AMD

AMPS 3.0 User Guide

AMD Management Plugin for SCCM

Issue Date: March 2016

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

Table of Contents

Table of Figures

Abbreviations

- **DASH: D**esktop and Mobile **A**rchitecture for **S**ystem **H**ardware.
  A DASH Capable System is a computer system that conforms to the DMTF DASH standards.
  The DMTF client management standard produced by DMTF specifies the transport, management protocol (WS-Man), and DMTF CIM profiles that are used to manage desktop/mobile PC.
- **DMTF: D**istributed **M**anagement **T**ask **F**orce.
  This is the industry y organization developing system management standards such as DASH and WS-Management.
- **MC**: **M**anagement **C**ontroller.
- **SCCM**: **S**ystem **C**enter **C**onfiguration **M**anager.
- **AMPS**: AMD Management Plugin for SCCM. This is also synonymously referred to as SCCM Plugin or Plugin in this document.

Notations Used

Notations	Description
DASH MC	The MC that implements the external DASH protocol stack. It interfaces with other platform components (BIOS, SB, and IMDs) to get needed information or control the platform.
Out-of-band management	Management tasks that are performed independent of the power or OS state on the managed client or system.

Revision History

Date	Revision	Description
February 4th, 2016	1.5	Content for 3.0 Release
October 26th , 2015	1.4	Content for 2.5 Release
June 10th , 2015	1.3	Content for 2.3 Release
February 23rd, 2015	1.2	Content for 2.2 Release
September 23rd, 2014	1.1	Content for 2.1 Release
August 08th, 2014	1.0	Content for 2.0 Release
July 25th, 2014	0.8	Contents for beta
July 5th 2014	0.5	First draft

Chapter 1 Introduction

This document describes features and usages of the AMPS v3.0 - AMD Management plugin for System Center Configuration Manger (SCCM). AMPS v3.0 supports SCCM 2012/SCCM 2012 R2.

1.1 Architecture Overview

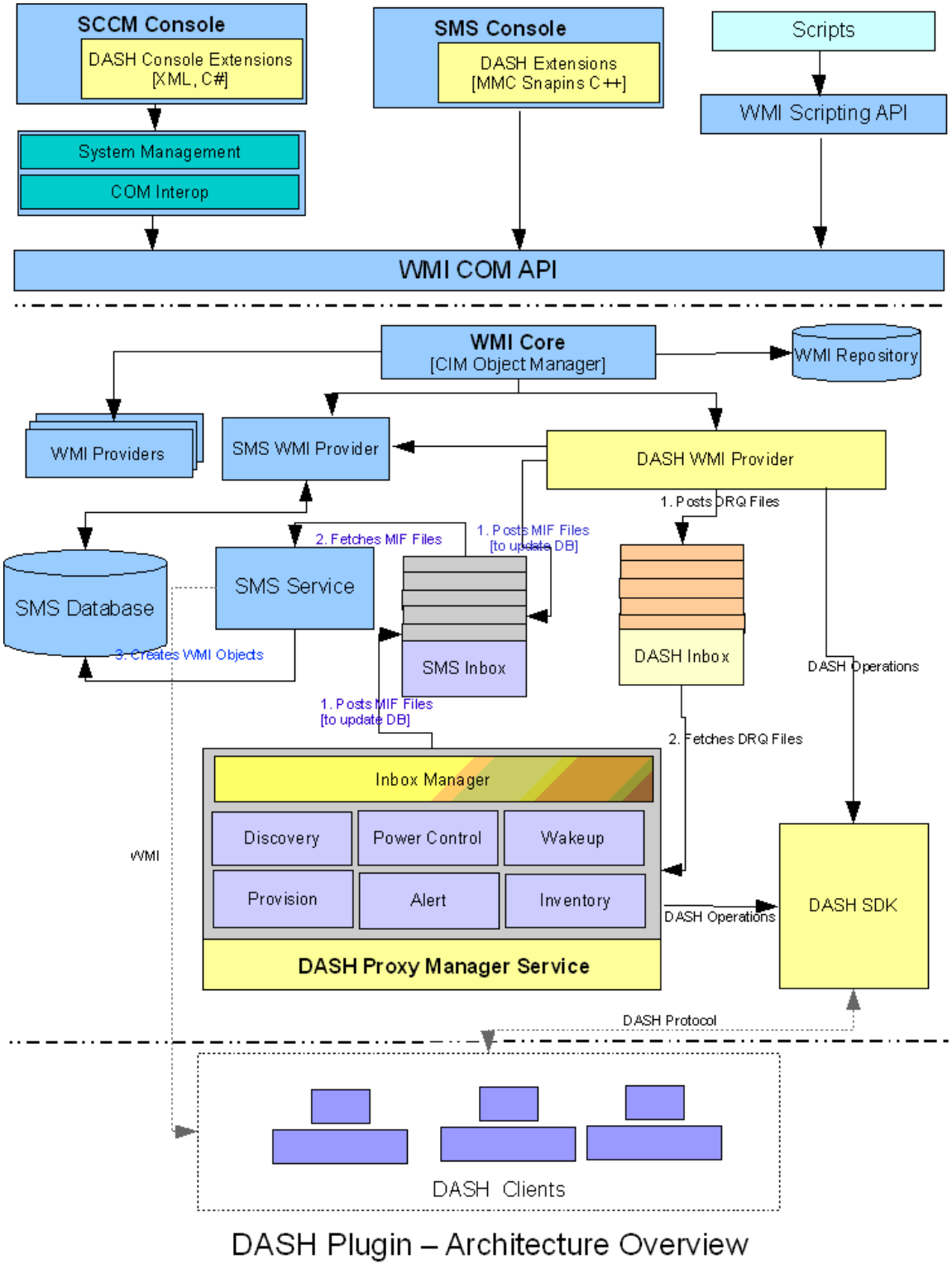
The AMPS 3.0 is a plugin for SCCM 2012. It allows SCCM 2012 users to remotely manage client systems that support the DMTF DASH standard irrespective of the state of the clients OS.

The plugin v3.0 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.
- Record Log
- Alert subscription and reception.
- Scheduled Power Control on a collection.
- Boot Text Image

The architectural overview of the DASH plugin for SCCM 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.



DASH Plugin – Architecture Overview

Figure 1-1: AMPS Architectural Overview

1.2 Prerequisites and System Requirements

The prerequisites to install Microsoft SCCM 2012 are:

- System Center Configuration Manager 2012/2012 R2 must be installed.
- The Site server must be configured.

For information on the hardware and software requirements, refer to the following web location: *http://technet.microsoft.com/en-us/library/dn281925.aspx*

1.3 Installing and Un-installing AMPS

You can deploy AMPS in three possible scenarios.

- **AMPS with SCCM Console and Standalone Site Server**: In this scenario, the SCCM Site server and the console are on the same system. Install AMPS on this system that has both the Site server and console.
- **AMPS with SCCM Console:** In this scenario, the SCCM site server and SCCM console are on two different systems. Therefore, you need to install AMPS twice, once on the site server system and once on the SCCM 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 severs 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.

Alternatively,

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

1.4 Using the AMPS Features

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

AMPS provides the following features:

- Configure SCCM 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 SCCM console, first install it to the primary site.

1.4.1 Accessing the DASH Configuration node

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

1. In the **System Center 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 1-2 illustrates these steps.

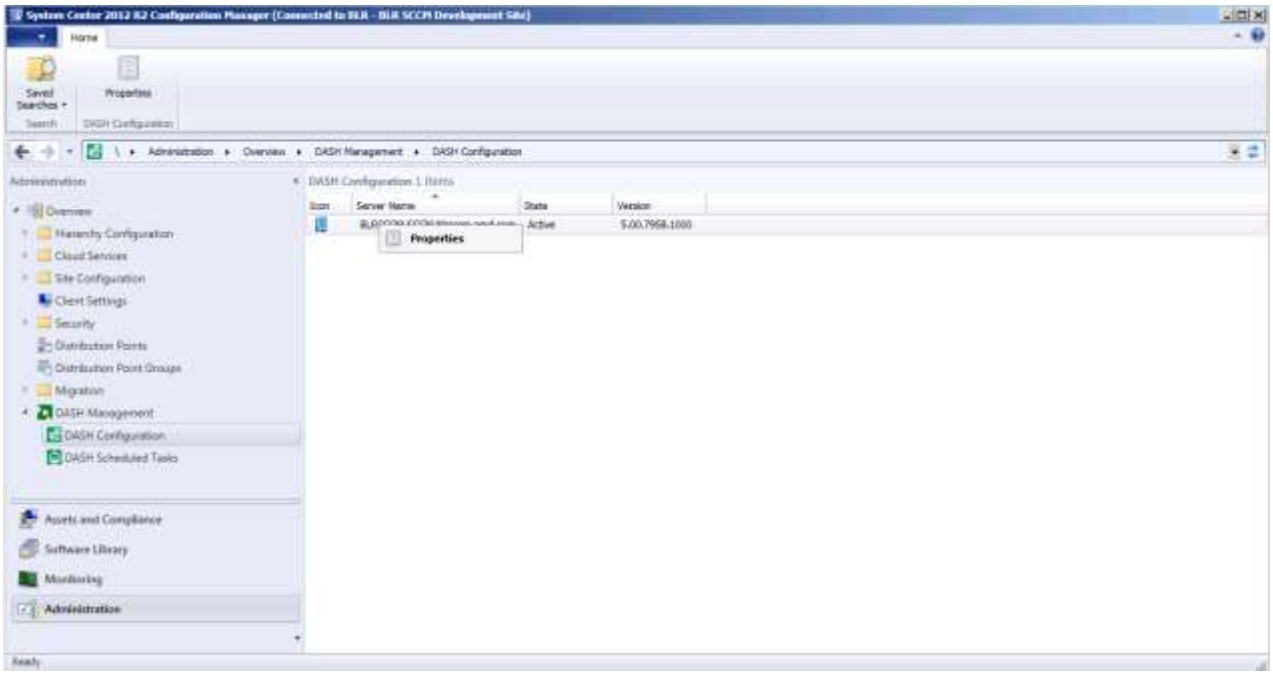


Figure 1-2: Configure SCCM for DASH operations

1.4.2 Accessing the DASH Scheduled Tasks node

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

1. In the **System Center 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 1-3 illustrates these steps.

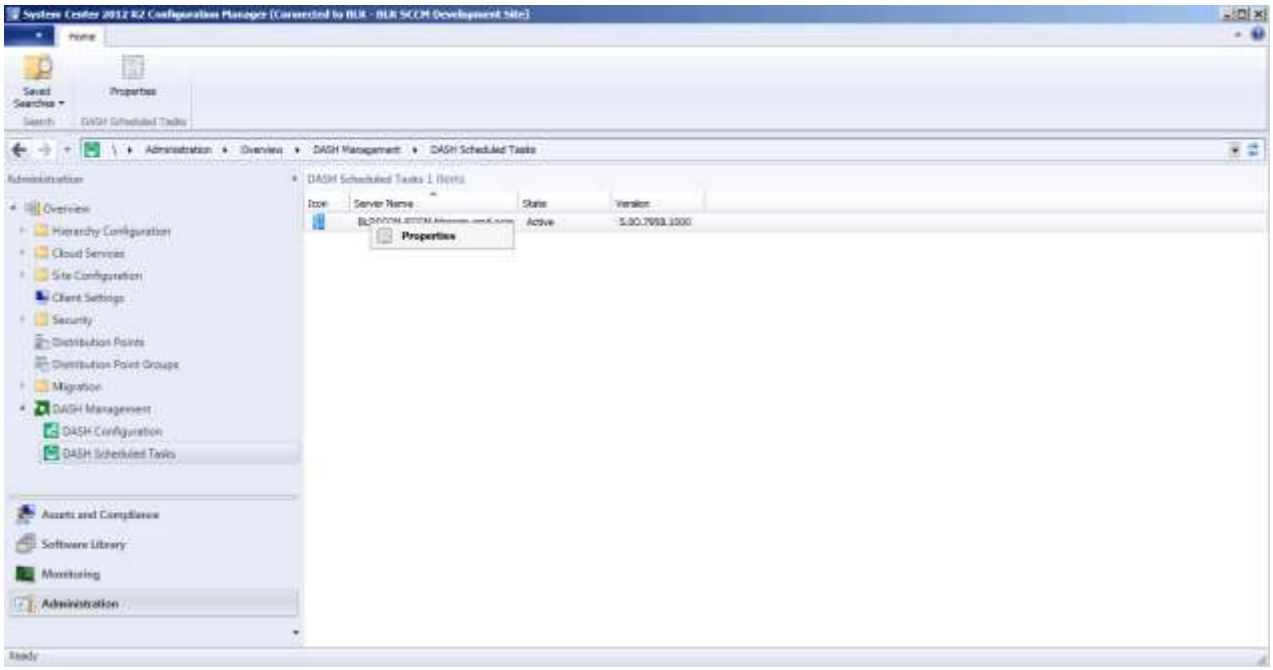


Figure 1-3: DASH Scheduled Tasks Node

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 **System Center 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 1-4 illustrates the steps mentioned above.

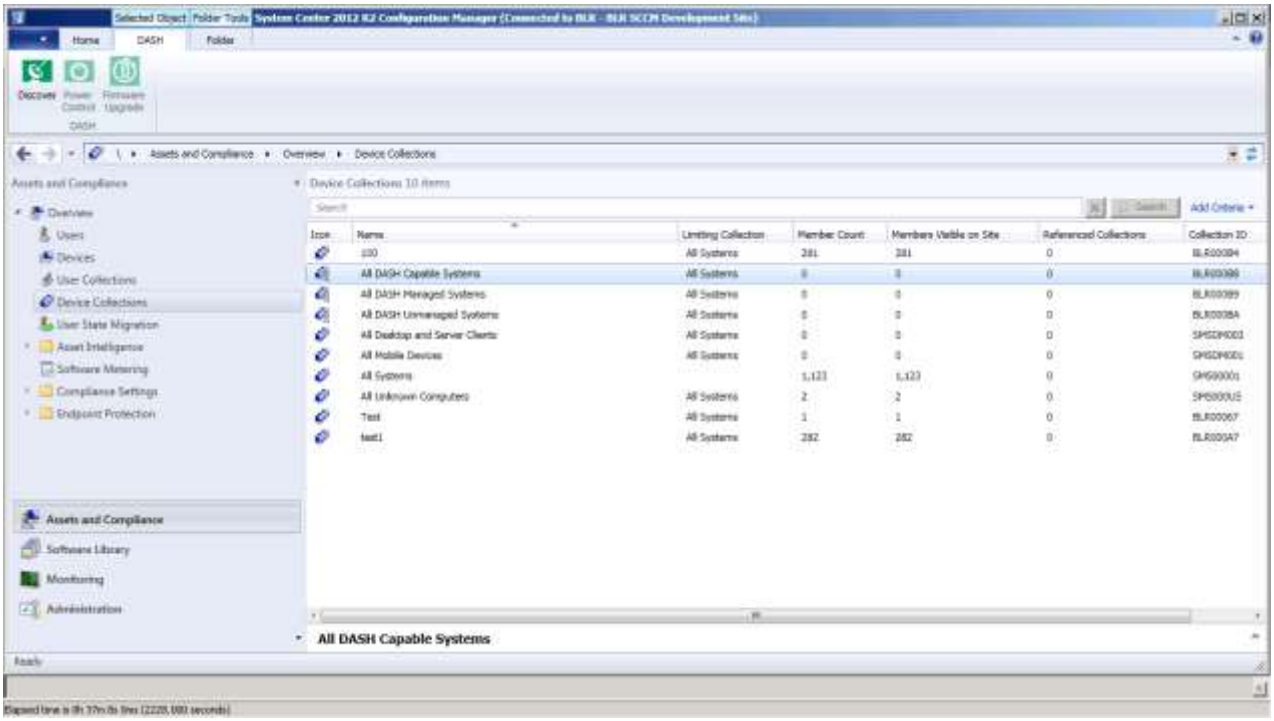


Figure 1-4: All DASH Capable Systems Node

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 **System Center 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 1-5 illustrates the steps mentioned above.

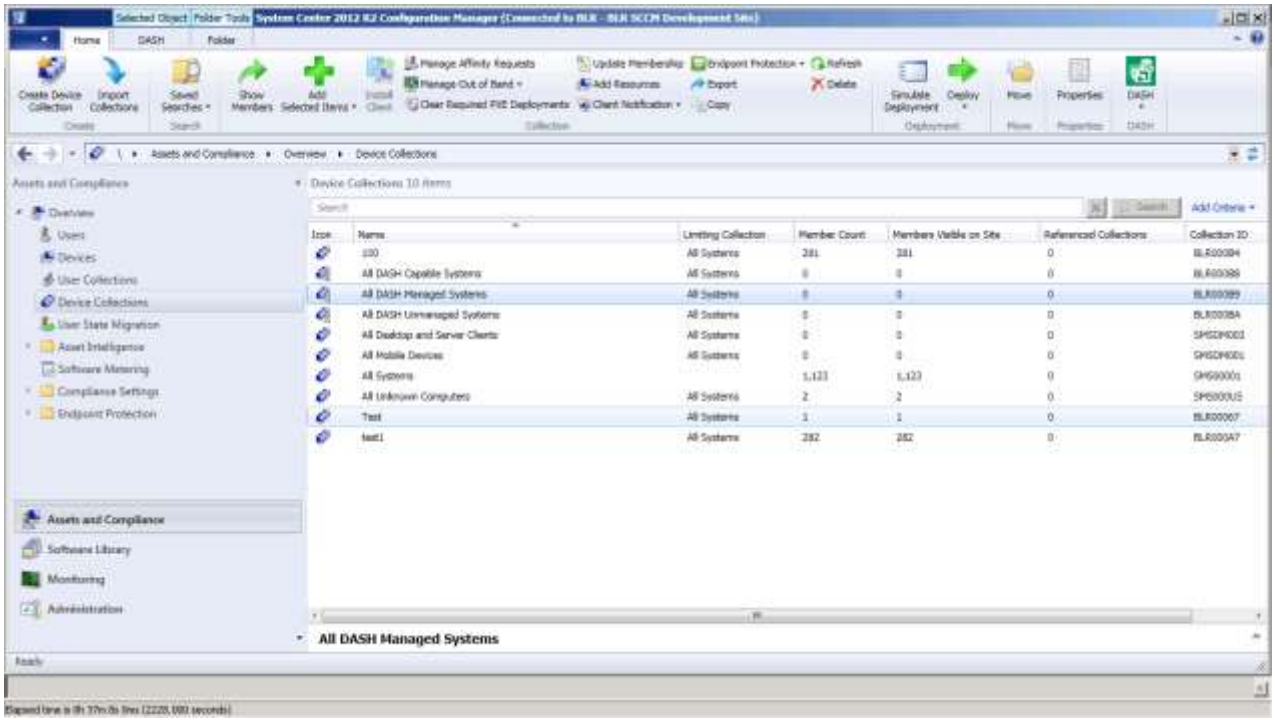


Figure 1-5: All DASH Managed Systems Node

1.4.5 Accessing the All DASH Unmanaged Systems node

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

1. In the **System Center 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 1-6 illustrates the steps mentioned above.

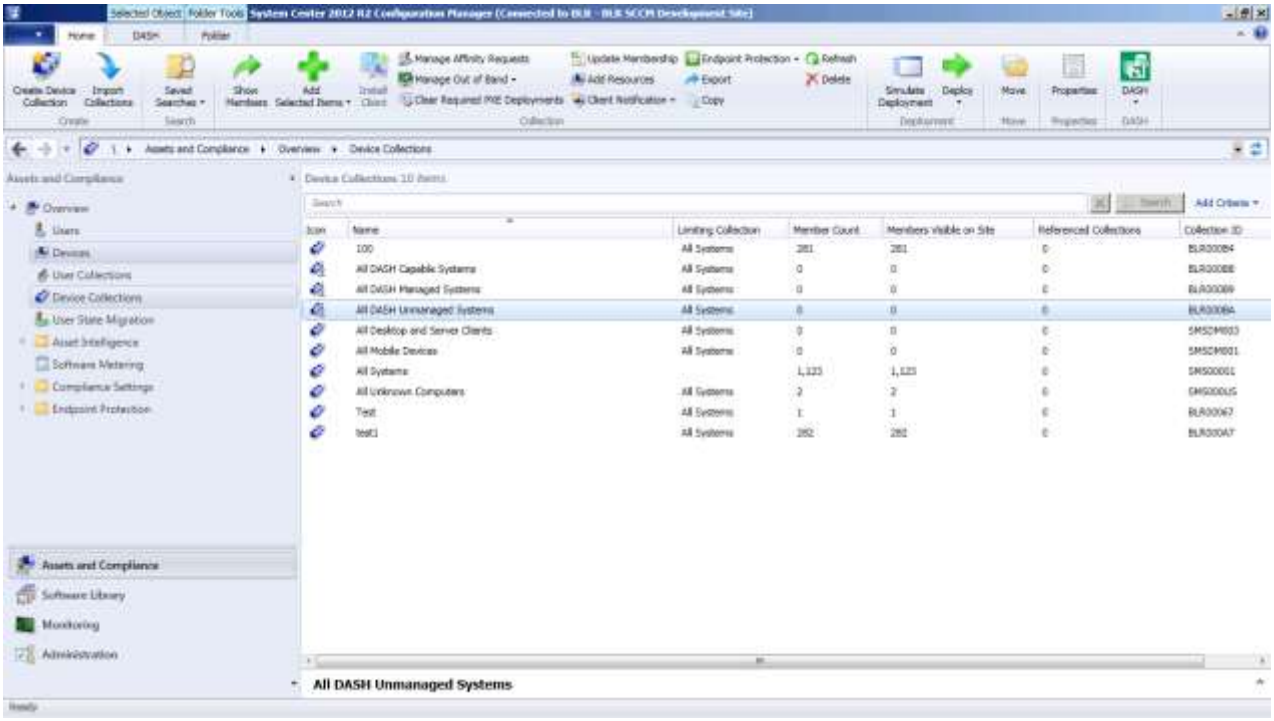


Figure 1-6: All DASH Unmanaged Systems Node

Chapter 2 Configuring DASH in SCCM

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

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 2-1: DASH Configuration Screen appears.

Note: See section **2.5** for configuring in CAS infrastructure.

2.1 Authentication

AMPS supports up-to 3 authentication entries. Each authentication entry has an authentication scheme and corresponding credentials. Provide the 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 (Scheme, Username, and Password). To manage the target, AMPS uses the three entries in sequential order to authenticate itself.

Notes:

- Among the authentication entries, Scheme + Username is unique.
- You cannot have two entries with same scheme and username.
- 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 on either HTTP or HTTPS transport.

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 2-**.
- 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 2-.

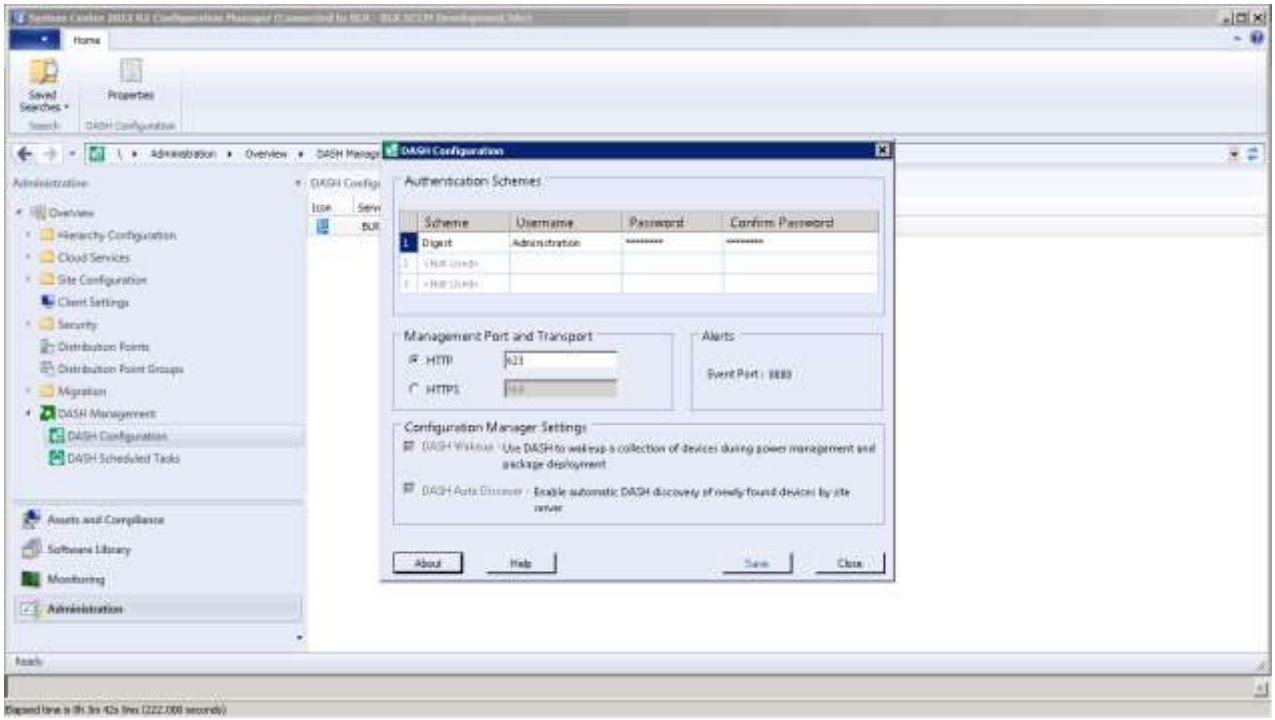


Figure 2-1: DASH Configuration Screen

2.4 Configuration Manager Settings

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

- DASH Wakeup.
- DASH Auto Discovery.

