

AMD DASHConfig Tool

Document version: 1.0

March 27th, 2013

White Paper Descriptor

This whitepaper provides users with detailed description about using AMD DASHConfig tool.

DASHConfig is for provisioning DASH parameters on a DASH-capable system(s). This paper gives details on using DASHConfig tool either as a standalone application or via package deployment tool using Microsoft® System Center Configuration Manager 2007.

Disclaimer

Advanced Micro Devices, Inc. ("AMD") makes no representations or warranties with respect to the accuracy or completeness of the contents of this publication, and reserves the right to discontinue or make changes to products, specifications, product descriptions or documentation at any time without notice. No license, whether express, implied, arising by estoppel, other 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 designed, intended, authorized or warranted for use as components in systems intended for surgical implant into the body, or in other applications intended to support or sustain life, or in any other application in which the failure of AMD's product could create a situation where personal injury, death, or severe property or environmental damage may occur.

While every precaution has been taken in the preparation of this document, Advanced Micro Devices, Inc. assumes no liability of any kind with respect to the operation or use of AMD hardware, software or other products and documentation described herein, for any act or omission of AMD concerning such products or this documentation, for any interruption of service, loss or interruption of business, loss of anticipatory profits, or for punitive, incidental or consequential damages in connection with the furnishing, performance or use of the AMD hardware, software or other products and documentation provided herein. Ensure that you have the latest documentation.

Trademark Attribution

AMD, the AMD Arrow logo and combinations thereof are trademarks of Advanced Micro Devices, Inc. in the United States and/or other jurisdictions. Microsoft and Windows are registered trademarks of Microsoft Corporation. Other names used in this presentation are for identification purposes only and may be trademarks of their respective owners.

©2013 Advanced Micro Devices, Inc. All rights reserved.

Table of Contents

Introduction	4
Prerequisites	4
How DASHConfig Works	4
Tasks Supported in DASHConfig Tool	5
DASHConfig Tool Parameters	5
XML Tags Used for Provisioning	6
Deployment Steps	8
Creating Advertisement	13
Appendix	15
Provisioning XML File Format	15
Case Study	16
Frequently Asked Questions (FAQ)	19
Glossary	20
Conclusion	21
More Information	21

Introduction

Distributed Management Task Force's (DMTF) Desktop and mobile Architecture for System Hardware (DASH) standard is a suite of specifications that is designed to take advantage of DMTF's Web Services for Management (WS -Management) specification, which delivers standards-based web services management for desktop and mobile client systems. Through DASH, DMTF provides the next generation of standards for secure out-of-band (OOB) and remote management of desktop and mobile systems. Configuring and managing DASH-capable systems is an everyday challenge for IT administrators. Administrators must use a variety of tools provided by hardware vendors to configure DASH settings to manage the system remotely. AMD's DASHConfig tool is one attempt to help IT administrators and other end users configure DASH-capable targets more effectively. It is an in-band, Windows® operating system-only tool.

Prerequisites

DASHConfig requires that .NET Framework 2.0, local admin rights, and the vendor-specific DASH agent are installed on the client systems on which the network controller/management target is installed. This support may be found on the OEM's (HP, Dell, etc.) driver support website for the appropriate model.

How DASHConfig Works

Figure 1 describes the flow of DASHConfig. This will interact with the vendor-provided management agent (Windows Management Instrumentation, or WMI, provider); the management agent talks to the DASH firmware and configures the changes provided by the user in an XML file.

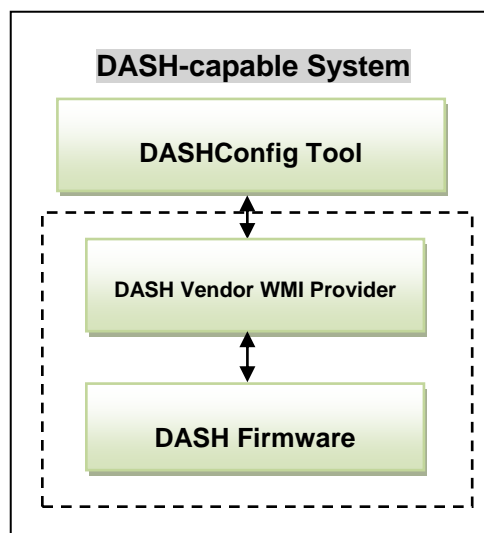


Figure 1: DASHConfig Flow

Note: User must provide the configuration inputs in the XML file. Dotted lines in Figure 1 represent the vendor-provided stack of WMI provider and firmware.

Tasks Supported in DASHConfig Tool

- Enable/Disable DASH management controller
- Set HTTP/HTTPS ports
- Set digital certificates
- Limit discovery (disable HTTP except for discovery)
- Create digest user accounts
- Assign roles
- Active Directory(AD) Provisioning
 - Security Identifier(SID) configuration
 - AD password

DASHConfig Tool Parameters

DASHConfig provides six case-sensitive parameters (-v, -xf, -lf, -dx, -mif and -help) that are defined in the following table.

Parameter	Description
-v	Displays the DASHConfig version information to the console
-xf	Represents the XML file parameter that informs the tool of the location of the XML file used to provision a DASH-capable system.
-lf	Creates the log file to the user-specified path.
-dx	Instructs the DASHConfig utility to delete the provisioning XML file after processing has been completed.
-mif	Instructs the DASHConfig utility to create a Microsoft® installation status MIF file on exit. This is expected to enhance the integration of DASHConfig into products like Microsoft System Center Configuration Manager (SCCM).
-help	This parameter will print out short help documentation about the command line parameters to the console.

