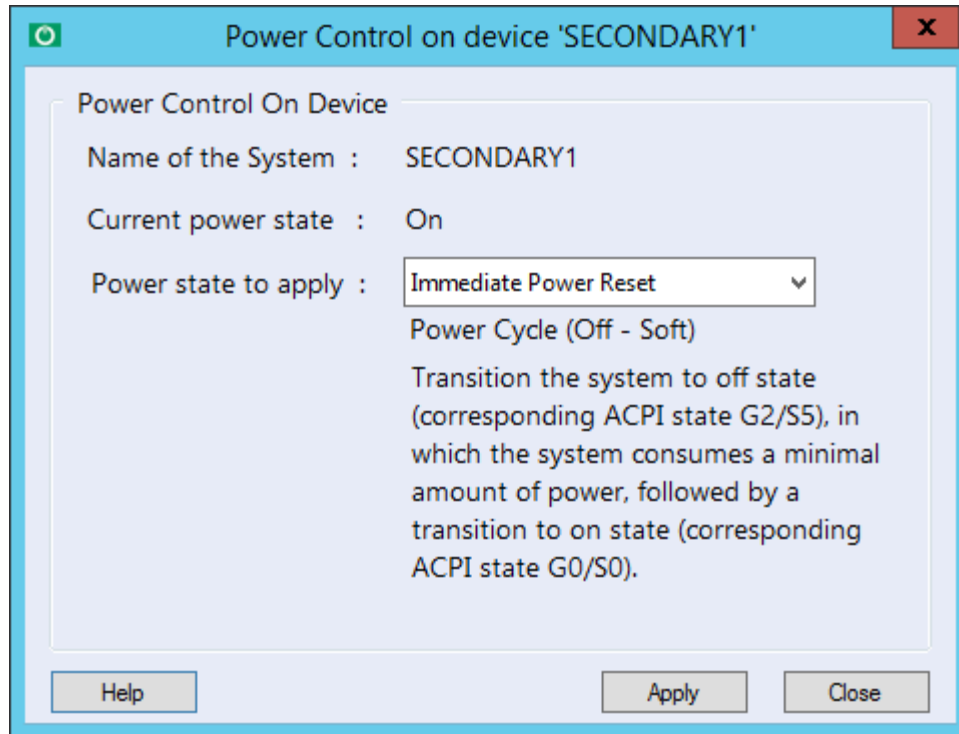


Figure 28: Power Control on Device

The Power Control on Device dialog box appears as shown in Figure 29.



**Figure 29: Power Control on Device**

5. In the **Power Control on Device** dialog box,
  - a. From the **Power state to apply** drop-down list, select the required value.
  - b. To set the selected power state, click the **Apply** button.

### 3.2.3 Power States

The following table lists the possible power states that a computer system can support.

Power State	Friendly Name	Description	Corresponding ACPI State
Power On	On/Power On	Initiates the transition of the system to full on state.	G0/S0
Sleep – Light	Sleeping Lightly / Sleep Light	Initiates the transition of the system to standby or sleep state.	G1/S1 or G1/S2
Sleep – Deep	Sleeping/Sleep	Initiates the transition of the system to standby or sleep state.	G1/S3
Power Cycle (Off Soft)	Immediate Power Reset	Initiates the 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 then G0/S0
Power Off – Hard	N/A	Initiates the transition of the system to power off state, in which the power consumption is zero except for the real-time clock.	G3
Hibernate	Hibernating / Hibernate	Initiates the transition of the system to hibernation state. – write system context to non-volatile storage, power off the system and devices.	G1/S4
Power Off – Soft	Off / Immediate Power Off	Initiates the transition of the system to off state, in which the system consumes a minimal amount of power.	G2/S5
Power Cycle (Off Hard)	N/A	Initiates the 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
Master Bus Reset	Immediate Warm Reset	Performs hardware reset on the system.	
Diagnostic Interrupt (NMI)	Immediate Diagnostic Interrupt	Asserts an NMI on the system.	

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

### 3.2.4 Scheduled Power Control

If you want to power on all the systems at a particular time of the day, perform the following steps.

1. Utilize the MEM's **Power Management** feature screen as illustrated in Figure 30.
2. Select the **Wakeup time (desktop computers)** check box.

**Notes:**

- AMPS looks for the status of the **Wakeup time** checkbox in MEM's power management feature screen and the **DASH Wakeup** checkbox in the **DASH Configuration** screen (refer to Figure 30).
- If both the checkboxes are checked, AMPS performs an authenticated DASH power on to ensure that the devices in question are powered on at the appropriate time as scheduled.

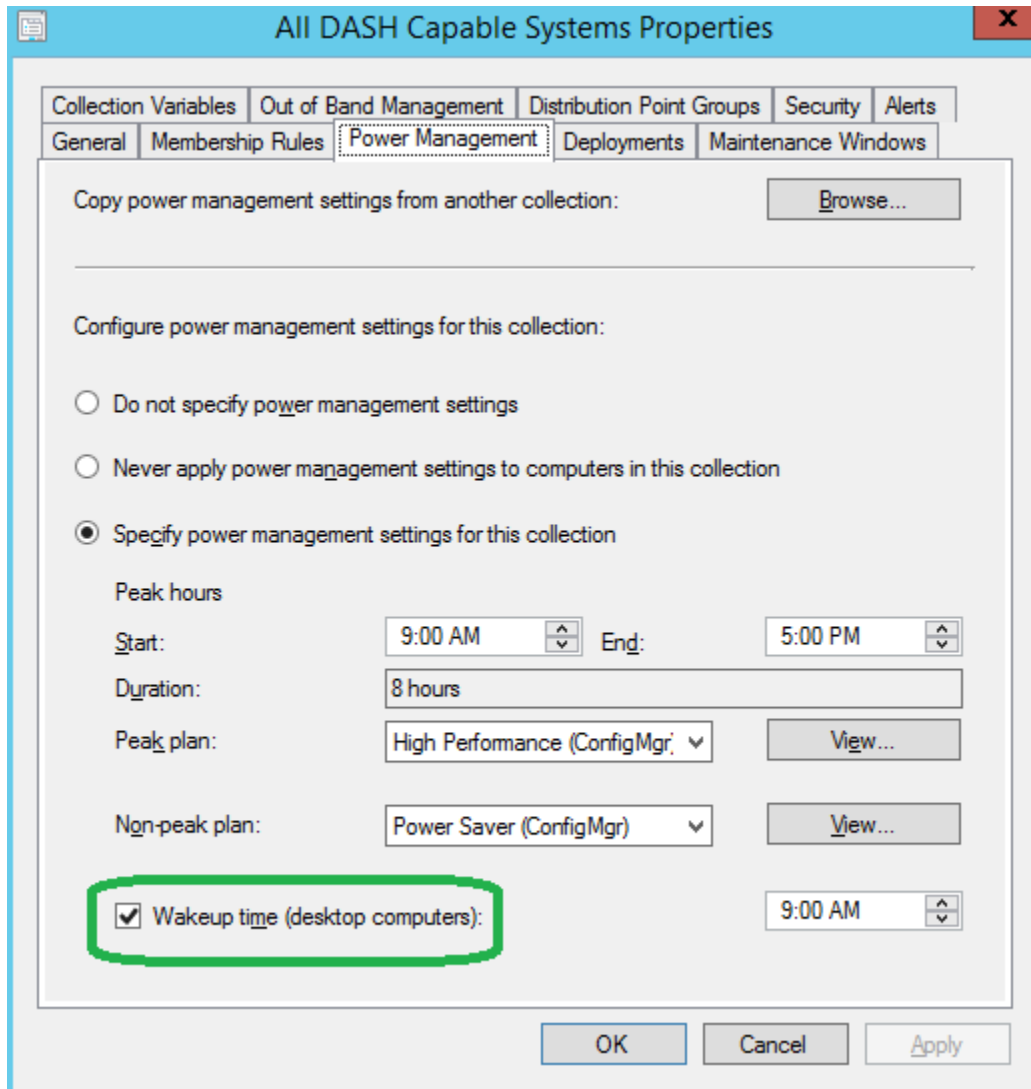


Figure 30: Scheduled Power Control

### 3.3 Boot Control

A boot configuration consists of a boot order, which specifies the order of boot devices.

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 boot order needs to be followed during the next boot process.

AMPS'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 IT administrator to modify the boot order, if required. This version of AMPS only informs the present value of the setting data) but does not allow you to modify this.

To perform the Boot task, perform the following steps in AMPS:

1. Expand the **Assets and Compliance** node.
2. Expand the **Devices** node and click **All Systems**.

- 3. In the right pane, right-click the device on which you want to change the boot order.  
The shortcut menu appears.
- 4. In the shortcut menu, point to **DASH** and then click **Boot Control**.

This procedure is illustrated in Figure 31.

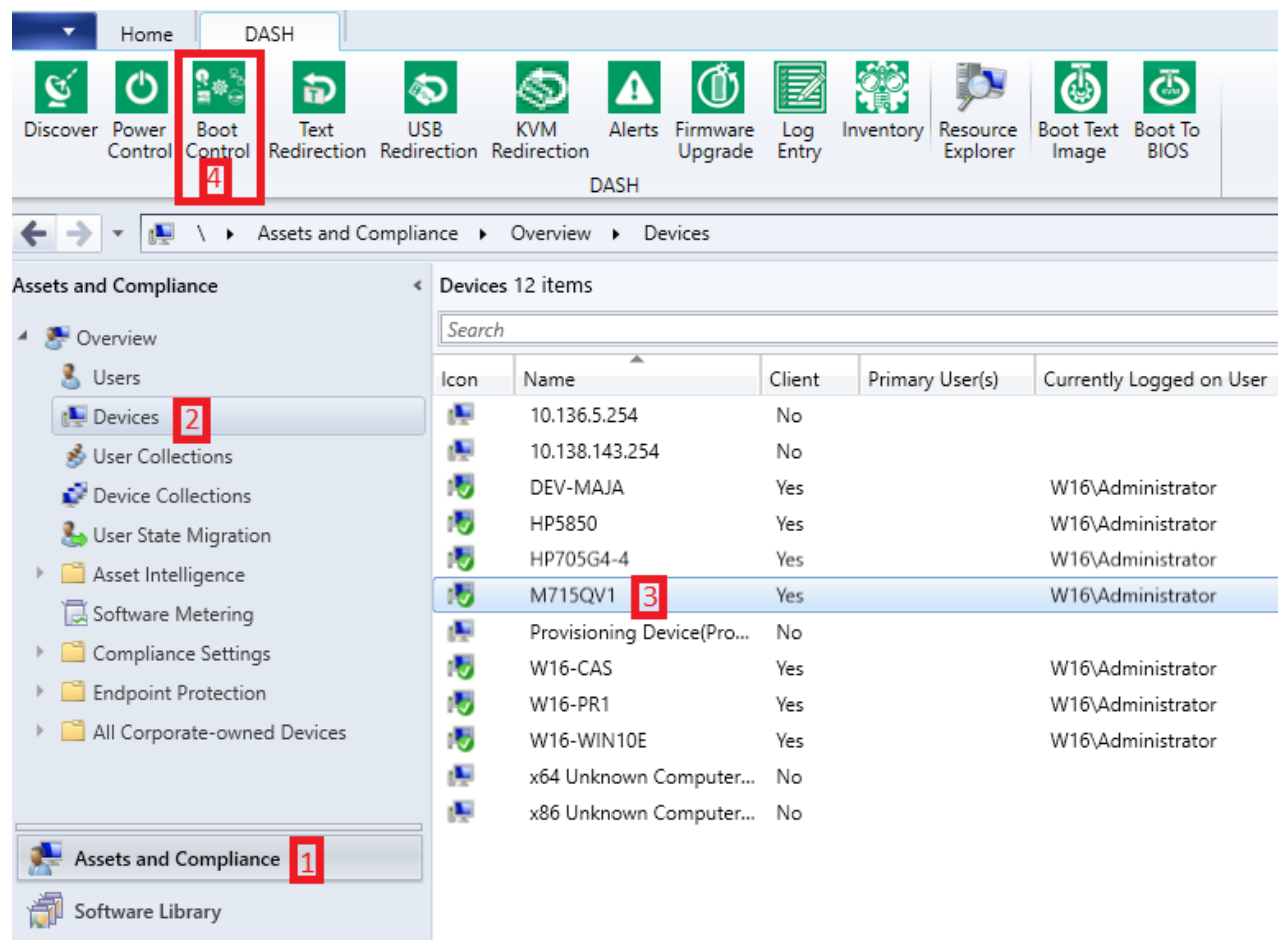
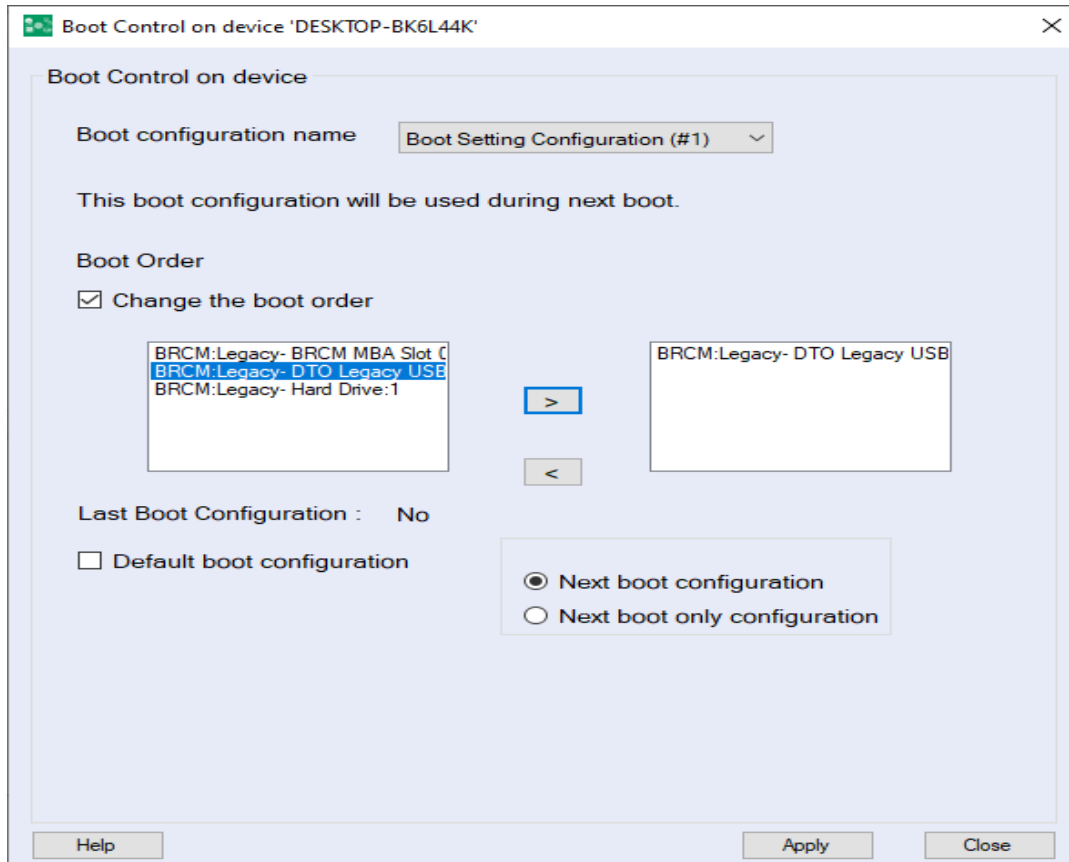


Figure 31: DASH Boot Control on Device

The **Boot Control on Device** dialog box appears as shown in Figure 32.



**Figure 32: Boot Control on Device**

5. In the **Boot Control** on Device dialog box,
  - a. From the Boot configuration name drop-down list, select a **Boot configuration setting**.
  - b. If you want to change the Boot order, under Boot Order, select the Change the Boot order check box
  - c. To save the selection in the right pane, in the left pane, select the required boot order(s) and click the '>' button.
  - d. User can change Default boot configuration by clicking checkbox and can change Next boot configuration with Next boot only configuration.
  - e. To save the changes, click the Apply button.

**Notes:**

- You don't need to move all the Boot devices from the left pane to the right pane 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.

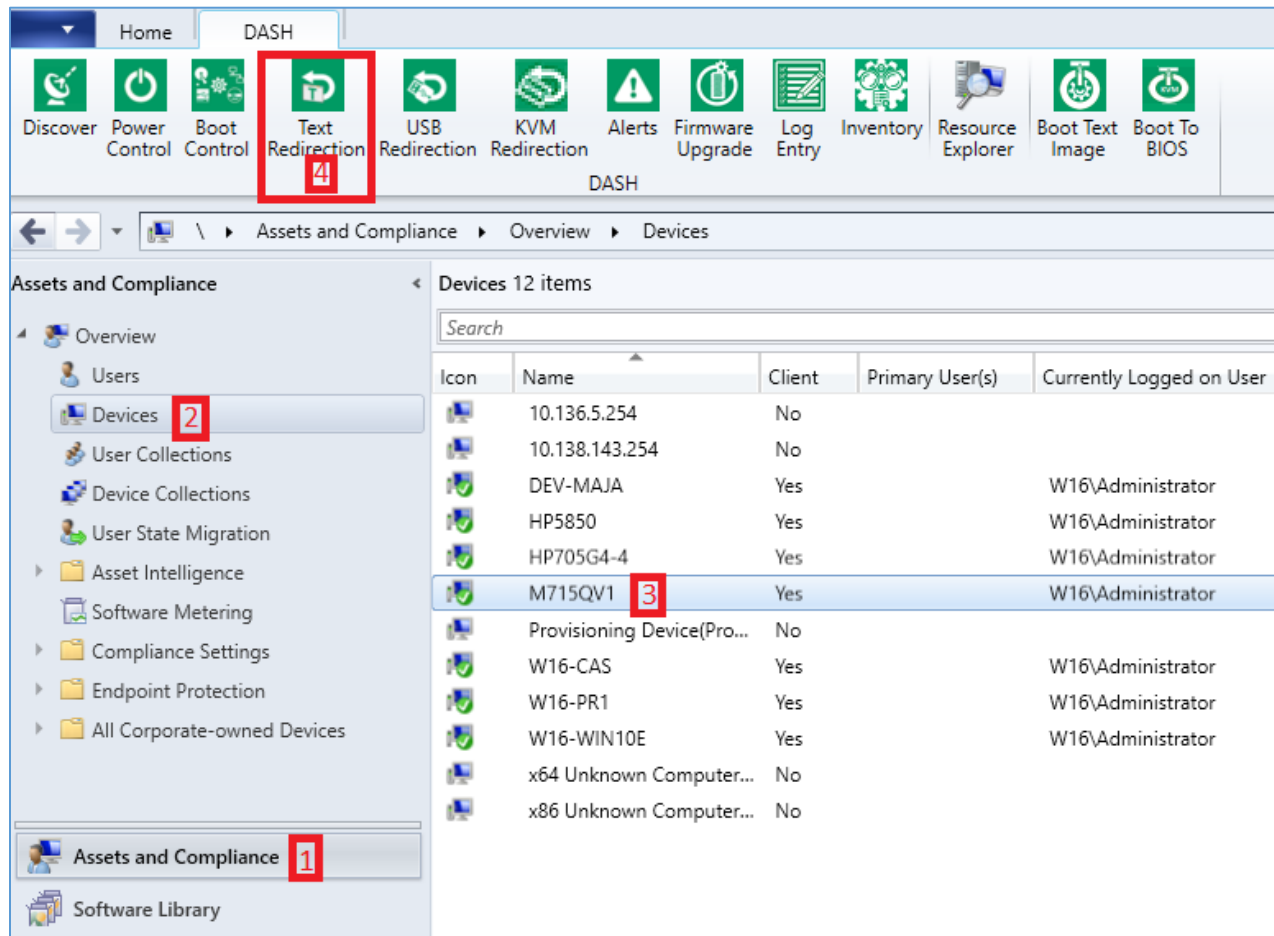
## 3.4 Text Redirection

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. AMPS has a terminal screen through 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 AMPS.

To perform the same follow these steps in AMPS:

1. Expand the **Assets and Compliance** node.
2. Expand the **Overview** node.
3. Expand the **Devices** node and click **All Systems**.
4. In the right pane, right-click the device on which you want to perform Text Redirection. The shortcut menu appears.
5. In the shortcut menu, point to **DASH** and then click **Text Redirection**. Alternatively, on the ribbon icon, click **DASH** and then click **Text Redirection**.



**Figure 33: Text Redirection on device**

6. 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.
7. From the **select protocol** drop-down list,select the required protocol.
8. Click the **Connect** button.

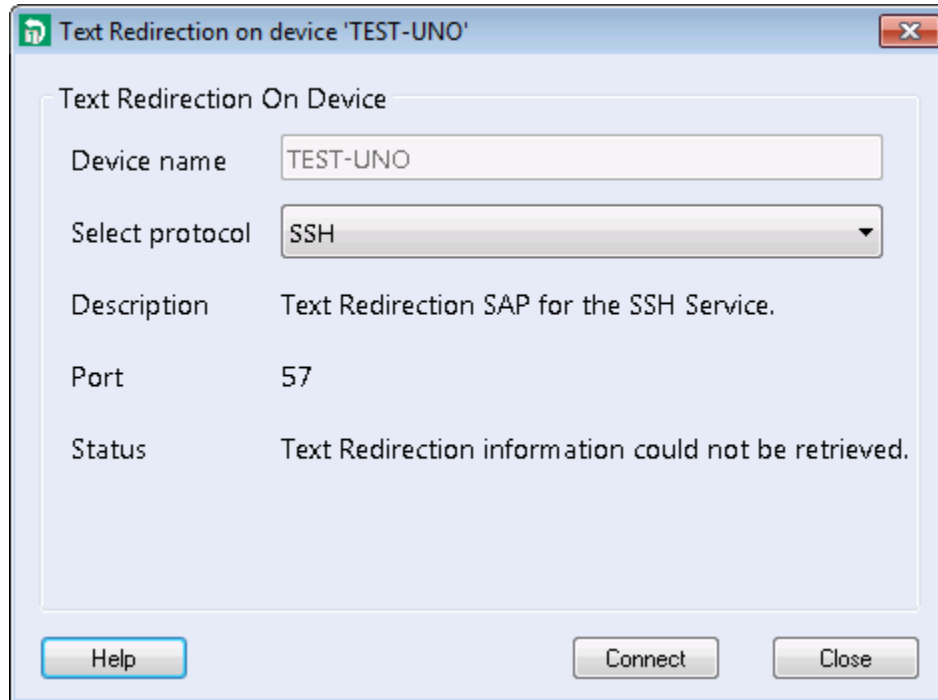
If the connection is successful , the **Text Redirection** screen closes and the **Terminal Console** screen appears .



9. If Text Redirection is no more required from the said system, close the Terminal Console screen.

**Notes:**

- If OTP is supported, the Terminal Console connects automatically to the system.
- If OTP is not supported, in the Terminal Console, enter the credentials. On successful authentication, text activity on the system is redirected to the Terminal Console.



**Figure 34: Text Redirection**

To view and manage the BIOS remotely from AMPS:

1. Select a system for which you want to view and manage the BIOS.
2. To activate the Terminal Console in order to receive the redirected text from the system, perform the steps 2 to 6 listed above.
3. From the available power states, click the **Power** icon and select the **graceful power cycle** option.
4. To change the power state, click the **Apply** button.

The **Terminal Console** screen launched by AMPS receives the **Boot** screen remotely and you can interact with the remote system using the keystrokes from the AMPS system.

## 3.5 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.

To initiate a USB redirection for a system, perform the below steps:

1. Expand the **Assets and Compliance** node.
2. Expand the **Overview** node.
3. Expand the **Devices** node and then click **All Systems**.
4. In the right pane, right-click the device on which you want to perform USB redirection. The shortcut menu appears.
5. In the shortcut menu, point to **DASH** and then click **USB Redirection**.  
If the managed system is capable of redirecting the USB, the **USB Redirection** screen appears.

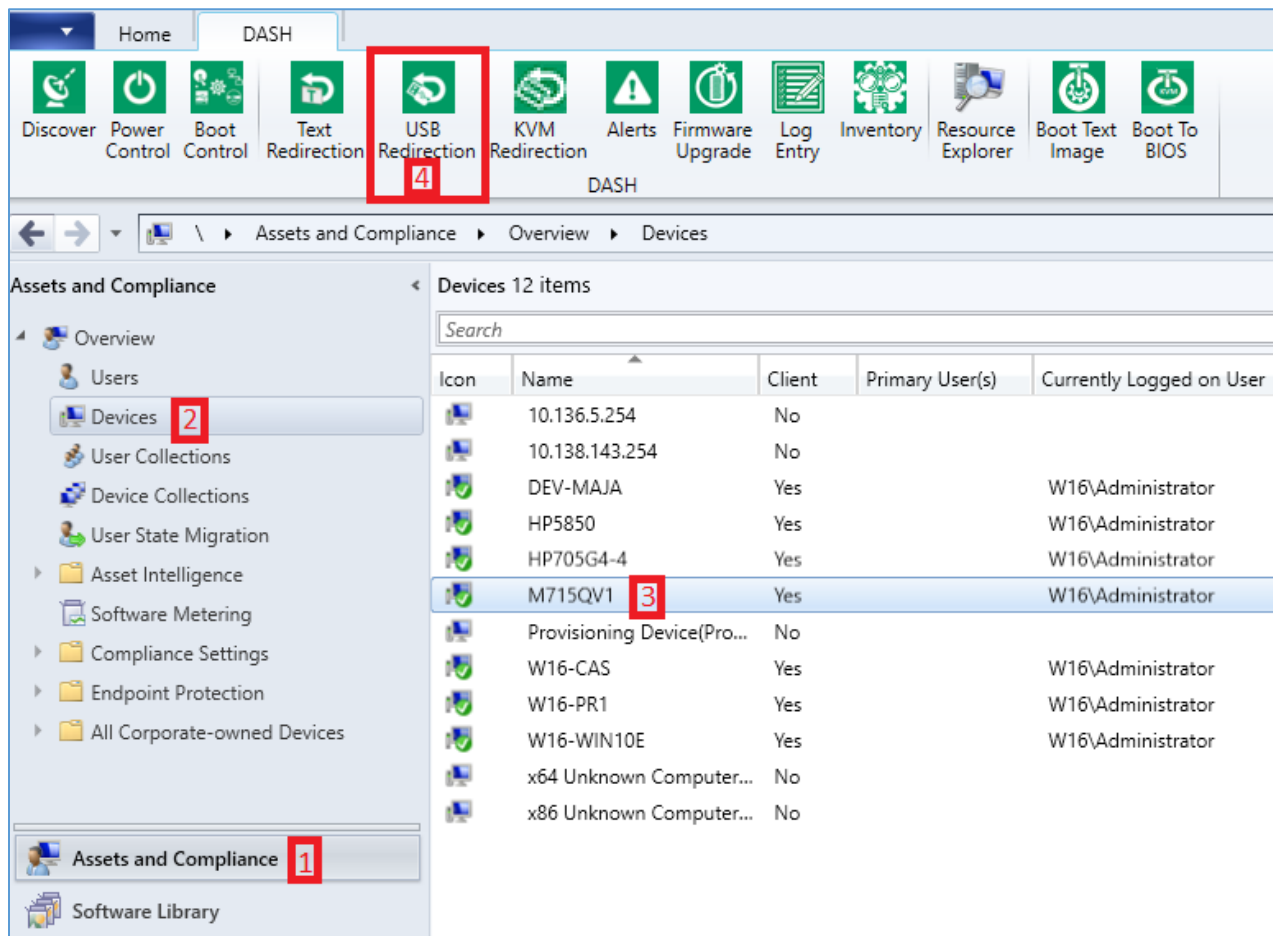


Figure 35: USB Redirection on Device

6. The USB Redirection Screen displays the following :
  - a. The name of the system for whose USB,AMPS is going to attach the remote URL.
  - b. The URL that has to be attached to the systems USB.
    - i. If the USB is already attached to the remote URL,then the attached URL is displayed , and the option to edit the URL field is grayed out. You can disconnect the attached USB by clicking the **Disconnect** button on the screen.
    - ii. If the USB is not attached , you can replace/update any existing URL or enter a new valid URL and click the **Connect** button.

A template and example is shown below as URL example on the correct format for the URL. AMPS only validate the URL format. Ensure the existence of the URL and accessibility of the URL by the managed target as this is outside the scope of AMPS. The result of the operation is displayed .

7. To close the USB Redirection screen , click the Close button.

USB Redirection On Device'HP6005-AA'

**USB Redirection On Device**

Device Name: HP6005-AA

Redirection Name: USB Redirection SAP

Element Name:

Connection Mode: Connect

URL \*: http://10.138.142.86:3274/dos.iso

Enabled State: Disabled

URL example:  
 http://username:password@192.168.1.20/filename.iso  
 http://192.168.1.20/filename.iso

\* Provide valid URL which is accessible from the managed device.

Buttons: Help, Connect, Disconnect, Close

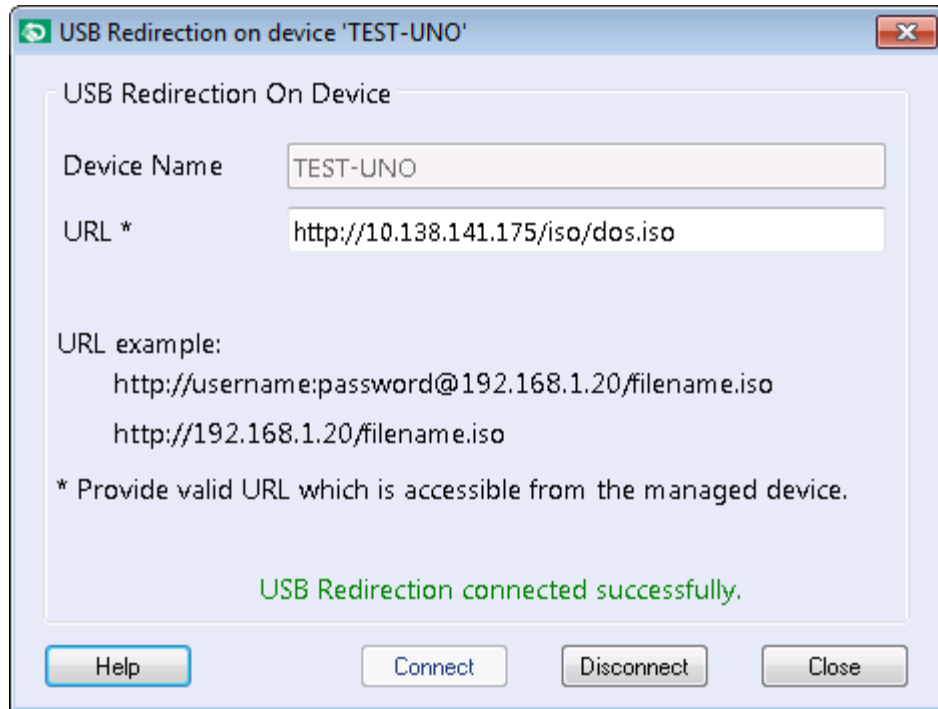
**Figure 36: USB Redirection**

### 3.5.1 Connecting USB Redirection

When the specific system is selected and USB Redirection is opened, **Device Name** field is filled automatically and grayed out.

When you enter the URL, it checks to confirm whether the URL is valid or not.

- If the URL is valid, a message, **USB Redirection connected**, appears as shown in Figure 37.
- If the URL is invalid, error message appears.



**Figure 37: USB Redirection Connect**

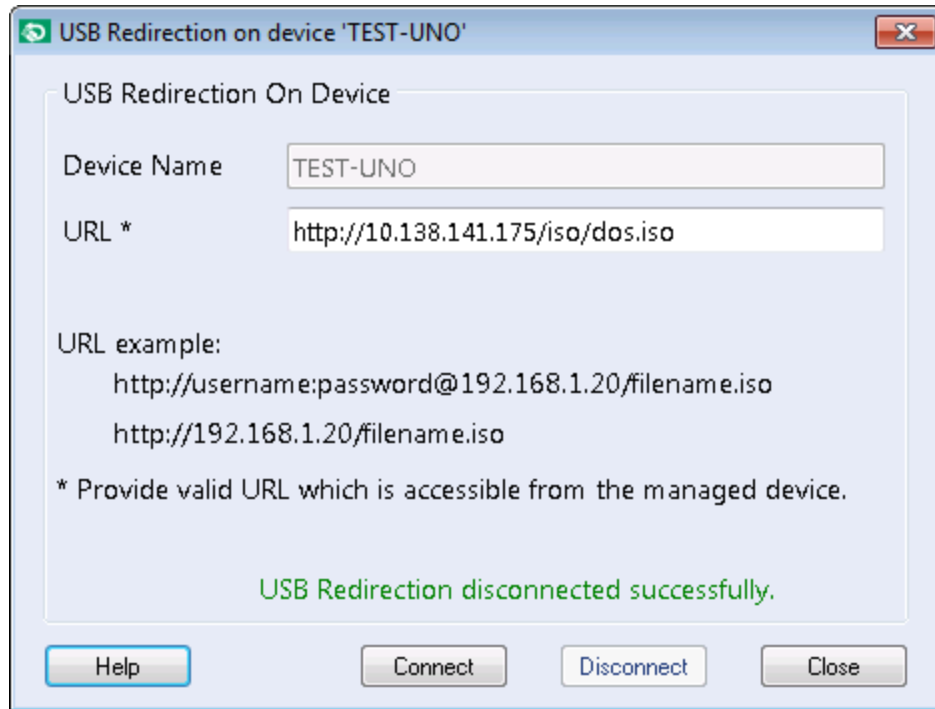
### 3.5.2 Disconnecting USB Redirection

Once the USB Redirection is connected, it is not possible to modify the URL field and the option to edit the URL field will be disabled.

To disconnect the USB Redirection,

- Click the **Disconnect** button.

If the USB redirection is successfully disconnected, the screen updates the same with a message.



**Figure 38: USB Redirection Disconnect**

## 3.6 Subscribing/Un-Subscribing Alerts

AMPS can subscribe or unsubscribe to alerts generated by the managed systems.

The types of alerts are:

- Platform.
- Boot-progress.
- Lifecycle events. (These events include temperature alerts, fan failure, chassis intrusion, Prochot, ThermTrip, and BIOS boot failure.)

AMPS shows:

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

Before subscribing or unsubscribing alerts, perform the below steps:

1. Expand the **Assets and Compliance** node.
2. Expand the **Overview** node.
3. Expand the **Devices** node and click **All Systems**.
4. In the right pane, right-click the device on which you want to perform Alert configuration. The shortcut menu appears.
5. In the shortcut menu, point to **DASH** and then click **Alerts**.  
Alternatively, click the ribbon icon **Alerts**.

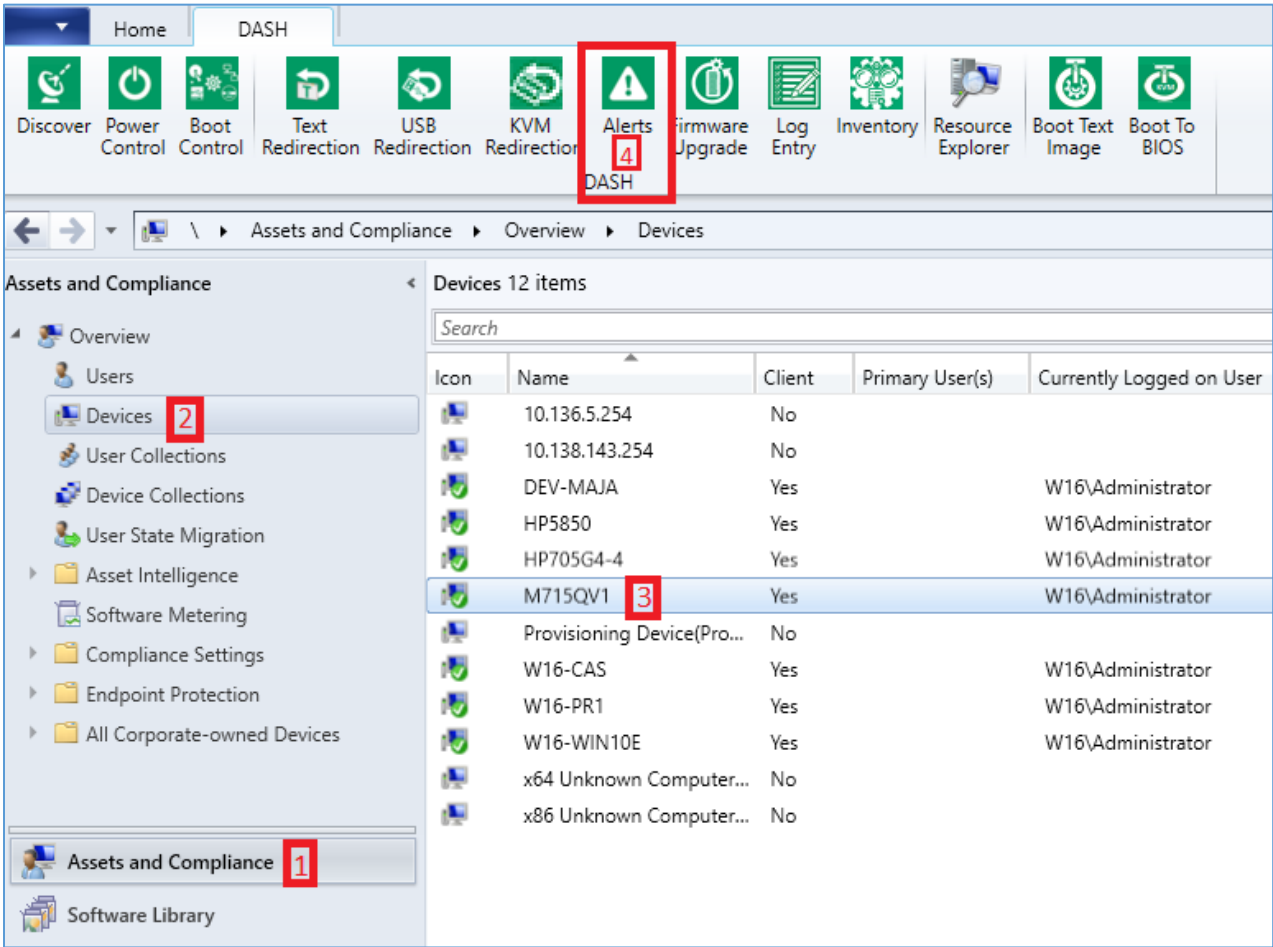


Figure 39: Alerts on device

6. The Alert screen displays the following:
1. **Aavailable filters** as a list box in the left pane. This is a events that this system is capable of sending.
  2. **Subscribed filters** as a list box in the left pane. This is a list of events for which the subscription is already in place.

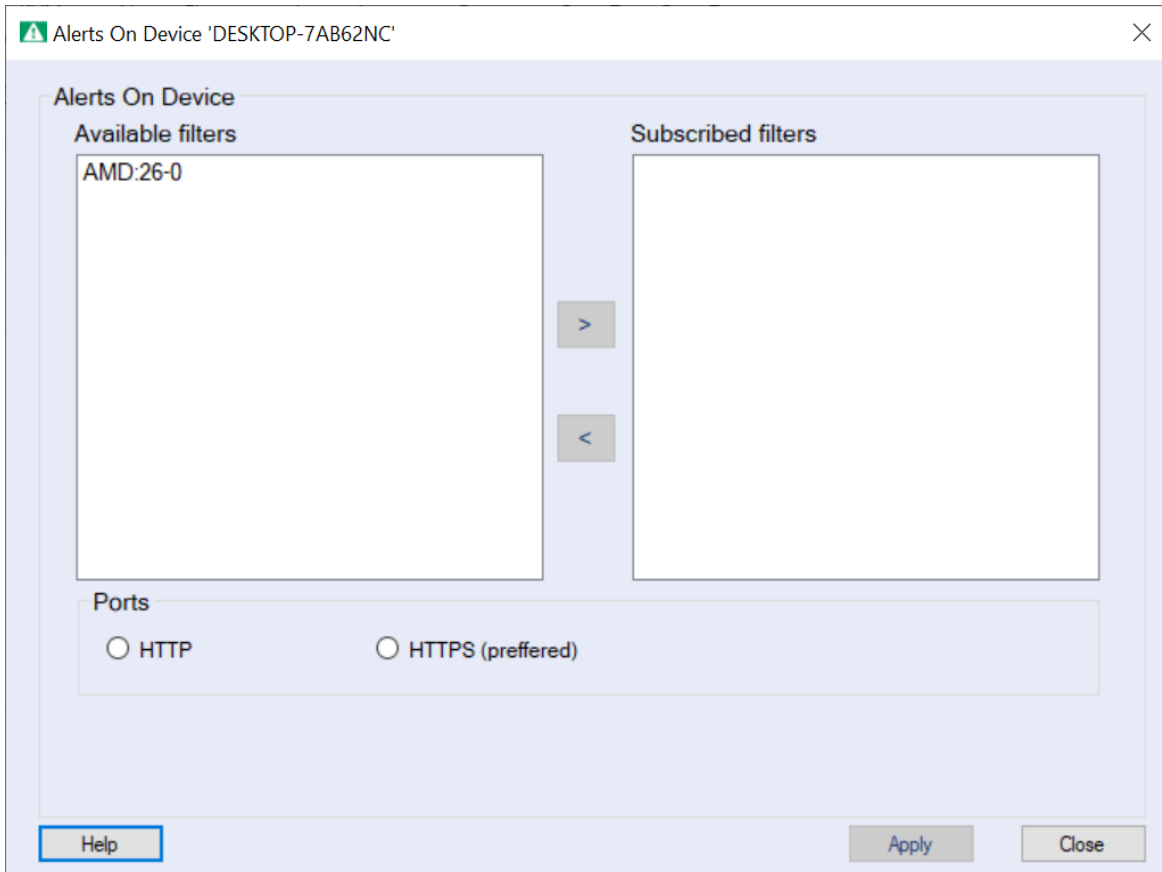
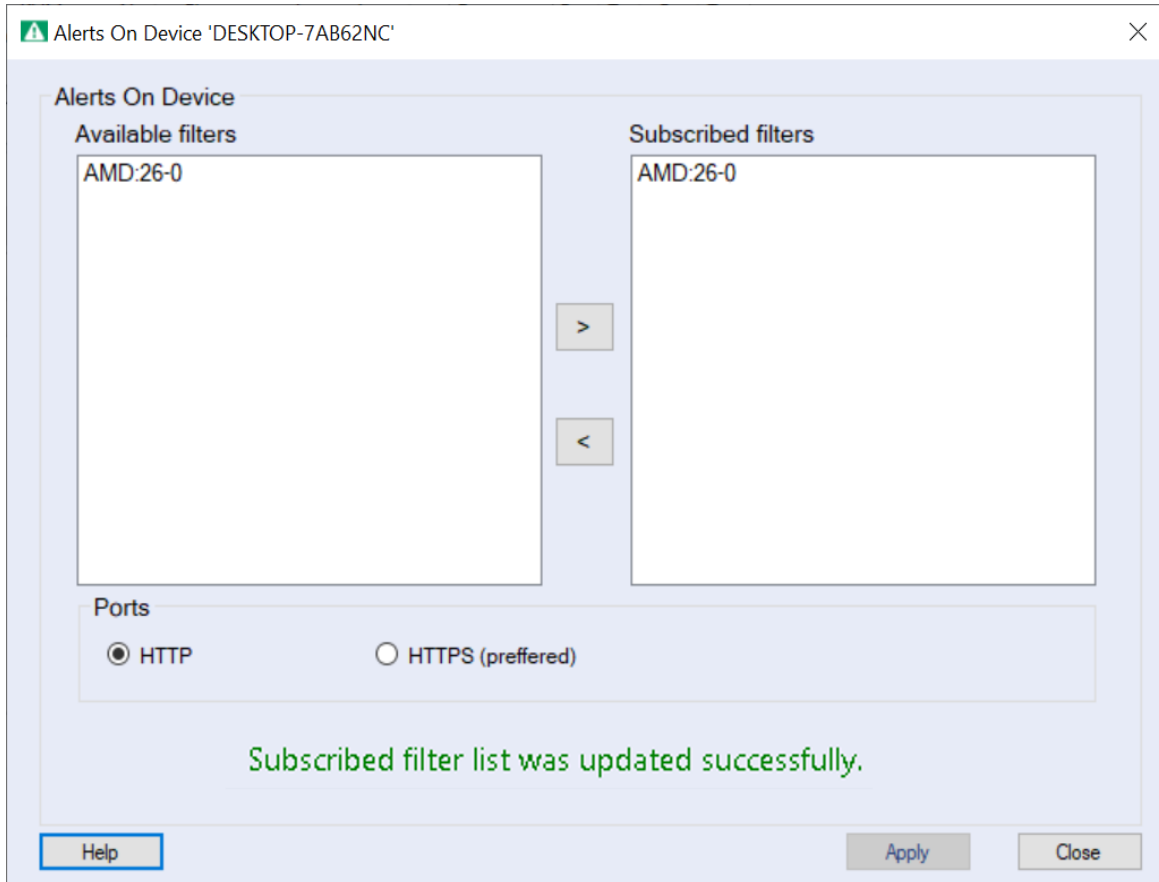


Figure 40: Alerts

### 3.6.1 Subscribing Alerts

To subscribe alerts, perform the following steps:

1. From the **Available filters** list, select any item.
2. To move the item to the **Subscribed filters** list, click the '>' icon.
3. Alerts can be subscribed through HTTP or HTTPS protocols.
4. Once all the changes are done, click the **Apply** button.  
On occurrence of an event for which subscription exists, the managed system sends an alert to AMPS which will be displayed.
5. To close the **Alert Subscription/Un-Subscription** screen, click the **Close** button.



**Figure 41: Alerts Subscription**

### 3.6.2 Un-Subscribing Alerts

To unsubscribe alerts, perform the following steps:

1. From the **Subscribed filters** list, select any item.
2. To move the item to the **Available filters** list, click the '<' icon.
3. User can select either HTTP or HTTPS ports to subscribe Alerts.
4. Once all the changes are done, click the **Apply** button.  
On occurrence of an event for which un-subscription exists, the managed system sends an alert to AMPS which will be displayed.
5. To close the **Alert Subscription/Un-Subscription** screen, click the **Close** button.



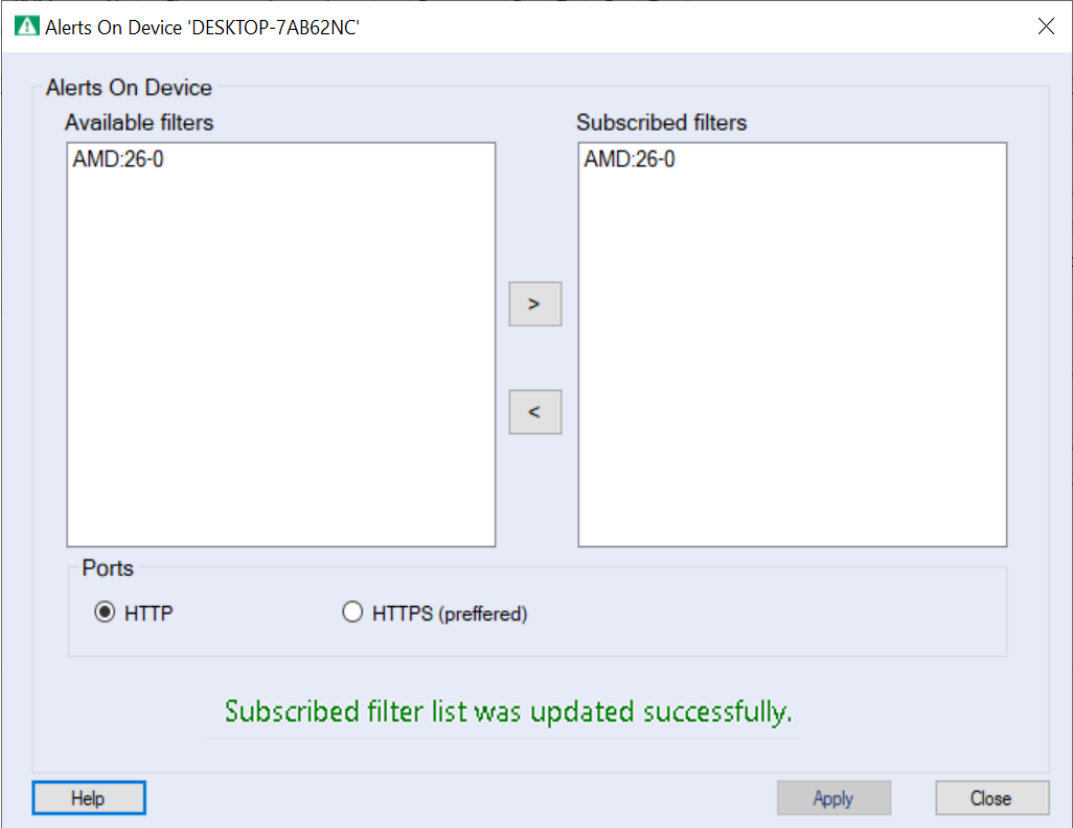


Figure 42: Alerts Un-Subscription

3.6.3 Receiving Alerts

Once the alert filters are subscribed in the Alerts screen, you can view the received alerts in **Configuration Manager Status Message Viewer**. Path in Administrative Console: \Monitoring\Overview\System Status>Status Message Queries\All Status Messages. Filter with component as 'AMPS' will list only AMPS messages.

Configuration Manager Status Message Viewer for <WP1> <W16 CAS Setup>

File Edit View Help

All AMPS Status Messages

Severity	Type	Site code	Date / Time	System	Component	Me...	Description
①	Milestone	WP1	13-10-2020 19:48:36	W16-PR1.W16.amd.com	AMPS	39997	Log entry on 'HP5850' completed successfully.
①	Milestone	WP1	13-10-2020 19:47:26	W16-PR1.W16.AMD.COM	AMPS	39999	User <W16\Administrator> Log Entry failed on the device <M715QV1>.
①	Milestone	WP1	13-10-2020 19:04:56	W16-PR1.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated Discover on the collection <All Systems>.
①	Milestone	WP1	13-10-2020 19:04:56	W16-PR1.W16.amd.com	AMPS	39997	""Discovery"" occurs one time at 2020-10-13 07:05 PM" is scheduled successfully on collection 'SMS00001'.
①	Milestone	WP1	13-10-2020 17:20:23	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'W16-WIN10E'.
①	Milestone	WP1	13-10-2020 17:20:20	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <W16-WIN10E>.
①	Milestone	WP1	13-10-2020 16:44:15	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'W16-WIN10E'.
①	Milestone	WP1	13-10-2020 16:44:12	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <W16-WIN10E>.
①	Milestone	WP1	13-10-2020 16:44:09	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'M715QV1'.
①	Milestone	WP1	13-10-2020 16:43:54	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <M715QV1>.
①	Milestone	WP1	13-10-2020 16:43:44	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'HP705G4-4'.
①	Milestone	WP1	13-10-2020 16:43:30	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <HP705G4-4>.
①	Milestone	WP1	13-10-2020 16:43:05	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'HP5850'.
①	Milestone	WP1	13-10-2020 16:42:55	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <HP5850>.
①	Milestone	WP1	13-10-2020 16:42:36	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'DEV-MAJA'.
①	Milestone	WP1	13-10-2020 16:42:24	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <DEV-MAJA>.
①	Milestone	WP1	13-10-2020 16:09:57	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated Discover on the collection <All Systems>.
①	Milestone	WP1	13-10-2020 16:09:57	W16-PR1.W16.amd.com	AMPS	39997	""Discovery"" occurs one time at 2020-10-13 04:15 PM" is scheduled successfully on collection 'SMS00001'.
①	Milestone	WP1	13-10-2020 16:08:26	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> modified DASH settings for the site server <W16-PR1.W16.amd.com>.
①	Milestone	WP1	13-10-2020 16:08:25	W16-PR1.W16.amd.com	AMPS	39997	DASH Configuration was updated successfully.
①	Milestone	WP1	13-10-2020 16:08:24	W16-PR1.W16.amd.com	AMPS	39997	DASH authentication list was updated successfully.
①	Milestone	WP1	13-10-2020 12:27:35	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'W16-WIN10E'.
①	Milestone	WP1	13-10-2020 12:27:33	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <W16-WIN10E>.
①	Milestone	WP1	13-10-2020 11:53:12	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'W16-WIN10E'.

All AMPS Status Messages: 46 of 46 messages displayed. 1 selected.

Figure 43: Alerts Reception

## 3.7 Inventory

MEM shows the Information that it collects about the managed device in the **Resource Explorer** window. Information collected by the AMPS plugin also ends up in the Resource explorer.

The below sections explain how the information is collected from the managed device and how to view them. Inventory is successful after successful client push.

### 3.7.1 Inventory Collection

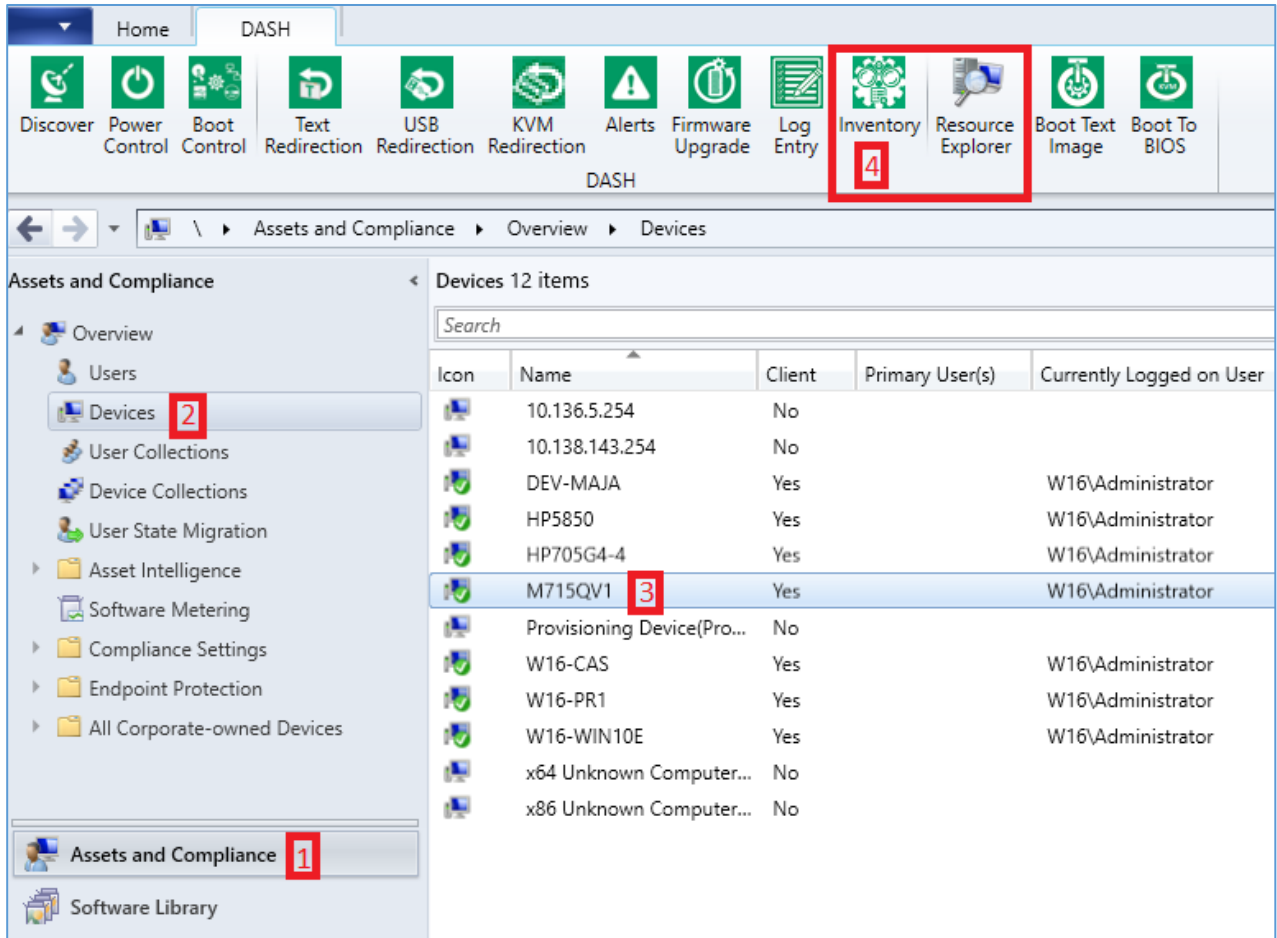
Inventory information is collected from the managed device during,

- The discovery process on the device.
- By initiating inventory collection task against a managed device.

The DASH discovery process is explained in earlier chapters let us see how to initiate inventory collection task against a managed device.

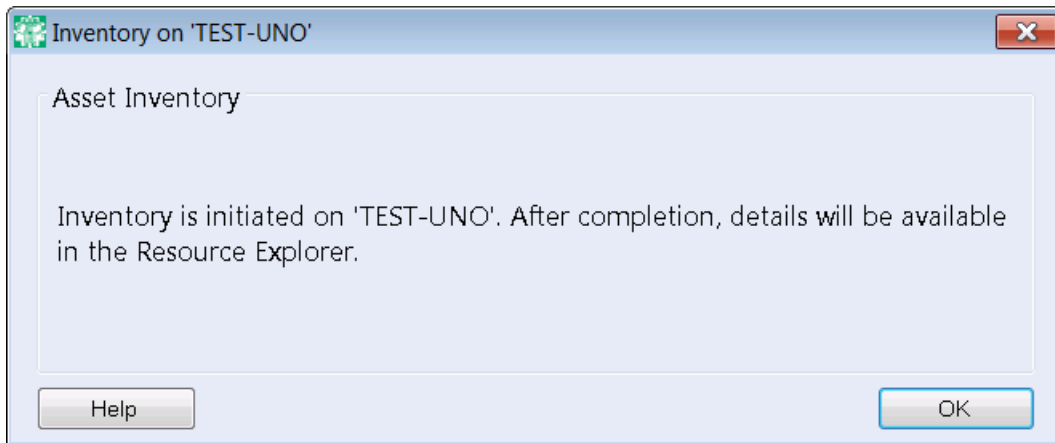
To collect inventory, perform the following steps:

1. Expand the **Assets and Compliance** node.
2. Expand the **Overview** node.
3. Expand the **Devices** node and click **All Systems**.
4. In the right pane, right-click the device on which you want to collect the inventory. The shortcut menu appears.
5. In the shortcut menu, point to **DASH** and then click **Inventory**.



**Figure 44: Inventory on device**

- When the Inventory screen appears, it displays a message with initiating the inventory.



**Figure 45: Inventory**

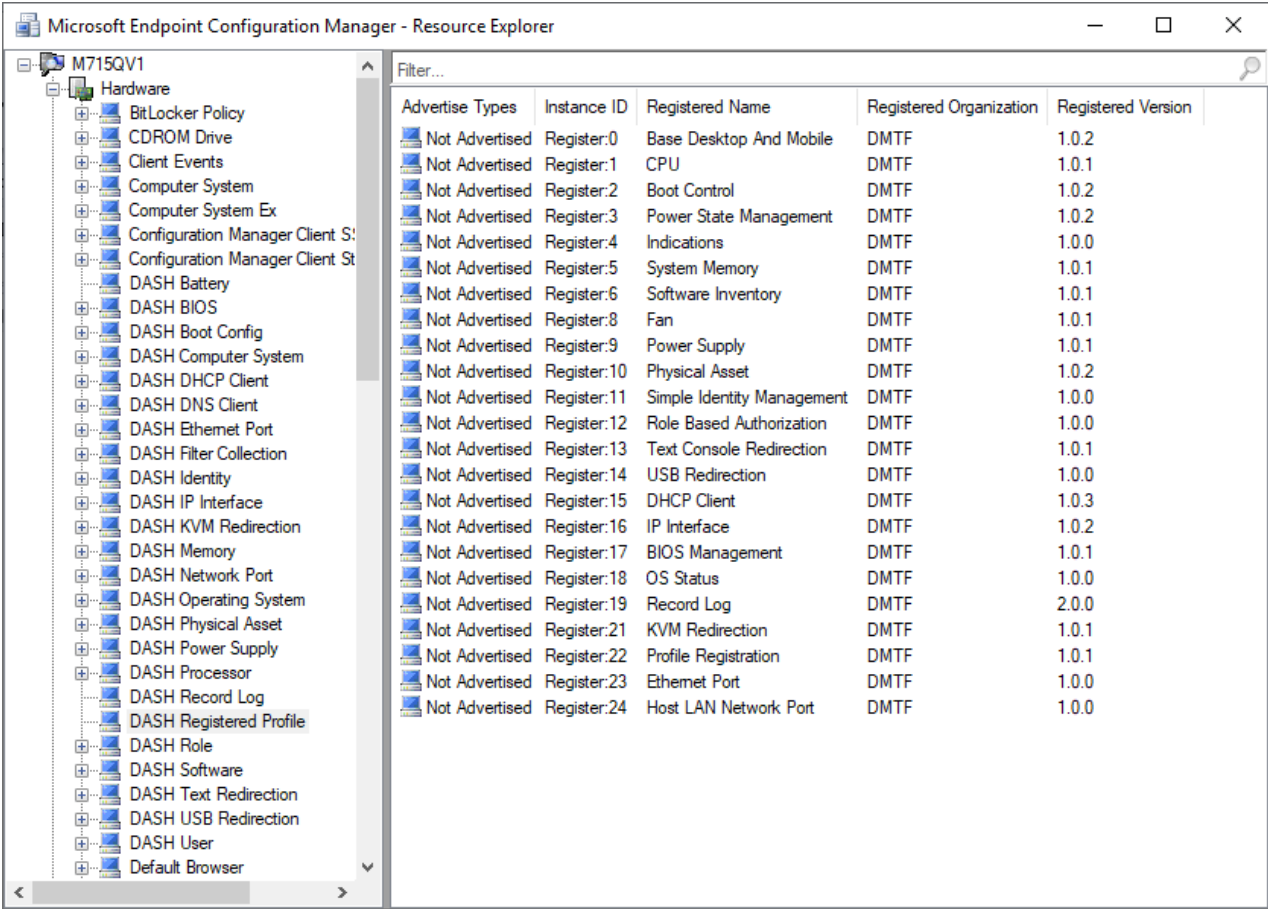
### 3.7.2 Viewing the DASH Inventory or Resource Explorer

To view the DASH inventory, perform the following steps:

- Perform the DASH Discovery on Device steps. For more information on the DASH discovery on a device steps, refer to the section 3.1

2. Click on the inventory button as discussed in section 3.7.1.

DASH inventory is populated using out-of-band DASH protocol. DASH inventory is populated in Resource Explorer. DASH inventory is displayed in the path **\SystemName\Hardware\** as shown in Figure 46.



