Intel® vPro™ Technology Module for Microsoft* Windows* PowerShell*

Revision History

Revision	Revision History	Date
1.0	Initial release	August, 2010
2.0	Document additions and changes to support version 2.0 of the PowerShell Module for Intel vPro	October, 2010
3.0	Document additions and changes to support version 3.0 of the Windows PowerShell Module for Intel vPro Technology	March, 2011
3.1	Document additions and changes to support version 3.1 of the Windows PowerShell Module for Intel vPro Technology	June, 2011
3.2	Document additions and changes to support version 3.2 of the Windows PowerShell Module for Intel vPro Technology	Dec, 2011
3.2.2	Document additions and changes to support version 3.2.2 of the Windows PowerShell Module for Intel vPro Technology	Mar, 2012

Contents

Figures

Tables

1 Preface

Microsoft* Windows* PowerShell* is becoming more prevalent as an automation scripting language within many Information Technology (IT) environments. Whether writing scripts to automate tasks or taking advantage of native Windows PowerShell extensibility within existing management tools, the ability to Out of Band manage Intel® Active Management Technology (Intel® AMT) enabled clients with Windows PowerShell is a very attractive solution.

1.1 Document Scope

This document covers the requirements, installation and usage of the Windows PowerShell Module for Intel® vPro™ Technology.

1.2 Intended Audience

Windows PowerShell command line shell and scripting language helps IT professionals achieve greater control and productivity. Using a new administrator-focused scripting language and consistent syntax and utilities Windows PowerShell allows IT professionals to more easily control system administration and accelerate automation. This document is intended for IT professionals who desire to learn more about using the Intel® vPro™ Module for Windows PowerShell.

1.3 Related Documentation and Software

The download package, module installer and supporting files referenced in this document can be found at the following link:

http://www.intel.com/go/powershell

Microsoft Windows Management Framework (which includes Windows PowerShell):
http://support.microsoft.com/kb/968929

Microsoft Windows Remote Manager (WinRM):
http://www.microsoft.com/downloads/details.aspx?familyid=845289ca-16cc-4c73-8934-dd46b5ed1d33&displaylang=en

2   Introduction

The Windows PowerShell command line shell and scripting language helps IT professionals achieve greater control and productivity. Using a new administrator focused scripting language and consistent syntax and utilities, Windows PowerShell allows IT professionals to more easily control system administration and accelerate automation. Windows PowerShell is easy to adopt, learn, and use. It works with existing IT infrastructure and cmdlet investments. It runs on Windows XP, Windows Vista*, Windows Server* 2003 and is included as part of Windows 7, Windows Server 2008, and Windows Server 2008 R2. For more information on Windows PowerShell), please visit:

http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx

By leveraging the Out of Band Management cmdlets within the Windows PowerShell Module for Intel vPro Technology IT professionals can extend their PowerShell reach to include direct manageability of Intel AMT enabled clients independent of power or operating system health.

2.1   Requirements

IT / Console PC	Any PC with Microsoft Windows XP or later with: • Windows PowerShell 2.0 installed • Windows Remote Management (WinRM) **Note:** WinRM is not natively included with Windows XP and Windows Server 2003. Please ensure WinRM is installed prior to use: http://www.microsoft.com/downloads/details.aspx?familyid=845289ca-16cc-4c73-8934-dd46b5ed1d33&displaylang=en **Note:** Windows PowerShell is not included by default in Windows XP, Windows Vista, and Windows 2003 Server. Please ensure Windows PowerShell 2.0 is installed prior to use: http://technet.microsoft.com/en-us/scriptcenter/dd772288.aspx or http://support.microsoft.com/kb/968929
Managed Client with Intel vPro technology	• Intel® Active Management Technology (Intel® AMT) 3.0 or higher. • Intel® Management Engine is provisioned. • See subsections 2.1.1, 2.1.2, and 2.1.3 for further client requirements.

2.1.1 Setup and Configuration of the Intel® vPro™ Technology Based Client Prior to Module Use

Prior to using the Intel® vPro™ Technology module for Windows PowerShell the client's Intel AMT firmware must be set up and configured. Use existing Configuration Management software or reference the material on the Intel® vPro™ Expert Center below on how to set up and configure an Intel AMT enabled client.

http://communities.intel.com/community/openportit/vproexpert

The Intel vPro PowerShell module can be used to set up and configure an Intel AMT enabled client.

See section 5.10.2 for information on the **Enter-AMTRemoteConfiguration** cmdlet.

2.1.2 Cmdlet and Function Authentication

Credentials must be specified in order to invoke commands against the Intel vPro technology enabled client. Typical behavior of the Windows PowerShell Module for Intel vPro technology cmdlets and functions are as follows:

- When no credentials are provided, the cmdlets and functions will use the locally logged on Kerberos credential.
- When only the username (Kerberos or Digest) parameter is included a prompt will be displayed to provide the associated password.
- If the credentials are stored as a PowerShell variable, they may be passed into the cmdlets and functions with the credential parameter.

NOTE

For Active Directory authentication to work correctly, a hostname or the Fully Qualified Domain Name (FQDN) must be specified.

2.1.3 Cmdlet and Function Communication Encryption

If the Intel vPro technology enabled client is configured to use Transport Layer Security (TLS) by having a web server certificate issued to the Intel Management Engine the –TLS switch must be passed to the cmdlet.

When managing an Intel vPro technology enabled client over TLS (Port 16993), it is important that the computer name match the primary subject name of the issued TLS certificate. Typically, this is the Fully Qualified Domain Name (FQDN).

2.2 Configuration and Usage Process Overview

The Windows Powershell configuration and usage process consists of three primary steps:

1. Install Windows PowerShell if necessary.
2. Install the Windows PowerShell Module for Intel vPro Technology.
3. Use the Intel vPro PowerShell cmdlets.

3 Windows* PowerShell Setup and Configuration

This chapter and its subsections step through setting up and configuring the console PC to use Windows PowerShell, installing the Windows PowerShell Module for Intel vPro technology, and importing the module once it has been installed.

3.1 Installing Windows* PowerShell

Windows PowerShell is natively included with Windows Server 2008, Windows Server 2008 R2, and Windows 7.

Windows Management Framework makes some updated management functionality in Windows 7 and in Windows Server 2008 R2 available to be installed on Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. Windows Management Framework contains Windows Remote Management (WinRM) 2.0, Windows PowerShell 2.0, and Background Intelligent Transfer Service (BITS) 4.0.

To obtain a copy of the Windows Management Framework and install Windows PowerShell, click the link below.

http://support.microsoft.com/kb/968929

3.1.1 Configuring Windows PowerShell

By default Windows PowerShell has its ExecutionPolicy set to Restricted. This setting must be changed to execute the Out of Band Management PowerShell cmdlets and functions provided within the PowerShell Module for Intel vPro technology.

All the cmdlets and functions within the PowerShell Module for Intel vPro technology have been signed. At a minimum the PowerShell Execution Policy needs to be changed to RemoteSigned to execute the cmdlets and functions. If there are more restrictive security requirements set the ExecutionPolicy to AllSigned.

To apply the ExecutionPolicy to the LocalMachine run the following command within the Windows PowerShell Console (be sure to start the console with "Run as administrator"):

> **Set-ExecutionPolicy RemoteSigned**
> Or
> **Set-ExecutionPolicy –Scope LocalMachine RemoteSigned**

To apply the ExecutionPolicy to the current user only run the following command within the Windows PowerShell Console:

> **Set-ExecutionPolicy –Scope CurrentUser RemoteSigned**

To apply the ExecutionPolicy to the process only run the following command within the Windows PowerShell Console:

Set-ExecutionPolicy –Scope Process RemoteSigned

NOTE

If using an ExecutionPolicy based process, it will be required to run Set-ExecutionPolicy each time a Windows PowerShell Console is launched.

For more information on setting the Windows PowerShell ExecutionPolicy, please visit the following site:

http://msdn.microsoft.com/en-us/library/bb648601(VS.85).aspx

3.2 Installing the Windows PowerShell Module for Intel vPro Technology

This section describes how to install the Windows PowerShell Module for Intel vPro technology.

3.2.1 Downloading the Module

Download the latest copy of the Windows PowerShell Module for Intel vPro technology from the following location:

http://www.intel.com/go/powershell

3.2.2 Installing the Module

Install the Windows PowerShell Module for Intel vPro technology using the following procedure:

1. Uninstall previous versions of the Windows PowerShell Module for Intel vPro technology.
2. Decompress the zip file to a directory.
3. Navigate to the directory where the file was decompressed.
4. From within the **x64** or **x32 directory** run **setup.exe**.

NOTE

The installer must be run from an account with administrative rights.