XML Tags Used for Provisioning

The following table explains the tags used for provisioning. In the Type column, M = Mandatory and O = Optional

Tag ID	Type	Description
<ENABLEDASHTARGET>	M	Enables or disables DASH-capable systems.
<HTTPS>	O	Sets the HTTPS protocol values to be provisioned.
<HTTP>	O	Sets the HTTP protocol values to be provisioned.
<ENABLESUPPORT>	O	Enables or disables the HTTP, HTTPS, and Active Directory.
<TCPIPPORT>	O	Defines the TCP/IP port number and allows the management target to listen for incoming WS-MAN requests being sent over HTTP or HTTPS connections.
<HTTPREALM>	O	Assigns a new string value to protect the HTTP realm.
<HTTPSTARGETTOCONSOLE>	O	Required if mutual certificate-based authentication is required for HTTPS communication from the management target to the console.
<HTTPSCONSOLETOTARGET>	O	Required if mutual certificate-based authentication is required for HTTPS communication from the console to the management target.
<CERTIFICATEPATH>	O	Provides the certificate path for <HTTPSTARGETTOCONSOLE> and <HTTPSCONSOLETOTARGET> tags.
<LIMITTODISCOVERY>	O	Enables HTTP protocol but limits the protocol's use to only WS-MAN identity discovery requests.
<USERS>	M	Adds user accounts on the management target. Currently there is a limit of 10 provisioned users on any single management target.
<USER>	M	Creates users.
<USERID>	M	Provides the name of the account to be created.
<PASSWORD>	M	Provides the passwords used to authenticate against the associated USERID.
<ENABLE>	M	Determines whether the newly created user account is enabled for use.

Tag ID	Type	Description
<ORGANIZATION>	O	Provisions a group name for the newly created user account.
<ROLES>	O	Defines the roles (privileges) given to the newly created user account.
<ROLE>	O	Provides a specific role(s) to the user. Currently there are only four acceptable values for this node: Administrator Role, Operator Role, Read Only Role, and Auditor Role.
<ACTIVEDIRECTORY>	O	Supports Active Directory when it is provisioned.
<ACTIVEDIRECTORY_SPNACCOUNT>	O	Allows the name string of the Active Directory user account whose service principal name (SPN) property has been updated to include the target's SPN.
<SPNACCOUNT_PASSWORD>	O	Enables an Active Directory stored password for the user account defined by the <ACTIVEDIRECTORY_SPNACCOUNT> node.
<ACTIVEDIRECTORY_GROUPS>	M	Required if any Active Directory group(s) is to be provisioned on the management target. Currently there is a limit of four provisioned groups on any single management target.
<ACTIVEDIRECTORY_GROUP>	M	Required if the <ACTIVEDIRECTORY_GROUPS> node is included in the XML provisioning file.
<GROUPNAME>	O	Required if any Active Directory group(s) is to be provisioned on the management target.
<OBJECTSID>	O	Required for security descriptor string in the standard string representation (S-R-I-S-S) for the Active Directory user group defined by the <GROUPNAME> node.

How to Execute DASHConfig

DASHConfig can be executed in two ways:

- I. **Stand-alone:** If the user has very few DASH targets to configure (e.g., two targets), then the user can log into the respective machines and execute the DASHConfig.

For example:

- **Help:** To get the usage help.

```
DASHConfig.exe -help
```

- **Version:** To find the version information of DASHConfig

```
DASHConfig.exe -v
```

- **Provision DASH Settings :** To set the configuration use the following format

```
DASHConfig.exe -xf:TEST_XML_File.xml -lf:LOGFILE.log
```

- II. **Through deployment:** If the user has more systems to configure (e.g., 50 targets), the user can deploy DASHConfig through the SCCM deployment package. The deployment steps described in the next section show how to create the distribution package.

The user has to use the `-mif` parameter in the command during deployment, which instructs DASHConfig to create a Microsoft installation status MIF file on exit.

For example:

```
DASHConfig.exe -xf:TEST_XML_File.xml -lf:LOGFILE.log -dxf -mif
```

Deployment Steps

Follow these steps to create an SCCM software distribution package for deploying the DASHConfig tool.

Step 1: Open the SCCM Administrator Console Microsoft Management Console (MMC).

Step 2: Under New Package Wizard, enter the following information into the General page controls (Figure 2):

- a. Name: DASHConfig
- b. Version: 1.2
- c. Manufacturer: AMD
- d. Language: English

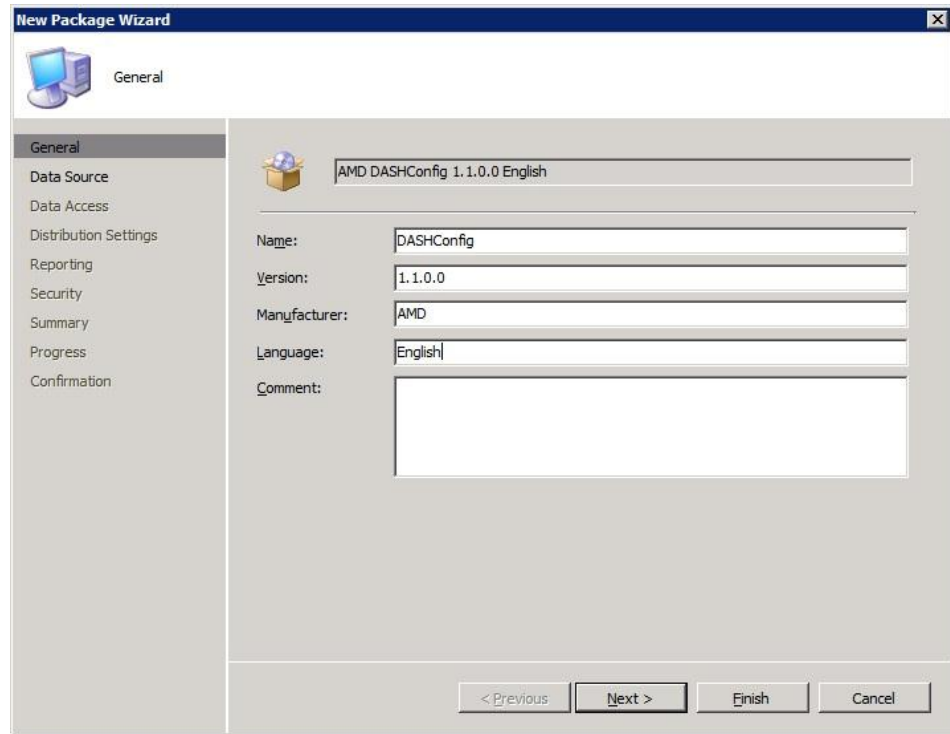


Figure 2: SCCM Administrator Console MMC's New Package Wizard - General

Step 3: On the Data Source page, select the "This package contains source files" checkbox (Figure 3):