**Figure 46: DASH Inventory shown in Resource Explorer**

Each DASH inventory item can be selected in the tree on the left hand side of the resource explorer to view the corresponding DASH profile inventory in the right.

On double clicking the inventory item, the Profile's instance can be viewed in a separate window in the form of Attribute Name, Value pair. Profile properties for which values are not available are displayed as blank.

Depending on Platform DASH support, some profiles may or may not be displayed inventory.

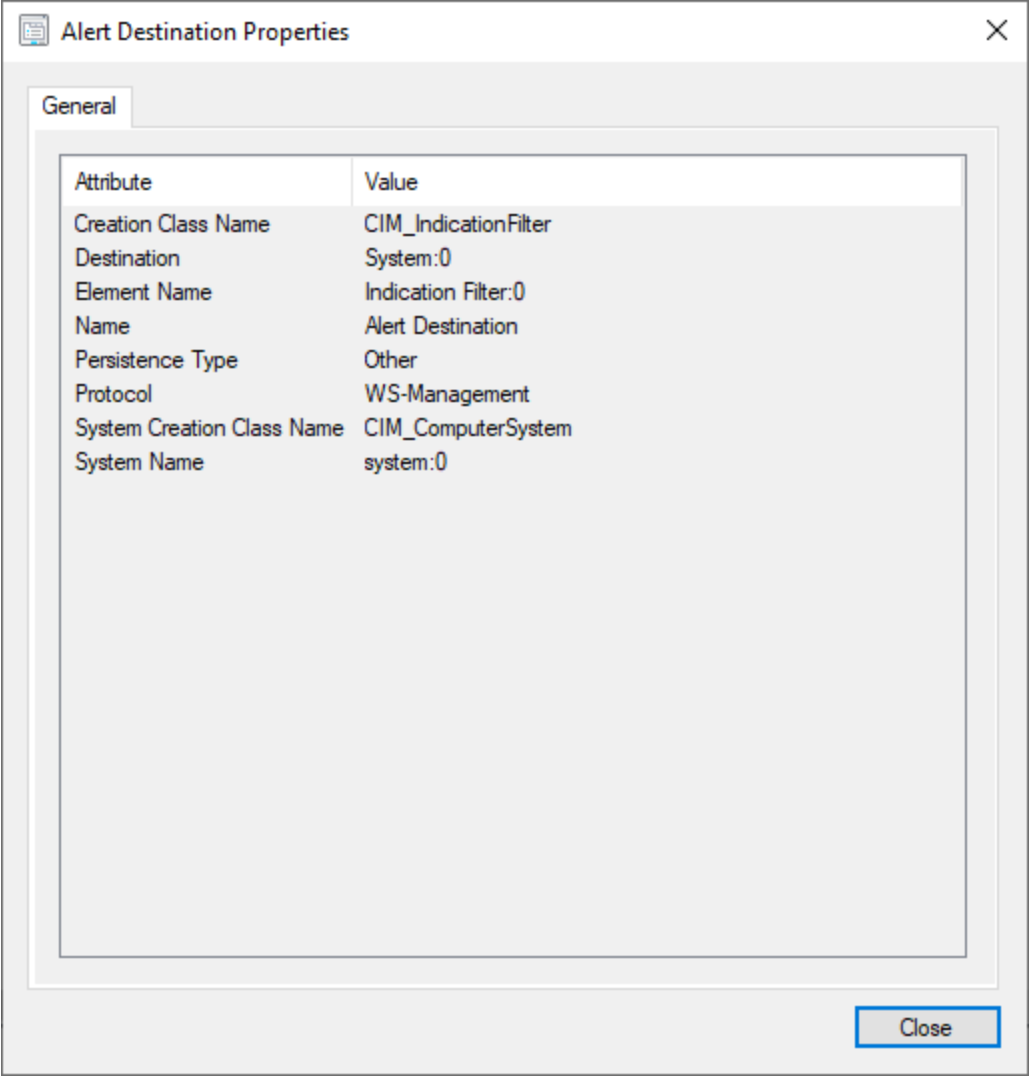


Figure 47: DASH 'Alert Destination' Profile Properties

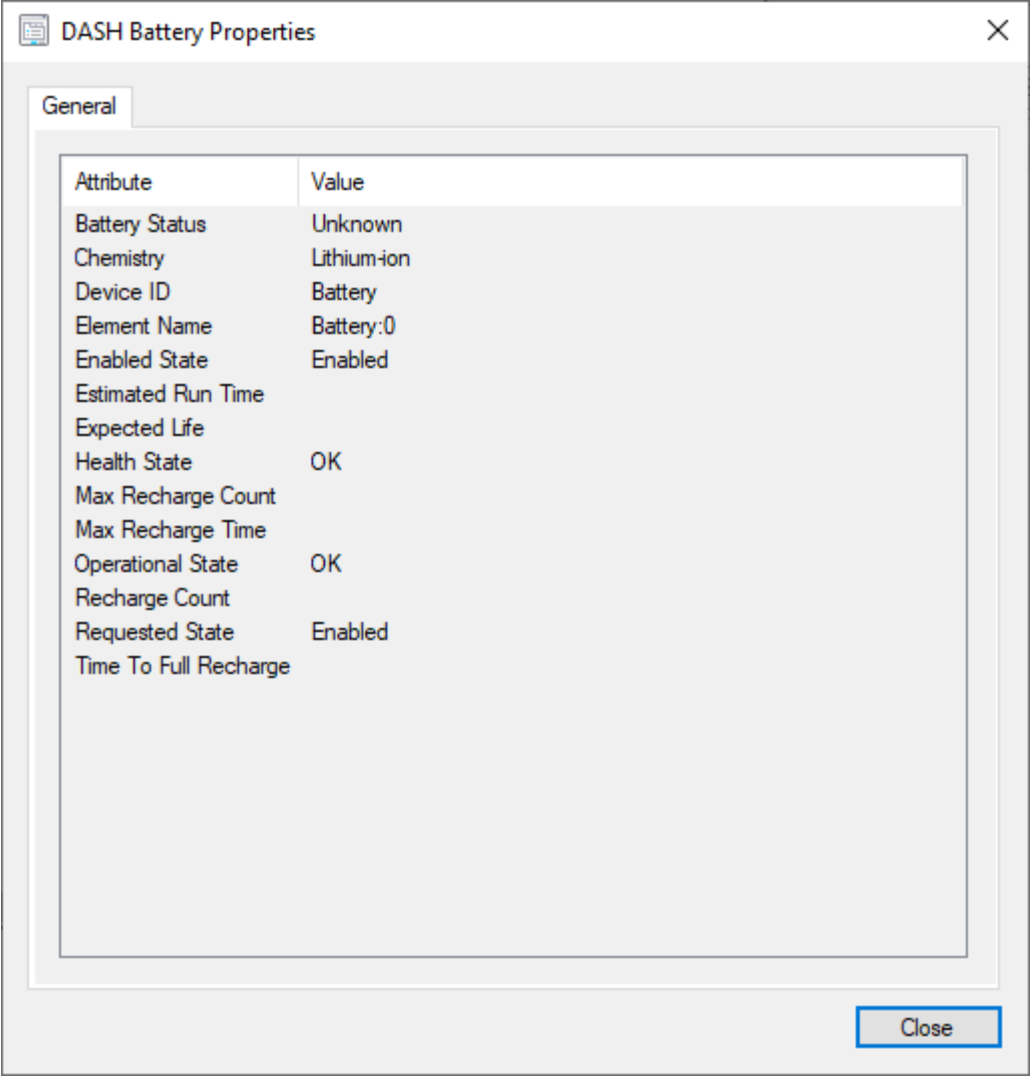


Figure 48: DASH ‘Battery’ Profile Inventory

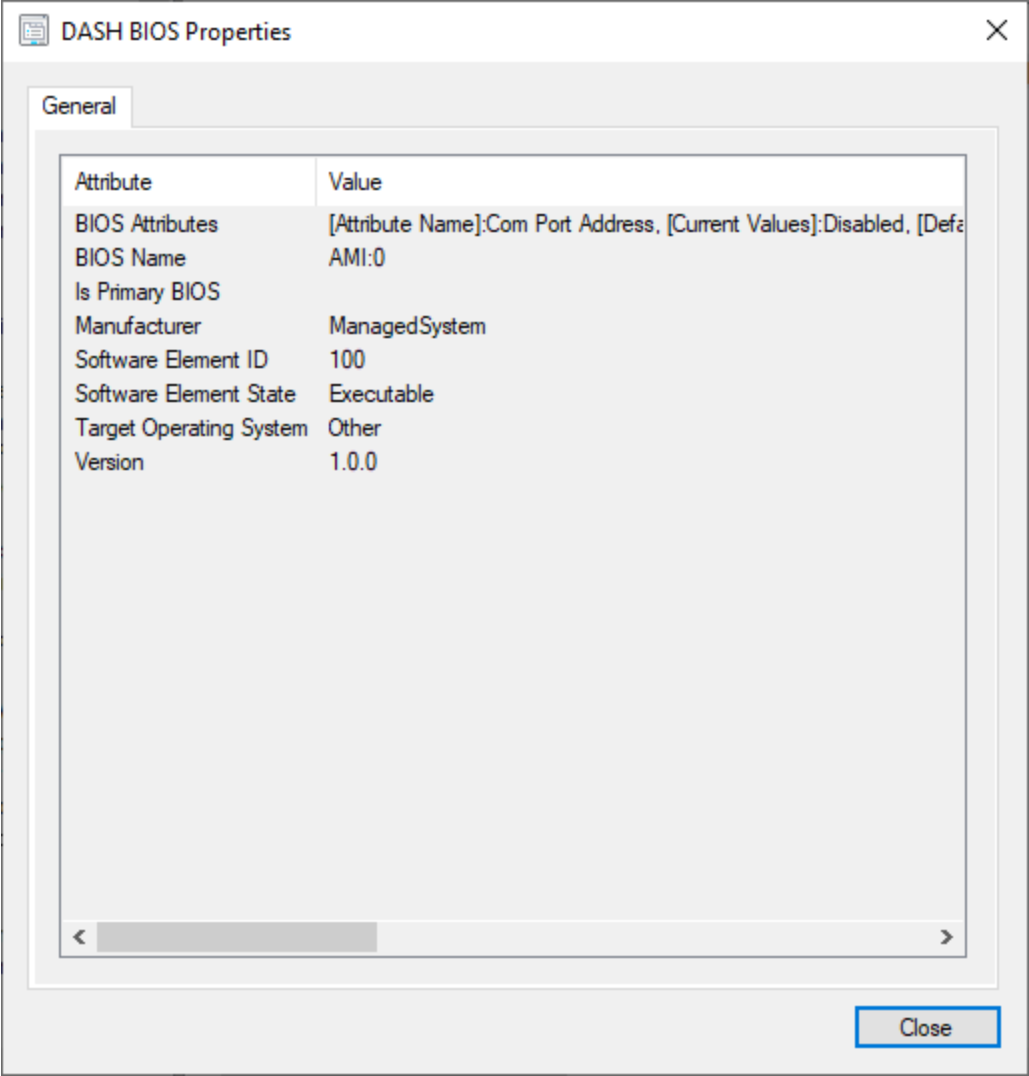


Figure 49: DASH 'BIOS' Profile Inventory

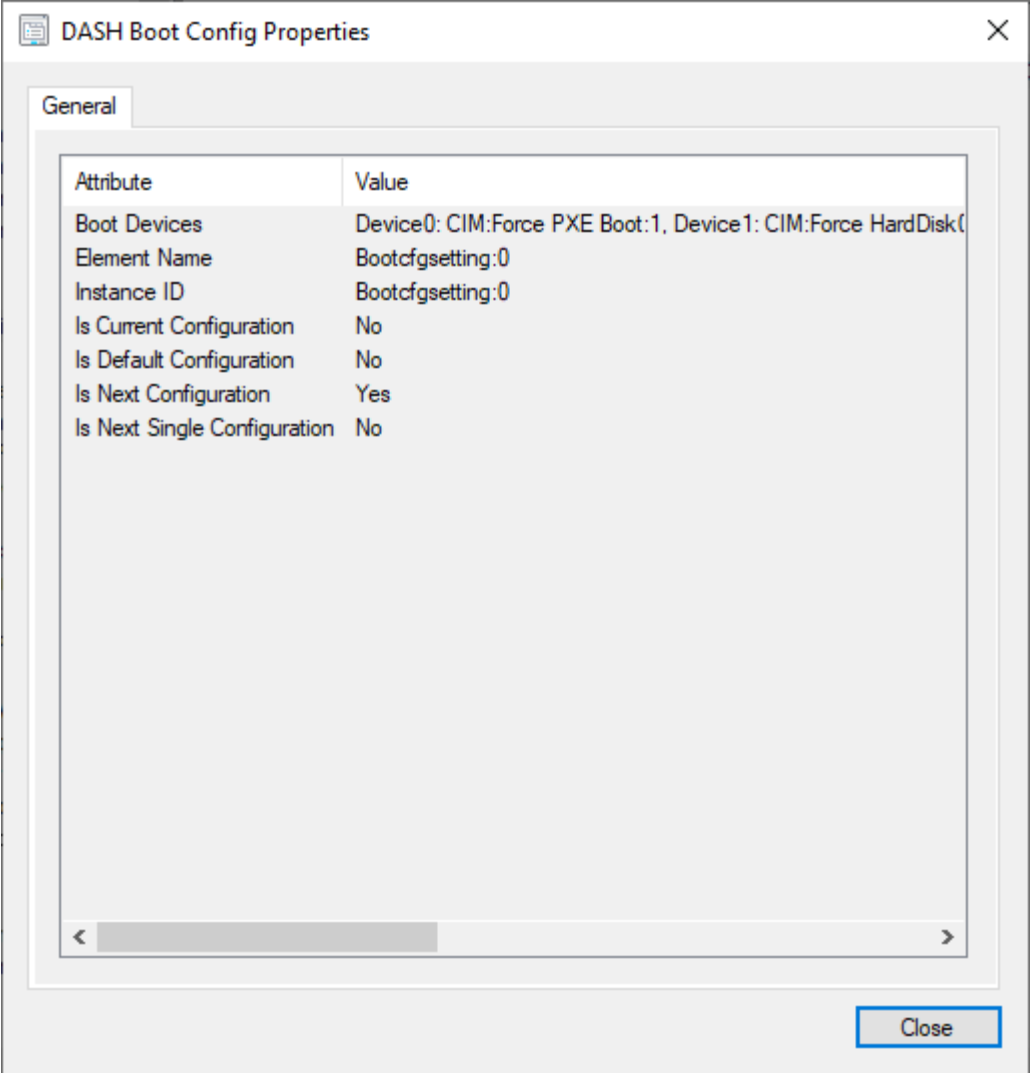


Figure 50: DASH 'Boot Config' Profile Inventory



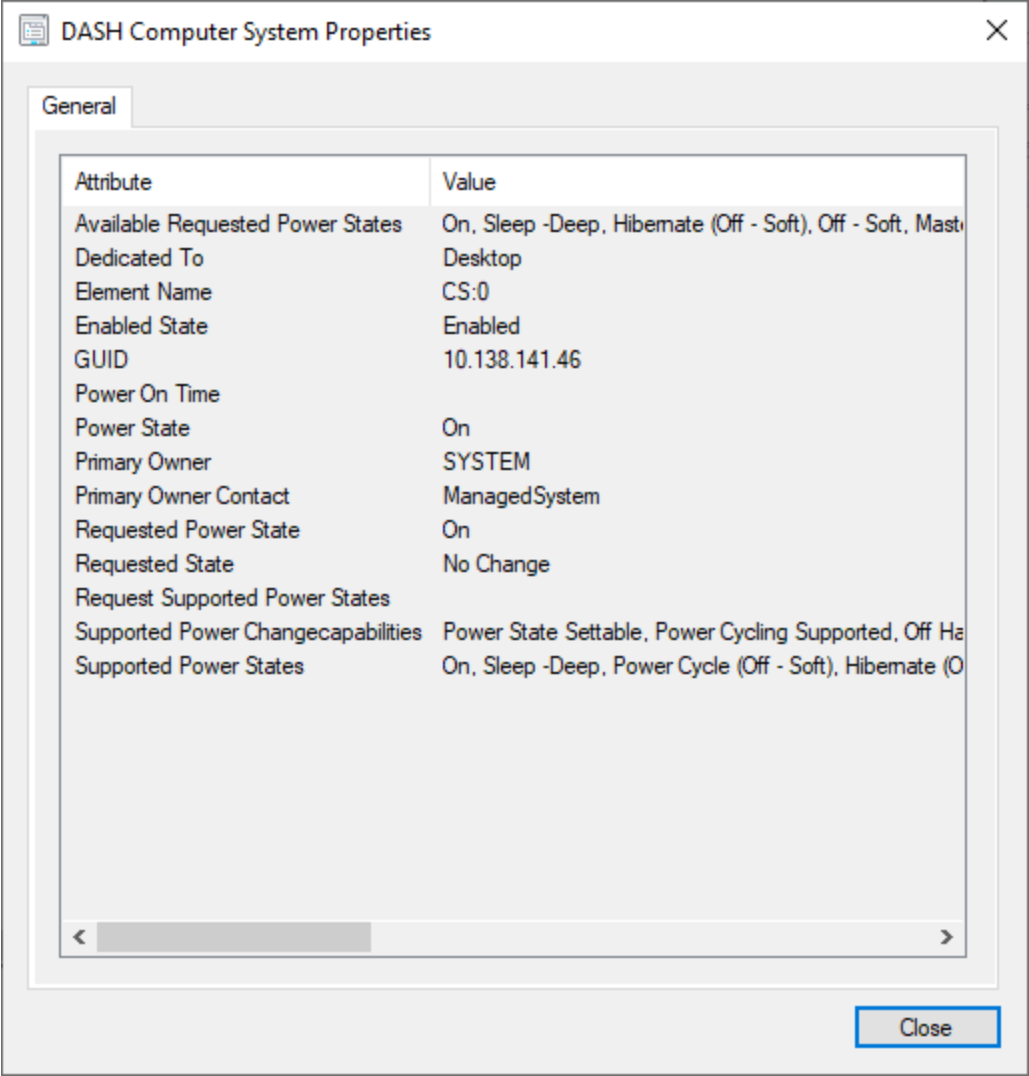


Figure 51: DASH 'Computer System' Profile Inventory

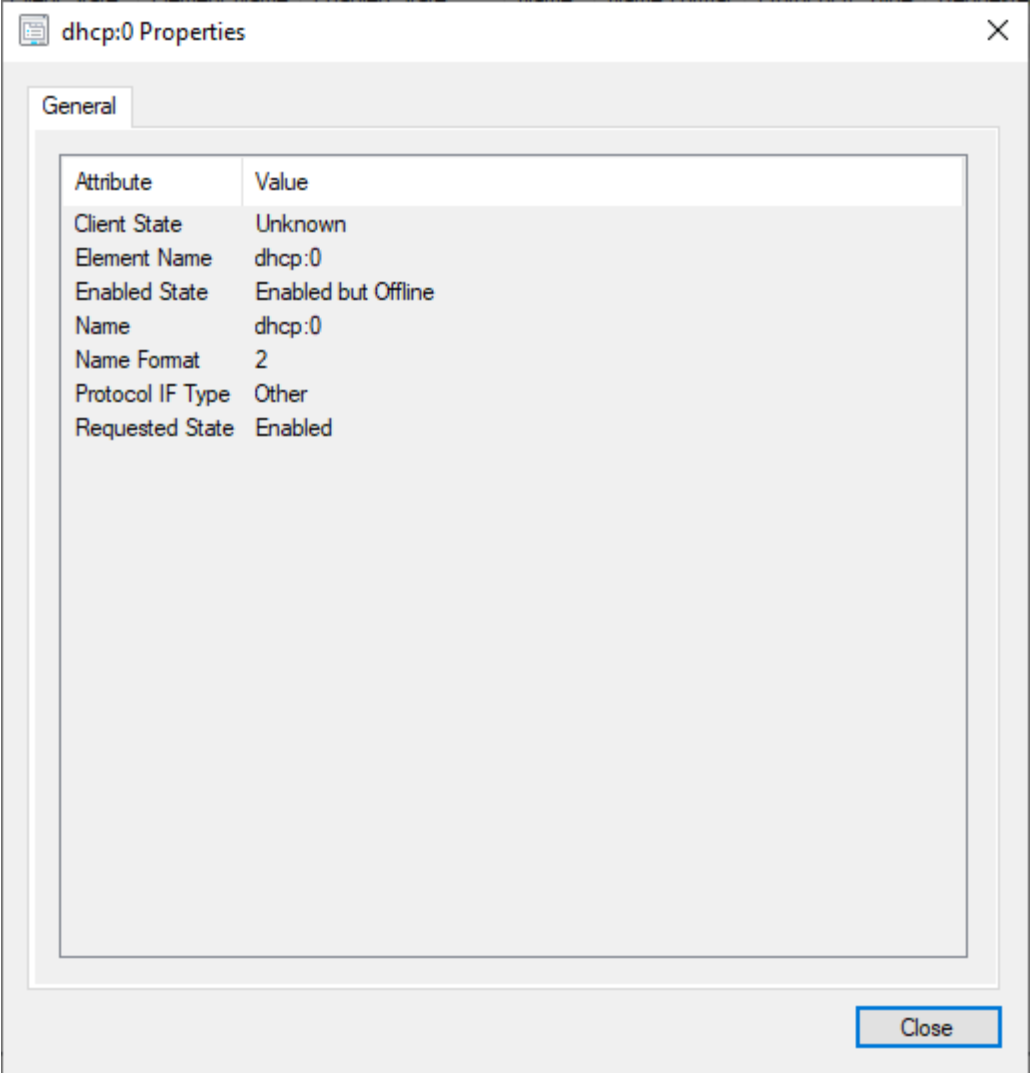


Figure 52: DASH 'DHCP Client' Profile Inventory

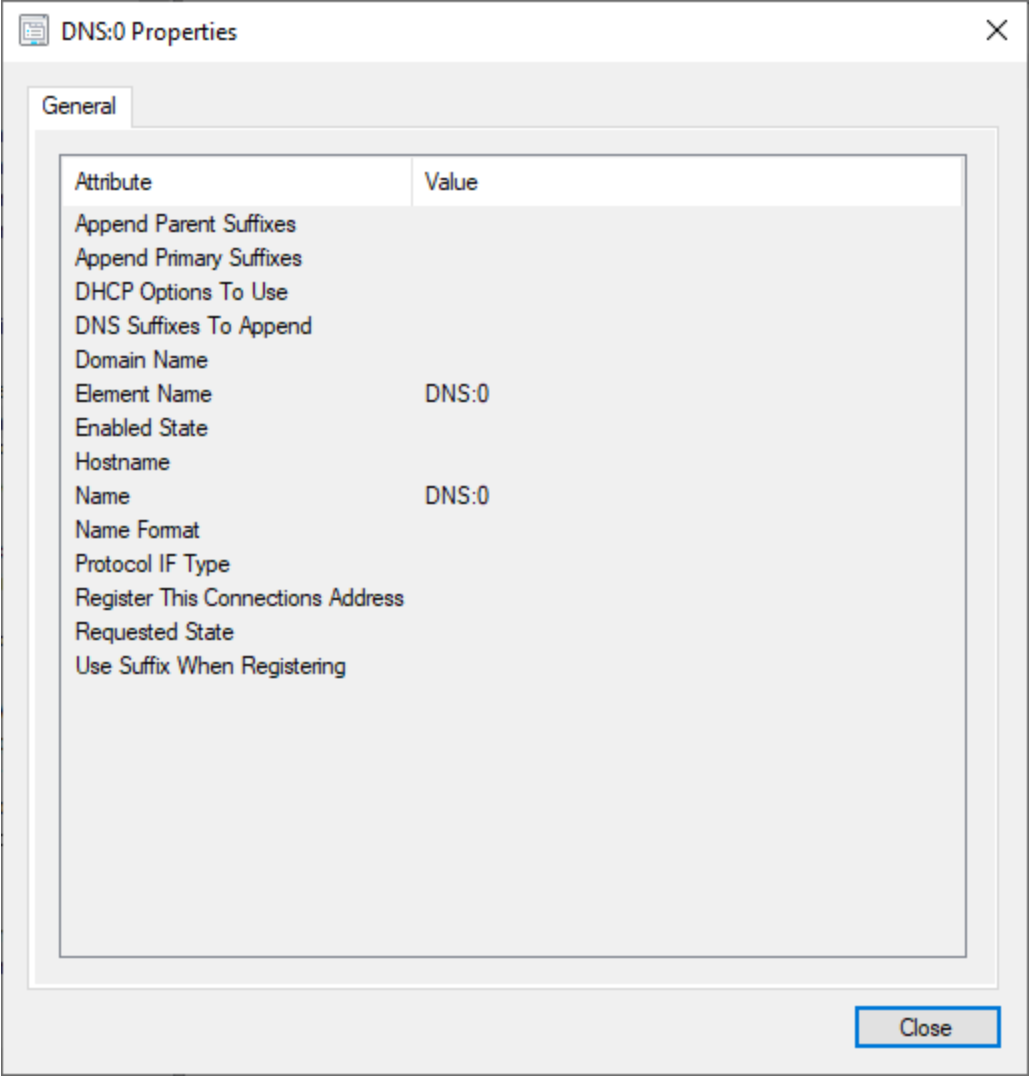


Figure 53: DASH ‘DNS Client’ Profile Inventory

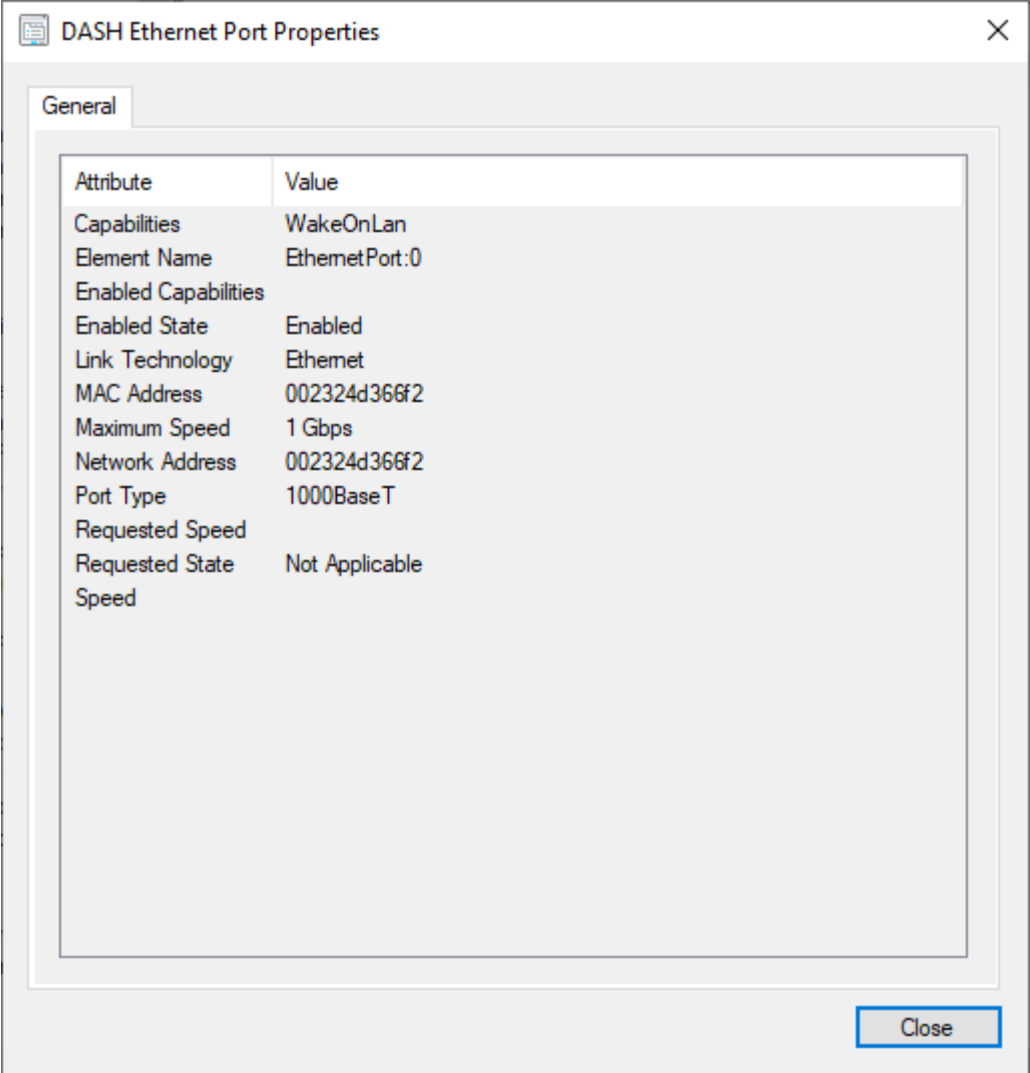


Figure 54: DASH ‘Ethernet Port’ Profile Inventory

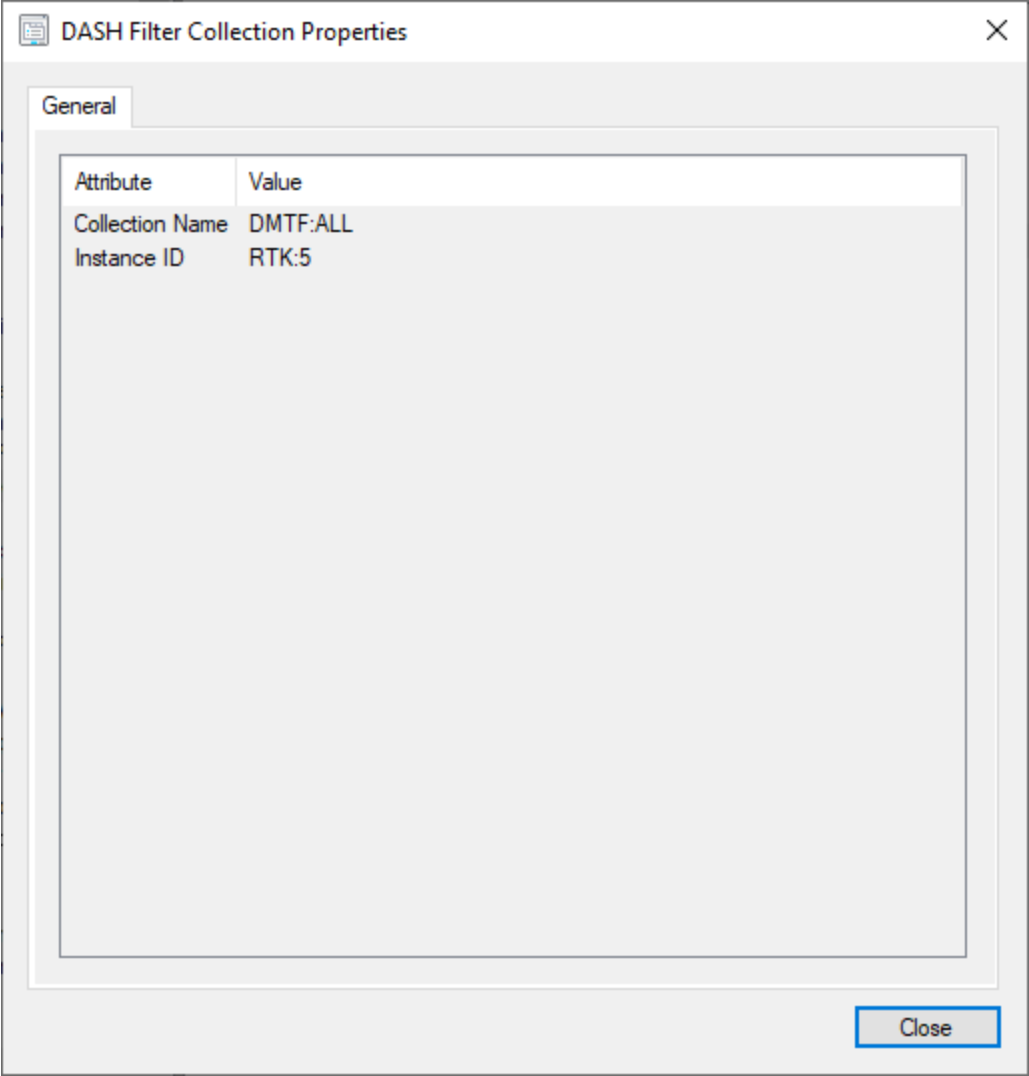


Figure 55: DASH 'Filter Collection' Profile Properties

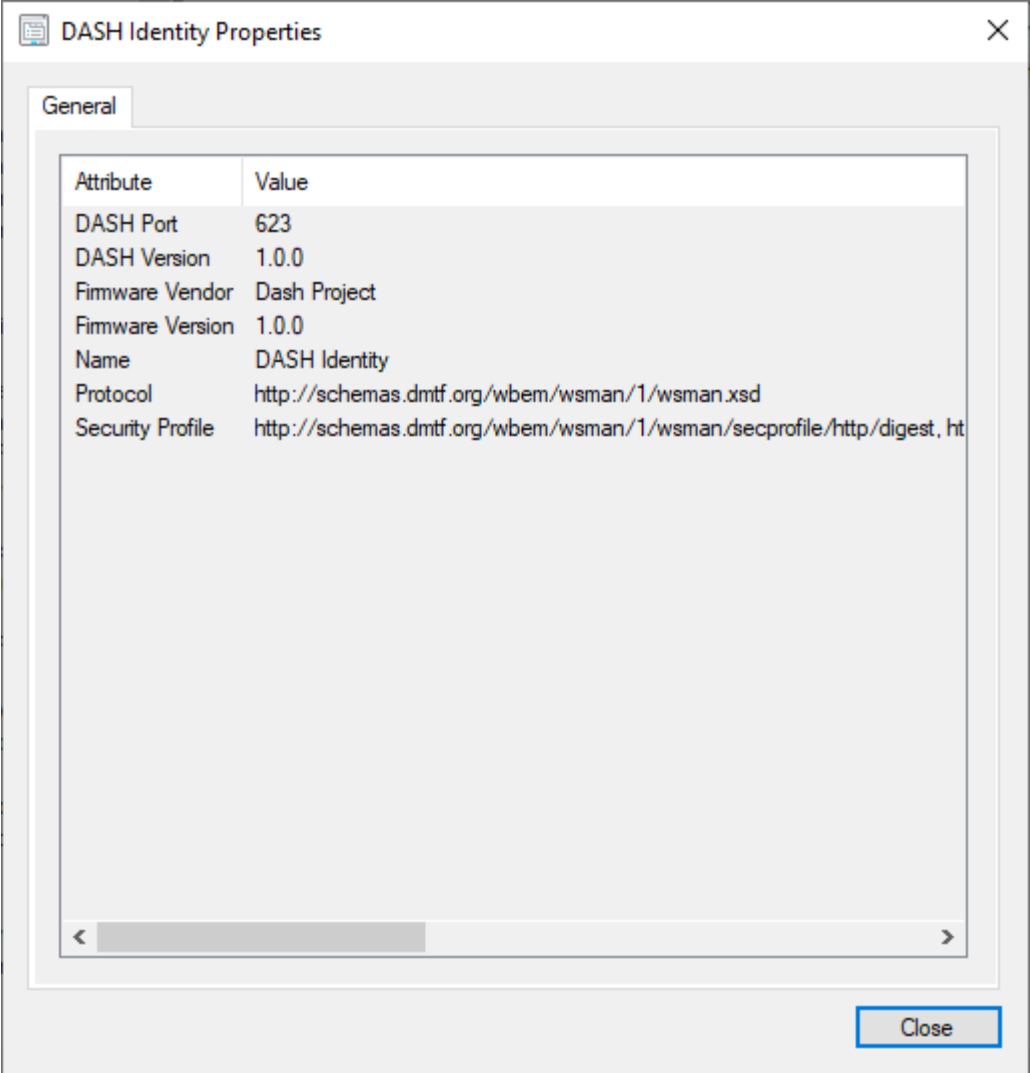


Figure 56: DASH 'Identity' Properties

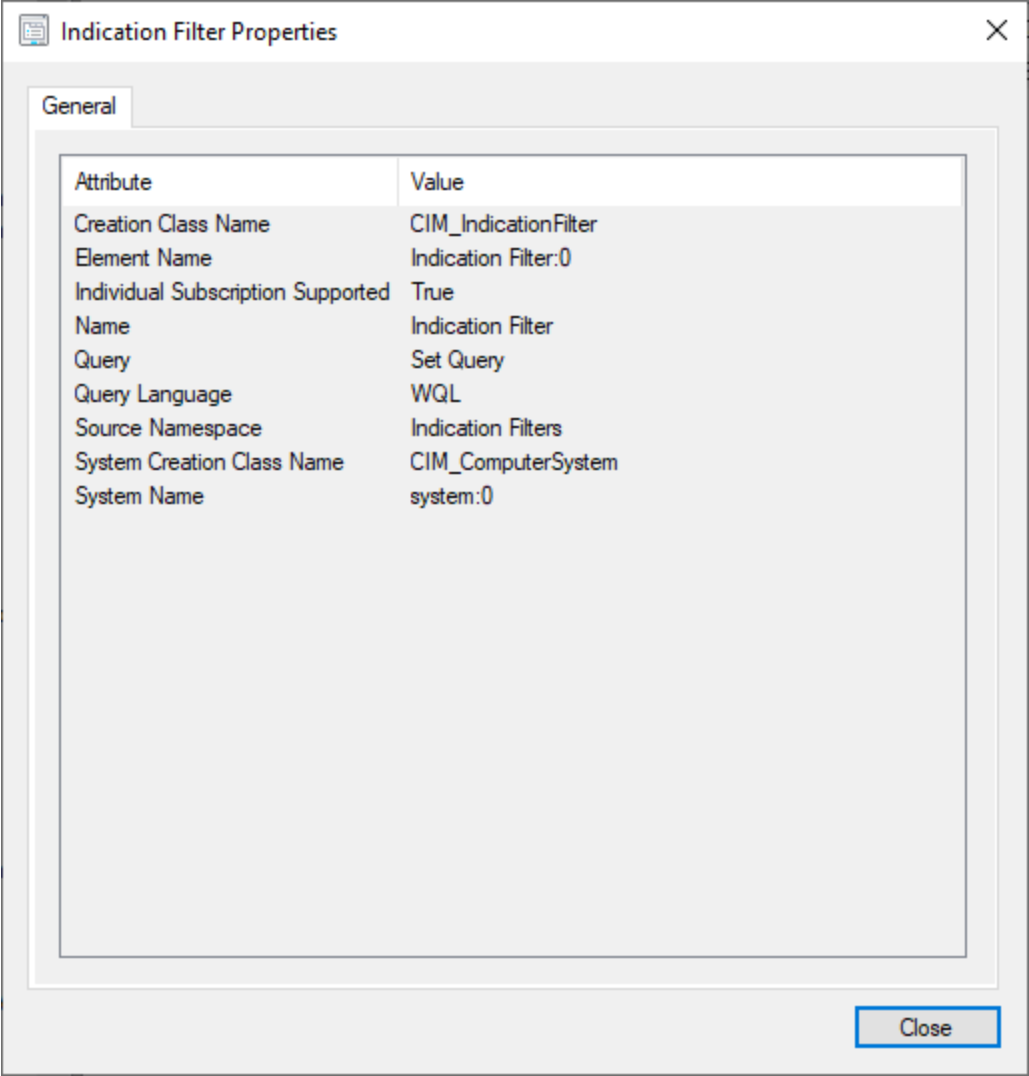
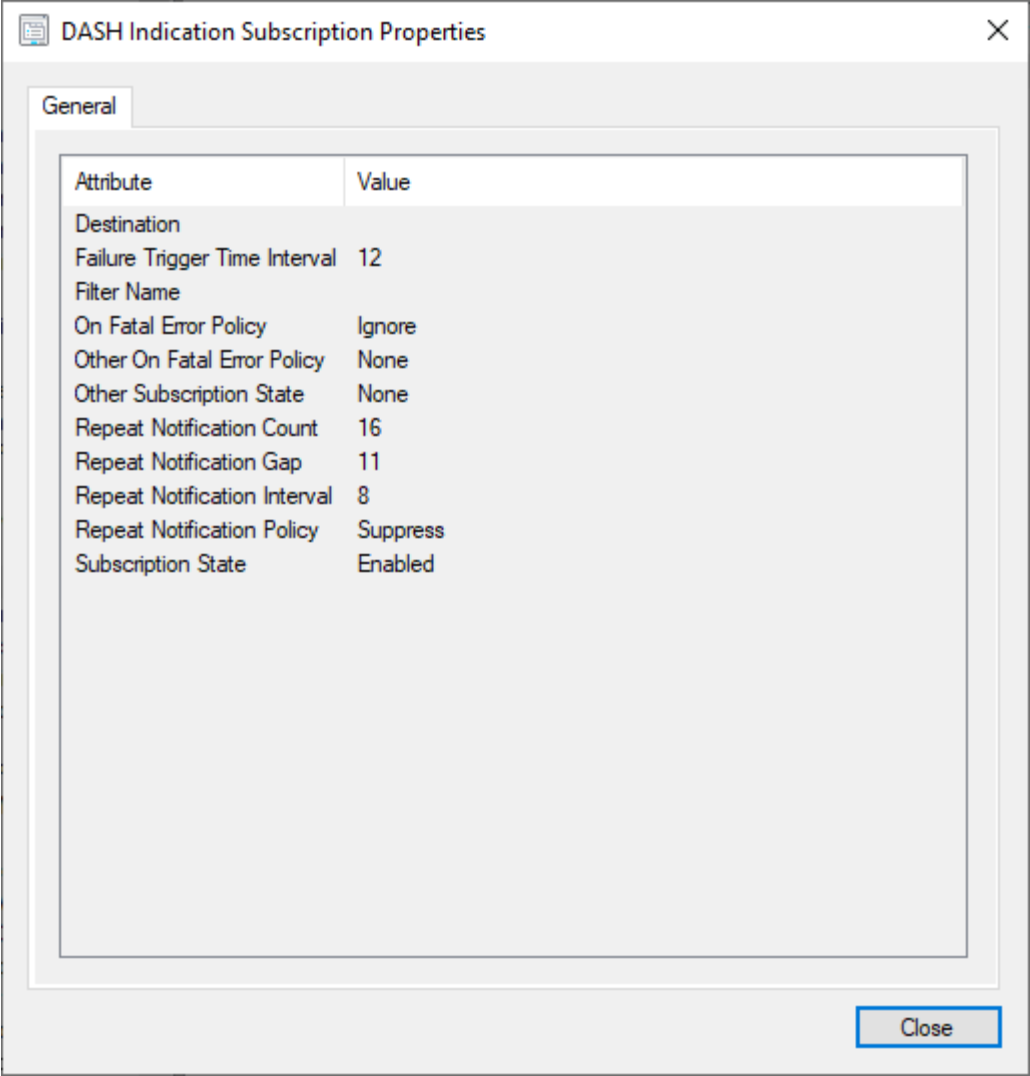