These features are explained in this section.

2.4.1 DASH Wakeup

The DASH Wakeup functionality enables SCCM 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 SCCM sends to the collection of devices before a software deployment activity is performed by SCCM.

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.

1. In the **DASH Configuration** screen (), Select the **DASH Wakeup** check box, if already not selected.
2. 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.

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 SCCM before the plugin was installed.

After AMPS installation, if a new device is added to SCCM 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 2-1: DASH Configuration Screen. Selecting the DASH auto discover checkbox removes the need to do the manual Discovery at a later stage.

2.5 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.

2.6 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 2-2: About Screen.**

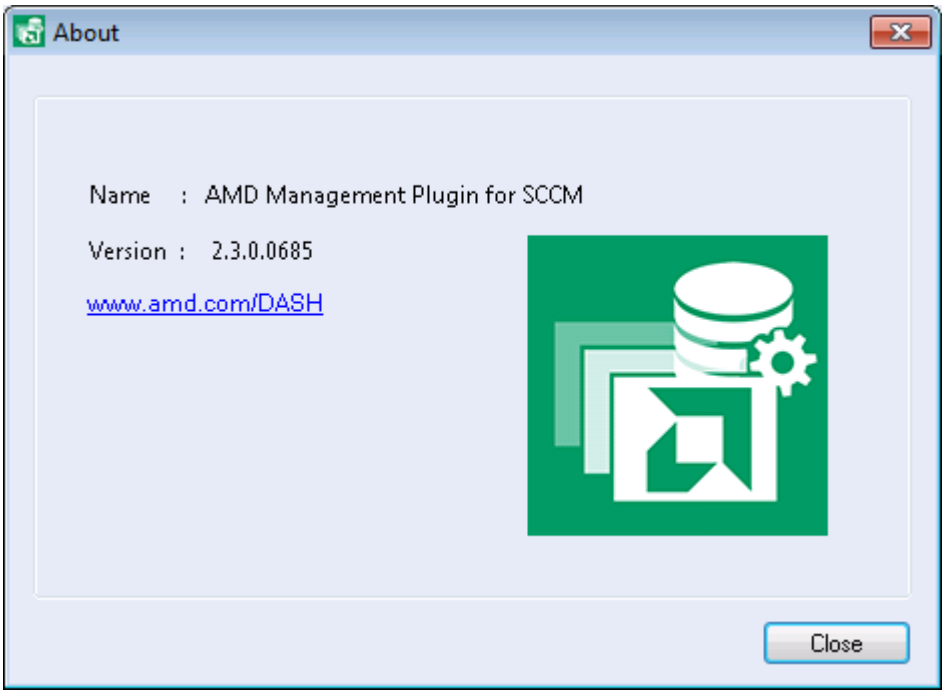


Figure 2-2: About Screen

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 **Accessing the DASH Scheduled Tasks node**

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

4. In the **System Center Configuration Manager** window, click **Administration**.
5. Expand the **Overview** node, then click the **DASH Management** node, and select **DASH Scheduled Tasks**.
6. Click the properties ribbon icon.
   The DASH configuration screen is displayed. For details on configuration, refer to **Chapter 2**.

Figure 1-3 illustrates these steps.

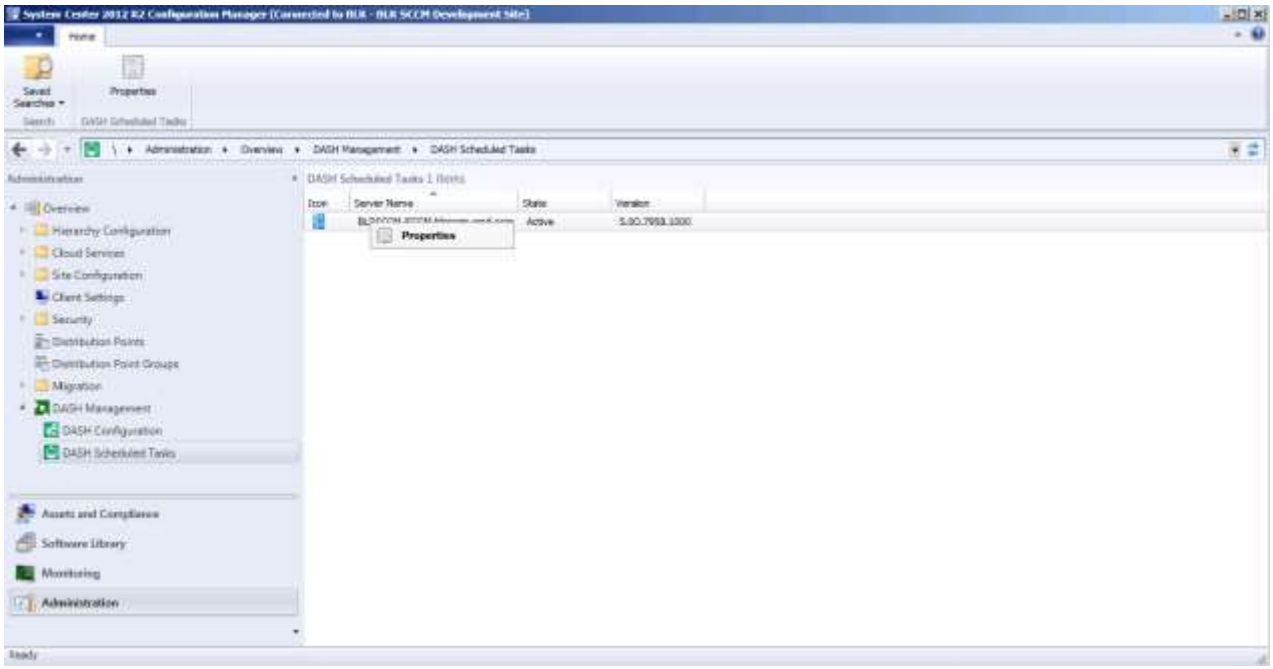


Figure 1-3: DASH Scheduled Tasks Node

Accessing the All DASH Capable Systems node section.

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

- Discovery.
- Power Control.
- Boot Control.
- Text Redirection.
- USB Redirection.
- Alerts.
- Record Log.
- Inventory.
- Resource Explorer.

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 SCCM DASH Plugin 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 3-1**.

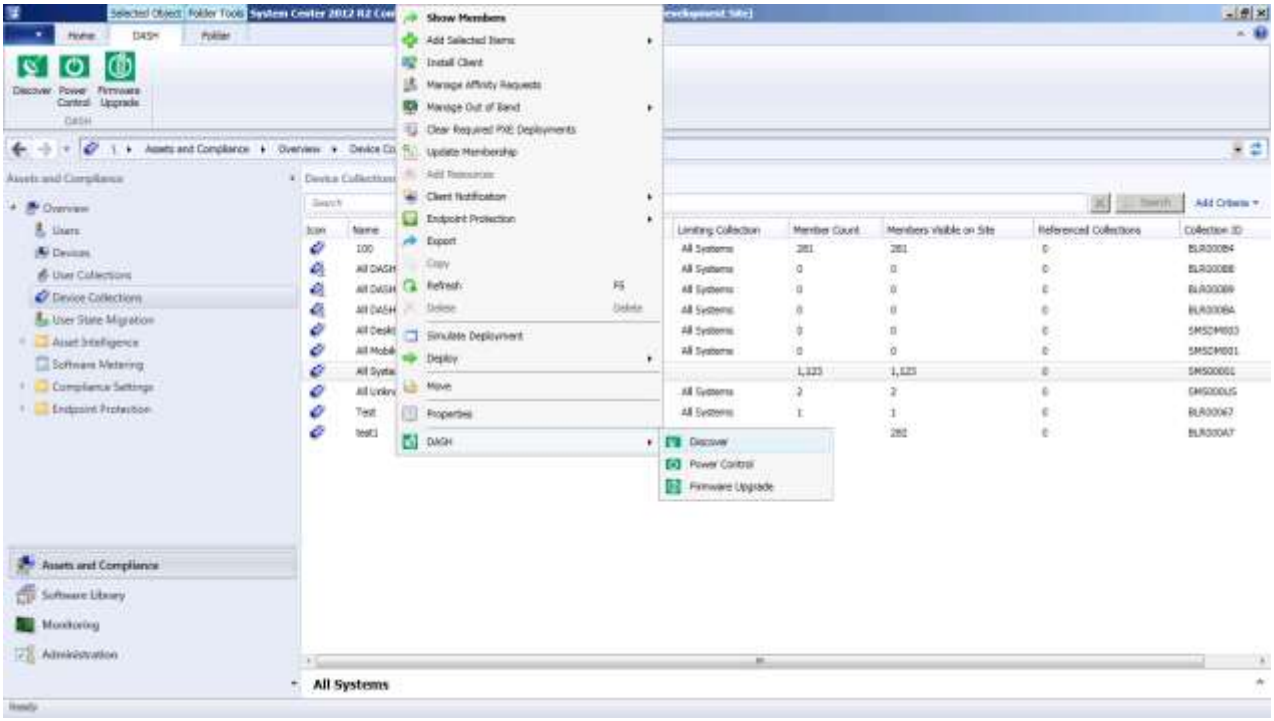


Figure 3-1: DASH Collection Node

The **Discover Collection** dialog box appears as shown in **Figure 3-2**.

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

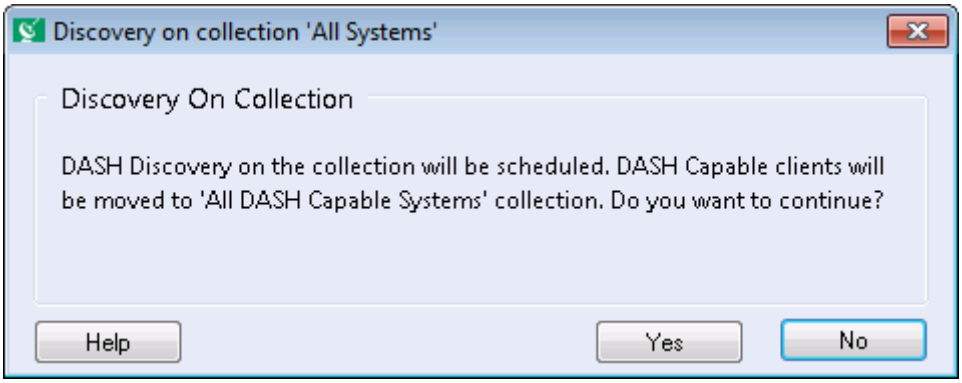


Figure 3-2: Discovery on Collection

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

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 3-3**.

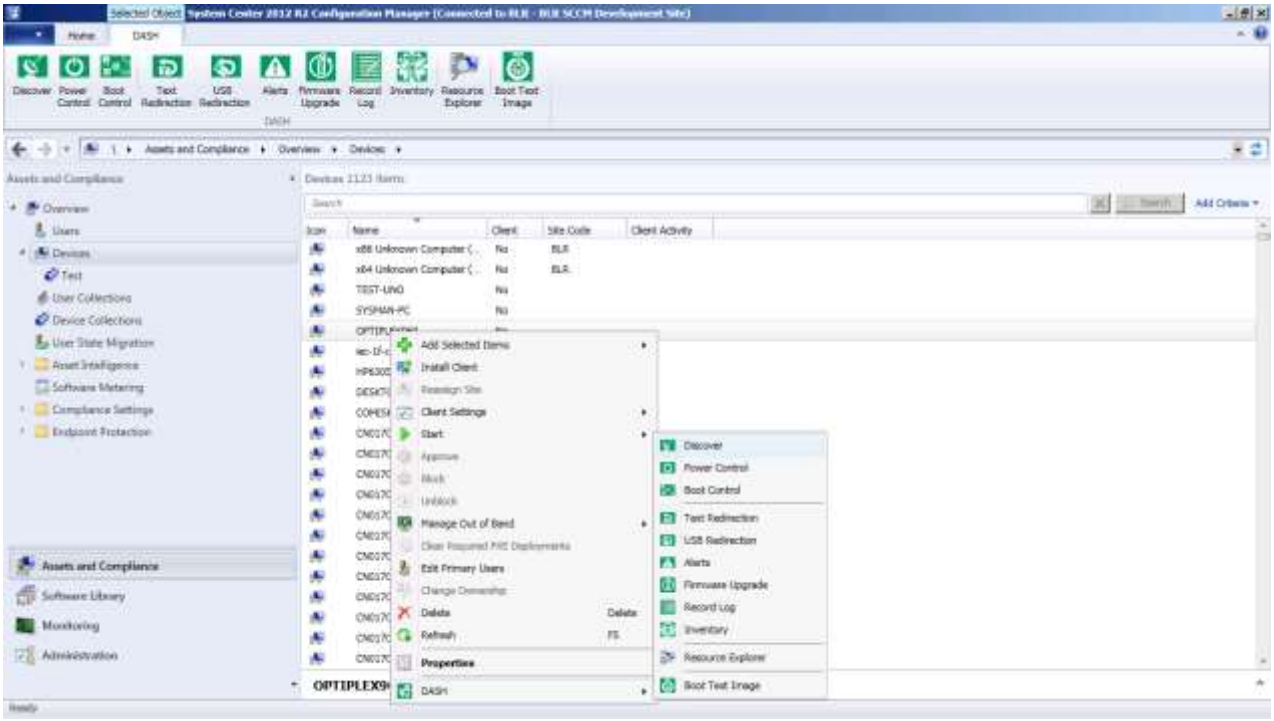


Figure 3-3: DASH Discovery on a Device

The **Discovery Result** dialog box appears as shown in **Figure 3-4**.

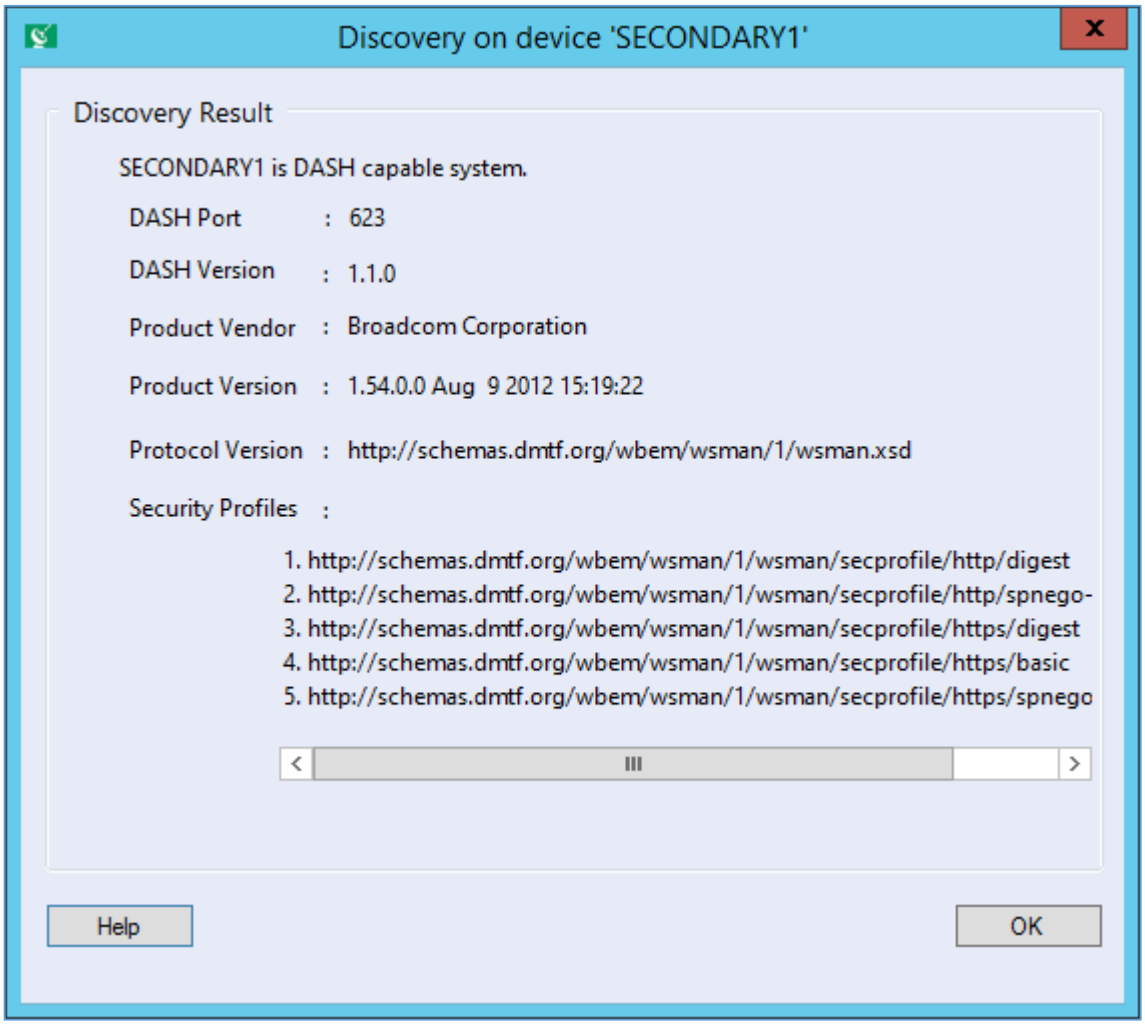


Figure 3-4: Result of Discovery on Device

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 4- illustrates the above steps.

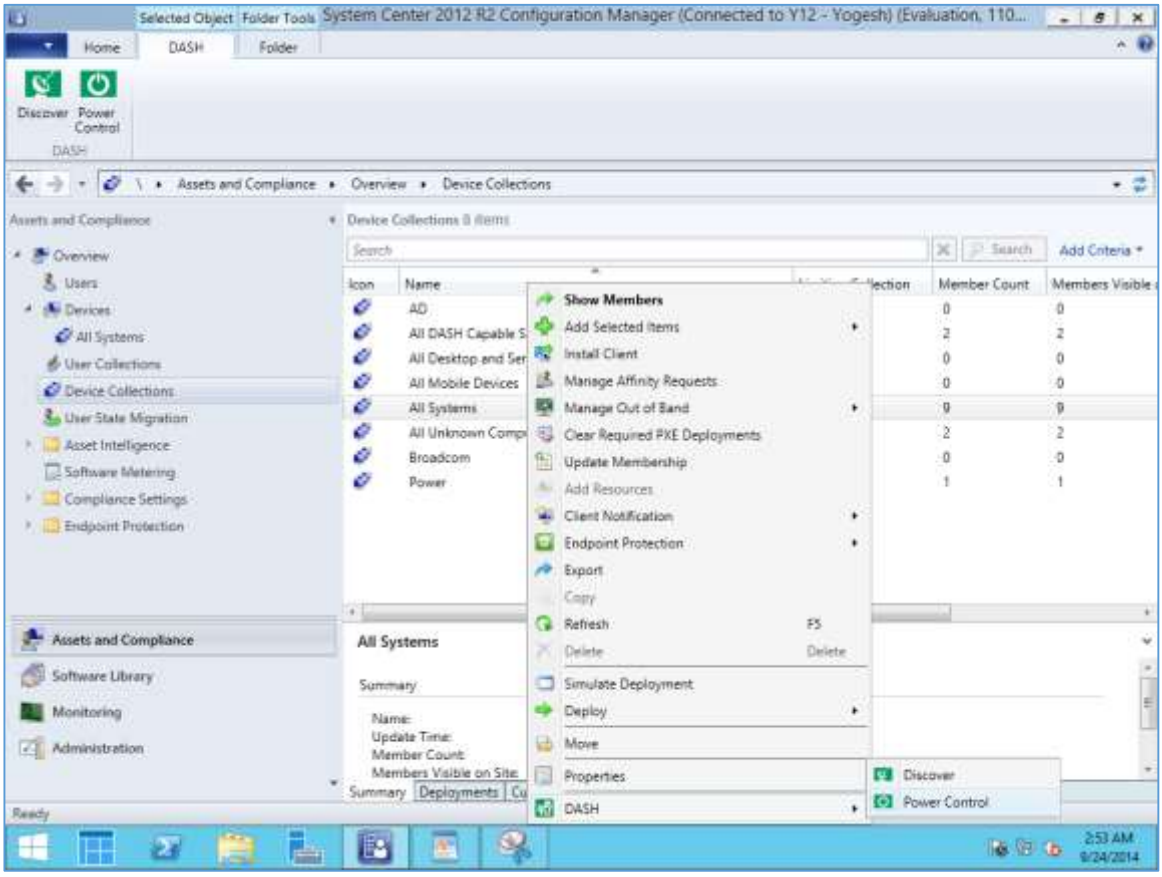


Figure 4-1: Power Control on Collection

The **Power Control on Collection** dialog box appears, as shown in **Figure 4-2** and **Figure 4-3**.