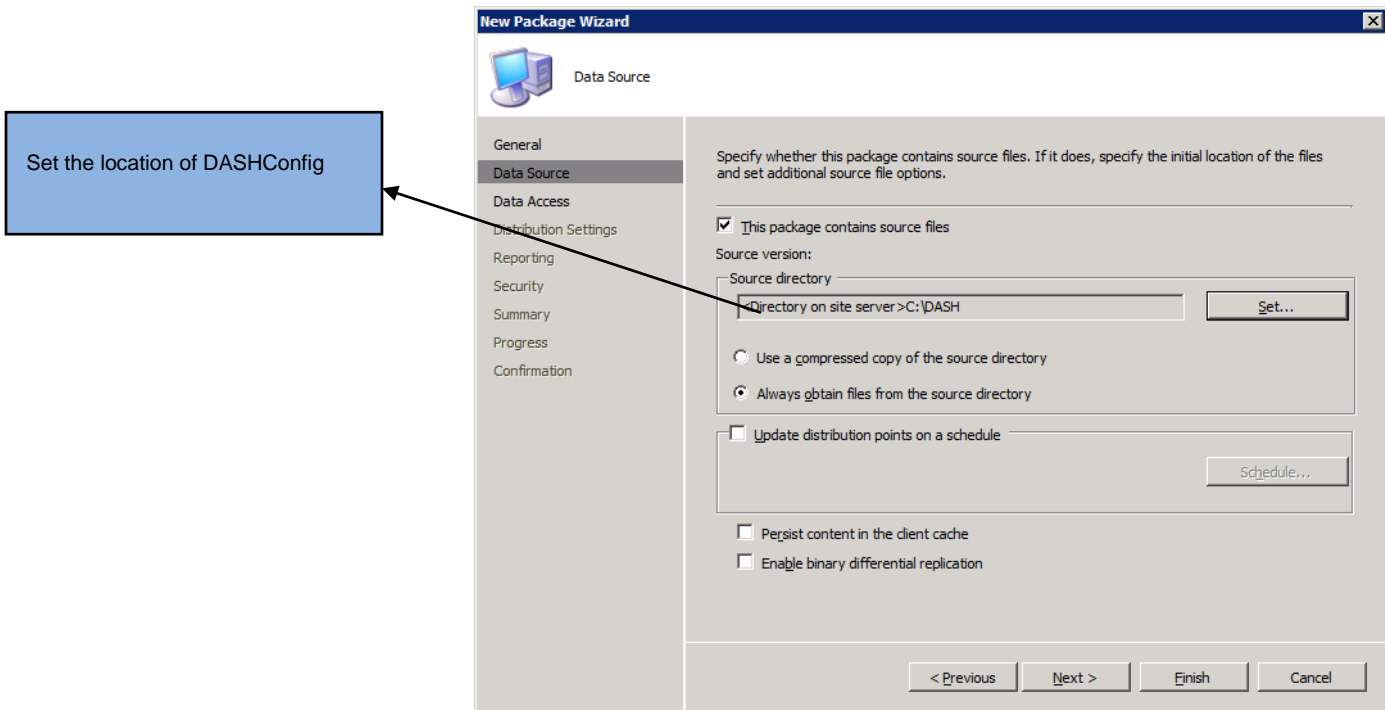


Figure 3: SCCM Administrator Console MMC's New Package Wizard – Data Source

Step 4: On the Distribution Settings page, in the "Sending priority" list box, select High (Figure 4).

Step 5: Also on the Distribution Settings page, in the "Branch distribution point content settings" group box, select the radio button to automatically download content (Figure 4).

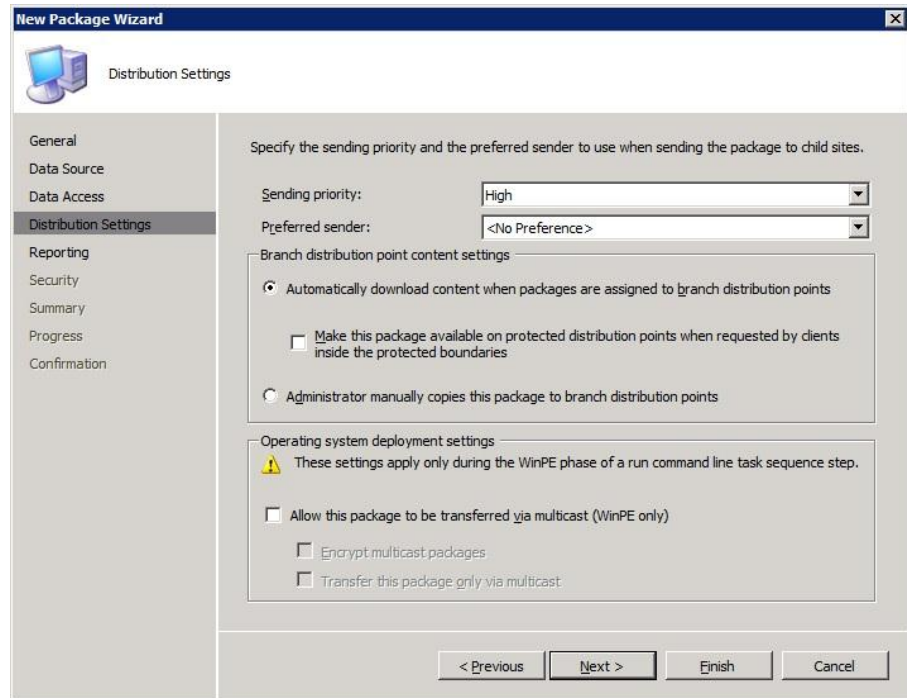


Figure 4: SCCM Administrator Console MMC's New Package Wizard – Distribution Settings

Step 6: On the Reporting page, select the radio button Use package properties for status MIF matching.