5. When the Installation Wizard appears click **Next.**
6. On the License Agreement confirmation screen, click **I Agree** and then click **Next** to continue with the installation.
7. There will be an opportunity to change the module installation folder. It is recommended that it be left to the default c:\Program Files\Intel Corporation\PowerShell\Modules. Click **Next**.
8. Click **Next** to confirm the installation.
9. If User Account Control is turned on a prompt will appear to continue.
10. When the installation complete screen appears, click **Close**.

The module installs into the following default directory:

C:\Program Files\Intel Corporation\PowerShell\Modules

3.2.3   Uninstalling the Module

To uninstall the Windows PowerShell Module for Intel vPro technology, use the Windows Add or Remote Programs feature or run the Module Installer of the version to uninstall.

3.2.3.1   Add or Remove Programs

1. In Windows under the Control Panel navigate to **Uninstall or change programs**.
2. Select **PowerShell Module for Intel(R) vPro(tm)** and select **Uninstall**.
3. If User Account Control is turned on a prompt will appear to continue.

NOTE

*When uninstalling Version 1 of the Windows PowerShell Module for Intel vPro technology, it will be listed as **IntelvPro Module for PowerShell**.*

3.2.3.2   Running the Module Installer

1. Navigate to the directory where the file was decompressed.
2. From within the **x64** or **x32 directory**, run **setup.exe**.
3. Select **Remove PowerShell Module for Intel(R) vPro(tm)** and click **Finish**.

NOTE

*When uninstalling Version 1 of the Windows PowerShell Module for Intel vPro technology, it will be listed as **IntelvPro Module for PowerShell**.*

3.3 Configuring a Profile for the Windows PowerShell Module for Intel vPro Technology

Microsoft states "A well-designed profile can make it even easier to use Windows PowerShell and to administer your system". This holds true for administering Intel vPro technology enabled devices. A well-designed PowerShell profile can make that task even easier.

Please view the link below from Microsoft for more information about PowerShell profiles:

http://msdn.microsoft.com/en-us/library/bb613488(v=vs.85).aspx

3.3.1 Setting Up a Profile for Intel vPro Technology

Below is an example of a profile you can put in %my documents%/WindowsPowerShell/Microsoft.PowerShell_profile.ps1.

```
function vPro
{
    Import-Module IntelvPro
}
```

Once you have created this profile, you can type **vPro** from within PowerShell to load the module.

3.3.2 Using Intel® AMT Credential Secure Storage

Intel AMT credentials can be securely stored in a PowerShell encrypted string using the Write-AMTCredential cmdlet. This allows the privileged administrator to store the Intel AMT required credentials without the credentials being exposed in plain text for any user to view.

Once credentials are stored once with Write-AMTCredential (see section 5.10.4) a later Powershell session can read them with Read-AMTCredential without exposing them.

To set your profile to load the module and set the Intel AMT credentials when you type **vPro** in a PowerShell session, change your profile as follows:

```
function vPro
{
    Import-Module IntelvPro
    New-Variable -Name AmtCred -Value (Read-AmtCredential)
}
```

13

3.3.3 Making Everything Load Automatically

To make the module load and the $AmtCred variable set (store first once with Write-AMTCredential (see section 5.10.4)) every time a PowerShell session is started modify the profile to include the following (not in a function block):

```
Import-Module IntelvPro
New-Variable -Name AmtCred -Value (Read-AmtCredential)
```

3.3.4 Easily Mounting an AMTSystem PowerShell Drive

To easily mount an AMTSystem Powershell Drive add the following function to the profile:

```
function mount-AMTDrive
{
  Param([string]$HostName,
[System.Management.Automation.PSCredential]$AMTCredential)
    process{
      New-PSdrive -scope global -name $HostName -psprovider amtsystem
        -root \ -computername $HostName -credential $AMTCredential
    }
}
```

Now mounting an AMTSystem Powershell drive by typing:

Mount-AMTDrive $HostName

The drive name will be $HostName and is listed when typing:

PSDrive

NOTE

The New-PSDrive cmdlet does not accept ~ / \ . : characters. It is recommended to use the Hostname instead of an IP address.
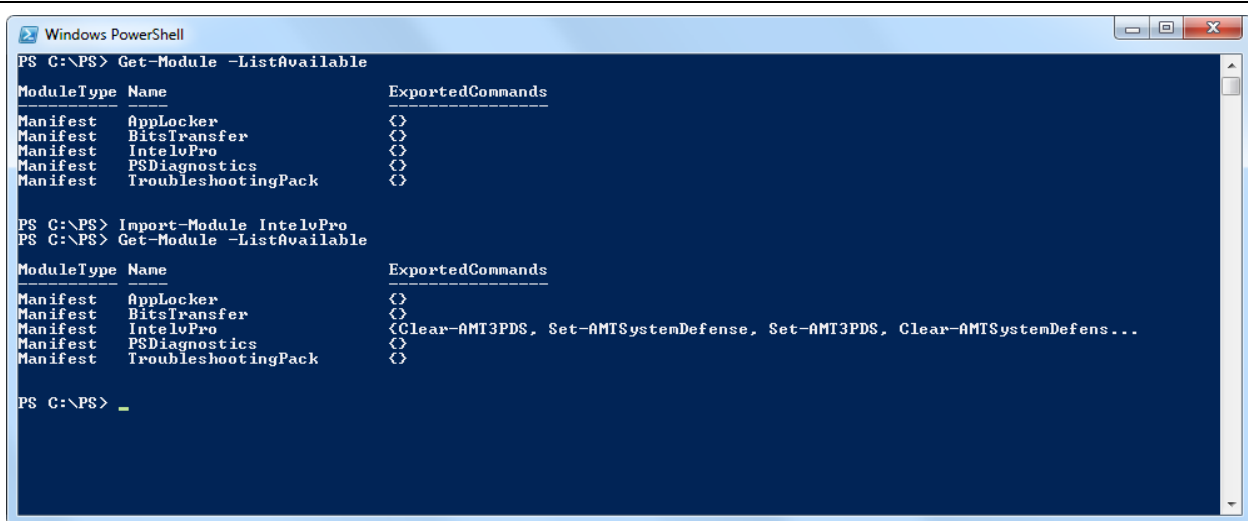
4 Using the Windows PowerShell Module for Intel vPro Technology

The Windows PowerShell console provides access to multiple modules at any given time. Before using a module's cmdlets and functions it must be imported. The module must be imported in each shell that the module will be used in.

4.1 Importing the Module

Run the Import-Module command to use a module's cmdlets and functions. To list the available modules type **Get-Module –ListAvailable** within Windows PowerShell. If the Windows PowerShell Module for Intel® vPro™ Technology is installed as described in section 3.2, **IntelvPro** will be listed as one of the available modules.

To import the Windows PowerShell Module for Intel vPro Technology type **Import-Module IntelvPro**, as shown below.

Figure 1: Importing the Module

After import type **Get-Module –ListAvailable** to show that the module has been imported along with the available Exported Commands.

To automatically load then module when Windows PowerShell is started, add **Import-Module IntelvPro** to the Windows PowerShell Profile.ps1 file.

Once the module has been imported, its cmdlets can be listed by using the **Get-Command –Module IntelvPro** command, as shown in Figure 2 below.
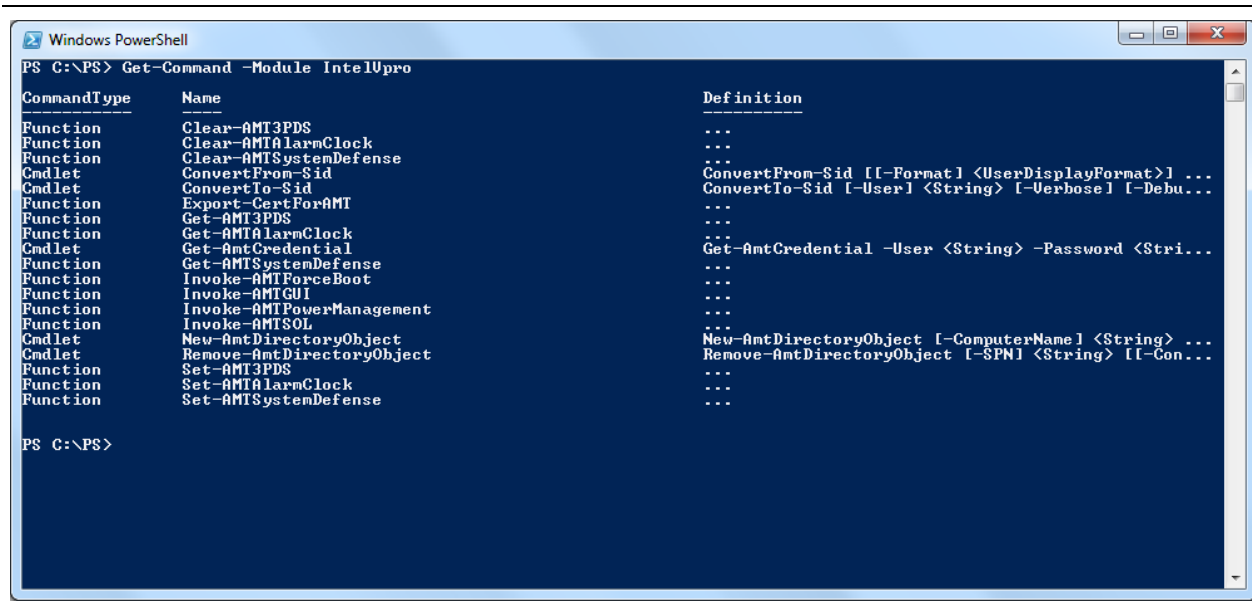
Figure 2: Listing the Available Cmdlets and Functions

4.2   Checking the Module Version

View the manifest for the module to see the installed version.
Type **Get-Module -ListAvailable -name intelvpro | format-list**

4.3   Usages

- Use Invoke-AMTPowerManagement (see section 5.1.1) to remotely power up, power down or power cycle the client Intel vPro system.