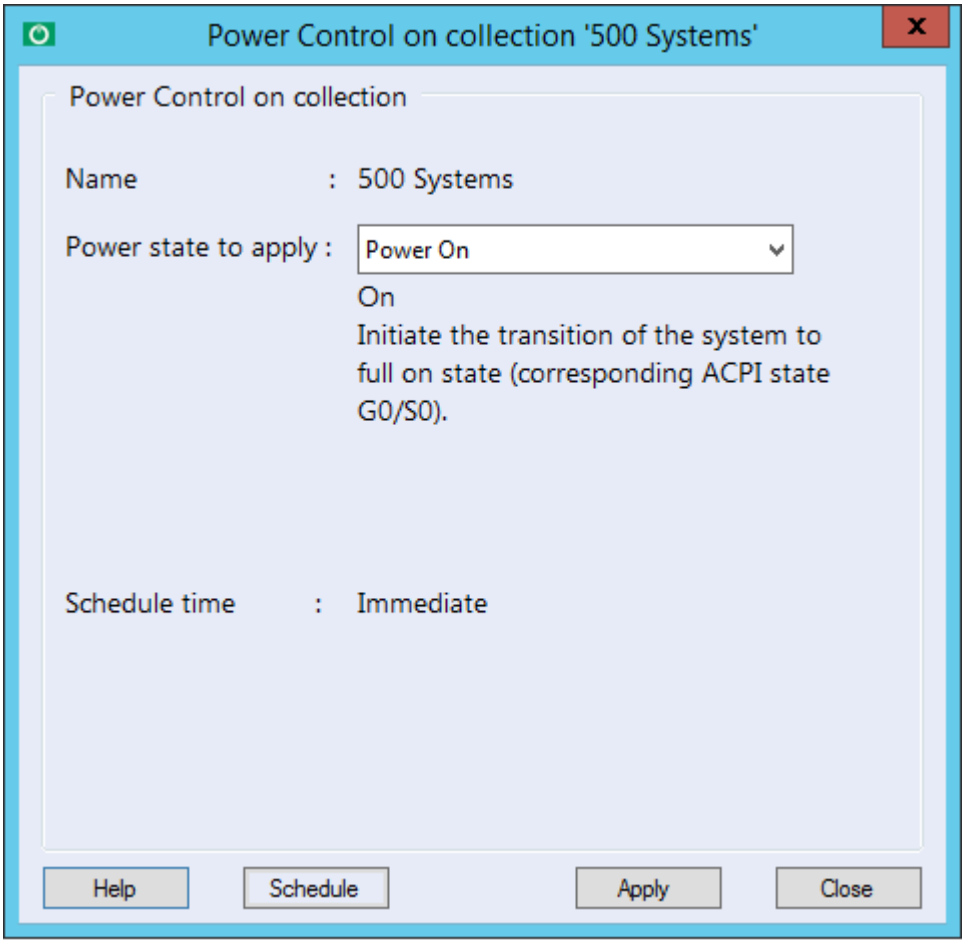


Figure 4-2: Immediate Power Control on Collection

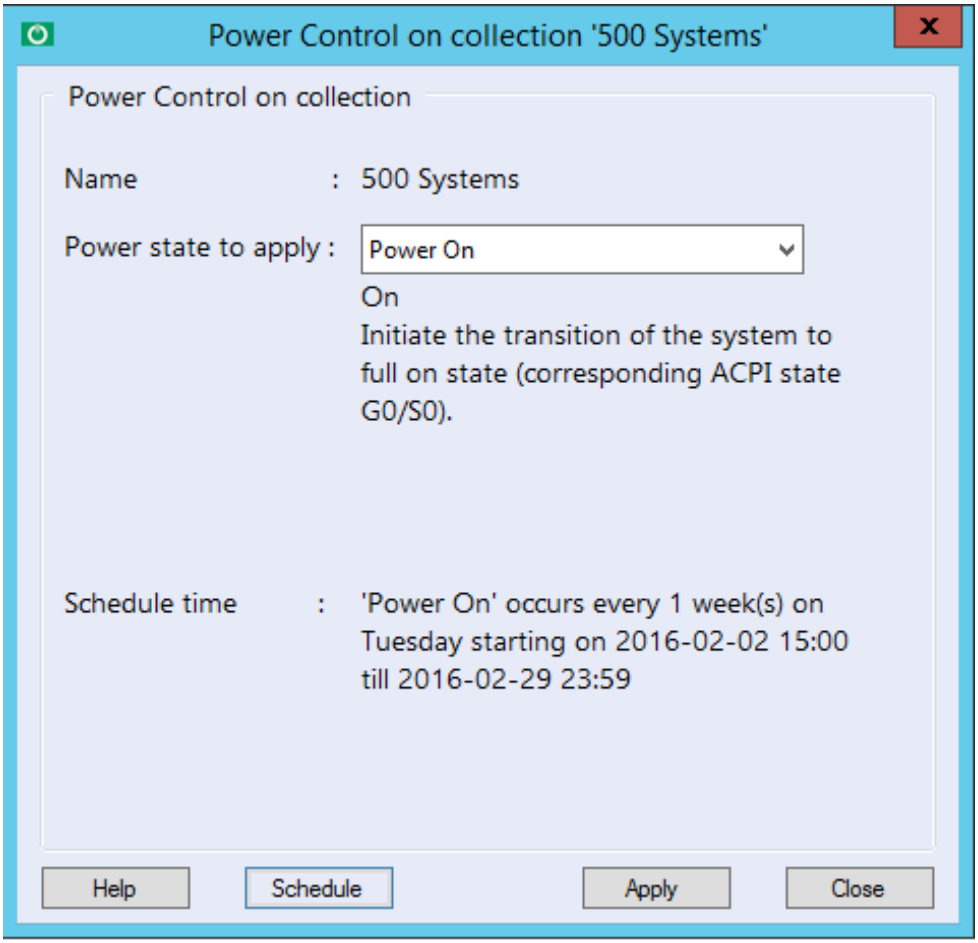


Figure 4-3: Scheduled Power Control on Collection

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 Fig 4.2.1) or Scheduled (shown in Fig 4.2.2).

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 4-4 illustrates the above procedure.

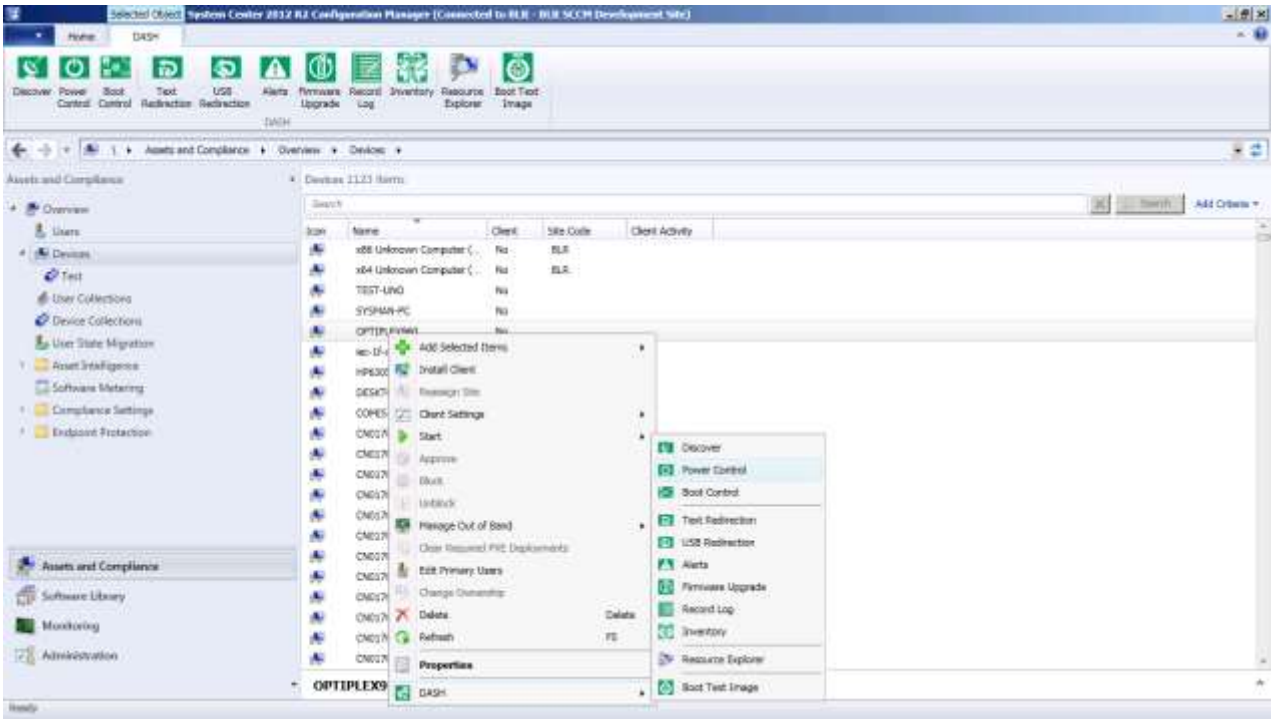


Figure 4-4: Power Control on Device

The **Power Control on Device** dialog box appears as shown in **Figure 4-5**.

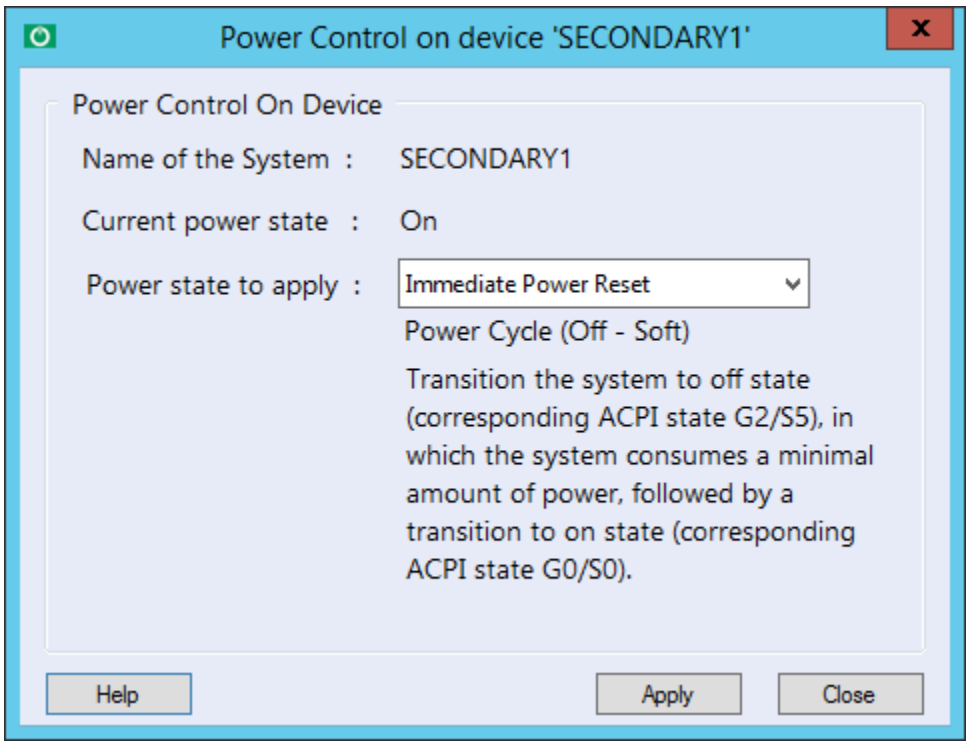


Figure 4-6: Power Control on Device

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 list 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 State	Friendly Name	Description	Corresponding ACPI State
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 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 State	Friendly Name	Description	Corresponding ACPI State
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 SCCM 2012's **Power Management** feature screen as illustrated in **Figure 4-6**.
2. Select the **Wakeup time (desktop computers)** check box.

Notes:

- AMPS looks for the status of the **Wakeup time** checkbox in SCCM 2012's power management feature screen and the **DASH Wakeup** checkbox in the **DASH Configuration** screen (refer to
- **Figure 2-**).
- 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.

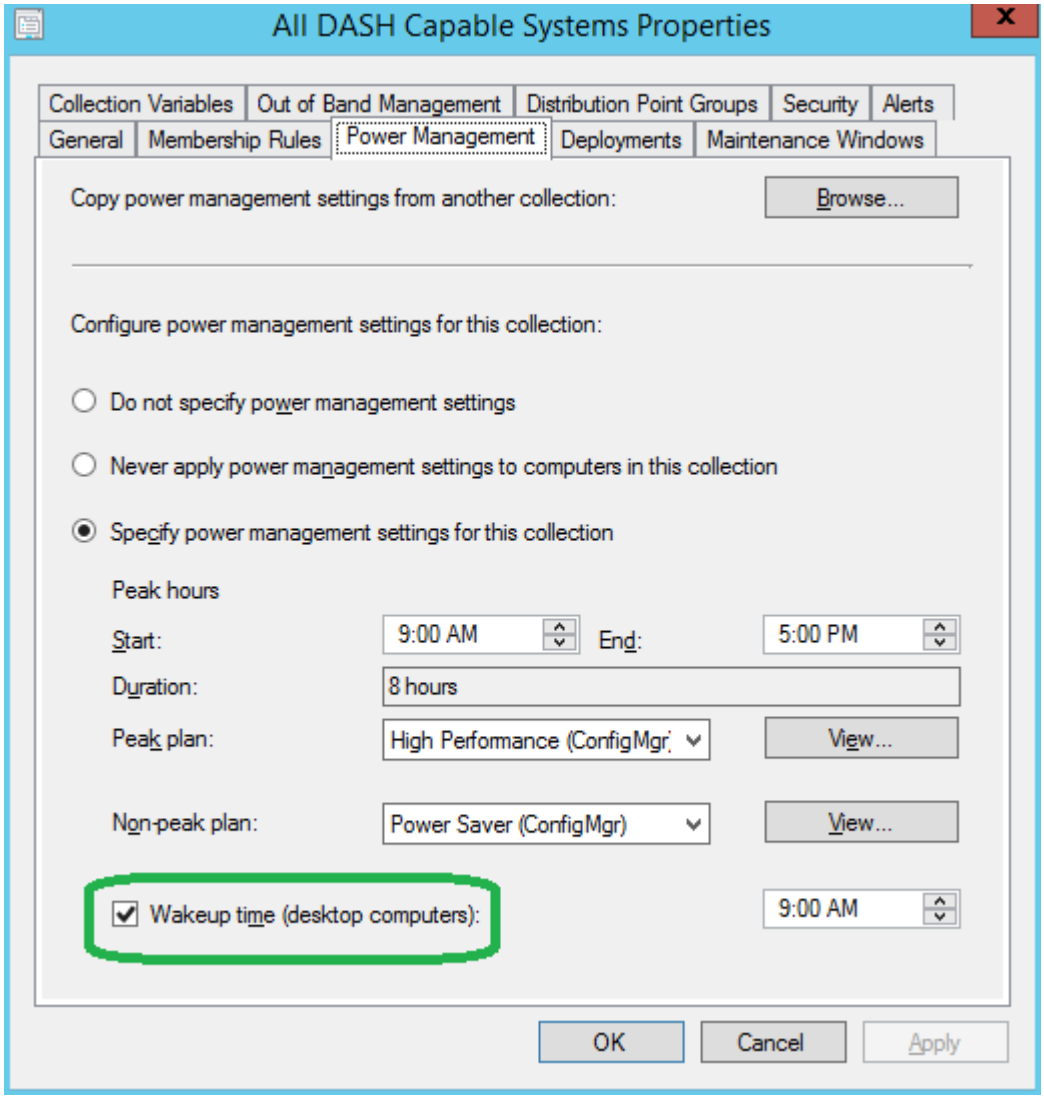


Figure 4-7: Scheduled Power Control

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 5-1**.

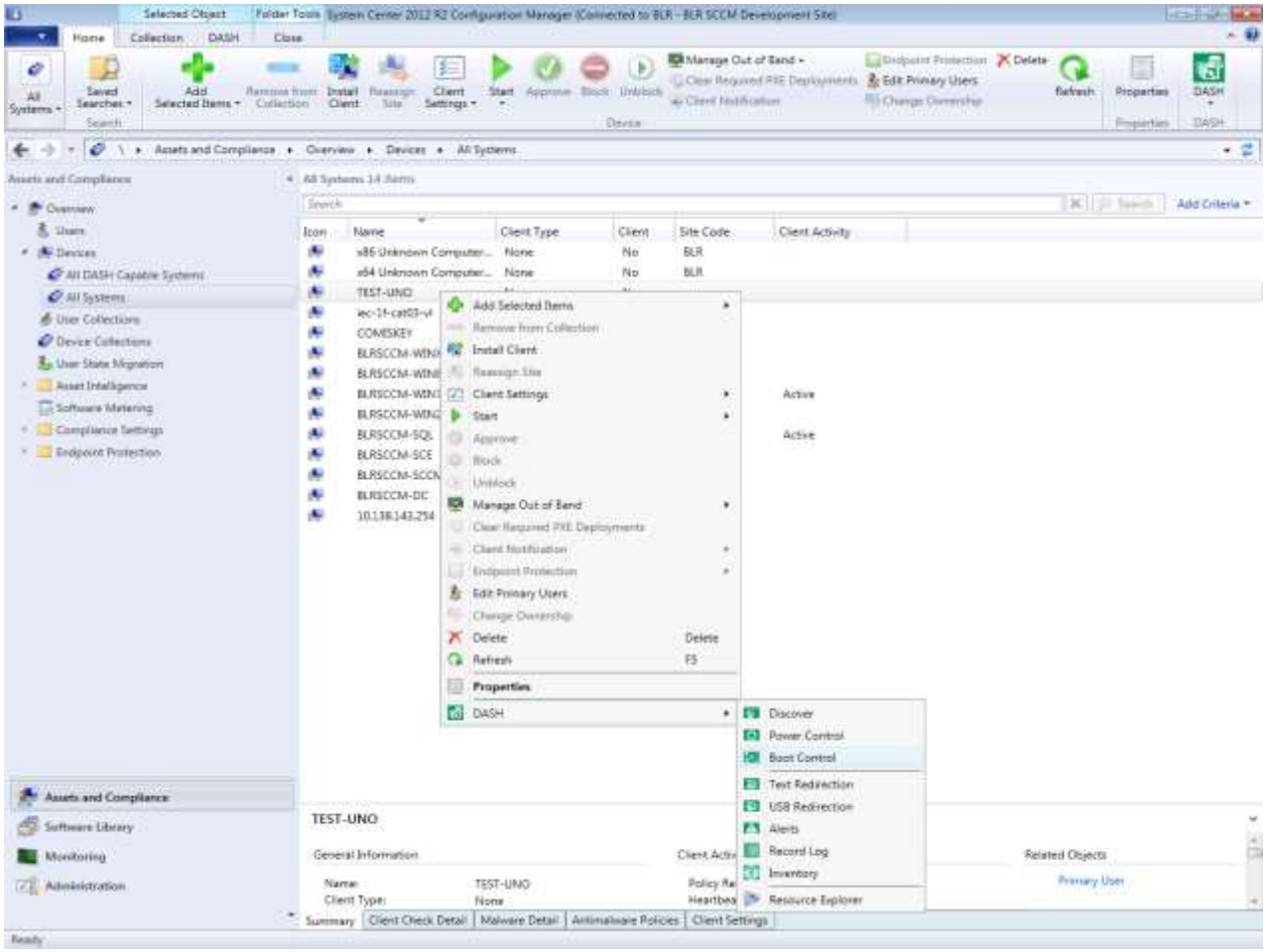


Figure 5-1: DASH Boot Control on Device

The **Boot Control on Device** dialog box appears as shown in **Figure 5-2**.

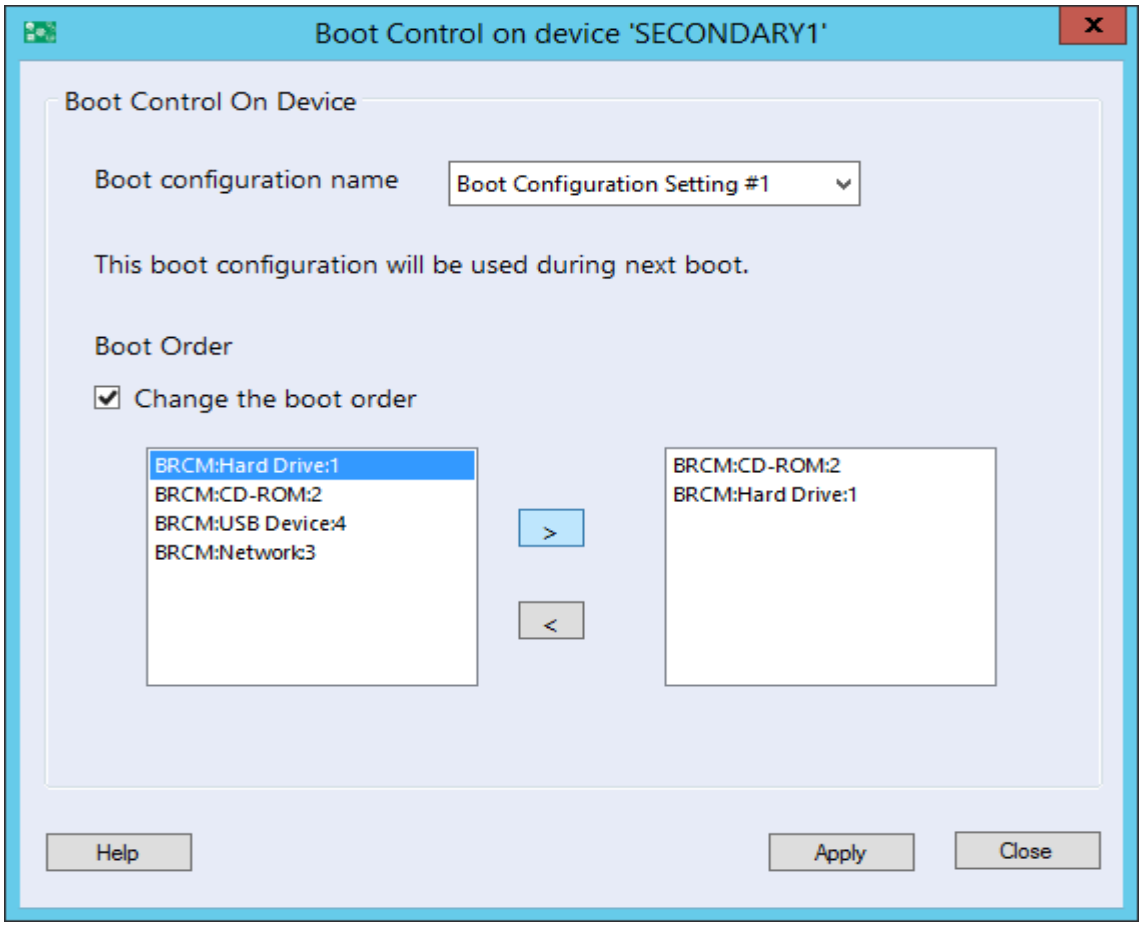


Figure 5-2: Boot Control on Device

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. 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.

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**.

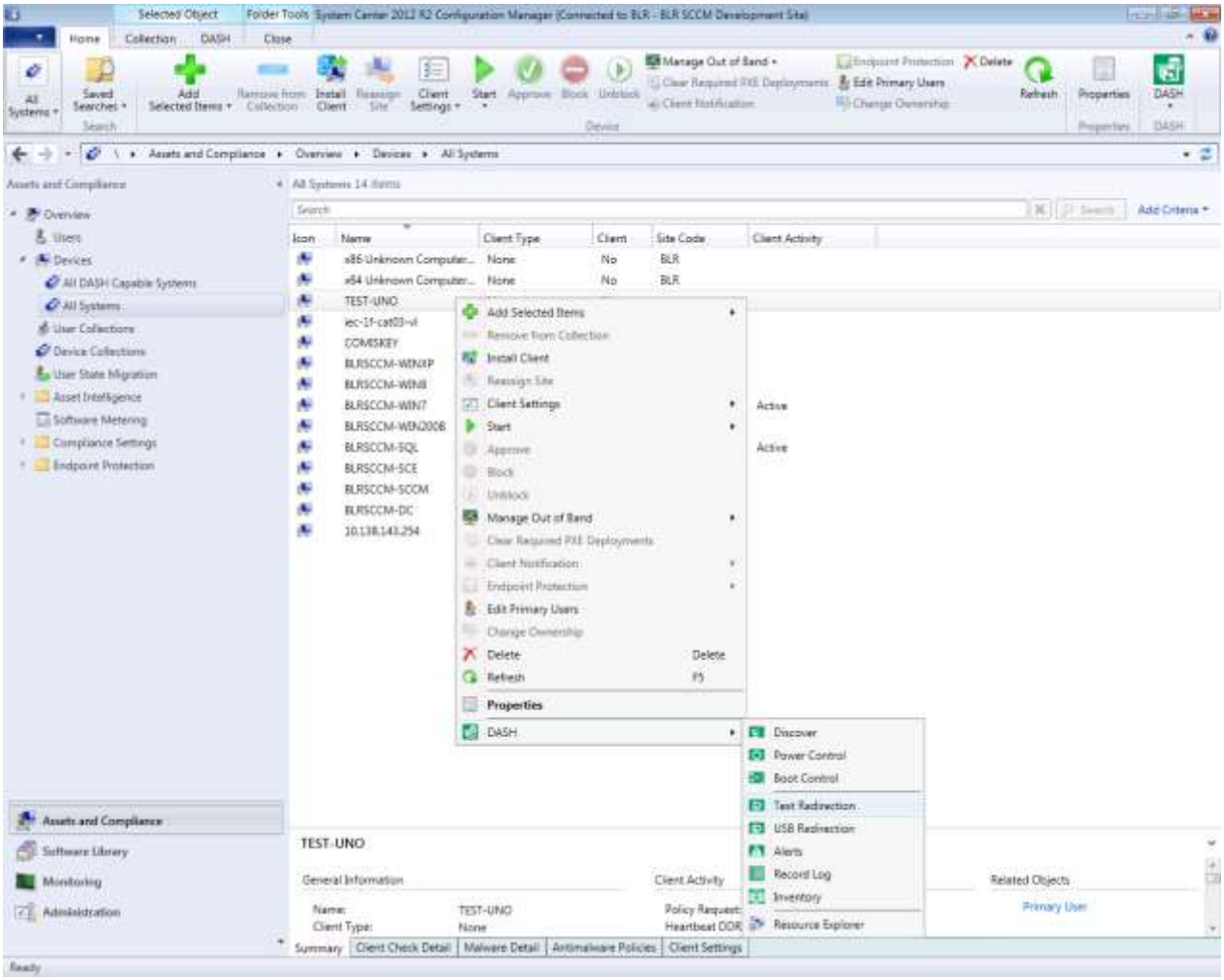


Figure 6-1: Text Redirection on device

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.