Step 7: On the Security page, make sure either the class or instance rights boxes include a domain account that is a member of the DASH system's Local Administrators group.

Step 8: Select the distribution point under New Distribution Points Wizard (Figure 5).

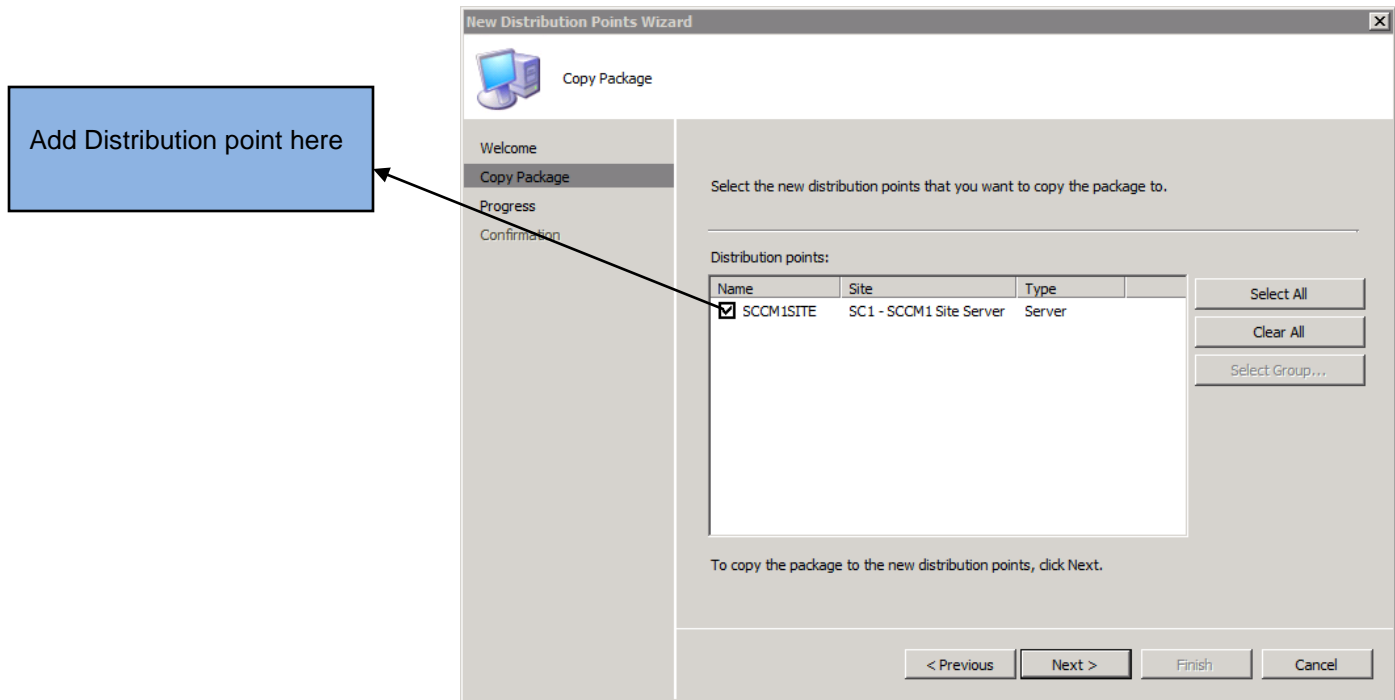


Figure 5: SCCM Administrator Console MMC's New Distribution Points Wizard – Copy Package

Step 9: When the New Program Wizard appears, enter the following information into the General page controls (Figure 6):

- a. Name: DASHConfig
- b. Command line: DASHConfig -xf:DASHConfigExample.xml -dx -mif -lf:DASHConfig.log
- c. Run: Normal