Figure 57: DASH 'Indication Filter' Profile Properties



**Figure 58: DASH 'Indication Subscription' Profile Properties**



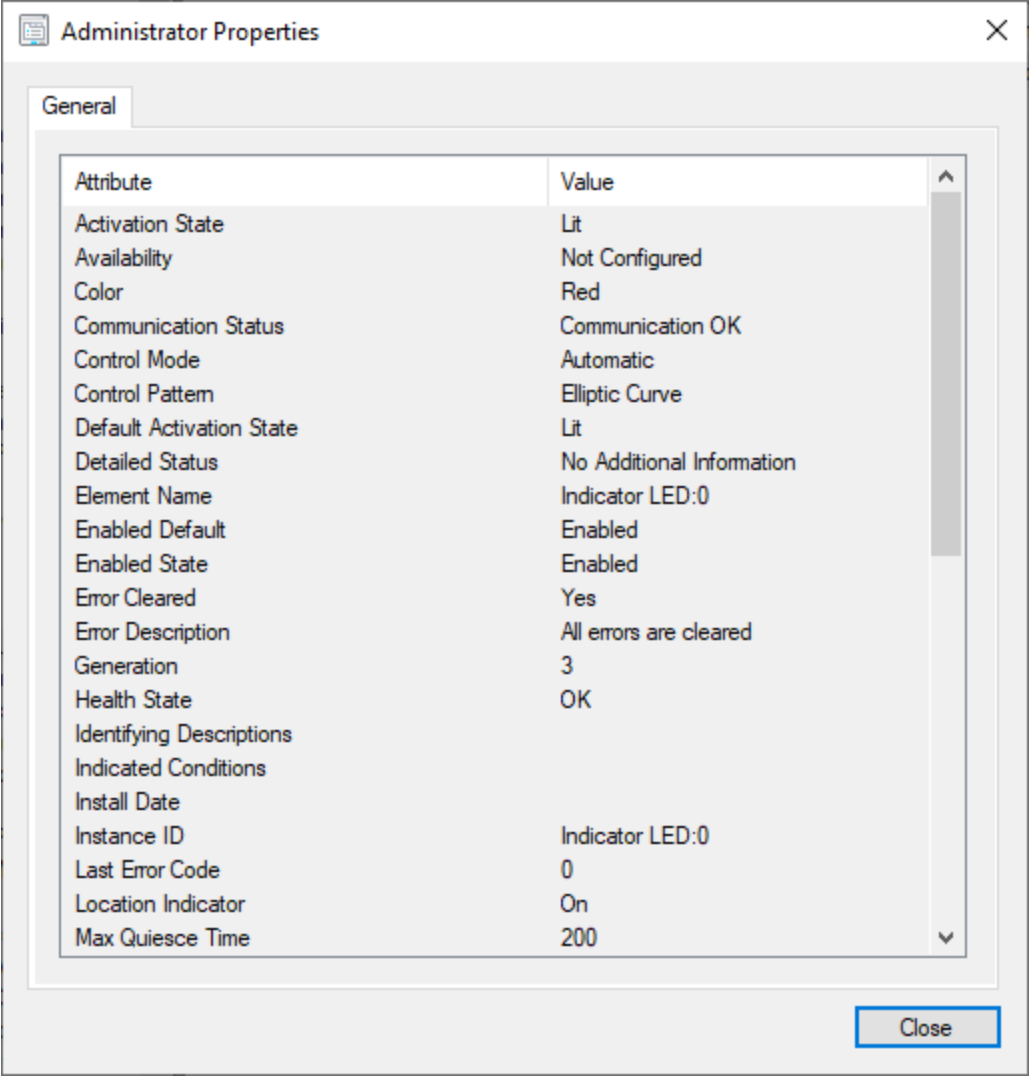


Figure 59: DASH 'Indicator LED' Profile Properties

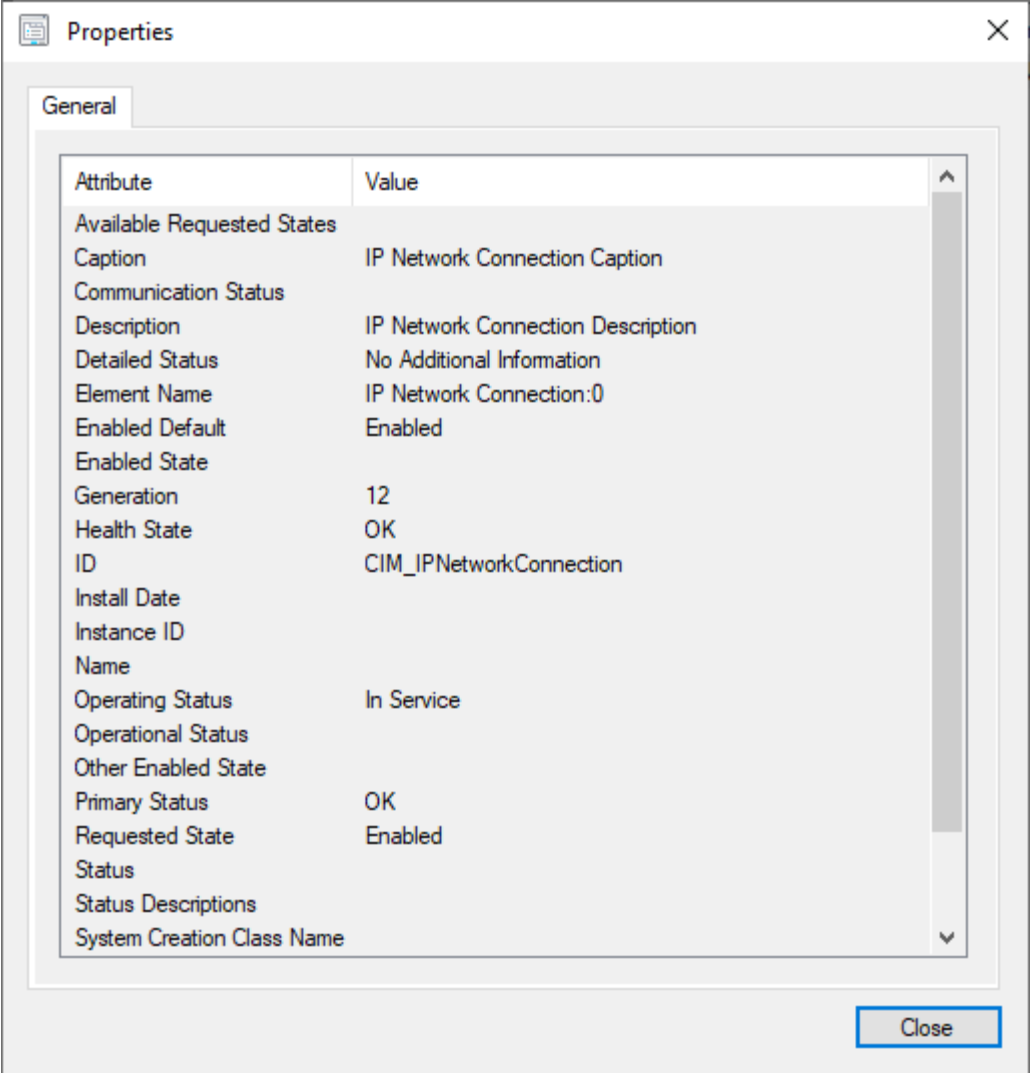


Figure 60: DASH 'IP Configuration' Profile Properties

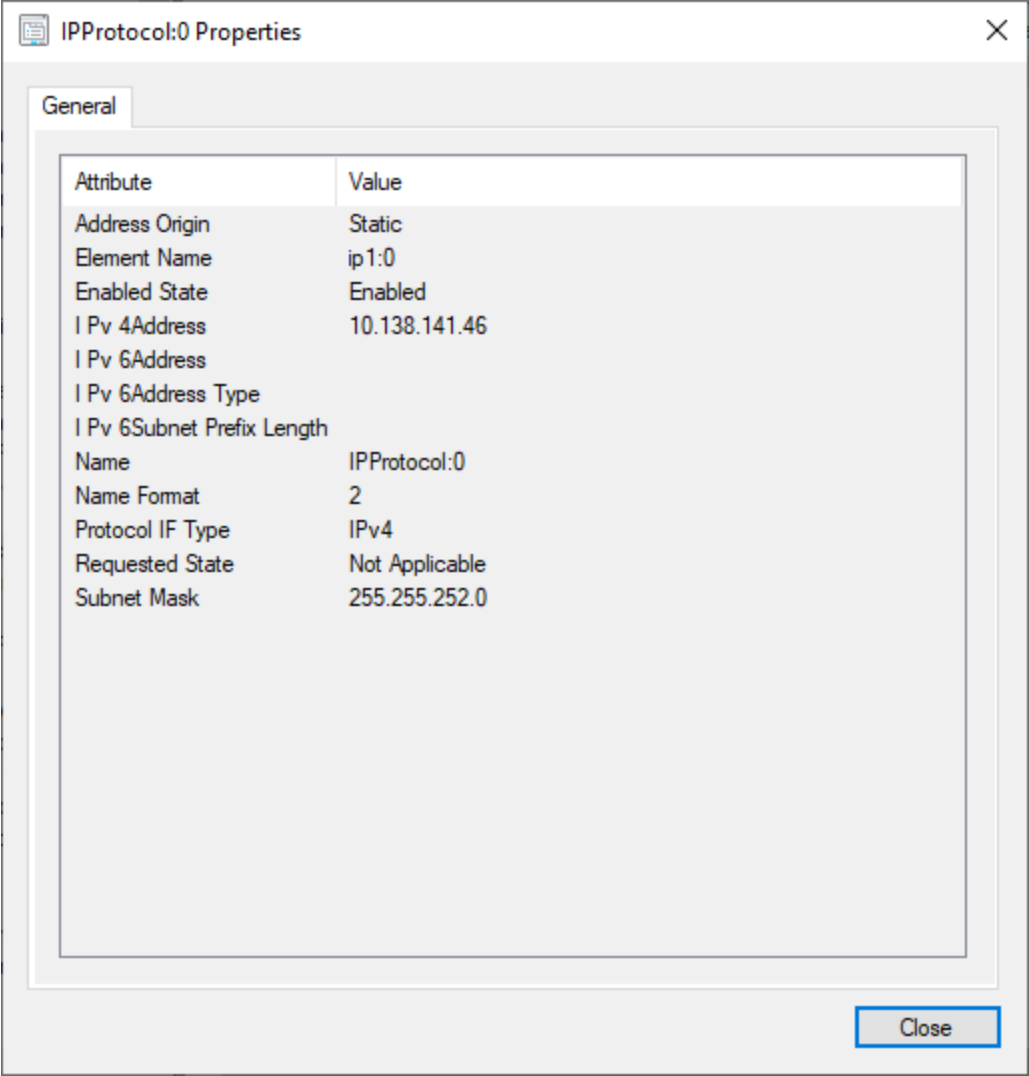


Figure 61: DASH 'IP Interface' Profile Properties

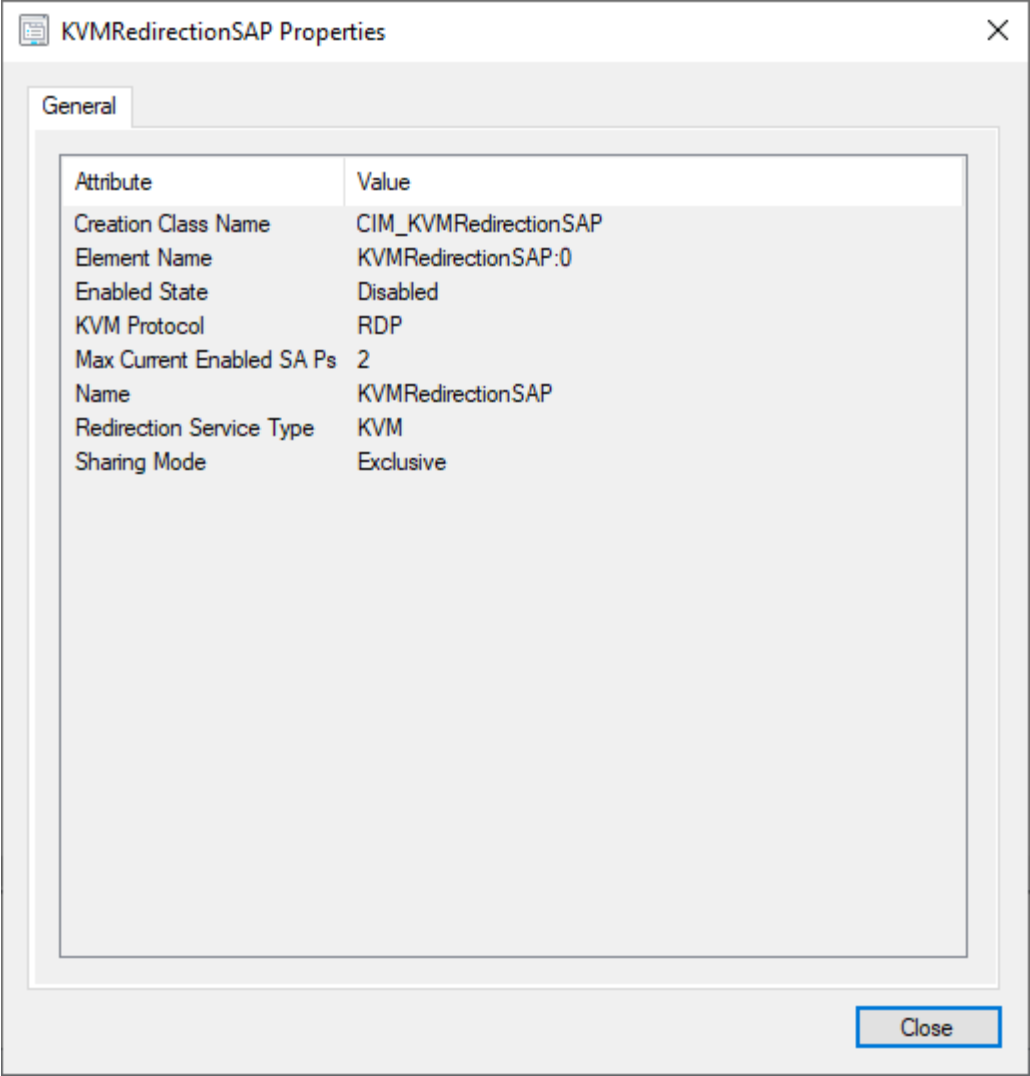


Figure 62: DASH 'KVM Redirection' Profile Properties

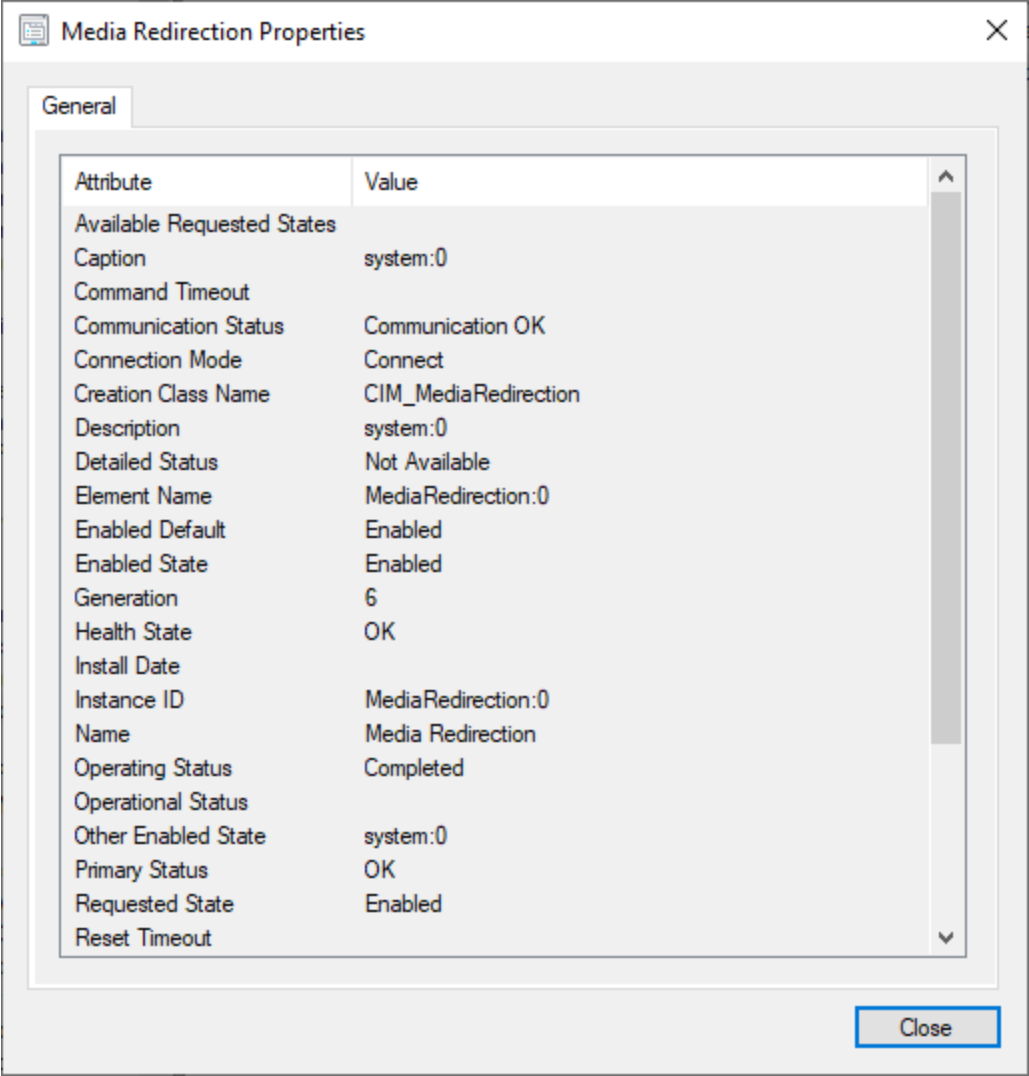


Figure 63: DASH 'Media Redirection' Profile Properties

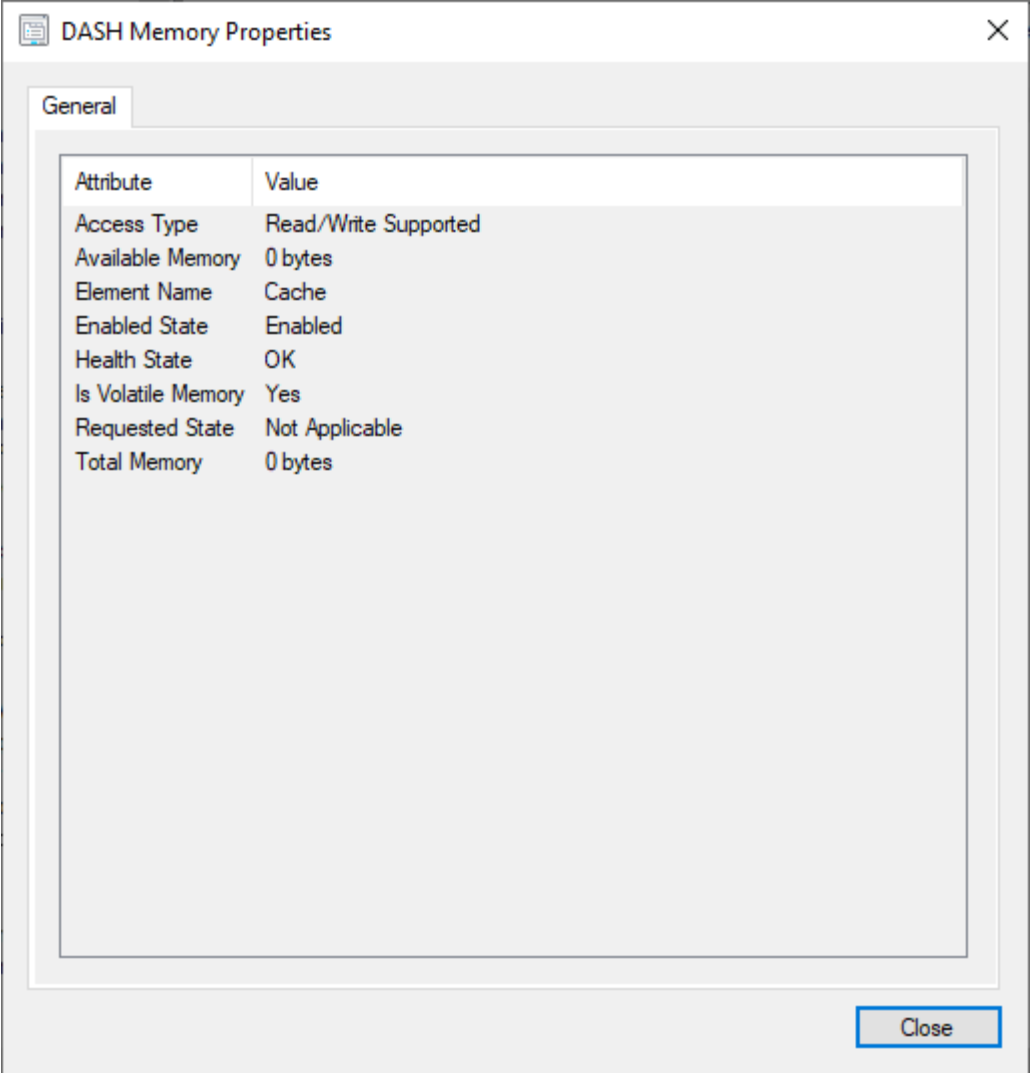


Figure 64: DASH 'Memory' Profile Properties

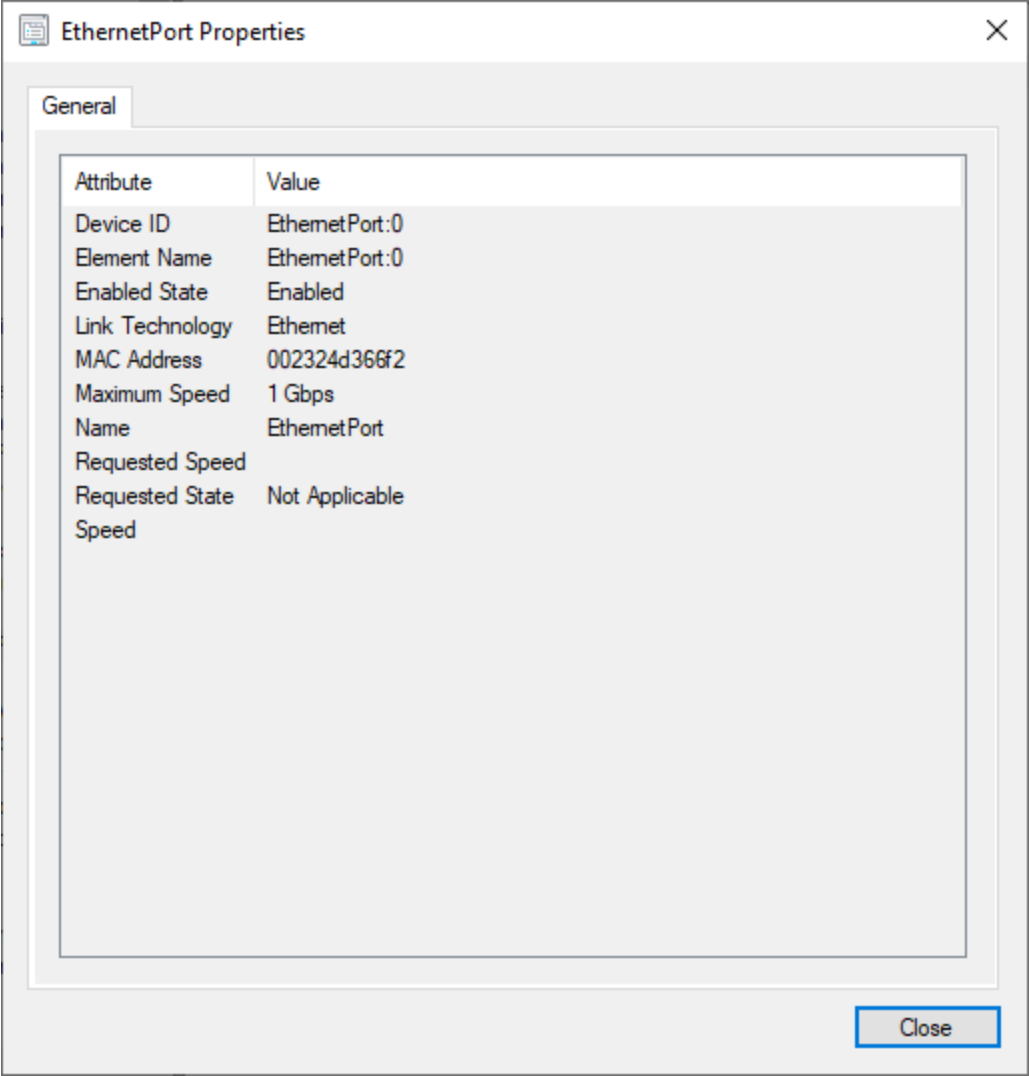


Figure 65: DASH 'Network Port' Properties

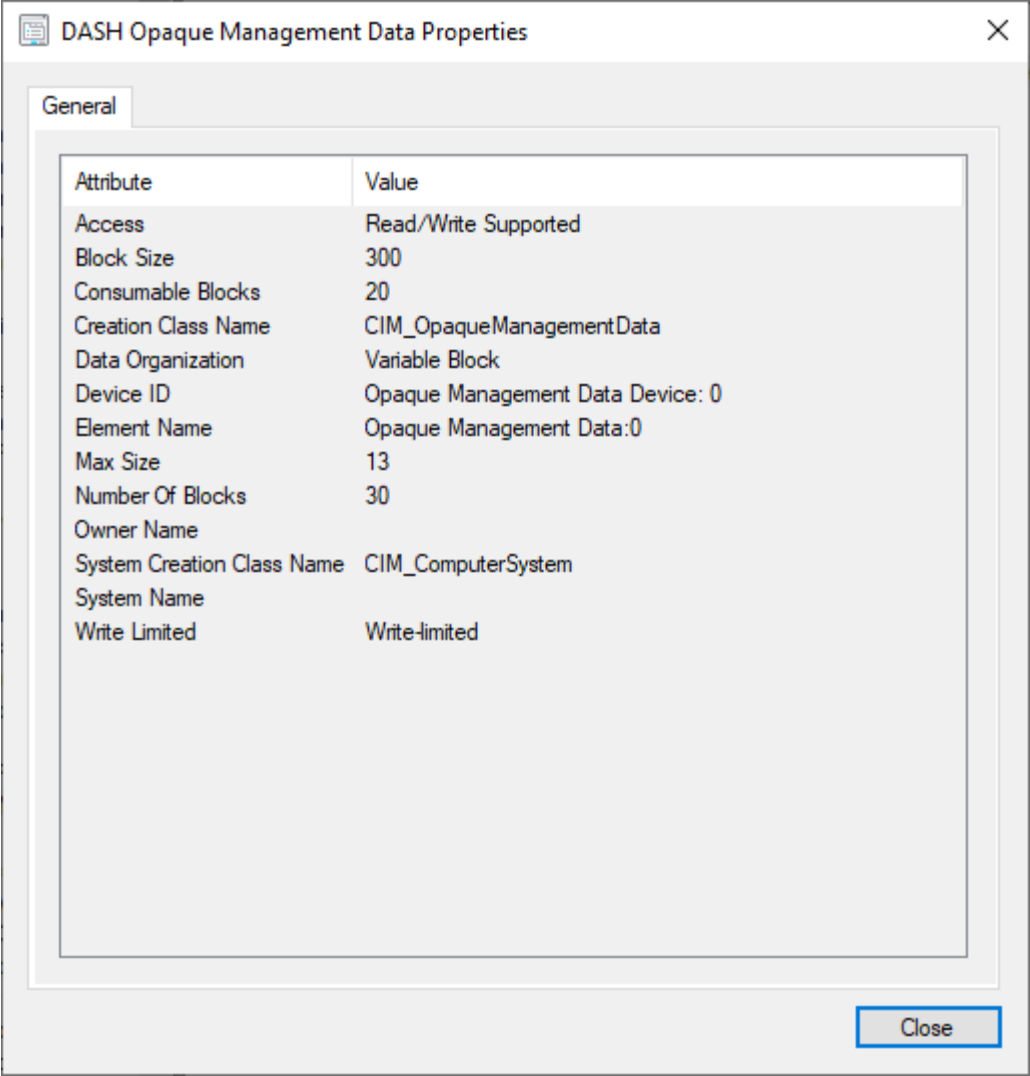


Figure 66: DASH 'Opaque Management Data' Profile Properties



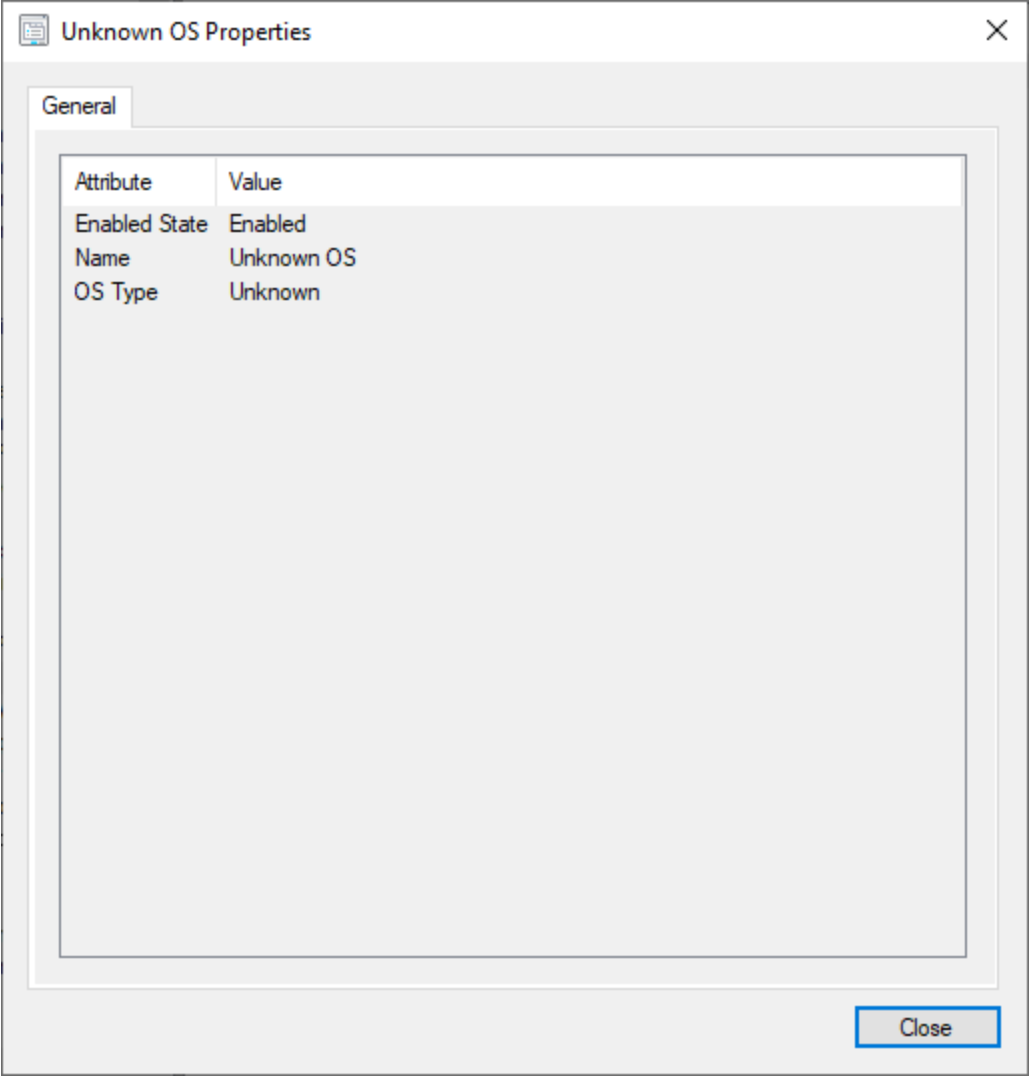


Figure 67: DASH 'Operating System' Profile Properties

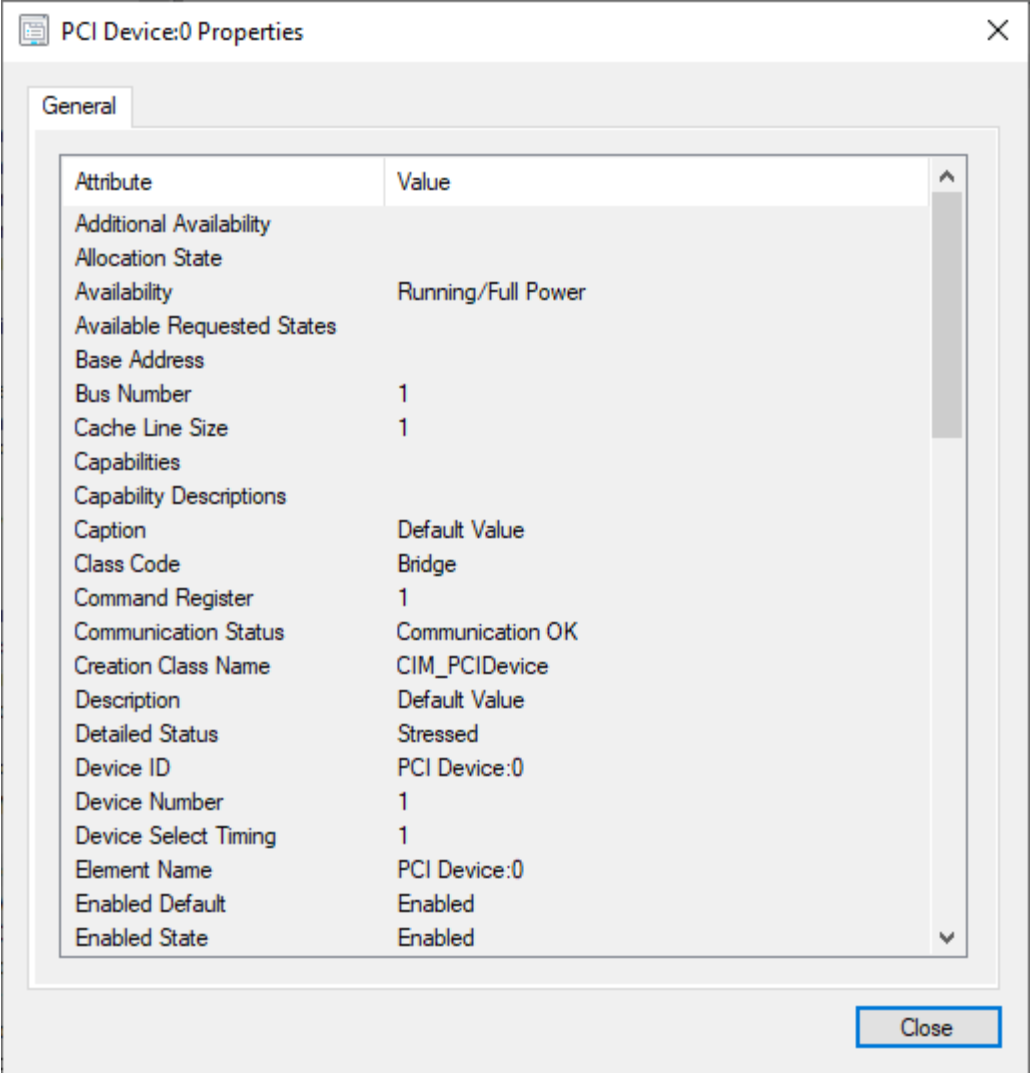


Figure 68: DASH 'PCI Device' Profile Properties

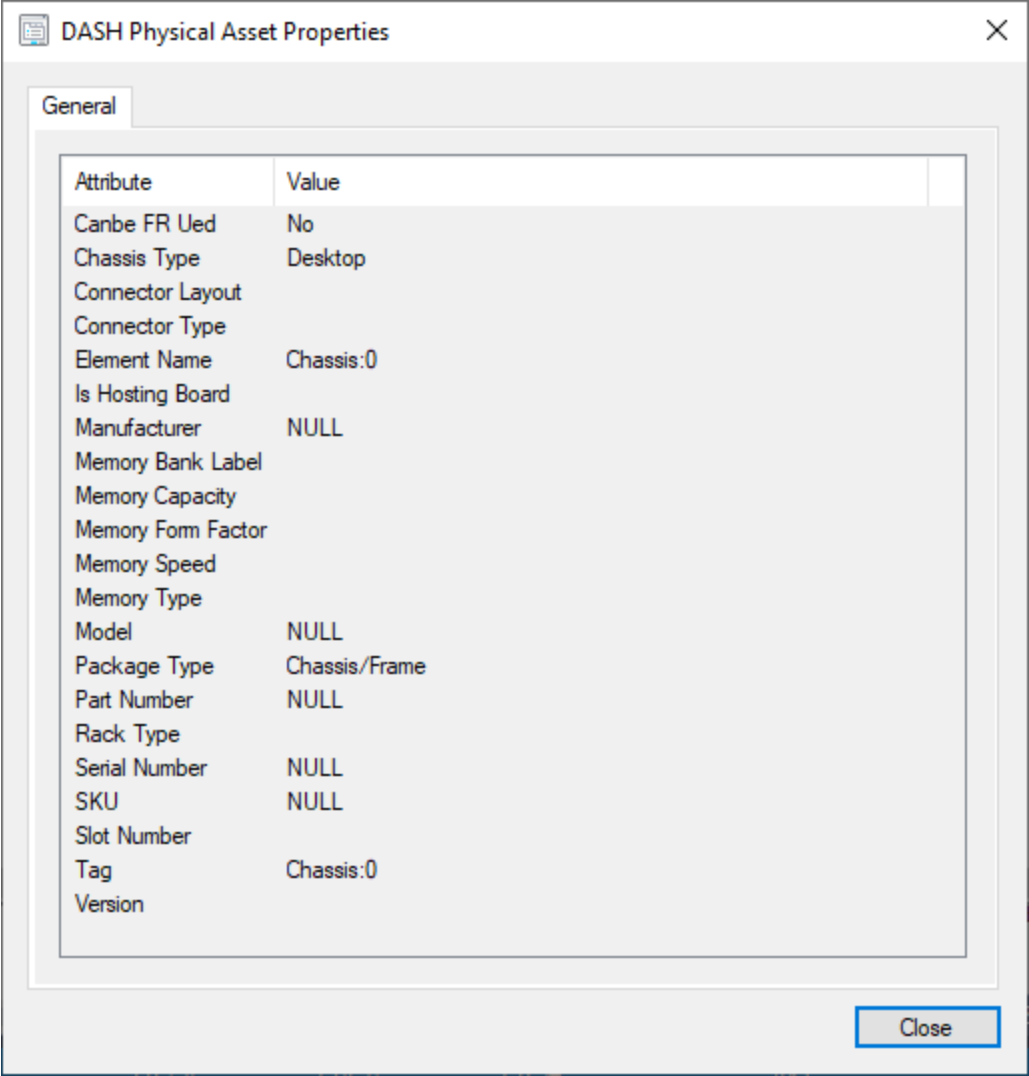
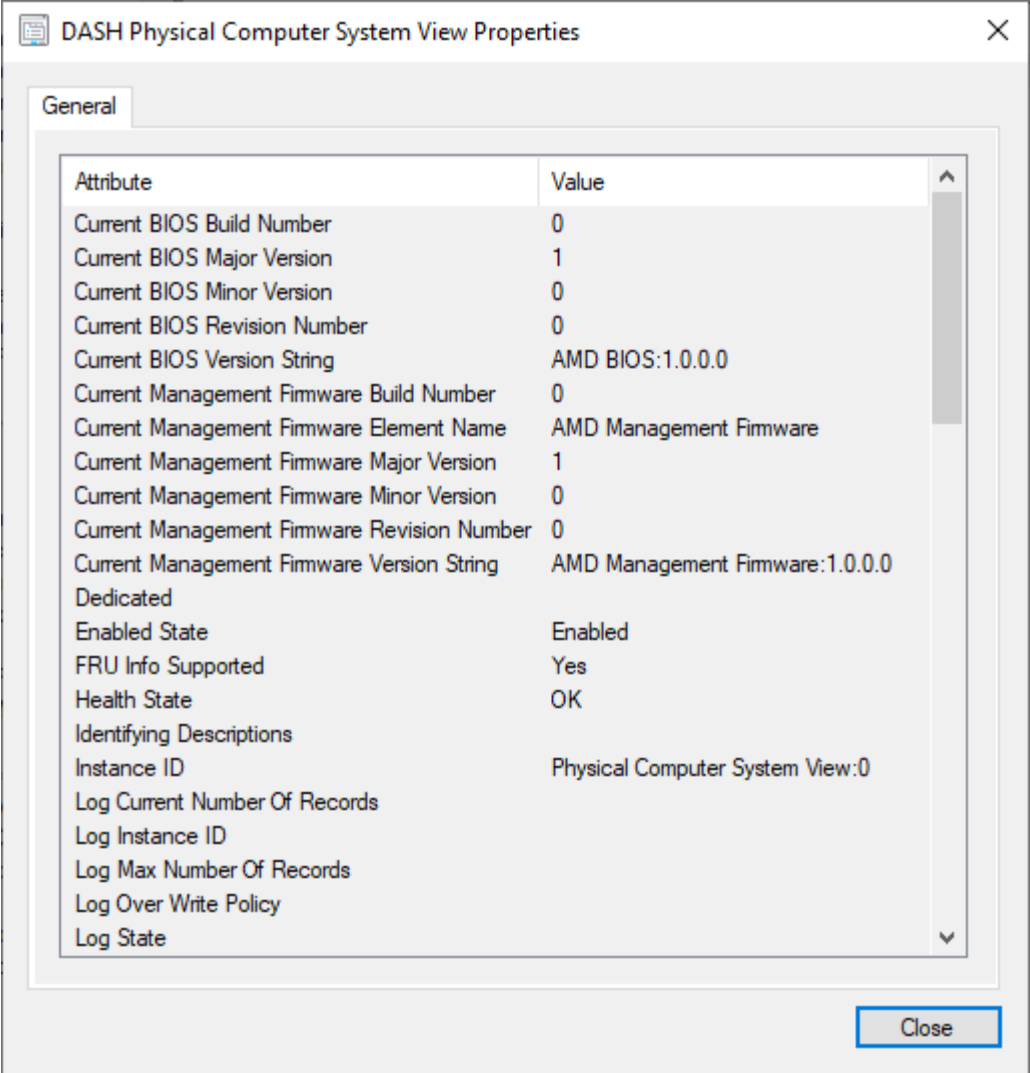


Figure 69: DASH 'Physical Asset' Profile Properties



**Figure 70: DASH 'Physical Computer System View' Profile Properties**

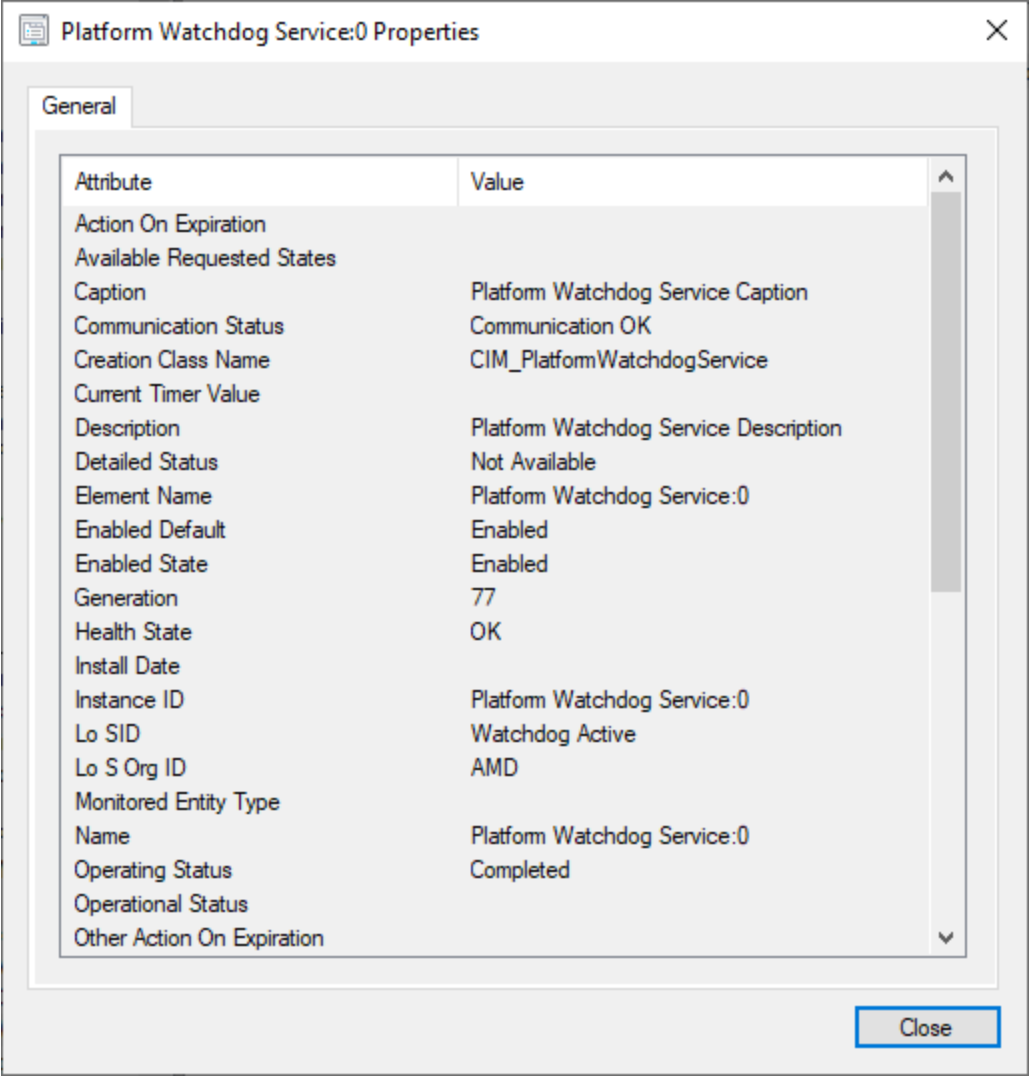


Figure 71: DASH 'Platform Watchdog Service' Profile Properties

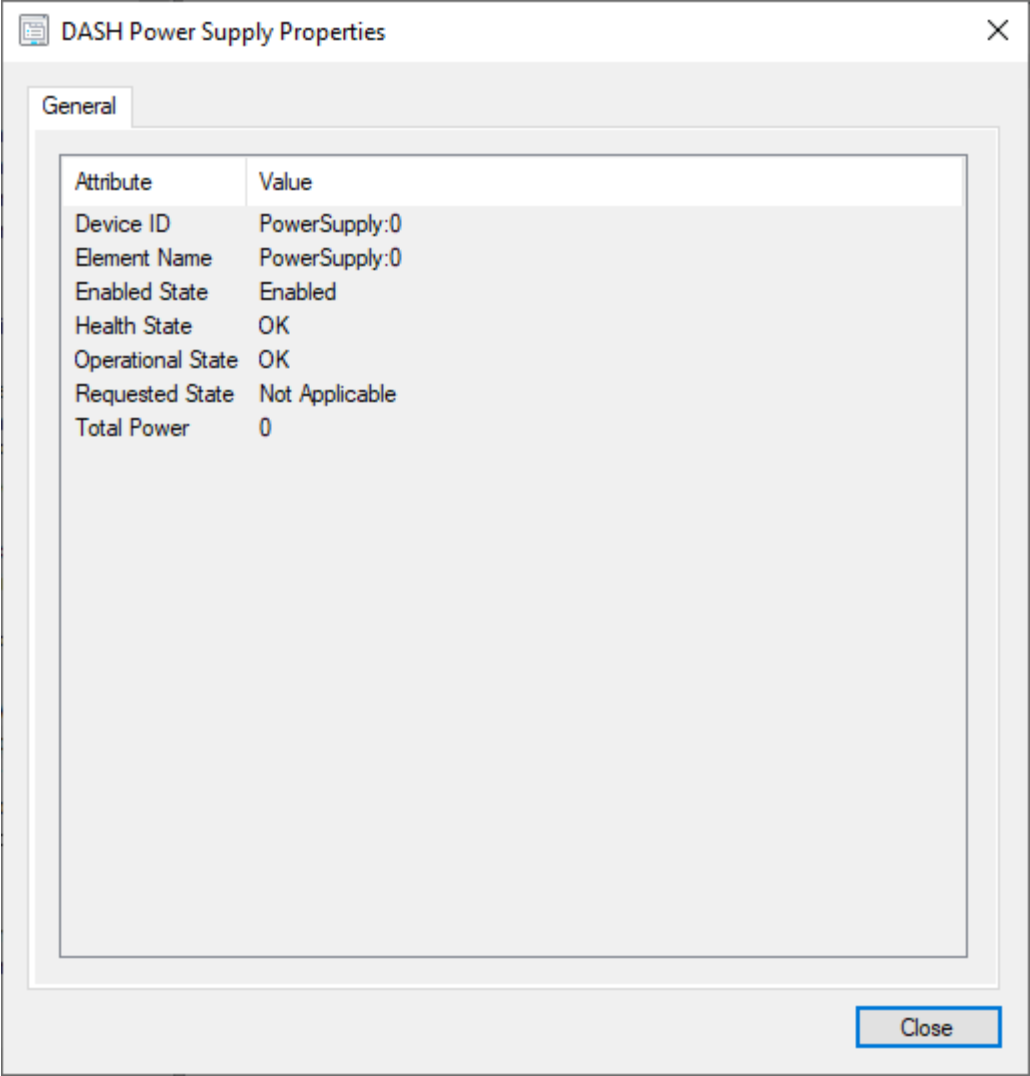
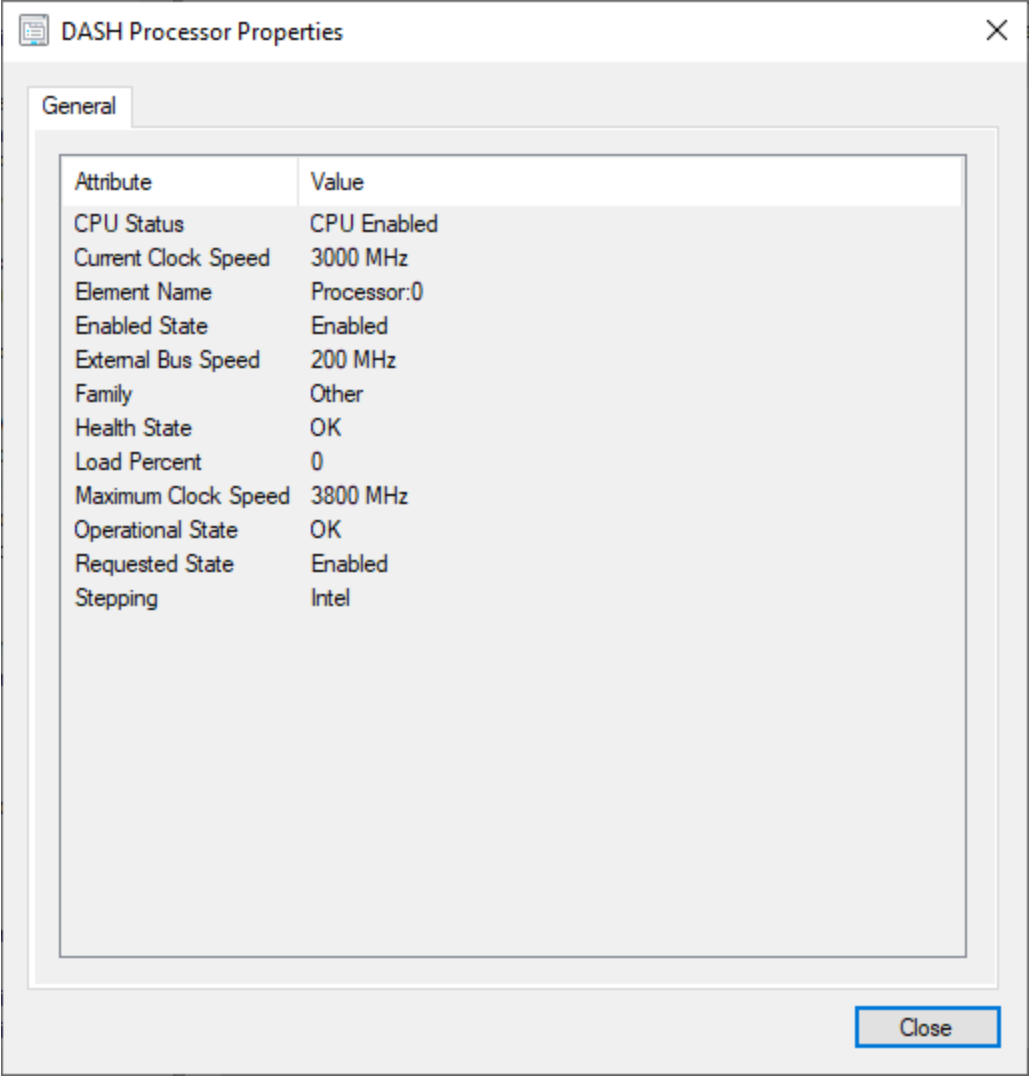


Figure 72: DASH 'Power Supply' Profile Properties



**Figure 73: DASH 'Processor' Profile Properties**

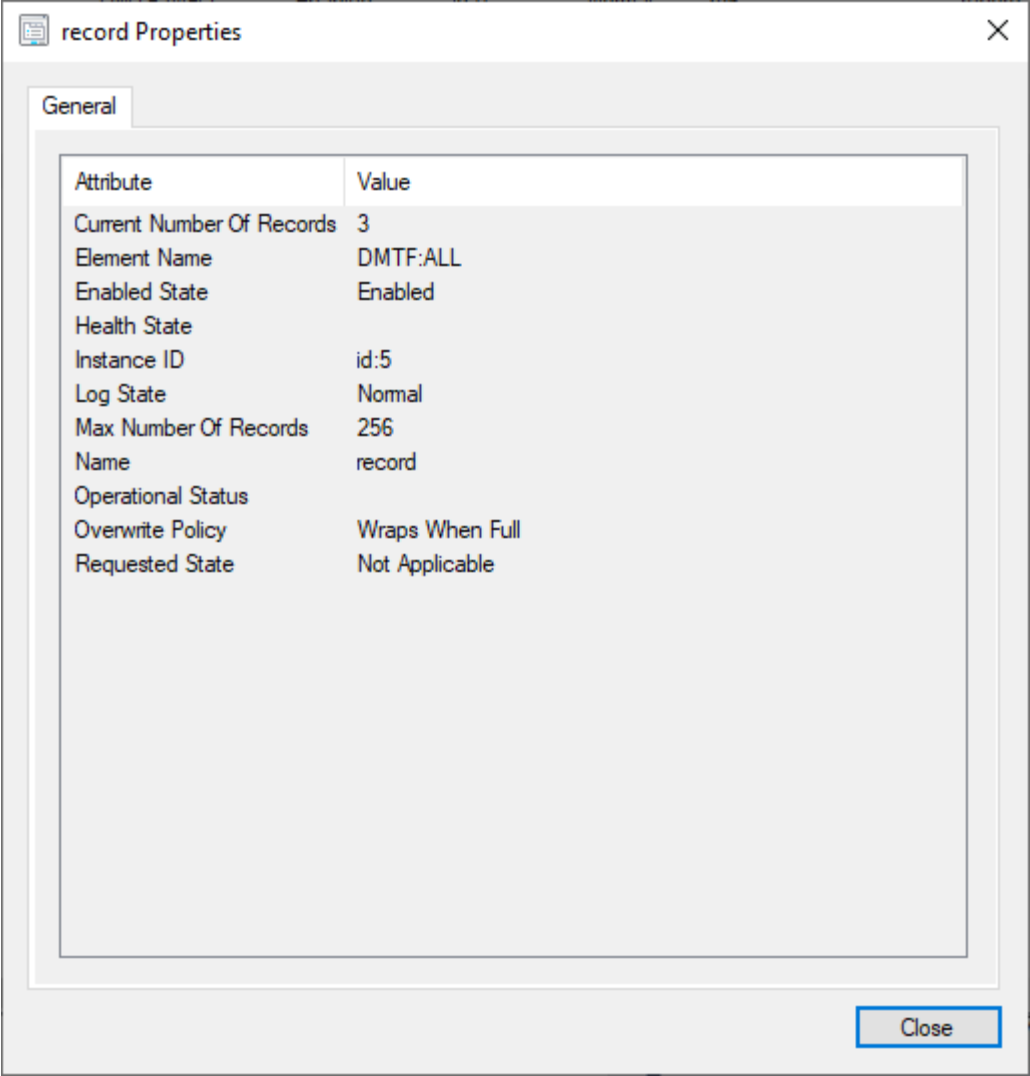
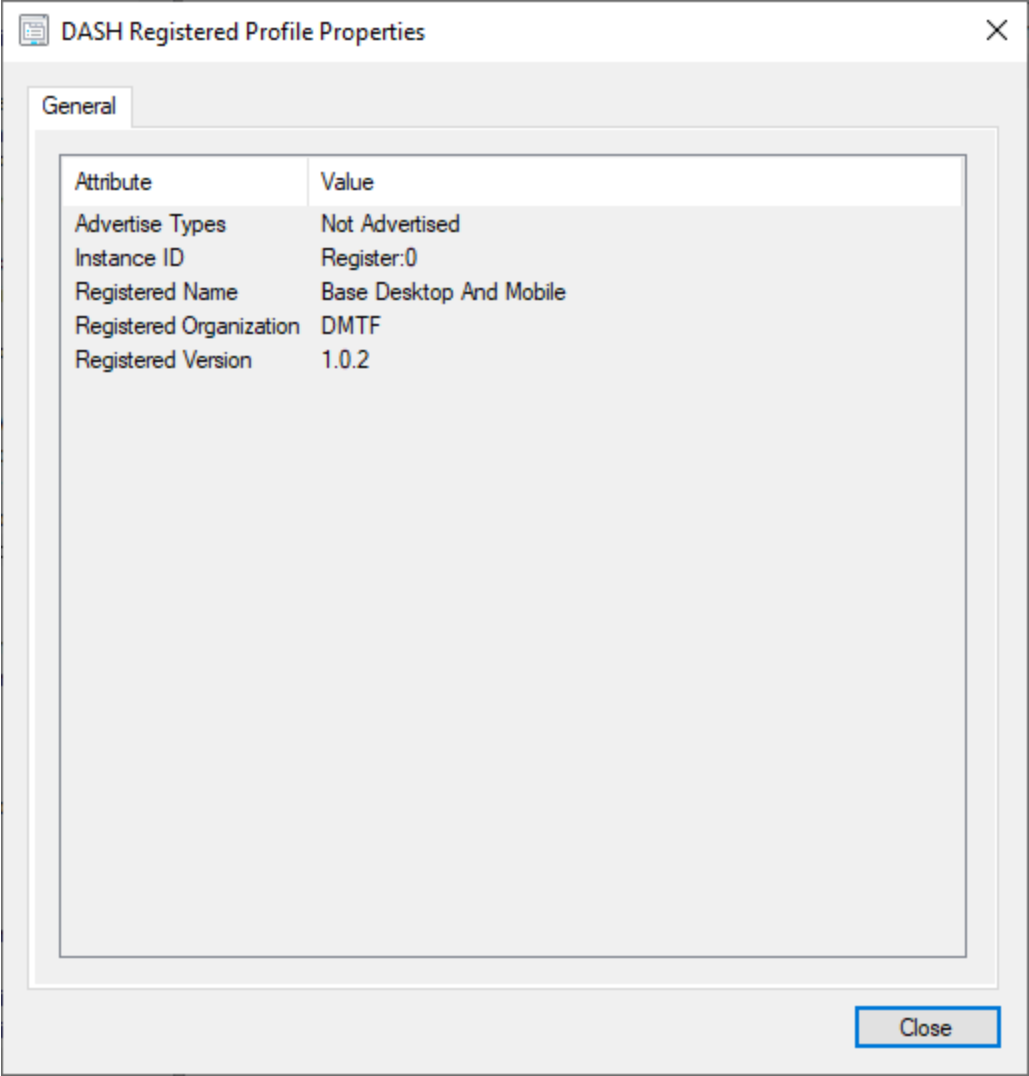


Figure 74: DASH 'Record Log' Profile Properties





**Figure 75: DASH 'Registered Profile' Profile Properties**

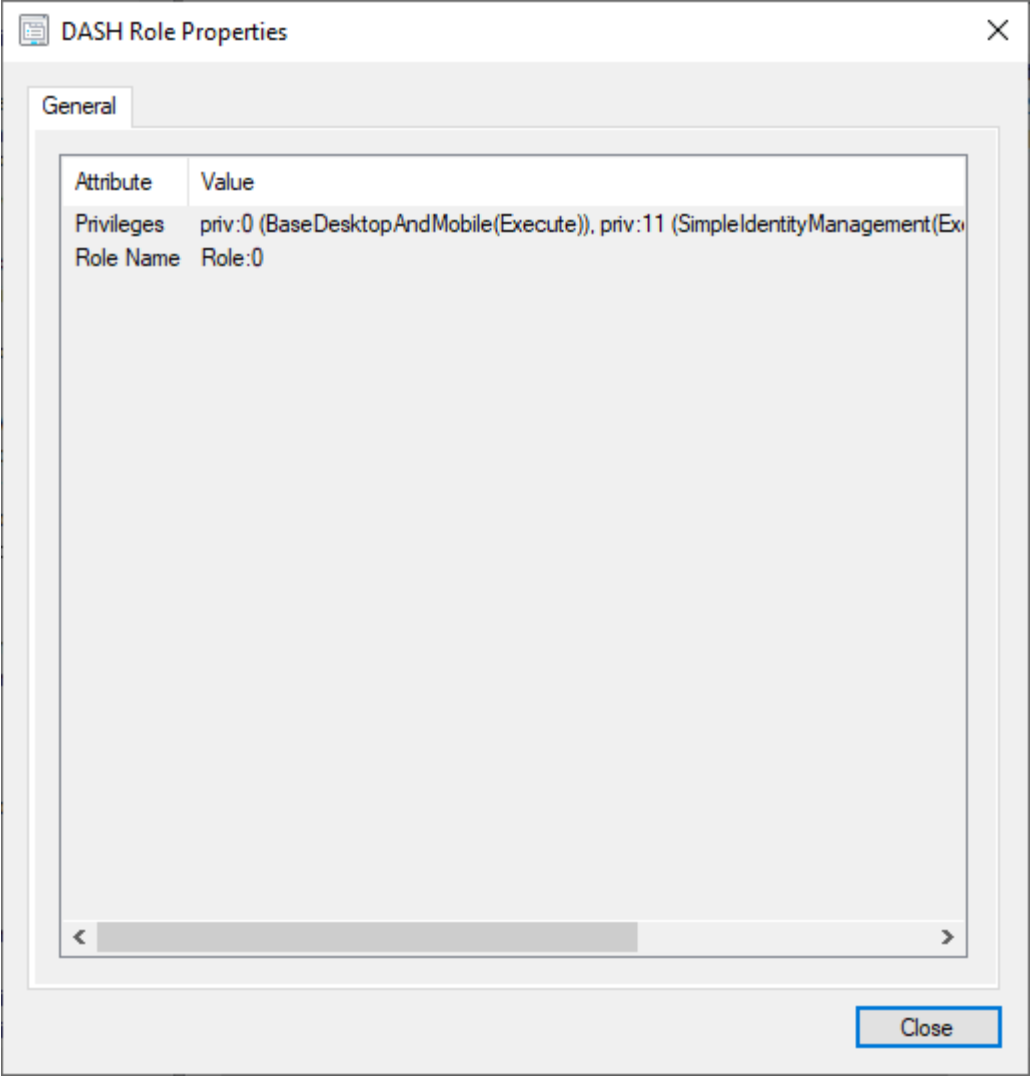


Figure 76: DASH 'Role' Profile Properties

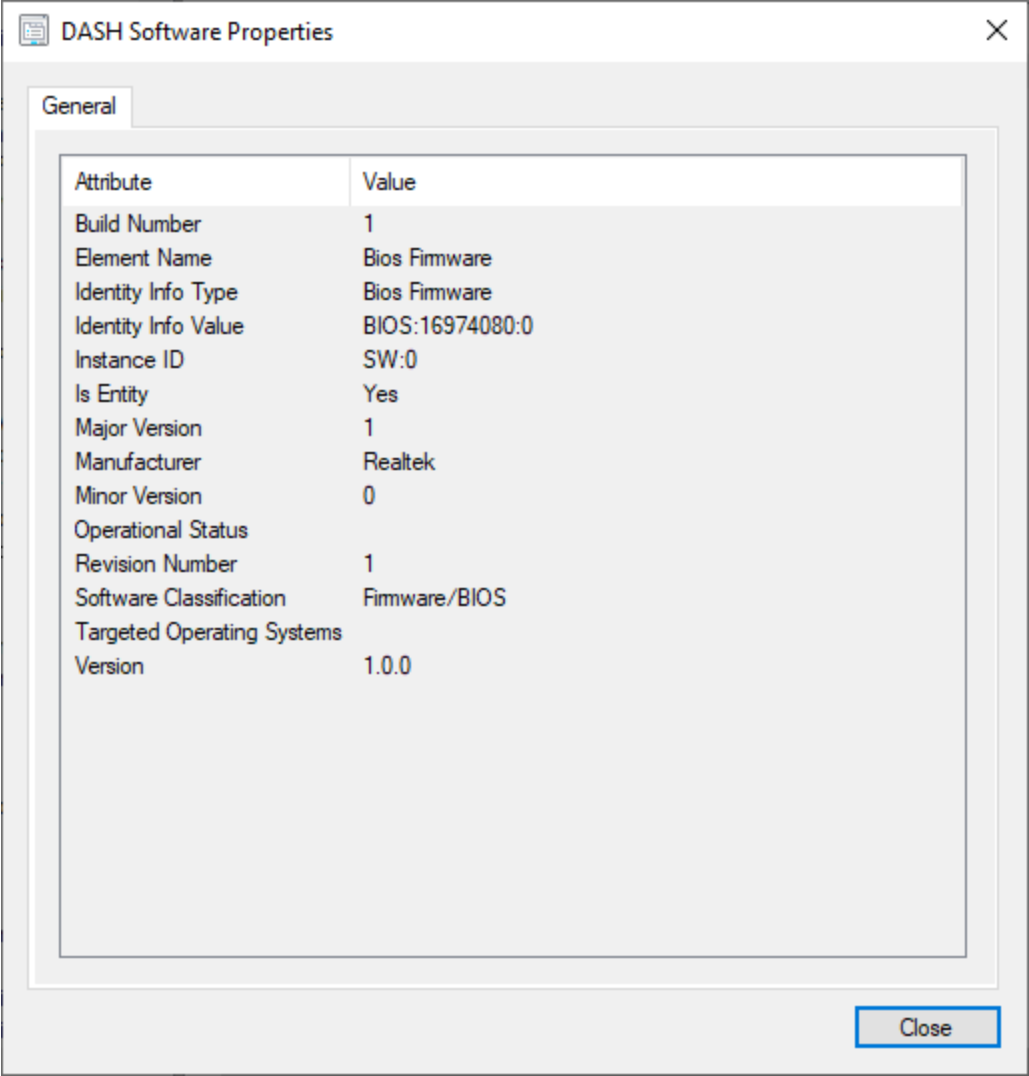


Figure 77: DASH 'Software' Profile Properties

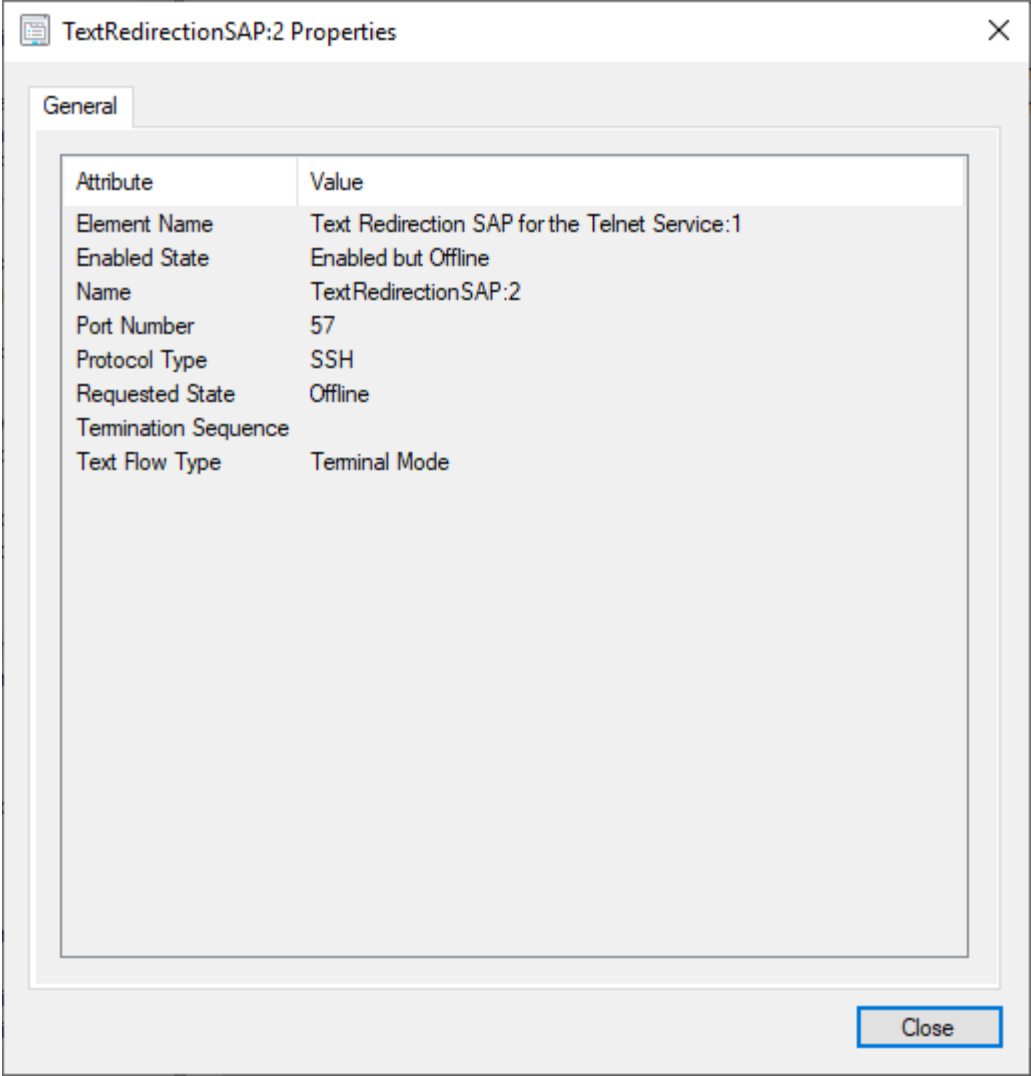


Figure 78: DASH 'Text Redirection' Profile Properties

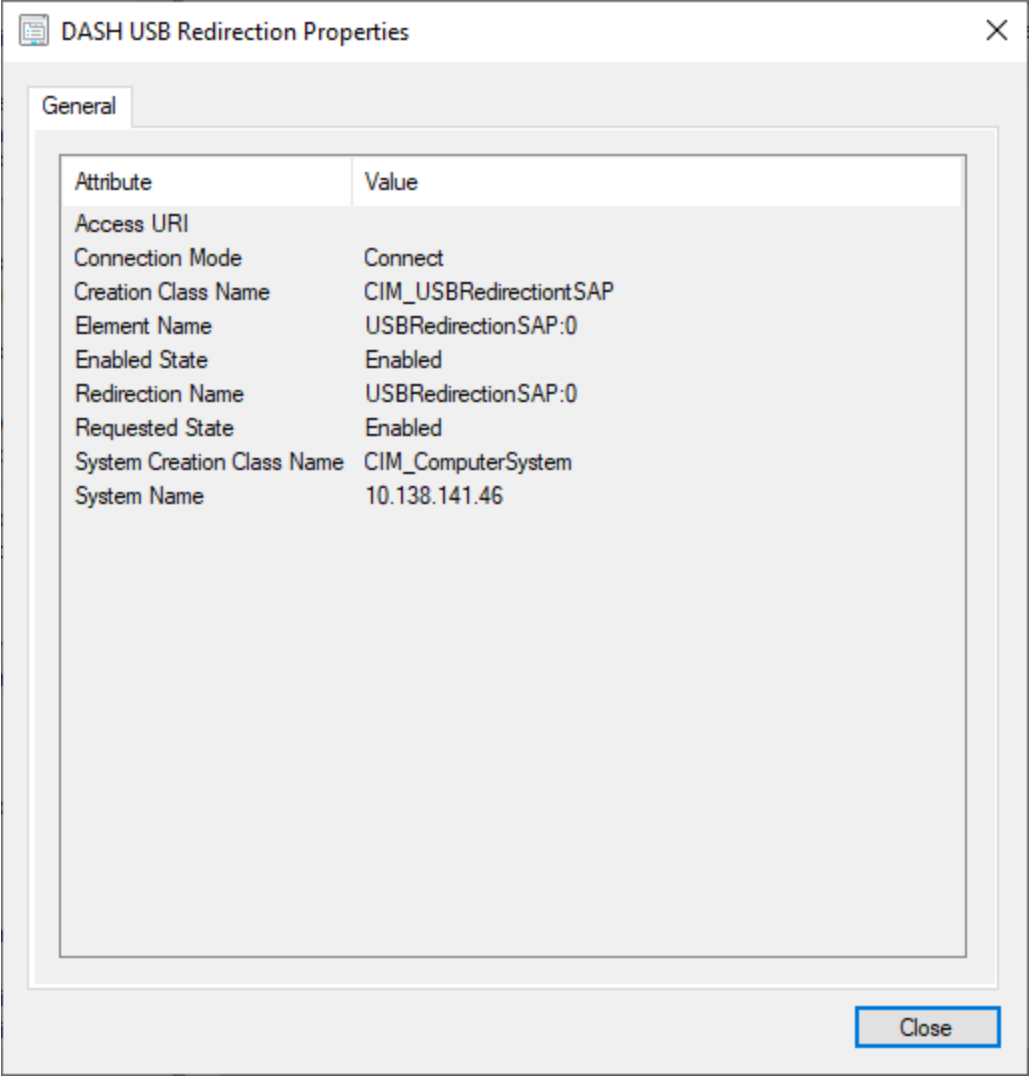


Figure 79: DASH ‘USB Redirection’ Profile Properties

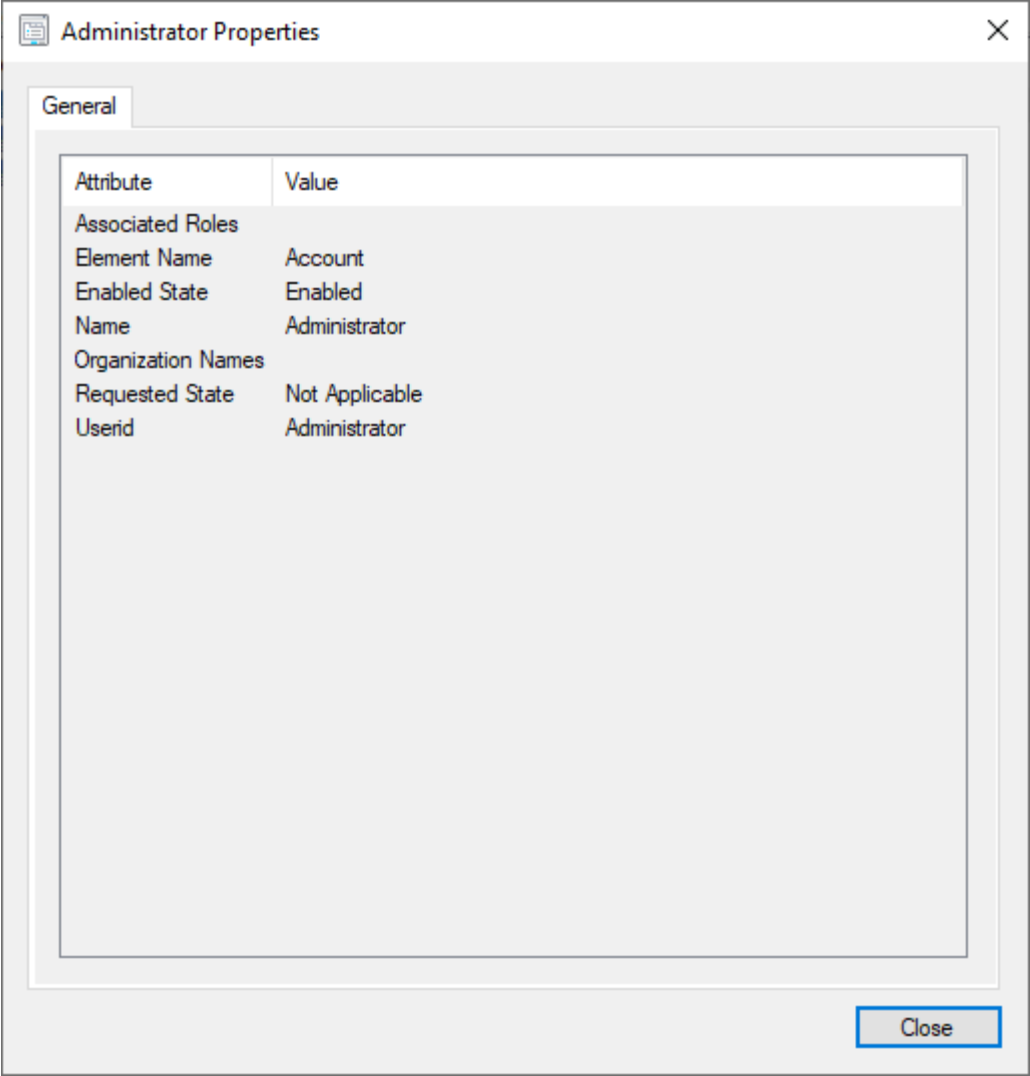


Figure 80: DASH 'User' Profile Properties

DASH Hardware history is recorded in **\SystemName\Hardware History**. The time of inventory collection and change in system inventory is recorded in this section.