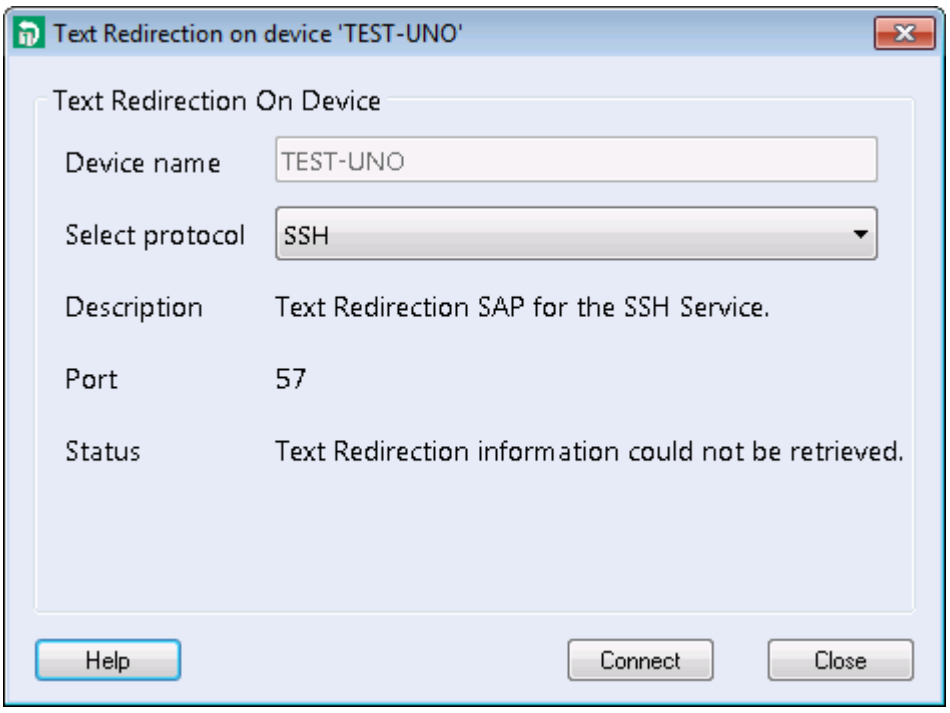


Figure 6-2: Text Redirection

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.

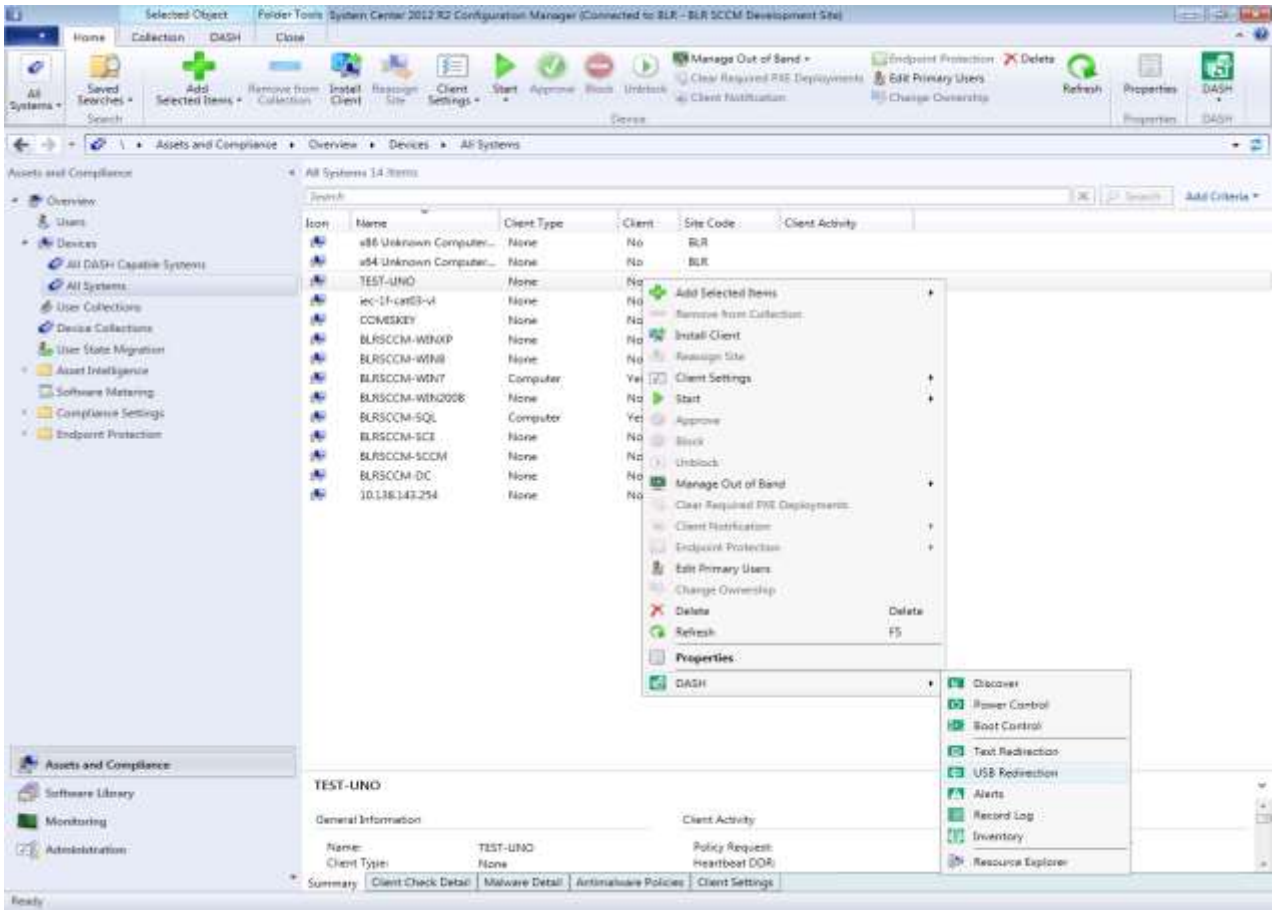


Figure 7-1: USB Redirection on Device

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** icon.

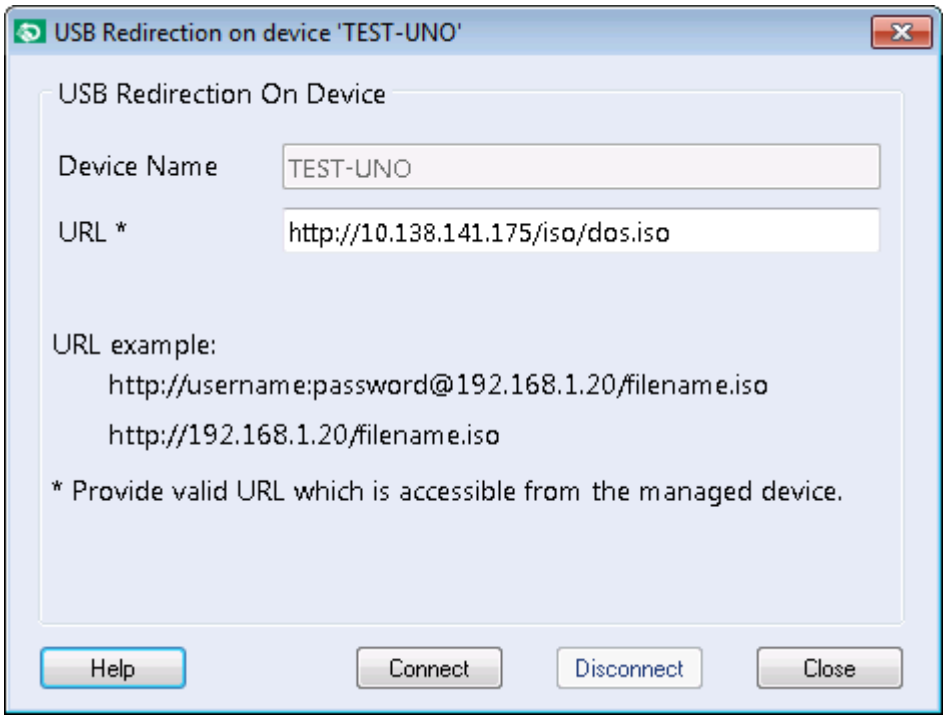


Figure 7-2: USB Redirection

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 7-3**.
- If the URL is invalid, error message appears.

Figure 7-3: 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 7-4: 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**.

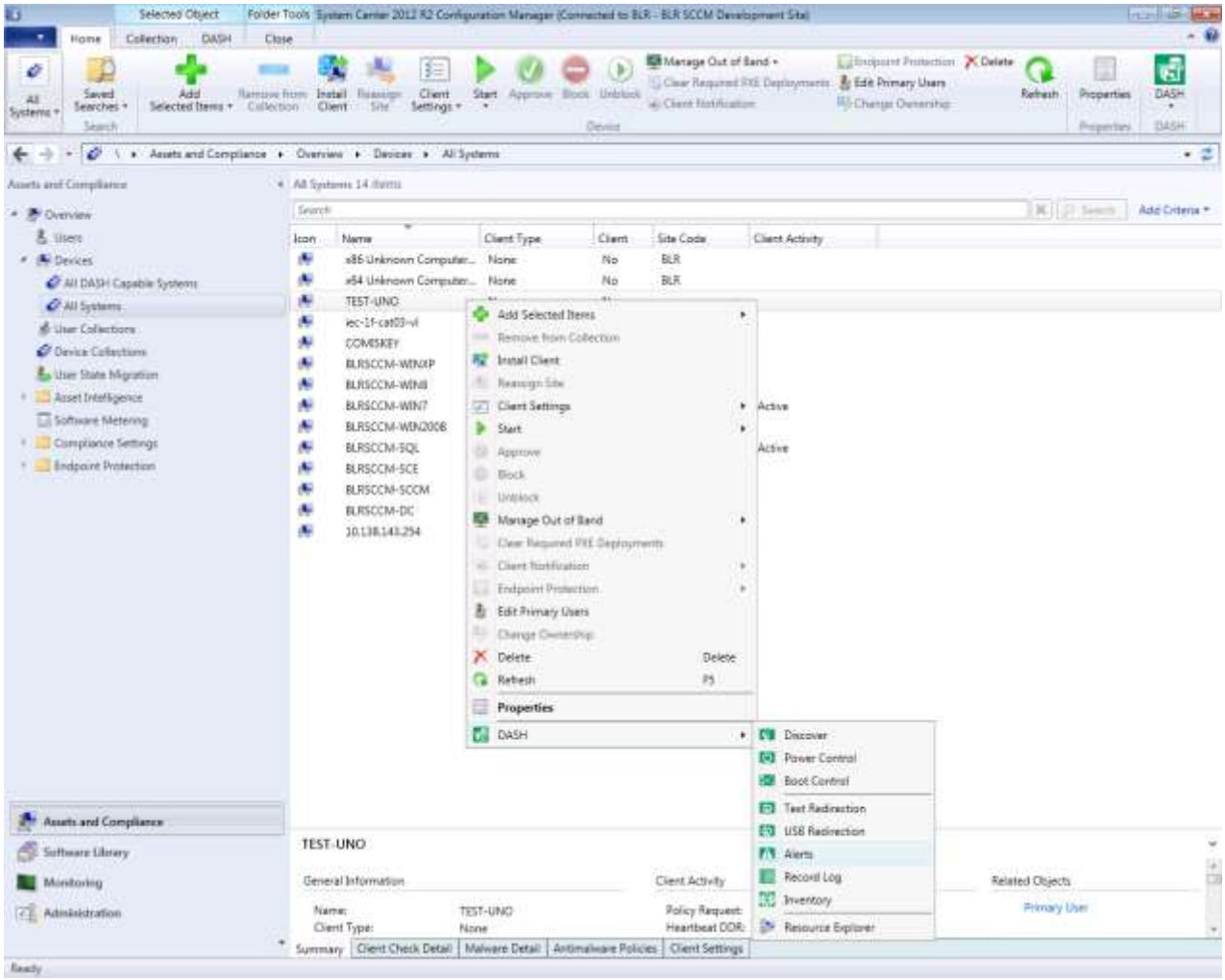


Figure 8-1: Alerts on device

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

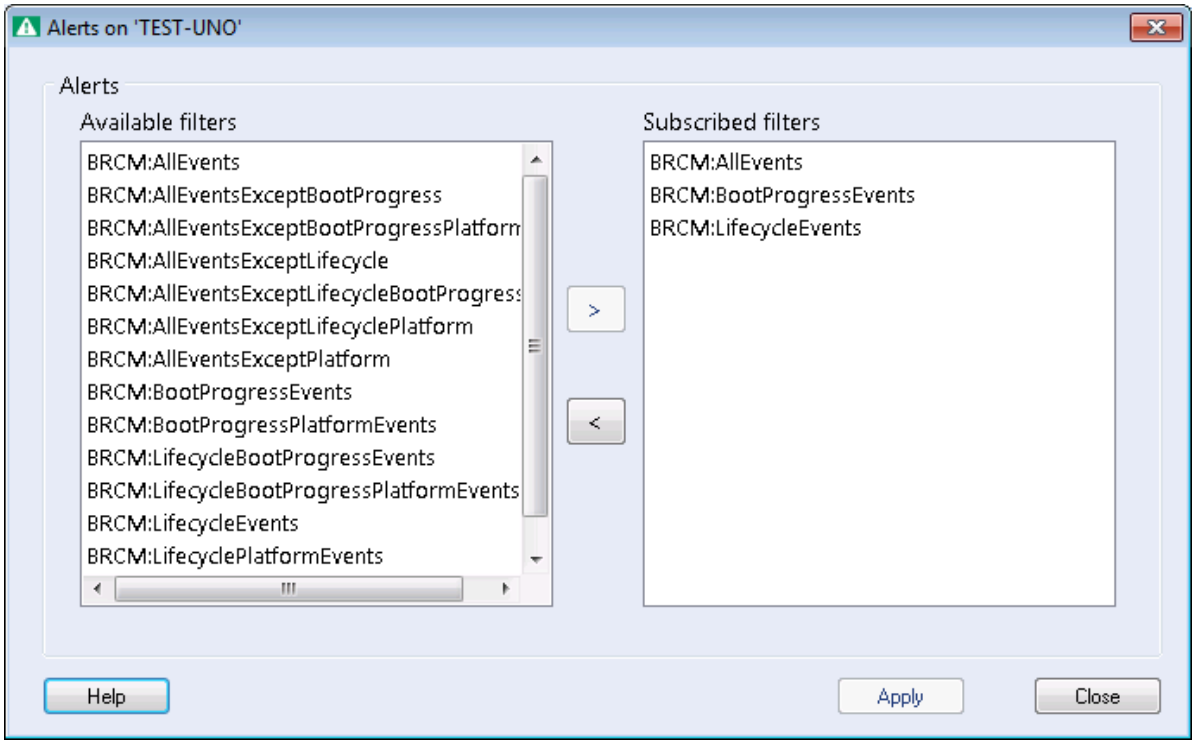


Figure 8-2: Alerts

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. 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.
4. To close the **Alert Subscription/Un-Subscription** screen, click the **Close** icon.

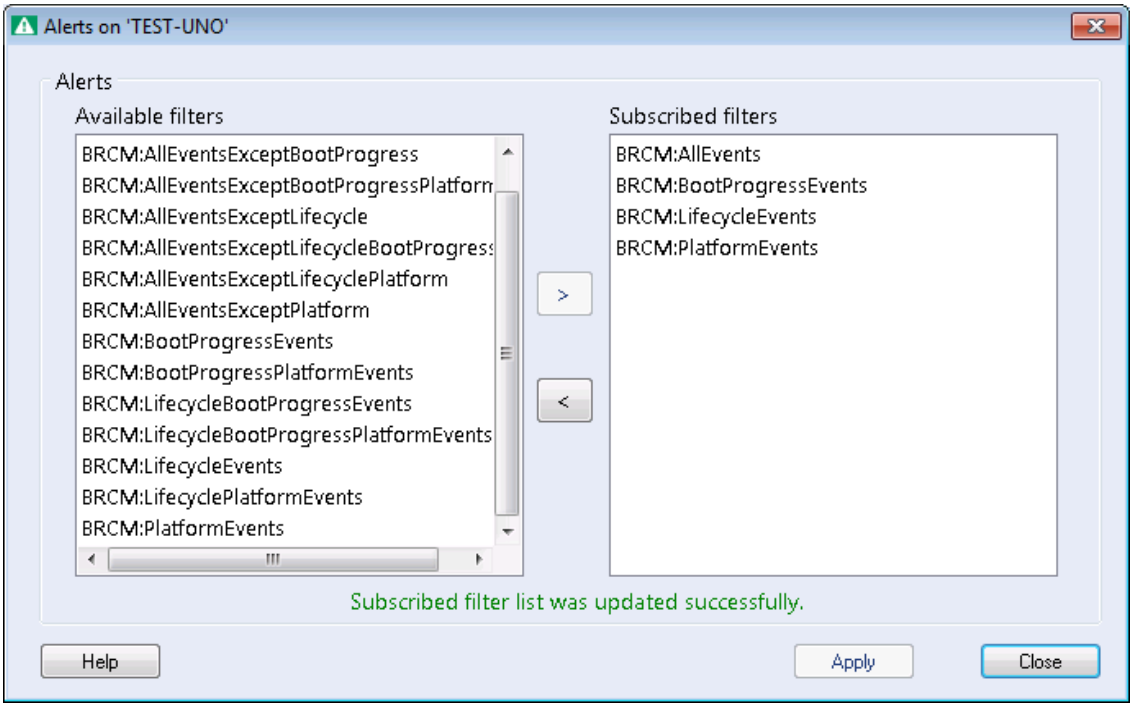


Figure 8-3: Alerts Subscription

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. 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.
4. To close the **Alert Subscription/Un-Subscription** screen, click the **Close** icon.

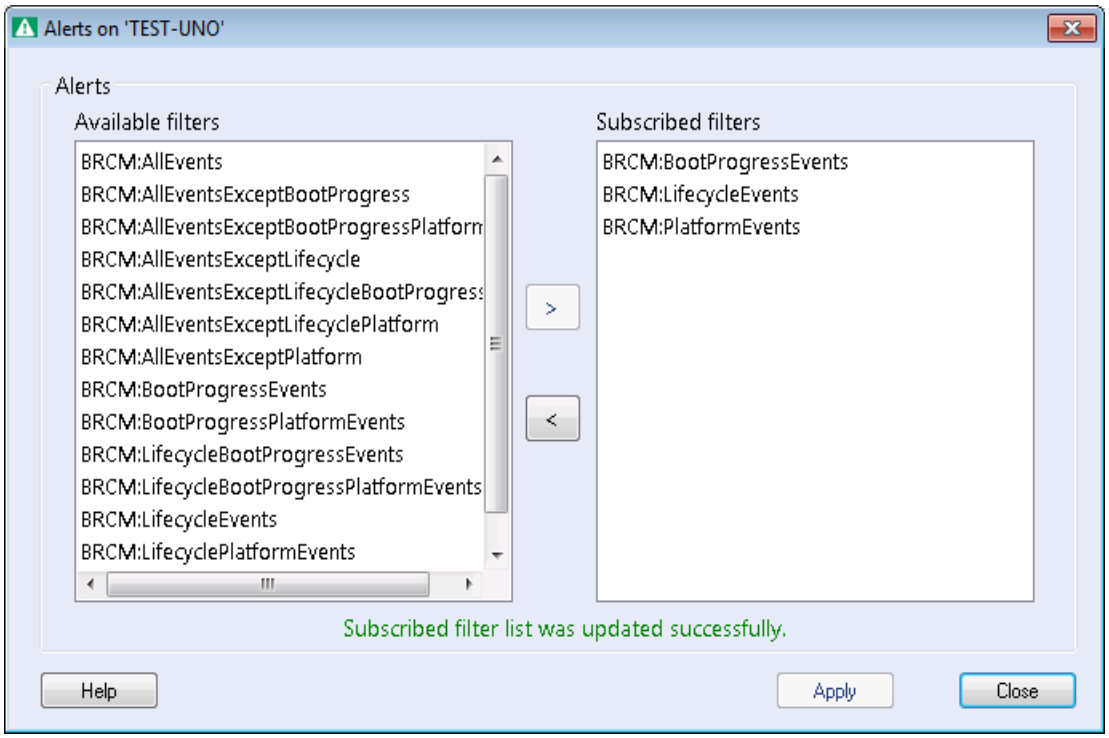


Figure 8-4: Alerts Un-Subscription

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 'DASH Plug-in' will list only AMPS messages.

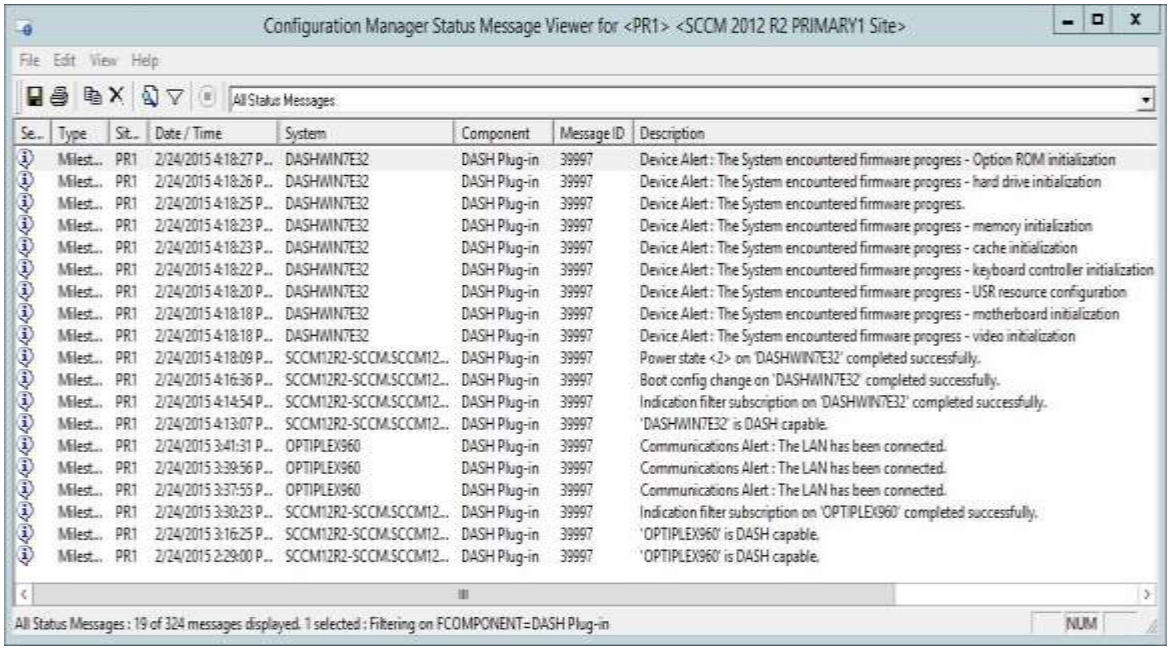


Figure 8-5: Alerts Reception

3.7 Inventory

SCCM 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.

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**.