- Need to perform remediation on a system? Use Invoke-AMTForceBoot (see section 5.2.1) to redirect the system's boot process, forcing it to boot from a network share, bootable CD-ROM or DVD, remediation drive, PXE or other boot device.

- Invoke-AMTForceBoot (section 5.2.1) will also redirect the system's I/O via console redirection through serial over LAN (SOL). This feature supports remote troubleshooting, remote repair, software upgrades, and similar processes.

- To access and change BIOS settings remotely use Invoke-AMTForceBoot (section 5.2.1). Even if the system's power is off, the OS is down, or hardware has failed you can still perform remote updates and corrections of configuration settings.

16

- Use Get-AMTAccessMonitor (see section 5.11.1) and Get-AMTEventLog (see section 5.11.2) to display persistent logs stored in protected memory. The event log is available even if the OS is down or the hardware has already failed.

- Store information in the Third Party data Store with Set-AMT3PDS (see section 5.6.1). For example, an Anti-Virus program could store version information in the protected memory that is available for out of band access. A different cmdlet could then use Get-AMT3PDS (see section 5.6.2) to identify systems that need updating.

- To see what hardware a system has use Get-AMTHArdwareAsset (see section 5.11.4) to perform a hardware inventory. Hardware asset information is updated every time the system runs through power-on self-test (POST).

- The Intel vPro PowerShell Module does not natively support KVM Remote Control, but PowerShell can be used to start an application that does. For instance, to start RealVNC VNC* Viewer Plus, type the following:
  .\vncviewerplus.exe $ComputerName -amtusername=admin

5   Cmdlet Information

Table 1: Cmdlet Support of Intel AMT Versions

	3.0	3.2	5.1	6.0 and greater
Invoke-AMTPowerManagement	X	X	X	X
Invoke-AMTForceBoot	X	X	X	X
Invoke-AMTSOL	X	X	X	X
Set-AMTAlarmClock			X	X
Get-AMTAlarmClock			X	X
Set-AMTSystemDefense	X	X	X	X
Clear-AMTSystemDefense	X	X	X	X
Set-AMT3PDS	X	X	X	X
Get-AMT3PDS	X	X	X	X
Clear-AMT3PDS	X	X	X	X
Invoke-AMGUI	X	X	X	X
Get-AMTIDER	X	X	X	X
Start-AMTIDER	X	X	X	X
Stop-AMTIDER	X	X	X	X
Get-AMTAccessMonitor		X	X	X
Get-AMTEventLog		X	X	X
Get-AMTFirmwareVersion		X	X	X
Get-AMTHardwareAsset		X	X	X
Get-AMTPowerState		X	X	X

5.1 Intel AMT Power Management

Intel AMT Power Management can remotely power up, power down, or reset a client independent of Operating System or hardware state.

5.1.1 Invoke-AMTPowerManagement

NAME

Invoke-AMTPowerManagement

SYNOPSIS

Invokes an Intel Active Management Technology power control command

SYNTAX

Invoke-AMTPowerManagement [-ComputerName] <String[]> [-Port] <String> [-Operation] <String>[-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

The valid parameters for –Operation are {PowerOn, PowerOff, Reset}.

DESCRIPTION

This cmdlet invokes an Intel Active Management Technology power control operations (Power On, Power Off, and Power Reset) from clients that have Intel AMT firmware version 3.0 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Invoke-AMTPowerManagement –Full

```
------------------------- EXAMPLE 1 -------------------------

C:\PS>Invoke-AMTPowerManagement -computer:vproclient.vprodemo.com -TLS
-Operation:PowerOn


ComputerName                   Port       Operation            Status
------------                   ----       ---------            ------
vproclient.vprodemo.com        16993      PowerOn              Successful


------------------------- EXAMPLE 2 -------------------------

C:\PS>Invoke-AMTPowerManagement vproclient -Operation:Reset -Username:amtuser


Will prompt for digest username password.

ComputerName                   Port       Operation            Status
------------                   ----       ---------            ------
vproclient                     16992      Reset                Successful
------------------------- EXAMPLE 3 -------------------------

C:\PS>Invoke-AMTPowerManagement vproclient.vprodemo.com -Operation PowerOff
-Username:vprodemo\ITHelpDesk
```

```
Will prompt for Kerberos username password.

ComputerName                  Port      Operation          Status
------------                  ----      ---------          ------
vproclient.vprodemo.com       16992     PowerOff           Successful




----------------------- EXAMPLE 4 -------------------------

C:\PS>Invoke-AMTPowerManagement -ComputerName:vproclient.vprodemo.com
-Operation:PowerOff -credential $AMTCredential -TLS

ComputerName                  Port      Operation          Status
------------                  ----      ---------          ------
vproclient.vprodemo.com       16993     PowerOff           Successful
```

5.2   Intel AMT Force Boot

The Intel AMT Force Boot cmdlet remotely boots a client to a specified boot device such as PXE, CD/DVD, or local hard drive.

5.2.1   Invoke-AMTForceBoot

NAME

Invoke-AMTForceBoot

SYNOPSIS

Invokes the Intel Active Management Technology force boot command

SYNTAX

Invoke-AMTForceBoot [-ComputerName] <String[]> [[-Port] <String>] [-TLS] [-Operation] <String> [-Device] <String> [[-IDERPath] <String>] [[-Console] <String>] [[-SOLTerminalPath] <String>] [[-SOLTerminalArgList] <String>] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

The valid parameters for –Operation are {PowerOn, Reset}.

The valid parameters for –Device are {HardDrive, PXE, Optical, IDER, BIOSSetup}.

- HardDrive forces a boot to the hard drive, regardless of inserted bootable media.
- PXE forces a PXE boot.
- Optical forces a boot from the media in the optical drive.

- IDER forces an Intel vPro IDE Redirection boot.
- BIOSSetup forces a boot to the BIOS Setup configuration screens.

The valid parameter for –Console is {SOL}

If SOL is sepecifed than a Serial Over LAN connection is made to the target system. The local endpoint of this serial session is 127.0.0.1. A path to terminal program as well as arguments to invoke that terminal program must be specified. The Invoke-AMTForceBoot cmdlet will determine the port to connect to, so the argument list must define a '%Port' variable so the cmdlet knows where to put the actual port number.

For example to use Microsoft telnet the following would be defined:

> $SOLTerminalPath = "telnet"

> $SOLTerminalArgList = "-t ANSI 127.0.0.1 %Port"

DESCRIPTION

This cmdlet invokes an Intel Active Management Technology force boot to a PXE server, the local hard drive, CD/DVD ROM drive, or remote DVD/CD ISO image from clients that have Intel AMT firmware version 3.0 or higher.