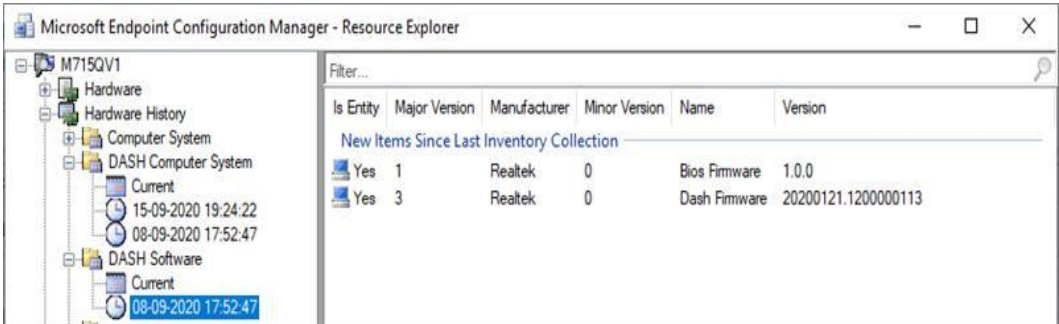


Figure 81: DASH Hardware History

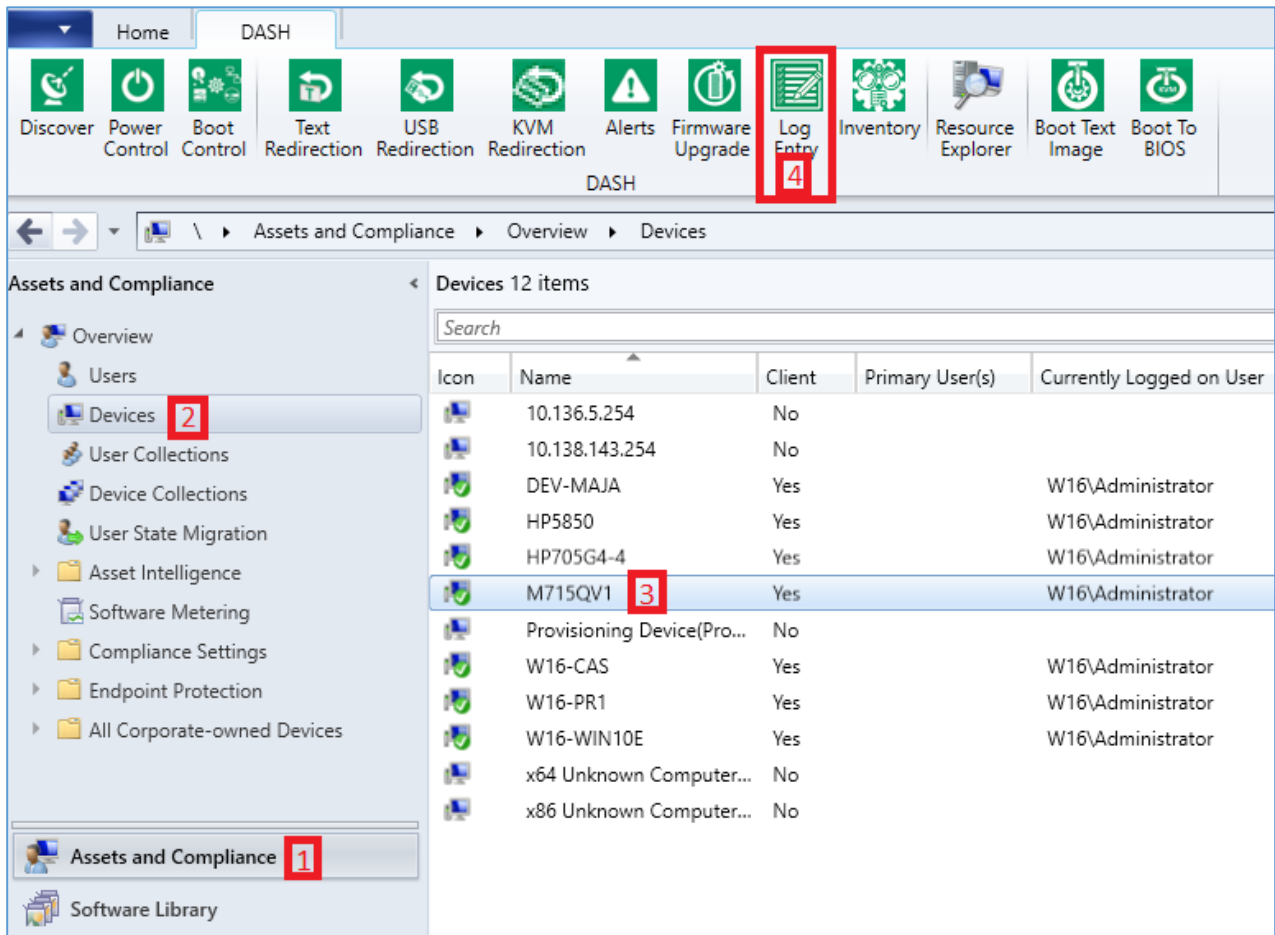
## 3.8 Log Entry

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

AMPS can read log files maintained by the managed DASH computer system, if available. AMPS displays a maximum of twenty log entries per screen as shown in Figure 83. Users can navigate the log screen using the provided controls.

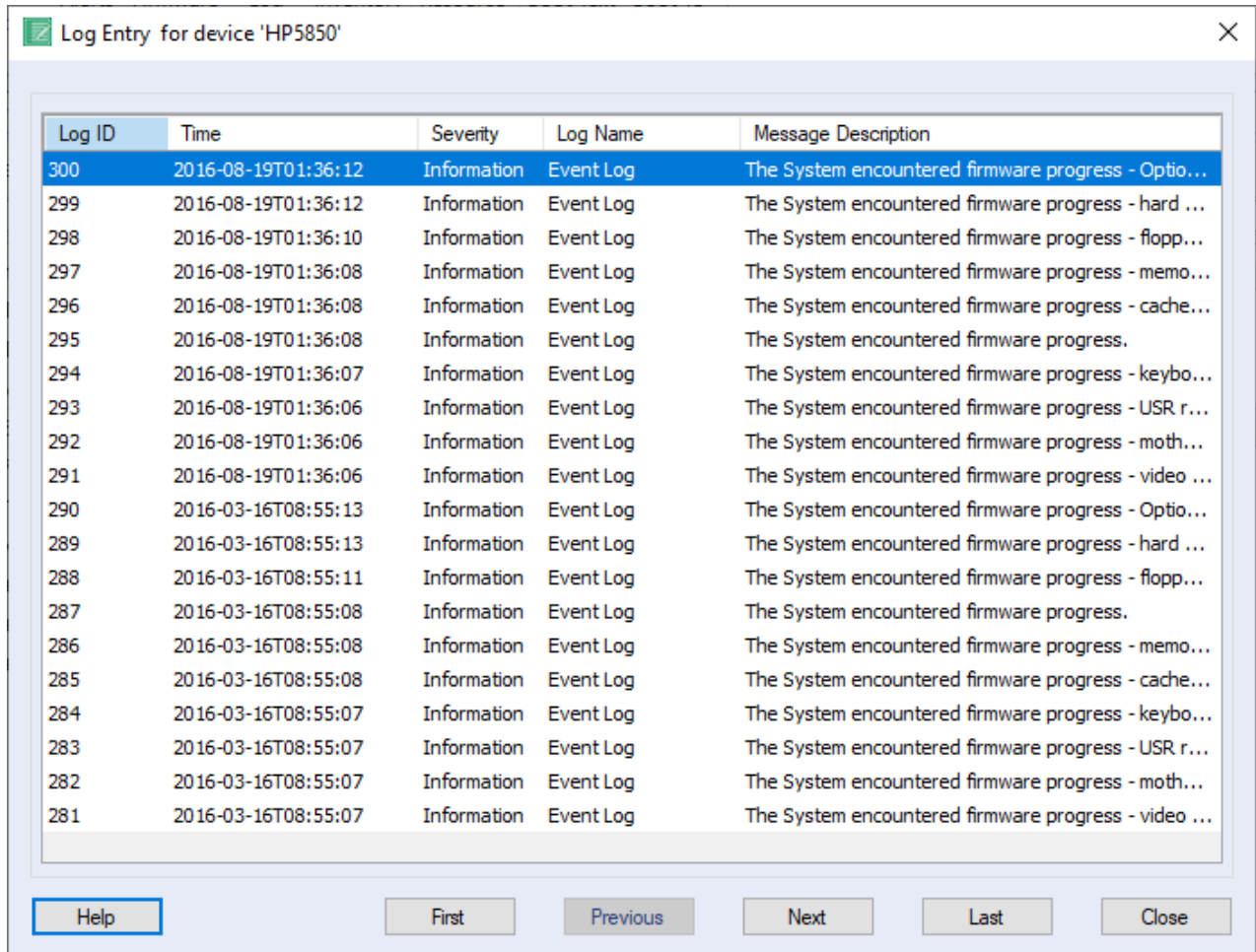
To view the log entry of a managed device:

1. Expand the **Assets and Compliance** node.
2. Expand the **Overview** node.
3. Expand the **Devices** node and click **All Systems**.
4. In the right pane, right-click the device on which you want to view the log entry. The shortcut menu is displayed.
5. In the shortcut menu, point to **DASH** and then click **Log Entry**. The log entry screen appears.



**Figure 82: Viewing the Log Entry of a device**

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.



Log ID	Time	Severity	Log Name	Message Description
300	2016-08-19T01:36:12	Information	Event Log	The System encountered firmware progress - Optio...
299	2016-08-19T01:36:12	Information	Event Log	The System encountered firmware progress - hard ...
298	2016-08-19T01:36:10	Information	Event Log	The System encountered firmware progress - flopp...
297	2016-08-19T01:36:08	Information	Event Log	The System encountered firmware progress - memo...
296	2016-08-19T01:36:08	Information	Event Log	The System encountered firmware progress - cache...
295	2016-08-19T01:36:08	Information	Event Log	The System encountered firmware progress.
294	2016-08-19T01:36:07	Information	Event Log	The System encountered firmware progress - keybo...
293	2016-08-19T01:36:06	Information	Event Log	The System encountered firmware progress - USR r...
292	2016-08-19T01:36:06	Information	Event Log	The System encountered firmware progress - moth...
291	2016-08-19T01:36:06	Information	Event Log	The System encountered firmware progress - video ...
290	2016-03-16T08:55:13	Information	Event Log	The System encountered firmware progress - Optio...
289	2016-03-16T08:55:13	Information	Event Log	The System encountered firmware progress - hard ...
288	2016-03-16T08:55:11	Information	Event Log	The System encountered firmware progress - flopp...
287	2016-03-16T08:55:08	Information	Event Log	The System encountered firmware progress.
286	2016-03-16T08:55:08	Information	Event Log	The System encountered firmware progress - memo...
285	2016-03-16T08:55:08	Information	Event Log	The System encountered firmware progress - cache...
284	2016-03-16T08:55:07	Information	Event Log	The System encountered firmware progress - keybo...
283	2016-03-16T08:55:07	Information	Event Log	The System encountered firmware progress - USR r...
282	2016-03-16T08:55:07	Information	Event Log	The System encountered firmware progress - moth...
281	2016-03-16T08:55:07	Information	Event Log	The System encountered firmware progress - video ...

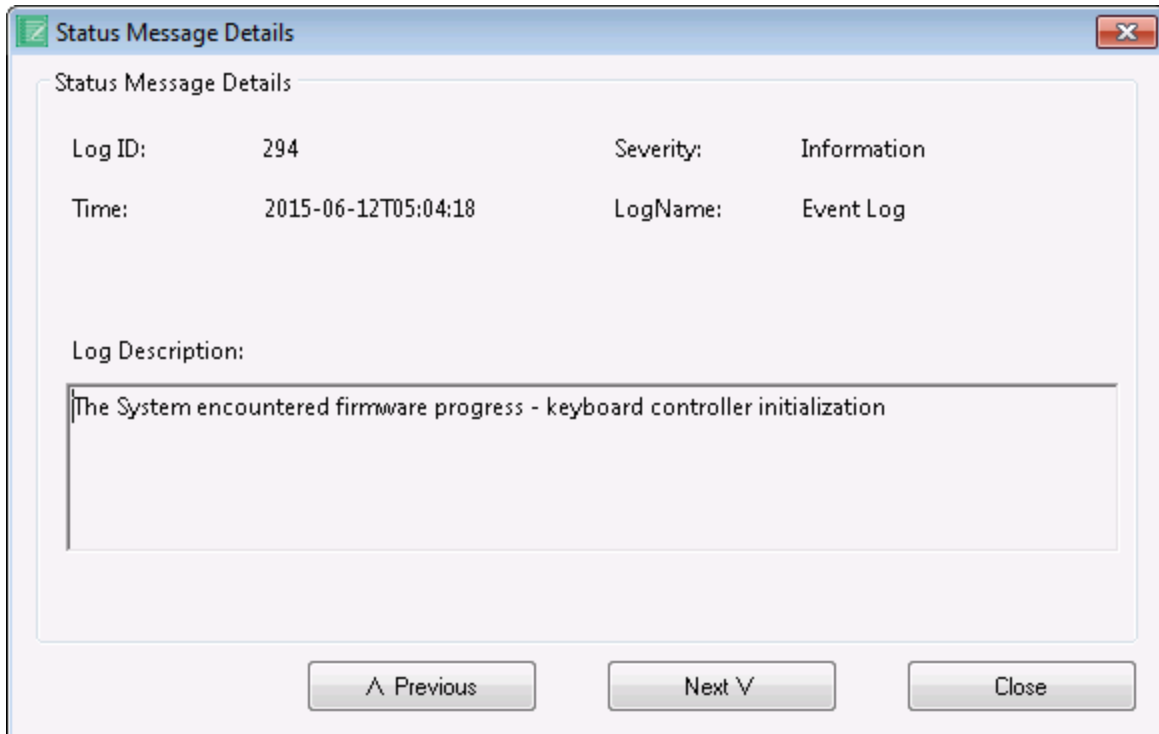
**Figure 83: Log Entry**

When the user double clicks on a log entry, a separate popup window is launched which displays log entry in detail.

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 84 illustrates the Status Message Detail screen which is displayed on double clicking on a log entry.





**Figure 84: Status Message Details**

## 3.9 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.

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.
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.

The managed system boots to the URL image and the boot process can be seen in the SSH terminal session.

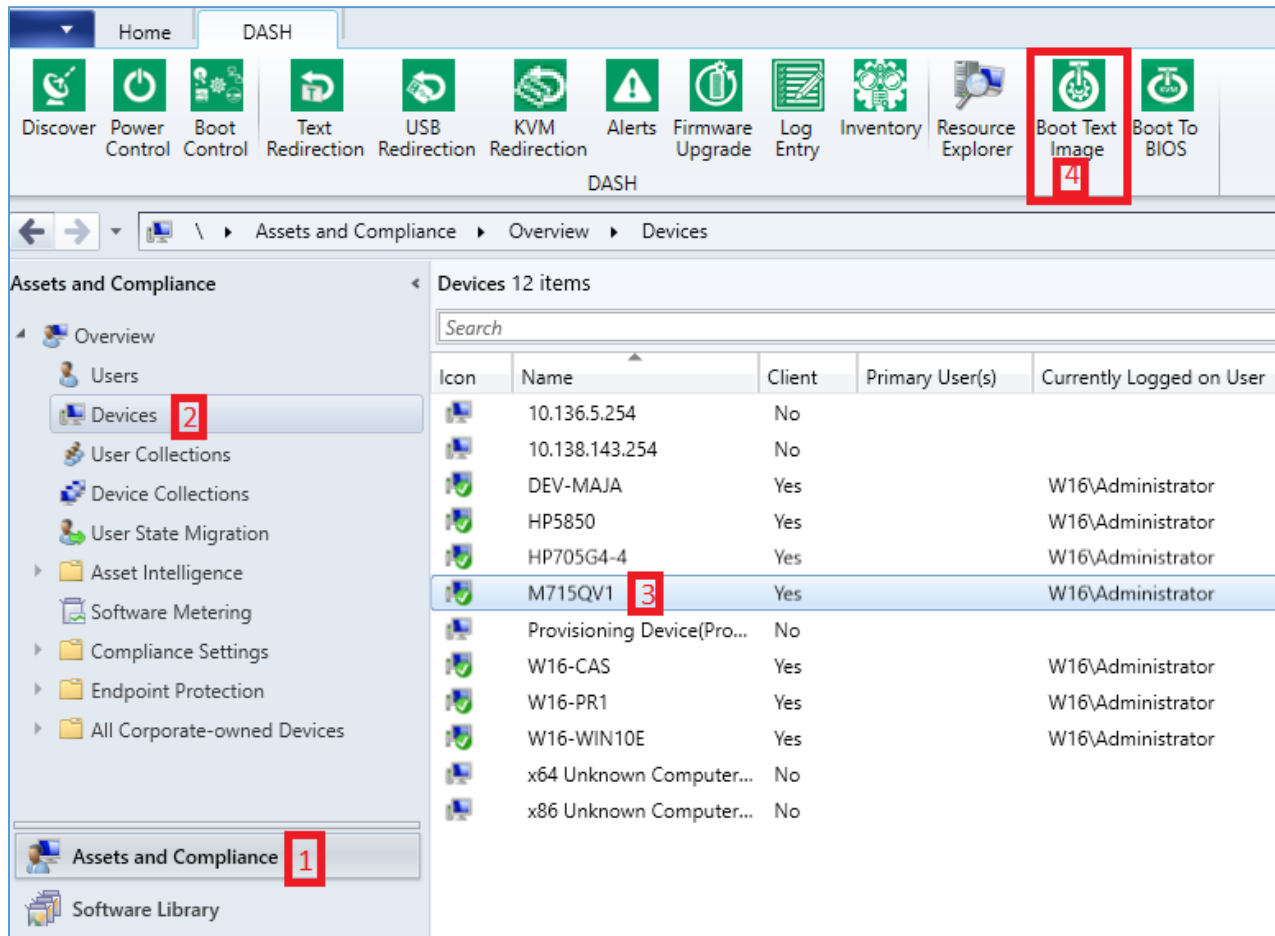
Note: After successfully booting to a remote image file, the boot order of that particular remote system will be changed to 'USB' as first boot device. So, after the terminal session is completed, perform these steps on the DASH system to bring it back to original state:

- Disconnect USB Using USB Redirection screen.
- Change boot order to original state.

To perform Boot Text Image task,

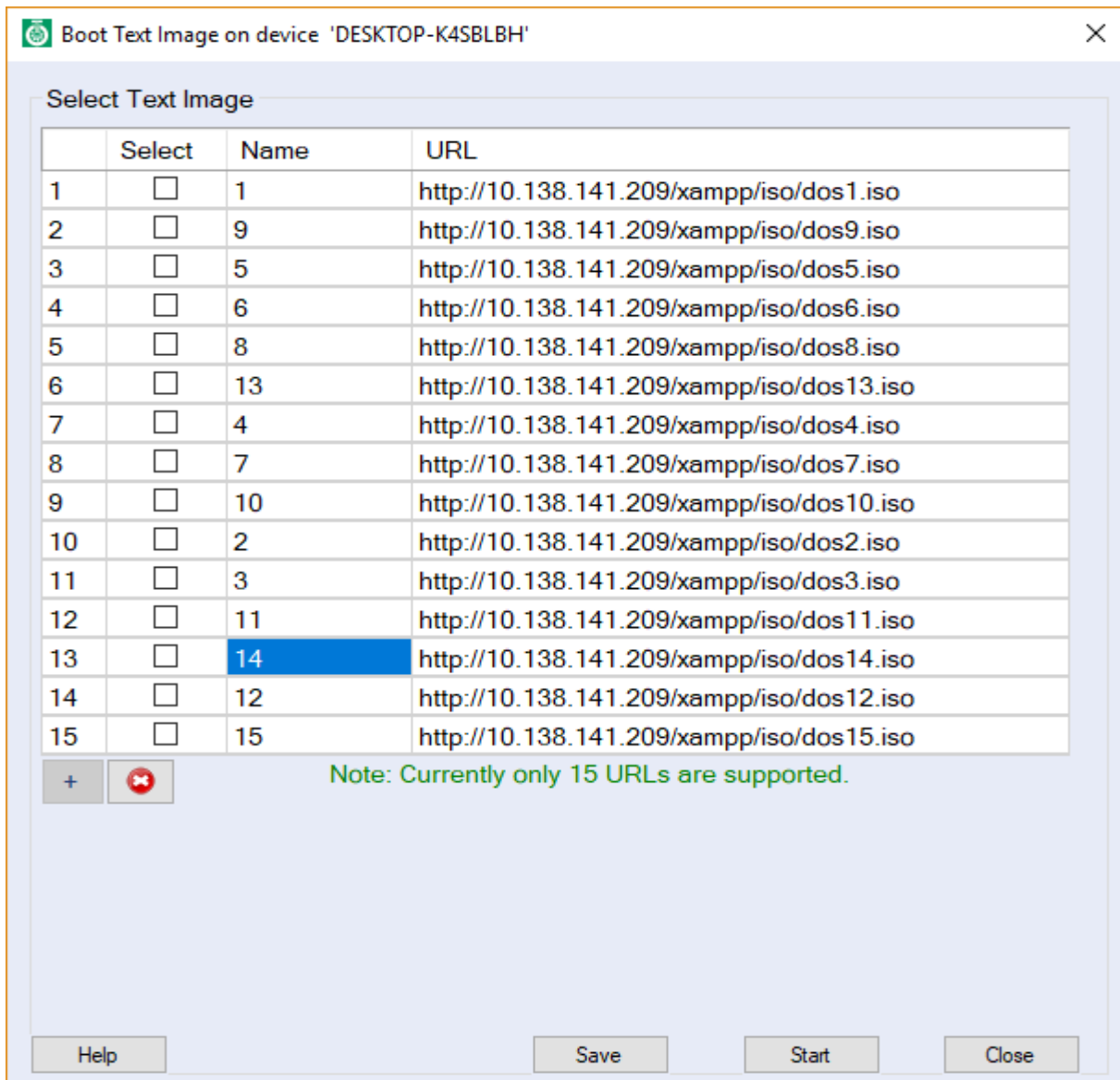
- Expand the **Assets and Compliance** node .
- Expand the **Overview** node.
- Expand the **Devices** node that appears on the left pane and click on **All Systems**.
- In the right pane, right click the device on which you want to perform Boot Text Image.
- You will be able to see the DASH in the menu, expand DASH and click on **Boot Text Image**.  
Alternatively , on the ribbon icon click DASH tab and then click on **Boot Text Image**.

These steps are illustrated in figure below.




**Figure 85: Boot Text Image on device**

Boot Text Image screen will appear as shown in the figure below:



**Figure 86: Boot Text Image**

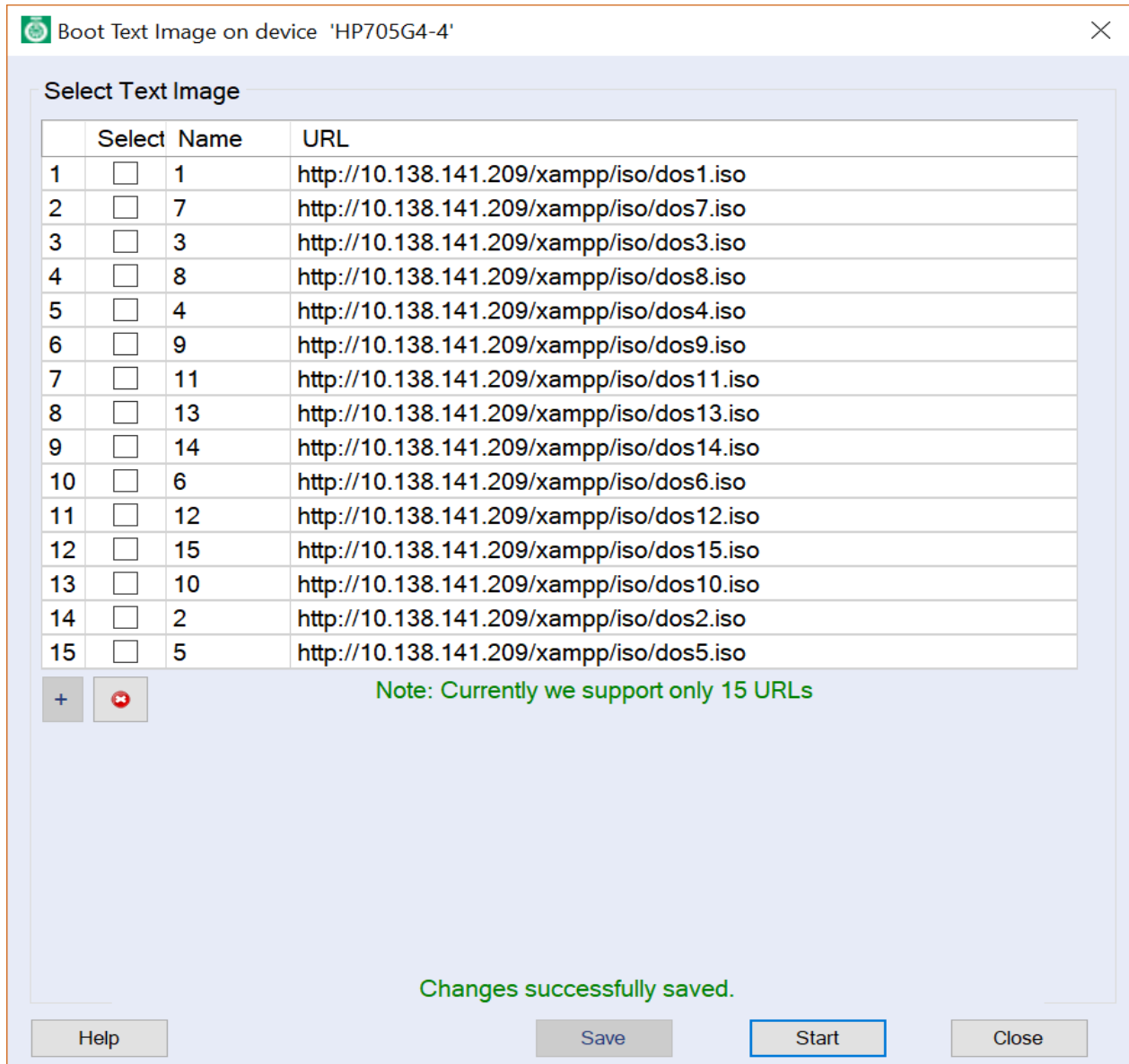
In the Boot Text Image screen,

- 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 multiple or single URL at a time.
- 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:

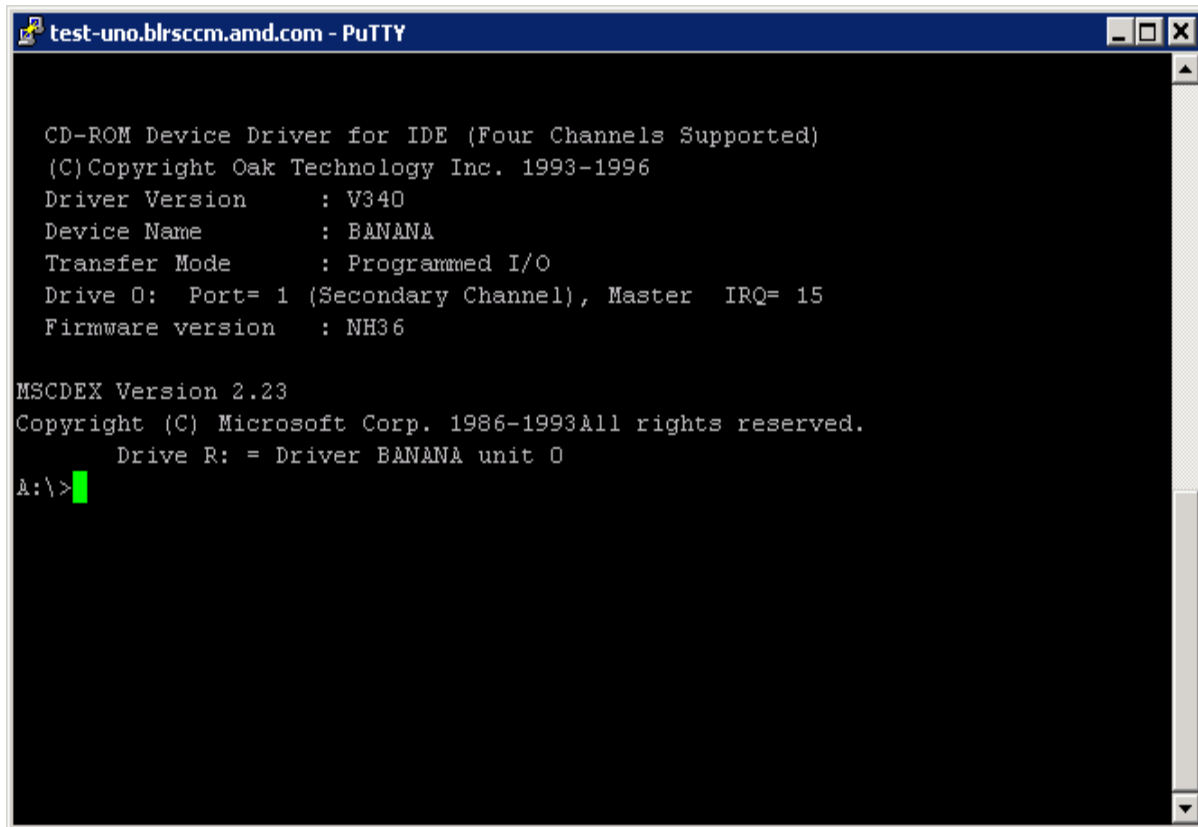
- Clicking 'start' button won't save the list. URL list has to be saved by clicking 'Save' button.
- If an URL is already connected, that URL is shown as checked in the URLs list.
- User can save up to 15 URLs in the list.

Below figure will show the after adding and saving the URL:



**Figure 87: Boot Text Image after adding URL**

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



```

test-uno.blrscdm.amd.com - PuTTY

CD-ROM Device Driver for IDE (Four Channels Supported)
(C) Copyright Oak Technology Inc. 1993-1996
Driver Version      : V340
Device Name         : BANANA
Transfer Mode        : Programmed I/O
Drive 0: Port= 1 (Secondary Channel), Master  IRQ= 15
Firmware version     : NH36

MSCDEX Version 2.23
Copyright (C) Microsoft Corp. 1986-1993 All rights reserved.
Drive R: = Driver BANANA unit 0
A:\>

```

**Figure 88: Boot Text Image after booted to URL**

### 3.9.1 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 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.

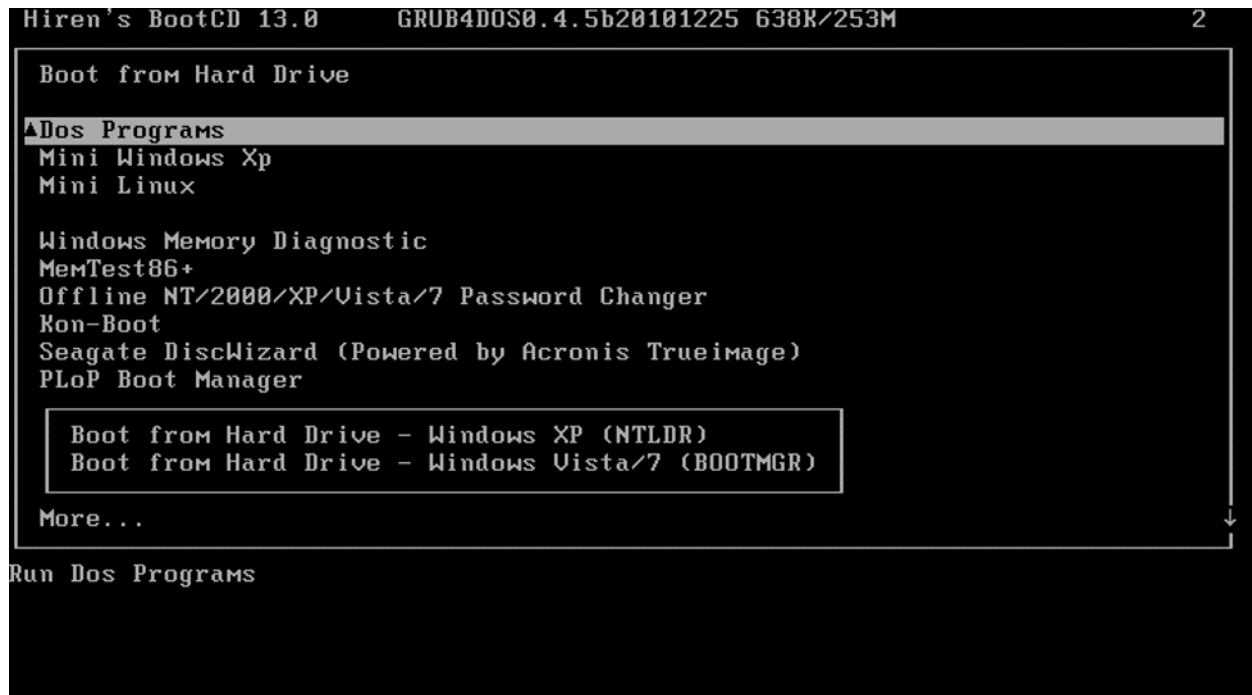


Figure 89: Selecting DOS Image

## 3.10 Firmware Update

This feature allows you to update the firmware on selected devices or collections.

### 3.10.1 Firmware Update on Collection

AMPS allow you update the firmware for a group of systems in a given collection.

To update the firmware on collection, perform the following steps:

1. Expand the **Assets and Compliance** node.
2. Expand the **Overview** node and click **Device Collections**.  
In the right pane, the list of all the available collections appears.
3. Right-click the collection for which you want to initiate power control.  
The shortcut menu appears.
4. In the shortcut menu, select **DASH** and then click **Firmware Upgrade**.

The above procedure is illustrated in Figure 90.

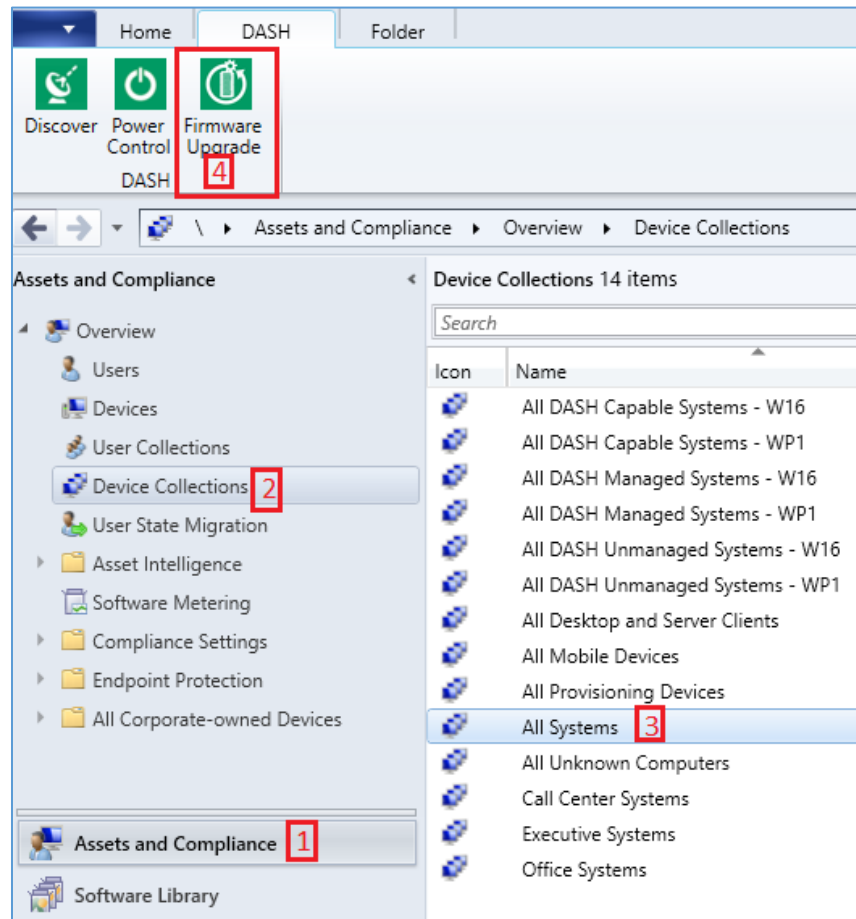


Figure 90: Firmware Update on Collection

The **Firmware Update on Collection** dialog box appears as shown in Figure 91 and Figure 92

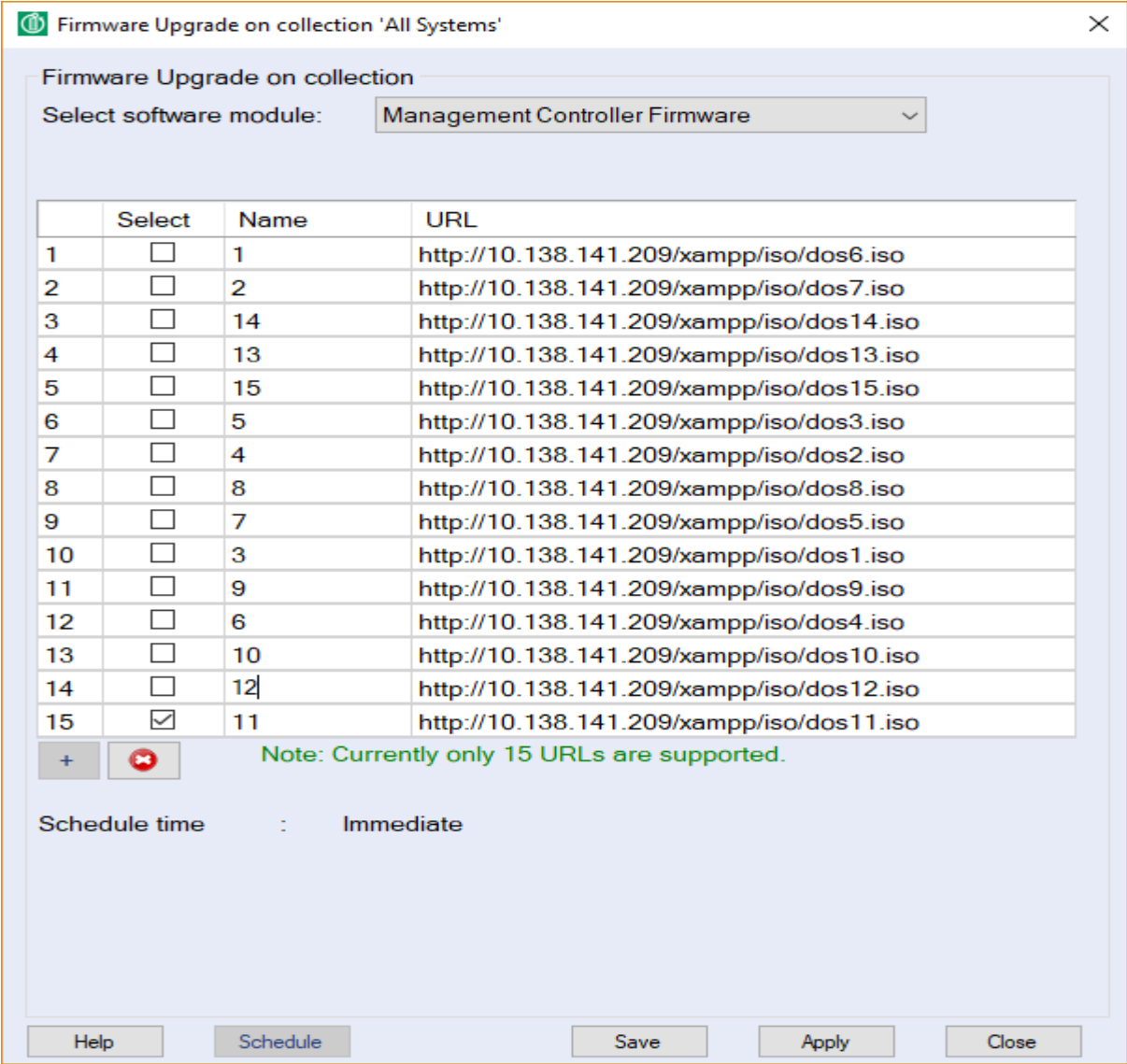
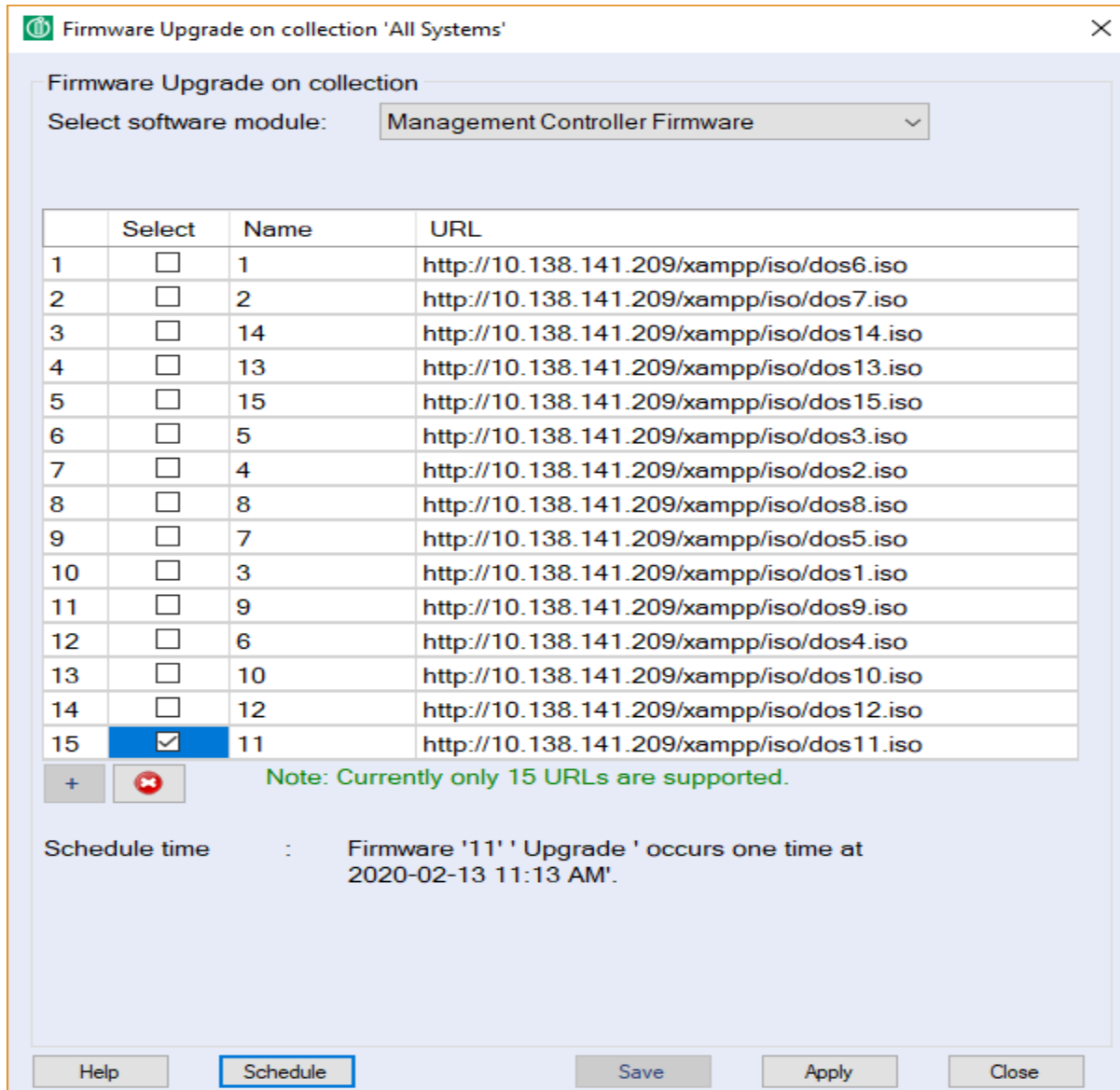



Figure 91: Immediate Firmware Update on Collection





**Figure 92: Scheduled Firmware Update on Collection**

5. In the Firmware Upgrade on Collection dialog box,
  - a) Select the Software Module from the drop-down list. The available Software module options are as follows:
    - Management Controller Firmware
  - b) Schedule Time states the occurrence of the specified firmware update task. It can be immediate (shown in Figure 91) or scheduled (shown in Figure 92).
  - c) The grid shown in the dialog box lists the Firmware URLs of the devices with their Names and Name field .  
 To update the firmware of the collection of devices, select the checkboxes next to the devices you wish to update, and click on the **Apply** button to initiate Firmware update on collection.  
 To delete a URL, click the Delete  button.

To add a new firmware URL to the list, click the Add(+) button.

After you are done adding or removing devices, click the **Save** button to save the list of Firmware URLs.

- d) To schedule a firmware update task for collection, click the **Schedule** button.

### 3.10.2 Firmware Update on Device

AMPS allows you to control the power state of an individual DASH client. To control a DASH client's power state, perform the following steps:

1. Expand the **Assets and Compliance** node.
2. Expand the **Overview** node.
3. Expand the **Devices** node and click **All Systems**.
4. In the right pane, right-click the device on which you want to apply power control. The shortcut menu appears.
5. In the shortcut menu, select **DASH** and then click **Firmware Upgrade**.

The above procedure is illustrated in Figure 93.

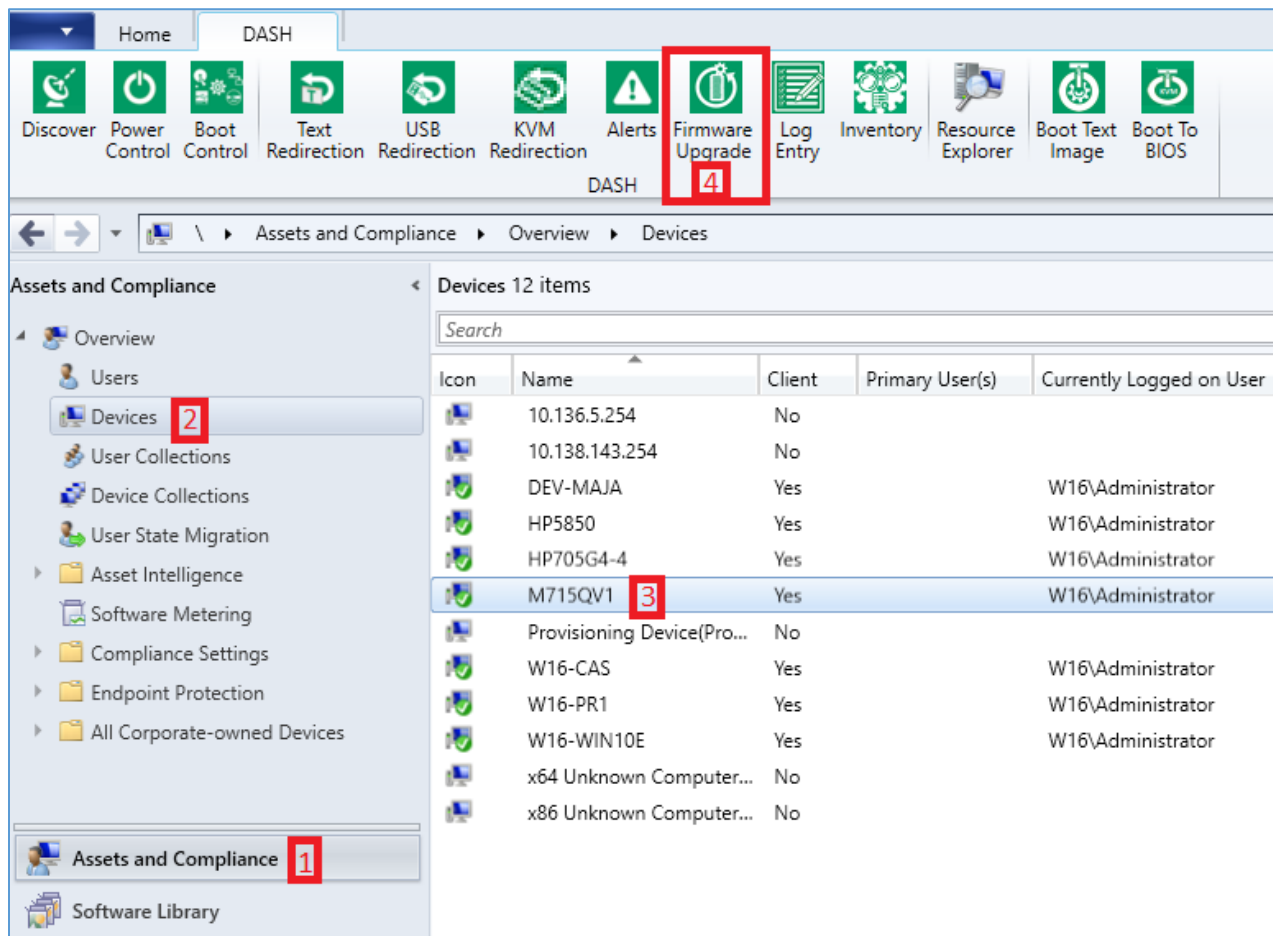
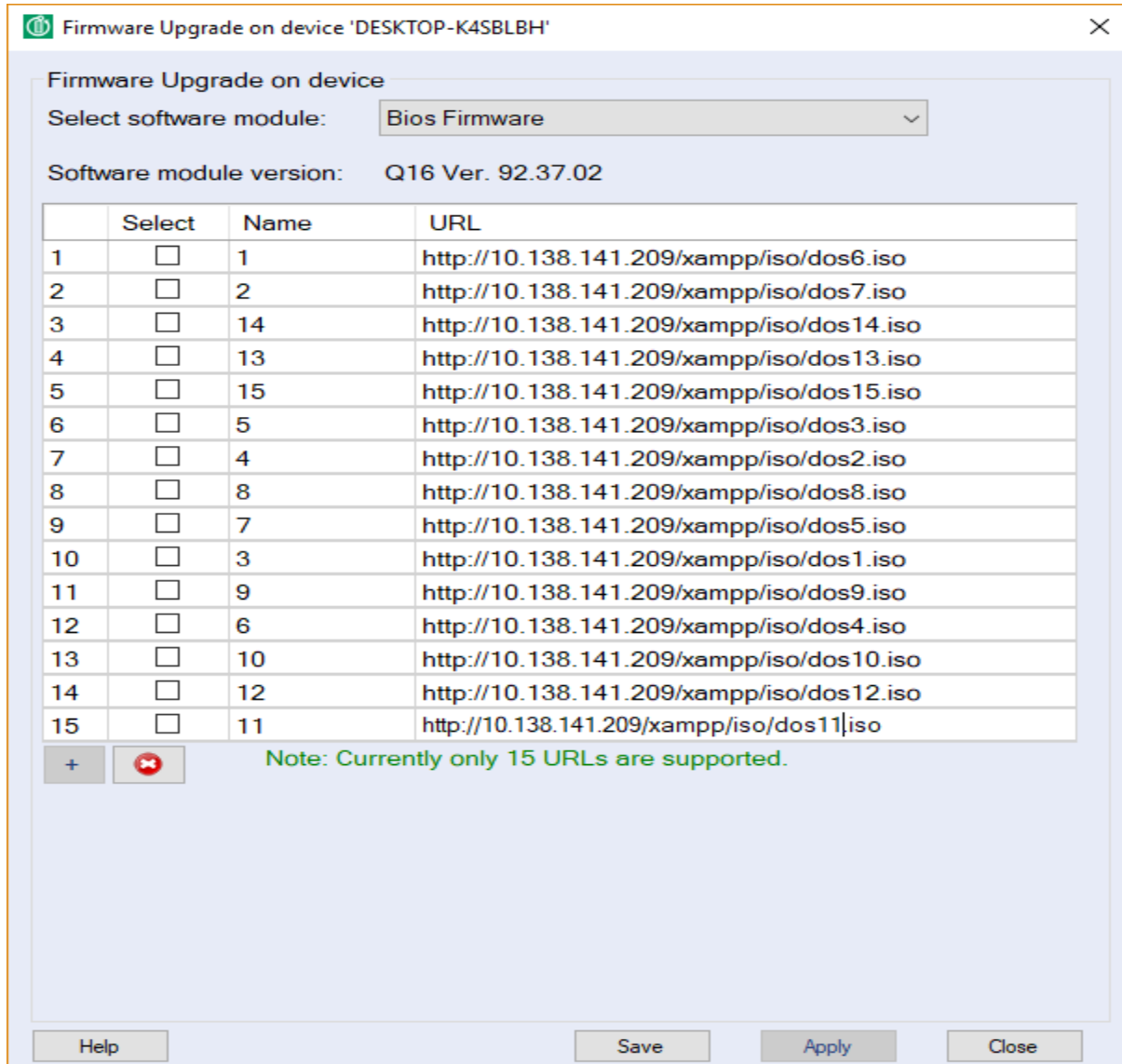


Figure 93: Firmware Update on Device

The **Firmware Update on Device** dialog box appears, as shown in Figure 94.



**Figure 94: Firmware Update on Device**

6. In the **Firmware Update on Device** dialog box,
  - a. From the **Software Module** drop-down list, select the required Software module.
  - b. 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.  
 To delete a URL, click the Delete button.  
 To add a new firmware URL to the list, click the Add(+) button.  
 After you are done adding or removing devices, click the **Save** button to save the list of Firmware URLs.

**Note:**

- Clicking **Start** button won't save the list. To save the URL list, click the **save** button.
- Up to 15 Firmware URLs can be saved in the list.

- User can delete **single** or **multiple** URLs at a time by selecting the **checkbox**.

## 3.11 Boot to BIOS (KVM Profile)

This feature allows you to get the BIOS screen when system is booting on selected devices.

### 3.11.1 Boot to BIOS on Device

AMPS allows you to control the power state of an individual DASH client. To control a DASH client's power state, perform the following steps:

1. Expand the Assets and Compliance node.
2. Expand the Overview node.
3. Expand the Devices node and click All Systems.
4. In the right pane, right-click the device on which you want to apply power control.  
The shortcut menu appears.
5. In the shortcut menu, select DASH and then click Boot to BIOS.

The above procedure is illustrated in Figure 95.

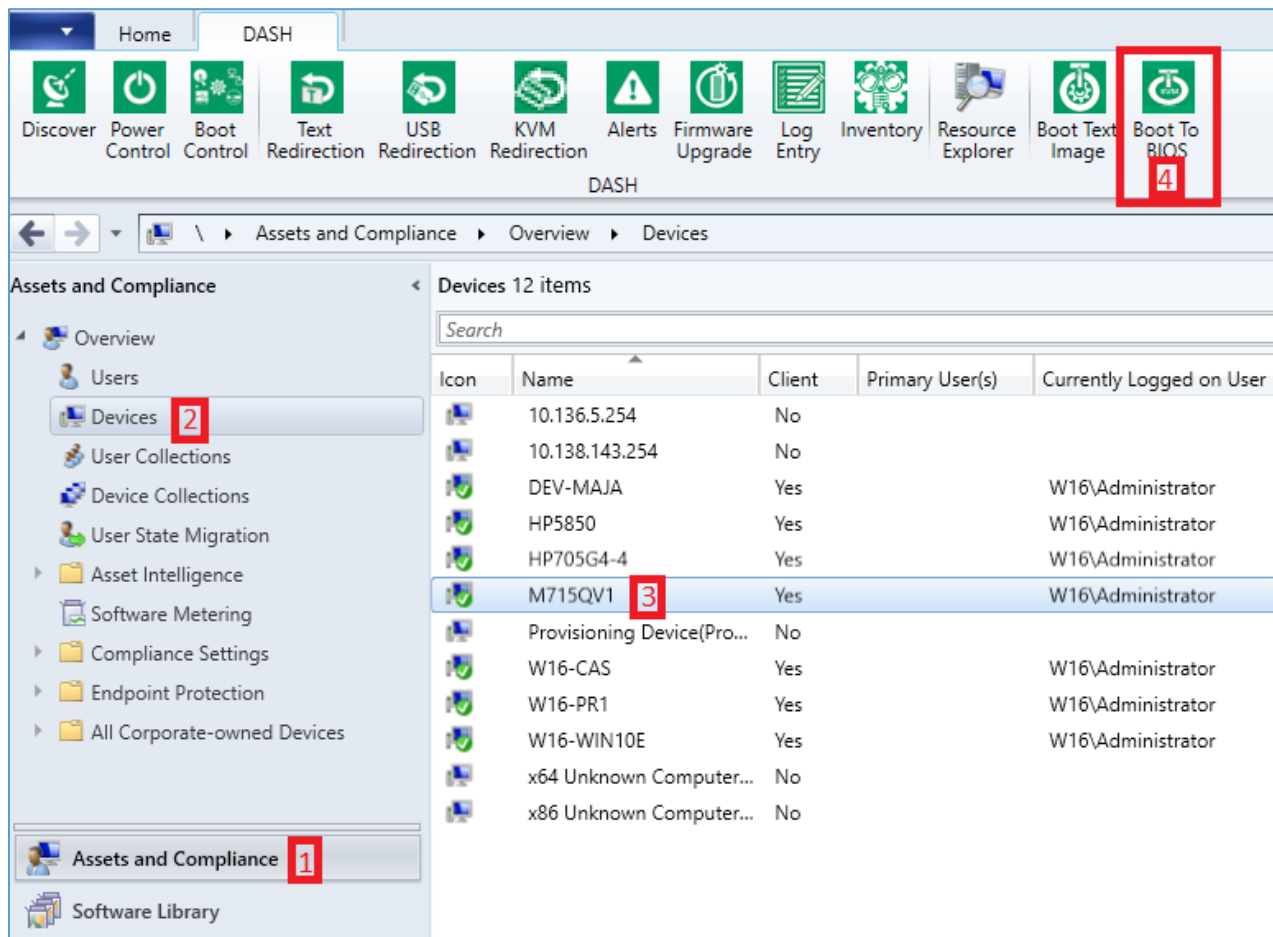


Figure 95: Boot to BIOS on Device

The **Boot to BIOS on Device** dialog box appears, as shown in Figure 96.

**KVM Redirection On Device**

Device name: BIRMAN-GPT1-CQE

KVM Redirection: VNC-RFB-AMF

KVM workflow:
 

- ☐ Boot to BIOS
- ☒ OS KVM
- ☐ WinRE

KVM SSH Key: C:\Users\Administrator\Desktop\Guru\Pro [Browse](#)

Maximum VNC sessions: 1

Protocol: VNC-RFB-AMF

Status: Disabled

**On clicking Start**

1. KVM session will be enabled on the managed system.
2. The viewer will be launched to show the managed systems OS Screen.

\* These operation may take few minutes to complete.

Buttons: Help, Start, Close

**Figure 96: Boot to BIOS**

2) In the **Boot to BIOS on Device** dialog box,

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

1. KVM enable command is sent to the managed system.
2. The managed system is rebooted.

3. After the managed system boots to BIOS setup screen and once the VNC server is ready, VNC viewer is launched.

**Note:**

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



**Figure 97: BIOS Screen in VNC Viewer**

## 3.12 KVM Redirection

This feature allows you to get the Windows screen when system is booting on selected devices.