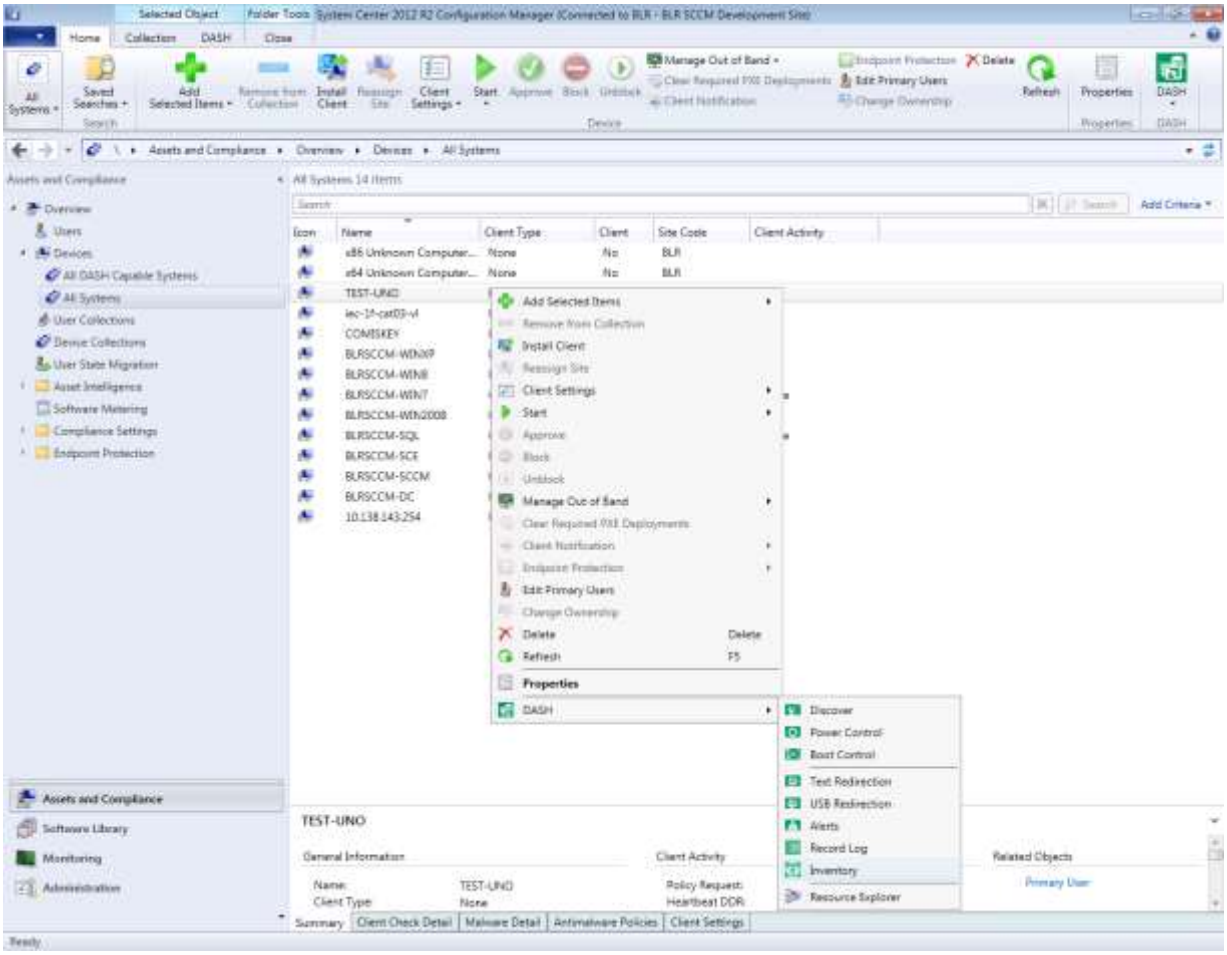


Figure 9-1: Inventory on device

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

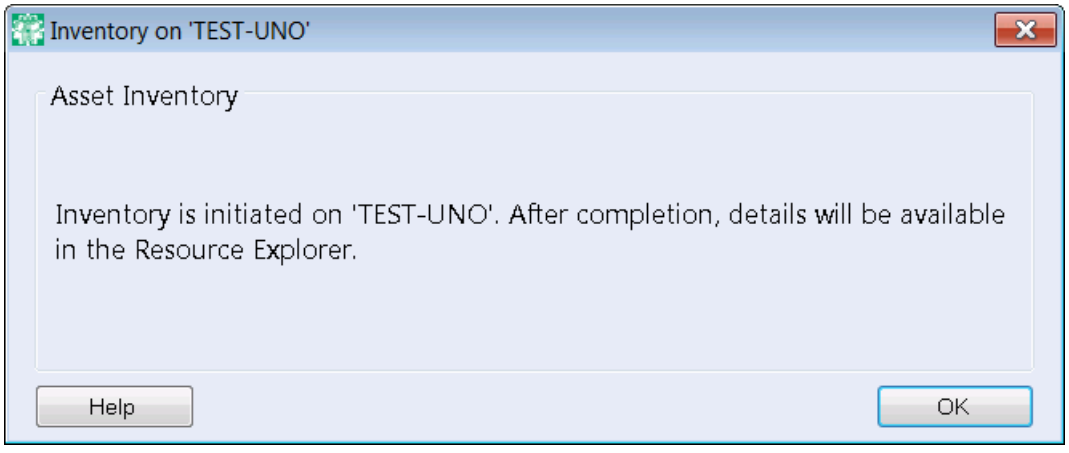


Figure 9-2: Inventory

3.7.2 Viewing the DASH Inventory or Resource Explorer

To view the DASH inventory, perform the following steps:

1. Perform the DASH Discovery on Device steps. For more information on the DASH discovery on a device steps, refer to the Discovering a Device section.
2. Expand the **Assets and Compliance** node.
3. Expand the **Devices Collections** node.
4. Click on the collection containing the desired DASH device for which inventory has to be viewed.
5. Select and Right click on the DASH device for which inventory has to be viewed.
   The shortcut menu appears.
6. In the shortcut menu, point to **DASH** and then click **Resource Explorer**.

On following the steps above the resource explorer screen appears.

Note: All tree items with DASH prefix are data collected through DASH from the managed device.

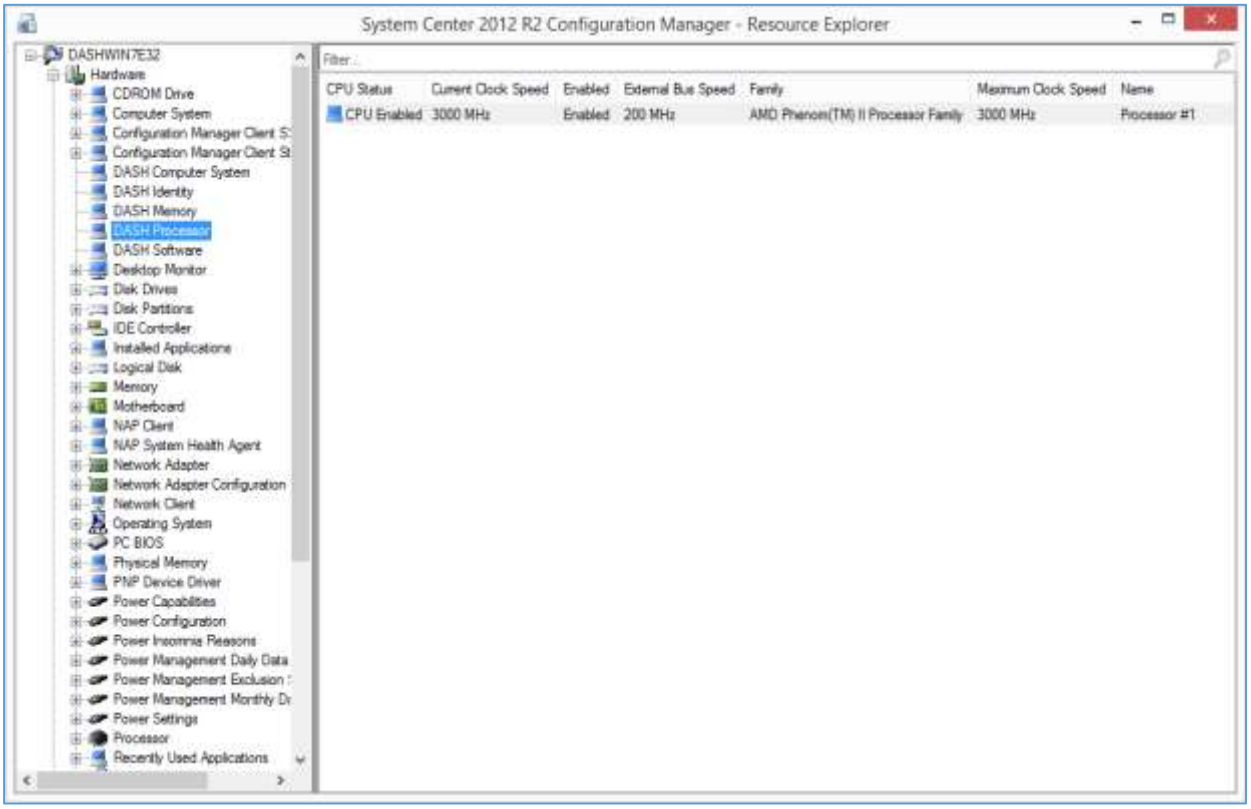


Figure 9-3: Viewing Inventory

3.8 Record Log

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 10-2: Record Log**. Users can navigate the log screen using the provided controls.

To view the record log 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 record log. The shortcut menu is displayed.
5. In the shortcut menu, point to **DASH** and then click **Record Log**. The record log screen appears.

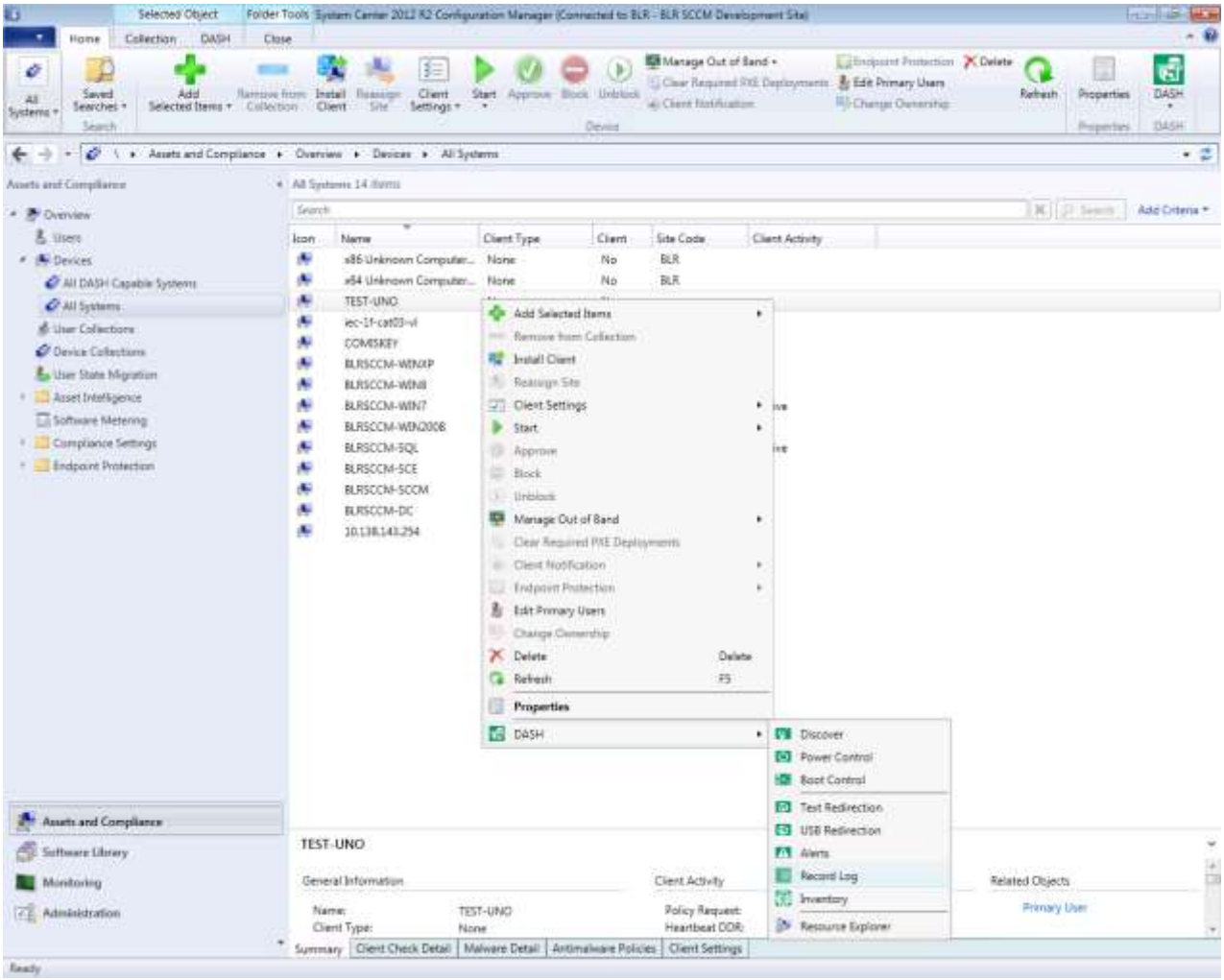


Figure 10-1: Viewing the Record Log of a device

The Record Log 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.

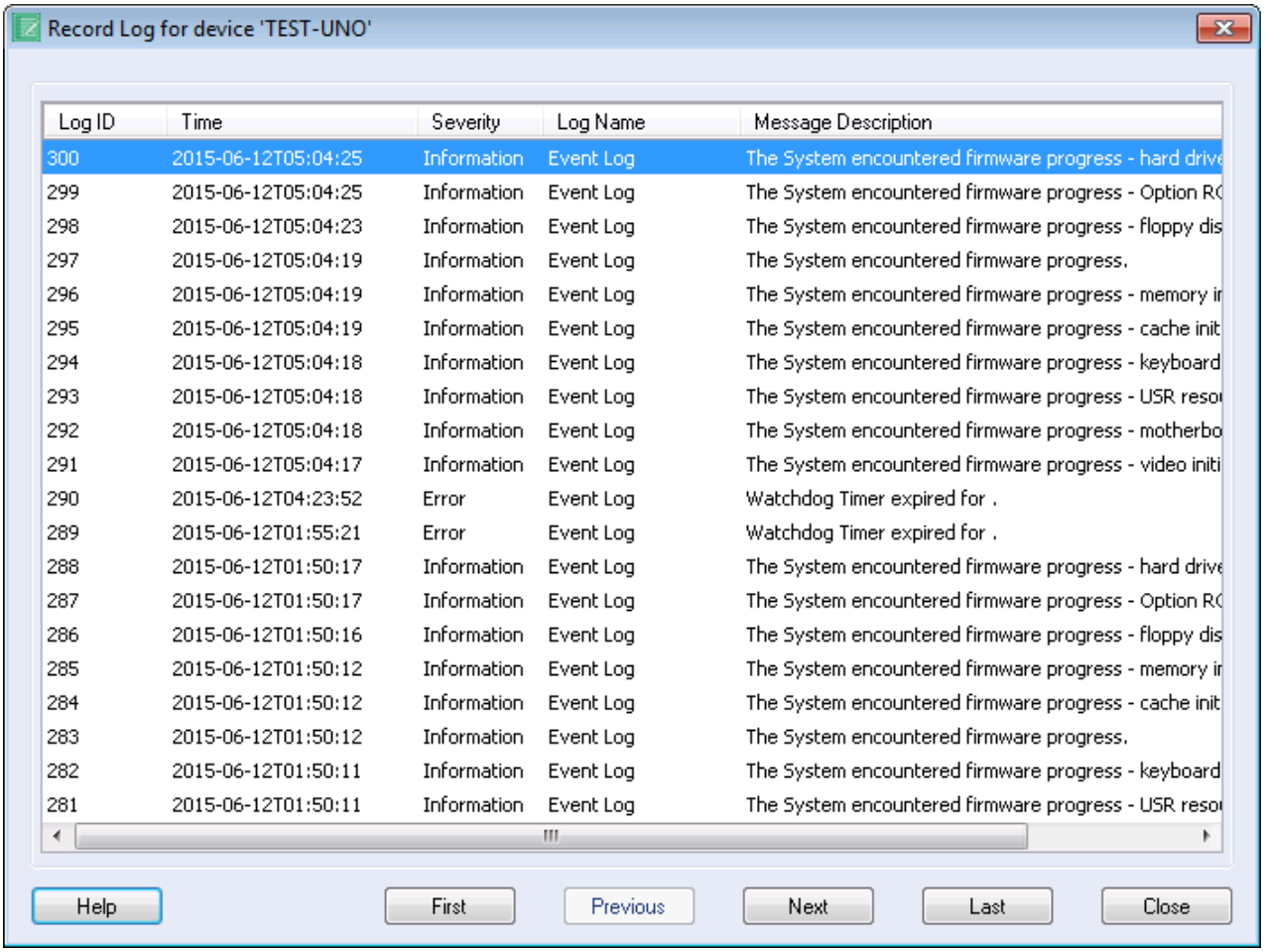


Figure 10-2: Record Log

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 **Nex**t which navigate to the older and newer log entries in the record log, and updates the fields in the pop up screen.

Figure 10-3 illustrates the Status Message Detail screen which is displayed on double clicking on a log entry.

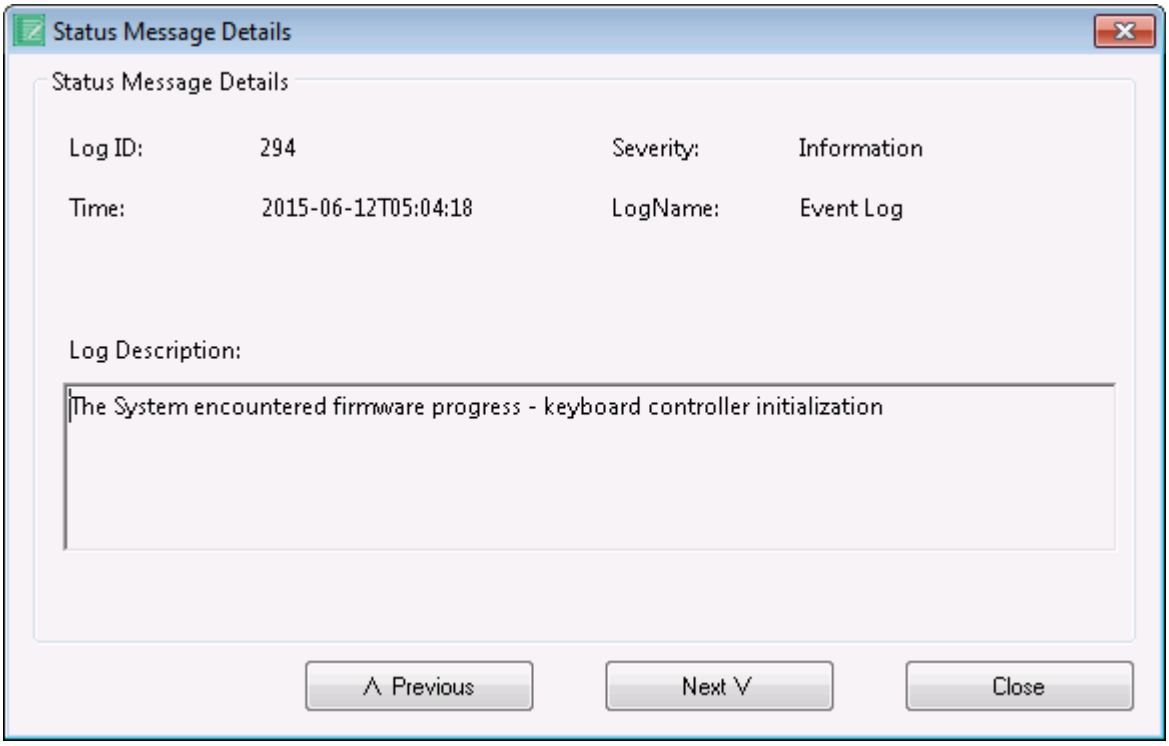


Figure 10-3: Status Message Details

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.

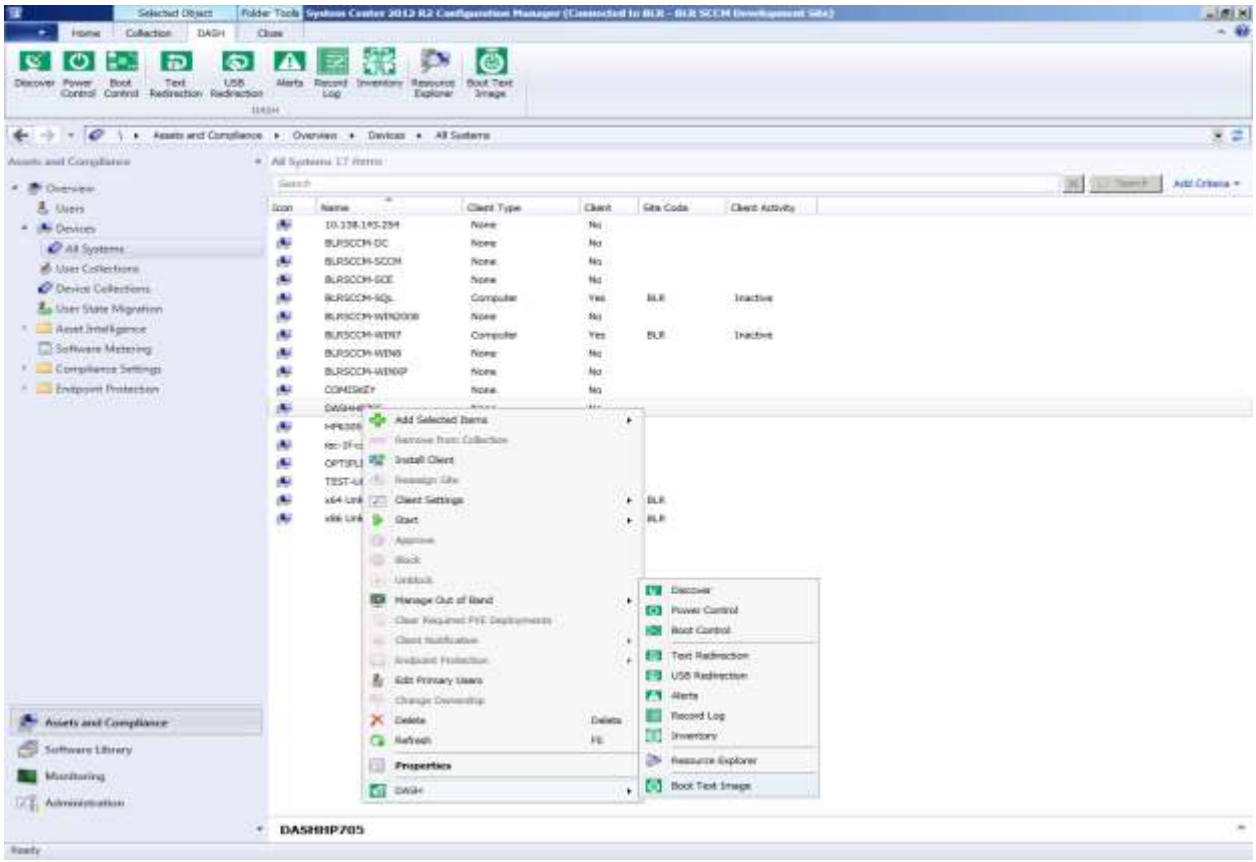


Figure 11-1: Boot Text Image on device

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

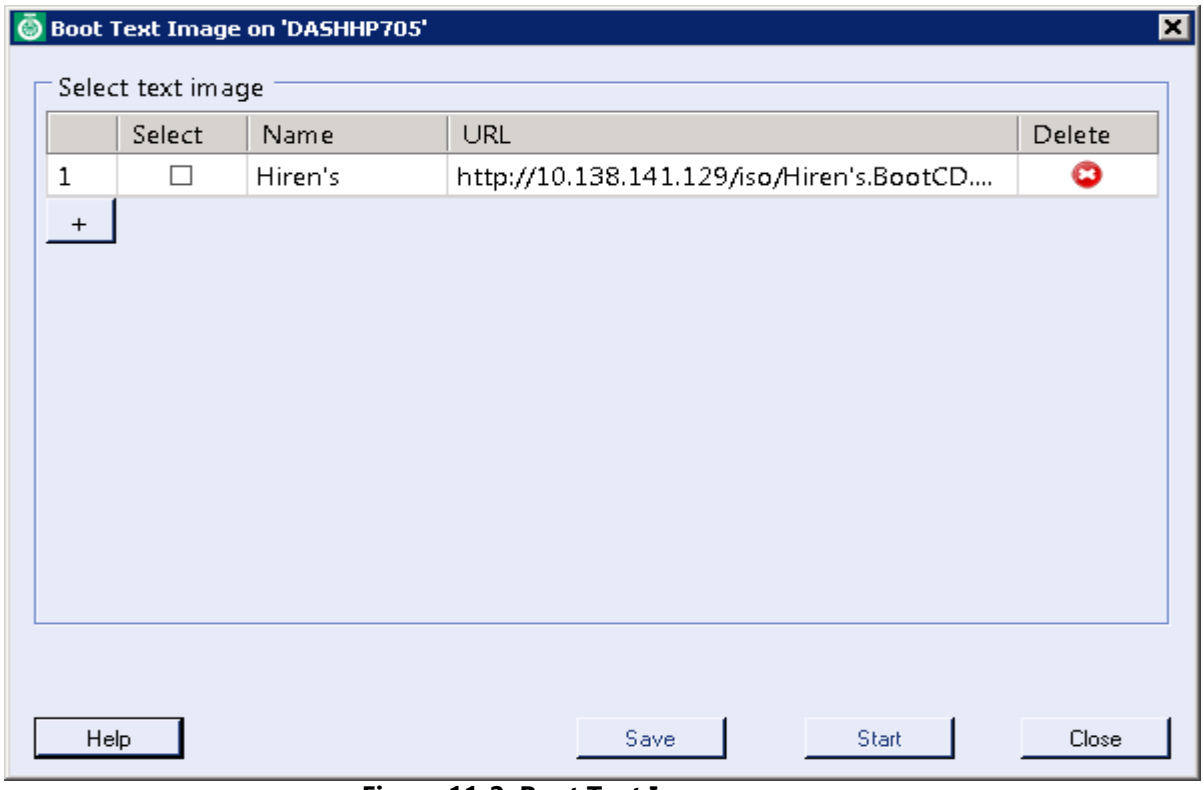


Figure 11-2: Boot Text Image

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 URL.
- User can click on Add (+) button to add new URL to list.
- User has to click the Save button to save the list of URLs.
- User has to click on the Start button to initiate deploy to text image task.

