Security Rights-based authorization in DASH Plugin for SCCM

An overview of the "User Permission Checking" feature

White Paper Descriptor

This white paper describes how a role-based security model can be adopted for performing DASH operations on a DASH-capable system from Microsoft® System Center Configuration Manager 2007 using DASH Plugin v1.7

Document date:	27-Sep-2012
Document version:	1.0

Table of contents

Table of figures

Introduction

Microsoft System Center Configuration Manager 2007 R2 (SCCM) is the solution for comprehensively assessing, deploying, and updating servers, clients, and devices across physical, virtual, distributed, and mobile environments. Optimized for Windows® desktop and server platforms, it is the best choice for centralizing management from the datacenter to the desktop.

DASH Plugin extends SCCM to support out-of-band (OOB) management tasks using Distributed Management Task Force (DMTF)-defined DASH protocols. DASH Plugin is a simple install over SCCM and enables SCCM to perform DASH operations on a DASH-capable system.

The release of DASH Plugin version 1.7 implements a security rights-based authorization model for DASH operations. This feature is also called user permission checking. Using the object security rights of users on collections of SCCM, IT administrators can authorize and manage which users are permitted to perform a given DASH operation on a system.

Note*:* Throughout this document, the term "SCCM" is used to refer to Microsoft System Center Configuration Manager 2007 R2, and the term "DASH Plugin" is used to refer to DASH Plugin v1.7 for SCCM.

Audience

This document is intended for IT administrators interested in implementing a security rights-based authorization model in SCCM for DASH Plugin tasks. It provides a technical overview of the object security rights defined for DASH tasks. It also describes how to configure the SCCM and DASH Plugin for checking a user's permission prior to performing any DASH operation.

Prior knowledge

The administrator should have knowledge of the following technologies:

- System Center Configuration Manager 2007.
- DASH Plugin for SCCM.
- Object security in SCCM for collection, site classes, and instances.

Overview of collections in SCCM

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

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

For example, a new version of an OS-specific graphics driver can be deployed across the enterprise (spanning multiple geographies) by creating OS-specific collections created by querying the OS of all systems to find systems running Windows XP, Windows Vista, Windows 7, or Windows 2008.

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

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

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

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

Overview of collection object's security in SCCM

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

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

Security for an SCCM collection can be configured at either the class level or at the instance level:

Class level

This level grants users permissions for all object types in a specific class -- for example, Collections.

Instance level

This level grants permissions for a specific instance of an object type, such as the "All Windows 7 Systems" collection or a "New York City Systems" collection.

In both cases, permissions can be granted or denied on a per-user or user-group basis.
Collection class and collection instances are depicted in Figure 1.

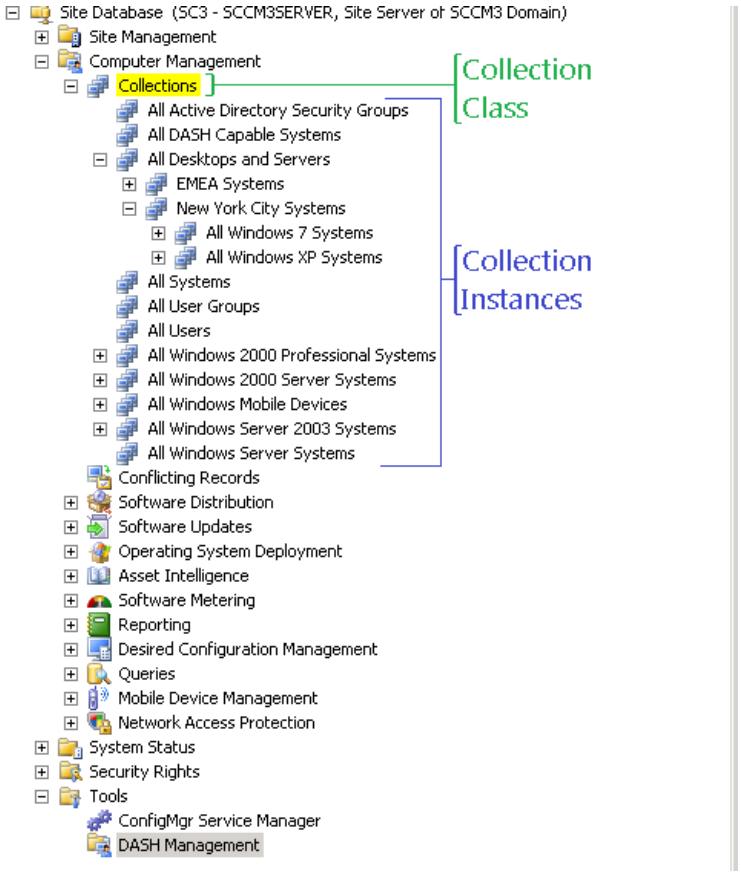


Figure : Collection class and collections instances as seen in SCCM Administrator Console.