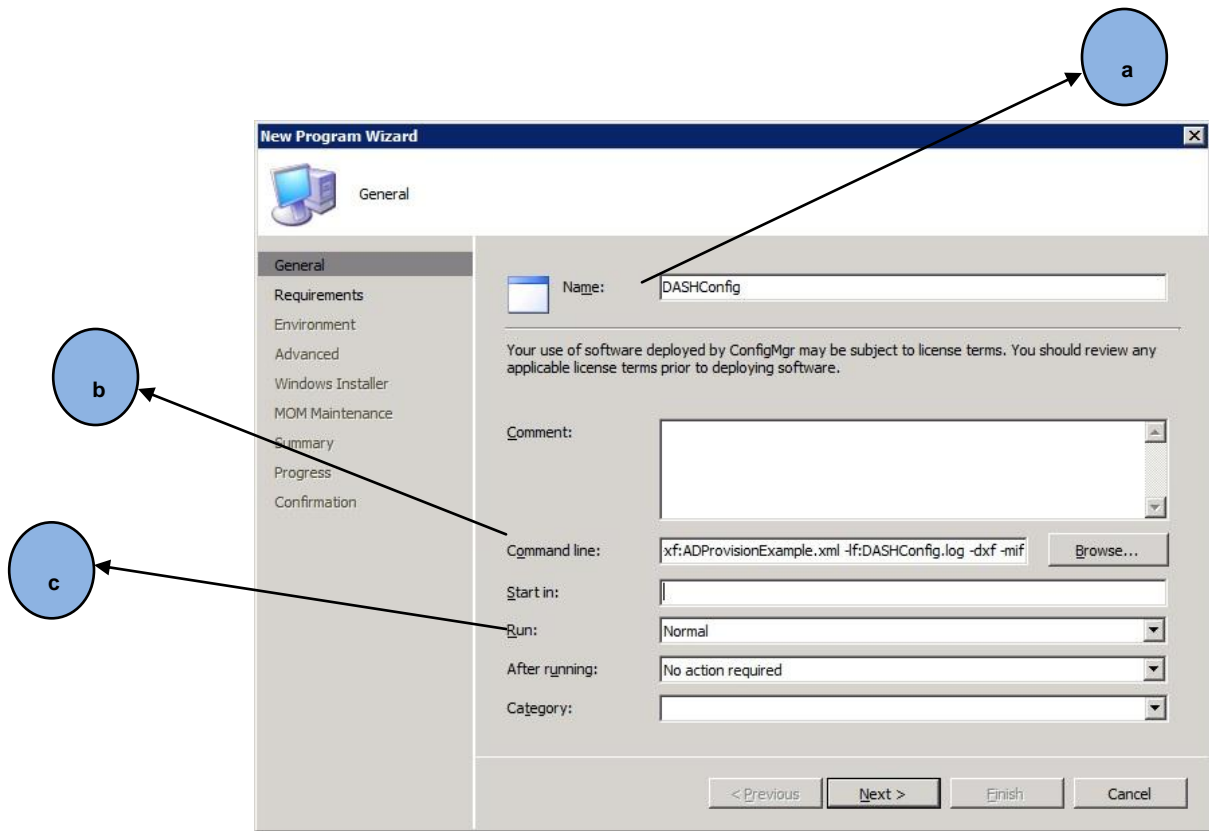


Figure 6: SCCM Administrator Console MMC's New Program Wizard – General

Step 10: Under Requirements, select specific client platforms (Figure 7):

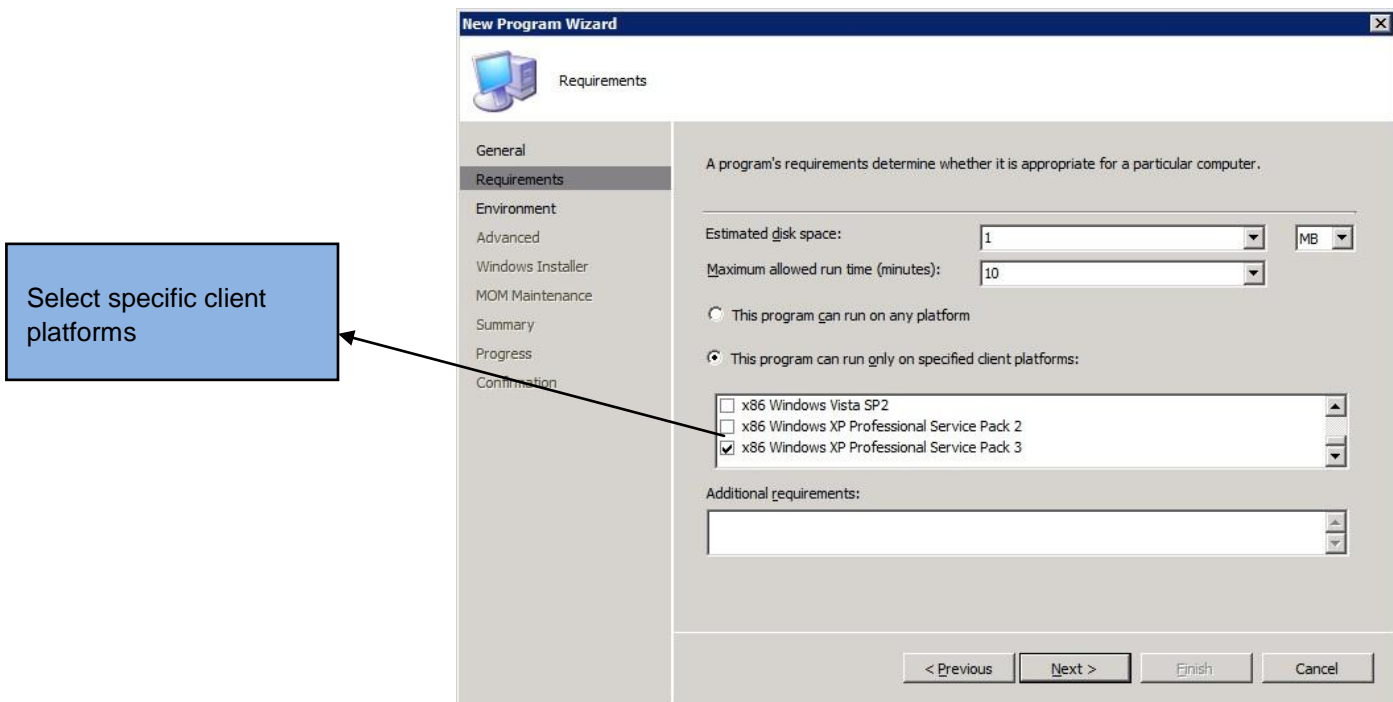


Figure 7: SCCM Administrator Console MMC's New Program Wizard – Requirements

Creating Advertisement

Step 1: Under the New Advertisement Wizard, provide the following information on the General page (Figure 8):

- a. Name: DASH Targets Provisioning
- b. Package: AMD DASHConfig 1.2.0.0 English
- c. Collection: All DASH Capable Systems