Note:

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

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

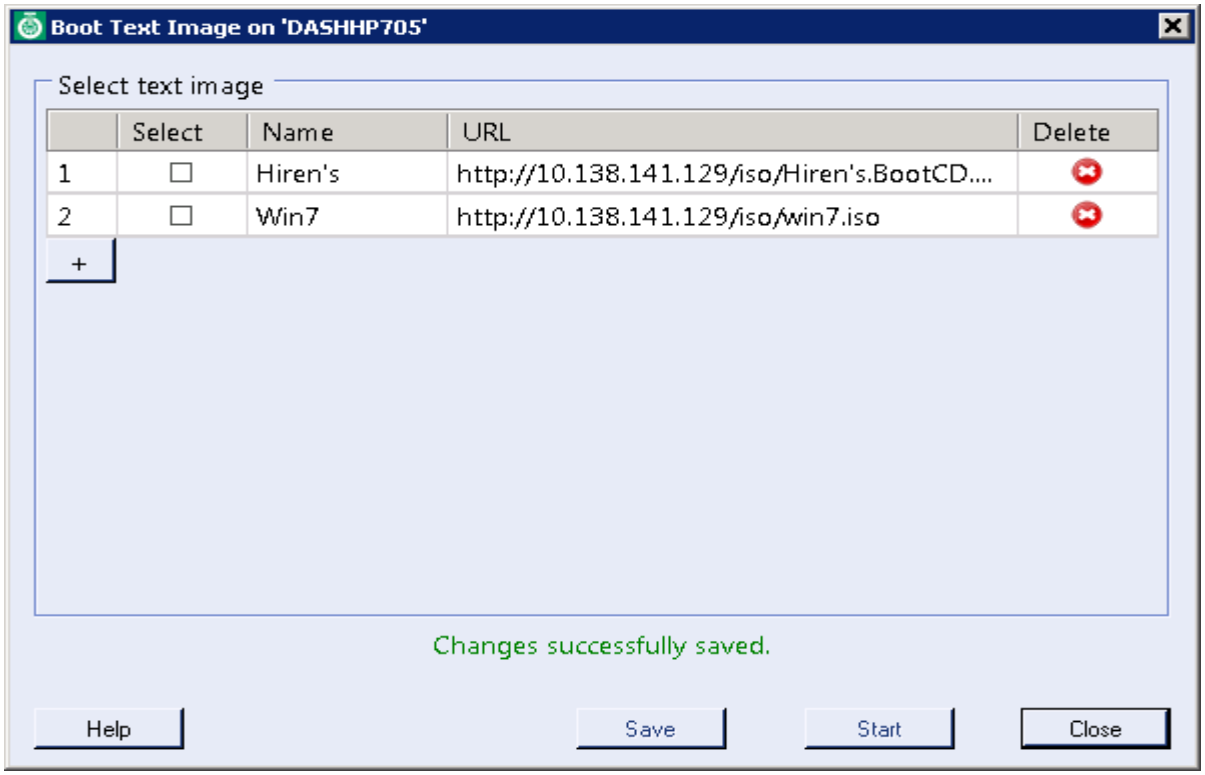


Figure 11-3: Boot Text Image after adding URL

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

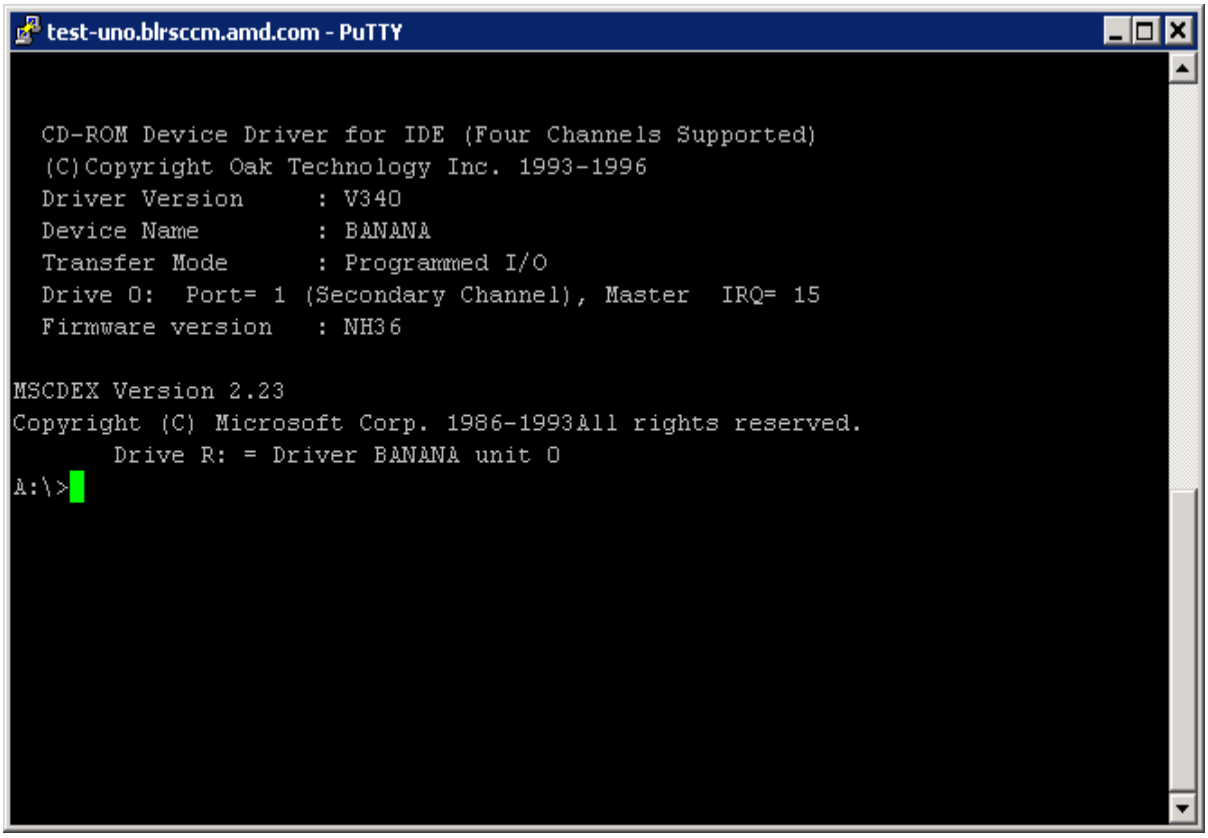


Figure 11-4: Boot Text Image after booted to URL

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.

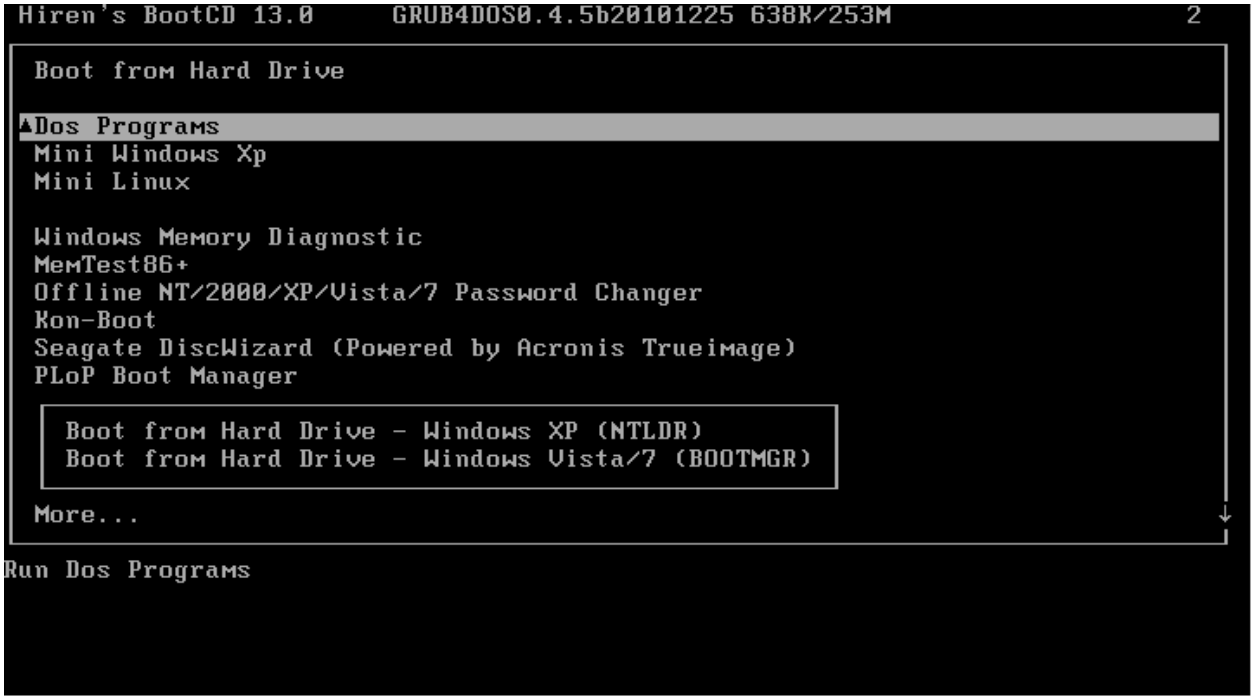


Figure 11-5: Sample usecase for Boot Text Image

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 4-**.

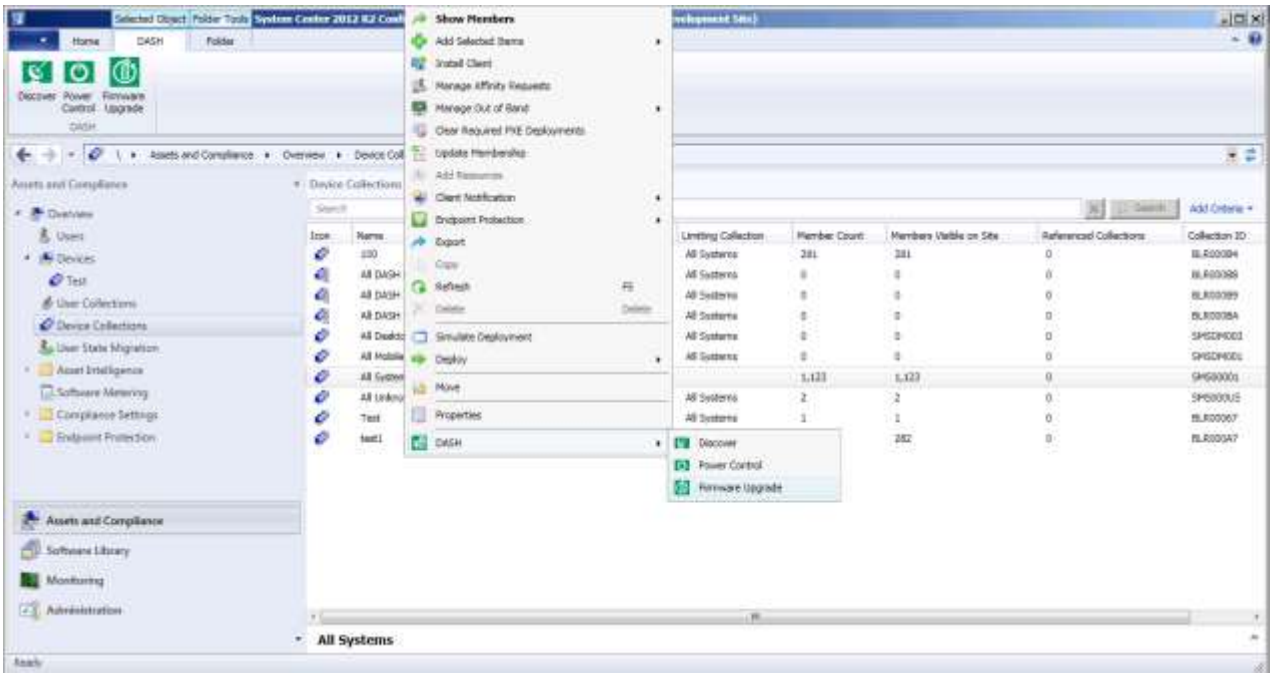


Figure 12-1: Firmware Update on Collection

The **Firware Update on Collection** dialog box appears as shown in **Figure 12-2 and Figure 12-3**

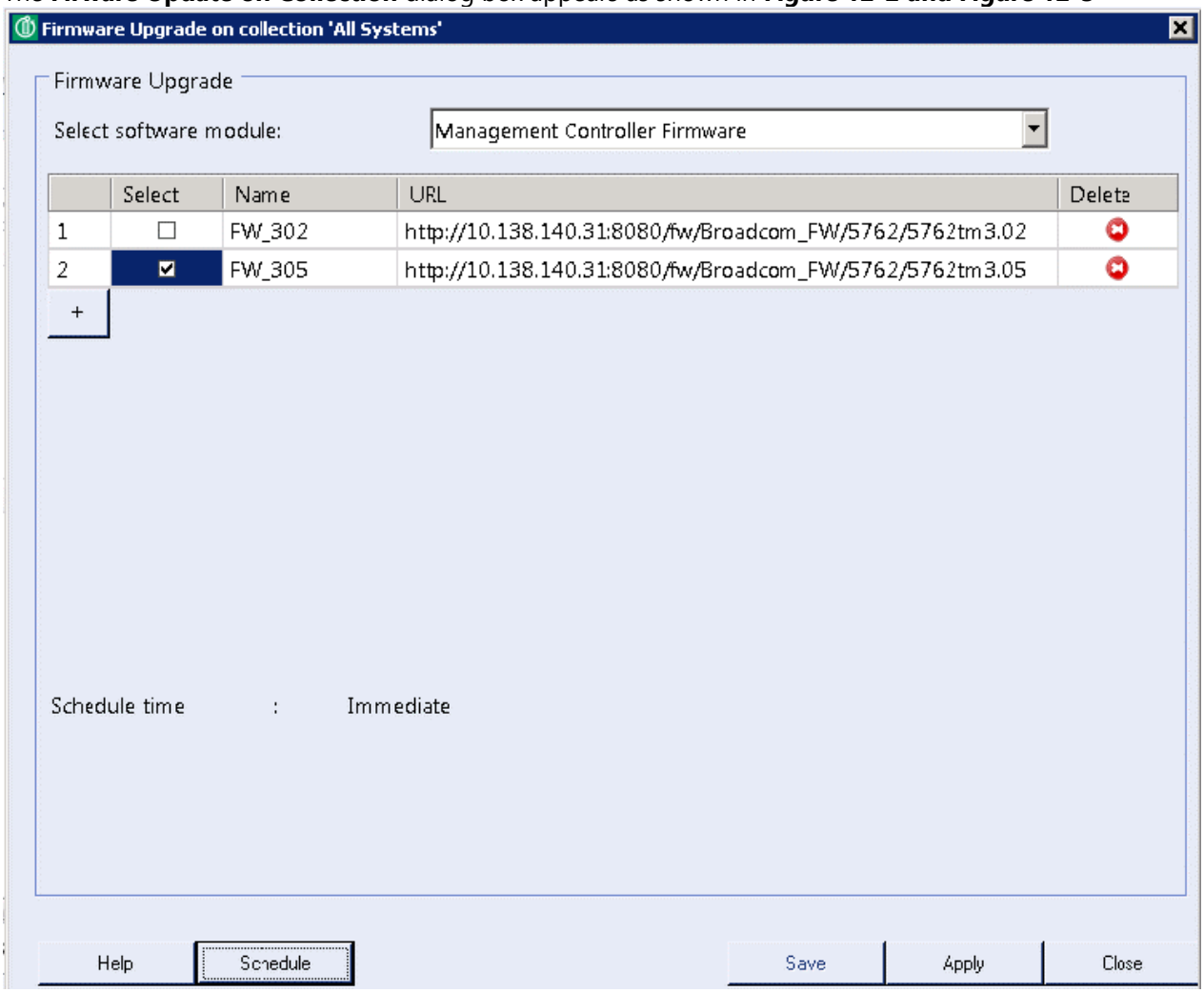


Figure 12-2: Immediate Firmware Update on Collection

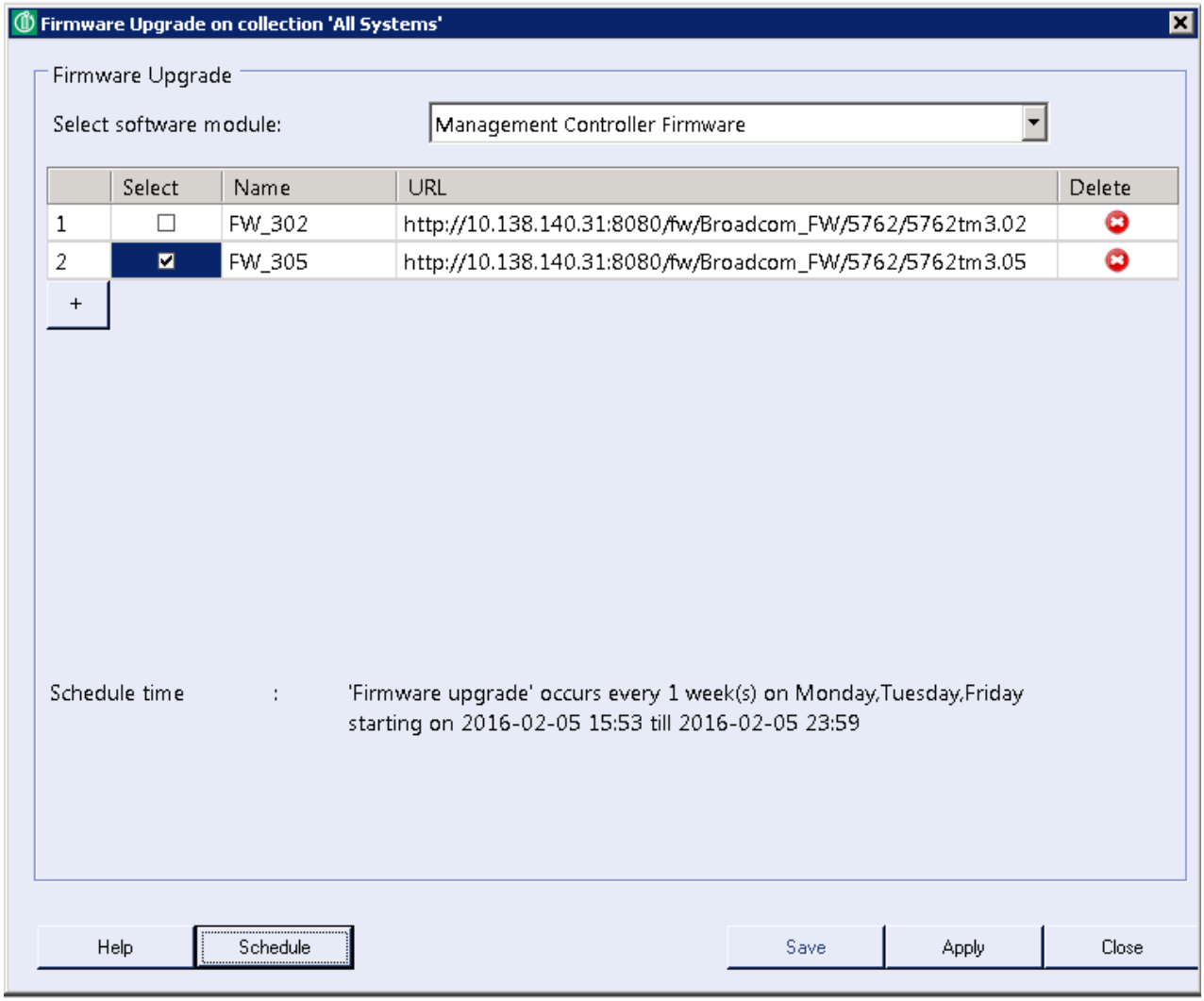


Figure 12-3: Scheduled Firmware Update on Collection

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 Fig 12.2.1) or scheduled (shown in Fig 12.2.2).

   c) The grid shown in the dialog box lists the Firmware URLs of the devices with their Names.
   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 next to the device URL.
   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 12-4**.

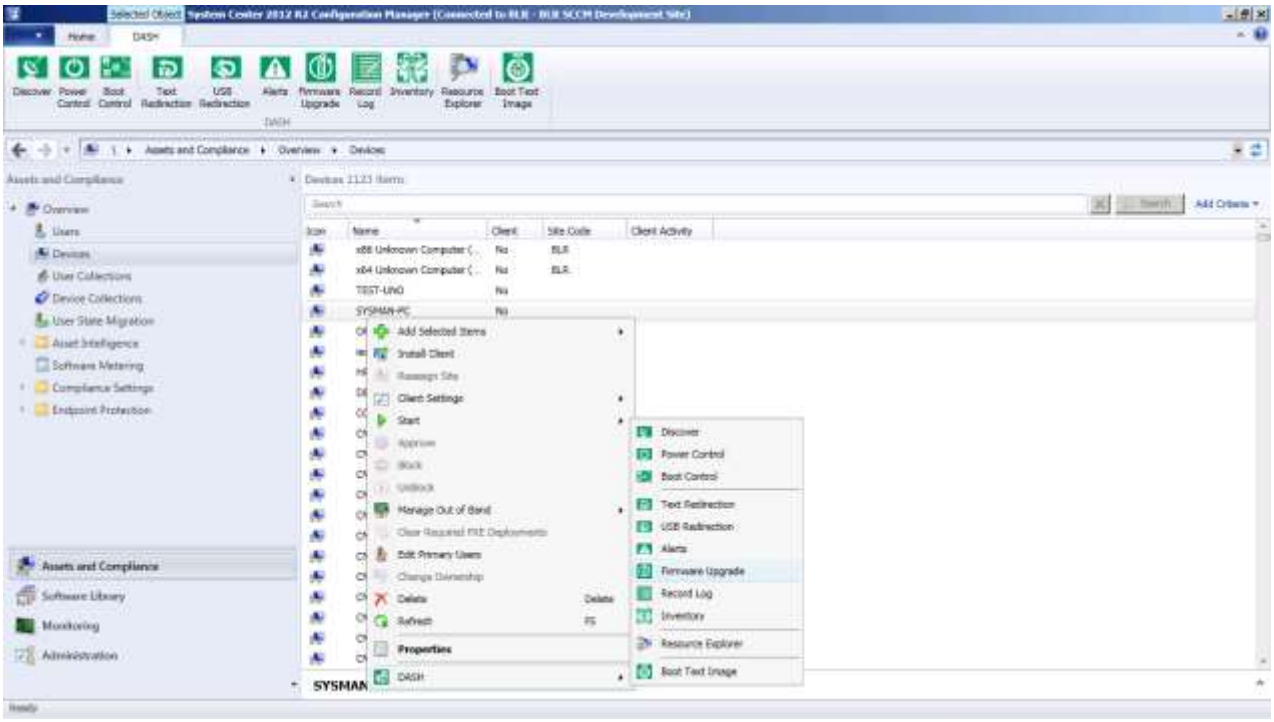


Figure 12-4: Firmware Update on Device

The **Firmware Update on Device** dialog box appears, as shown in **Figure 12-5**.