For more details, review the PowerShell integrated help by typing:

Get-Help Invoke-AMTForceBoot –Full

```
------------------------ EXAMPLE 1 --------------------------
    C:\PS>Invoke-AMTForceBoot -Computer:vproclient.vprodemo.com -TLS
-Operation:PowerOn -Device:PXE


    ComputerName              Port   Operation        Device                  Status
    ------------              ----   ---------        ------                  ------
    vproclient.vprodemo.com 16993   PowerOn          PXE                     Successful




    ------------------------ EXAMPLE 2 --------------------------
    C:\PS>Invoke-AMTForceBoot 192.168.1.100 PowerOn PXE -credential $AMTCredential
-TLS


    ComputerName              Port   Operation        Device                  Status
    ------------              ----   ---------        ------                  ------
    192.168.1.100           16992   PowerOn          PXE                     Successful




    ------------------------ EXAMPLE 3 --------------------------
    C:\PS>Invoke-AMTForceBoot vproclient Reset –Device:Optical -Username:amtuser


    Will prompt for digest username password.
```

```
        ComputerName              Port    Operation      Device          Status
        ------------              ----    ---------      ------          ------
        vproclient                16992   Reset          Optical         Successful




        ------------------------ EXAMPLE 4 --------------------------

        C:\PS>Invoke-AMTForceBoot vproclient.vprodemo.com -Operation PowerOn
    -Device:HardDrive -Username:vprodemo\ITHelpDesk

        Will prompt for Kerberos username password.

        ComputerName              Port    Operation      Device          Status
        ------------              ----    ---------      ------          ------
        vproclient.vprodemo.com   16992   PowerOn        HardDrive       Successful




        ------------------------ EXAMPLE 5 --------------------------

        C:\PS>Invoke-AMTForceBoot -Computer:vproclient.vprodemo.com -Operation:Reset
    -Device:IDER -IDERPath:"C:\bootable_image.iso"

        ComputerName              Port    Operation      Device          Status
        ------------              ----    ---------      ------          ------
        vproclient.vprodemo.com   16992   PowerOn        IDER            Successful




        ------------------------ EXAMPLE 6 --------------------------

        C:\PS>Invoke-AMTForceBoot -ComputerName computer1.vprodemo.com,
    doesnotexist.vprodemo.com -TLS -Operation Reset -Device:Optical | Where {$_.Status
    -eq "Failed"}

        Will perform the power operation on every AMT client in the list, but only
    display the ones that failed.

        ComputerName              Port    Operation      Device          Status
        ------------              ----    ---------      ------          ------
        doesnotexist.vprodem...   16993   Reset          Optical         Failed




        ------------------------ EXAMPLE 7 --------------------------

        C:\PS>Get-SomeDataFromOtherCMDLet | Select ComputerName | Invoke-AMTForceBoot
    -TLS -Operation PowerOn -Device:HardDrive


        Get-SomeDataFromOtherCMDLet is a custom cmdlet that has an output of
    ComputerName, Port, and Operation; however, you only select ComputerName.
    Remaining parameters are manually provided.

        ComputerName              Port    Operation       Device          Status
        ------------              ----    ---------       ------          ------
    computer1.vprodemo.com   16993                      PowerOn         HardDrive
    Successful
        computer2.vprodemo.com   16993                      PowerOn
    HardDrive                 Successful
        computer3.vprodemo.com   16993                      PowerOn
    HardDrive                 Successful
```

```
------------------------ EXAMPLE 8 ------------------------

    C:\PS>Invoke-AMTForceBoot vproclient.vprodemo.com -Operation:Reset
-Device:BIOSSetup -Credential $AMTCredential -Console SOL -SOLTerminalPath "telnet"
-SOLTerminalArgList "-t ANSI 127.0.0.1 %Port"


    This will reboot the client to the BIOS Setup screens while connecting SOL to a
telnet window.

    Ok

    ComputerName : 192.168.1.106
    Port         : 16992
    Operation    : reset
    Device       : BIOSSetup
    Status       : Successful
```

5.3   Intel AMT Serial Over LAN

Serial Over LAN (SOL) is an Intel AMT capability that enables the input and output of the serial port of a managed system to be sent over the network. Console redirection can be performed over this SOL interface.

5.3.1   Invoke-AMTSOL

NAME

Invoke-AMTSOL

SYNOPSIS

Establishes a Serial Over LAN (SOL) session

SYNTAX

Invoke-AMTSOL [-ComputerName] <String[]> [-Port] <String> [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet establishes a Serial Over LAN communication to interact with clients that have Intel AMT firmware version 3.0 or higher.

For more details, review the PowerShell integrated help by typing:

Get-Help Invoke-AMTSOL –Full

```
------------------------ EXAMPLE 1 -------------------------
C:\PS>Invoke-AMTSOL -computer:vproclient.vprodemo.com -username:admin


------------------------ EXAMPLE 2 -------------------------
C:\PS>Invoke-AMTSOL 192.168.1.100 -credential $AMTCredential -TLS
```

5.4   Intel AMT Alarm Clock

The Intel AMT Alarm Clock can be configured to wake a managed system once at a specific time or multiple times with a periodical interval.

5.4.1   Set-AMTAlarmClock

NAME

Set-AMTAlarmClock

SYNOPSIS

Sets a Intel® Active Management Technology alarm clock timer

SYNTAX

Set-AMTAlarmClock [-ComputerName] <String[]> [-Port] <String> [-AlarmTime] <String> [-Interval <String>] [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

AlarmTime:

   The AlarmTime parameter is the date and time to wake the client. It is set as [YYYY]-[MM]-[DD]T[HH]:[MM]:[SS] Example: 2010-07-14T02:00:00 would wake the client on July 14, 2010 @ 02:00.

If the user sets the alarm date and time on a client in a different time zone, the alarm time specified will be set to the proper GMT for the client. For example, if running the cmdlet from a client in the Pacific Time zone to configure the wake up time on a client configured with Eastern Time for 08:00, the alarm clock will wake the client at 08:00 Eastern time.

Interval:

   Interval parameter is the desired reoccurrence interval for the alarm to be set. The format is: [DD]-[HH]-[MM]-[SS] Example: 07-00:00:00 would have a reoccurrence of every seven day at the same time. Example: 00-02:30:00 would have a reoccurrence of every 2 hours 30 minutes.

DESCRIPTION

This cmdlet allows the user to set a wake timer on clients that have Intel® Active Management Technology firmware version 5.1 or higher.

For more details, review the Windows PowerShell integrated help by typing:

   Get-Help Set-AMTAlarmClock -Full

```
    ------------------------- EXAMPLE 1 --------------------------

    C:\PS>Set-AMTAlarmClock -ComputerName:vproclient.vprodemo.com -TLS
-AlarmTime:2010-07-14T02:00:00


    Sets one time occurrence for wake up alarmclock.

    ComputerName  : vproclient.vprodemo.com
    Port          : 16993
    NextAlarmTime : Wednesday, July 14, 2010 2:00:00 AM
    Status        : Successful



    ------------------------- EXAMPLE 2 --------------------------

    C:\PS>Set-AMTAlarmClock vproclient.vprodemo.com -TLS -AlarmTime:2010-07-
14T02:00:00 -UserName vprodemo\administrator


    Will prompt for Kerberos User Password then Sets one time occurrence for wake
up alarmclock.

    ComputerName  : vproclient.vprodemo.com
    Port          : 16993
    NextAlarmTime : Wednesday, July 14, 2010 2:00:00 AM
    Status        : Successful



    ----------------------- EXAMPLE 3 ------------------------

    C:\PS>Set-AMTAlarmClock vproclient -UserName:admin -AlarmTime:2010-07-
14T02:00:00 -Interval:07-00:00:00


    Will prompt for Digest User Password then sets reoccuring wake up alarmclock
for once a week at that time.

    ComputerName     : vproclient
    Port             : 16992
    NextAlarmTime    : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval : P0Y0M07DT00H00M
    Status           : Successful
```

```
------------------------- EXAMPLE 4 --------------------------

    C:\PS>Get-Content computers.txt | Set-AMTAlarmClock -credential $AMTCredential
-TLS -AlarmTime:2010-07-14T02:00:00 -Interval:00-01:00:00 -credential
$SomeStoredPSCredential


    Will pull the list of amt clients from a text file and pipe them in the Set-
AMTAlarmClock CMDLet.
    Sets reoccuring wake up alarmclock for once every hour on and after that time.

    ComputerName     : computer1.vprodemo.com
    Port             : 16993
    NextAlarmTime    : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval : P0Y0M00DT02H00M
    Status           : Successful

    ComputerName     : computer2.vprodemo.com
    Port             : 16993
    NextAlarmTime    : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval : P0Y0M00DT02H00M
    Status           : Successful
```