SCCM collection security rights

Commonly used security rights of a collection object:

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

Security rights defined for DASH tasks

Some of the DASH tasks are:

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

Collection class/instance

The security rights, "Read Resource" or "Use Remote Tools" on Collection class or Collection class instance, control the user's permission for DASH tasks.

Read resource

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

- View hardware inventory
- Check power status
- Retrieve boot order
  Perform DASH discovery

Use remote tools

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

Security rights for DASH operations

Table : Security rights required for DASH tasks

DASH Task	Right	Grants the ability to
Discover	Create, Modify, and Read Resource	Identify whether a system is DASH-capable or not. Get version information and the profiles supported.
Power	Read Resource	Obtain current power state of the system.
	Use Remote Tools	Change power state of the system.
Boot	Read Resource	Obtain boot order information.
	Use Remote Tools	Change boot order of the system.
Inventory	Read Resource	Obtain hardware inventory of the system.
Text and USB Redirection	Read Resource and Use Remote Tools	Redirect BIOS screen, boot to remote ISO image.
Alerts/Events	Read Resource and Use Remote Tools	Subscribe and unsubscribe to all or selected event alerting.
Account Management	Read Resource	View list of digest accounts on DASH-capable system.
	Use Remote Tools	Modify the digest account on DASH-capable system.

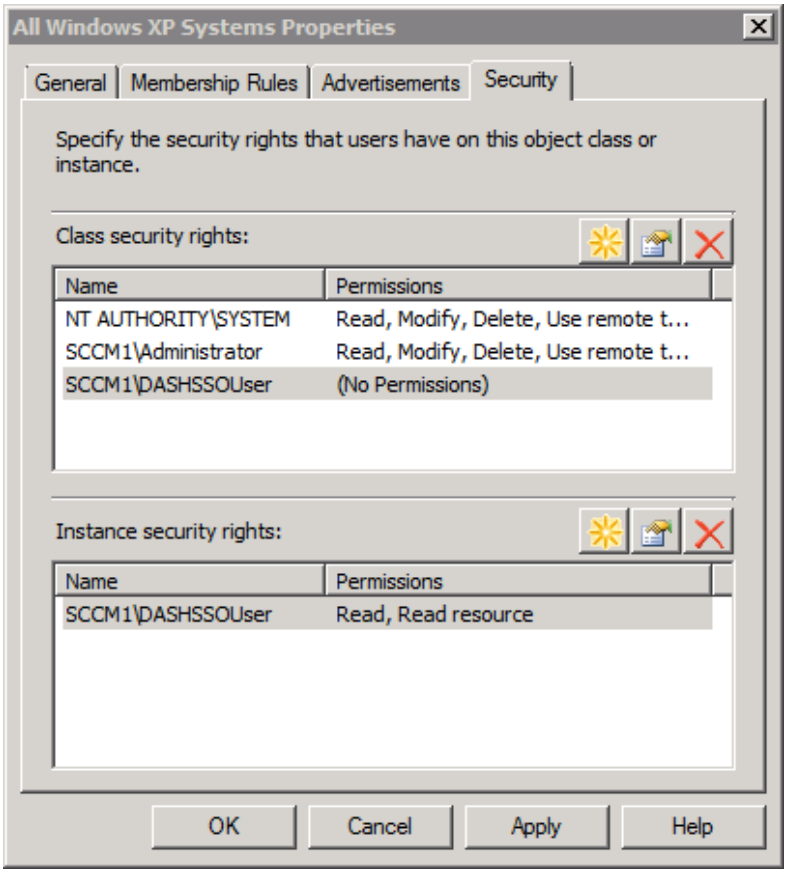


Figure : The domain user DASHSSOUser has Read and Read resource security rights on the All Windows XP Systems collection instance and does not have any permissions on the rest of the collection class.

Security rights defined for DASH settings

The security rights model applies for modifying DASH settings in the "DASH Management Properties" window in the SCCM Administrator Console. This will allow the administrator to control which users can modify the DASH settings, which users can view the settings, and which users should not have access to the settings window.