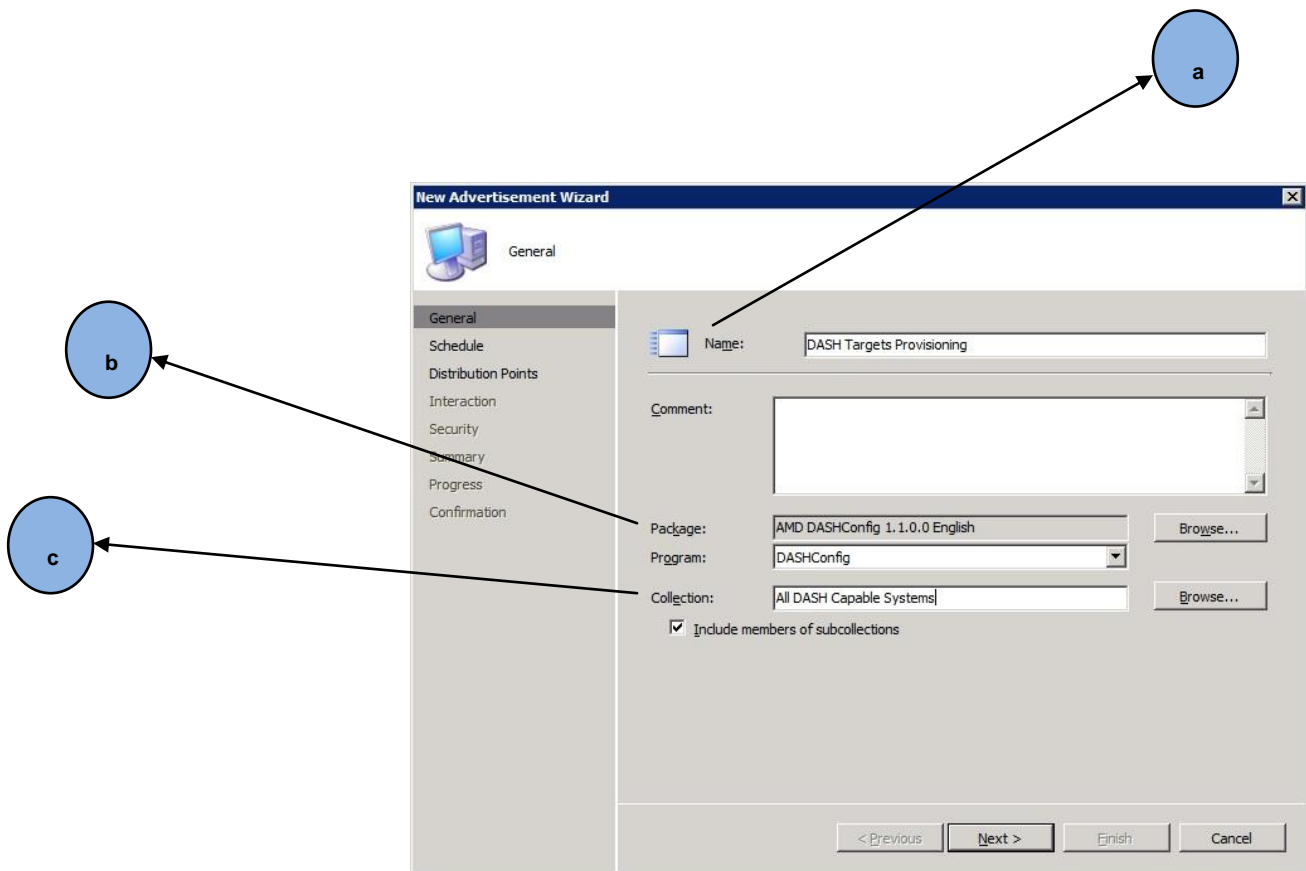


Figure 8: SCCM Administrator Console MMC's New Advertisement Wizard – General

Step 2: Under Schedule, make the following selections (Figure 9):

- a. Mandatory Assignment : As soon as possible
- b. Priority :High
- c. Program rerun behavior :Never rerun advertised program