5.4.2   Get-AMTAlarmClock

NAME

Get-AMTAlarmClock

SYNOPSIS

Returns status of the Intel Active Management Technology alarm clock timers

SYNTAX

Get-AMTAlarmClock [-ComputerName] <String[]> [-Port] <String> [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet returns the status of Intel Active Management Technology alarm clock timers from clients that have Intel AMT firmware version 5.1 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTAlarmClock -Full

```
------------------------- EXAMPLE 1 --------------------------

    C:\PS>Get-AMTAlarmClock -computer:vproclient.vprodemo.com -TLS


    ComputerName     : vproclient.vprodemo.com
    Port             : 16993
    NextAlarmTime    : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval : [None Set]
    Status           : Successful




------------------------- EXAMPLE 2 --------------------------

    C:\PS>Get-AMTAlarmClock vproclient -Username:amtuser -TLS


    Will prompt for digest username password.

    ComputerName     : vproclient
    Port             : 16993
    NextAlarmTime    : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval : 7 days, 0 hours, 0 minutes, 0 seconds
    Status           : Successful




------------------------- EXAMPLE 3 --------------------------

    C:\PS>Get-AMTAlarmClock vproclient.vprodemo.com -Username
vprodemo\administrator-TLS


    Will prompt for Kerberos username password.

    ComputerName     : vproclient
    Port             : 16993
    NextAlarmTime    : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval : [None Set]
    Status           : Successful




------------------------- EXAMPLE 4 --------------------------

    C:\PS>Get-AMTAlarmClock -ComputerName:vproclient.vprodemo.com -credential
$AMTCredential -TLS


    ComputerName     : vproclient
    Port             : 16993
    NextAlarmTime    : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval : [None Set]
    Status           : Successful
```

```
                        ------------------------- EXAMPLE 5 -------------------------

    C:\PS>Get-AMTAlarmClock -ComputerName
computer1.vprodemo.com,doesnotexist.vprodemo.com -TLS | Where {$_.Status -eq
    "Failed"}


    Will perform the clear Alarm clock operation on every AMT client in the list,
but only display the ones that failed
    .

    ComputerName      : doesnotexist.vprodemo.com
    Port              : 16993
    Status            : Failed
    NextAlarmTime     : [None Set]
    PeriodicInterval  : [None Set]




                        ------------------------- EXAMPLE 6 -------------------------

    C:\PS>Get-Content computers.txt | Get-AMTAlarmClock -Port:16993


    Will pull the list of amt clients from a text file and pipe them into Get-
AMTAlarmClock.

    ComputerName      : computer1.vprodemo.com
    Port              : 16993
    NextAlarmTime     : [None Set]
    PeriodicInterval  : [None Set]
    Status            : Successful

    ComputerName      : computer2.vprodemo.com
    Port              : 16993
    NextAlarmTime     : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval  : 7 days, 0 hours, 0 minutes, 0 seconds
    Status            : Successful

    ComputerName      : computer3.vprodemo.com
    Port              : 16993
    NextAlarmTime     : Wednesday, July 14, 2010 2:00:00 AM
    PeriodicInterval  : [None Set]
    Status            : Successful
```

5.4.3　　　Clear-AMTAlarmClock

NAME

Clear-AMTAlarmClock

SYNOPSIS

Clears Intel Active Management Technology alarm clock timers

SYNTAX

Clear-AMTAlarmClock [-ComputerName] <String[]> [-Port] <String> [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet clears the Intel Active Management Technology alarm clock timers from clients that have Intel AMT firmware version 5.1 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Clear-AMTAlarmClock -Full

```
C:\PS>Clear-AMTAlarmClock -computer:vproclient.vprodemo.com


ComputerName     : vproclient.vprodemo.com
Port             : 16992
NextAlarmTime    : [None Set]
PeriodicInterval : [None Set]
Status           : Successful



------------------------ EXAMPLE 2 -------------------------

C:\PS>Clear-AMTAlarmClock vproclient -Username:amtuser


Will prompt for digest username password.

ComputerName     : vproclient
Port             : 16992
NextAlarmTime    : [None Set]
PeriodicInterval : [None Set]
Status           : Successful



------------------------ EXAMPLE 3 -------------------------

C:\PS>Clear-AMTAlarmClock vproclient.vprodemo.com -Username
vprodemo\administrator


Will prompt for Kerberos username password.

ComputerName     : vproclient.vprodemo.com
Port             : 16993
NextAlarmTime    : [None Set]
PeriodicInterval : [None Set]
Status           : Successful



------------------------ EXAMPLE 4 -------------------------

C:\PS>Clear-AMTAlarmClock -ComputerName:vproclient.vprodemo.com -credential
$AMTCredential -TLS


ComputerName     : vproclient.vprodemo.com
Port             : 16993
```

```
        NextAlarmTime    : [None Set]
        PeriodicInterval : [None Set]
        Status           : Successful



        ------------------------- EXAMPLE 5 -------------------------

        C:\PS>Clear-AMTAlarmClock -ComputerName
computer1.vprodemo.com,doesnotexist.vprodemo.com | Where {$_.Status -eq "Fa
        iled"}


        Will perform the clear Alarm clock operation on every AMT client in the list,
but only display the ones that failed.

        ComputerName      : doesnotexist.vprodemo.com
        Port              : 16992
        Status            : Failed
        NextAlarmTime     : [None Set]
        PeriodicInterval  : [None Set]



        ------------------------- EXAMPLE 6 -------------------------

        C:\PS>Get-Content computers.txt | Clear-AMTAlarmClock -TLS


        Will pull the list of amt clients from a text file and pipe them into the
Clear-AMTAlarmClock CMDLet.

        ComputerName      : computer1.vprodemo.com
        Port              : 16993
        NextAlarmTime     : [None Set]
        PeriodicInterval  : [None Set]
        Status            : Successful

        ComputerName      : computer2.vprodemo.com
        Port              : 16993
        NextAlarmTime     : [None Set]
        PeriodicInterval  : [None Set]
        Status            : Successful

        ComputerName      : computer3.vprodemo.com
        Port              : 16993
        NextAlarmTime     : [None Set]
        PeriodicInterval  : [None Set]
        Status            : Successful
```

5.5   Intel AMT System Defense

System Defense is an Intel AMT capability that enforces network security policies such as filtering and preventing network traffic from getting to the operating system while still managing the client Out of Band with Intel AMT.

5.5.1   Set-AMTSystemDefense

NAME

Set-AMTSystemDefense

SYNOPSIS

Enables Intel Active Management Technology System Defense

SYNTAX

Set-AMTSystemDefense [-ComputerName] <String[]> [-Port] <String> [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet disables network access using Intel Active Management Technology System Defense from clients that have Intel AMT Firmware version 3.0 and Higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Set-AMTSystemDefense –Full

```
------------------------ EXAMPLE 1 ------------------------
C:\PS>Set-AMTSystemDefense vproclient.vprodemo.com -TLS


ComputerName                    Port      Status       EnabledOnInterfaces
-----------                     ----      ------       -------------------
vproclient.vprodemo.com         16993     Successful   Wireless1, Wired




------------------------ EXAMPLE 2 ------------------------
C:\PS>Set-AMTSystemDefense vproclient 16992  -username:amtuser


Will prompt for digest username password.


ComputerName                    Port      Status       EnabledOnInterfaces
-----------                     ----      ------       -------------------
vproclient                      16992     Successful   Wireless1, Wired0




------------------------ EXAMPLE 3 ------------------------
```

```
C:\PS>Get-Content computers.txt | Set-AMTSystemDefense -TLS


Will pull the list of amt clients from a text file and pipe them in the set-
AMTSystemDefense Cmdlet.

ComputerName                      Port        Status        EnabledOnInterfaces
------------                      ----        ------        -------------------
Computer1.vprodemo.com            16993       Successful     Wireless1, Wired0
Computer2.vprodemo.com            16993       Successful     Wired0
```

5.5.2　　　Get-AMTSystemDefense

NAME

Get-AMTSystemDefense

SYNOPSIS

Returns status of Intel Active Management Technology System Defense policies

SYNTAX

Get-AMTSystemDefense [-ComputerName] <String[]> [-Port] <String> [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet returns status of Intel Active Management Technology System Defense network access policies from clients that have Intel AMT firmware version 3.0 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTSystemDefense –Full

```
----------------------- EXAMPLE 1 -------------------------
C:\PS>Get-AMTSystemDefense vproclient.vprodemo.com -TLS

ComputerName                      Port        Status        EnabledOnInterfaces
------------                      ----        ------        ------------------
vproclient.vprodemo.com           16993       Successful    [None]




----------------------- EXAMPLE 2 -------------------------
C:\PS>Get-AMTSystemDefense vproclient 16992   –username:amtuser
```

```
    Will prompt for digest username password.

    ComputerName                       Port        Status       EnabledOnInterfaces
    ------------                       ----        ------       -------------------
    vproclient                         16992       Successful   Wireless1, Wired0




    ------------------------ EXAMPLE 3 ------------------------

    C:\PS>Get-AMTSystemDefense -ComputerName:vproclient.vprodemo.com -credential
$AMTCredential -TLS

    ComputerName                       Port        Status       EnabledOnInterfaces
    ------------                       ----        ------       -------------------
    vproclient.vprodemo.com            16993       Successful   Wired0




    ------------------------ EXAMPLE 4 ------------------------

    C:\PS>Get-Content computers.txt | Set-AMTSystemDefense -TLS


    Will pull the list of amt clients from a text file and pipe them into set-
AMTSystemDefense.
    ComputerName                       Port        Status       EnabledOnInterfaces
    ------------                       ----        ------       -------------------
    Computer1.vprodemo.com             16993       Successful   Wireless1, Wired0
    Computer2.vprodemo.com             16993       Successful   [None]
```