AMPS allows you to control the power state of an individual DASH client. To control a DASH client's power state, perform the following steps:

1. Expand the Assets and Compliance node.
2. Expand the Overview node.
3. Expand the Devices node and click All Systems.

- 4. In the right pane, right-click the device on which you want to perform kvm redirection.  
The shortcut menu appears.
  - 5. In the shortcut menu, select DASH and then click KVM Redirection.
- The above procedure is illustrated in Figure 98

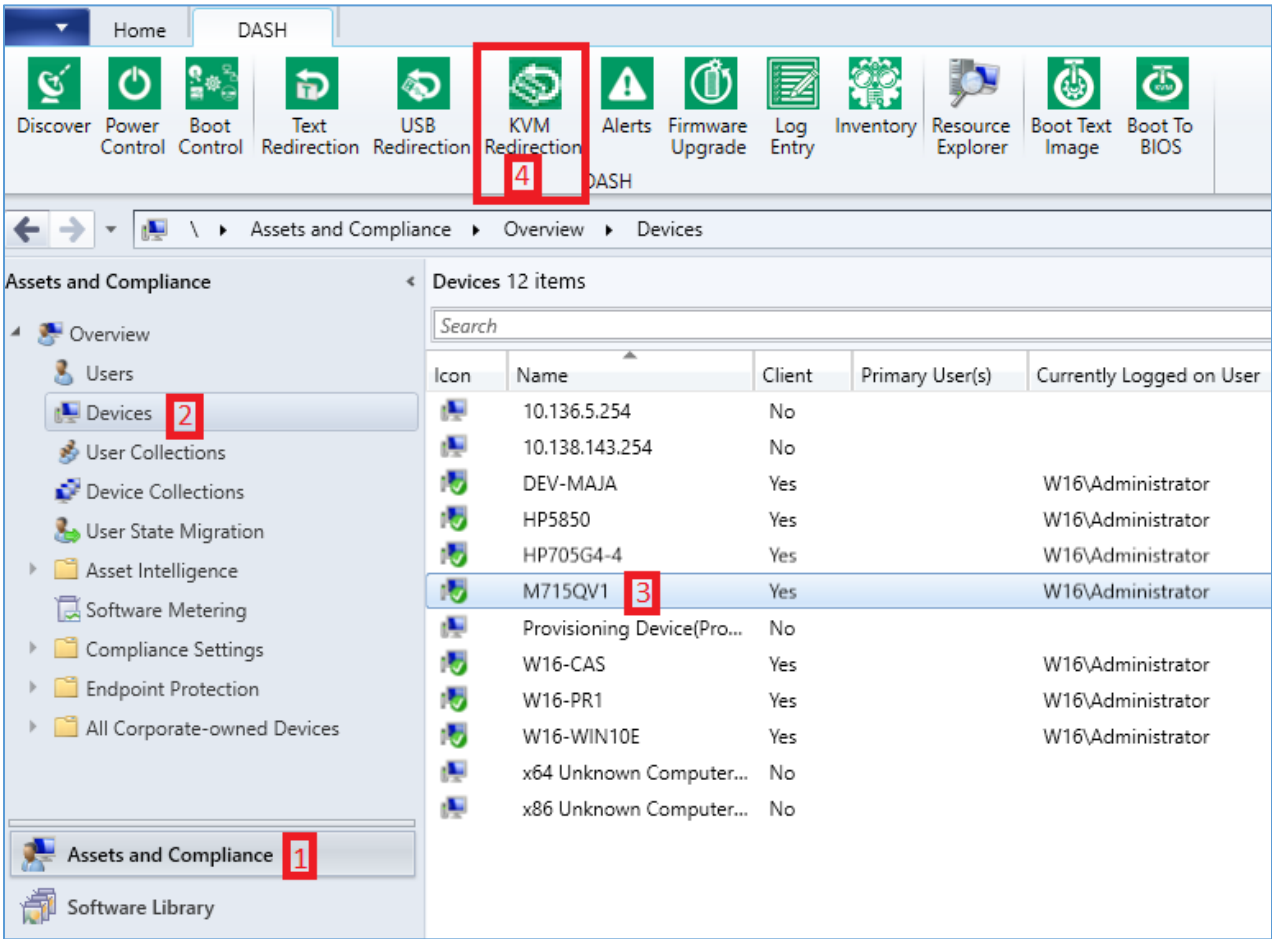
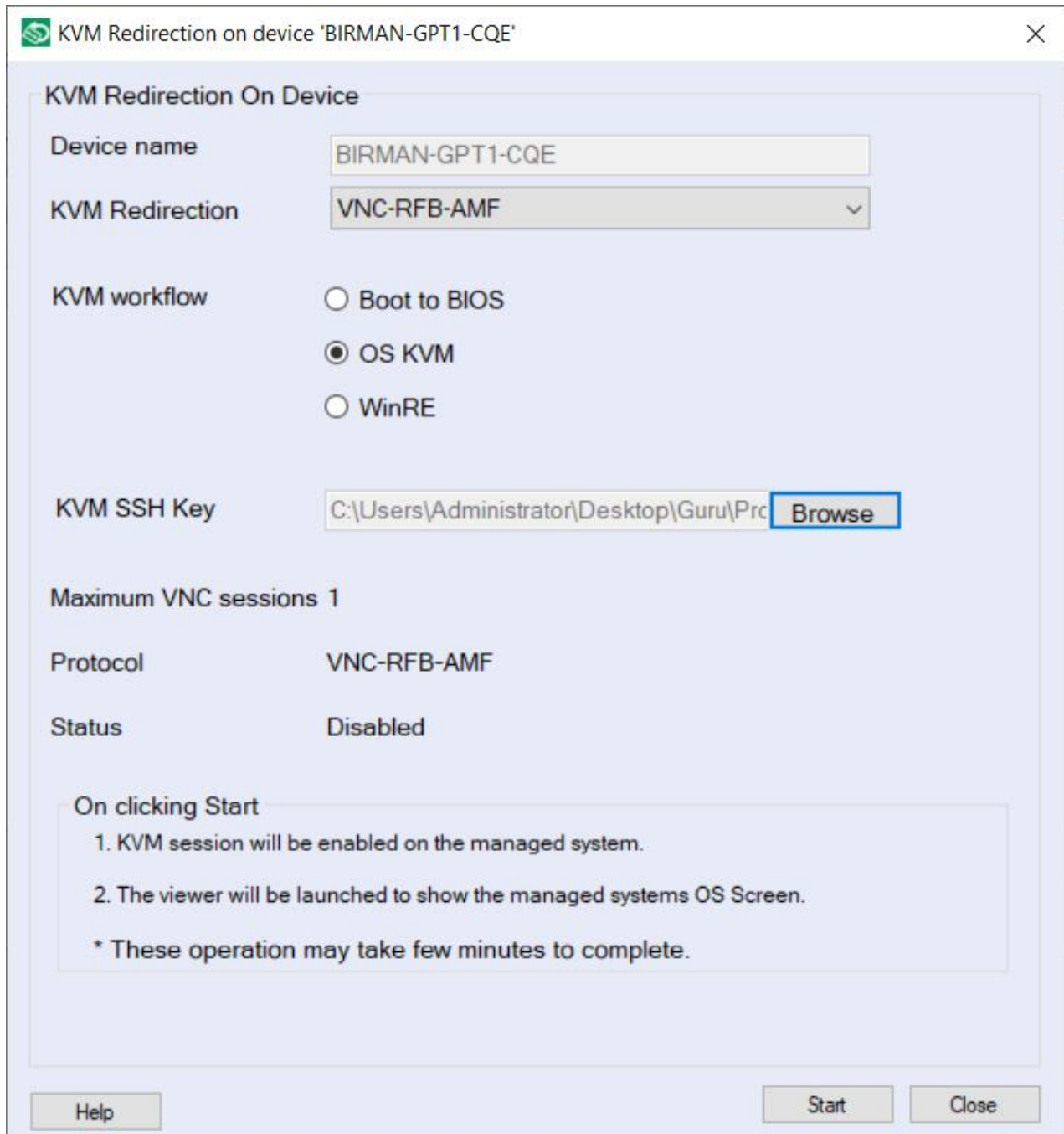


Figure 98: KVM Redirection on Device

The **KVM Redirection on Device** dialog box appears, as shown in Figure 99



**Figure 99: KVM Redirection On Device**

3) In the **KVM Redirection on Device** dialog box,

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

1. Enabling KVM on the managed system.
2. The managed system is rebooted if Boot to BIOS/WinRE is selected.
3. Once the managed system's KVM Redirection setup screen is ready, respective viewer will be launched to redirect remote systems screen in the viewer..

**Note:**




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



**Figure 100: Windows Screen in RtkDASH Viewer**

### 3.13 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 as shown in the below screenshot.

 Opaque Management Data on device 'GURUSTX'

Opaque Management Data

Element Name

Data

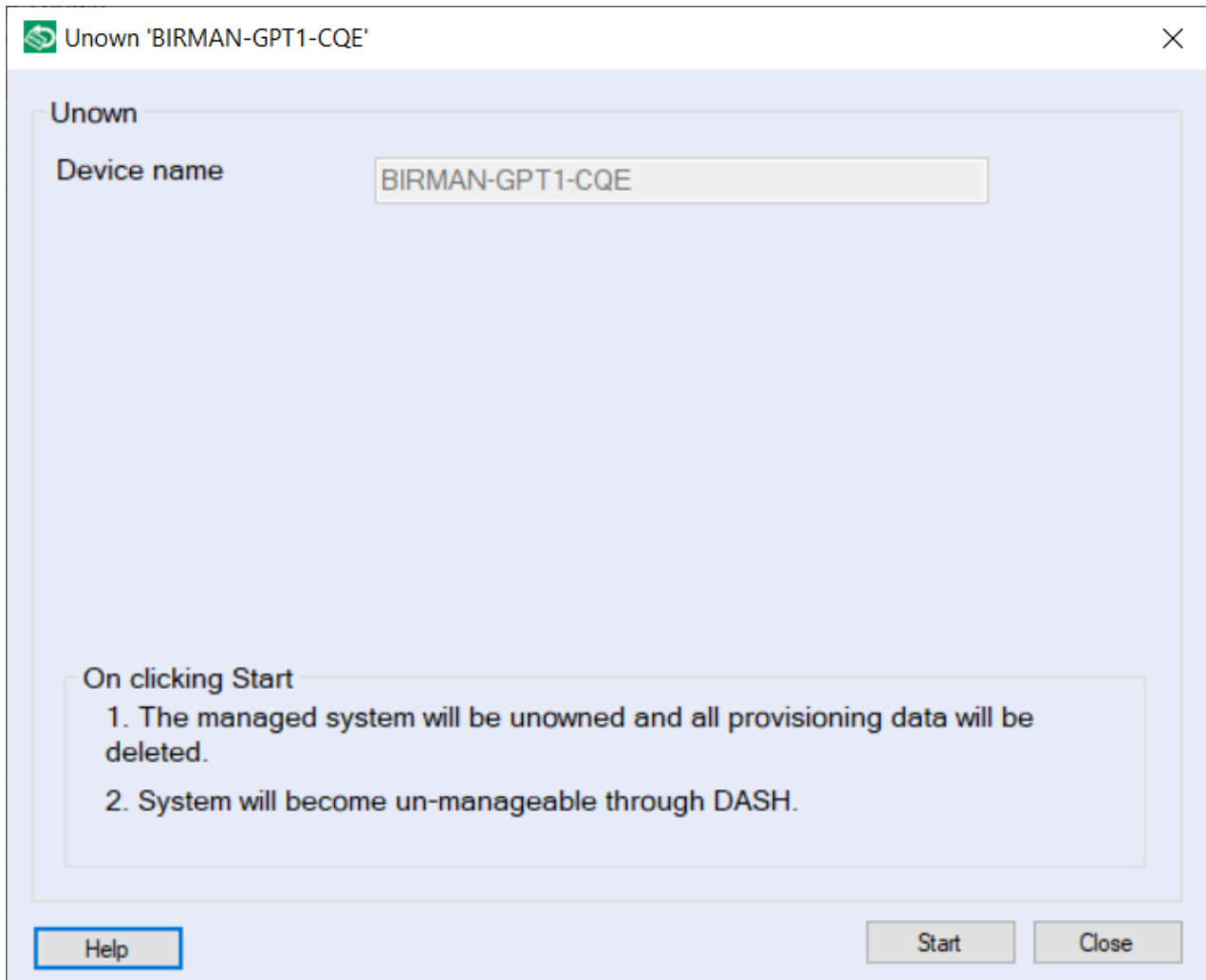
Help

Create

Delete

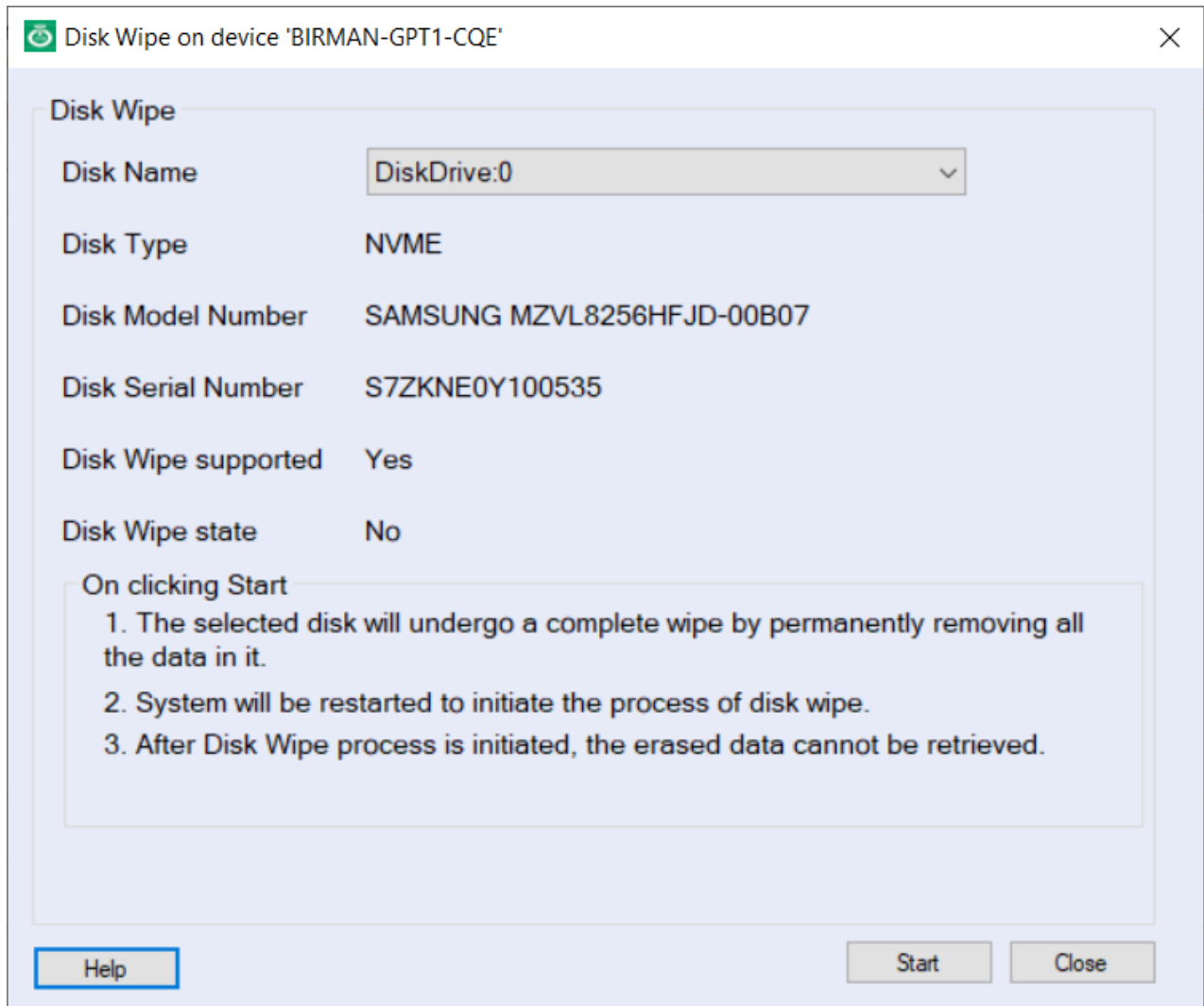
### 3.14 Unown

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



## 3.15 Disk Wipe

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



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.

## 3.16 Troubleshooting

In this section we cover how to interpret the Error messages shown from AMPS and what Remediation actions to take to fix the errors.

### 3.16.1 Troubleshooting DASH issues

Screen	Error	Remediation
Configuration	The authentication account was not found.	Check authentication accounts
	The configuration was not updated since one or more of the transport parameters is invalid.	Check HTTP input port value
	The configuration was not updated since one or more of the authentication parameters is invalid.	Check input credentials properly
	The configuration was not updated since one or more of the setting(s) is invalid.	Check input credentials properly
	The domain user name or password is incorrect.	Check Domain username and password correctly.
Power	Power task on the system failed.	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.	Supported power status not available in selected group of target machines or please check your credentials once again(ex: power OFF, power ON, Sleep, Hibernate etc.)
	No power state available.	Supported power status not available in selected target machine(ex: power OFF, power ON, Sleep, Hibernate etc.)
	Unauthorized. Verify authentication credentials or port configuration.	Please check the credentials
Boot Config	No boot configuration instances found.	Boot configuration instances are not found in selected target, please verify the target once
	Changed Boot order had failed.	Changing boot order on selected target is failed please retry again
	Default configuration failed.	Changing default configuration on selected target is failed please retry again
	Object reference not set to an instance of object	When Boot Config profile has not devices listed. The NIC vendor has not added Devices in Boot config.

	Boot config failed.	Please check the credentials
	Boot config enumeration failed.	Please check the credentials
	Boot config change boot order failed.	Error occurred while changing Boot order please retry again.
	Next configuration failed.	Changing next configuration on selected target is failed please retry again
Text Redirection	End the existing session and try again.	Please close the current Putty window.
	Verify if the system supports Text Redirection and try again.	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.	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.	Text Redirection not enabled on the selected target machine
USB Redirection	Verify if the system supports USB Redirection and try again.	Selected target not supports USB Redirection or please verify your credentials once
	No USB Redirection instance found.	USB Redirection not enabled on the selected target
	Already USB Redirected, either Modify or Disconnect.	USB Redirection already enabled in the selected target you may disconnect it or you can modify it.
	No USB Redirection instance found.	USB Redirection not enabled on the selected target
	USB Redirection failed.	Check input credentials properly and check whether target supports USB Rdirection
	USB Redirection disconnect failed.	Error occurred while disconnecting USB attached on target device please retry again.
	Length of URI specified is beyond allowed limit	Check Image URL properly and try again
	USB Redirection connect failed.	Error while attaching USB file on target . Please retry again
	Verify if URL exists.	May be Entered URL doesn't exist check again
	Text redirection failed. Verify if the system supports text redirection and try again.	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.	KVM redirection not supported by selected target or please verify your credentials once
	Supported KVM Redirection Instance not found.	KVM instance not found on the selected target please verify it once
	KVM Redirection failed.	Please check the credentials
	KVM Redirection not supported.	Check whether target supports KVM Redirection and retry again
	KVM Redirection enumeration failed.	Check whether target supports KVM Redirection and retry again
	KVM Redirection Status query failed.	Check whether target supports KVM Redirection and retry again
	KVM Redirection reboot failed.	There is an error while rebooting the target
	KVM Redirection connect failed.	There is an error while connecting to the target
	KVM Redirection timed out.	Time expired while connecting to target
	KVM Redirection request aborted.	Connection aborted by the target
	Unable to perform operation, Verify if KVM Redirection is supported by the managed system.	Please check the credentials and whether target supports KVM Redirection
	Enumeration failed for IP Interface	Check targets supports KVM Extended mode
	Unable to connect to AMC Service.	Check your AMC service once, Go to services.msc and check these <b>AMCAAlertservice, AMCDASHService, AMCWebService</b>
System Health	System Health information not found.	System health not supported on selected target or please verify your target once
Firmware Upgrade	Firmware Upgrade is not supported for this device.	Firmware upgrade not supported on selected target or please verify your credentials once
	Firmware Upgrade task failed..	Firmware upgrade failed on selected target please retry again
Log Entry	Log Entry operation failed.	Log Entry not supported on selected target or please verify your credentials once
Alerts	No Indication filters were found.	Alerts are not supported on selected target or please verify your credentials once
	Indications failed.	Please check the credentials
	Subscription of indication failed.	Operation failed on subscribing alerts please retry once again
	Unsubscription of indication failed.	Operation failed on Unsubscribing alerts please retry once again

	Subscription quota limit is reached.	Alerts subscription limit is reached.
	Enumeration of filter collections failed.	Error while getting the alerts list please try again .
	Enumeration of subscribed indications failed.	Error while getting the alerts list please try again .
	Subscribed filter list had failed.	Operation failed on subscribing alerts please retry once again
	Enumeration of subscribed indication failed	When the platform does not support any events for subscription this error can be seen.
Boot to Text	Boot To Text Power state change failed.	Please check the credentials
	Boot To Text Power task not allowed on localsystem.	Please try Boot To Text on remote system.
	Boot To Text Power Management enumeration failed.	Please check the credentials and try again.
	Boot To Text USB Instances are not found.	Check whether target supports Boot To Text and retry again
	Boot To Text URL diconnect failed.	Error while disconnecting Boot To Text on target, please try again.
	Boot To Text URL connect failed.	Error while connecting Boot To Text on target, please try again.
	Boot To Text Get instance failed.	Check credentials and try again.
	Boot To Text Boot Order change failed.	Error while changing Boot order change.
	Boot To Text Boot instances are not found.	Check credentials and try again.
	Boot To Text Boot config change boot order failed.	Error while changing Boot order change.
	Boot To Text Boot device decription string retrieval failed.	Error while changing Boot order change.
	Boot To Text Boot config change order failed.	Error while changing Boot order change.
	Boot To Text failed to perform Text Redirection	Check credentials and try again.
	Boot To Text Text Redirection Disable failed	Error while disabling Boot To Text on target please try again
	Boot To Text failed to perform Text Redirection connect operation	Error while connecting Boot To Text on target please try again
	No BootToTextImage data found in the response	Boot text image not supported on selected target or please verify your credentials once



Boot to BIOS	KVM redirection failed.	KVM Redirection failed on selected target please verify your credentials once
	System does not support KVM redirection.	Selected target doesn't supports KVM Redirection please verify your target
	Supported KVM Redirection Instance not found.	KVM Instance not found in the selected target
	KVM Redirection enumeration failed	Upon enumeration 0 instances are found. Check with NIC vendor if KVM support is added
Remote Access	Supported KVM Redirection Instance not found.	Please check target whether it supports In band KVM
	KVM Redirection enumeration failed	Upon enumeration 0 instances are found. Check with NIC vendor if KVM support is added

### 3.16.2 Troubleshooting KVM issues

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.

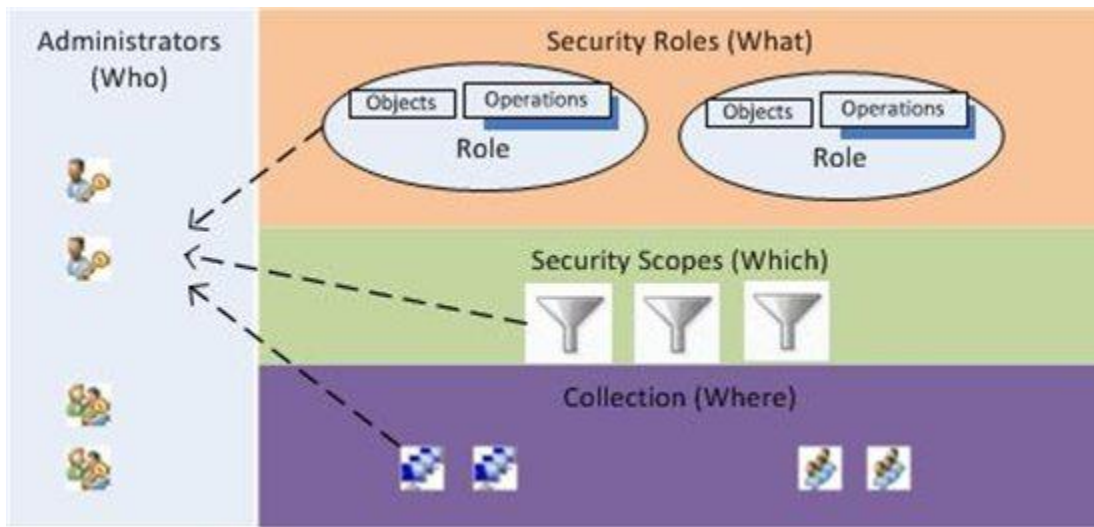
4	Error 23	Connection Key failed	This error can be seen if the platform did not successfully connect to the SSH connection with the provided key for KVM 1.9 and above. When this error occurs, SSH connection with KVM 1.8 is then attempted for KVM Redirection
5	Error 24	Not Supported	This error can be 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

## Chapter 4 Role-Based Administration

Role-Based Administration (RBA) is a Role-Based Access Control (RBAC) mechanism in Configuration Manager for restricting MEM access to authorized users.

RBA provides Configuration Manager Administrators an easy way to implement the security model that allows them to assign and manage administrative permissions. It is implemented by assigning the actions authorized users are able to perform using security roles, the users and systems they can manage through collections, and the objects they can access using security scopes.

AMPS extends the Configurations Manager's security model and defines which groups of users can perform DASH tasks, and which groups of users can modify the DASH configuration.



**Figure 101: Role Based Administration mechanism in MEM**

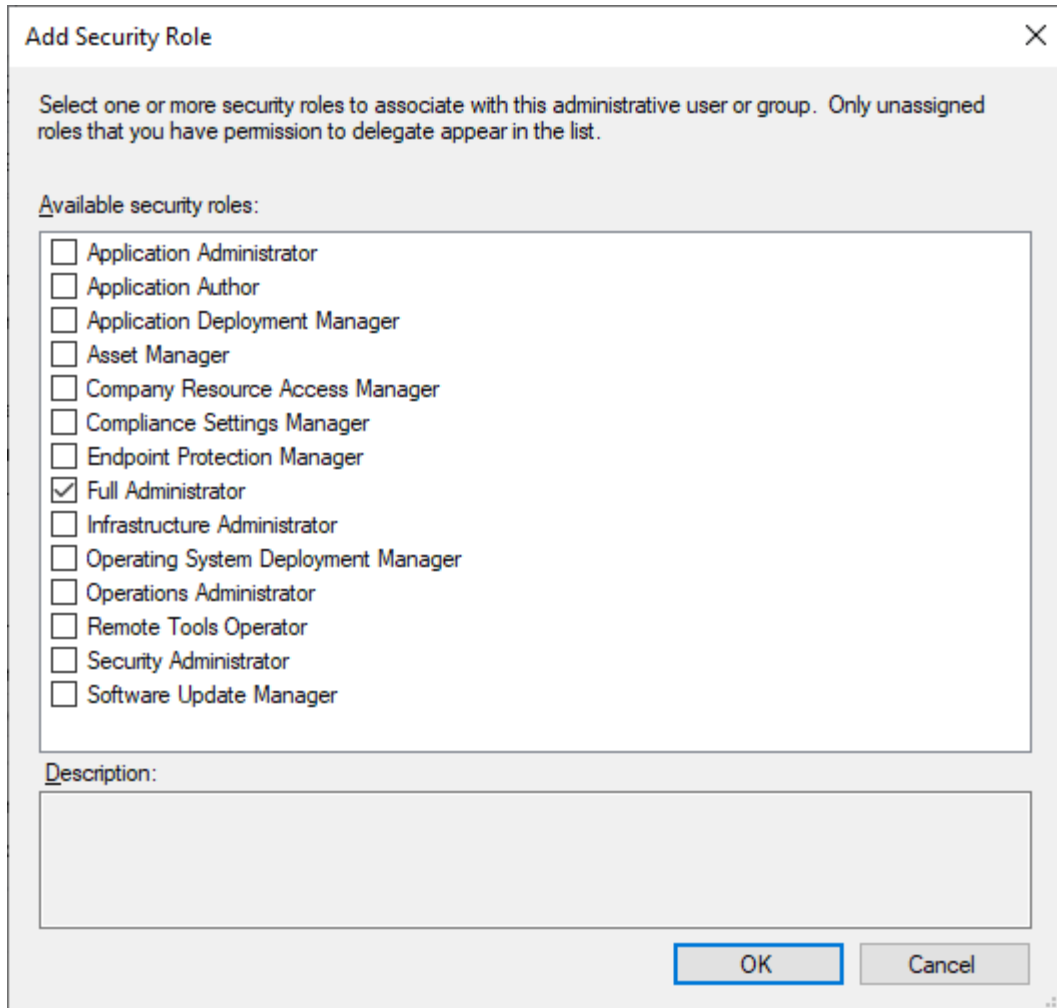
### 4.1 Security Role

Security Role defines the Configuration Manager administrative users' job functions. Configuration Manager provides several built-in roles which perform functions such as Software Update Manager for managing software updates, and Full Administrator and Remote Tools Operator for performing restrictive DASH operations.

#### 4.1.1 Full Administrator Security Role

Full Administrators possess all permissions in Configuration Manager. The administrative user who first creates a new Configuration Manager installation is associated with this security role, all scopes, and all collections. All DASH operations can be performed by users having Full Administrator role.

The screen for selecting Full Administrator security role appears as shown in Figure 102.



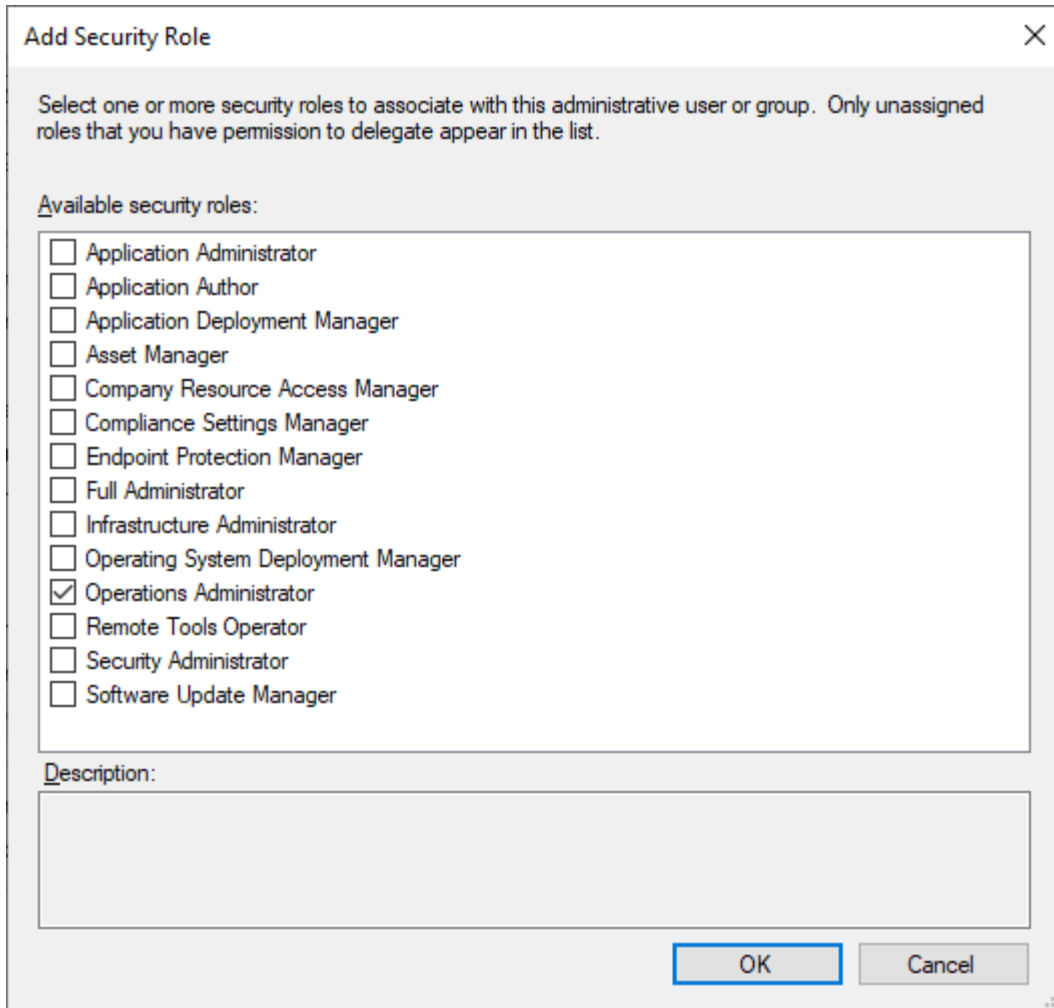
**Figure 102: Selecting Full Administrator role**

#### 4.1.2 Operations Administrator Security Role

Operations Administrator users run and audit remote administration tools that help users resolve computer issues. Administrative users associated with this role can run Remote Control, Remote Assistance and Remote Desktop from the Configuration Manager console. This user is restricted with just read-only access to DASH Configuration page.

In addition, AMPS allows Operations Administrator users to run all out of band management operations such as DASH tasks, except the DASH Configuration operation which can only be performed by the Full Administrator Role user.

The screen for selecting Operations Administrator security role appears as shown in Figure 103.



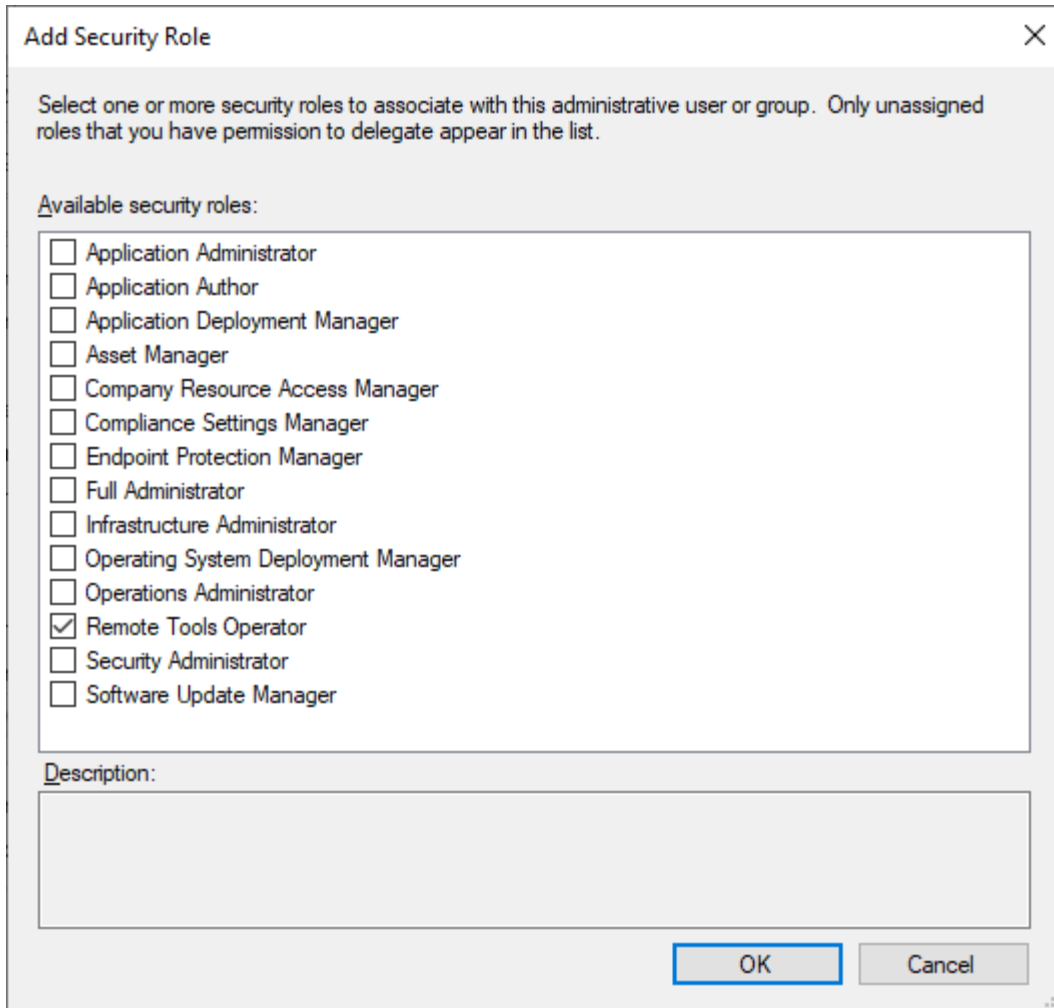
**Figure 103: Selecting Operations Administrator role**

### 4.1.3 Remote Tools Operator Security Role

Remote Tools Operator users run and audit remote administration tools that help users resolve computer issues. Administrative users associated with this role can run Remote Control, Remote Assistance and Remote Desktop from the Configuration Manager console.

In addition, AMPS allows Remote Tools Operator users to run all out of band management operations such as DASH tasks, except the DASH Configuration operation which can only be performed by the Full Administrator Role user.

The screen for selecting Remote Tools Operator security role appears as shown in Figure 104.



**Figure 104: Selecting Remote Tools Operator role**

## 4.2 Configuration in MEM for AMPS

MEM is the premier application to manage computers in large enterprises -- on the order of 100,000 systems in stand-alone configuration and much more in distributed configuration.

### 4.2.1 Overview of collections in MEM

In MEM, collections provide a way to manage users, computers, and other resources in the organization. Collections give a means of organizing the computers and a mechanism to distribute software packages to clients and users. MEM derives its power from its ability to target applications at client systems with very specific properties by using query-based collections. Query-based collections allow an administrator to provide any criteria that the MEM database holds about its systems and automatically make those systems a member of that collection.

For example, a new version of an OS-specific graphics driver can be deployed across the enterprise (spanning multiple geographies) by creating OS-specific collections created by querying the OS of all

systems to find user systems running Windows 10, Windows 11, or server system running Windows 2016, Windows 2019, Windows 2022.

Similarly, an application can be deployed at only one site (say, a city) by grouping all the systems at that site in a collection (based on a query such as IP subnet).

In summary, collections are logical grouping of computers created based on a unique property (or a unique set of properties). The collections thus created can be used for multiple purposes, such as monitoring, deploying applications, and so forth. Administrators can enforce very strict authorization on these collections and limit:

- who can access these collections, and
- what they access in these collections.

For instance, the enterprise administrator (at the head office) can create a remote office-specific collection and give monitoring rights to that remote office administrator while keeping application deployment rights at the head office. The enterprise administrator can deny any kind of access to that remote office for rest of the administrators in the enterprise.

#### 4.2.2 Overview of collection object's security in MEM

MEM enforces security, defined on the collections, when a client of that collection is accessed through the MEM Administrator Console. The same security model is enforced when that client is accessed programmatically via any MEM Windows Management Instrumentation (WMI) provider. MEM compares the user who is attempting to access the collection to the MEM security permissions on that collection and determines if the user has the security right to access or change the objects. The MEM enforces this security every time a client is accessed through the MEM Administrator Console or through a program that access MEM through WMI (such as wbemtest application).

Permission can be granted on a collection to a single user or to a group of users within a domain. For example, all members of the Domain Users Group can be permitted to manage a collection, or a specific set of users can be permitted to edit and manage the collections. For a given collection, any defined permissions can be granted. The rich set of permissions gives great control in defining who can access MEM clients and who can access settings in the MEM site database.

Security for a MEM collection can be configured at either the class level or at the instance level:

- **Class level** - This level grants users-permissions for all object types in a specific class -- for example, Collections.
- **Instance level** - This level grants permissions for a specific instance of an object type, such as the "All Windows 10 Systems" collection or a "New York City Systems" collection.

In both cases, permissions can be granted or denied on a per-user or user-group basis.

Collection class and collection instances are depicted for Users in Figure 105 and for Devices in Figure 106.

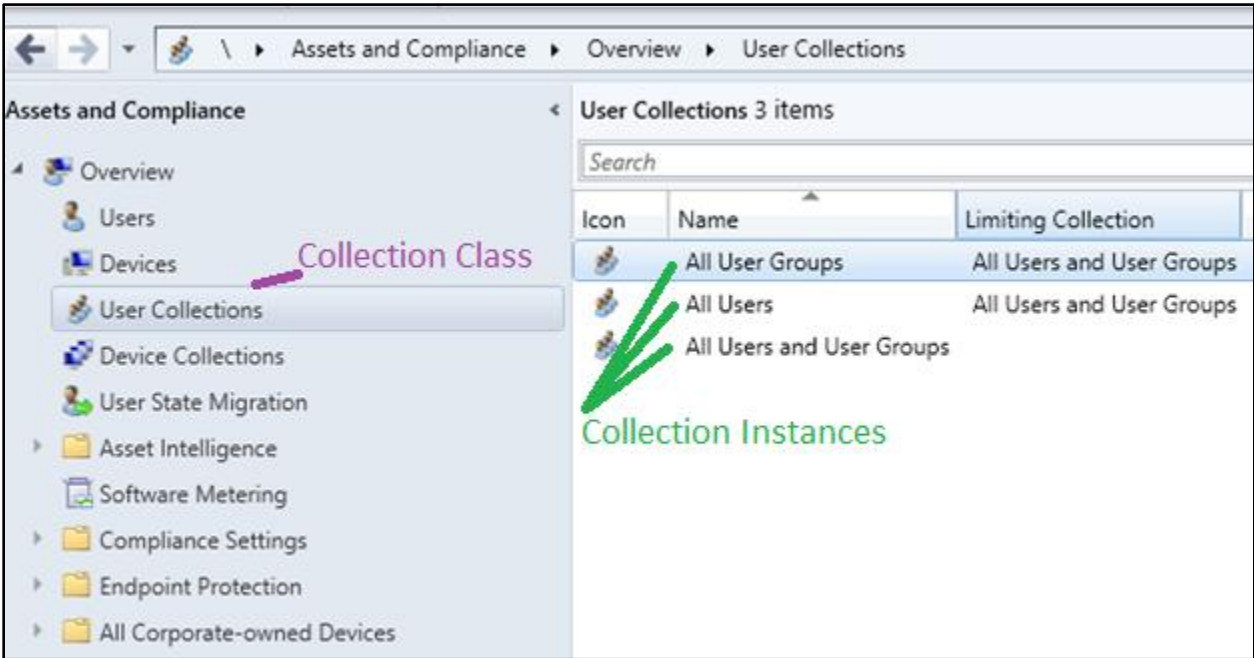


Figure 105: User Collection

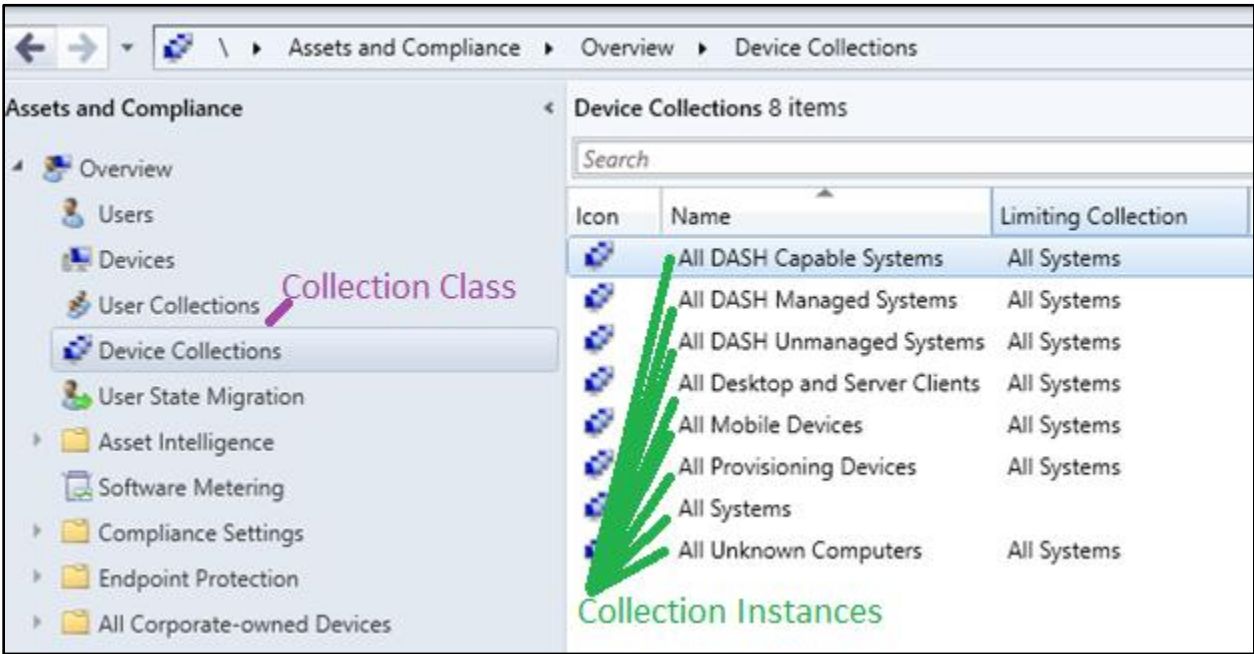


Figure 106: Device Collection

4.2.3 MEM collection security rights

Commonly used security rights of a collection object can be seen in Table 1.

Table 1: Table with mapping between Rights and Abilities

Right	Grants the ability to
-------	-----------------------



Administer	Assign or remove any user security rights for a collection class to oneself or to any other user. You must explicitly grant other security rights appropriate to the object type. Granting the Administer right to a user does not automatically give the user Create, Modify, or Delete rights for that object type.
Create	Create an instance of collection.
Delete	Delete a collection or a sub-collection.
Delete Resource	Delete a client from a collection.
Modify	Modify an instance of an object type.
Read	View an instance and its properties.

#### 4.2.4 Security rights defined for DASH tasks

Some of the DASH tasks are:

- Change power state
- Modify boot order
- Subscribe and unsubscribe to event alerts
- Perform KVM, USB or text redirection
- Perform hardware inventory

##### 4.2.4.1 Collection class/instance

The security roles, "Full Administrator", "Operations Administrator" and "Remote Tools Operator" can perform DASH tasks on Collection class or Collection class instances.

##### 4.2.4.2 Read operations

View or read the status of a client in a collection by performing a DASH operation. Some of the tasks that require this security right are:

- View hardware inventory
- Check power status
- Retrieve boot order

##### 4.2.4.3 Modify operations

Change setting or perform "Modify" DASH operation such as change power state, modify boot order, and subscribe to alerts. Redirection activities such as KVM, Text and USB require this security right.

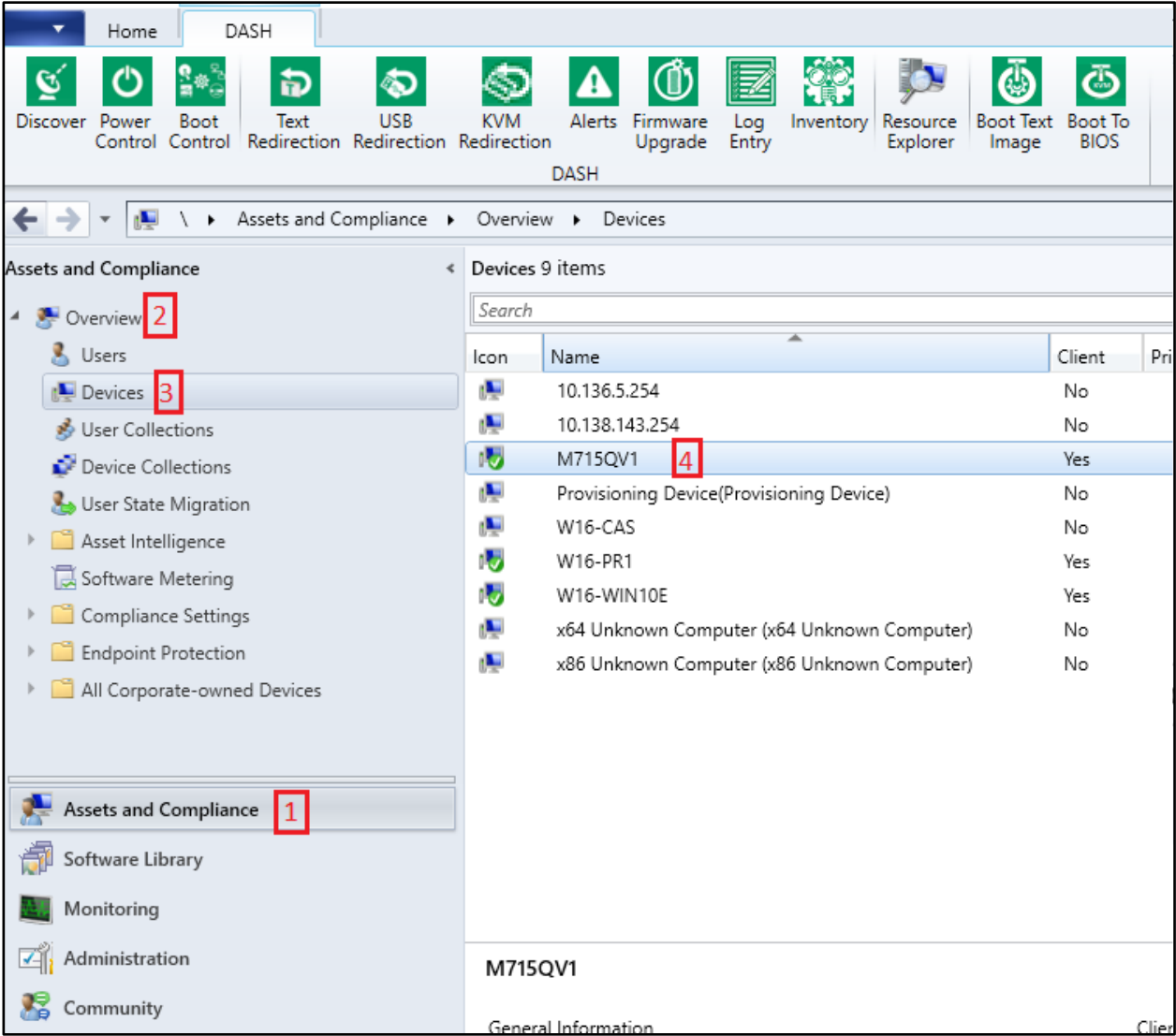
#### 4.2.5 Security rights for DASH operations

A mapping between DASH Tasks, what rights are required for the DASH tasks and what abilities they grant can be seen in Table 2

**Table 2: Security rights required for DASH tasks**

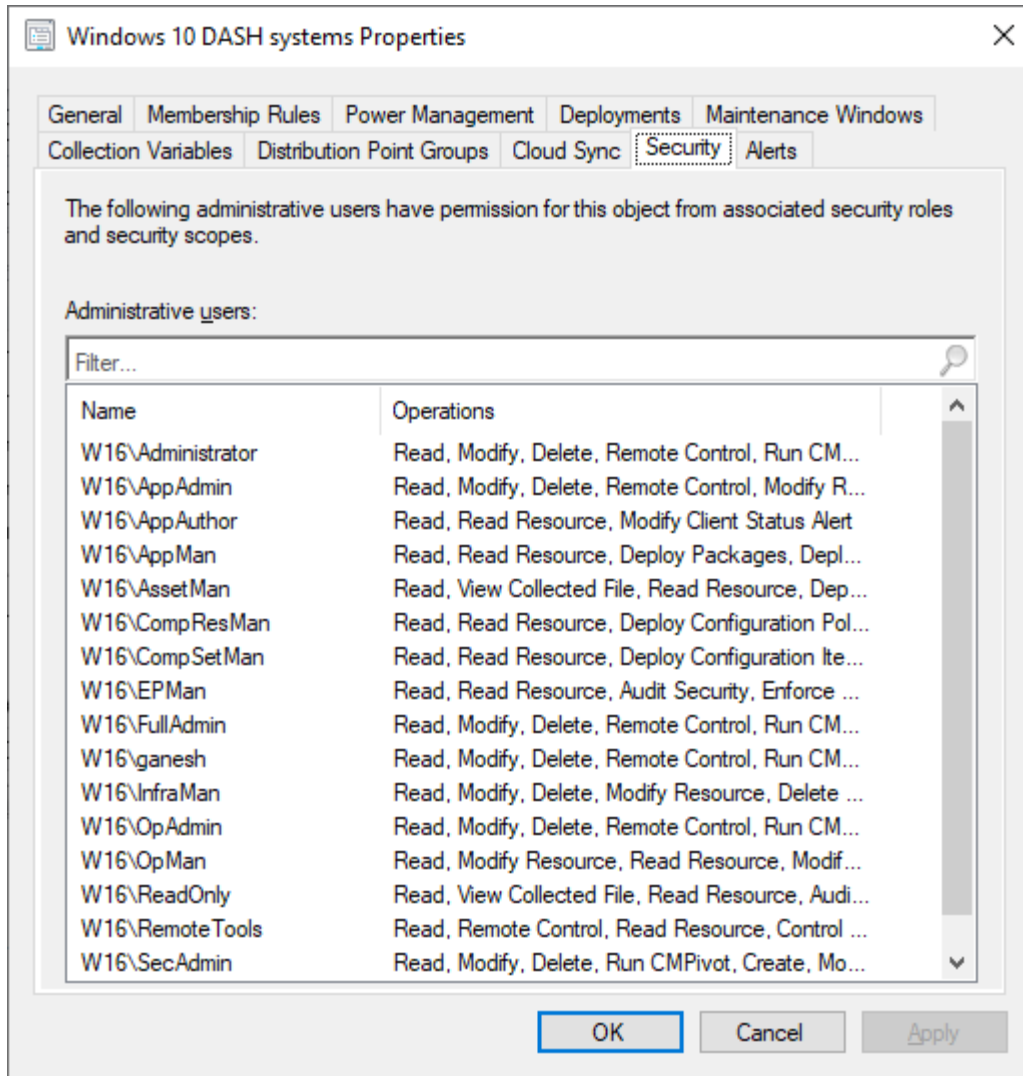
<b>DASH Task</b>	<b>Right</b>	<b>Grants the ability to</b>
Discover	Create, Modify, and Read Resource	Identify whether a system is DASH-capable or not. Get version information and the profiles supported.
Power	Read Resource	Obtain current power state of the system.
	Use Remote Tools	Change power state of the system.
Boot	Read Resource	Obtain boot order information.
	Use Remote Tools	Change boot order of the system.
Inventory	Read Resource	Obtain hardware inventory of the system.
KVM, USB and Text Redirection	Read Resource and Use Remote Tools	Redirect BIOS screen, boot to remote ISO image.
Alerts/Events	Read Resource and Use Remote Tools	Subscribe and unsubscribe to all or selected event alerting.
Account Management	Read Resource	View list of digest accounts on DASH-capable system.
	Use Remote Tools	Modify the digest account on DASH-capable system.
Firmware Upgrade	Read Resource	View list of firmware Images
	Use Remote Tools	Add\Modify the list of firmware images
Log Entry	Read Resource	Obtain hardware inventory of the system.
Boot to Text Image Workflow	Read Resource	View list of remote ISO images
	Use Remote Tools	Flash Image then Redirect to Text BIOS
Boot to BIOS Workflow	Read Resource	View list of KVM Redirection Instances to boot to BIOS
	Use Remote Tools	Reboot the System and Redirect BIOS screen

To view DASH tasks on a DASH enabled system, navigate to **\Assets and Compliance\Overview\Devices** and click on Properties and depicted in Figure 107.



**Figure 107: Security rights for DASH operation**

The User collection that can access a device collection can be viewed by navigating to \Assets and Compliance\Overview\Device Collections. Upon right clicking on an instance like “Windows 10 DASH systems” and selecting properties, the user collections with security permissions to access the collection can be viewed as shown in Figure 108.



**Figure 108: Security permissions for different roles for a collection.**

#### 4.2.6 Security rights defined for DASH settings

The security rights model applies for modifying DASH settings in the “DASH Configuration” window in the MEM Administrator Console.

A few of the DASH settings that can be changed in the “DASH Configuration” window are:

- Manage inventory schedules
- Modify digest and active directory authentication
- Modify HTTP/HTTPS settings
- Change DASH port numbers
- Enable/Disable DASH Auto Discovery and DASH wakeup

The security rights allows Read or Modify on Site class or Site class instance control the user’s permission for DASH settings.

#### 4.2.6.1 Read

The Read security right allows the user to open the “DASH Configuration” window and view the settings. The user cannot save the settings. A user with “Full Administrator” or “Operations Administrator” role can read the settings.

#### 4.2.6.2 Modify

The user can open the “DASH Configuration” windows and modify and save the settings.

Note: Only users with “Full Administrator” rights can modify and save the DASH Configuration window.

Navigate to \Administration\Overview\Site Configuration\Sites as per Figure 109 to check this setting.

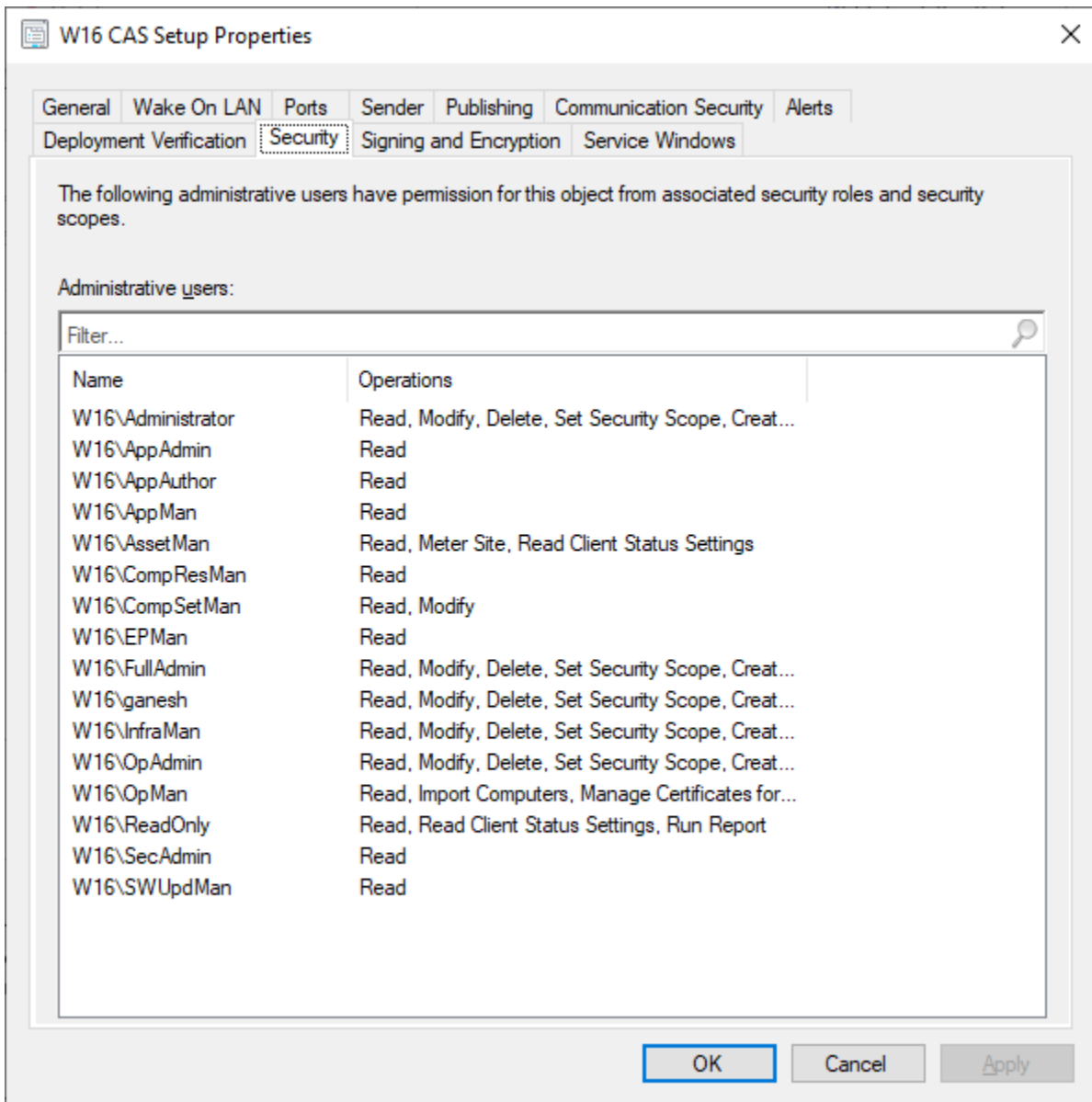


Figure 109: Security rights user collection and access mapping

## 4.2.7 Configuration of AMPS

In AMPS, the administrator has the option to either enable or disable the user permission checking feature. This is a global setting and affects all users.

Note: To change the setting, the user must have “Full Administrator” access.

### 4.2.7.1 Steps

1. In the MEM console, navigate to **\Administration\Overview\DASH Management\DASH Configuration**. Go to DASH Configuration then click on Properties as per Figure 110.
2. Users can choose to save up to 3 Schemes and save both Digest and Active Directory settings
3. Users can also set the “DASH Wakeup” / “DASH Auto Discovery” options.
4. When HTTPS Scheme is selected users also have the option to ignore self-signed certificate or configure a valid HTTPS certificate for connection.

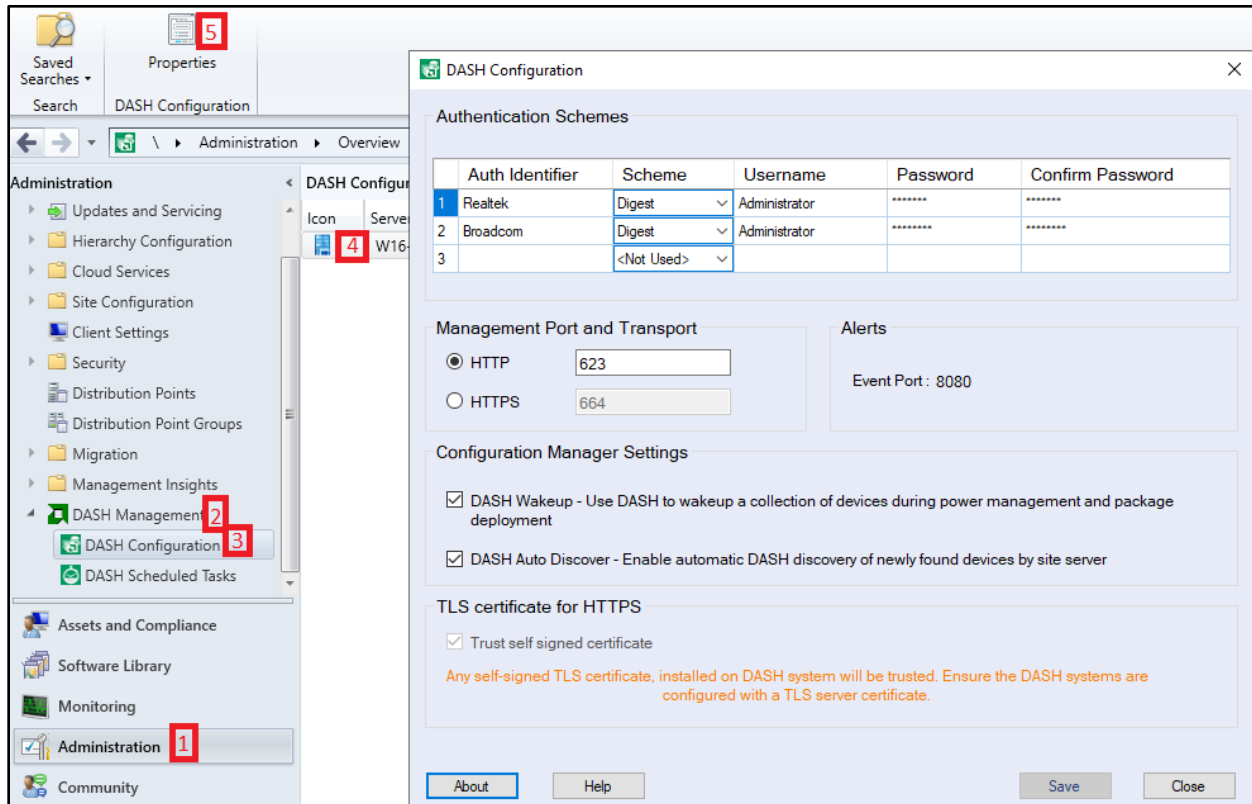


Figure 110: Opening the DASH Configuration window.

## 4.2.8 Security Scope

Security scopes limit administrative users' access to specific secured objects. While security roles grant the class level permission to the user such as “Read Applications”, security scopes grant instance level

permission for *which* applications they can read. Refer Configuration Manager documentation for more information. Security scopes are not considered for either DASH tasks or DASH configuration changes.

#### 4.2.8.1 Collection

A Collection is the group of devices or users the administrative user can manage. For performing DASH tasks, the Remote Tool Operator role users must have access to the collection. Users with Full Administrator role have access to all collections.

### 4.3 Case Study

Here, a typical IT deployment case is considered for illustration.