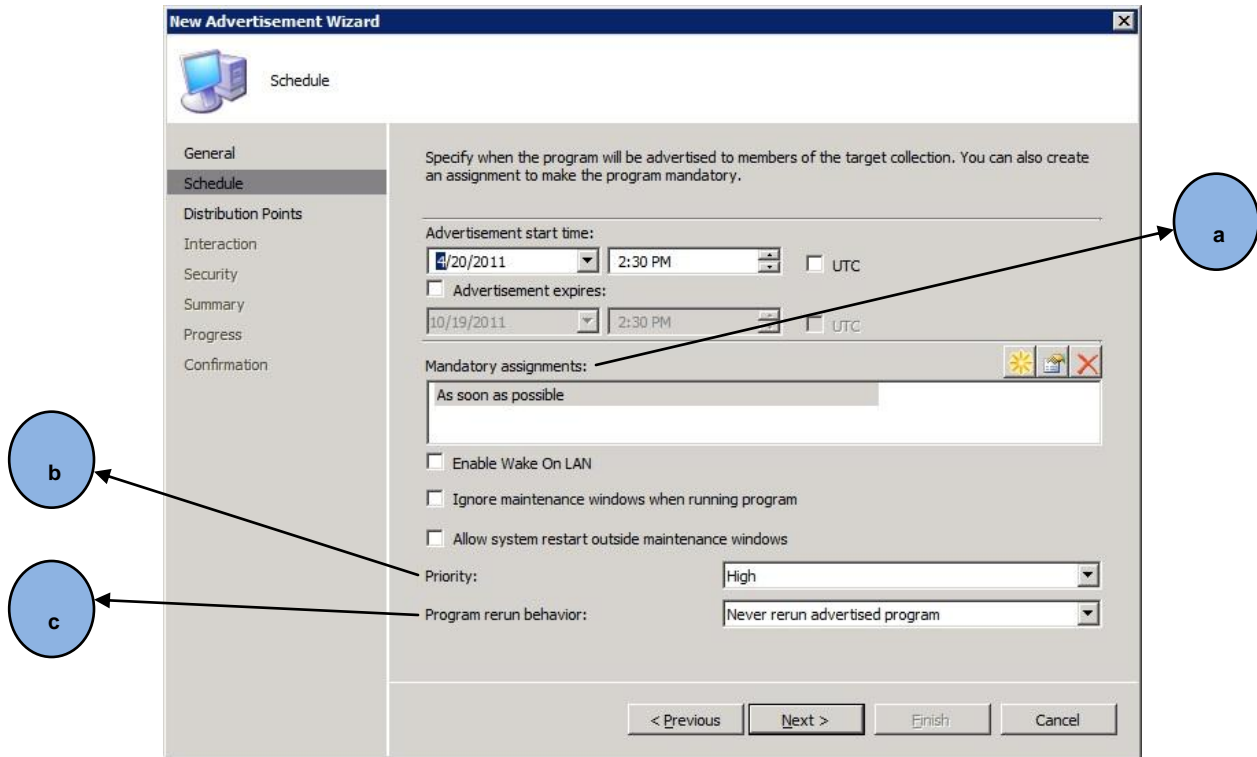


Figure 9: SCCM Administrator Console MMC's New Advertisement Wizard – Schedule

Step 3: Make sure that the advertisement was successfully created. You can check the SCCM system status logs to determine the success of the advertisement, package delivery, and program execution. You can also check the `execmgr.log` file in the DASH machine's `Windows\System32\CCM\Logs` folder. Finally, in the `CCM\cache` folder, check the package's folder for the `DASHConfig.log` file.

Appendix

Provisioning XML File Format

```
<?xml version="1.0" encoding="utf-8" ?>
- <DASHPROVISIONSETTINGS>
- <MANAGEMENTTARGET>
- <GLOBAL>
  <ENABLEDASHTARGET>true</ENABLEDASHTARGET>
  - <HTTPS>
    <ENABLESUPPORT>true</ENABLESUPPORT>
    <TCPSPORT>664</TCPSPORT>
    <HTTPREALM>Broadcom Management Service</HTTPREALM>
  - <HTTPSTARGETTOCONSOLE>
    <CERTIFICATEPATH>DASHAD.cer</CERTIFICATEPATH>
    </HTTPSTARGETTOCONSOLE>
  - <HTTPSCONSOLETOTARGET>
    <CERTIFICATEPATH>DASHAD.cer</CERTIFICATEPATH>
    </HTTPSCONSOLETOTARGET>
  </HTTPS>
  - <HTTP>
    <ENABLESUPPORT>true</ENABLESUPPORT>
    <LIMITTODISCOVERY>true</LIMITTODISCOVERY>
    <TCPSPORT>623</TCPSPORT>
    <HTTPREALM>Broadcom Management Service</HTTPREALM>
  </HTTP>
</GLOBAL>
- <USERS>
- <USER>
  <USERID>Administrator</USERID>
  <PASSWORD>adminpassword</PASSWORD>
  <ORGANIZATION>IT</ORGANIZATION>
  <ENABLE>true</ENABLE>
  - <ROLES>
    <ROLE>Administrator Role</ROLE>
  </ROLES>
</USER>
- <USER>
  <USERID>Auditor</USERID>
  <PASSWORD>readpassword</PASSWORD>
  <ORGANIZATION>IT</ORGANIZATION>
  <ENABLE>true</ENABLE>
  - <ROLES>
    <ROLE>Auditor Role</ROLE>
    <ROLE>Read Only Role</ROLE>
  </ROLES>
</USER>
</USERS>
- <ACTIVEDIRECTORY>
  <ENABLESUPPORT>true</ENABLESUPPORT>
  <ACTIVEDIRECTORY_SPNACCOUNT>DASHSpnUser</ACTIVEDIRECTORY_SPNACCOUNT>
  <SPNACCOUNT_PASSWORD>spnpassword</SPNACCOUNT_PASSWORD>
  - <ACTIVEDIRECTORY_GROUPS>
  - <ACTIVEDIRECTORY_GROUP>
    <GROUPNAME>DASH Admins</GROUPNAME>
    <OBJECTSID>S-1-5-21-000000169-0004209000-0005141000-1155</OBJECTSID>
    - <ROLES>
      <ROLE>Administrator Role</ROLE>
    </ROLES>
  </ACTIVEDIRECTORY_GROUP>
  - <ACTIVEDIRECTORY_GROUP>
    <GROUPNAME>DASH Auditors</GROUPNAME>
    <OBJECTSID>S-1-5-21-000000169-0004209000-0005141000-1156</OBJECTSID>
    - <ROLES>
      <ROLE>Auditor Role</ROLE>
      <ROLE>Read Only Role</ROLE>
    </ROLES>
  </ACTIVEDIRECTORY_GROUP>
</ACTIVEDIRECTORY_GROUPS>
</ACTIVEDIRECTORY>
</MANAGEMENTTARGET>
</DASHPROVISIONSETTINGS>
```

Case Study

This case study illustrates deployment of the DASHConfig tool in a pharmaceutical company.

Business Scenario

Years of dramatic growth through acquisitions and new business opportunities had created one of the US's largest pharmaceutical companies, with 80,000 employees across 255 sites in 160 countries and more than 90,000 IT assets ranging from notebooks and desktops to enterprise-wide applications. To provide remote management of IT assets, as well as to install and update software, the company relied on Microsoft SCCM. While SCCM provides a solution for patch management, inventory reporting, and IT assets reporting, out-of-band management (i.e., ability to manage the system when the OS is not fully up) still remained as biggest challenge.

The IT department had foreseen this challenge and ordered more than 1,000 DASH-capable systems across sites to meet its ever-increasing service-level agreement (SLA) challenge. But enabling DASH functionality on these systems still remained elusive because these systems were dispersed geographically.

Solution Description

In this scenario, the IT department can deploy DASHConfig through Microsoft System Center Configuration Manager (SCCM) to configure the DASH Systems.