A few of the DASH settings that can be changed in the "DASH Management Properties" window are:

- Manage inventory schedules
- Modify digest and active directory authentication
- Modify HTTP/HTTPS settings
- Change DASH port numbers

Site class/instance

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

Read

The Read security right allows the user to open the "DASH Management Properties" window and view the settings. The user cannot save the settings.

Modify

The user can open the "DASH Management Properties" windows and modify and save the settings.

Note: Users without either Read or Modify rights cannot open the DASH settings window.

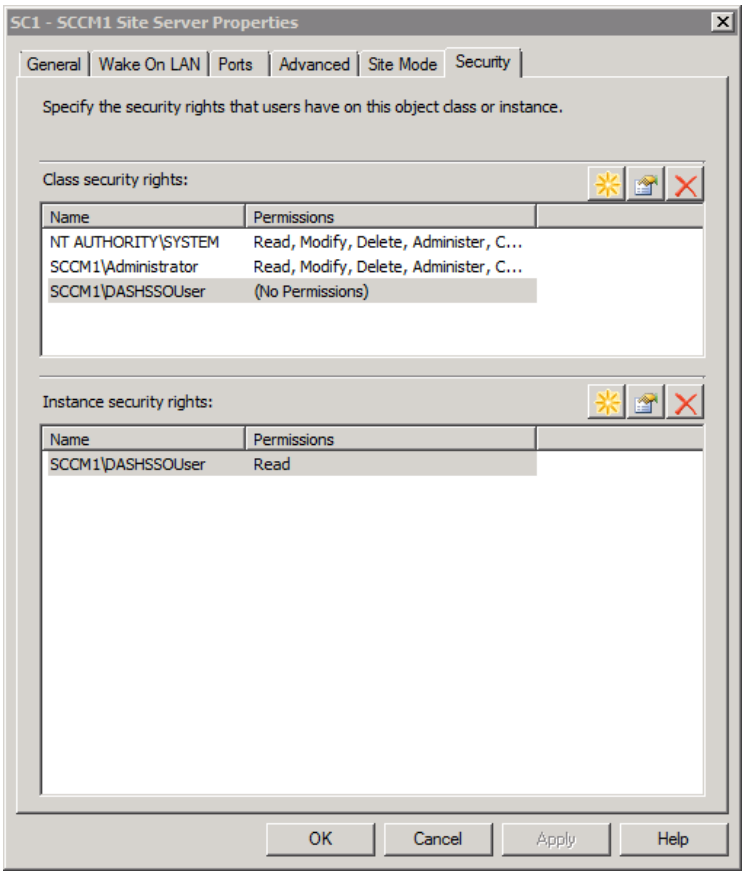


Figure : The domain user DASHSSOUser has Read security right on SC1 instance of Site class, while Administrator has both Read and Modify security rights.

Configuration of DASH Plugin

In DASH Plugin v1.7, the administrator has the option to either enable or disable the user permission checking feature. This is a global setting and affects all users.

Note: To change the setting, the user must have at least Modify security right on Site class instance.

Steps:

1. In the SCCM console, navigate to System Center Configuration Manager / Site Database / Tools / DASH Management. Right-click on DASH Management and click Properties.
2. Go to Authentication tab.
3. Check "Enable User Permission Checking" to enable the feature.
4. This feature can be turned off by unchecking this option.