#### 4.3.1 Business scenario

XYZ Corp is a large call center with 1,000 seats. It has around 100 office staff supporting the call center business, and there are roughly 20 top executives across all functions. The company has 25 IT personnel to administer all the desktops, and few servers in the facility. All the desktops are DASH-compliant.

XYZ Corp wants to define the IT personnel who will administer call center, office, and executive desktops. A set of only three IT Admins are identified who must have access to executive systems. A dedicated set of 15 IT personnel will administer only call center desktops because call center desktops must have minimal down time. The remaining IT personnel administer office and call center desktops.

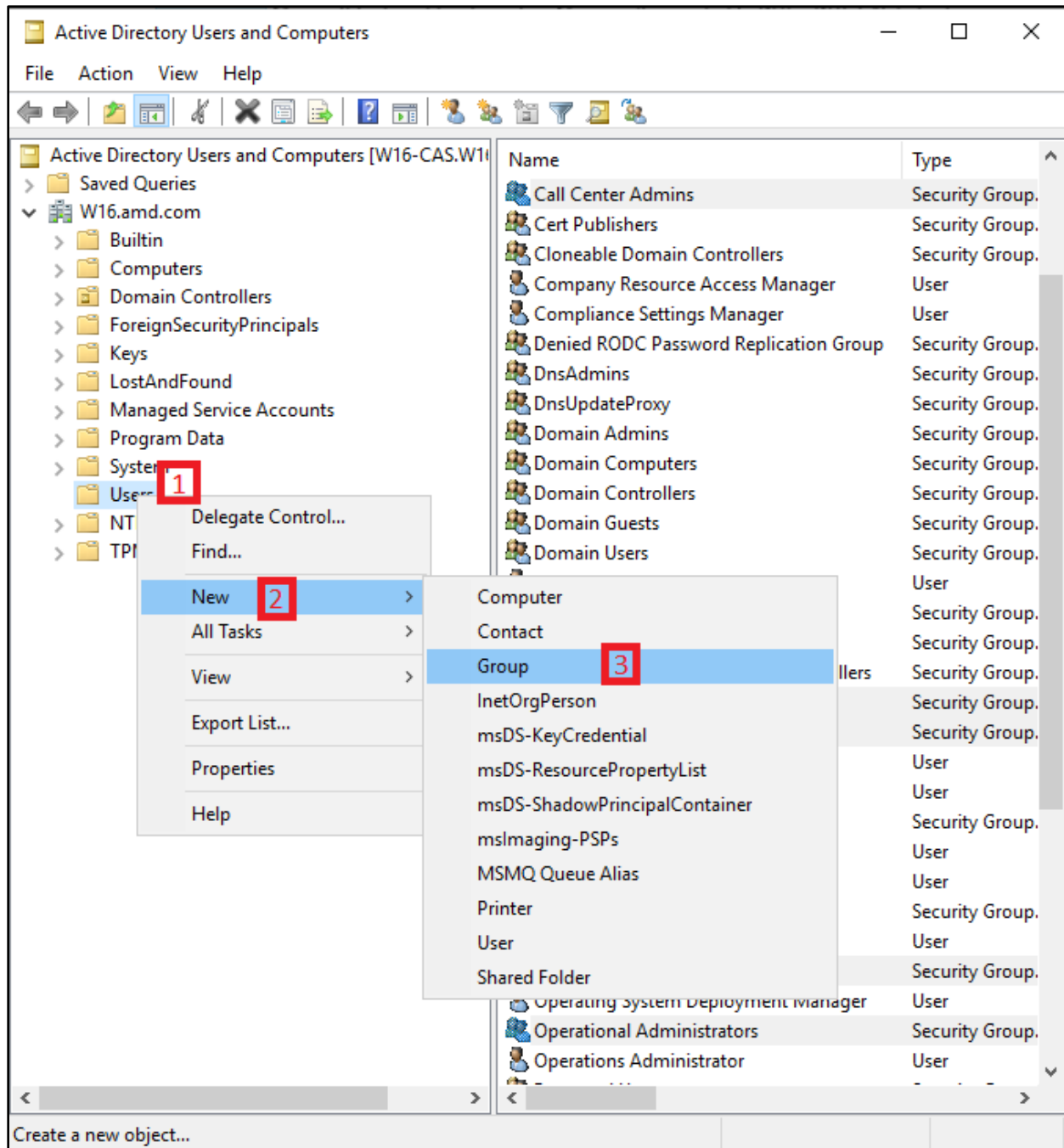
Additionally, XYZ Corp must have its desktops audited periodically by an external regulator. The auditor must have only Read access to hardware information of the desktops.

XYZ Corp wants only three IT Admins who manage executive systems to have permission to change DASH settings. The rest of the IT Admins can have view-only access. The external auditor need not have any access to any of the DASH settings.

#### 4.3.2 Solution Description

- I. Create groups in Active Directory

Open Active Directory Users and Computers under Windows Administrative tools and then right click on Users, select New and then select Group as per Figure 111.

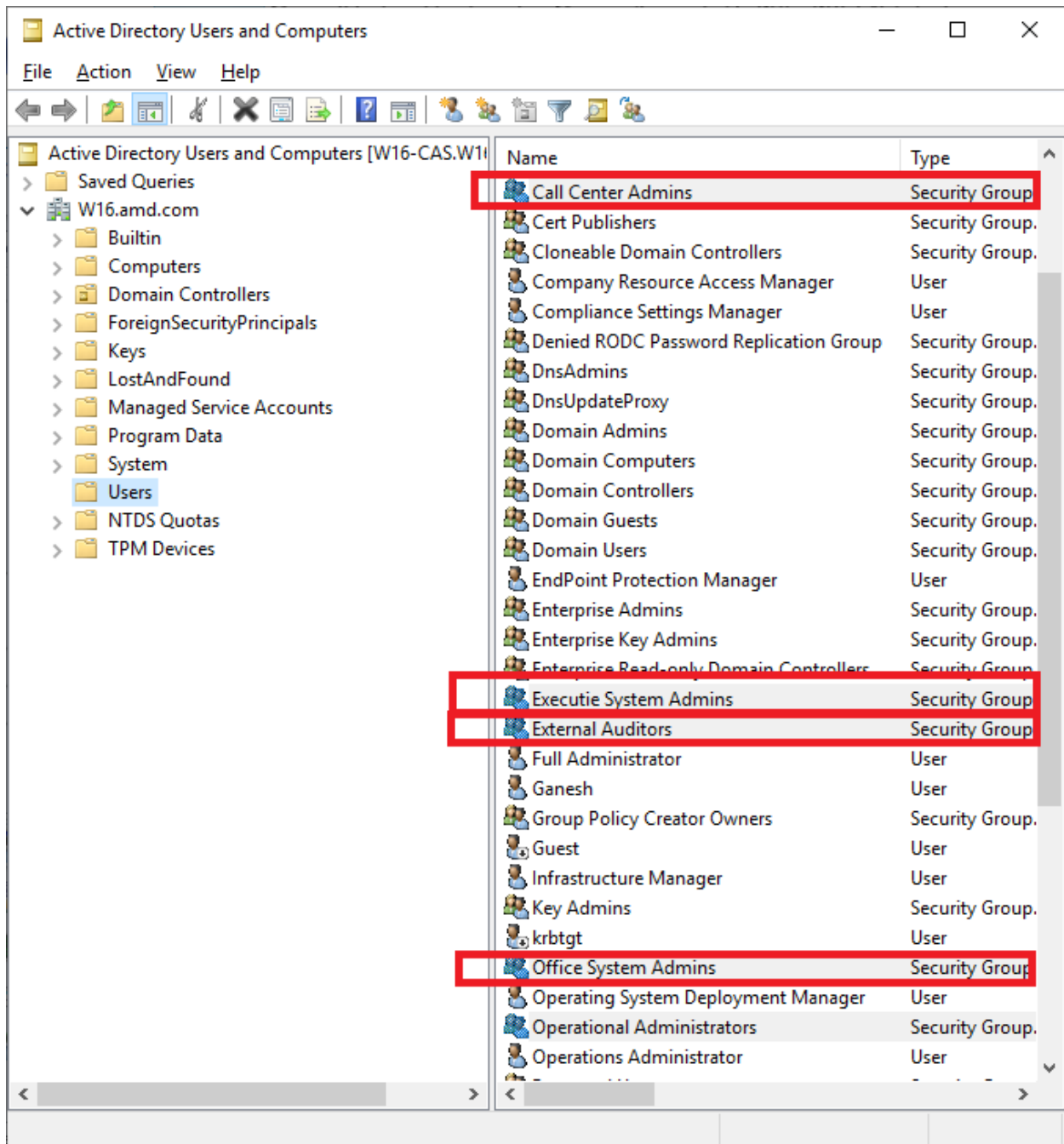


**Figure 111: Creating user group in “Active Directory Users and Computers” Application**

XYZ Corp could create four groups in Active Directory and assign the respective IT personnel into their authorized groups as per Figure 112:

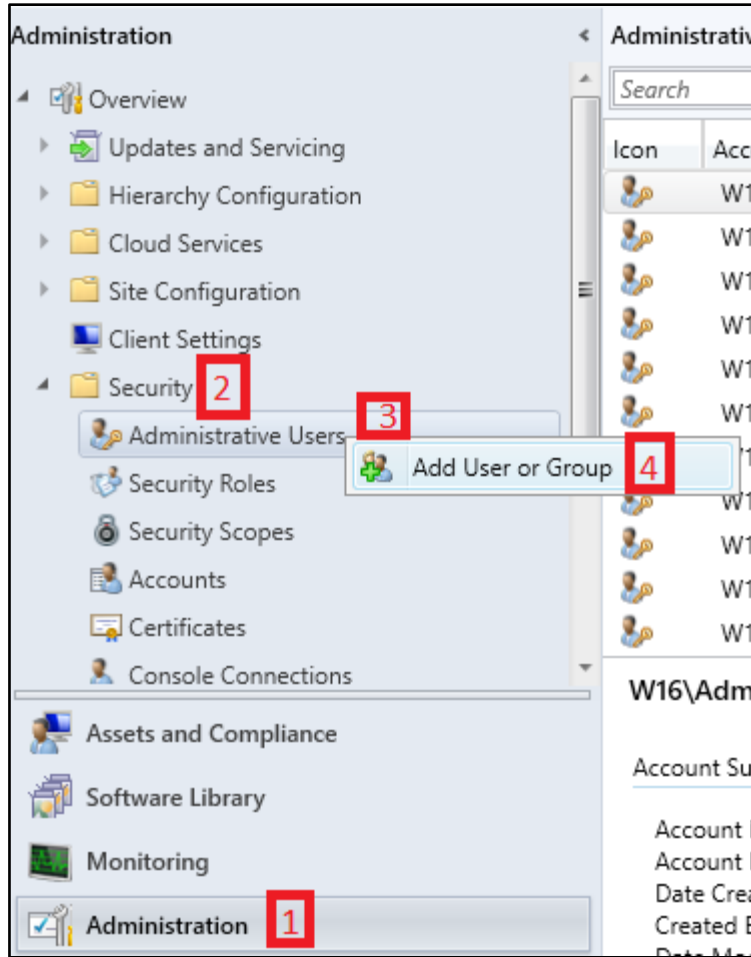
- Call Center Admins
- Office System Admins
- Executive System Admins
- External Auditors





**Figure 112: Adding Users in “Active Directory Users and Computers” application**

In the MEM console, navigate to **\Administration\Overview\Security\Administrative Users**. Right click on “Administrative Users” and choose “Add User or Group” as per Figure 113.



**Figure 113: Adding Users to Administrative Users**

Using this utility, add the four active directory domains groups as four MEM Users as per Figure 114 and Figure 115 . Do not assign any security right for any of these four MEM users.

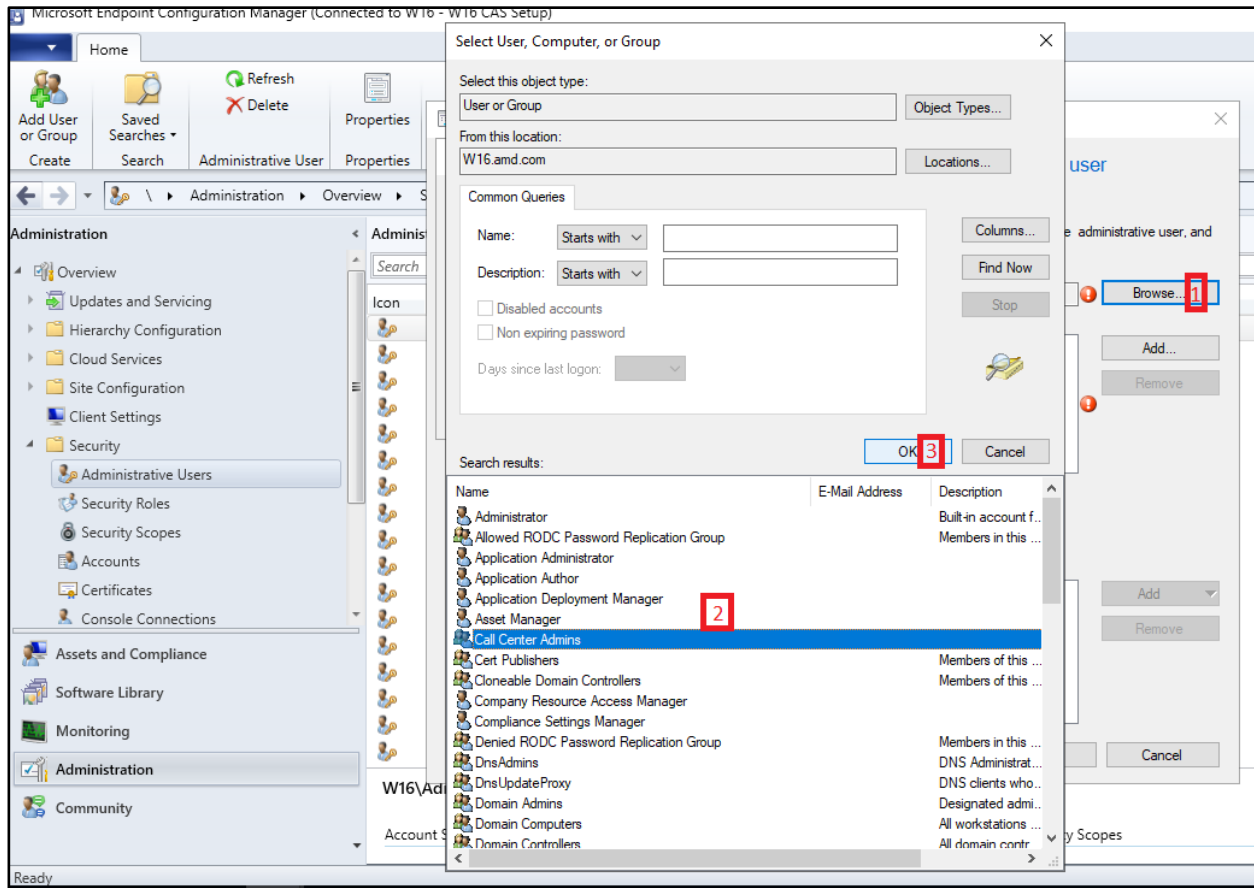


Figure 114: Adding "Call Center Admins" to "Administrative Users"

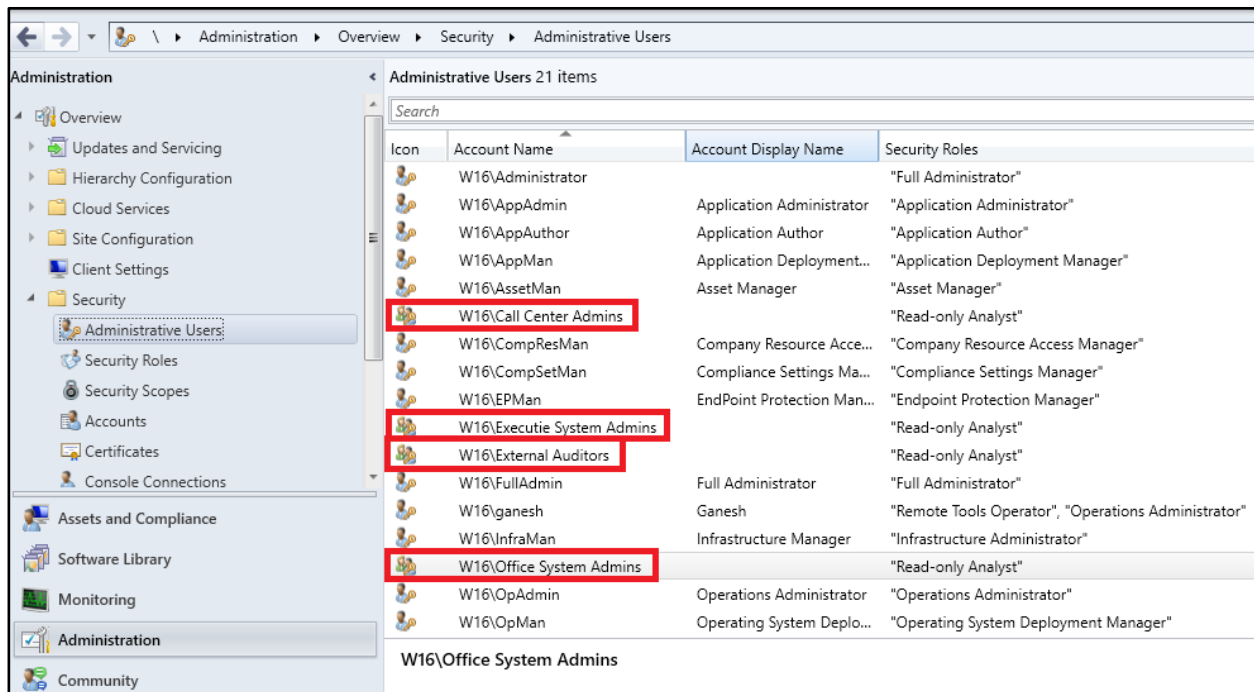


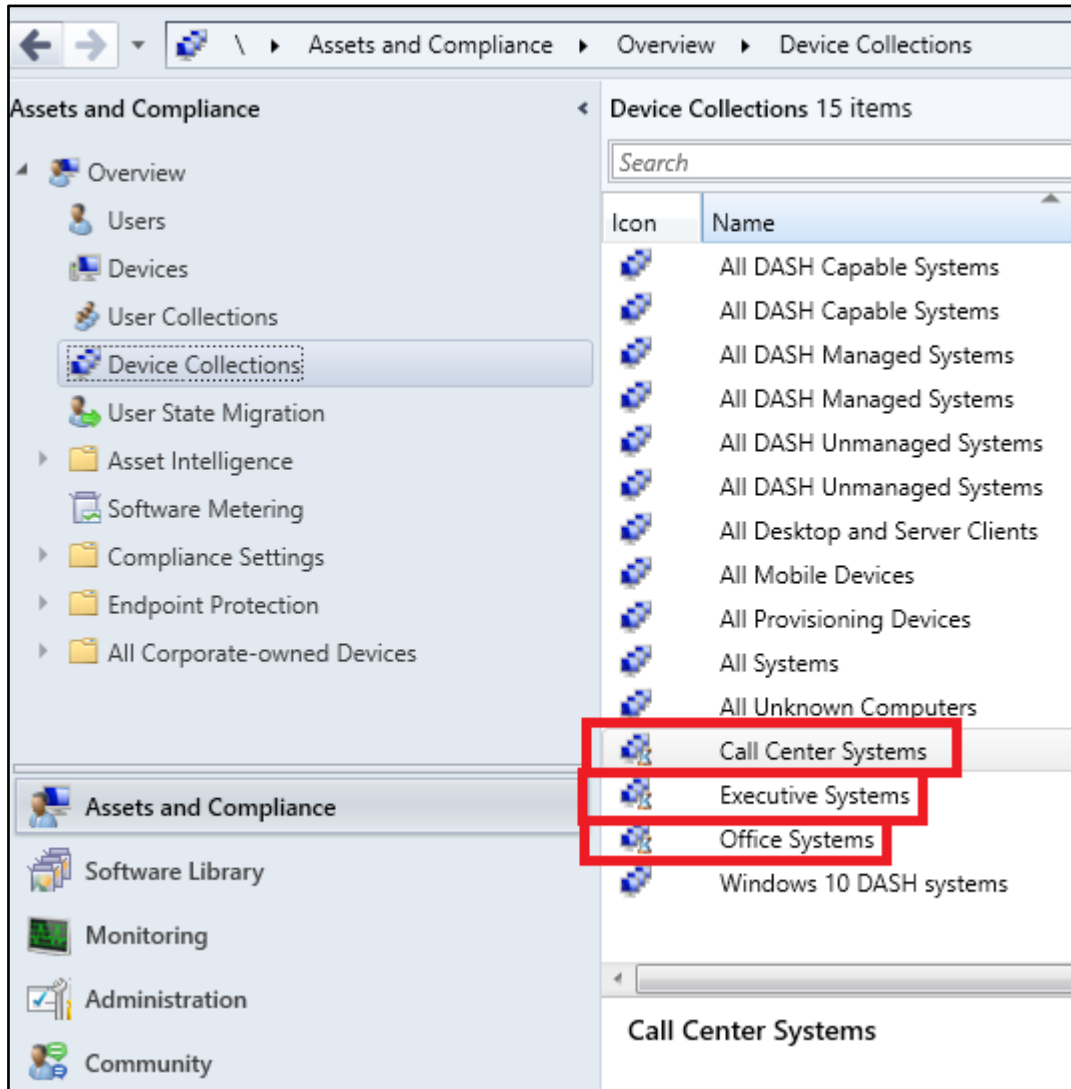
Figure 115: Creating 4 user collections in "Administrative Users"

## II. Create Collections in MEM

In MEM, three top-level collections are created to hold the three categories of desktops:

- Call Center Systems
- Office Systems
- Executive Systems

Define a collection membership rule so Call Center Systems collections has only call center desktops, and so forth for the other two collections as per Figure 116.



**Figure 116: Creating "Device Collection" for Device Management**

## III. Assign security rights for the collections

Right-click on a Call Center Systems collection node, click Properties, and in the Properties window, click the Security tab. In the Instance security, provide "Read-only Analyst" and "Remote Tools Operator" security rights for the Call Center Admins MEM User as per Figure 117, Figure 118 and Figure 119.

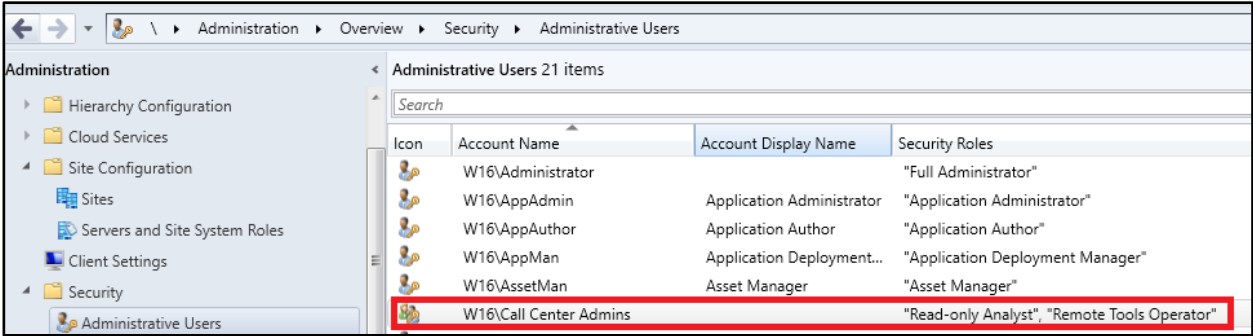


Figure 117: Adding Roles to Call Center Admins

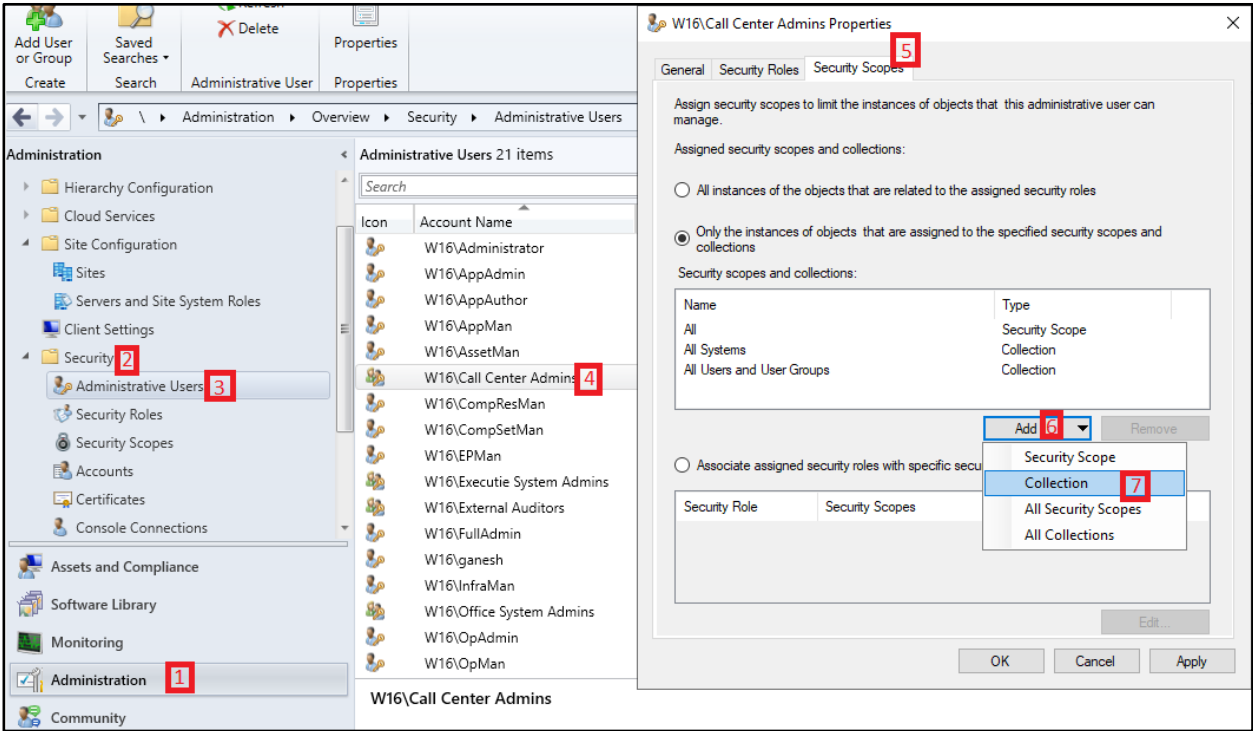
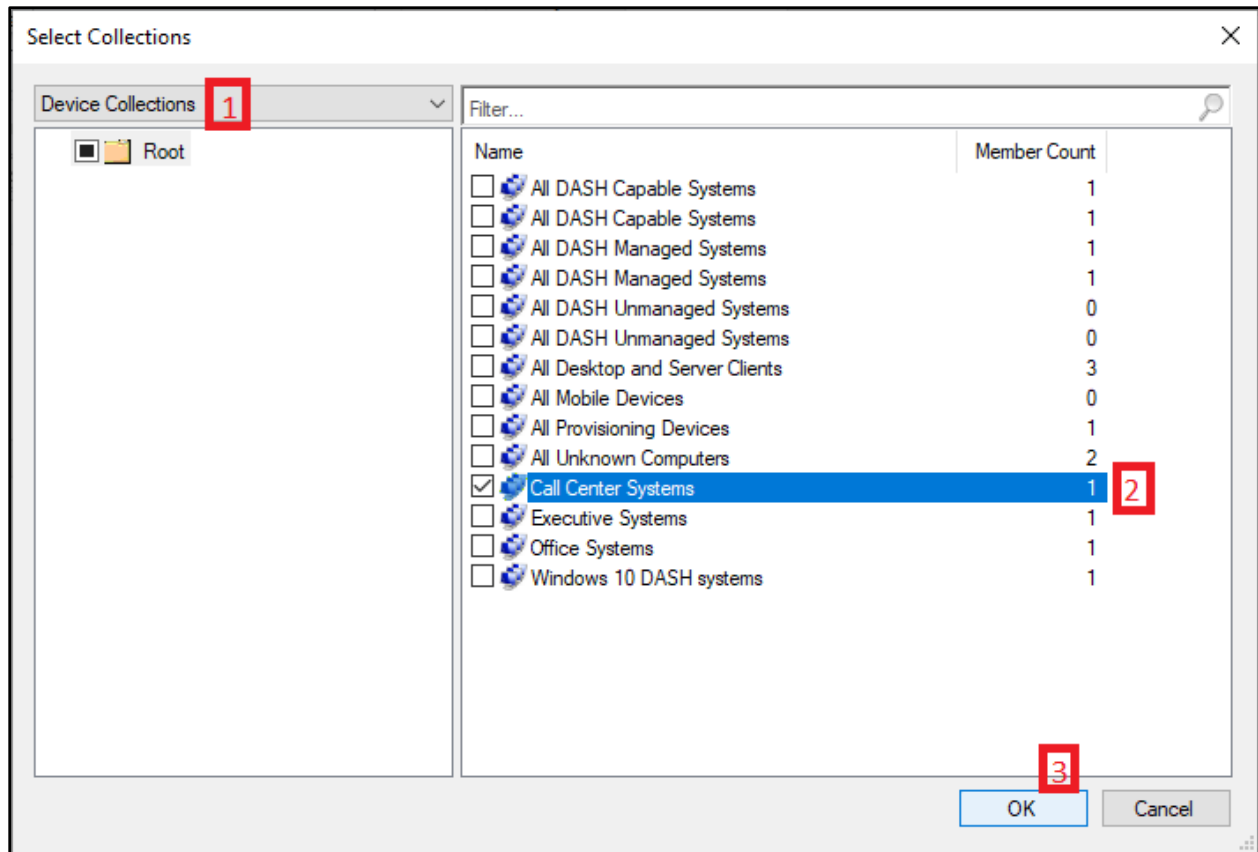


Figure 118: Assigning Call Center Device Collection to Call Center Administrator Users

- Similarly, provide "Read-only Analyst" and "Remote Tools Operator" security rights to:
- Office System Admins on the collections Office Systems and Call Center Systems.
  - Executive Admins on the collections Executive Systems, Office Systems, and Call Center Systems.



**Figure 119: Choose the Call Center Systems from Device Collections**

Apart from the assigned users, ensure none of the other MEM users have “Read-only Analyst” and “Remote Tools Operator” on these collections.

Provide only Read Resource security right to MEM user External Auditors on all three collections. This will ensure the external auditor can perform inventory queries on all systems but cannot change or modify the system or state.

When IT Admins open the MEM Administrator Console, they will have access only to those desktops for which they are authorized.

#### IV. Assign security rights for the DASH settings

Navigate to **\Administration\Overview\Security\Administrative Users**. Right-click on Site Server and click Properties. In the Properties window, click the Security tab. In the Instance security, provide

1. Modify right to Executive System Admins.
2. Read right to Call Center Admins and Office System Admins.
3. For the External Auditors user, do not provide any security right.

The external auditor can use the DASH Explorer utility of the AMPS to view hardware inventory information on any client in the MEM Administrator Console.

## V. Summary of assigned security rights

Check Figure 120 and Table 3 for a summary of how Security roles are assigned to Administrative users so that operations can be performed on the selected device collection.

**Table 3: Admin, access and security rights mapping**

IT Admin Group	Collection Access	Security Rights
Executive System Admins	Executive Systems, Office Systems, and Call Center Systems	Read Resource and Use Remote Tools
Office System Admins	Office Systems and Call Center Systems	Read Resource and Use Remote Tools
Call Center Admins	Call Center Systems	Read Resource and Use Remote Tools
External Auditor	Executive Systems, Office Systems, and Call Center Systems	Read Resource

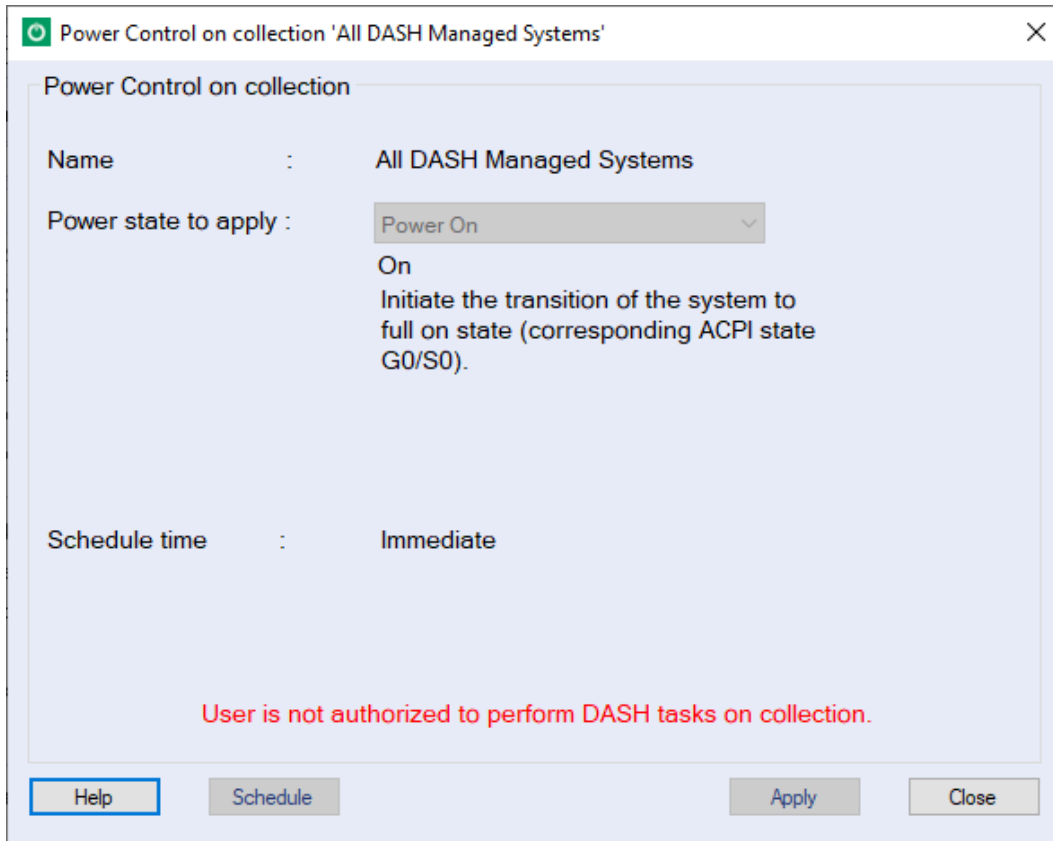
Icon	Account Name	Security Roles	Collections
	W16\Administrator	"Full Administrator"	"All Systems", "All Users and User Groups"
	W16\AppAdmin	"Application Administrator"	"All Systems", "All Users and User Groups"
	W16\AppAuthor	"Application Author"	"All Systems", "All Users and User Groups"
	W16\AppMan	"Application Deployment Manager"	"All Systems", "All Users and User Groups"
	W16\AssetMan	"Asset Manager"	"All Systems", "All Users and User Groups"
	W16\Call Center Admins	"Read-only Analyst", "Remote Tools Operator"	"All Systems", "All Users and User Groups", "Call Center Systems"
	W16\CompResMan	"Company Resource Access Manager"	"All Systems", "All Users and User Groups"
	W16\CompSetMan	"Compliance Settings Manager"	"All Systems", "All Users and User Groups"
	W16\EPMan	"Endpoint Protection Manager"	"All Systems", "All Users and User Groups"
	W16\Executive System Admins	"Read-only Analyst", "Remote Tools Operator"	"All Systems", "All Users and User Groups", "Call Center Systems", "Office Systems", "Executive Systems"
	W16\External Auditors	"Read-only Analyst"	"All Systems", "All Users and User Groups", "Call Center Systems", "Office Systems", "Executive Systems"
	W16\FullAdmin	"Full Administrator"	"All Systems", "All Users and User Groups"
	W16\ganesh	"Remote Tools Operator", "Operations Administrator"	"All Systems", "All Users and User Groups"
	W16\InfraMan	"Infrastructure Administrator"	"All Systems", "All Users and User Groups"
	W16\Office System Admins	"Read-only Analyst", "Remote Tools Operator"	"All Systems", "All Users and User Groups", "Call Center Systems", "Office Systems"
	W16\OpAdmin	"Operations Administrator"	"All Systems", "All Users and User Groups"

**Figure 120: Summary of 4 Accounts and Collection mapping and security Roles assigned**

Note: After making the necessary settings, ensure Admins not authorized for a collection do not have access; for example, ensure Call Center Admins don't have access to Executive Systems. In case the Call Center Admins have access to the Executive Systems collection, then the settings must be reviewed and implemented again.

## 4.4 Error Messages

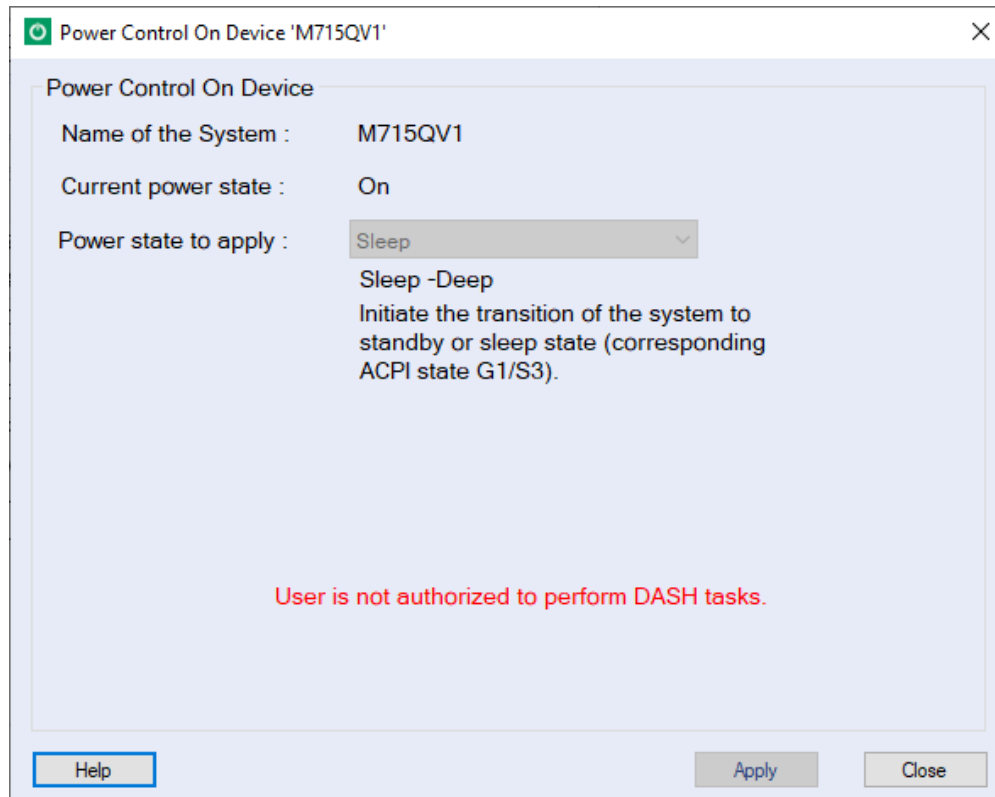
- When user is not authorized to perform DASH tasks on collection:



**Figure 121: Collection Error**

- When user is not authorized to perform DASH tasks:





**Figure 122: Device Error**

- When user is not authorized to perform DASH Configuration:

DASH Configuration

Authentication Schemes

	Auth Identifier	Scheme	Username	Password	Confirm Password
1	Realtek	Digest	Administrator	*****	*****
2	Broadcom	Digest	Administrator	*****	*****
3		<Not Used>			

Management Port and Transport

☐ HTTP

623

☐ HTTPS

664

Alerts

Event Port : 8080

Configuration Manager Settings

☒ DASH Wakeup - Use DASH to wakeup a collection of devices during power management and package deployment

☒ DASH Auto Discover - Enable automatic DASH discovery of newly found devices by site server

TLS certificate for HTTPS

☒ Trust self signed certificate

Any self-signed TLS certificate, installed on DASH system will be trusted. Ensure the DASH systems are configured with a TLS server certificate.

User is not authorized to perform DASH administrative tasks.

About

Help

Save

Close

Figure 123: DASH Configuration Error

**Note :** Active directory domain controller must be accessible for the Configuration Manager console user for checking authorization information. If the domain controller is down, user will be reported as unauthorized.

# Chapter 5      DASH Scheduled Tasks

---

The DASH Tasks Scheduler provides the ability to schedule the initiation of DASH tasks at pre-defined times or after specified time intervals.

## 5.1 Schedule DASH Tasks

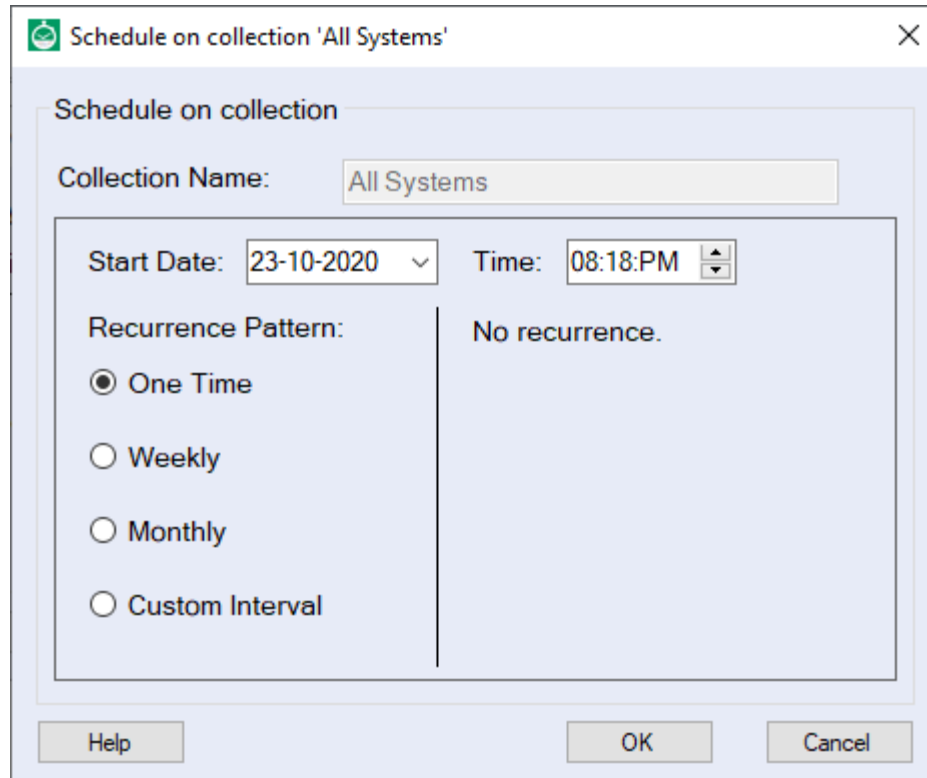
The user can schedule the following tasks:

- Discovery on collection task.
- Power on collection task.
- Firmware upgrade on collection task.

The **Schedule** button is provided on supported screens. When a user clicks **Schedule**, the **DASH Task Scheduler** screen is launched, as shown in Figure 124.

To schedule a new DASH task, perform the following steps:

1. Click the **Schedule** button. (See sections 3.1.1, 3.2.1 and 3.10.1)
2. Select the "Start Date" and "Time" to run the scheduled task.
3. Select a "Recurrence Pattern" for the DASH task.  
Tasks can be scheduled to run periodically (one time, weekly, monthly, or custom).
4. If the recurrence pattern is other than "One Time", specify the expiry date of the task in the "End Date" field.
5. For Monthly and Weekly Recurrence patterns, set the "Recur Every" field to define the interval between each cycle.



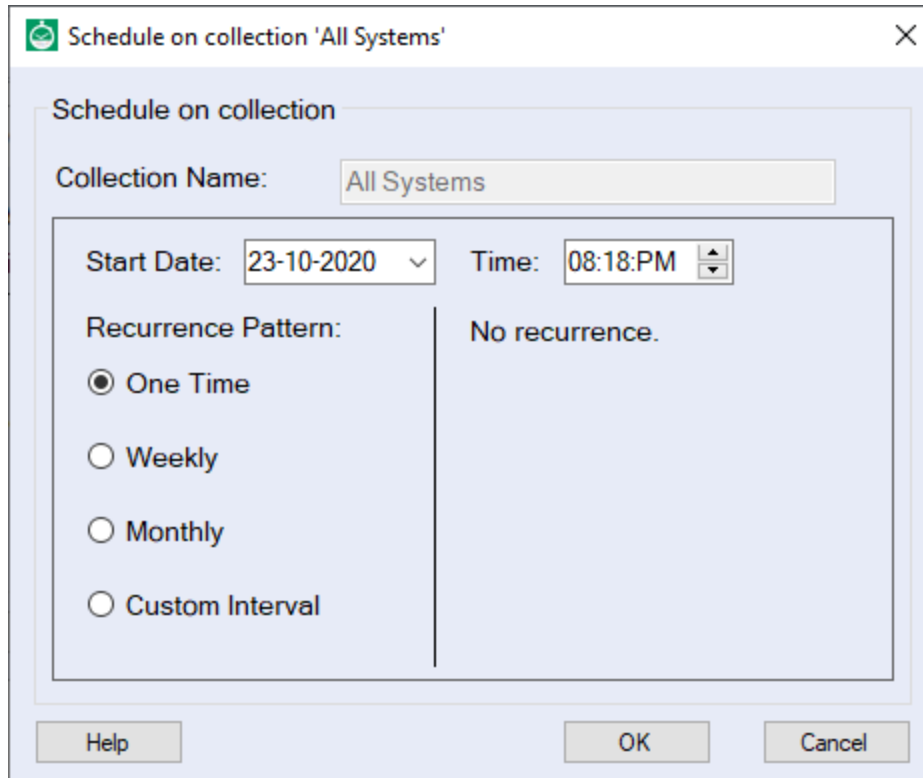
**Figure 124: DASH Task Scheduler**

### 5.1.1 Recurrence Patterns

The DASH task Scheduler supports the following four recurrence patterns:

#### 5.1.1.1 One time Recurrence Pattern

You can schedule the DASH tasks to run only once.



**Figure 125: DASH Task Scheduler One Time**

### **5.1.1.2 Weekly Recurrence Pattern**

You can schedule the DASH tasks to run every week on a particular weekday or on a set of weekdays.

The screenshot shows a dialog box titled "Schedule on collection 'All Systems'". Inside, there is a section "Schedule on collection" with a "Collection Name" field set to "All Systems". Below this, there are fields for "Start Date" (23-10-2020) and "Time" (08:18:PM). The "Recurrence Pattern" section has four radio buttons: "One Time", "Weekly" (selected), "Monthly", and "Custom Interval". To the right of the "Weekly" option, there is a "Recur every" field set to "1" with a "week" label. Below this, there are checkboxes for days of the week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday (checked), and Saturday. At the bottom right of the recurrence section is an "End Date" field set to 23-10-2020. At the bottom of the dialog are three buttons: "Help", "OK", and "Cancel".

**Figure 126: DASH Task Scheduler Weekly**

### 5.1.1.3 Monthly Recurrence Pattern

You can schedule the DASH tasks to run every month in one of the following patterns:

- On a particular date
- On the last day of the month
- On a  $n^{\text{th}}$  day of the week

**Schedule on collection 'All Systems'**

Schedule on collection

Collection Name: All Systems

Start Date: 23-10-2020 Time: 08:18:PM

Recurrence Pattern:

☐ One Time

☐ Weekly

☒ Monthly

☐ Custom Interval

Recur every: 1 month

☒ Day 1

☐ The last day of the month

☐ The First Sunday

End Date: 23-10-2020

Help OK Cancel

**Figure 127: DASH Task Scheduler Monthly**

#### **5.1.1.4 Custom Recurrence Pattern**

You can also set custom recurrence patterns. The following patterns are supported:

- Every  $n^{\text{th}}$  Hour
- Every  $n^{\text{th}}$  Day

Figure 128: DASH Task Scheduler Custom

## 5.2 DASH Scheduled Tasks

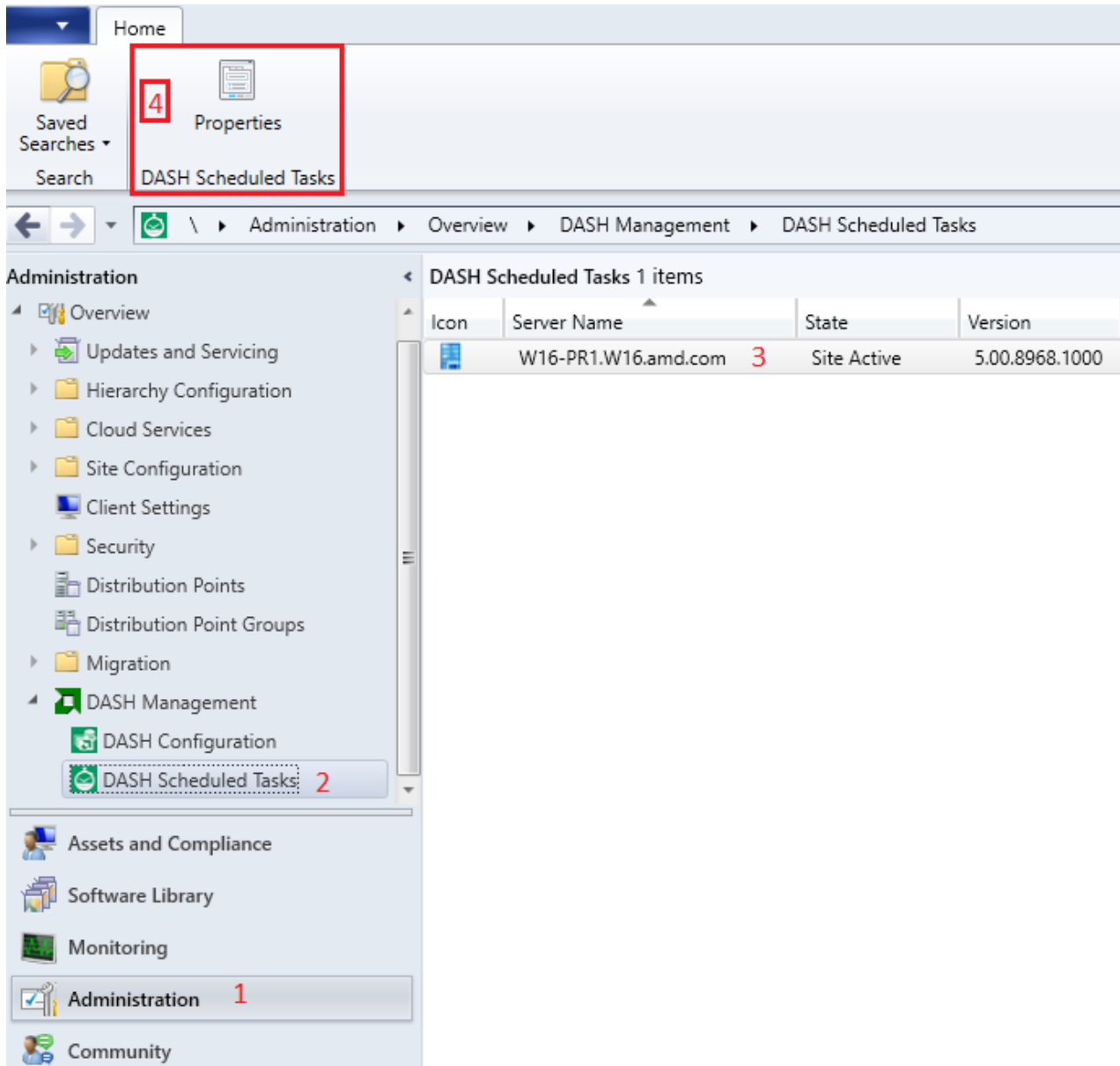
The **DASH Scheduled Tasks** console enables you to view all the scheduled DASH tasks in the **Administration** tab of MEM.

It also allows you to enable/disable or delete the scheduled DASH task.

To view the scheduled DASH tasks, perform the following steps:

1. Expand the **Administration** node.
2. Click **Overview**, expand the **DASH Management** node and click **DASH Scheduled Tasks**. In the right pane, all the servers are listed.
3. Right-click the server whose properties you wish to monitor.

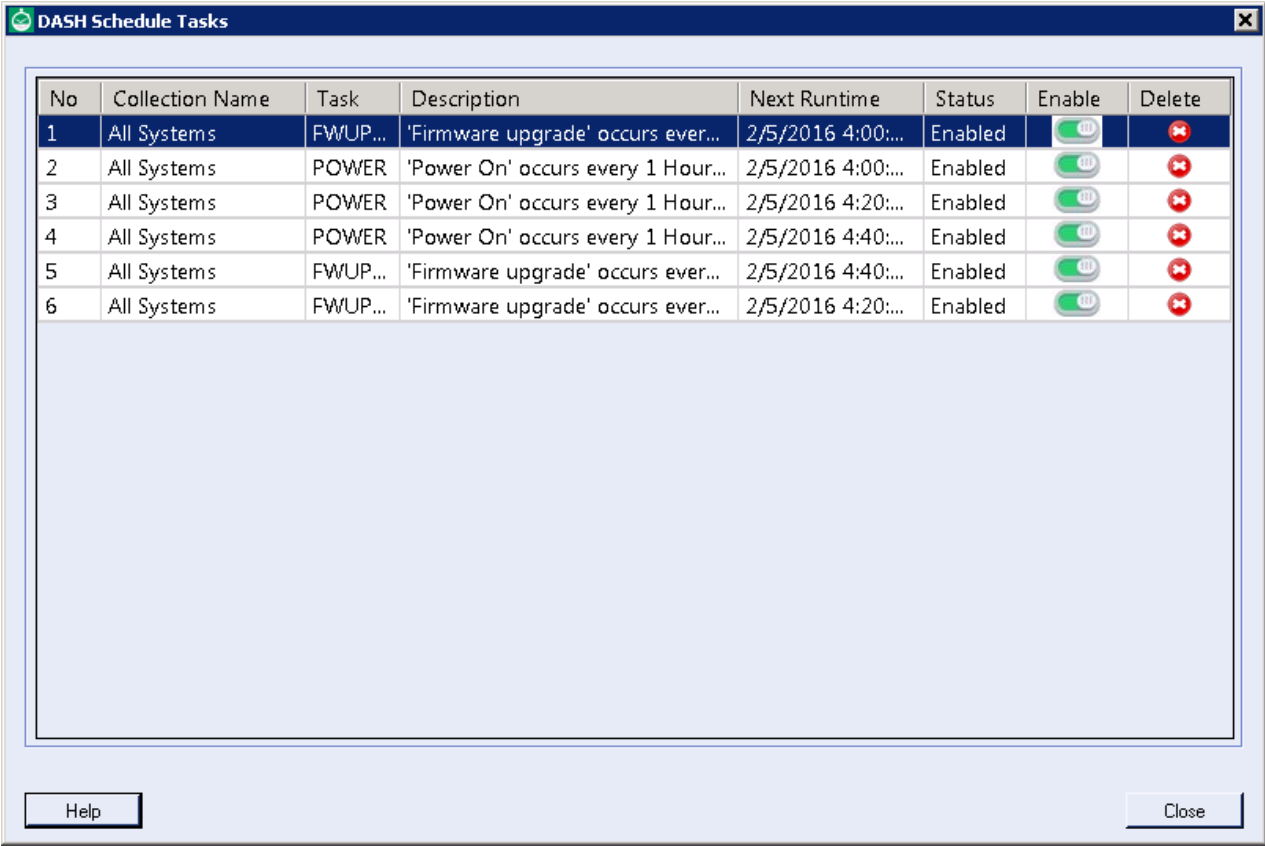




**Figure 129: DASH Scheduled Tasks Node**

4. Select **Properties** to view the properties of the scheduled DASH Tasks. The following attributes of scheduled tasks are displayed:
  - Collection Name, which shows the collection name which a task is scheduled for.
  - Task Name, which specifies the DASH task.
  - Description, which describes the task start time, end time, and recurrence pattern.
  - Next Run time, which shows the next run time of the tasks.
  - Status, which shows the current status.  
The status can be enabled, disabled and expired. The status is set to expired only when the end date has elapsed.
5. Task Operations:
  - You can change the status from enable to disable or viceversa by sliding the enable slider.

- You can delete a particular task by clicking the Delete option next to that task.



**Figure 130: DASH Scheduled Tasks**

- You can view the DASH Scheduled Tasks Details by double clicking a particular scheduled task. A window with the details of the scheduled task is displayed :

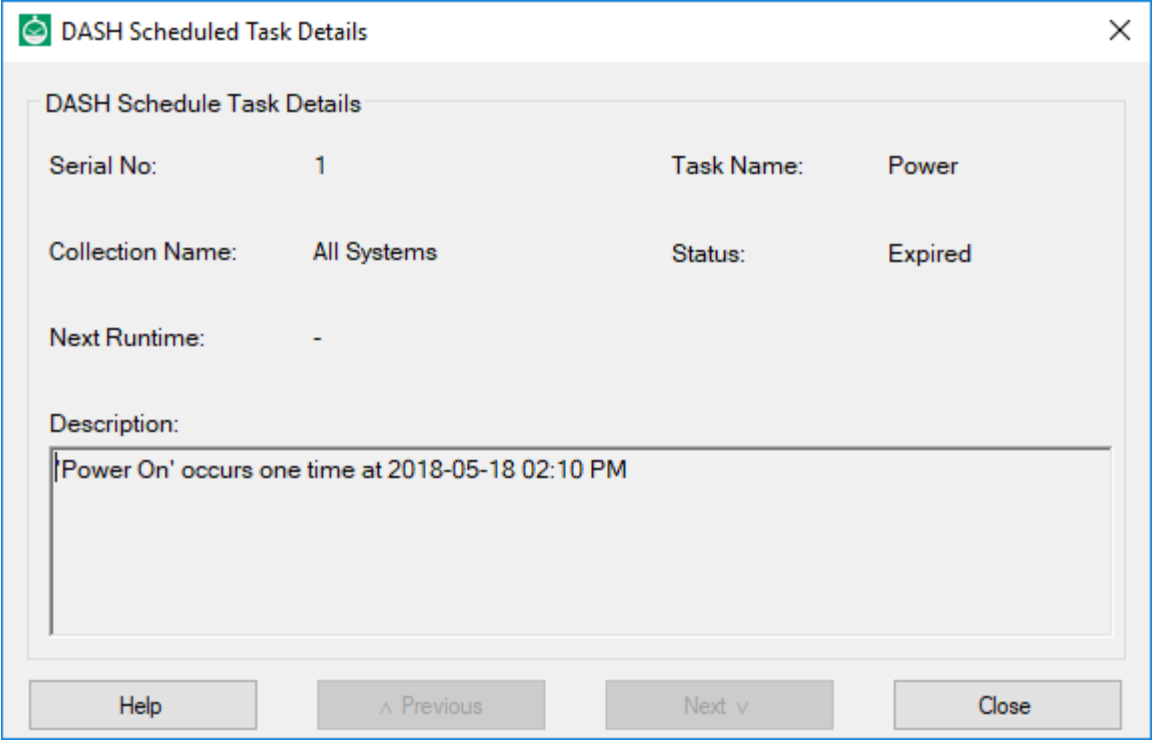


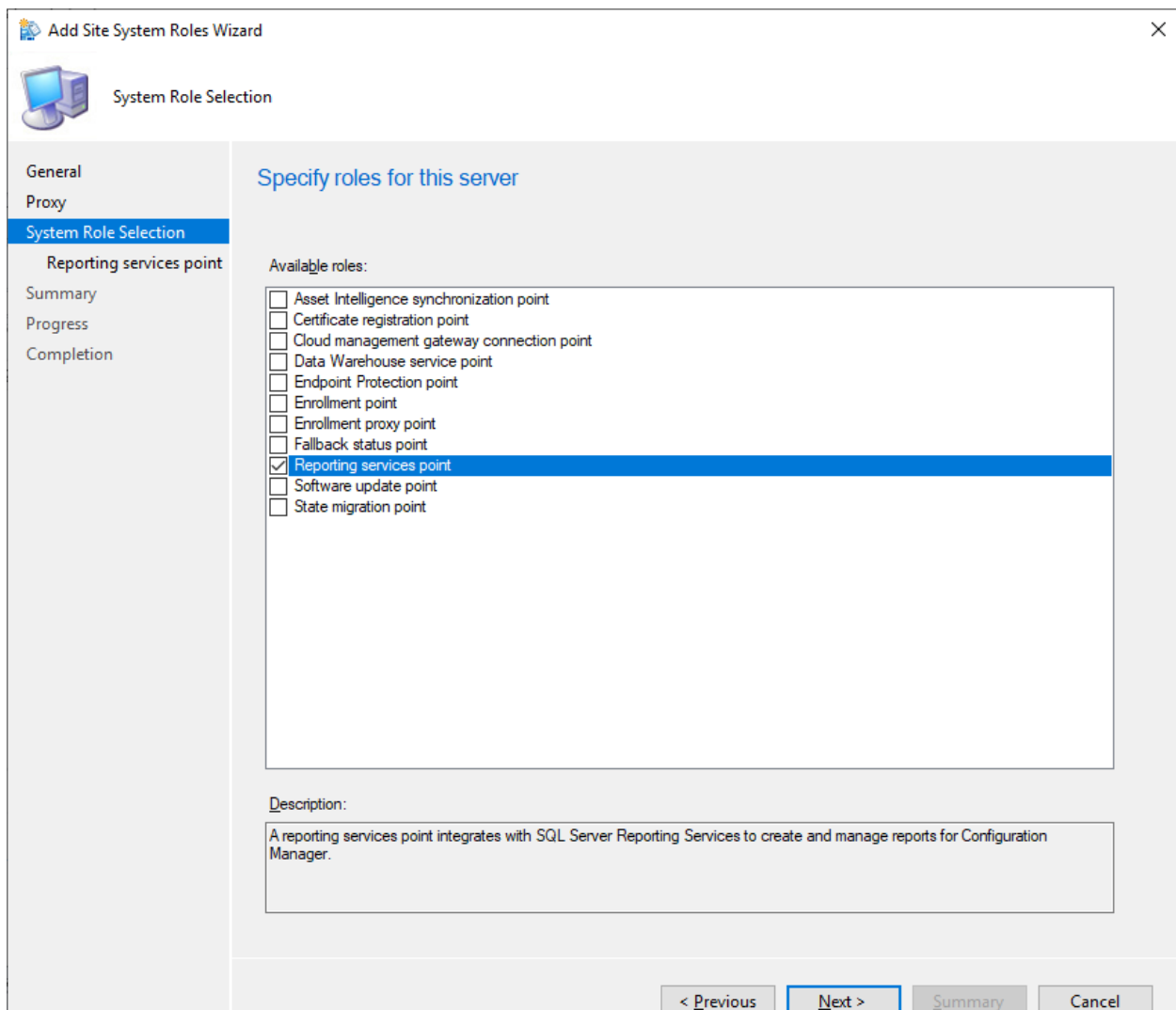
Figure 131: DASH Scheduled Task Details

# Chapter 6      Creating User Action Report for AMPS

DASH User Action Report helps user to accumulate and organize all DASH activities along with details of user. This report is enabled with AMPS.