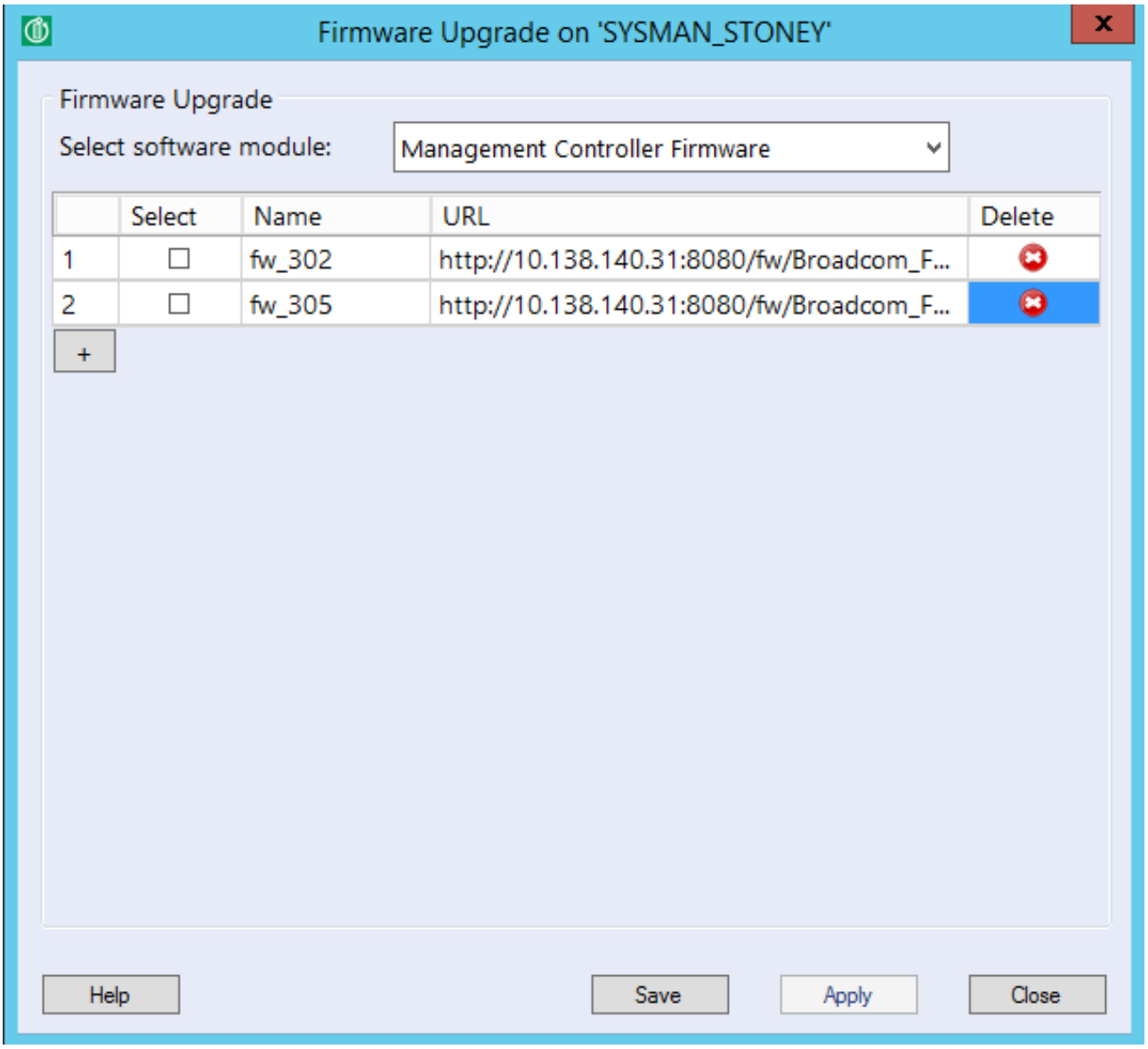


Figure 12-5: Firmware Update on Device

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 ssytem 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 next to the device URL.
    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 10 Firmware URLs can be saved in the list.

Chapter 4 Role-Based Administration

Role-Based Administration (RBA) is a Role-Based Access Control (RBAC) mechanism in Configuration Manager for restricting SCCM 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.

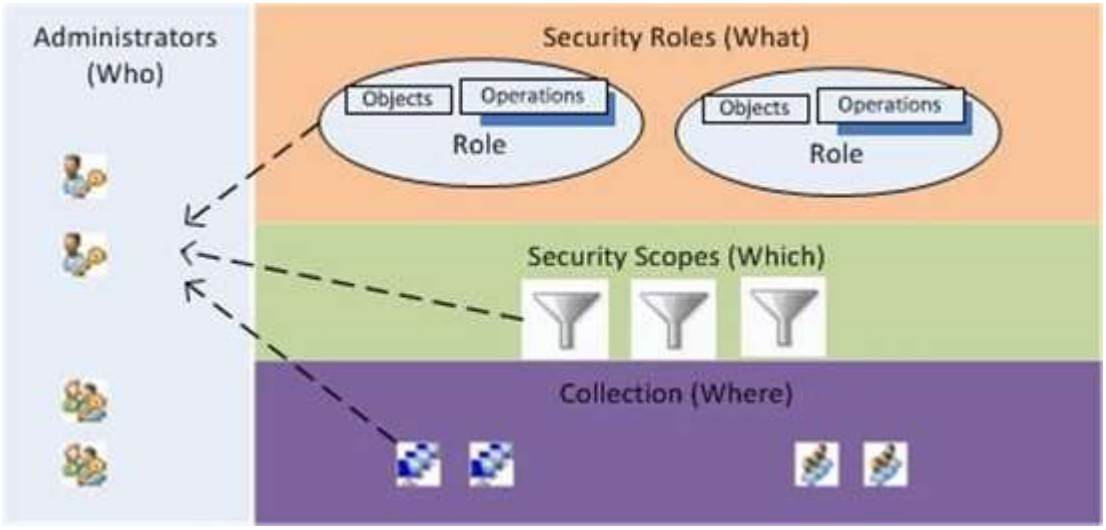


Figure 13-1: Role Based Administration mechanism in SCCM

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 13-2: Selecting Full Administrator role.**

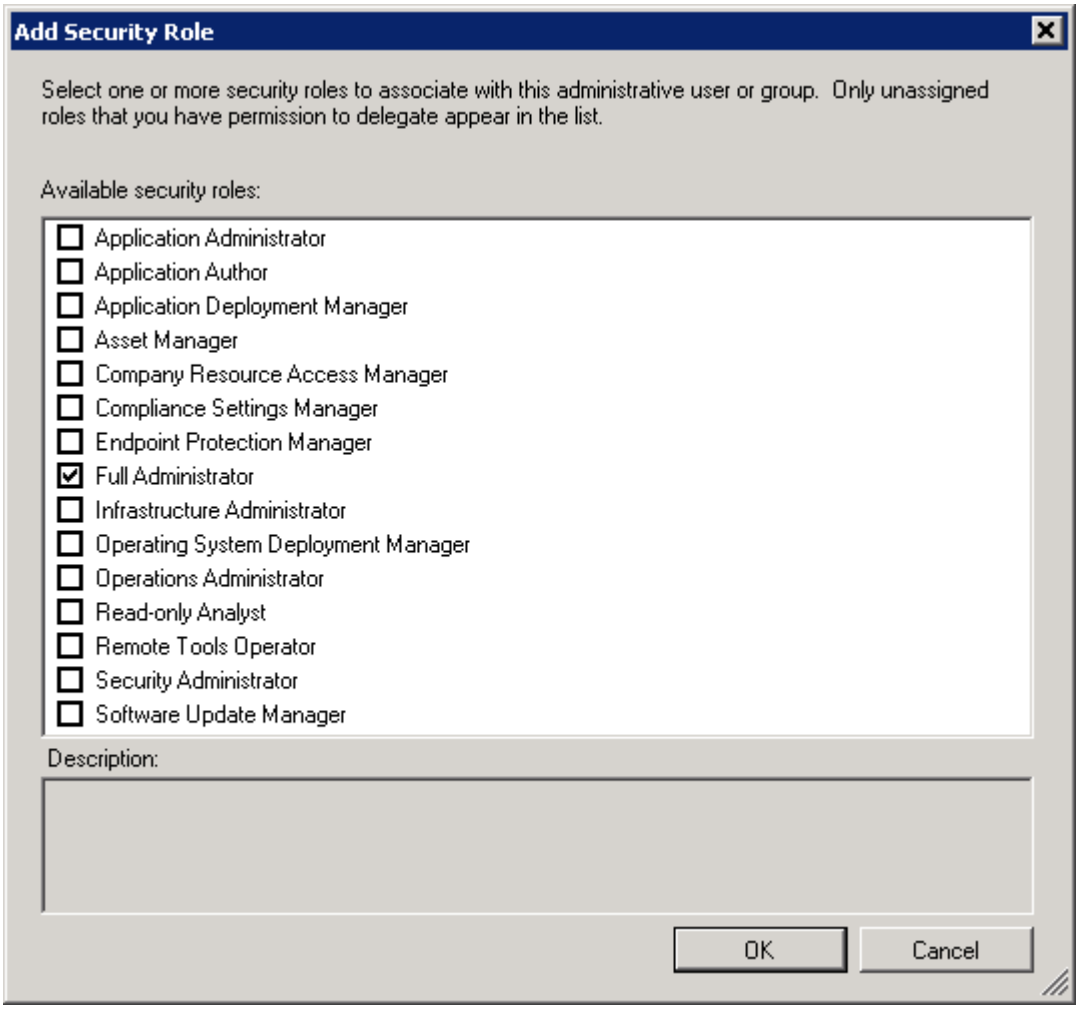


Figure 13-2: Selecting Full Administrator role

4.1.2 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 13-3: Selecting Remote Tools Operator role.**

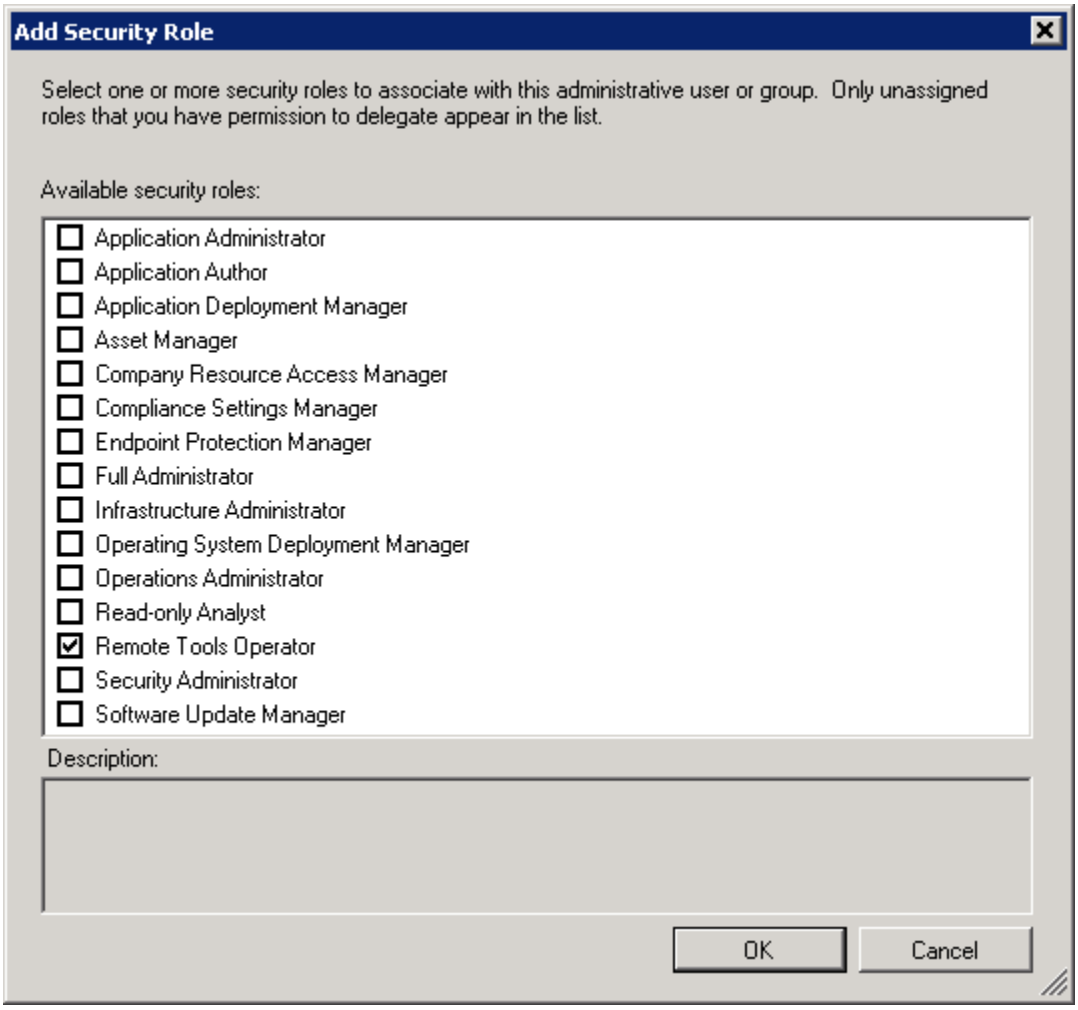


Figure 13-3: Selecting Remote Tools Operator role

4.1.3 DASH Operation

For performing restrictive DASH operations, the Configuration Manager administrative user must have one of these roles:

- Full Administrator
- Remote Tool Operator

User with either Full Administrator role or Remote Tool Operator role can:

- Discover new device
- Change power state
- Change boot order
- Connect via Text redirection
- Connect via USB redirection
- Subscribe and unsubscribe alert filters
- Initiate inventory

All other role users can perform read-only DASH operations such as power status query, view boot configuration, text redirection status, USB redirection status, and subscribed alerts.

4.1.4 DASH Configuration

For modifying DASH configuration settings, the Configuration Manager administrative user must have the Full Administrator role,

All other role users will be able to open DASH Configuration window but do not have permission to change any settings.

4.2 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.

4.3 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.

4.4 Error Messages

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

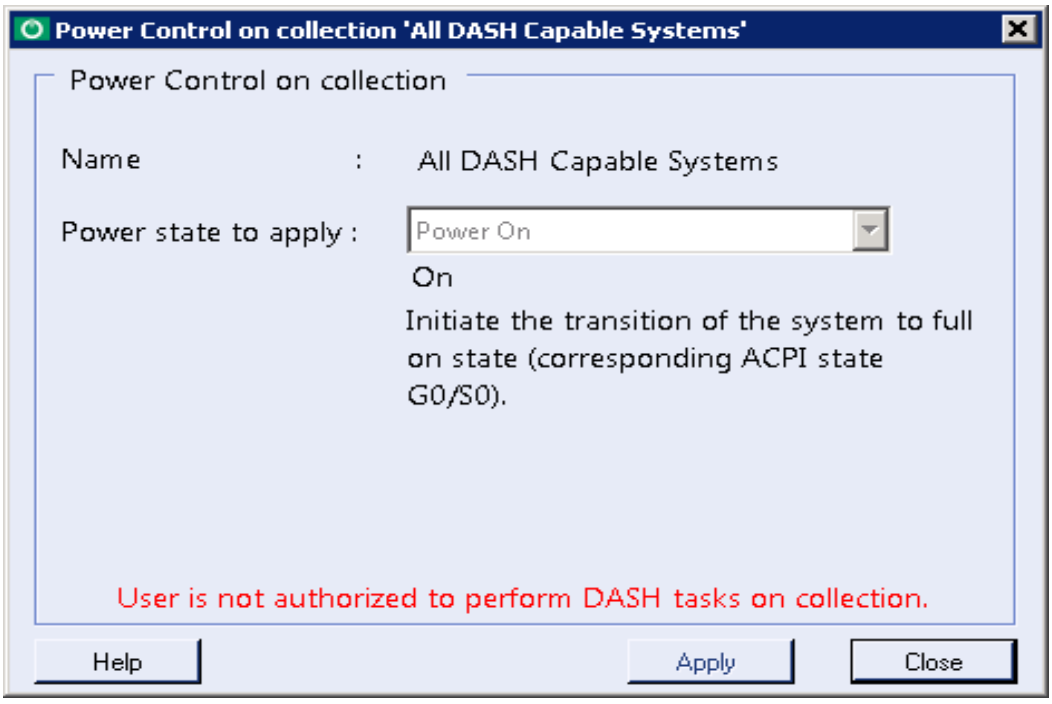


Figure 13-4: Collection Error

- When user is not authorized to perform DASH tasks:

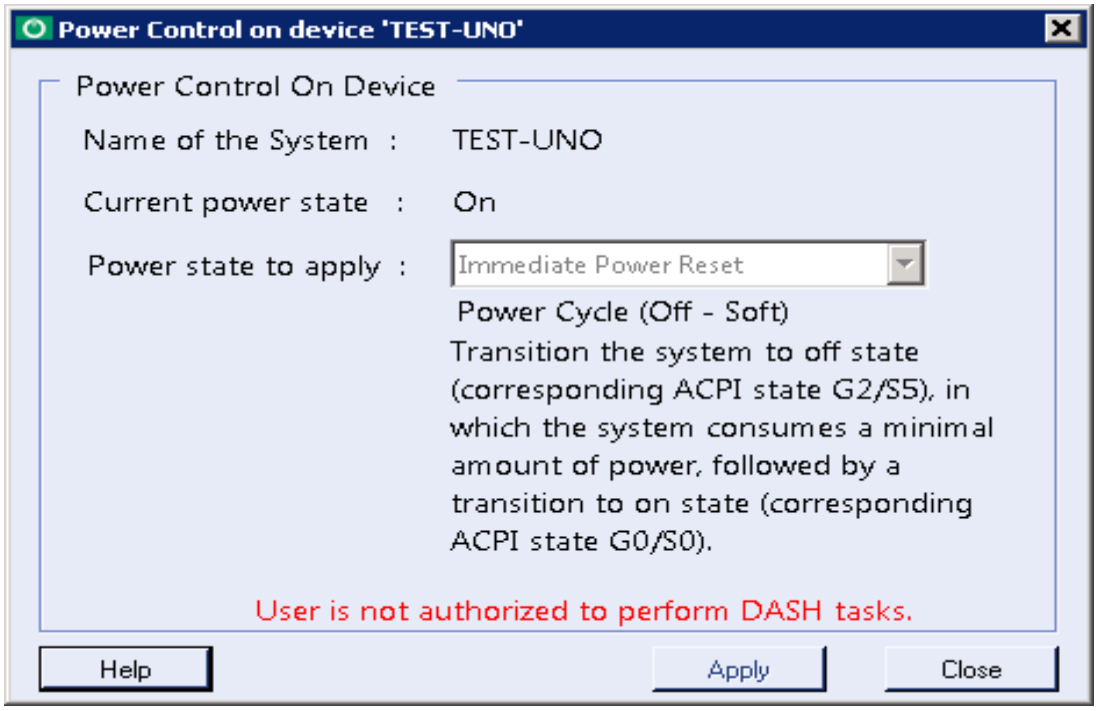


Figure 13-5: Device Error

- When user is not authorized to perform DASH Configuration:

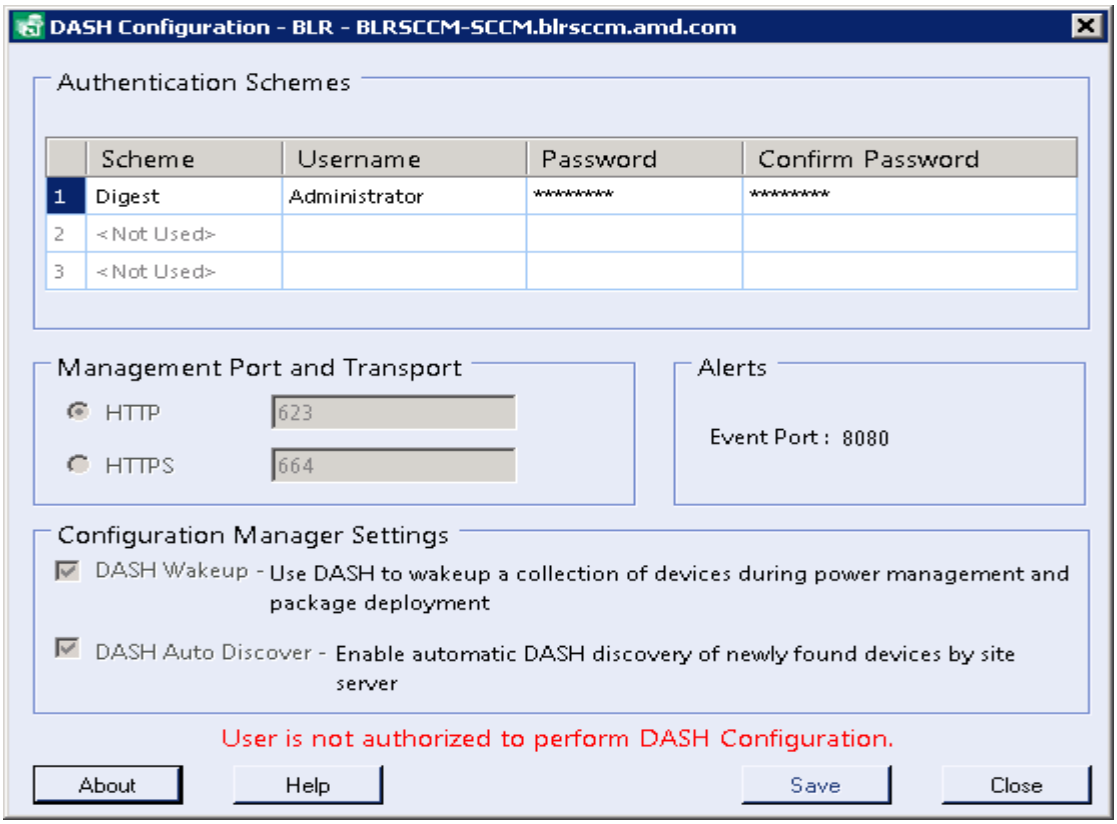


Figure 13-6: DASH Configuration Error

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

5.1 Schedule DASH Tasks

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

- 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 14.1.