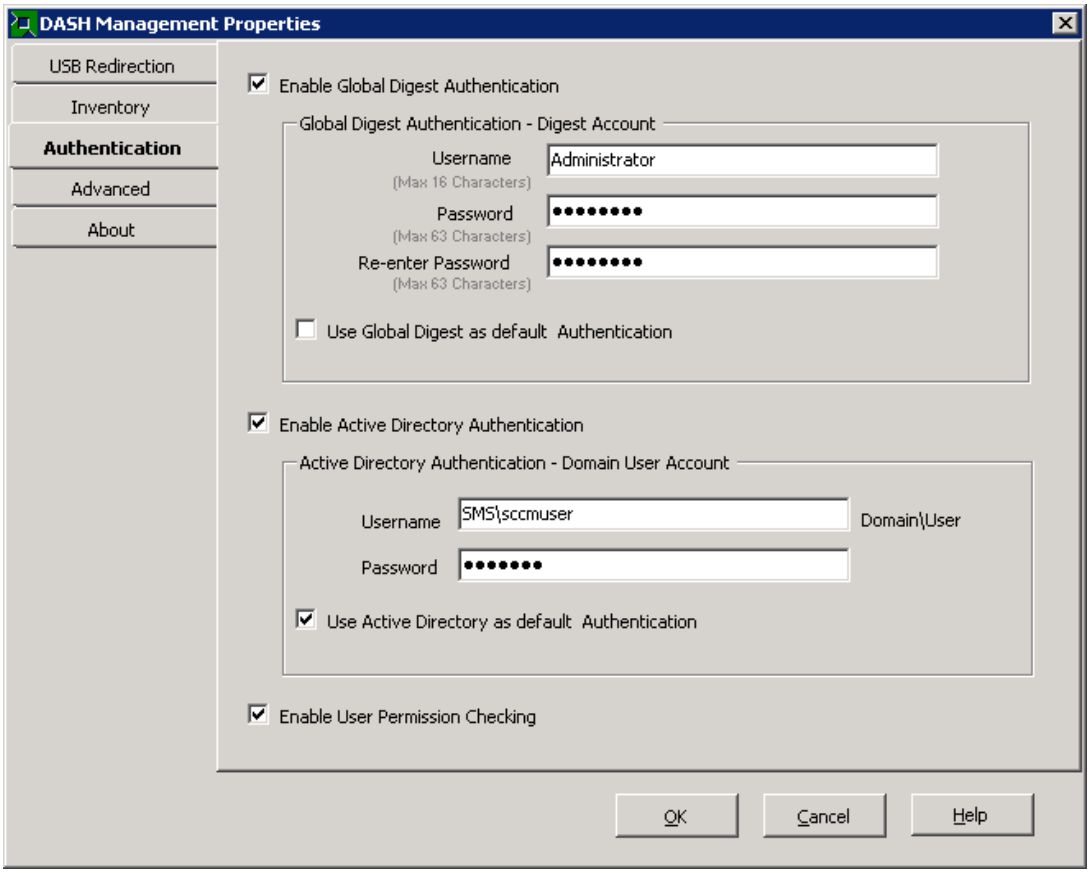


Figure : 'Enable User Permission Checking' is checked.

Case study

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

Business scenario

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

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

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

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

Solution Description

I. Create groups in Active Directory

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

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

In the SCCM console, navigate to System Center Configuration Manager / Site Database / Security Rights. Right-click on Security Rights and select Manage ConfigMgr Users. Using this utility, add the four active directory domains groups as four SCCM Users. Do not assign any security right for any of these four SCCM users.

II. Create Collections in SCCM

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

- Call Center Systems
- Office Systems
- Executive Systems

Define a collection membership rule so Call Center Systems collections has only call center desktops, and so forth for the other two collections (check this link for help on this step: http://technet.microsoft.com/en-us/library/bb680821).

III. Assign security rights for the collections

Right-click on a Call Center Systems collection node, click Properties, and in the Properties window, click the Security tab. In the Instance security, provide Read Resource and Use Remote Tools security rights for the Call Center Admins SCCM User. Ensure none of the other SCCM users (leaving out Administrator and SYSTEM users) have Read Resource and Use Remote Tools on Call Center Systems collection.

Similarly, provide Read Resource and Use Remote Tools security rights to:

- Office System Admins on the collections Office Systems and Call Center Systems.
- Executive Admins on the collections Executive Systems, Office Systems, and Call Center Systems.

Apart from the assigned users, ensure none of the other SCCM users have Read Resource and Use Remote Tools on these collections.

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

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

IV. Assign security rights for the DASH settings

In the SCCM Administrator Console, navigate to System Center Configuration Manager / Site Database / Site Management / Site Server. Right-click on Site Server and click Properties. In the Properties window, click the Security tab. In the Instance security, provide

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

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

V. Summary of assigned security rights

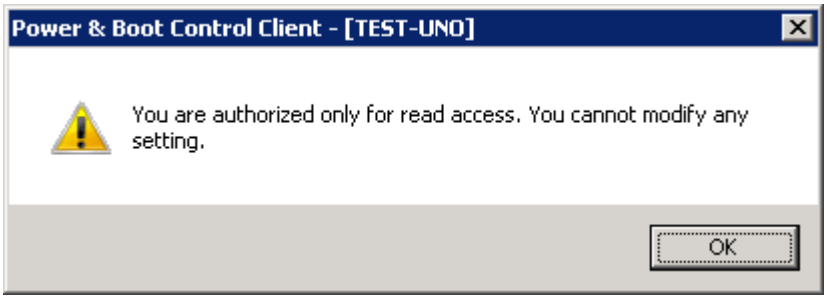
IT Admin Group	Collection Access	Security Rights
Executive System Admins	Executive Systems, Office Systems, and Call Center Systems	Read Resource and Use Remote Tools
Office System Admins	Office Systems and Call Center Systems	Read Resource and Use Remote Tools
Call Center Admins	Call Center Systems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

