

AMD Cloud Manageability User Guide

Publication #	**CSG-3** Revision: **1.0**
Issue Date:	**March 2023**

Advanced Micro Devices

© 2023 Advanced Micro Devices, Inc. All rights reserved.

The information contained herein is for informational purposes only, and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD's products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale. Any unauthorized copying, alteration, distribution, transmission, performance, display or other use of this material is prohibited.

Trademarks

AMD, the AMD Arrow logo, AMD AllDay, AMD Virtualization, AMD-V, PowerPlay, Vari-Bright, and combinations thereof are trademarks of Advanced Micro Devices, Inc. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

Dolby is a trademark of Dolby Laboratories.

HDMI is a trademark of HDMI Licensing, LLC.

HyperTransport is a licensed trademark of the HyperTransport Technology Consortium.

Microsoft, Windows, Windows Vista, and DirectX are registered trademarks of Microsoft Corporation in the US and/or other countries.

MMX is a trademark of Intel Corporation.

OpenCL is a trademark of Apple Inc. used by permission by Khronos.

PCIe is a registered trademark of PCI-Special Interest Group (PCI-SIG).

USB Type-C® and USB-C® are registered trademarks of USB Implementers Forum.

Reverse engineering or disassembly is prohibited.

USE OF THIS PRODUCT IN ANY MANNER THAT COMPLIES WITH THE MPEG ACTUAL OR DE FACTO VIDEO AND/OR AUDIO STANDARDS IS EXPRESSLY PROHIBITED WITHOUT ALL NECESSARY LICENSES UNDER APPLICABLE PATENTS. SUCH LICENSES MAY BE ACQUIRED FROM VARIOUS THIRD PARTIES INCLUDING, BUT NOT LIMITED TO, IN THE MPEG PATENT PORTFOLIO, WHICH LICENSE IS AVAILABLE FROM MPEG LA, L.L.C., 6312 S. FIDDLERS GREEN CIRCLE, SUITE 400E, GREENWOOD VILLAGE, COLORADO 80111.

Contents

Contents **3**
List of Figures **4**
Revision History **5**
Chapter 1 Introduction **6**
Chapter 2 Requirements **7**
2.1 ACMS 7
2.2 AMD Integrated Management Technology (AIM-T) 7
2.3 IT Console 7
2.4 AMD Provisioning Console (APC) 7
Chapter 3 Installation and Setup **8**
3.1 APC8
3.2 ACMS 9
3.2.1 Installation 9
3.2.2 Uninstallation 10
3.2.3 Configuration 10
3.2.4 Port and Firewall 11
3.3 AIM-T 11
3.4 DASH CLI 12
3.4.1 Configuration 12
Chapter 4 Testing the Setup **13**
Chapter 5 Troubleshooting **15**

List of Figures

Figure 1. ACMS Use Case 6
Figure 1. APC Page 8

Revision History

Date	Revision	Description
March 2023	1.0	First version.

Chapter 1 Introduction

AMD Manageability solution enables the IT administrators to effectively manage enterprise systems when the system is powered on/off. It is built on DMTF's DASH specification, which is an open standard (*https://www.dmtf.org/standards/dash*). AMD Manageability covers organizations of all sizes (small, medium, and large enterprises). For more details, refer to the AMD portal (*www.amd.com/DASH*).

AMD Cloud Manageability Service (ACMS) is a software product within AMD Manageability that enables the IT administrators to manage enterprise systems even when those systems are outside the enterprise network.

A block diagram of the ACMS use case is as follows:

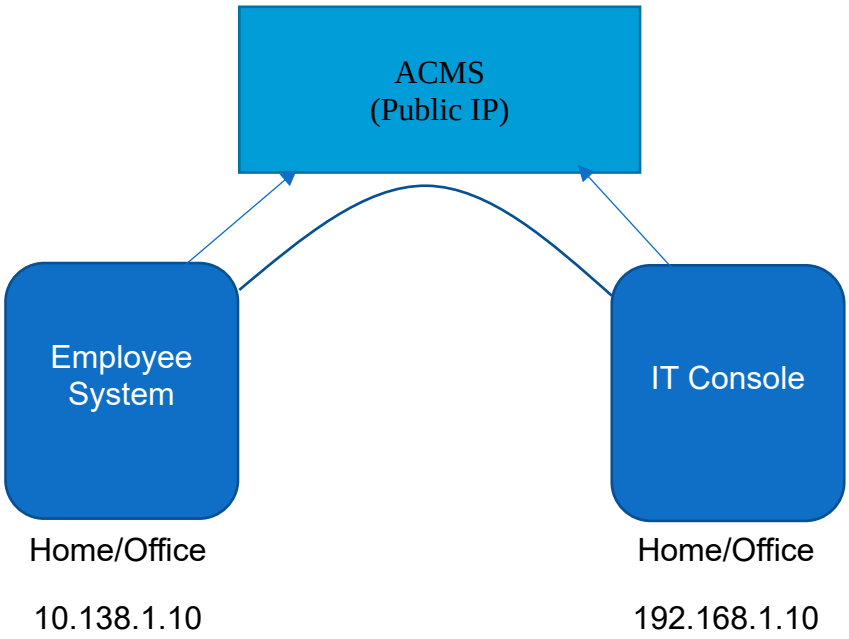


Figure 1. ACMS Use Case

ACMS is installed on a system with public IP address. Both the employee system and IT console must be able to access ACMS. The employee systems, when powered on, register with ACMS. IT console can query ACMS for registered systems, get connected to it and perform manageability operations.

The entire end-to-end traffic is encrypted using a TLS connection.

Chapter 2 Requirements

2.1 ACMS

ACMS is deployed on:

- Linux® system capable of running Ubuntu® 20.04 LTS.
- Public IP

On public clouds, it can be achieved by spawning Ubuntu 20.04 Virtual Machine (VM) in public subnet. The recommended configuration for all the systems is 4-core x64 with at least 4 GB of RAM.

You can get the ACMS software from the download section of the AMD portal (*https://www.amd.com/DASH*).

2.2 AMD Integrated Management Technology (AIM-T)

AIM-T 2.0 and later supports AMD Cloud Manageability. Ensure that AMS 2.0 or later is installed on Windows®. AIM-T system must be provisioned with cloud option enabled using AMD Provisioning Console.

2.3 IT Console

You can use DASH CLI to issue the manageability commands over cloud. DASH CLI 4.5 and later support AMD Cloud Manageability.

2.4 AMD Provisioning Console (APC)

APC is used to generate TLS certificates and to configure ACMS server hostname in managed systems. APC 2.0 and later have the cloud option.

Chapter 3 Installation and Setup

3.1 APC

APC is used to generates certificate, key, and certificate authority for ACMS, DASH CLI and AIM-T.

The following figure shows various options of the APC page:

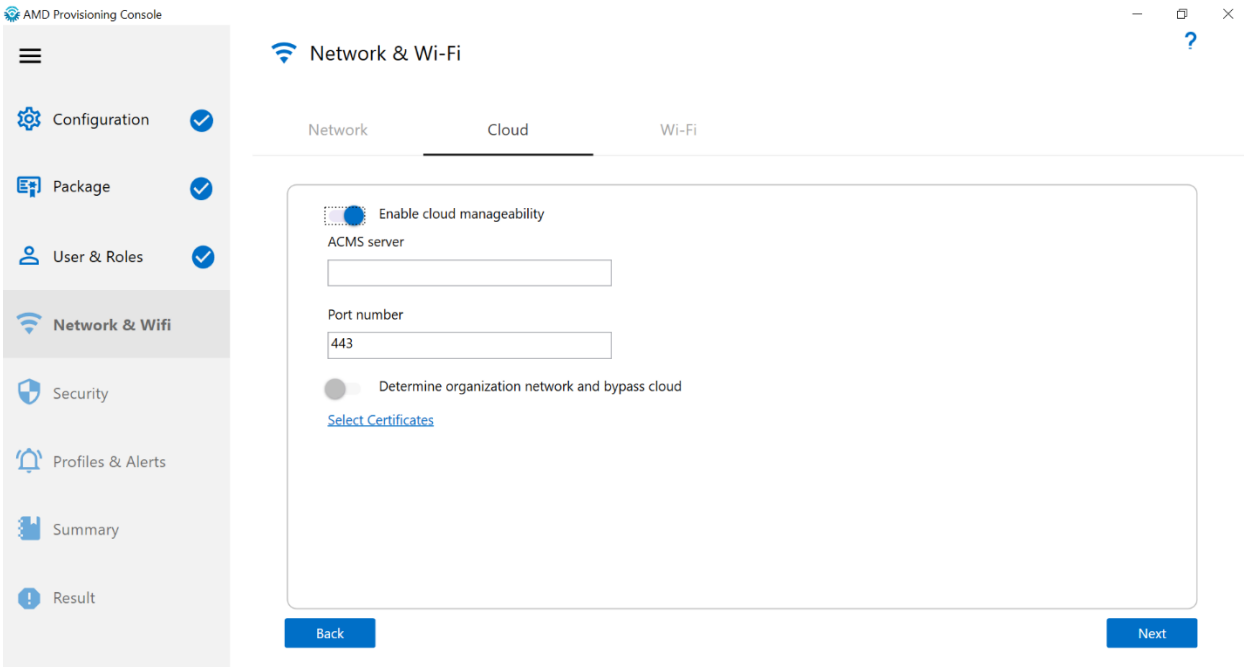


Figure 2. APC Page

The generated files are at the following path:

$(SecurePath)\AMD Provisioning Console\Packages\$(PackageName)\Cloud

$(SecurePath) is the path provided to the APC tool, $(PackageName) is the package name provided by the user. The following three folders are present at this location:

- ACMS
  - *acmscert.pem*
  - *acmskey.pem*
  - *trustedclients.pem*

- Console
  - *acmscert.pem*
  - *consolecert.pem*
- AIM-T
  - *nodecert.pem*
  - *nodekey.pem*
  - *acmscert.pem*

3.2 ACMS

3.2.1 Installation

Complete the following steps to install ACMS:

1. On Ubuntu 20.04, install the package as follows:

```
$ sudo apt install ./acms_1.0.0.1099_amd64.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'acms' instead of './acms_1.0.0.1099_amd64.deb'
The following NEW packages will be installed:
  acms
0 upgraded, 1 newly installed, 0 to remove and 62 not upgraded.
After this operation, 1,474 kB of additional disk space will be used.
Get:1 /home/amd/certs-work/acms_1.0.0.1099_amd64.deb acms amd64 1.0.0.1099 [417 kB]
Selecting previously unselected package acms.
(Reading database ... 254233 files and directories currently installed.)
Preparing to unpack .../acms_1.0.0.1099_amd64.deb ...
Unpacking acms (1.0.0.1099) ...
Setting up acms (1.0.0.1099) ...
```

2. Start ACMS:

```
$ sudo systemctl start acms
```

3. Verify that it is running on port 443:

```
$ systemctl status amcs
● acms.service - AMD Cloud Manageability Service
     Loaded: loaded (/lib/systemd/system/acms.service; enabled; vendor preset:
enabled)
     Active: active (running) since Tue 2023-01-31 13:51:22 IST; 2s ago
   Main PID: 485996 (acms)
      Tasks: 1 (limit: 9375)
     Memory: 756.0K
     CGroup: /system.slice/acms.service
             └─485996 /bin/acms --bind 0.0.0.0:443 --poll 60 --cert
/etc/acms/acmscert.pem --key /etc/acms/acmskey.pem --ca /etc/acms/trustedclients.pem

Jan 31 13:51:22 acms-host systemd[1]: Started AMD Cloud Manageability Service.
```

4. (Optional) Enable it to start automatically at boot time:

```
$ sudo systemctl enable acms
Created symlink /etc/systemd/system/multi-user.target.wants/acms.service →
/lib/systemd/system/acms.service.
```