## 6.1 Prerequisites

- 1) Install SQL Server Reporting Service
- 2) Microsoft Report Builder
- 3) Site server needs to have "Reporting services point" role as shown in Figure 132



**Figure 132: Reporting services point role**

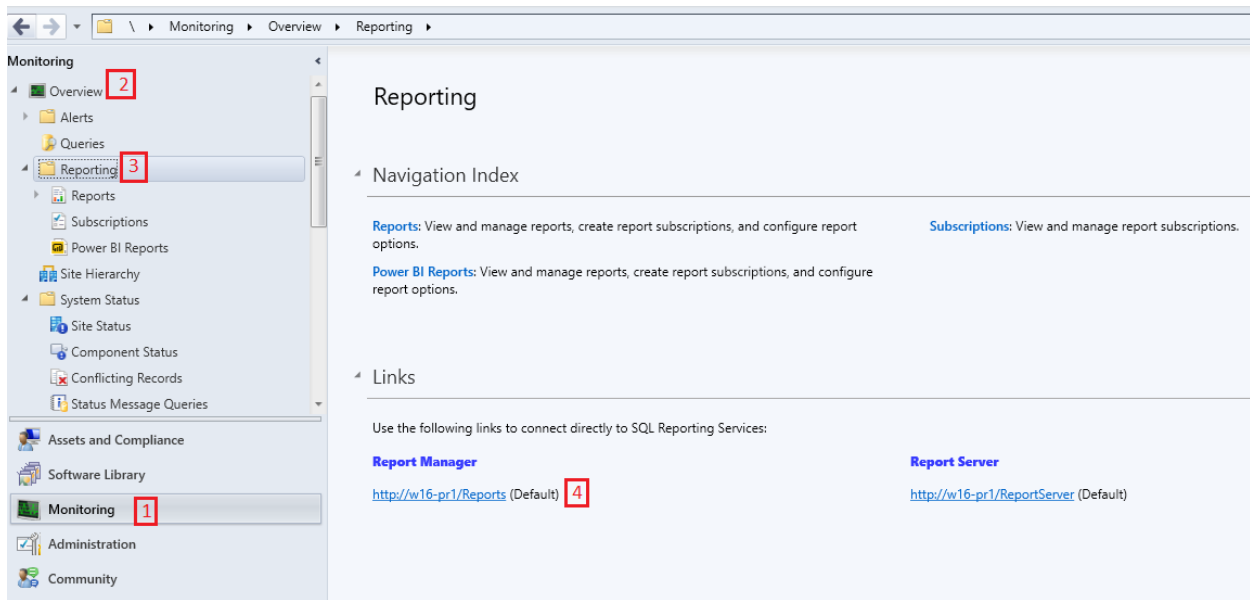
In our examples we have used the following:

- 1) MEM System: w16-pr1
- 2) Site code: wp1

I am using a CAS-Primary setup where the Domain controller is installed on the CAS system. I am using the Primary system for DASH Reporting.

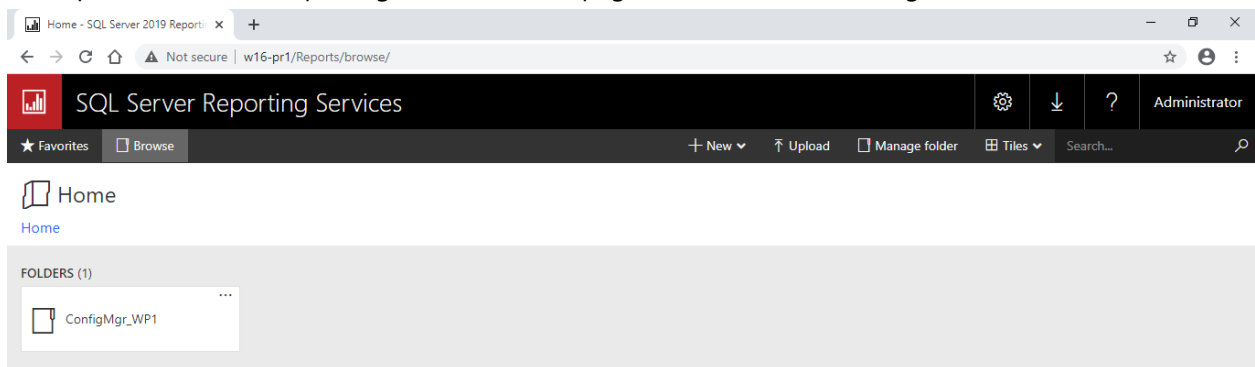
## 6.2 Opening SSRS from MEM

Navigate to \Monitoring\Overview\Reporting and click on 'Report Manager' Link (<http://w16-pr1/Reports>) as in Figure 133.



**Figure 133: Opening Report Manager Link**

This opens SQL Server Reporting Services (SSRS) page in the browser as in Figure 134.



**Figure 134: SQL Server Reporting Services**

The home page of SSRS should have a folder ConfigMgr\_<SiteCode> (for us this is ConfigMgr\_WP1). Click on the folder and then click on "New" followed by "Folder" from the Menu as shown in Figure 135.

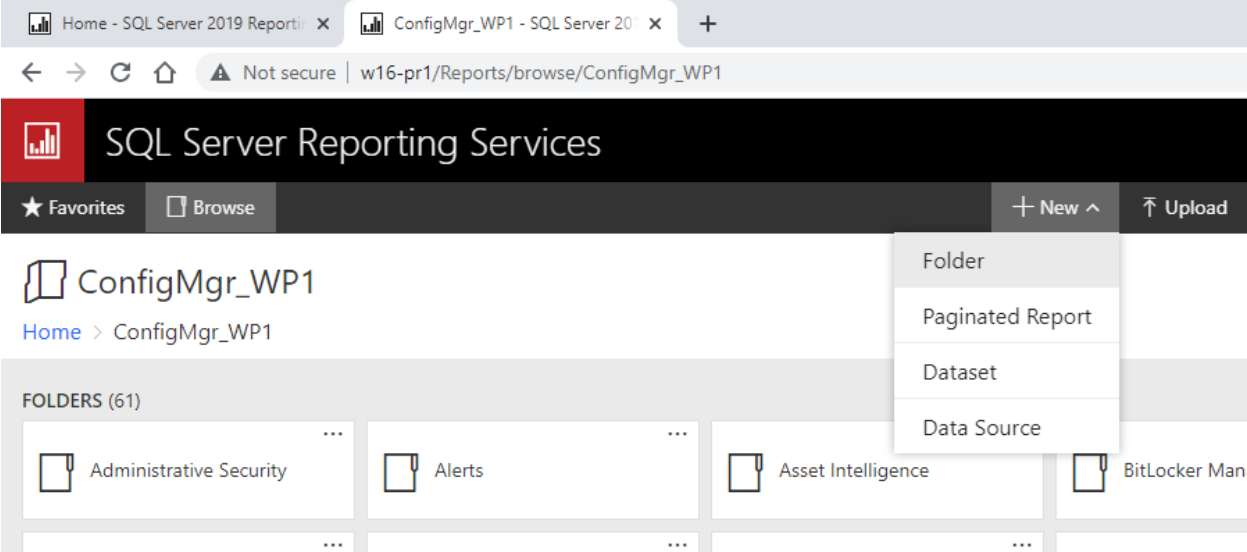


Figure 135: Adding new folder to SSRS

Enter the name “DASH Reports” as shown in Figure 136 and click on “Create” button.

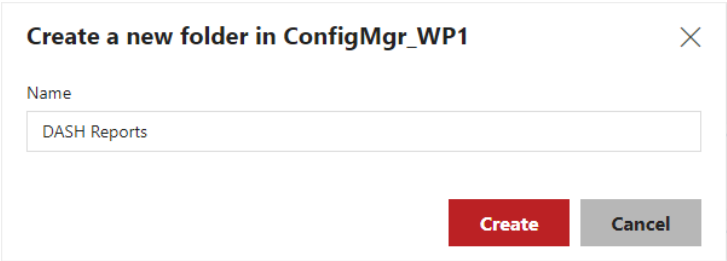
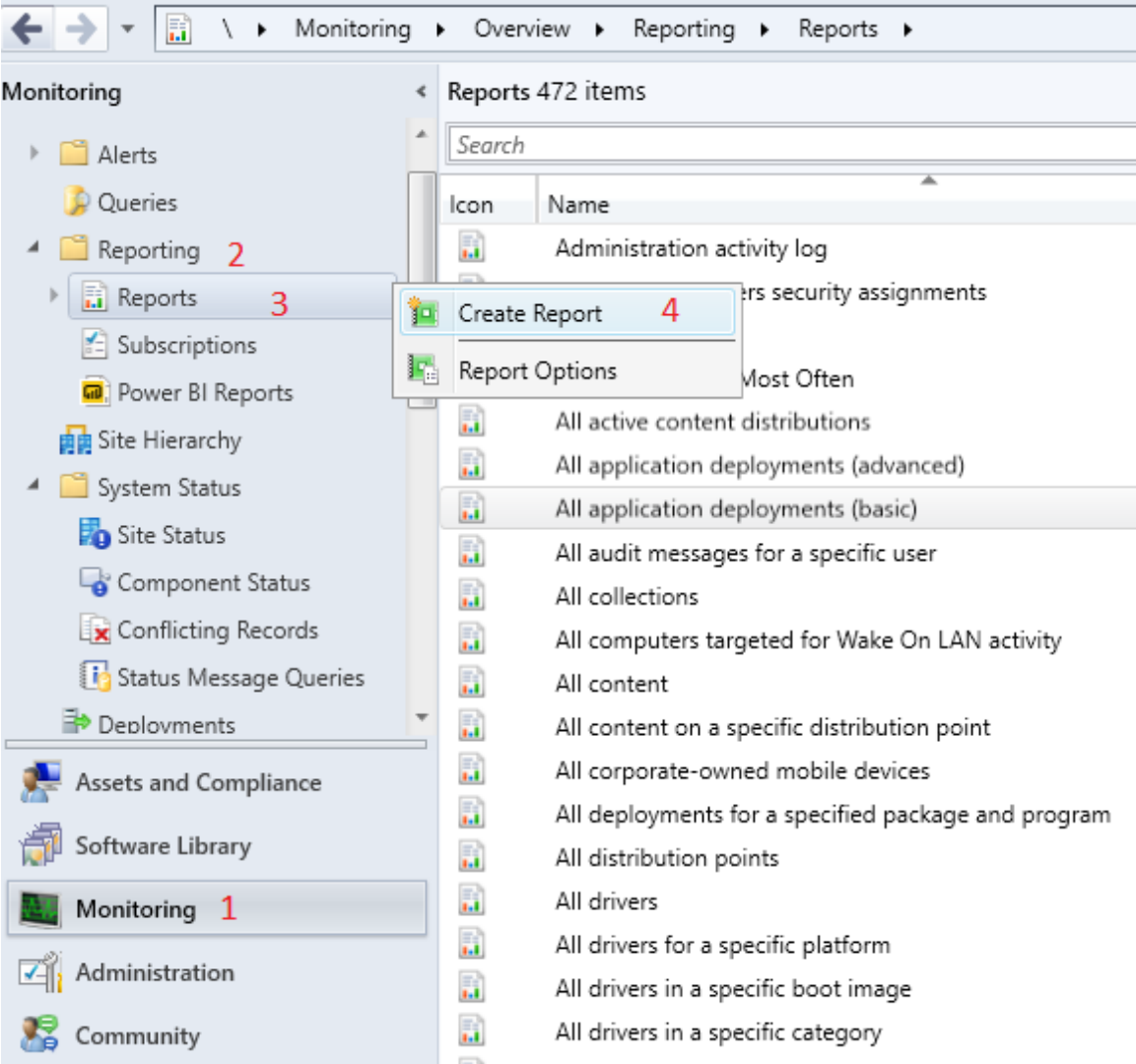


Figure 136: New Folder prompt with Name field

In MEM navigate to \Monitoring\Overview\Reporting\Reports  
Right click on “Reports” and then click on “Create Report” as shown in Figure 137.



**Figure 137: Create Report option**

For name enter “DASH User Action Reports”. Click on the Browse button and Select the folder “DASH Reports” from “Report Path” window as shown in Figure 138.

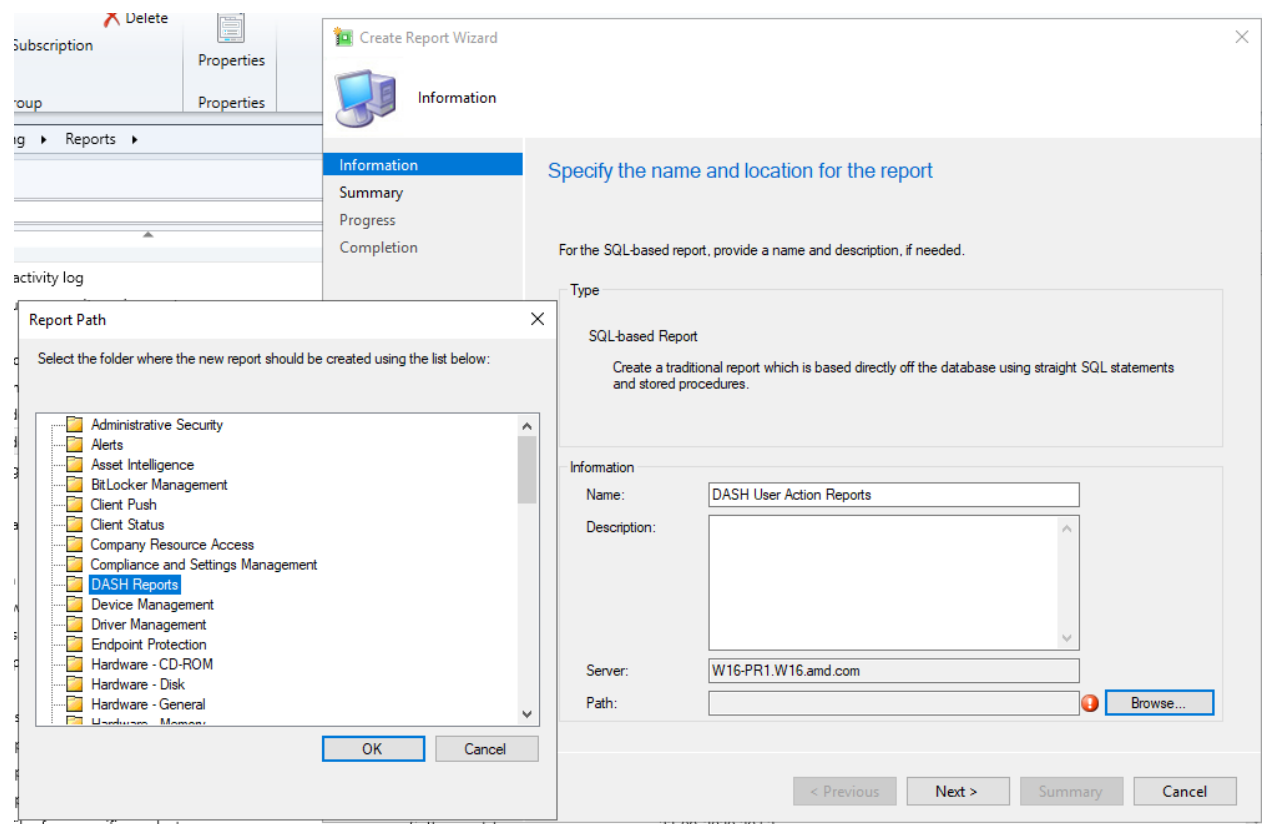
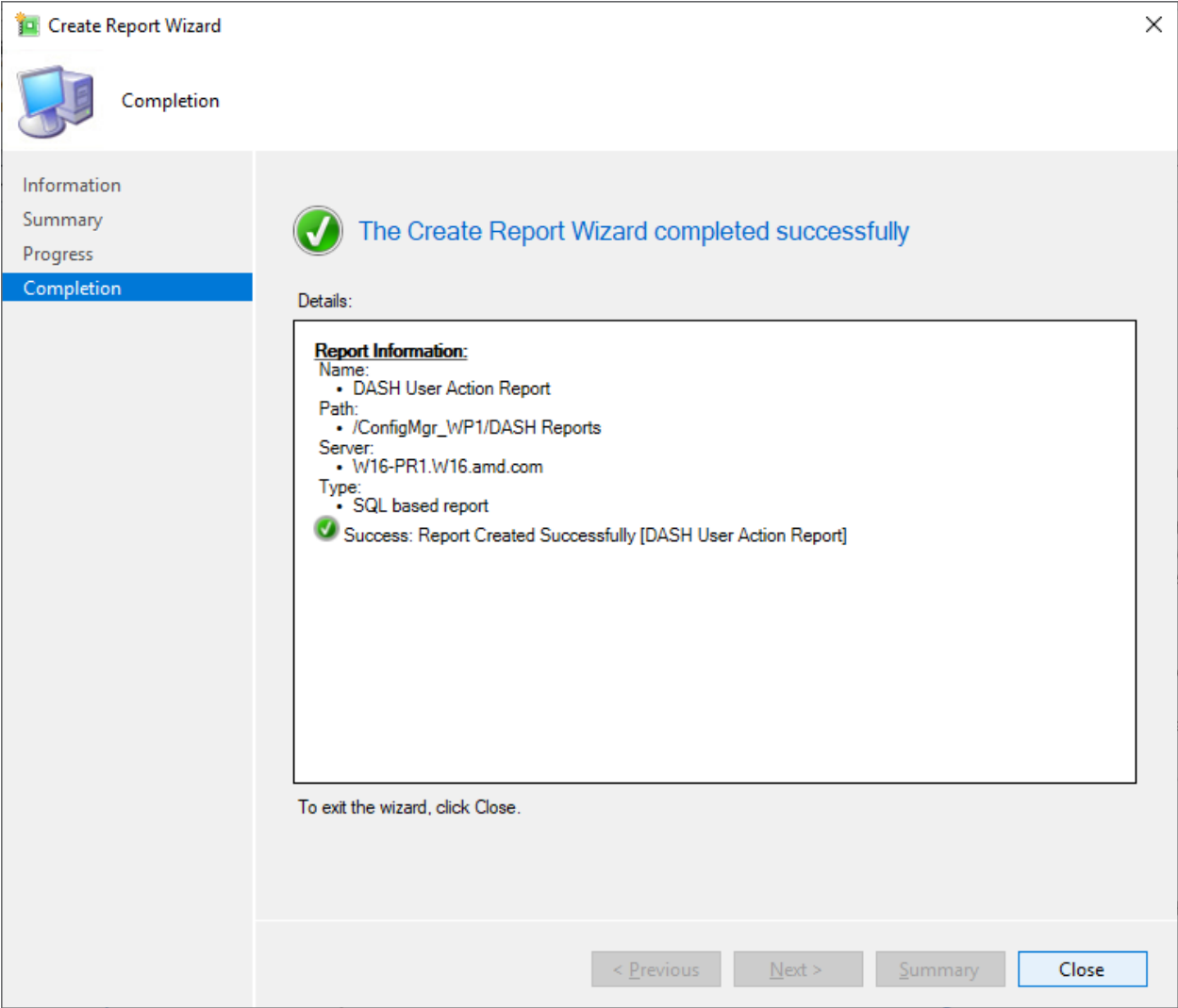


Figure 138: Adding Report Name and Path

Then click on “Next” button till you get the screen that says “the Create Reports Wizard completed successfully” as shown in Figure 139.





**Figure 139: Create Reports Wizard completed successfully**

Once you exit the wizard by clicking close, it popus up “Microsoft Report Builder” utility as shown in Figure 140.

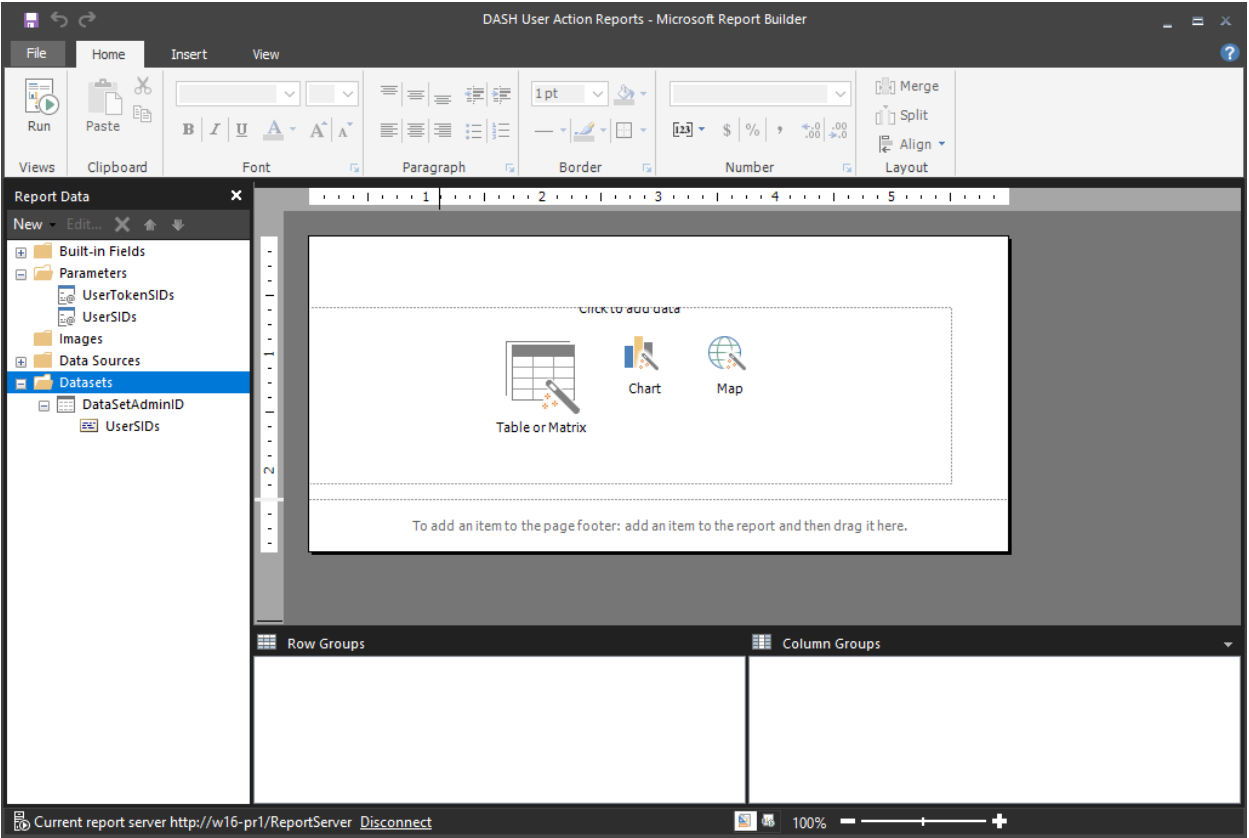


Figure 140: Microsoft Report Builder utility

### 6.3 Delete Default Datasets and Properties

Expand “Parameters” and “Datasets” from the “Report Data” window.  
Right click on the default Datasets and click on “Delete” to delete the dataset as shown in Figure 141.

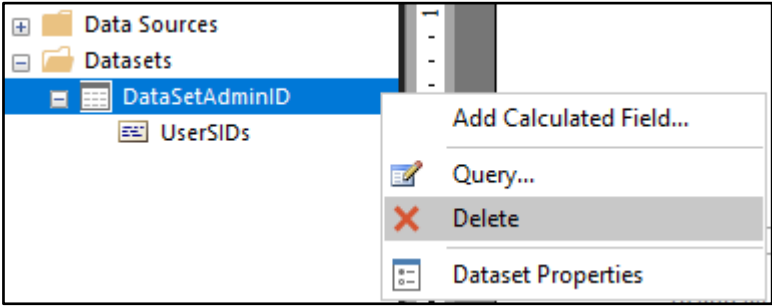


Figure 141: Deleting Datasets

Similarly, delete the default Parameters.

## 6.4 Adding new Datasets

### 6.4.1 DASHUserActionLogs

Right click on Datasets and click on “Add Dataset” as shown in Figure 142.

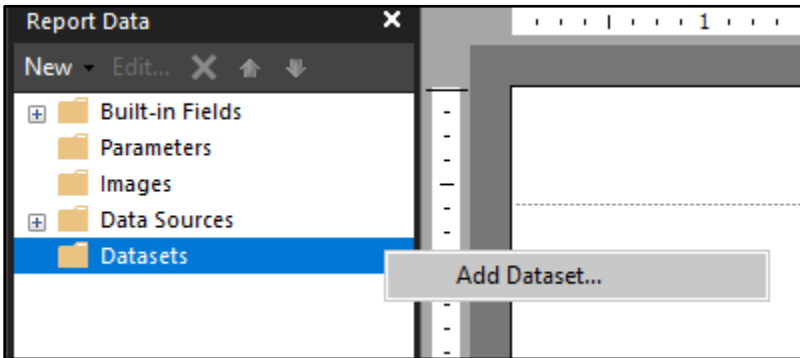


Figure 142: Adding Datasets

Set the following values to the dataset:

Name	DASHUserActionLogs
	Use a dataset embedded in my report
Data Source	Choose the default entry from dropdown
Query Type	Text
Query	<pre>SELECT     [ComputerName0],     [Creation_Date0],     [EventDetails0],     [RecordID0],     [Severity0],     [SiteCode0],     [Username0] FROM     [CM_WP1].[dbo].[v_R_DASHUserActionLogs_2_0_0] WHERE     (         (@Severity = 0)     OR (         @Severity = 1         AND Severity0 = 'Informational'     )     OR (         @Severity = 2         AND Severity0 = 'Warning'     )     )</pre>

```

OR (
    @Severity = 3
    AND Severity0 = 'Error'
)
)
AND Username0 = @Login
AND (
    (@DateRange = 0)
    OR (
        @DateRange = 1
        AND Creation_Date0 >= DATEADD(
            dd,
            DATEDIFF(
                dd,
                0,
                GETDATE()
            ),
            0
        )
    )
    OR (
        @DateRange = 2
        AND Creation_Date0 >= DATEADD(
            dd,
            DATEDIFF(
                dd,
                0,
                GETDATE()
            ) - 30,
            0
        )
    )
    OR (
        @DateRange = 3
        AND Creation_Date0 >= DATEADD(
            dd,
            DATEDIFF(
                dd,
                0,
                GETDATE()
            ) - 90,
            0
        )
    )
)
OR (

```

	<pre>@DateRange = 4 AND Creation_Date0 &gt;= DATEADD(     dd,     DATEDIFF(         dd,         0,         GETDATE()     ) -365,     0 ) ) )</pre>
--	--

After filling the values, click OK as shown in Figure 143.

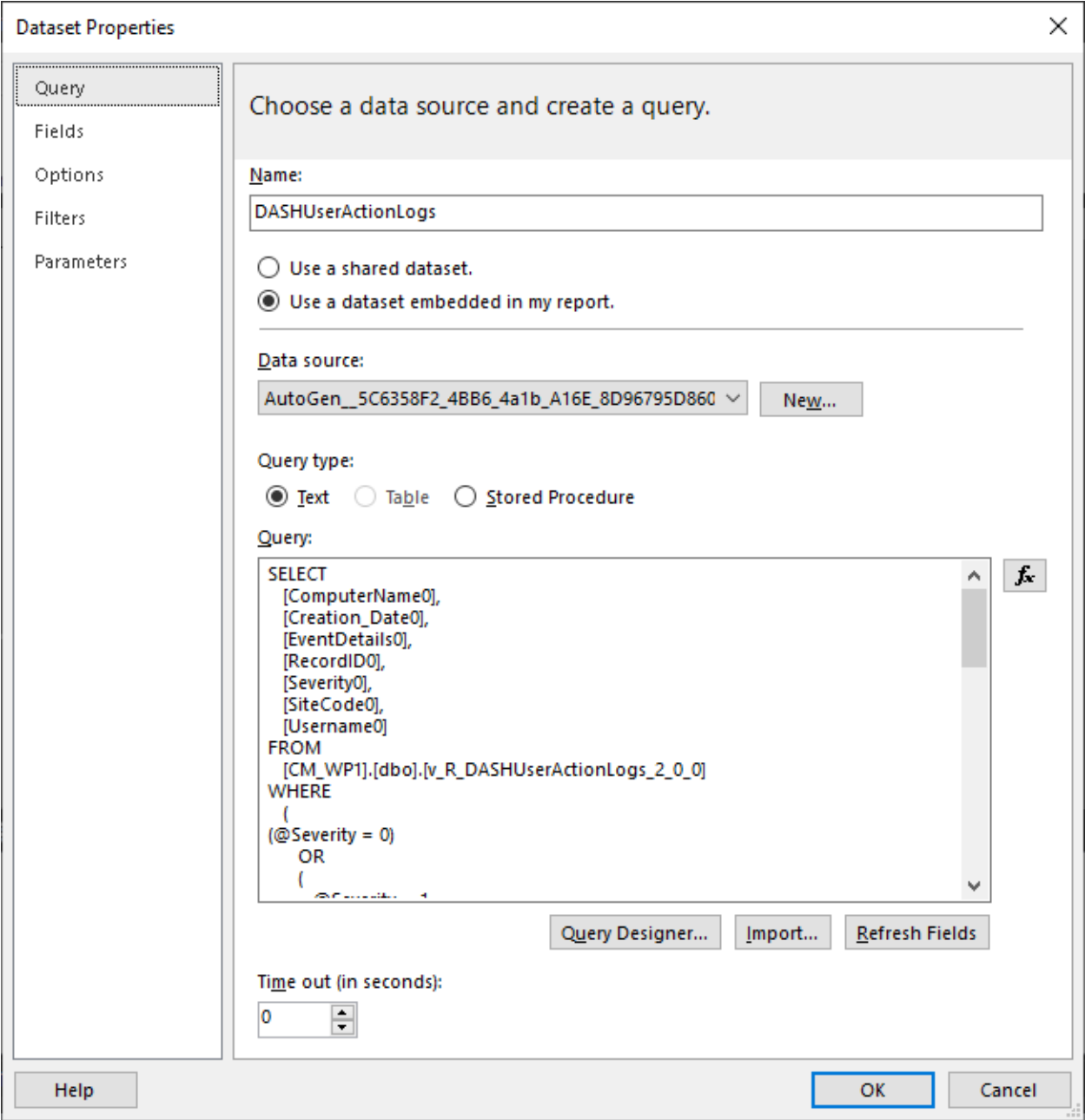


Figure 143: Setting values to DASH User Action Logs

**Note:** in the From clause, replace [CM\_WP1] with your specific sitecode [CM\_<site Code>]  
On clicking OK, the Datasets and Parameters are updated as in Figure 144.

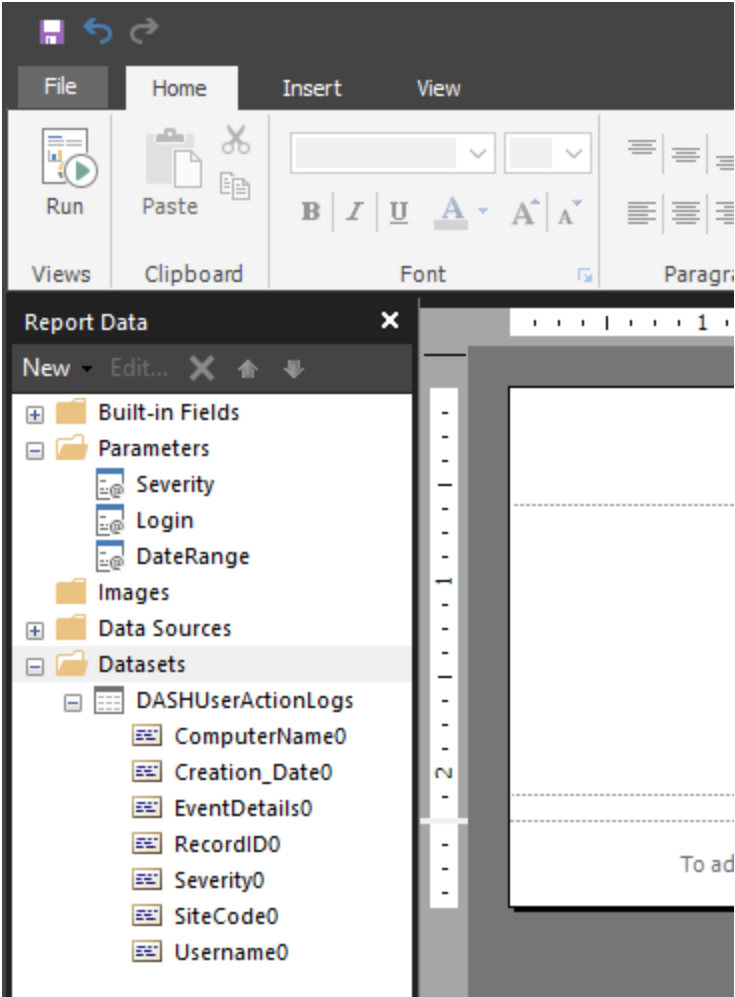


Figure 144: Updated Datasets and Parameters

6.4.2 Users

Similarly, create users Dataset with the following values:

Name	Users
	Use a dataset embedded in our report
Data Source	Choose an default entry from dropdown
Type	Query text
Query	<pre>SELECT     DISTINCT [LogonName] FROM     [CM_WP1].[dbo].[v_Admins]</pre>

**Note:** in the From clause, replace [CM\_WP1] with your specific sitecode [CM\_<site Code>]  
After filling the values click on OK as shown in Figure 145.

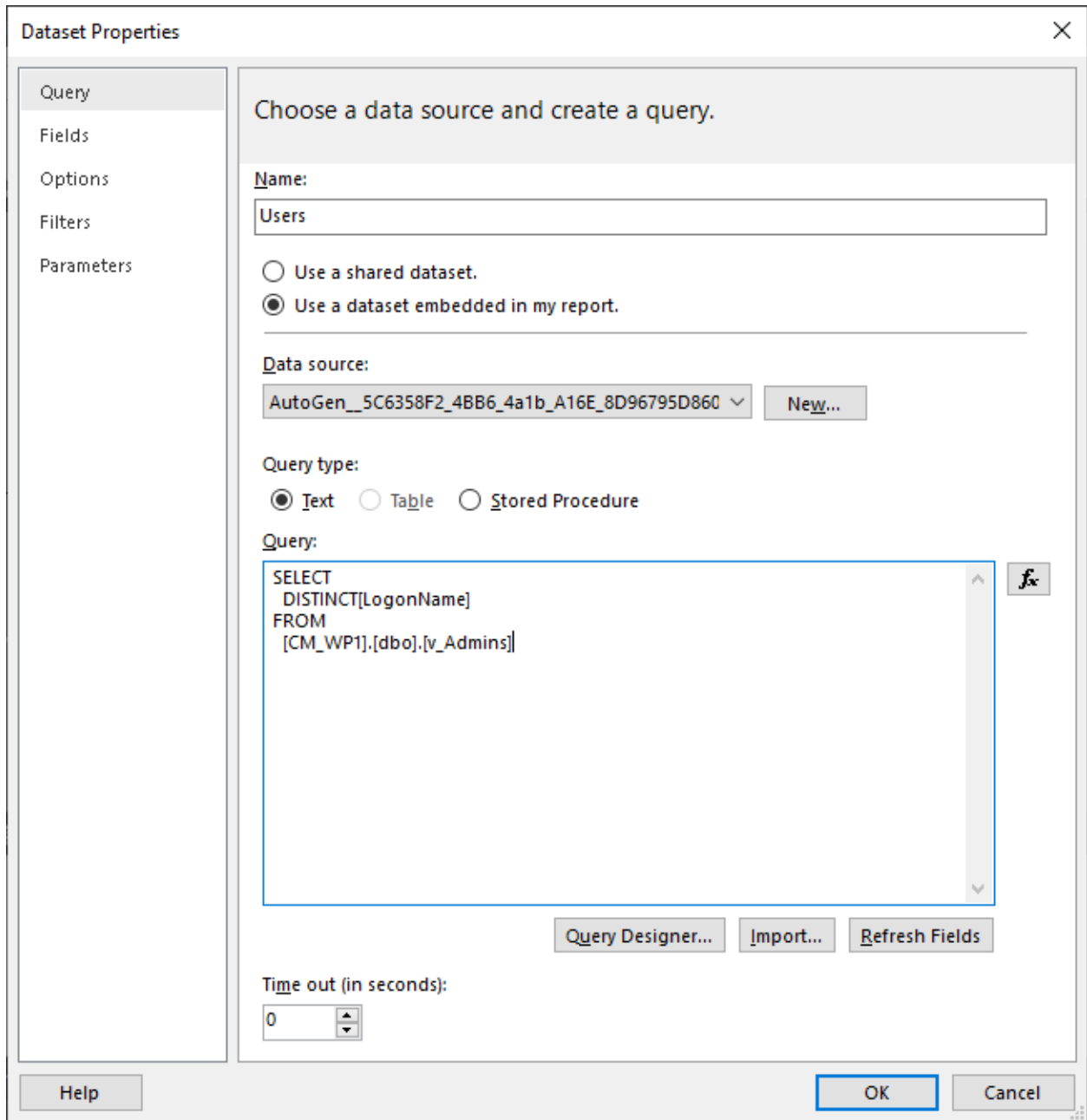


Figure 145: Creating Users dataset

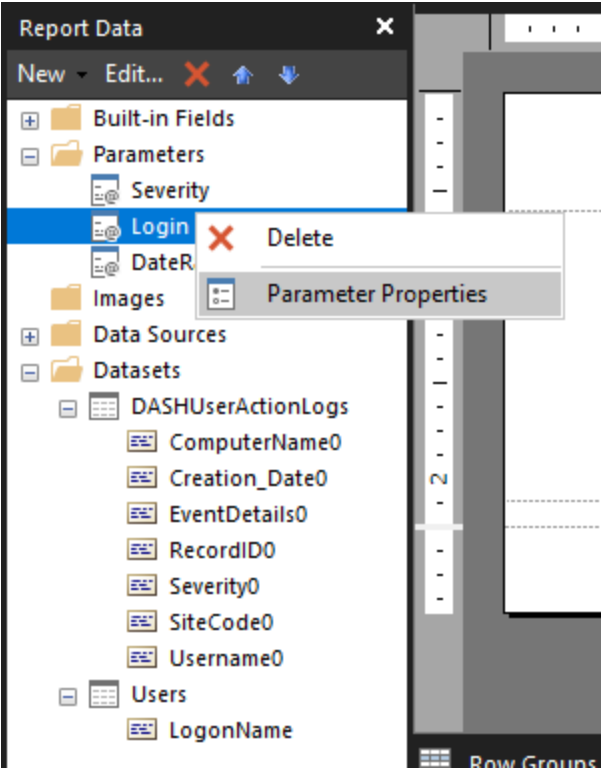
## 6.5 Setting Parameter Properties

The default values set for the three parameters can be customized to our needs.

### 6.5.1 Login

Right click on the Login Parameter and click on "Parameter Properties" as shown in Figure 146.





**Figure 146: Editing Parameter Properties**

Change the "Prompt" value to "Users". Then click on "Available Values" as shown in Figure 147.

Report Parameter Properties

General

Available Values **2**

Default Values

Advanced

Change name, data type, and other options.

Name:

Login

Prompt: **1**

Users

Data type:

Text

☐ Allow blank value ("")

☐ Allow null value

☐ Allow multiple values

Select parameter visibility:

☒ Visible

☐ Hidden

☐ Internal

Help OK Cancel

**Figure 147: Editing Available Values**

Click on "Get values from a query". From Datasets dropdown choose the "Users" dataset we created. Then in "Value field" and "Label field" choose "LogonName" and click OK as shown in Figure 148.

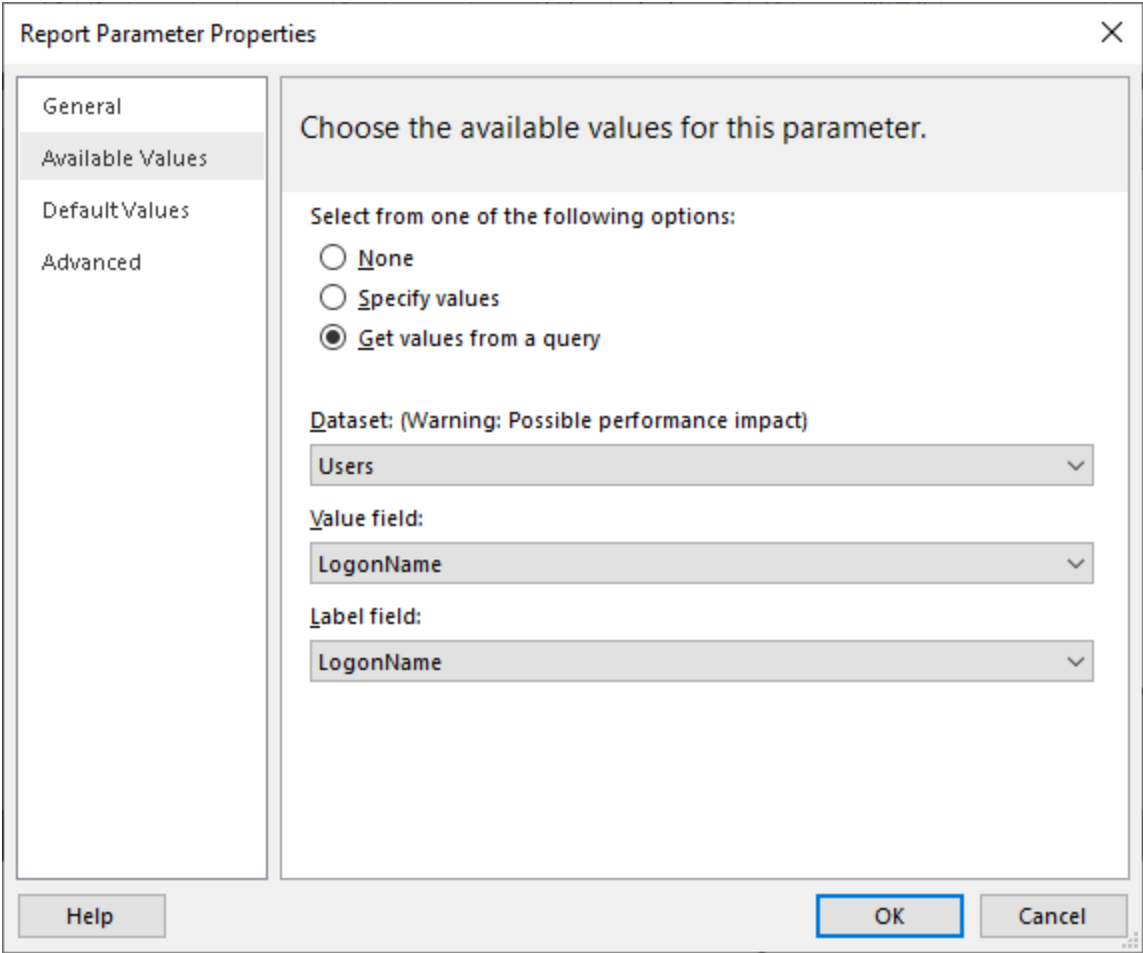


Figure 148: Setting Available Values to Login Parameter

6.5.2 Severity

As done for Login, right click on the "Severity" property and click on "Parameter Properties". Then click on "Available Values".

Here Select the "Specify Values" option and add the following entries by clicking on "Add" button for each value.

Label	Value
<All Values>	0
Informational	1
Warning	2
Error	3

Then click on OK as shown in Figure 149.

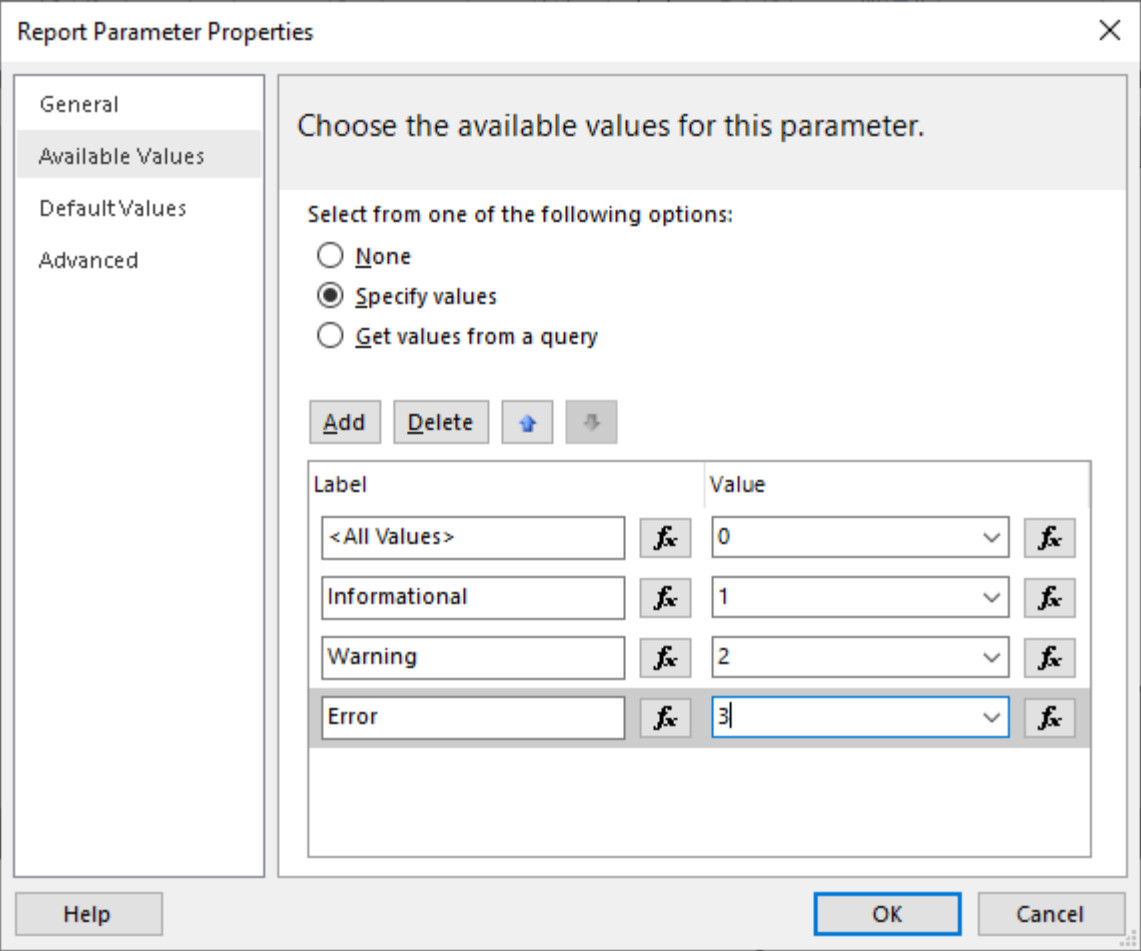


Figure 149: Setting Available Properties to Severity parameter

6.5.3      **DateRange**

As done for Login and Severity, right click on the “DateRange” property and click on “Parameter Properties”.

Then click on “Available Values”.

Here Select the “Specify Values” option and add the following entries by clicking on “Add” button for each value.

Label	Value
<All Values>	0
During Today	1
During Last 30 Days	2
During Last 90 Days	3
During Last 365 Days	4

Then click on OK as shown in Figure 150.

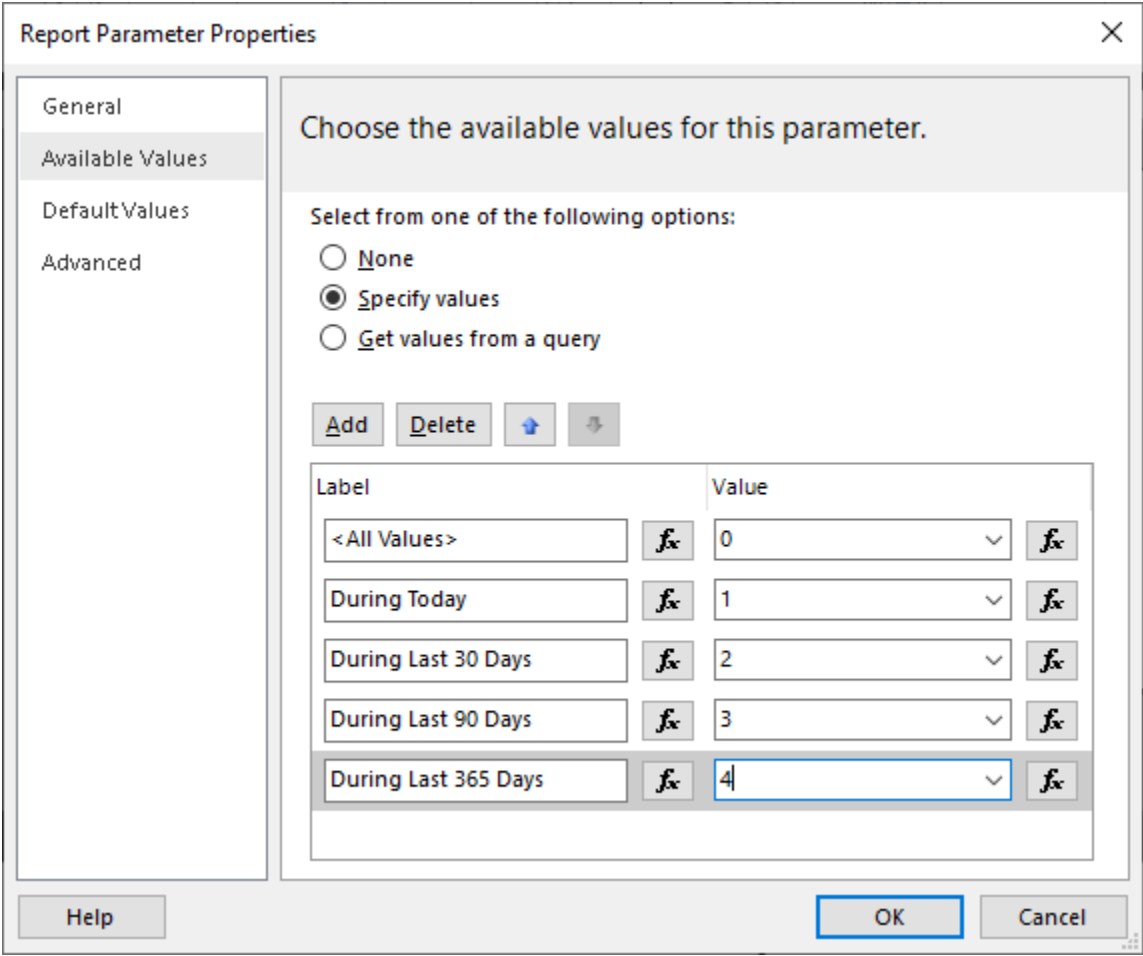
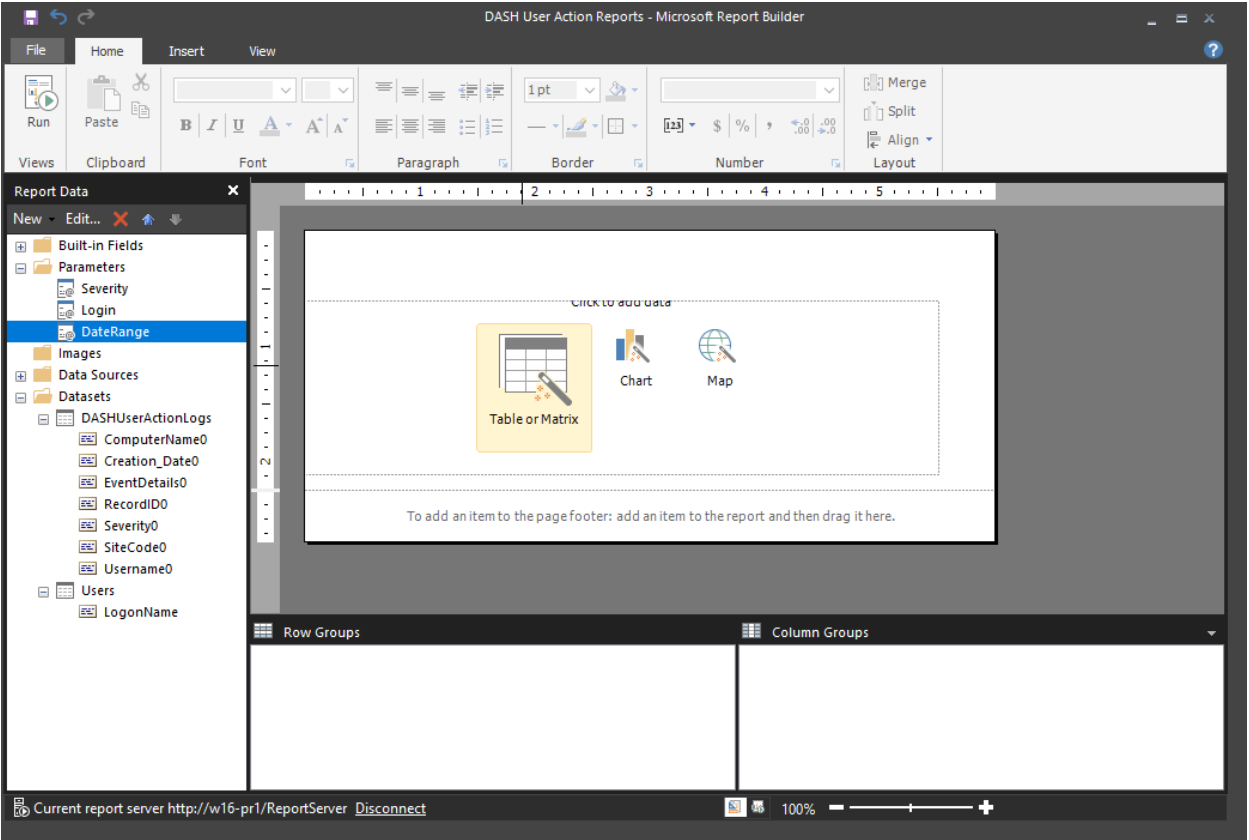


Figure 150: Setting Available Values to Date Range parameter

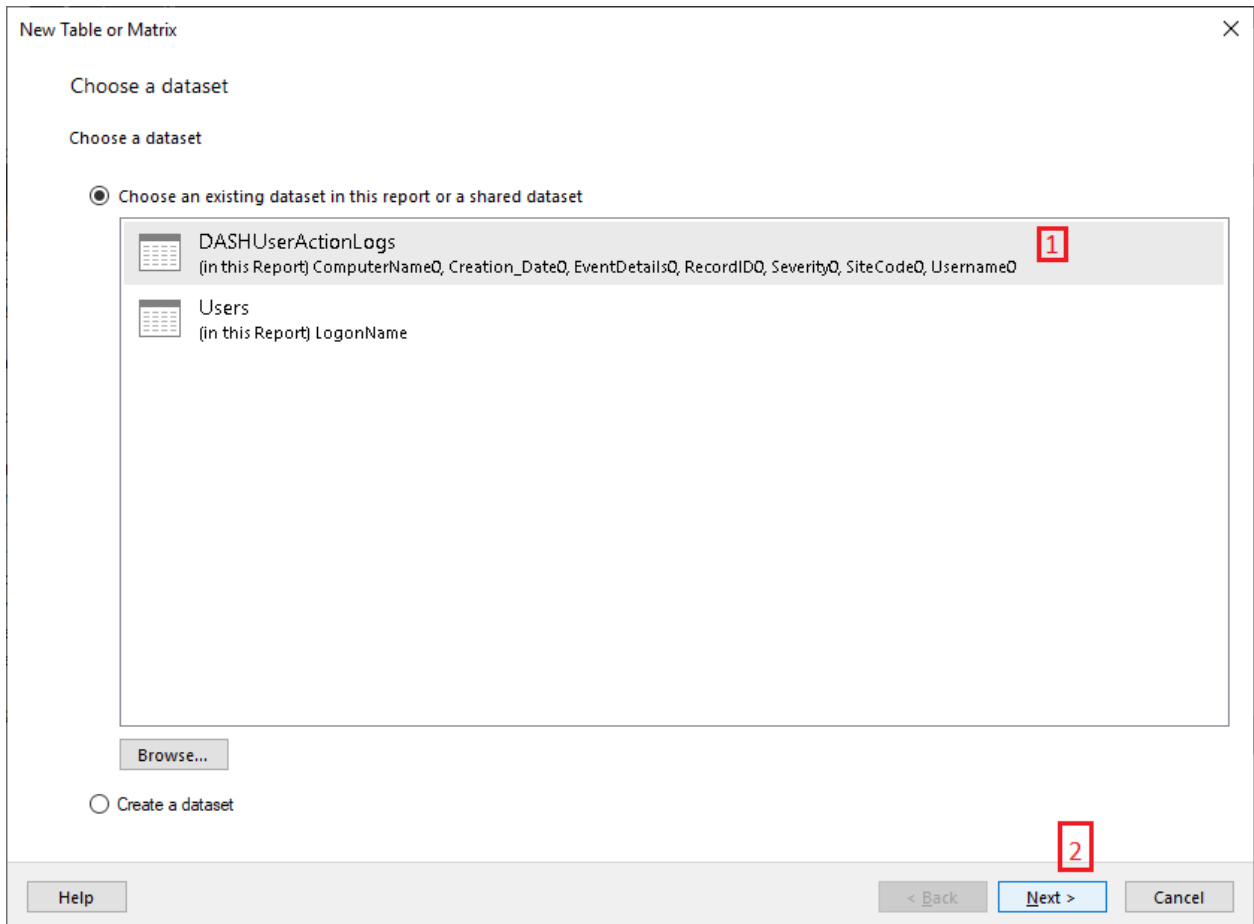
## 6.6 Arranging the Values in the report

Click on the "Table or Matrix" button from the center pane as shown in Figure 151.



**Figure 151: Table or Matrix option in Report Builder**

Select "DASHUserActionLogs" dataset as shown in Figure 152.