5.5.3   Clear-AMTSystemDefense

NAME

Clear-AMTSystemDefense

SYNOPSIS

Clears the Intel Active Management Technology System Defense policy

SYNTAX

Clear-AMTSystemDefense [-ComputerName] <String[]> [-Port <String>] [-CleanFlag
<Boolean>] [-TLS] [-Username <String>] [-Password <String>] [[-Credential]
<PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet clears the Intel Active Management Technology network access policy from clients that have Intel AMT firmware version 3.0 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Clear-AMTSystemDefense –Full

```
------------------------ EXAMPLE 1 -------------------------
C:\PS>Clear-AMTSystemDefense vproclient.vprodemo.com -TLS


ComputerName                    Port        Status      EnabledOnInterfaces
------------                    ----        ------      -------------------
vproclient.vprodemo.com         16993       Successful  [None]




------------------------ EXAMPLE 2 -------------------------
C:\PS>Clear-AMTSystemDefense vproclient 16992 -username:amtuser


Will prompt for digest username password.

ComputerName                    Port        Status      EnabledOnInterfaces
------------                    ----        ------      -------------------
vproclient                      16992       Successful  [None]




------------------------ EXAMPLE 3 -------------------------
    C:\PS>Clear-AMTSystemDefense -ComputerName:vproclient.vprodemo.com -credential
$AMTCredential -TLS

ComputerName                    Port        Status      EnabledOnInterfaces
------------                    ----        ------      -------------------
vproclient.vprodemo.com         16993       Successful  [None]




------------------------ EXAMPLE 4 -------------------------
    C:\PS>Get-Content computers.txt | Clear-AMTSystemDefense -TLS


    Will pull the list of clients from a text file and pipe them into Clear-
AMTSystemDefense.

ComputerName                    Port        Status      EnabledOnInterfaces
------------                    ----        ------      -------------------
vproclient1.vprodemo.com        16993       Successful  [None]
vproclient2.vprodemo.com        16993       Successful  [None]
```

5.6   Intel AMT Third Party Data Storage (3PDS)

The Intel AMT 3PDS is a persistent, nonvolatile memory space available to write and read data even when the OS is unresponsive or management agents are missing.

5.6.1   Set-AMT3PDS

NAME

Set-AMT3PDS

SYNOPSIS

Stores data in the Intel Active Management Technology Third Party Data Storage (3PDS)

SYNTAX

Set-AMT3PDS [-ComputerName] <String[]> [-Port] <String> [-Operation] <String> [-Enterprise] <String> [-Vendor] <String> [-Application] <String> [-Block] <String> [[-BlockData] <String>] [-BlockHidden <Boolean>] [-AppendWrite <Boolean>] [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

The valid parameters for –Operation are {Create, Write, CreateWrite}.

- *Create* makes a new block.
- *Write* writes the data to the block. All data is overwritten unless the –AppendWrite switch is specified.
- *CreateWrite* is a combination of the two operations – create a new block and write data to it.

Understanding 3PDS structure:

Data stored within the 3PDS is stored within blocks of nonvolatile memory in a hierarchical structure. Each block must be associated to a tiered structure of Enterprise -> Vendor -> Application -> Block Name.

3PDS Machine UUID:

When a block is created the application that created the block will specify a GUID to identify itself as the entity that created the block. When modifying blocks that were created by a different entity it may be necessary to specify the Machine UUID as part of the cmdlet parameter.

DESCRIPTION

This cmdlet stores data into the Intel Active Management Technology Third Party Data Storage (3PDS) of clients that have Intel® AMT firmware version 3.0 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Set-AMT3PDS –Full

```
------------------------- EXAMPLE 1 --------------------------

C:\PS>Set-AMT3PDS -computer:vproclient.vprodemo.com –TLS -Operation:Create
-Enterprise:Intel –Vendor:Intel -Application:PowerShell -Block:TestName


Creates Block using Kerberos credentials.

ComputerName                    Port           Operation          Status
------------                    ----           ---------          ------
vproclient.vprodemo.com         16993          Create             Successful




------------------------- EXAMPLE 2 --------------------------

C:\PS>Set-AMT3PDS 192.168.1.100 Write –credential $AMTCredential –
Enterprise:Intel –Vendor:Intel –Application:Power
Shell –Block:TestName –BlockData:"This is test"


Creates Block and write data to block

ComputerName                    Port           Operation          Status
------------                    ----           ---------          ------
192.168.1.100                   16992          Create             Successful




------------------------- EXAMPLE 3 --------------------------

C:\PS>Set-AMT3PDS -ComputerName:vproclient.vprodemo.com –TLS -Operation:Write
-Enterprise:Intel –Vendor:Intel -Application:PowerShell -Block:TestName –
BlockData:"Append this to existing data in block" -AppendWrite $true


Appends the data to data in existing block.

ComputerName                    Port           Operation          Status
------------                    ----           ---------          ------
vproclient.vprodemo.com         16993          Write              Successful




------------------------- EXAMPLE 4 --------------------------

C:\PS>Get-Content computers.txt | Set-AMT3PDS –TLS -Operation:Write
-Enterprise:Intel –Vendor:Intel -Application:PowerShell -Block:TestName
-BlockData:"This is test"


Will pull the list of amt clients from a text file and pipe them in the Set-
AMT3PDS CMDLet.
```

5.6.2   Get-AMT3PDS

NAME

Get-AMT3PDS

SYNOPSIS

Retrieves data from the Intel Active Management Technology Third Party Data Storage

SYNTAX

Get-AMT3PDS [-ComputerName] <String[]> [-Port] <String> [-Operation] <String> [[-Enterprise] <String>] [[-Vendor] <String>] [[-Application] <String>] [[-Block] <String>] [[-MachineUUID] <String>] [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

The valid parameters for –Operation are {Read, ListBlocks}.

- Read reads the data.
- ListBlocks retrieves all the available blocks.

DESCRIPTION

This cmdlet enables the user to retrieve data from Intel® Active Management Technology Third Party Data Storage (3PDS) from clients that have Intel® AMT firmware version 3.0 or higher.

When accessing the 3PDS the Enterprise, Vendor, Application must be set. A UUID may be optional. When reading data from the 3PDS the Get-AMT3PDS cmdlet will have read access to all blocks made using the same Enterprise, Vendor, and Application.

Understanding 3PDS structure:

Data stored within the 3PDS is stored within blocks of nonvolatile memory in a hierarchical structure. Each block must be associated to a tiered structure of Enterprise -> Vendor -> Application -> Block Name.

3PDS Machine UUID:

When a block is created the application that created the block will specify a GUID to identify itself as the entity that created the block. When modifying blocks that were created by a different entity it may be necessary to specify the Machine UUID as part of the cmdlet parameter.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMT3PDS –Full

```
------------------------ EXAMPLE 1 ------------------------

    C:\PS>Get-AMT3PDS -computerName:vproclient.vprodemo.com -TLS
-Operation:ListBlocks


    Retrieves all the availible blocks.

    ComputerName    : vproclient.vprodemo.com
    Port            : 16993
    Operation       : listblocks
    Status          : Success
    UUID            : BEAEE8BF2C09406DAE533F16080D2A6F
    Enterprise      : Virtualization
    Vendor          : Microsoft
    Application     : System Center ConfigMgr
    BlockName       : Out Of Band Management
    NumberOfBlocks  : 1


------------------------ EXAMPLE 2 ------------------------

    C:\PS>Get-AMT3PDS 192.168.1.100 –Operation ListBlocks -credential
$AMTCredential -TLS


    ComputerName    : 192.168.1.100
    Port            : 16993
    Operation       : listblocks
    Status          : Success
    UUID            : A1DF77DC16E2469188B2E1F389E5A472
    Enterprise      : Intel
    Vendor          : Intel
    Application     : PowerShell
    BlockName       : Test
    NumberOfBlocks  : 1


------------------------ EXAMPLE 3 ------------------------

    C:\PS>Get-AMT3PDS vproclient.vprodemo.com -Operation:Read
-Username:vprodemo\ITHelpDesk -Enterprise:Intel -Vendor:Intel
-Application:PowerShell -Block:Test


    Will prompt for Kerberos username password and then retrieve Data.

    ComputerName : vproclient.vprodemo.com
    Port         : 16992
    Operation    : read
    Status       : Success
    Blocks       : 1
    Data         : Test Data


------------------------ EXAMPLE 4 ------------------------

    C:\PS>Get-Content computers.txt | Get-AMT3PDS -TLS -Operation:ListBlocks


    Will pull the list of amt clients from a text file and pipe them in Get-
AMT3PDS.
```

```
------------------------- EXAMPLE 5 --------------------------

    C:\PS>Get-AMT3PDS-computerName:vproclient.vprodemo.com -port:16993
-Operation:read -Enterprise:"Virtualization" -Vendor:"Microsoft"
-Application:"System Center ConfigMgr"
-Block:"Out Of Band Management"
-MachineUUID:"BEAEE8BF2C09406DAE533F16080D2A6F"


    Example to pull data from the AMT 3PDS accessible by System Center
Configuration Manager
```