Note: It is assumed that all the DASH Systems are in the Active Directory domain.

Step1: Move all the new DASH systems to a collection.

- Create a sub collection (e.g., NewDASHSystems) on SCCM collection tree.
- Make sure that all the DASH systems in the domain controller are listed in SCCM (use discovery methods to confirm).
- Create a rule to move all the DASH-systems to the sub-collection NewDASHSystems.
- Update the collection NewDASHSystems.

Step2: Create a DASH Systems User group.

- Create a DASH systems group (e.g. DASHAdmins) in the domain controller.
- Add IT administrators who are authorized to run DASHConfig to this group.
- Obtain a group SID value from group properties or through the wmic command(e.g., wmic group where "Name='DASHAdmins'" get sid).

Step3: Build the XML based on the following sample format with required DASH configurations.

- The following XML file allows configuration of DASH features like enable DASH target, HTTP/HTTPS ports, digest authentication user, roles and Active Directory .


```

<?xml version="1.0" encoding="utf-8" ?>
<DASHPROVISIONSETTINGS>
  <MANAGEMENTTARGET>
    <GLOBAL>
      <ENABLEDASHTARGET> true</ENABLEDASHTARGET>
      <HTTPS>
        <ENABLESUPPORT> true</ENABLESUPPORT>
        <TCPIPPORT> 664</TCPIPPORT>
        <HTTPREALM> Vendor Management Service</HTTPREALM>
      </HTTPS>
      <HTTP>
        <ENABLESUPPORT> true</ENABLESUPPORT>
        <LIMITTODISCOVERY> false</LIMITTODISCOVERY>
        <TCPIPPORT> 623</TCPIPPORT>
        <HTTPREALM> Vendor Management Service</HTTPREALM>
      </HTTP>
    </GLOBAL>
    <USERS>
      <USER>
        <USERID> Administrator</USERID>
        <PASSWORD> adminpassword</PASSWORD>
        <ORGANIZATION> IT</ORGANIZATION>
        <ENABLE> true</ENABLE>
        <ROLES>
          <ROLE> Administrator Role</ROLE>
        </ROLES>
      </USER>
    </USERS>
    <ACTIVEDIRECTORY>
      <ENABLESUPPORT> true</ENABLESUPPORT>
      <ACTIVEDIRECTORY_SPNACCOUNT> DASHSpnUser</ACTIVEDIRECTORY_SPNACCOUNT>
      <SPNACCOUNT_PASSWORD> spnpassword</SPNACCOUNT_PASSWORD>
      <ACTIVEDIRECTORY_GROUPS>
        <ACTIVEDIRECTORY_GROUP>
          <GROUPNAME> DASHAdmins</GROUPNAME>
          <OBJECTSID> S-1-5-21-000000169-0004209000-0005141000-1155</OBJECTSID>
          <ROLES>
            <ROLE> Administrator Role</ROLE>
          </ROLES>
        </ACTIVEDIRECTORY_GROUP>
      </ACTIVEDIRECTORY_GROUPS>
    </ACTIVEDIRECTORY>
  </MANAGEMENTTARGET>
</DASHPROVISIONSETTINGS>

```

Step 4: Create an SCCM package.

- Use the deployment steps to create the package (refer to the Deployment Steps section earlier in this document).
- Provide the DASHConfig command line with -mif option during package creation (e.g., DASHConfig -xf:DASHConfigExample.xml -dx -mif -lf:DASHConfig.log)

Step 5: Create an advertisement.

- Create an advertisement on a collection NewDASHSystems to execute the DASHConfig utility on all DASH systems in the collection.

Step 6: Verify the log files

- Once DASHConfig is executed on DASH systems, mif and log files will be generated and stored in the respective DASH systems. The user can check the generated DASHConfig.log in C:\Windows\system32\CCM\Cache location and DASHConfig.mif in C:\Windows.

Benefits

- The IT administrator can avoid traveling to different geographical locations to configure the DASH PC's, which reduces the expenses of time, cost and other resources.
- Because configuring and reconfiguring DASH systems is easy via distribution-point deployment, information security policies such as password change can be deployed easily.
- The IT administrator can also enforce security hardening for HTTP/HTTPS settings such as limiting HTTP to discovery on a need-by-need basis.

Frequently Asked Questions (FAQ)

Q: Can I use the DASHConfig tool without administrative privileges?

A: No. You need administrative rights to execute DASHConfig.

Q: How do I provide the configuration settings?

A: Configuration settings data are provided in an XML file, an example of which is provided in this paper.

Q: Is DASHConfig CLI supported in Linux OSes?

A: No. As of now, DASHConfig is supported only on Windows OSes.

Q: Where can I get additional information on DASHConfig?

A: Visit the DASH discussion forum: www.amd.com/DASH

Glossary

The following terms are used to describe the components of DASHConfig.

DASH

Desktop Mobile Architecture for System Hardware, the new DMTF Commercial Client management standard produced by the DMTF DMWG. DASH specifies the transport, management protocol (WS-Man), and DMTF CIM profiles used to manage desktop and mobile PCs.

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.

Out-of-band management:

OOB management tasks are those performed independent of the power or OS state on the managed client or system.

Dash-capable system

A DASH-capable system is a computer system that conforms to the DMTF DASH standard.

SCCM

Microsoft System Center Configuration Manager 2007 R2

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).

.

DMTF

Distributed Management Task Force, Inc

Conclusion

DASHConfig is a tool which is used for setting the DASH configuration parameters like HTTP, HTTPS, Active Directory, digest authentication etc. on a DASH-capable system. It reduces the overhead of managing and configuring multiple DASH-capable systems in a IT network.

More Information

DASH Forum

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

System Center Configuration Manager 2007

<http://technet.microsoft.com/en-us/systemcenter/bb507744>

MYITForum

<http://www.myitforum.com/>