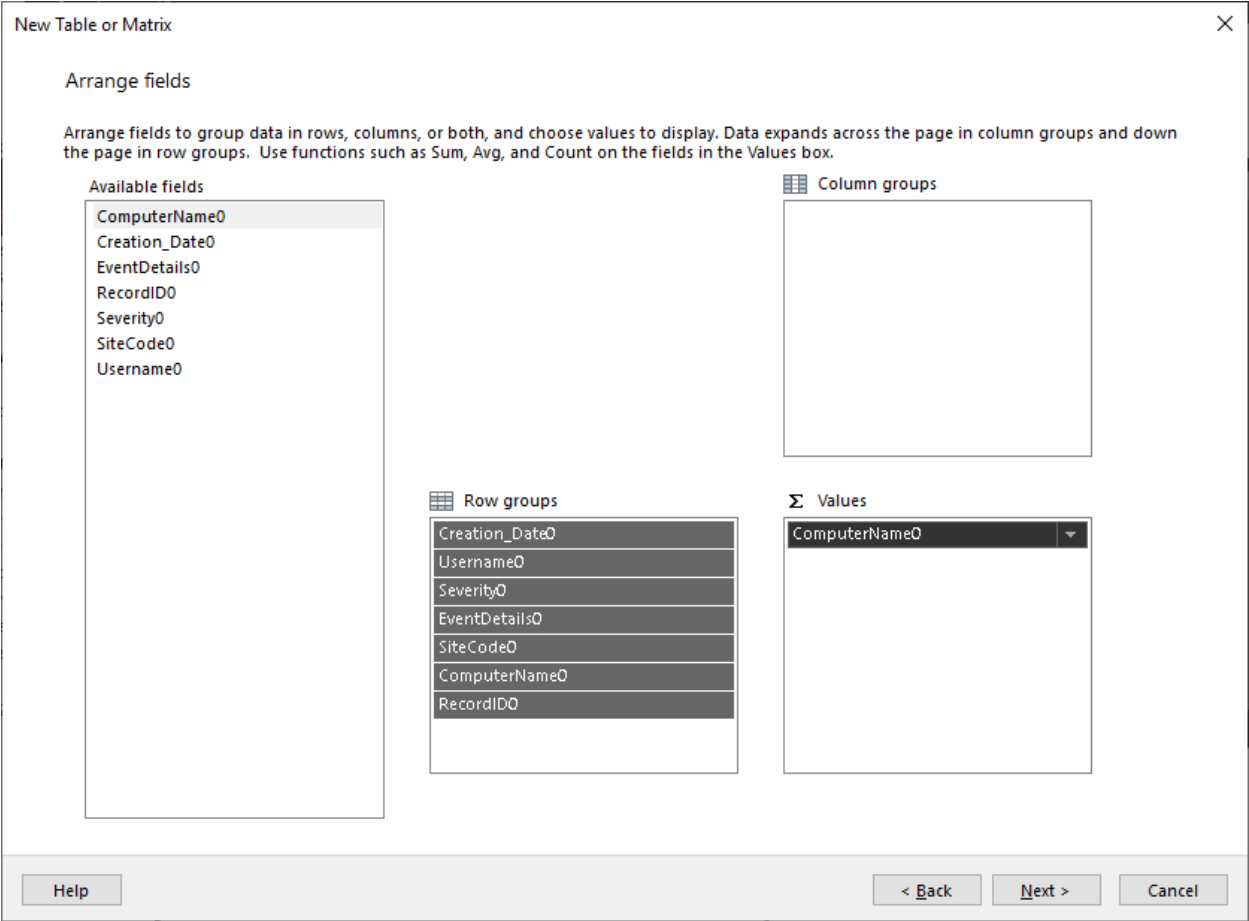


**Figure 152: Choosing the DASH User Action Logs Dataset**

Then drag and drop the fields from "Available fields" to "Row groups" in the order:

- 1) Creation\_Date0
- 2) Username0
- 3) Severity0
- 4) EventDetails0
- 5) SiteCode0
- 6) ComputerName0
- 7) RecordID0

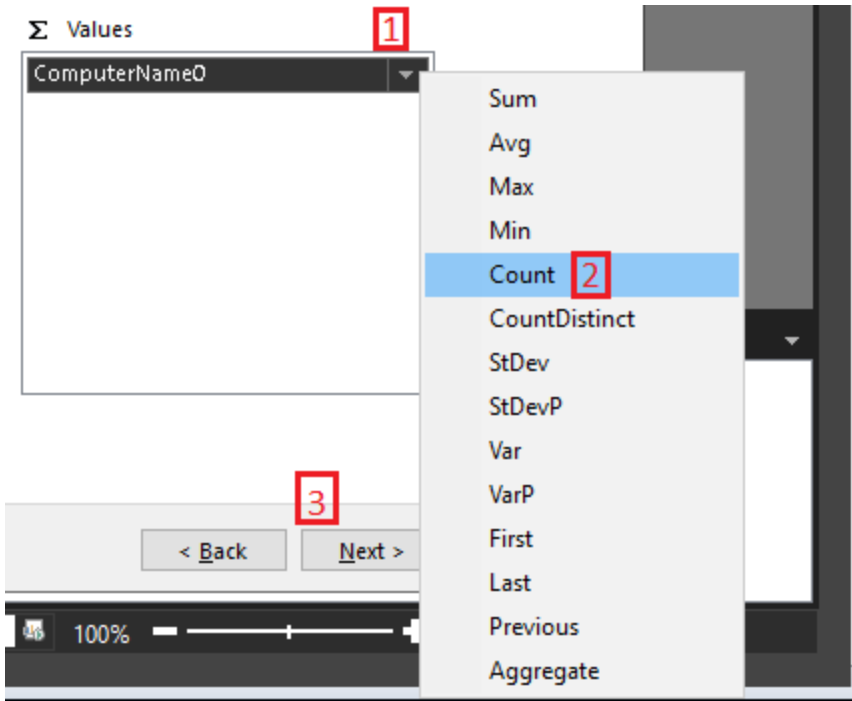
Also drag the field "ComputerName0" to "Values" field as shown in Figure 153.



**Figure 153: Setting Row Groups and Values**

From the dropdown of “ComputerName0” choose “Count” and then click on the “Next” button as shown in Figure 154.





**Figure 154: Choosing count property to Computer Name Value**

De-select the “Show subtotals and grand totals” checkbox and then click on “Next”. Preview the report and click on “Finish” button as shown in Figure 155.

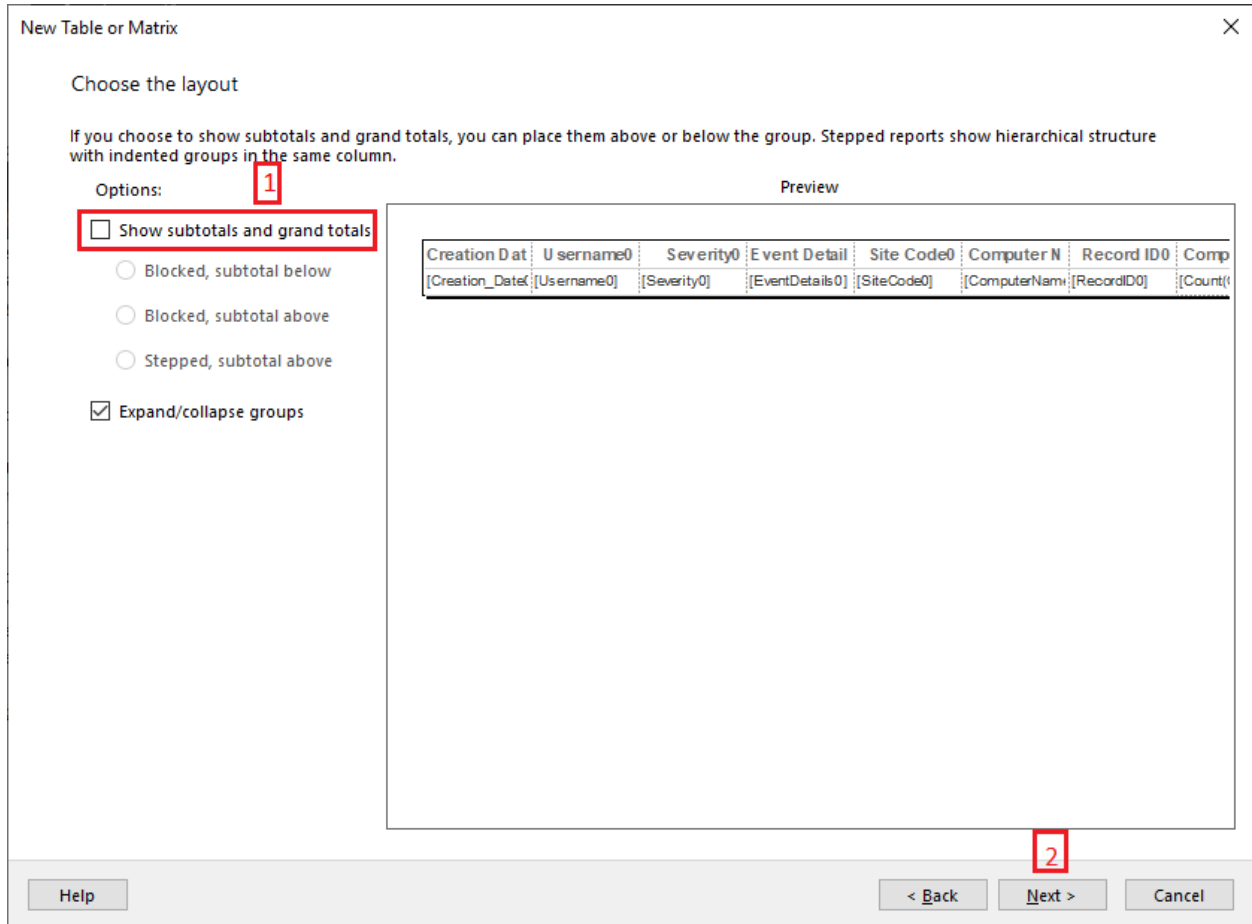


Figure 155: De-selecting "Show subtotals and grand totals" option

## 6.7 Renaming the reports headings

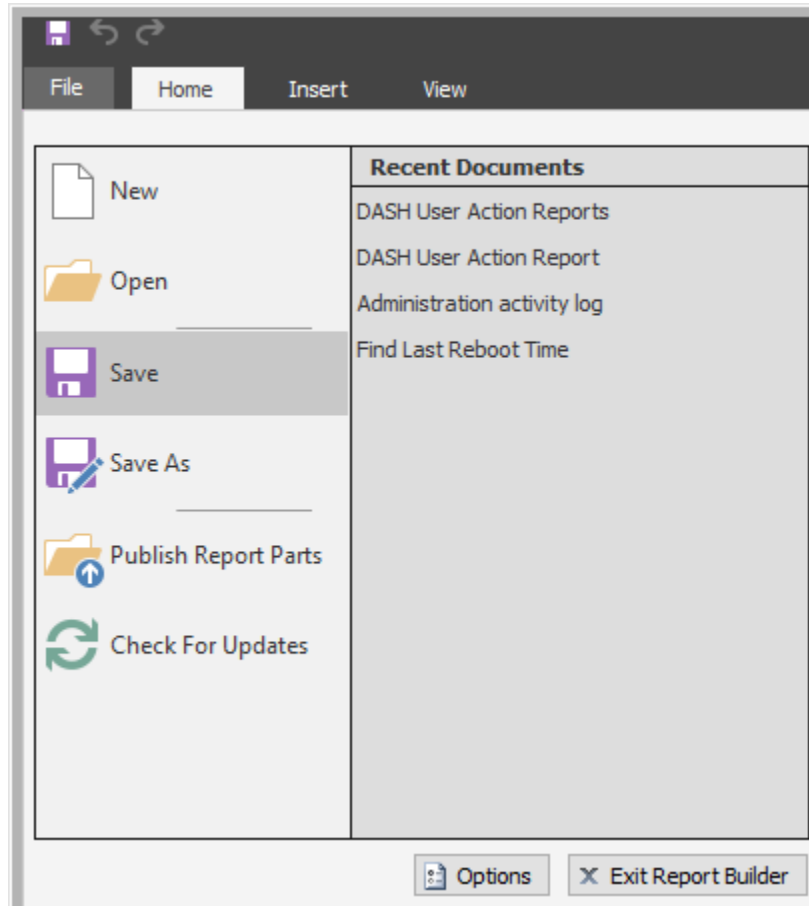
Rename the headings in the Center pane of Microsoft Report Builder as shown in Figure 156 to the following:

- [Creation\_Date0] - > Date Time (UTC)
- [Username0] -> Modified By
- [Severity0] - > Severity
- [EventDetails0] -> Event Details
- [SiteCode0] -> Site Code
- [ComputerName0] -> Resource Name
- [RecordID0] -> Record Id.
- [Count(ComputerName0)] -> Resource Count

Date Time (UTC)	Modified By	Severity	Event Details	Site Code	Resource Nam	Record ID	Resource Count
[Creation_Date0]	[Username0]	[Severity0]	[EventDetails0]	[SiteCode0]	[ComputerName0]	[RecordID0]	[Count(ComputerName0)]

Figure 156: Renaming the headers in the report

Click on “File” menu options and click on “Save” as shown in Figure 157.



**Figure 157: Save menu option in File menu**

## 6.8 Running report in MEM

In MEM navigate to \Monitoring\Overview\Reporting\Reports\DASH Reports

Right click on the “DASH User Action Reports” report and click on Run as shown in Figure 158.

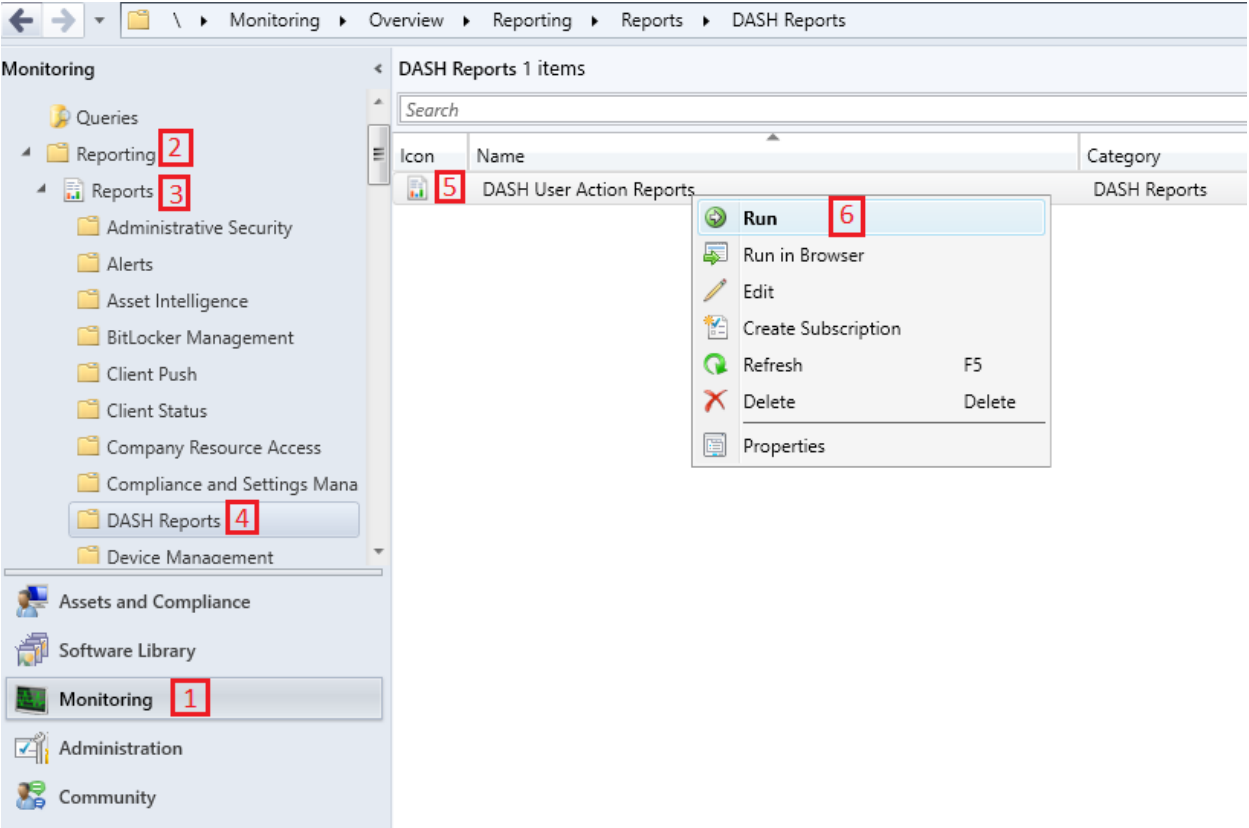
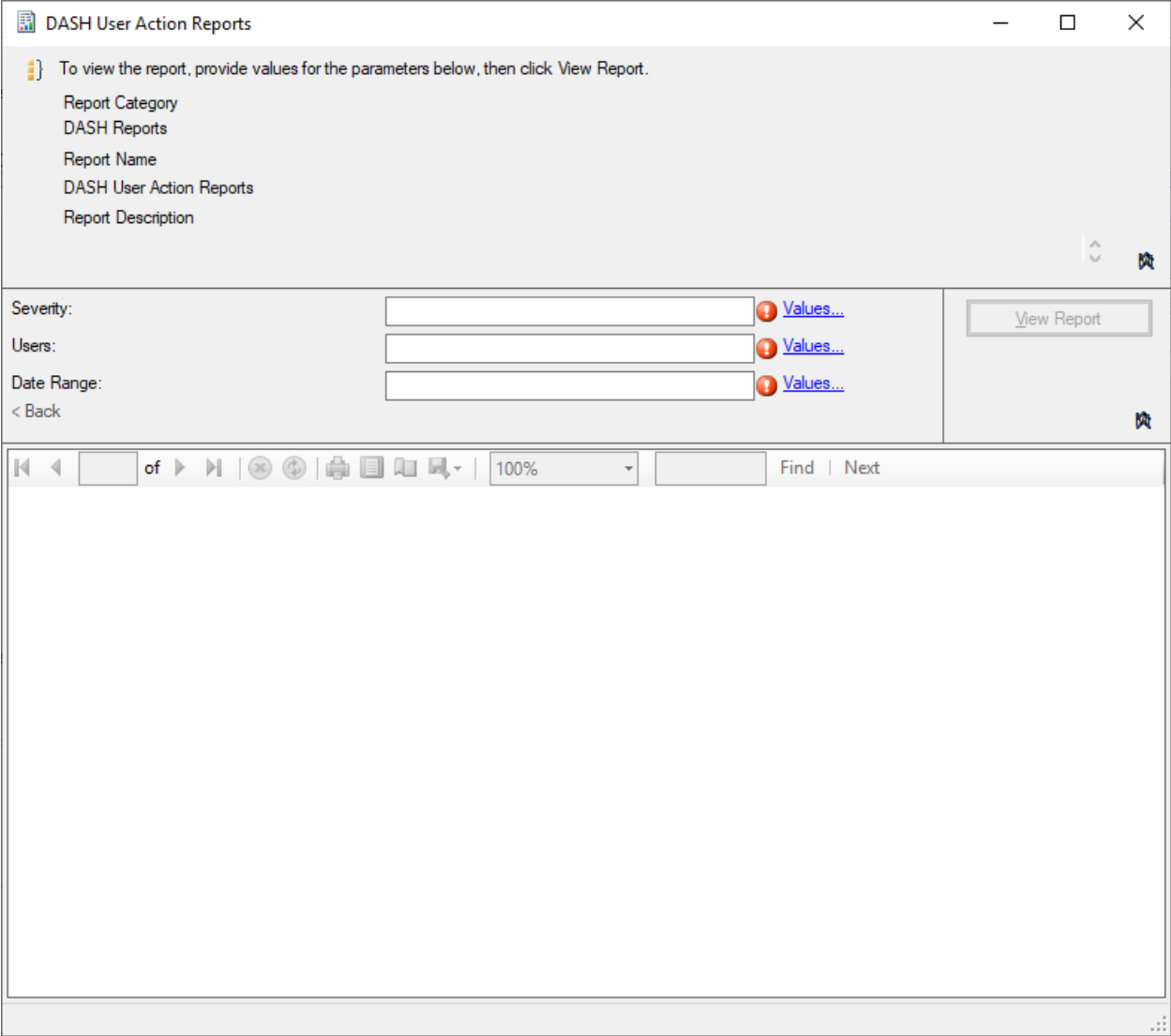


Figure 158: Running the report in MEM

This prompts the window “DASH User Action Reports” as shown in Figure 159, where we need to choose 3 values:  
Severity, Users and Data Range as designed in Microsoft Report Builder.



**Figure 159: DASH User Action Report window**

To choose the values click on the “Values...” link and select the values from the window popup.

- 1) Choose Severity as shown in Figure 160

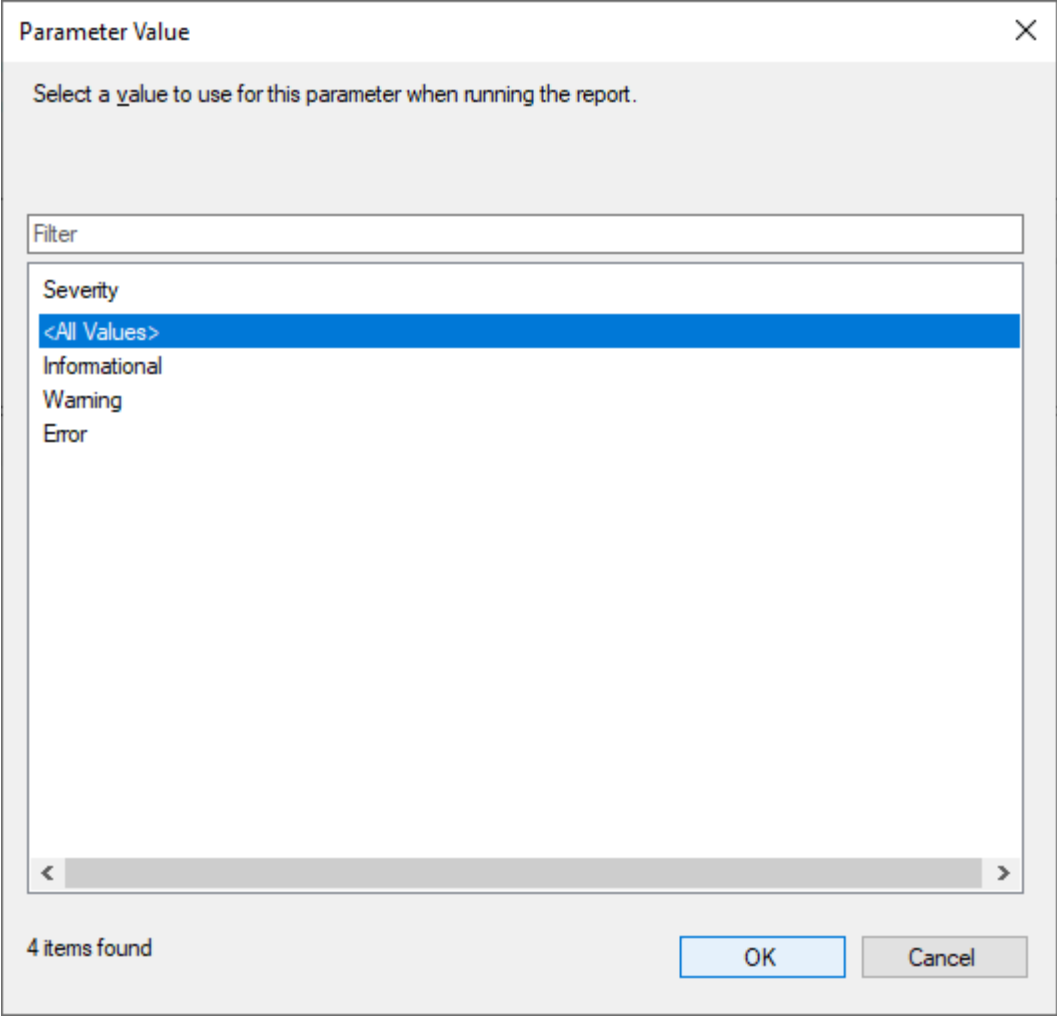


Figure 160: Choosing Severity

2) Choose Users as shown in Figure 161

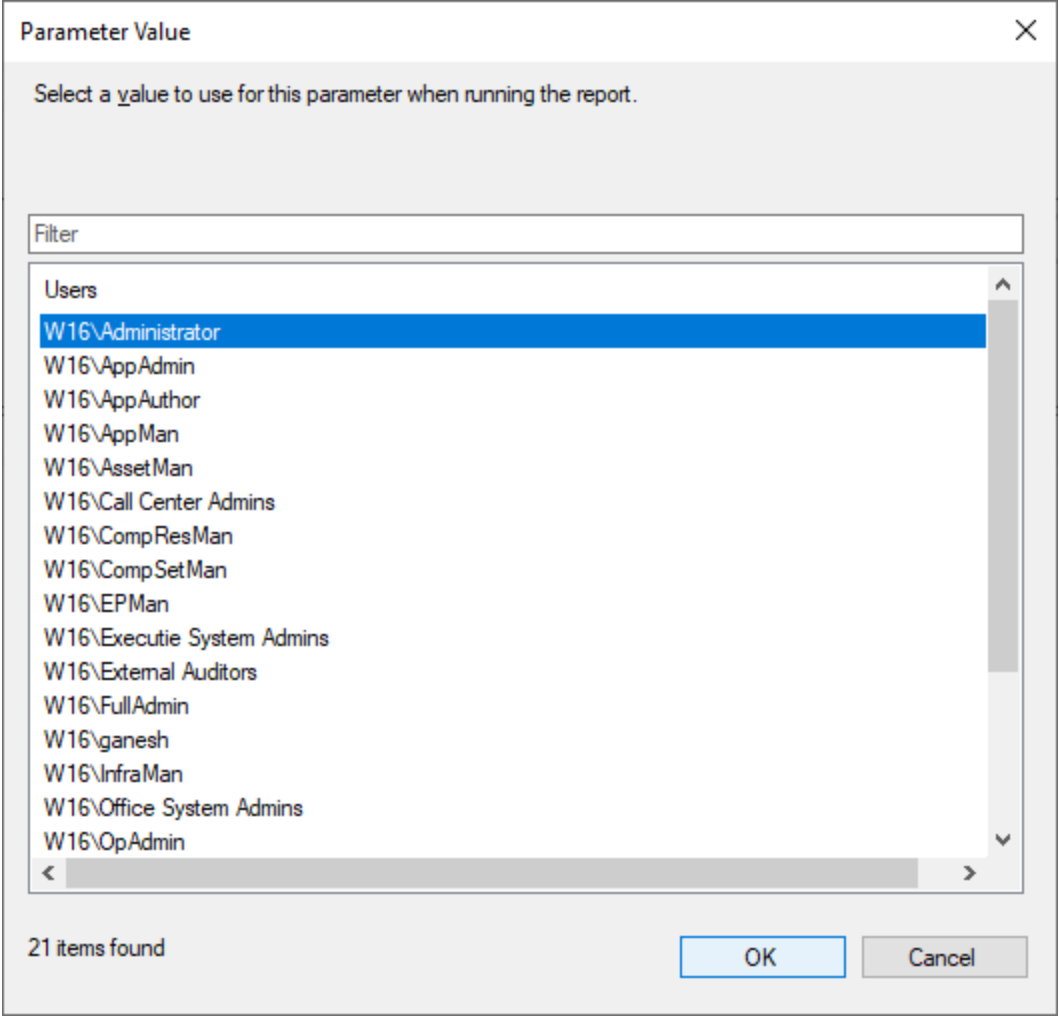
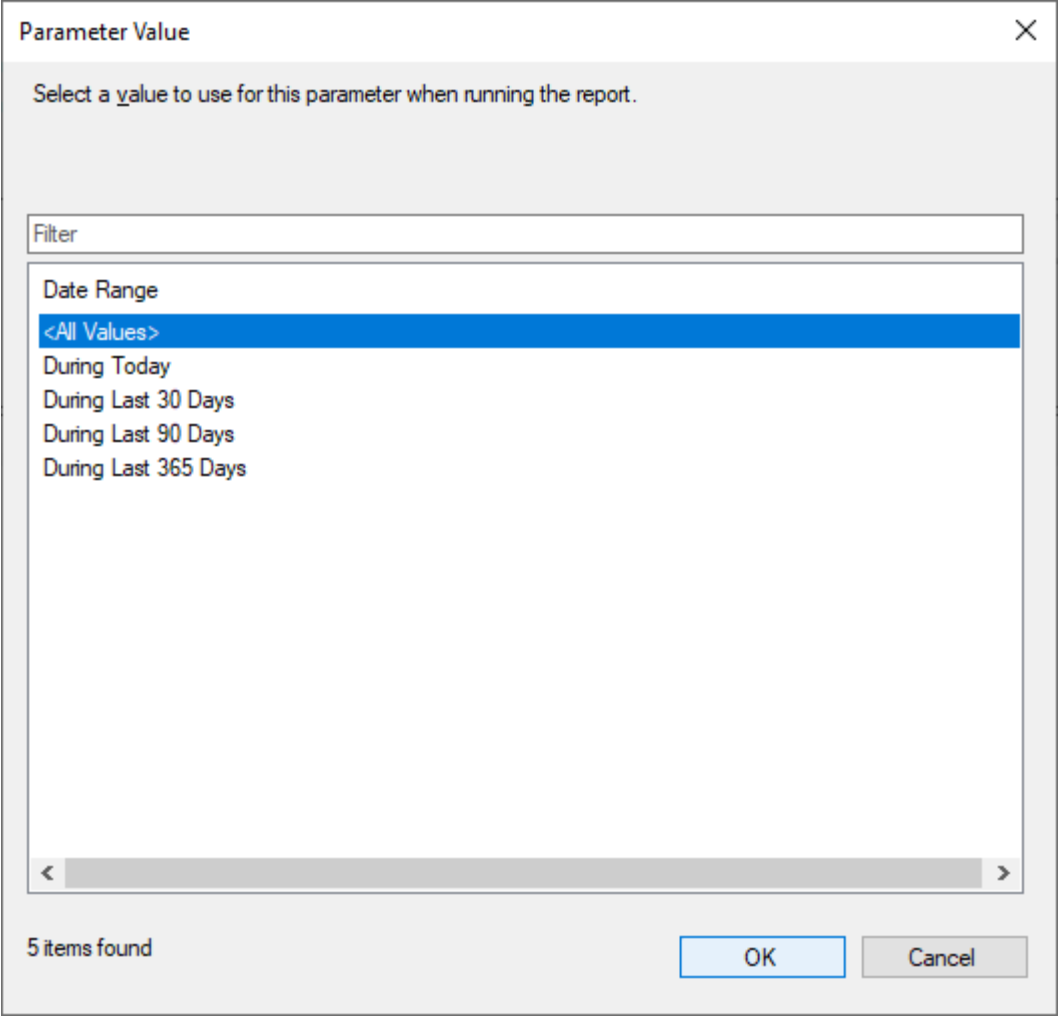


Figure 161: Choosing Users

- 3) Choose Date Range as shown in Figure 162



**Figure 162: Choosing Date Range**

Then click on “View Report” and expand the values in the report as shown in Figure 163.



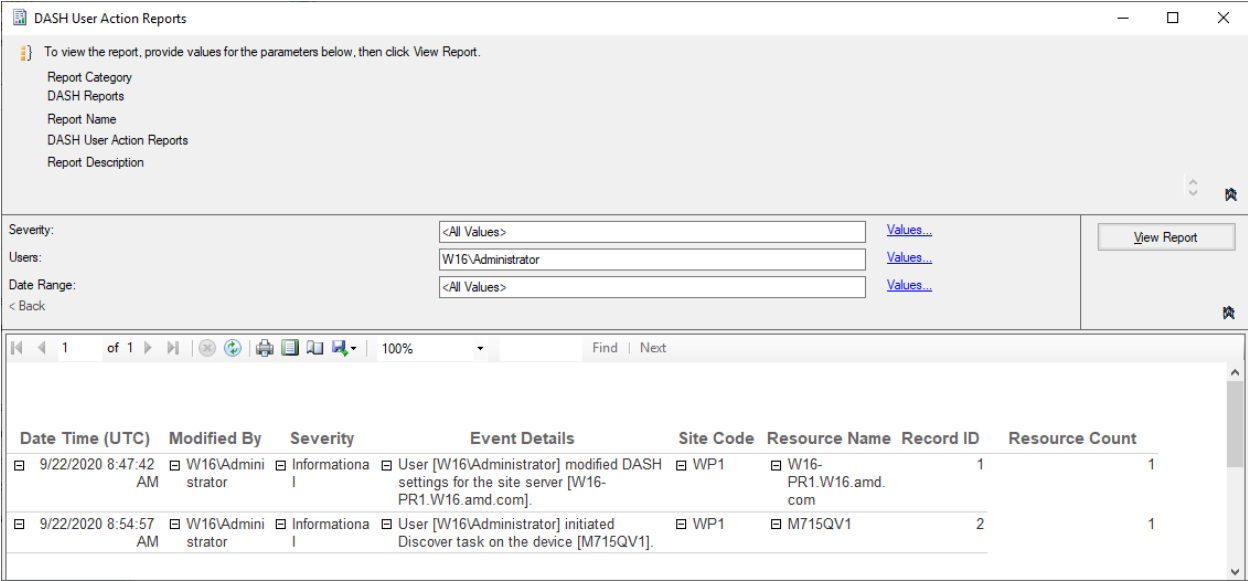


Figure 163: DASH User Action Report with values

## 6.9 Running report in SSRS

In MEM navigate to \Monitoring\Overview\Reporting\Reports\DASH Reports  
Right click on the "DASH User Action Reports" report and click on "Run in Browser" as shown in

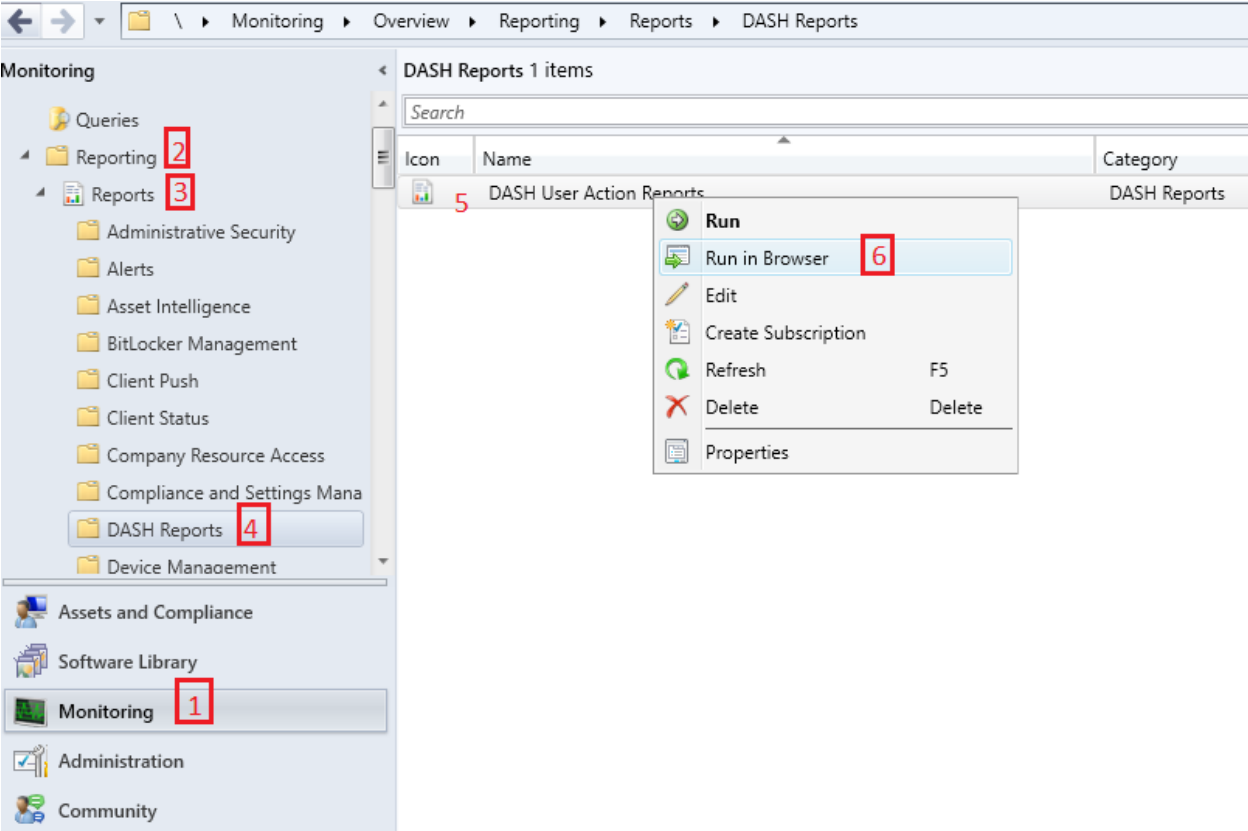
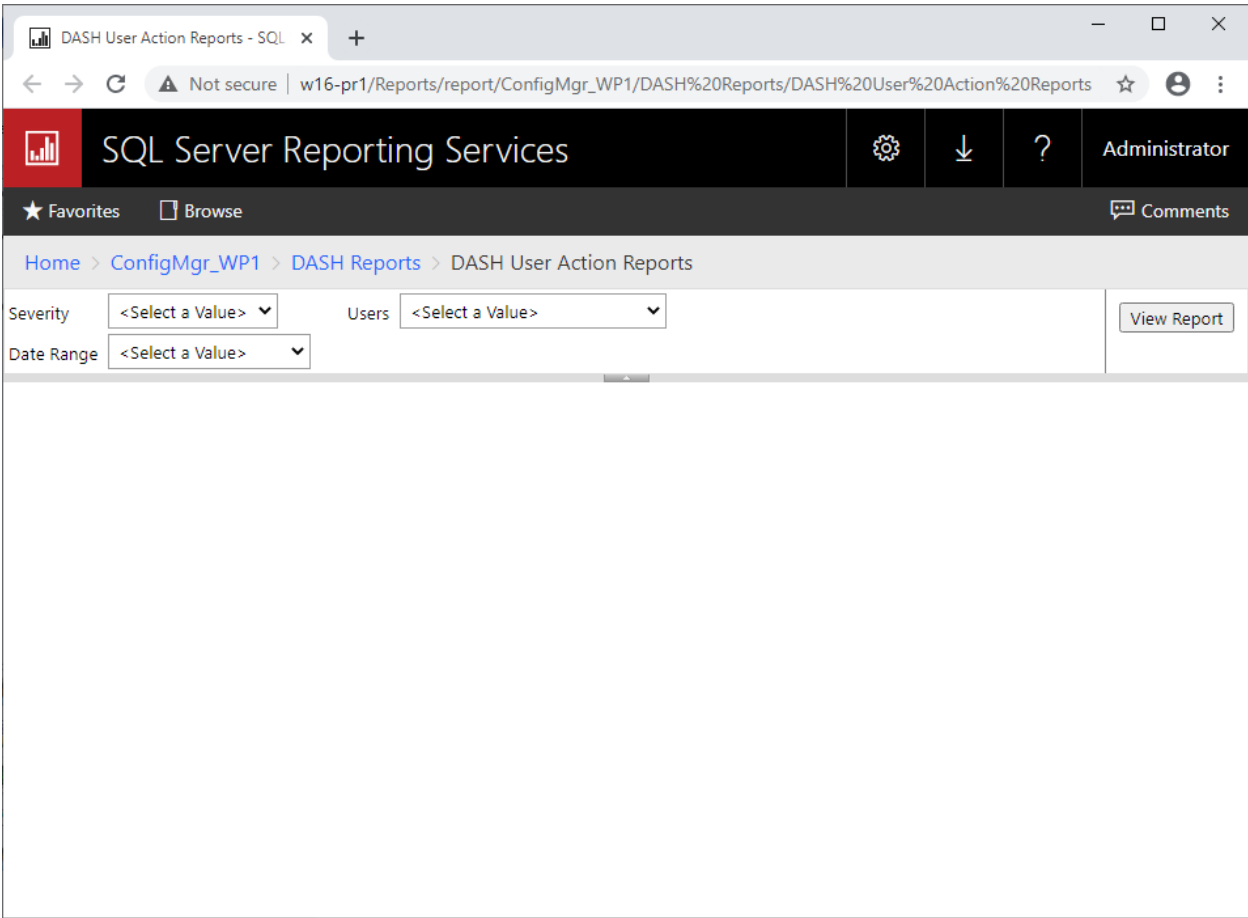


Figure 164: Running Report in SSRS from MEM

This opens the Report in SSRS where user can choose the required values for the 3 fields “Severity”, “Users” and “Date Range” as shown in Figure 165.



**Figure 165: DASH User Action Report in SSRS**

Upon selecting the values and clicking on “View Report”, the report can be viewed in SSRS as shown in Figure 166.

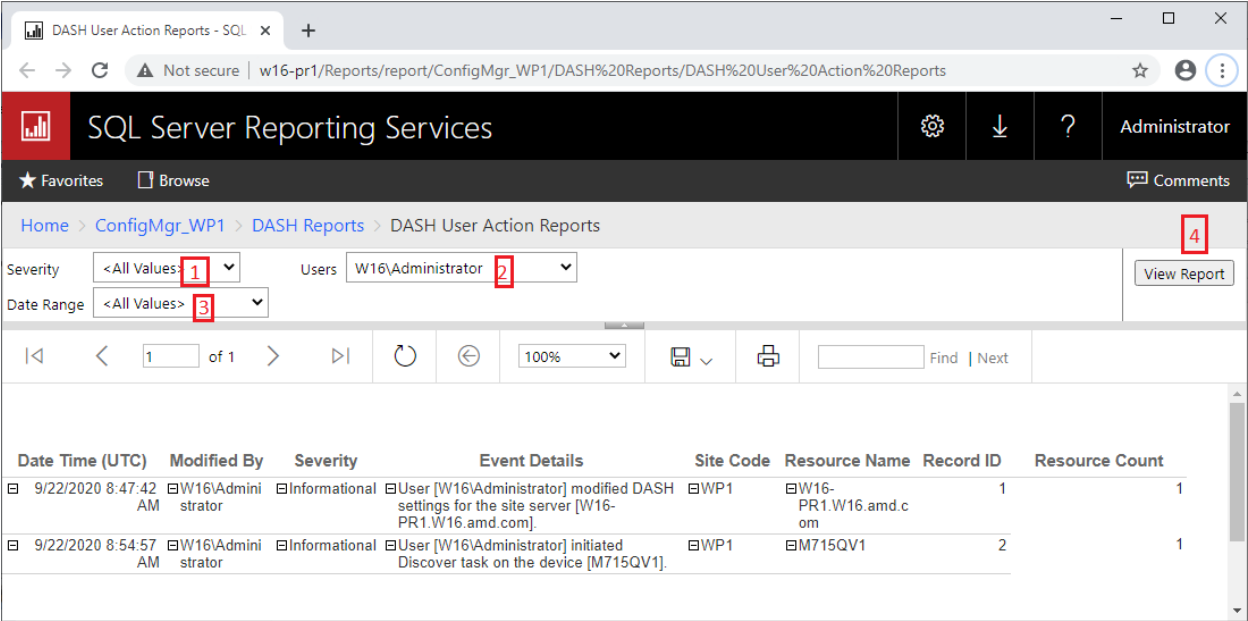


Figure 166: Viewing Report in SSRS

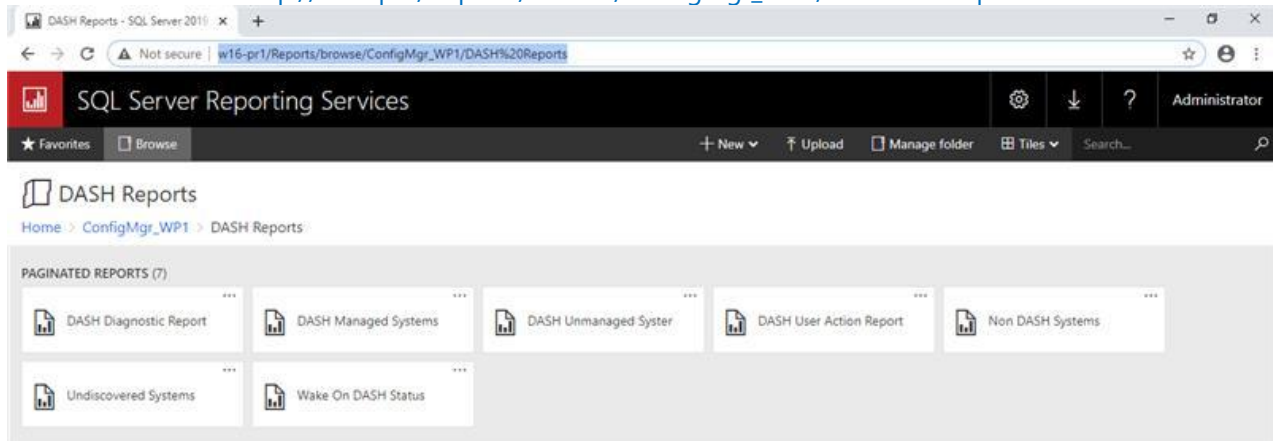
## Chapter 7 DASH Reports

DASH Reports gets deployed in 'DASH Reports' folder to MEM reports while installation of AMPS provided the site server has the role "Reporting services point". It is deployed in following path:

//<reportserver>/Reports/browse/ConfigMgr\_<SiteCode>/DASH Reports

**Eg:** On report server "w16-pr1" with site code "WP1", as shown in Figure 167 the path:

[http://w16-pr1/Reports/browse/ConfigMgr\\_WP1/DASH%20Reports](http://w16-pr1/Reports/browse/ConfigMgr_WP1/DASH%20Reports)



**Figure 167: DASH Reports in SSRS**

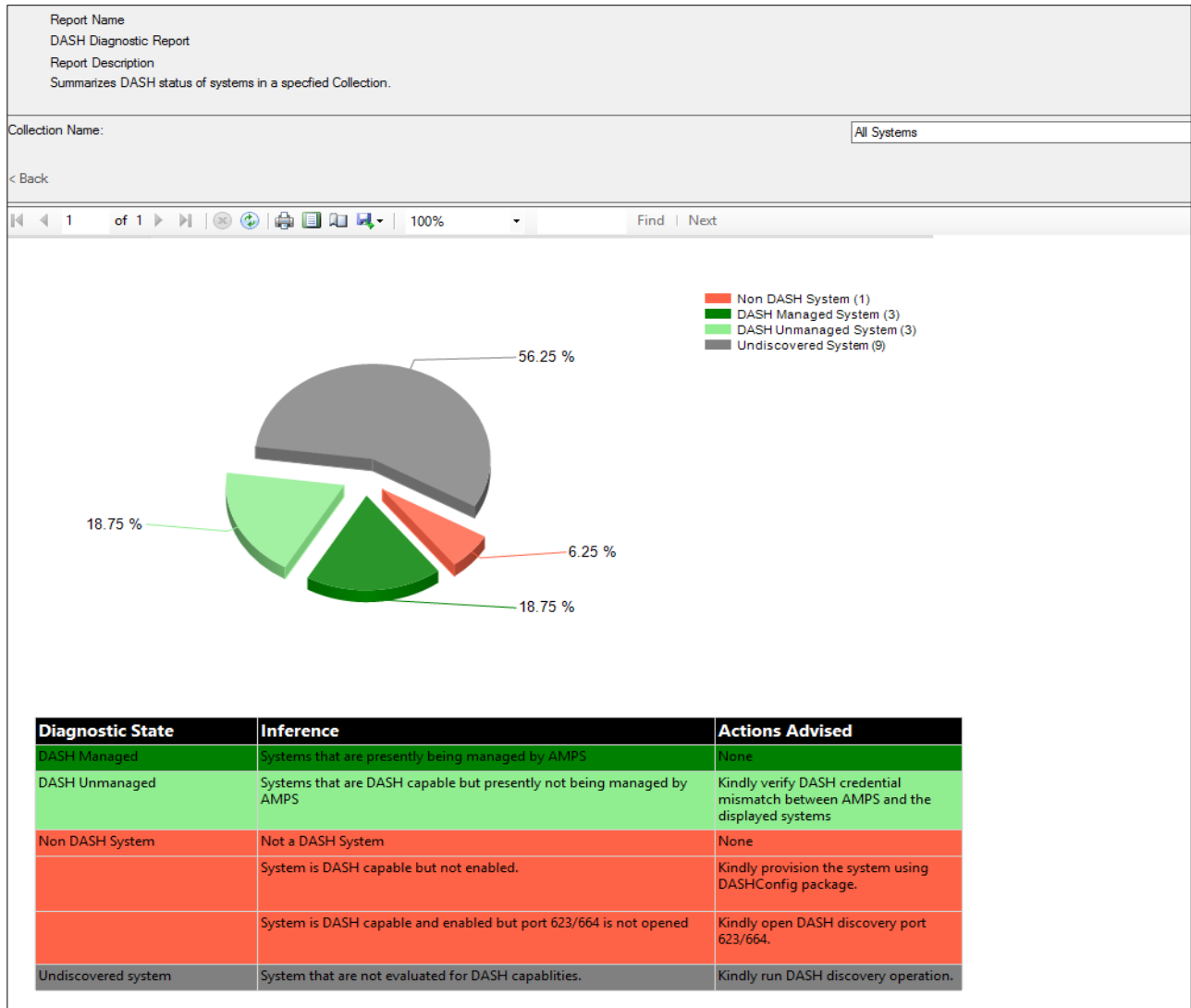
Following reports are available for DASH functionalities:

### 7.1 DASH Diagnostic Report

This report summarizes DASH status of systems in a specified Collection. User needs to provide the collection name for which DASH diagnosis report is to be run.

The systems in the collection are divided into 4 states:

Diagnostic State	Inference	Actions Advised
DASH Managed Systems	Systems that are presently being managed by AMPS.	None
DASH Unmanaged Systems	Systems that are DASH capable but presently not being managed by AMPS.	Verify DASH credential mismatch between AMPS and the displayed systems.
Non DASH Systems	Not DASH Systems.	None
	Systems are DASH capable but not enabled.	Provision the systems using DASHConfig package.
	Systems are DASH capable and enabled but port 623/664 is not opened.	Open DASH discovery port 623/664.
Undiscovered Systems	Systems that are not evaluated for DASH capabilities.	Run DASH discovery operation.



**Figure 168: Diagnostic Report**

## 7.2 DASH Wake On LAN Status Report

This report displays the result of 'DASH Wake on LAN' operation on systems in a specified collection. User needs to provide the collection name for which report is to be run.

The report will provide information on whether DASH Wake Up succeeded on the given device collection. The WOL status can have these values:

- 1) Success
- 2) Failed
- 3) Unknown (WOL may not have been enabled for this collection)

'WAKE ON DASH' Status of systems in a specified collection					
Description					
Name	Collection ID	Last WOL Time	WOL Status	Site Code	DASH Status
BL-IN-QAT1-61	P010000C	8/29/2016 9:59:17 AM	SUCCESS	P01	DASH MANAGED
BL-IN-QAT1-51	P010000C	8/29/2016 9:59:17 AM	FAILED	P01	DASH UNMANAGED
SYSMAN-BIANCHI	P010000C	8/24/2016 12:11:57 PM	FAILED	P01	DASH MANAGED
SYSMAN705-SFF	P010000C	8/29/2016 9:59:17 AM	SUCCESS	P01	DASH MANAGED
INTELSYSTEM	P010000C	8/29/2016 9:59:17 AM	FAILED	P01	DASH UNMANAGED
BL-IN-QAT1-56	P010000C	8/29/2016 9:59:17 AM	FAILED	P01	DASH UNMANAGED

Figure 169: DASH Wake on LAN Status Report

## 7.3 DASH Managed Systems Report

This report runs from Diagnostic report when user clicks on 'DASH Managed' pie slice. It displays the systems that are presently being managed by AMPS in a specified collection.

If this report is run independently, it displays the managed systems from 'All systems' collection.

The systems displayed in the result are fully configured for DASH. All DASH tasks were executed and completed successfully.

Managed DASH systems of specified collection			
Description			
This report displays systems that are presently being managed by AMPS			
Host Name	Collection ID	Computer Domain	Site Code
HP5850	SMS00001	W16	WP1
HP705G4-4	SMS00001	W16	WP1
M715QV1	SMS00001	W16	WP1
DEV-MAJA	SMS00001	W16	WP1

Figure 170: DASH Managed Systems Report

## 7.4 DASH Unmanaged Systems Report

This report runs from Diagnostic report when user clicks on 'DASH Unmanaged' pie slice. It displays systems which are DASH capable but presently not being managed by AMPS because of credential mismatch. If this report is run independently, it displays the unmanaged systems from 'All systems' collection.

The systems listed in this report might have to be provisioned again. For provisioning refer section Appendix 9.1.

Unmanaged DASH systems of specified collection			
Description			
Host Name	Collection ID	Computer Domain	Site Code
INTELSYSTEM	SMS00001	TEST	P01
BL-IN-QAT1-56	SMS00001	TEST	P01
BL-IN-QAT1-51	SMS00001	TEST	P01

Figure 171: DASH Unmanaged Systems Report

## 7.5 DASH Non DASH Systems Report

This report runs from Diagnostic report when user clicks on 'Non-DASH' pie slice. It displays systems which are not recognized by AMPS as DASH systems. If this report is run independently, it displays the non DASH systems from 'All systems' collection.

The systems in the result of this report are either

1. Non DASH supported systems
2. If DASH supported systems, DASH option might not have been enabled in the BIOS

Non DASH systems of specified collection			
Description			
Host Name	Collection ID	Computer Domain	Site Code
LM79	SMS00001		P01

Figure 172: DASH Non DASH Systems Report

## 7.6 DASH Undiscovered Systems Report

This report runs from Diagnostic report when user clicks on 'Undiscovered' pie slice. It displays systems that are not yet evaluated for DASH capabilities. If this report is run independently, it displays the undiscovered systems from 'All systems' collection.

For the systems in the result, AMPS has not yet run DASH discovery on systems. Discovery must be scheduled on these systems.

DASH Undiscovered systems of specified collection

☐ Description

This report displays systems that are not yet evaluated for DASH capabilities.

Host Name	↕	Collection ID	Domain	Site Code
Provisioning Device (Provisioning Device)		SMS00001	Provisioning Device (Provisioning Device)	
x86 Unknown Computer (x86 Unknown Computer)		SMS00001	x86 Unknown Computer (x86 Unknown Computer)	WP1
x64 Unknown Computer (x64 Unknown Computer)		SMS00001	x64 Unknown Computer (x64 Unknown Computer)	WP1
10.138.143.254		SMS00001		
10.136.5.254		SMS00001		

Figure 173: DASH Undiscovered Systems Report

## 7.7 DASH Memory Report

The report shows a consolidated DASH Memory Inventory of DASH systems. Users of AMPS can generate other reports of DASH inventory.

DASH Memory Report				
System Name	Resource ID	Element Name	Available Memory	Total Memory
DEV-MAJA	16777238	L1 - Cache	512 KB	512 KB
		L2 - Cache	4 MB	4 MB
		L3 - Cache	8 MB	8 MB
		Total System Memory:	0 16 GB	16 GB
HP5850	16777235	CPU #1 L1 Cache		256 KB
		CPU #1 L2 Cache		1 MB
		CPU #1 L3 Cache		0 bytes
		Total System Memory	767 MB	1 GB
HP705G4-4	16777236	L1 - Cache	384 KB	384 KB
		L2 - Cache	2 MB	2 MB
		L3 - Cache	4 MB	4 MB
		Total System Memory:	0 16 GB	16 GB
M715QV1	16777237	Cache	0 bytes	0 bytes
		Total System Memory:	0 0 bytes	0 bytes

Figure 174: DASH Memory Inventory Report



# Chapter 8      AMPS Status Monitoring

AMPS Status message in Monitoring category of MEM allows user to view all logged messages for the actions performed by user.

## 8.1 All AMPS Status Messages

To view 'All AMPS Status Messages', perform the following steps:

- 1. Expand the **Monitoring** node.
- 2. Expand **System Status** node.
- 3. Select **Status Message Queries**.
- 4. Click the **Show Message** of **All AMPS Status Message** ribbon icon as shown in Figure 175.
- 5. Provide **<Time>** parameter to view messages as shown in Figure 176.

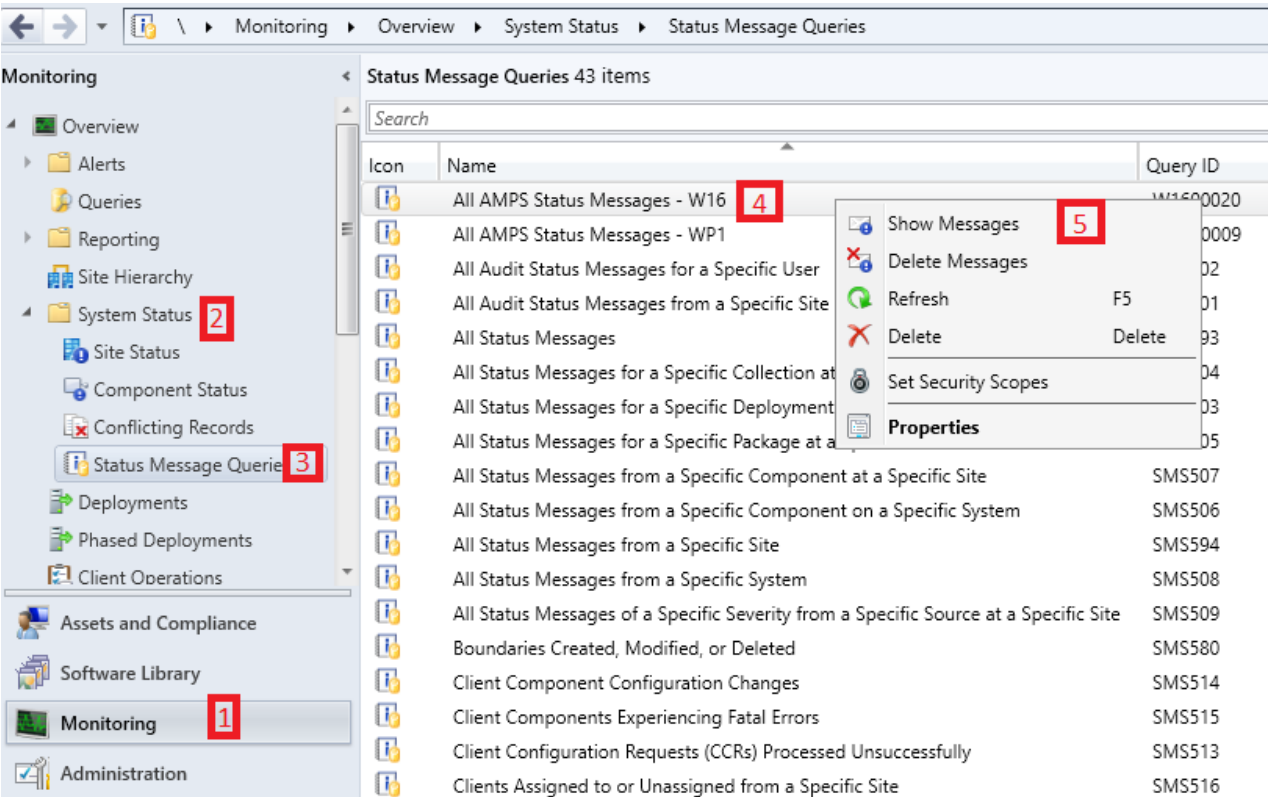


Figure 175: All AMPS Status Messages Queries

All AMPS Status Messages

Select each name in the prompted value list and specify the value before executing the query.

Prompted value:

Name	Value
Time	<Unresolved>

Value

Specify date and time:

12-10-2020

19:19:48

(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Select date and time:

12 hours ago

OK

Cancel

Figure 176: Select Date and Time for AMPS Status Messages

Configuration Manager Status Message Viewer for <WP1> <W16 CAS Setup>

File Edit View Help

All AMPS Status Messages

Severity	Type	Site code	Date / Time	System	Component	Me...	Description
	Milestone	WP1	12-10-2020 16:45:46	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'M715QV1'.
	Milestone	WP1	12-10-2020 16:45:31	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <M715QV1>.
	Milestone	WP1	12-10-2020 16:45:21	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'HP705G4-4'.
	Milestone	WP1	12-10-2020 16:45:07	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <HP705G4-4>.
	Milestone	WP1	12-10-2020 16:42:05	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'HP5850'.
	Milestone	WP1	12-10-2020 16:41:55	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <HP5850>.
	Milestone	WP1	12-10-2020 13:37:29	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <M715QV1>.
	Milestone	WP1	12-10-2020 13:37:24	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'HP705G4-4'.
	Milestone	WP1	12-10-2020 13:37:10	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <HP705G4-4>.
	Milestone	WP1	12-10-2020 13:37:03	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'HP5850'.
	Milestone	WP1	12-10-2020 13:36:53	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <HP5850>.
	Milestone	WP1	12-10-2020 13:36:26	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'DEV-MAJA'.
	Milestone	WP1	12-10-2020 13:36:15	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <DEV-MAJA>.
	Milestone	WP1	12-10-2020 13:35:50	W16-PR1.W16.amd.com	AMPS	39997	'HP5850' is Managed DASH capable.
	Milestone	WP1	12-10-2020 13:35:48	W16-PR1.W16.amd.com	AMPS	39997	'DEV-MAJA' is Managed DASH capable.
	Milestone	WP1	12-10-2020 13:26:08	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated Discover on the collection <All Systems>.
	Milestone	WP1	12-10-2020 13:26:08	W16-PR1.W16.amd.com	AMPS	39997	'Discover' occurs one time at 2020-10-12 01:35 PM" is scheduled successfully on collection 'SMS00001'.
	Milestone	WP1	12-10-2020 13:24:52	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> modified DASH settings for the site server <W16-PR1.W16.amd.com>.
	Milestone	WP1	12-10-2020 13:24:51	W16-PR1.W16.amd.com	AMPS	39997	DASH Configuration was updated successfully.
	Milestone	WP1	12-10-2020 13:24:51	W16-PR1.W16.amd.com	AMPS	39997	DASH authentication list was updated successfully.
	Milestone	WP1	12-10-2020 12:31:50	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'HP705G4-4'.
	Milestone	WP1	12-10-2020 12:31:24	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <HP705G4-4>.
	Milestone	WP1	12-10-2020 12:29:18	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'DEV-MAJA'.
	Milestone	WP1	12-10-2020 12:29:07	W16-CAS.W16.AMD.COM	AMPS	39997	User <W16\Administrator> initiated inventory on the device <DEV-MAJA>.
	Milestone	WP1	12-10-2020 11:51:07	W16-PR1.W16.amd.com	AMPS	39997	Inventory is completed on 'M715QV1'.

All AMPS Status Messages : 46 of 46 messages displayed. 1 selected.

Figure 177: All AMPS Status Messages

# Chapter 9      Appendix

---

For more information about the AMPS please go over this section

## 9.1 Provisioning

Refer section 2.4.2 in ActiveDirectoryConfiguration\_for\_MEM.pdf document.

## 9.2 Using self-signed certificates for HTTPS communication

Refer the document 'DASHCertificates.pdf' in the 'doc' folder of AMPS installation.

## 9.3 Discussion forum link

More details about AMPS features and AMPS updates can be found in:

Link: <http://www.amd.com/DASH>

## 9.4 Active Directory Configuration Documents

AMPS installation comes with 2 separate documents for active directory configuration.

1. ActiveDirectoryConfiguration\_for\_MEM.pdf
2. ActiveDirectoryConfiguration\_for\_SCCM.pdf

## 9.5 DASH support email

For your AMPS queries /feature request please write to our support email

Email: [dashsupport@amd.com](mailto:dashsupport@amd.com)

*Note: AMPS is based on the DMTF DASH specification. Some commands might not be supported by a given platform. Check the platform documentation on the DASH support.*