5.6.3 Clear-AMT3PDS

NAME

Clear-AMT3PDS

SYNOPSIS

Deletes data from the Intel® Active Management Technology Third Party Data Storage

SYNTAX

Clear-AMT3PDS [-ComputerName] <String[]> [-Port] <String> [-Enterprise] <String> [[-Vendor] <String>] [[-Application] <String>] [[-Block] <String>] [[-MachineUUID] <String>] [-TLS] [-Username <String>] [-Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet deletes data from the Intel® Active Management Technology Third Party Data Storage (3PDS) from clients that have Intel® AMT firmware version 3.0 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Clear-AMT3PDS –Full

```
------------------------- EXAMPLE 1 --------------------------
    C:\PS>Clear-AMT3PDS -computer:vproclient.vprodemo.com –TLS -Enterprise:Intel


    Will delete all block data under enterprise value specified.

ComputerName                    Port            Operation           Status
------------                    ----            ---------           ------
vproclient.vprodemo.com         16993           Delete              Successful


------------------------- EXAMPLE 2 --------------------------

    C:\PS>Clear-AMT3PDS 192.168.1.100 –credential $AMTCredential –Enterprise:Intel
-Vendor:Intel


    Will delete all block data under Enterprise, Vendor value specified.
```

```
    ComputerName                    Port            Operation        Status
    ------------                    ----            ---------        ------
    192.168.1.100                   16992           Delete           Successful




    ----------------------- EXAMPLE 3 ------------------------

    C:\PS>Clear-AMT3PDS vproclient 16992 -Username:amtuser -Enterprise:Intel
-Vendor:Intel -Application:PowerShell


    Will delete all block data under Enterprise, Vendor, Application value
specified.

    ComputerName                    Port            Operation        Status
    ------------                    ----            ---------        ------
    vproclient                      16992           Delete           Successful



    ----------------------- EXAMPLE 4 ------------------------

    C:\PS>Clear-AMT3PDS vproclient.vprodemo.com -credential $AMTCredential
-Enterprise:Intel -Vendor:Intel -Application
    :PowerShell -Block:Test


    Will delete block data under Enterprise, Vendor, Application, Block specified.

    ComputerName                    Port            Operation        Status
    ------------                    ----            ---------        ------
    vproclient.vprodemo.com         16992           Delete           Successful



    ----------------------- EXAMPLE 5 ------------------------

    C:\PS>Get-Content computers.txt | Clear-AMT3PDS -TLS -Enterprise:Intel
-Vendor:Intel -Application:PowerShell -Block
    :Test


    ComputerName                    Port            Operation        Status
    ------------                    ----            ---------        ------
    computer1.vprodemo.com          16993           Delete           Successful
    computer2.vprodemo.com          16993           Delete           Successful
    computer3.vprodemo.com          16993           Delete           Successful
```

5.7   Intel AMT PowerShell GUI

The Intel AMT PowerShell Graphical User Interface (GUI) provides a simple interface for invoking a majority of the commands supported within the module.

5.7.1   Invoke-AMTGUI

NAME

Invoke-AMTGUI

SYNOPSIS

GUI that invokes PowerShell Module for Intel® vPro™ technology cmdlets

SYNTAX

Invoke-AMTGUI [[-ComputerName] <String[]>] [-Credential <PSCredential>][-xmlConfig] <string> [<CommonParameters>]

DESCRIPTION

The Intel AMT PowerShell Graphical User Interface (GUI) provides a simple interface for invoking a majority of the commands supported within the module. An xml configuration file can be passed in to configure the GUI. See the default XML in the invoke-amtgui.ps1 file.
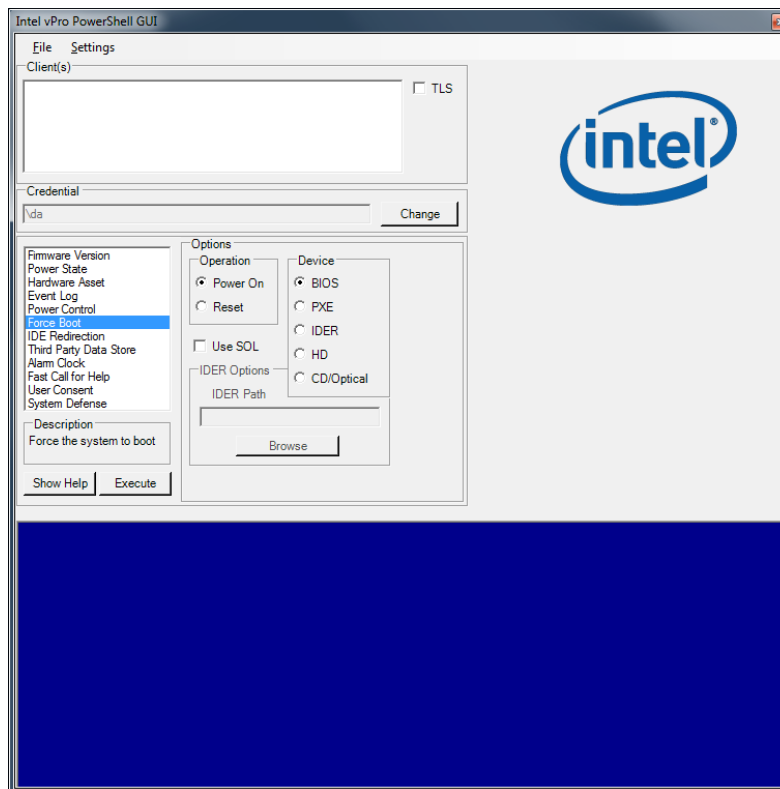
.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Invoke-AMTGUI –Full

```
------------------------- EXAMPLE 1 --------------------------


C:\PS>Invoke-AMTGUI


------------------------- EXAMPLE 2 -------------------------
C:\PS>Invoke-AMTGUI $computerName


------------------------- EXAMPLE 3 -------------------------
C:\PS>Invoke-AMTGUI $computerName -Credential $AmtCredential


------------------------- EXAMPLE 4 -------------------------
C:\PS>Invoke-AMTGUI -xmlConfig sample.xml
```

5.8 Intel AMT User Consent

Intel AMT User Consent is a method to query a user for consent to remotely manage the client. To enforce the user's consent to opt-in for a redirection session, a secure output window ("sprite") is displayed on the user's screen on top of any other window. The user is prompted to read out to the IT administrator a randomly-generated number. Only if the IT administrator types in the correct number will the redirection session is allowed to begin. Once a valid KVM Remote Control session is invoked, the user's entire screen will be surrounded by a red bar indicating that an IT administrator is in the process of a KVM Remote Control session.

5.8.1 Get-AMTUserConsent

NAME

Get-AMTUserConsent

SYNOPSIS

Gets the Intel AMT user consent state

SYNTAX

Get-AMTUserConsent [-ComputerName] <String[]> [[-Port] <String>] [-Username <String>] [-Password <String>] [-TLS] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet gets the Intel AMT user consent state from clients that have Intel AMT firmware version 3.0 and higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTUserConsent –Full

```
------------------------ EXAMPLE 1 -------------------------
C:\PS>Write-AmtCredential

------------------------ EXAMPLE 2 -------------------------
C:\PS>$AMTCredential = Write-AmtCredential   (will assume the digest account
"admin")

------------------------ EXAMPLE 3 -------------------------
C:\PS>$AMTCredential = Get-Credential


Write-AmtCredential –Username $AMTCredential.Username –Password
$AMTCredential.Password
```

5.8.2   Start-AMTUserConsent

NAME

Start-AMTUserConsent

SYNOPSIS

Starts the Intel AMT user consent process

SYNTAX

Start-AMTUserConsent [-ComputerName] <String[]> [-Port] <String> [-Username <String>] [-Password <String>] [-TLS] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet starts the user consent process on clients that have Intel AMT firmware version 3.0 and higher. The user consent screen is displayed on the remote client and the code must be passed into this cmdlet.