5. Use `journalctl` to view the logs from ACMS and `-f` option for the live logs:

```
$ journalctl -fu acms
```

6. Refer to the main page of `journalctl` for finer controls:

```
$ journalctl -u acms
Jan 31 13:39:53 acms-host acms[485017]: [10.139.8.79:53979] REVERSE_CONNECT
id=GuruDev host=gurudev port=664 uuid=029e3025-97d6-4d4e-b03d-f3e0ea038d70
Jan 31 13:39:53 acms-host acms[485017]: [10.139.8.79:54036] REVERSE_CONNECT_RETURN
errcode=0 uuid=029e3025-97d6-4d4e-b03d-f3e0ea038d70
Jan 31 13:39:53 acms-host acms[485017]: [10.252.94.168:56990] CONNECT_RETURN
id=gurudev host=gurudev port=664 uuid=
Jan 31 13:39:53 acms-host acms[485017]: splicing 10.252.94.168:56990 <=>
10.139.8.79:54036
Jan 31 13:40:00 acms-host acms[485017]: [10.252.94.168:56990] async_read_some:
asio.system:104
Jan 31 13:40:00 acms-host acms[485017]: complete 10.252.94.168:56990 <=>
10.139.8.79:54036 initiator_rx=26458 target_rx=54449
```

3.2.2 Uninstallation

Uninstall ACMS as follows:

```
$ sudo apt remove acms
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  acms
0 upgraded, 0 newly installed, 1 to remove and 62 not upgraded.
After this operation, 1,474 kB disk space will be freed.
Do you want to continue? [Y/n]
(Reading database ... 254239 files and directories currently installed.)
Removing acms (1.0.0.1099) ...
```

3.2.3 Configuration

ACMS implements 2-way-TLS for securing itself against unauthorized access. Hence, only the clients with trusted certificate will be able to connect. The certificates, private key, and certificate authority files in PEM format respectively are expected at the following locations:

```
/etc/acms/amcscert.pem
/etc/acms/acmskey.pem
/etc/acms/trustedclients.pem
```

Copy them from the *Cloud\ACMS* folder in the APC package.

3.2.4 Port and Firewall

ACMS listens on port 443 by default. It can be overridden by command-line arguments. Though the default port is 443, it does not conform to the HTTPS protocol. It was selected as it is reasonable to expect 443 is allowed through the firewalls.

To change the listening port, edit the `-bind` option in following file:

```
$ cat /lib/systemd/system/acms.service
[Unit]
Description=AMD Cloud Manageability Service
After=network.target

[Service]
ExecStart=/bin/acms \
        --bind 0.0.0.0:443 --poll 60 \
        --cert /etc/acms/acmscert.pem \
        --key /etc/acms/acmskey.pem \
        --ca /etc/acms/trustedclients.pem
Restart=always
RestartSec=30

[Install]
WantedBy=multi-user.target
```

Then, restart the service.

On plain Ubuntu 20.04 LTS installation, if the default iptables policy is not accepted, use `ufw` to open port 443:

```
$ sudo ufw allow 443/tcp
```

Notes:

- *Amazon Web Services (AWS) use security groups to control access to ports on EC2 instances. For more information, refer to AWS documentation (*https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html*)*
- *Microsoft® Azure too has a similar concept called network security group. For more information, refer to Microsoft Azure documentation (*https://docs.microsoft.com/en-us/azure/virtual-machines/windows/nsg-quickstart-portal*)*

3.3 AIM-T

For more information, refer to *AMD Provisioning Console User Guide*. Ensure that AIM-T provisioning package is generated with cloud option enabled.

3.4 DASH CLI

3.4.1 Configuration

DASH CLI uses the following certificates for authentication with ACMS:

```
%ProgramFiles(x86)%\DASH CLI 4.0\certs\consolecert.pem
%ProgramFiles(x86)%\DASH CLI 4.0\certs\acmscert.pem
```

Copy them from the *Cloud\Console* folder in the APC package.

Chapter 4 Testing the Setup

Test the local setup without ACMS. ACMS must be first to start followed by AMI-T. On *dash-cli-win10* execute *dashcli.exe* as follows:

```
dashcli.exe -C -h aimt-host -u admin -P adminpass enumerate commputersystem
```

The output might resemble as follows:

```
Error: Connection Failed : Could not resolve host
```

The equivalent command using `-r` option is as follows:

```
dashcli.exe -r acms-host -C -h aimt-host -u admin -P adminpass enumerate computersystem
```