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

1. Click the **Schedule** button. (See sections 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.

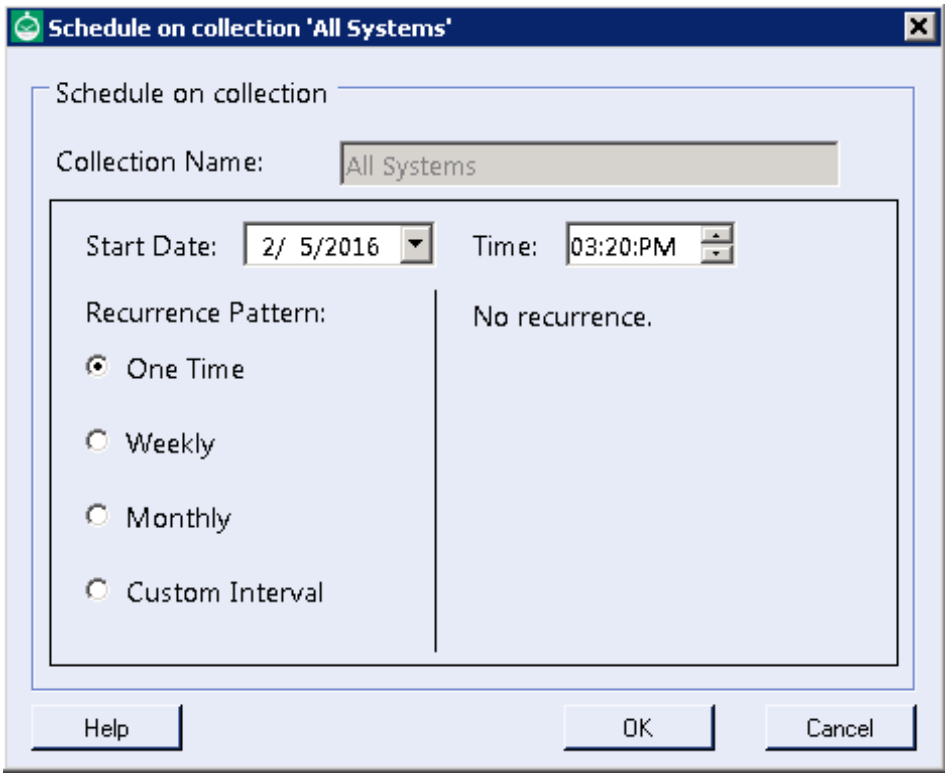


Figure 14-1: DASH Task Scheduler

5.1.1 Recurrence Patterns

The DASH task Sheduler supports the following four recurrence patterns:

5.1.1.1 One time Recurrence Pattern

You can schedule the DASH tasks to run only once.

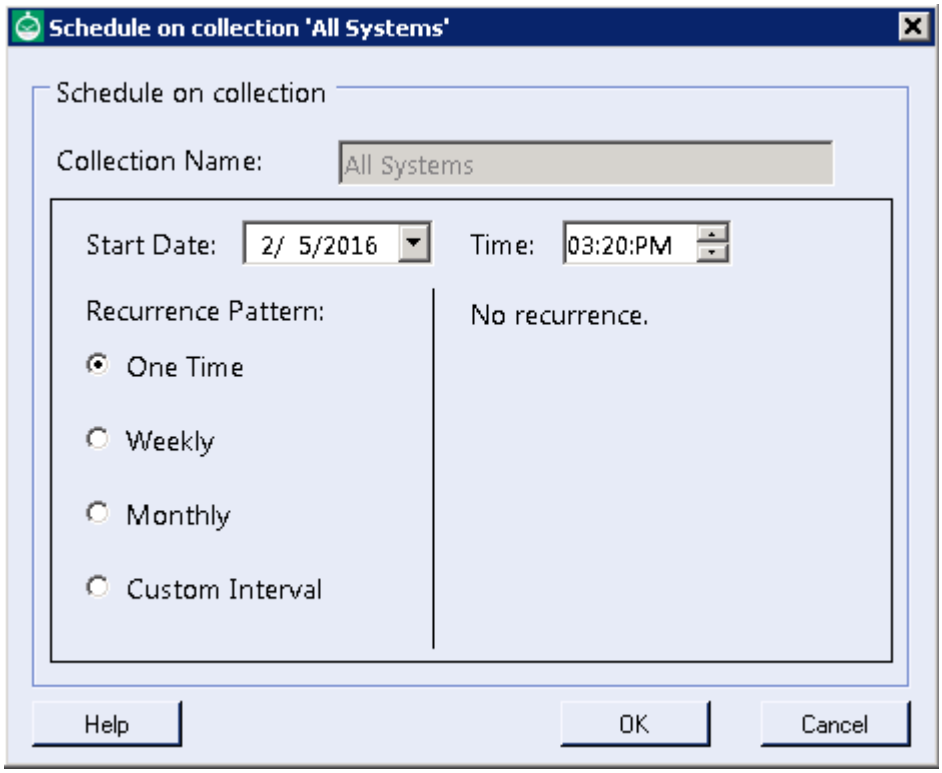


Figure 14-2: DASH Task Scheduler One Time

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 .

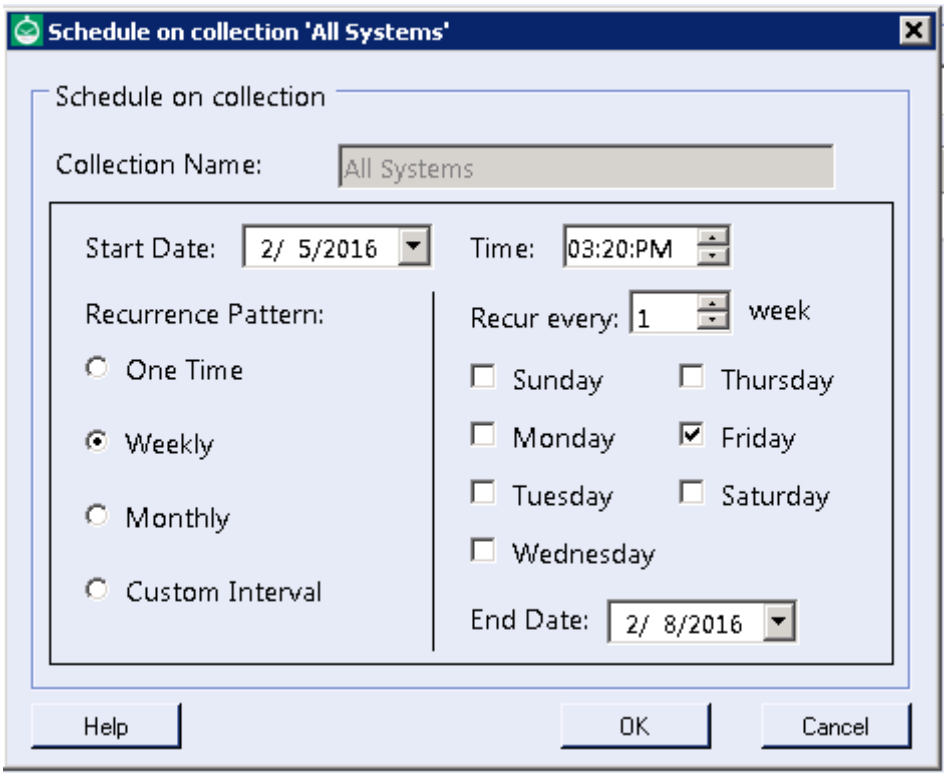


Figure 14-3: DASH Task Scheduler Weekly

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^{th} day of the week

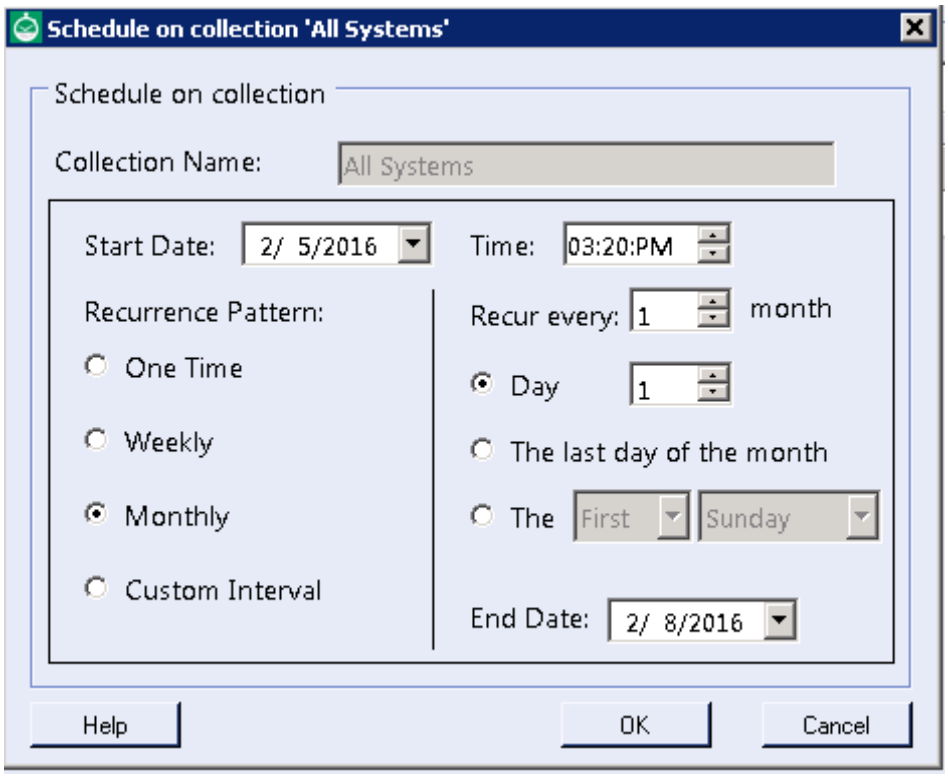


Figure 14-4: DASH Task Scheduler Monthly

5.1.1.4 Custom Recurrence Pattern

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

- Every nth Hour
- Every nth Day

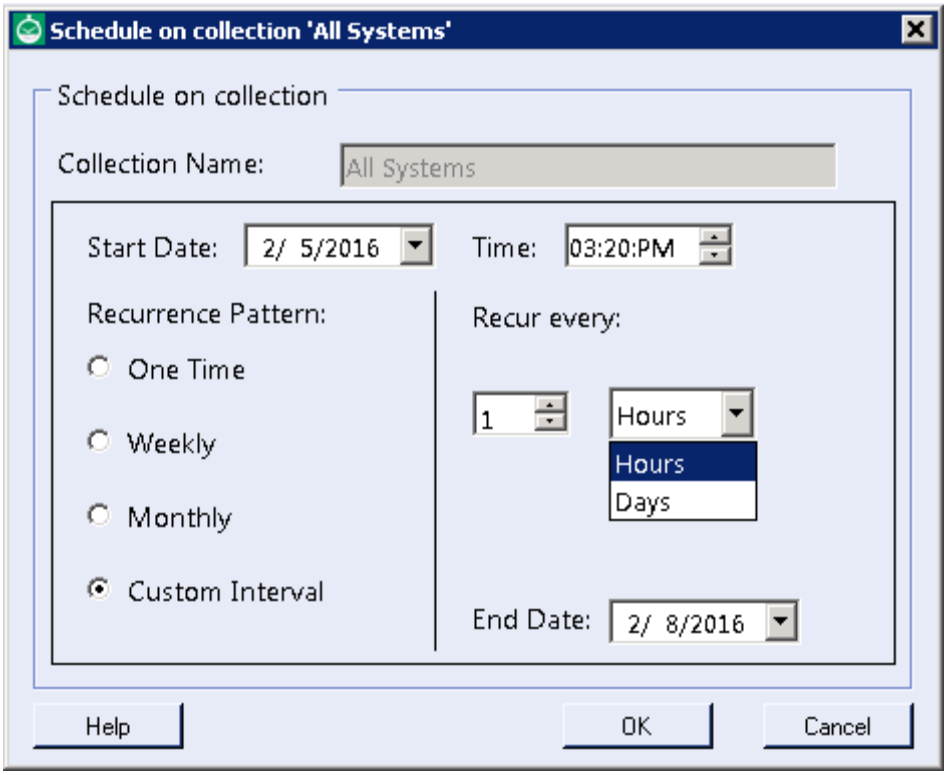


Figure 14-5: DASH Task Scheduler Custom

5.2 DASH Scheduled Tasks

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

It also allows you to 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.

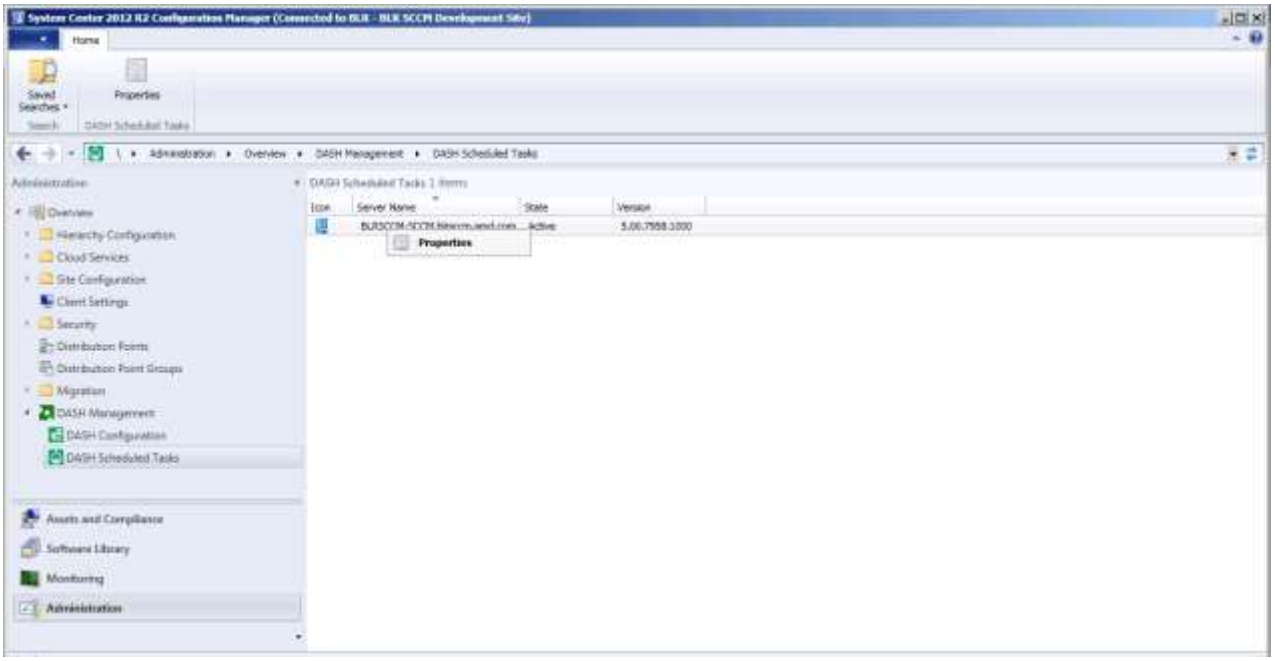


Figure 14-6: DASH Scheduled Tasks Node

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.

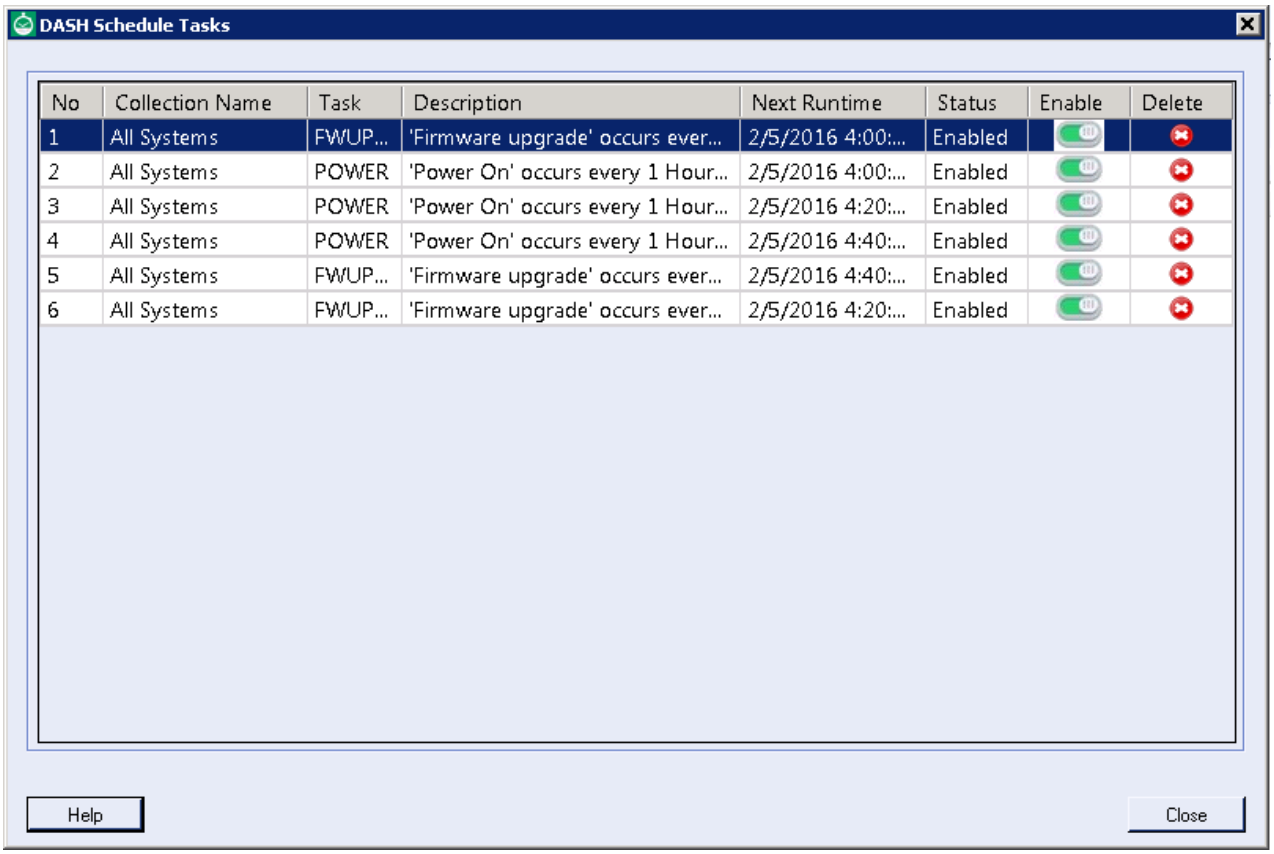


Figure 14-7: DASH Scheduled Tasks

Chapter 6 Reports

6.1 All AMPS Status Messages

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

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 14.1.**
5. Provide **<Time>** parameter to view messages as shown in **Figure 14.2.**

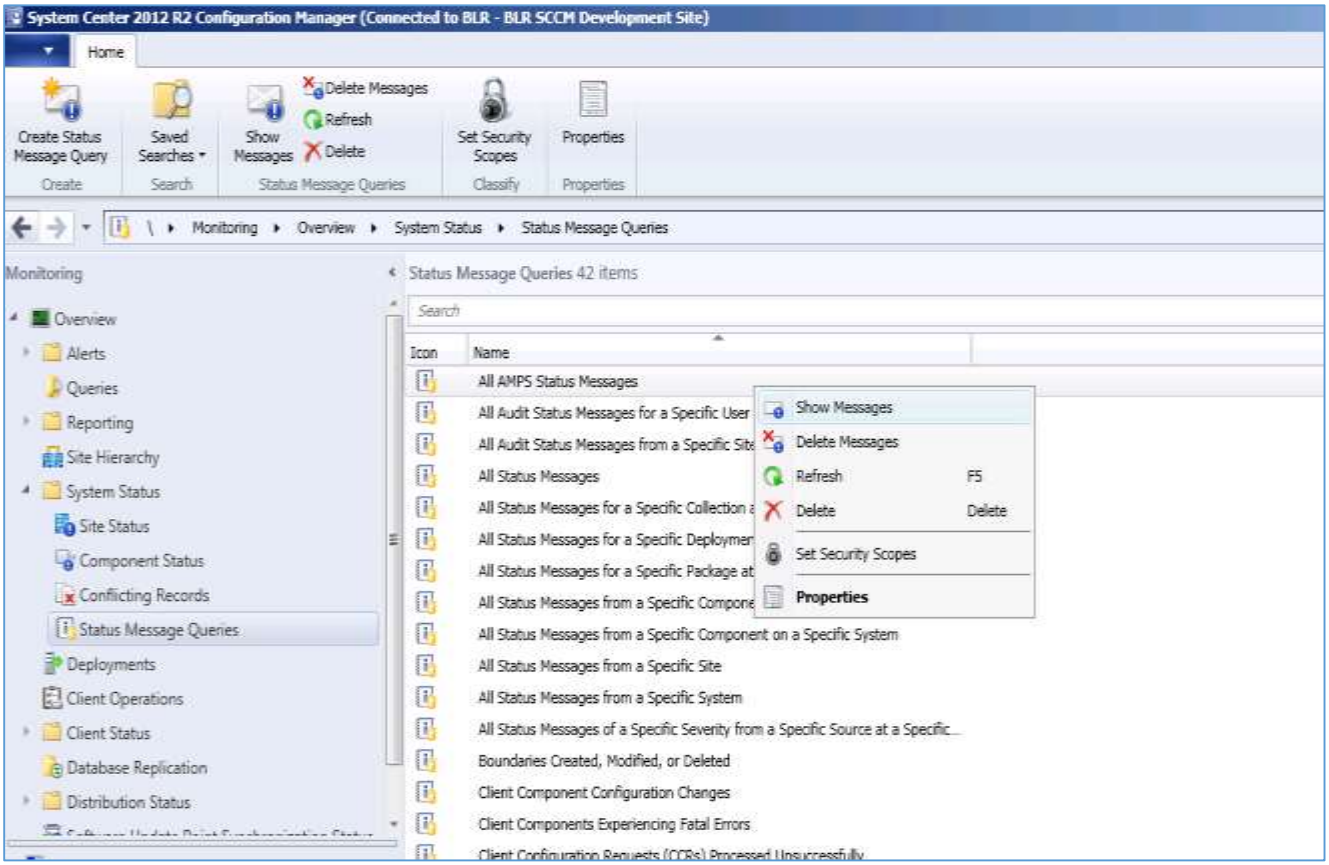


Figure 14-1: All AMPS Status Messages

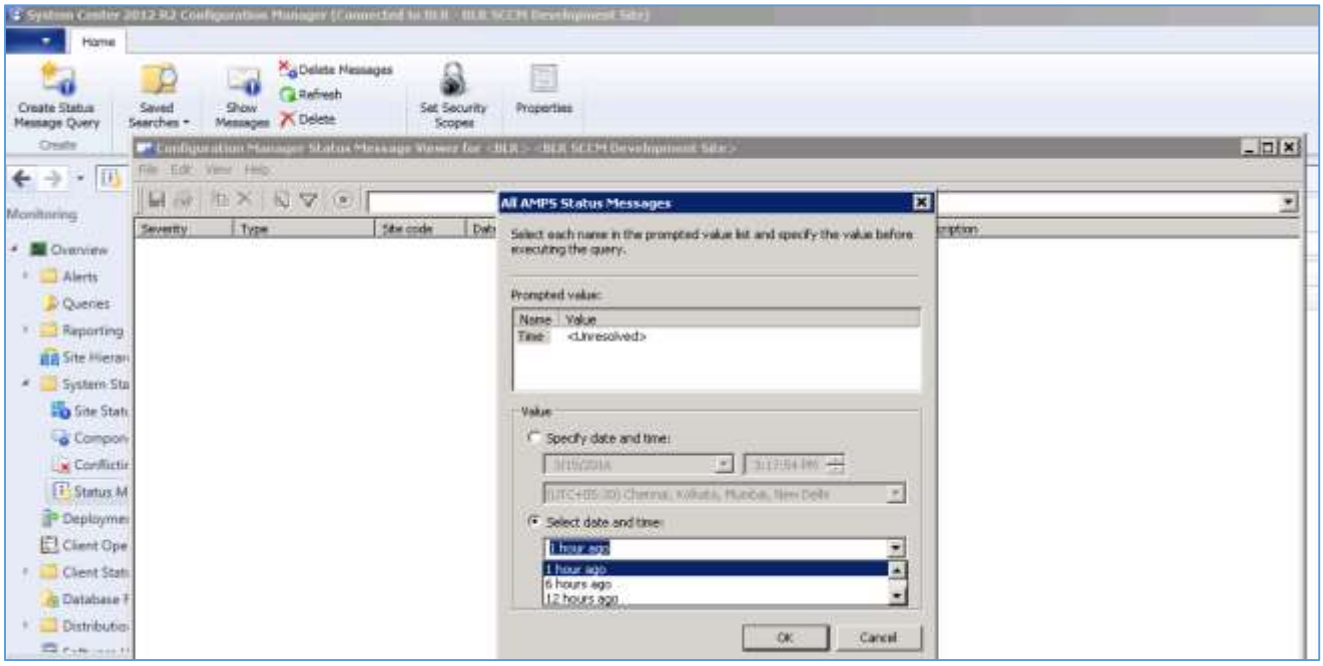


Figure 14-2: All AMPS Status Messages