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

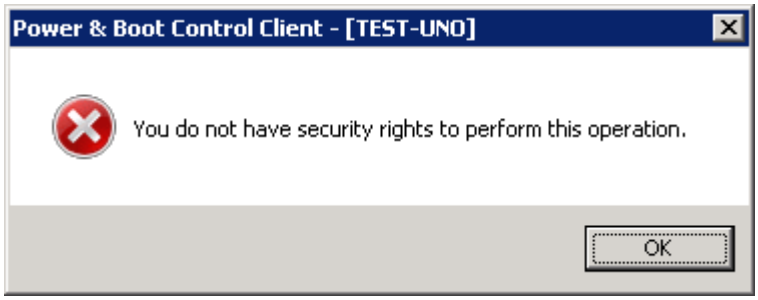
Frequently asked questions

User messages

Q: What message is shown to the user when that person has read-only DASH access?
A: A message box such as this one is shown to the user. Contact your IT Administrator if you see this message when you should have Modify rights.



Q: What message is shown to the user when that person is not authorized for any DASH access?
A: A message box such as this one is shown to the user. Contact your IT Administrator if you see this message.



Discovery

Q: What is the security right required for DASH Discovery?
A: Create, Modify, and Read Resource. Create and Modify are required to create a DASH-capable sub-collection. Read Resource security right is required to query a DASH-capable system.

Miscellaneous

Q: Where can I get additional information on the DASH Plugin?
A: Visit the DASH discussion forum: www.amd.com/DASH

Q: How can I check if a user can change DASH settings?
A: In the SCCM Administrator Console, navigate to System Center Configuration Manager / Site Database / Site Management / Site Server. Right-click on Site Server and click Properties. In the Properties window, click the Security tab. Check if the user has Modify security right permission either for class or for class instance.

Q: How can I view security rights for a collection?
A: Right-click on a collection node, click Properties, and in the Properties window, click the Security tab. Check the security right permissions in for class and class instance.

Q: I cannot see the Properties option after right-clicking on a collection.
A: Most likely, the Administer security right is not assigned to you as a user. Contact your administrator.

Q: How can I open the "DASH Management Properties" window?
A: In the SCCM Administrator Console, navigate to System Center Configuration Manager / Site Database / Tools / DASH Management. Right-click on DASH Management and click Properties.

Glossary

The following terms are used to describe the components of DASH Plugin.

Out-of-band management

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

DASH

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

DASH defines a set of interoperability standards for managing, monitoring, and controlling PCs, regardless of system power state (on, off, stand-by) or OS capability.

DASH-capable system

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

Management controller

Management controller enables OOB platform management capabilities with technologies such as DASH.

DASH management controller

The DASH management controller implements the DASH protocol stack. It interfaces with other platform components (BIOS, SB, IMDs, etc.) to get needed information or control the platform.

SCCM Administrator Console or SCCM console

This is the GUI interface of SCCM Site Server used for a managing SCCM servers. SCCM console is also called the configuration manager console.

Windows Management Instrumentation

WMI is the infrastructure for management data and operations on Windows-based OSes. It provides an interface through which instrumented components provide information and notification. WMI is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF).

Conclusion

The role-based authorization model in DASH Plugin provides administrators with greater control to authorize a user or a set of users to perform DASH tasks, and to authorize which users can make changes to DASH settings.

More information

- *Classes and Instances for Object Security in Configuration Manager*
  http://technet.microsoft.com/en-us/library/bb632791.aspx

- *How to Assign Rights for Objects to Users and Groups*
  http://technet.microsoft.com/en-us/library/bb680648.aspx

- *Information on collection membership rules in SCCM Console*
  http://technet.microsoft.com/en-us/library/bb680821

- *DASH Forum*
  http://www.amd.com/DASH

- *SCCM Forum*
  http://www.windows-noob.com/forums/index.php?/forum/54-configuration-manager-2007

- *MYITForum*
  http://www.myitforum.com/

DASH Plugin user manual and help file

The help file that gets installed with DASH Plugin provides detailed information on support for role-based authorization in DASH Plugin. The default location for the help file is 'C:\Program Files (x86)\SCCM DASH Plug-in\SCCMDASHPlugin.chm.' This information can also be found in the user manual document in the installer package.

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. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.