Observe the output, it will be identical to output displayed when connected directly:

```
Computer System Instance 0
Name                                : MS-WIN10
Element Name                        : Computer System:0
Primary Owner                       : AMD
Primary Owner Contact               : N/A
Enabled State                       : Enabled
Requested State                     : Not Applicable
Current Power State                 : On
Requested Power State               : Unknown
Power On Time                       : 2021/12/15 17:56:28
Dedicated To                        : Desktop
Supported Power Change Capabilities : Power State Settable,
                                      Power Cycling Supported,
                                      HW Reset Supported,
                                      Graceful Shutdown Supported
Supported Power States              : Sleep -Deep,
                                      Power Cycle (Off - Soft),
                                      Hibernate (Off - Soft),
                                      Off - Soft,
                                      Master Bus Reset,
                                      Off - Soft Graceful,
                                      Master Bus Reset Graceful,
                                      Power Cycle (Off - Soft Graceful)
Request Supported Power States      : Sleep -Deep,
                                      Power Cycle (Off - Soft),
                                      Hibernate (Off - Soft),
                                      Off - Soft,
                                      Master Bus Reset,
                                      Off - Soft Graceful,
                                      Master Bus Reset Graceful,
                                      Power Cycle (Off - Soft Graceful)
Available Requested Power States    : On,
                                      Off - Hard,
                                      Hibernate (Off - Soft),
                                      Off - Soft,
                                      Master Bus Reset
```

Observe the command above; the certificates and key PEM files paths were not specified. By default, DASH CLI reads the certificates and key from the *certs* folder in the installation location. Specify the corresponding options in the command line to override it:

`-rc` for certificate, `-rk` for key, and `-rca` for certificate authority. For example:

```
dashcli.exe -r acms-host ^
-rc %ProgramFiles(x86)%\certs\cert.pem ^
-rk %ProgramFiles(x86)%\certs\cert.pem ^
-rca %ProgramFiles(x86)%\certs\ca.pem ^
-C  -h aimt-host ^
-u admin -P adminpass enumerate computersystem
```

^ character is used as a line break in batch files and Windows command processor.

Note: *When using -r options, -h must be followed by the hostname and not the IP address.*

Chapter 5 Troubleshooting

- To view the ACMS logs to `systemd-journal`, use the command `journactl`:

```
# journactl -u acms
```

- To view the live logs, use the following `journactl` option:

```
# journactl -fu acms
```

- The most common cause of a failure might be misconfiguration of certificates. They are logged with path and if possible, with error explaining the failure. Another is an attempt to connect to an unregistered AIM-T host.
- Following are the sample logs when DASH CLI requests a connection to aimt-host:

```
Jan 31 13:39:41 acms-host acms[485017]: [10.252.94.168:56986] CONNECT id=gurudev
host=aimt-host port=664

Jan 31 13:39:41 acms-host acms[485017]: [10.139.8.79:53979] REVERSE_CONNECT
id=GuruDev host=aimt-host port=664 uuid=8a49c43e-b952-4e9c-a067-aeee7e0472d7

Jan 31 13:39:41 acms-host acms[485017]: [10.139.8.79:54033] REVERSE_CONNECT_RETURN
errcode=0 uuid=8a49c43e-b952-4e9c-a067-aeee7e0472d7

Jan 31 13:39:41 acms-host acms[485017]: [10.252.94.168:56986] CONNECT_RETURN
id=aimt-host host=aimt-host port=664 uuid=8a49c43e-b952-4e9c-a067-aeee7e0472d7
```

1. CONNECT is received from DASH CLI.
2. REVERSE_CONNECT is sent to *aimt-host* with the generated UUID.
3. *aimt-host* responds with REVERSE_CONNECT_RETURN.
4. On receiving REVERSE_CONNECT_RETURN; ACMS sends CONNECT_RETURN to DASH CLI with an error code. The UUID is unique for every negotiation.

- The following sample logs indicate that ACMS has created a tunnel between the two remote addresses:

```
Jan 31 13:39:41 acms-host acms[485017]: splicing 10.252.94.168:56986 <=>
10.139.8.79:54033
```

- When a tunnel is closed, the bytes transferred are logged as basic stats:

```
Jan 31 13:40:00 acms-host acms[485017]: complete 10.252.94.168:56990 <=>
10.139.8.79:54036 initiator_rx=26458 target_rx=54449
```