For more details, review the Windows PowerShell integrated help by typing:

   Get-Help Start-AMTUserConsent –Full

```
------------------------- EXAMPLE 1 --------------------------
C:\PS>Start-AMTUserConsent vproclient.vprodemo.com -credential $AMTCredential
```


5.8.3   Stop-AMTUserConsent

NAME

Stop-AMTUserConsent

SYNOPSIS

Stops the Intel AMT user consent process

SYNTAX

Stop-AMTUserConsent [-ComputerName] <String[]> [-Port] <String> [-Username <String>] [-Password <String>] [-TLS] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet stops the user consent process on clients that have Intel AMT firmware version 3.0 and higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Stop-AMTUserConsent –Full

```
------------------------- EXAMPLE 1 -------------------------

C:\PS>Stop-AMTUserConsent vproclient.vprodemo.com -credential $AMTCredential


ComputerName                 Port                         Status
------------                 ----                         ------
vproclient.vprodemo.com      16992                        Successful
```

5.9   Intel AMT IDER

Intel AMT IDE Redirection (IDER) is a technology that allows redirecting the floppy disk (IMG) or CD-ROM (ISO) from the console to a remote client. This client can then be booted from an ISO or IMG file for management or remediation.

5.9.1   Get-AMTIDER

NAME

Get-AMTIDER

SYNOPSIS

Lists the Intel AMT IDE Redirection sessions

SYNTAX

Get-AMTIDER [<CommonParameters>]

DESCRIPTION

This cmdlet lists the Intel AMT IDE redirection (IDER) sessions.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTIDER –Full

```
------------------------ EXAMPLE 1 -------------------------

C:\PS>Get-AMTIDER


ComputerName               IDERSessionID IDERPath        IDERState
------------               ------------- --------        --------
192.168.1.100                          1 boot.iso        Disabled
```

5.9.2   Start-AMTIDER

NAME

Start-AMTIDER

SYNOPSIS

Starts an Intel AMTIDE redirection session

SYNTAX

Start-AMTIDER [-ComputerName] <String[]> [-Operation] <String> [[-IDERPath]
<String>] [-TLS] [-Username <String>] [-Password <String>] [[-Credential]
<PSCredential>] [<CommonParameters>]

The valid parameters for –Operation are {PowerOn, Reset}.

DESCRIPTION

This cmdlet starts an Intel AMT IDE redirection (IDER) session to clients that have Intel AMT firmware version 3.0 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Start-AMTIDER –Full

```
------------------------- EXAMPLE 1 --------------------------

    C:\PS>Start-AMTider -computername:192.168.1.100 -operation:Reset
-iderpath:.\boot.iso -credential:$AMTCredential


    ComputerName            IDERSessionID IDERPath                      Status
    ------------            ------------- --------                      ------
    192.168.1.100                       1 boot.iso                     Successful
```

5.9.3 Stop-AMTIDER

NAME

Stop-AMTIDER

SYNOPSIS

Stops a specified Intel AMT IDE redirection session

SYNTAX

Stop-AMTIDER [[-IDERSessionID] <String[]>] [-CloseAllSessions] [<CommonParameters>]

DESCRIPTION

Stops a specified Intel AMT IDE Redirection (IDER) session. If no ID is specified the oldest IDER session is closed.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Stop-AMTIDER –Full

```
------------------------- EXAMPLE 1 --------------------------

  C:\PS>Stop-AMTider $SessionID


------------------------- EXAMPLE 2 --------------------------

  C:\PS>Stop-AMTIDER


  If no ID is specified the oldest IDER session is closed.
```

```
------------------------- EXAMPLE 3 --------------------------

C:\PS>Stop-AMTIDER -CloseAllSessions


Shuts down all IDER sessions
```

5.10   Configuration Cmdlets

This section describes cmdlets that help configure a system or provide more information about a client's configuration state.

5.10.1   Get-AMTSetup

NAME

Get-AMTSetup

SYNOPSIS

Returns Intel AMT setup information

SYNTAX

Get-AMTSetup [<CommonParameters>]

DESCRIPTION

This cmdlet gets Intel AMT setup information from the local system.

NOTES

Intel ME device drivers need to be installed.

This cmdlet requires elevated administrator privileges.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTSetup –Full

```
------------------------- EXAMPLE 1 --------------------------

C:\PS>Get-AmtSetup


SetupStatus                      : Unconfigured
CoreVersion                      : 7.0.0
BiosVersion                      : ASNBCPT1.86C.0036.B00.1008051344
RemoteConfigurationSupported     :
ConfigurationNonce               : bEYmf32WD19zvRvnNIjOzKGTg0U=
ClientControlSupported           : True
HostConfigurationSupported       : True
ActiveHashes                     : {742C3192E607E424EB4549542BE1BBC53E6174E2, 132D0
                                       D45534B6997CDB2D5C339E25576609B5CC6,
2796BAE63F1
                                       801E277261BA0D77770028F20EEE4,
D1EB23A46D17D68FD
                                       92564C2F1F1601764D8E349...}
HostName                         : VPROCOMPUTER
IPAddress                        : {192.168.1.100, fe80::84a1:ffcc:d82e:90d3}
DNSDomain                        : vprodemo.com
DHCPEnabled                      : True
UUID                             : 88888888-8887-8888-8888-878888888888
```

5.10.2 Enter-AMTRemoteConfiguration

NAME

Enter-AMTRemoteConfiguration

SYNOPSIS

Enters a Remote Configuration Session with an Intel AMT enabled client

SYNTAX

Enter-AmtRemoteConfiguration [-Session] <PSSession> [-Certificate]
<X509Certificate> [[-otp] <String>] [-Force] [<CommonParameters>]

Enter-AmtRemoteConfiguration [-ComputerName] <String> [-Certificate]
<X509Certificate> [[-Credential] <PSCredential>] [[-otp] <String>] [-Force]
[<CommonParameters>]

DESCRIPTION

The Enter-AmtRemoteConfiguration cmdlet starts an interactive configuration session
with an unconfigured Intel AMT enabled client with firmware version 3.2 and higher.

A PSRemoting session is required in order to discover information about the device and
start the configuration service. A remote WS-MAN session is then established with the
device and remains the active session until Stop-AMTConfiguration is called.

NOTES

Intel AMT Provisioning:

Intel AMT must in an unconfigured or remoteStarted state.

HECI Drivers must be installed and working on the target Intel® AMT system.

Intel AMT must be enabled in the BIOS.

Configuration Sessions are not supported over wireless connections.

The Intel onboard Wired LAN must be connected.

This command can only be used remotely.

$ConfigurationCertificate must be set to the thumbprint of the desired certificate in the directory Microsoft.PowerShell.Security\Certificate::CurrentUser\my

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Enter-AMTRemoteConfiguration –Full

```
------------------------ EXAMPLE 1 ------------------------

    C:\PS>Enter-AmtRemoteConfiguration vprocomputer.vprodemo.com
$ConfigurationCertificate
```

5.10.3   Read-AMTCredential

NAME

Read-AmtCredential

SYNOPSIS

Reads an Intel AMT credential from secure string storage

SYNTAX

Read-AmtCredential [[-FilePath] <String>] [[-Key] <String>]
[<CommonParameters>]

DESCRIPTION

Reads an Intel AMT credential from secure string storage.

NOTES

Reads System.Security.SecureString from the default user path.

An Intel AMT credential can be securely stored in a PowerShell encrypted string using the Write-AMTCredential cmdlet. This allows the privileged administrator to store the Intel AMT credential without them being exposed in plaintext for any user to view.

Once stored, a Powershell cmdlet in a later Powershell session can read the Intel AMT credential with Read-AMTCredential without exposing it.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Read-AMTCredential –Full

```
------------------------- EXAMPLE 1 -------------------------
C:\PS>Read-AmtCredential


------------------------- EXAMPLE 2 -------------------------
C:\PS>$AMTCredential = read-AmtCredential
```

5.10.4   Write-AMTCredential

NAME

Write-AmtCredential

SYNOPSIS

Writes an Intel AMT credential to secure string storage

SYNTAX

Write-AmtCredential [[-FilePath] <String>] [[-Key] <String>] [[-Hint] <String>] [[-AsPlainText]] [[-Force]] [[-Username] <String>] [-Password] <SecureString> [<CommonParameters>]

DESCRIPTION

Writes an Intel AMT credential to secure string storage.

An Intel AMT credential can be securely stored in a PowerShell encrypted string using the Write-AMTCredential cmdlet. This allows the privileged administrator to store the Intel AMT credential without them being exposed in plaintext for any user to view.

Once stored, a Powershell cmdlet in a later Powershell session can read the Intel AMT credential with Read-AMTCredential without exposing it. For testing purposes the –force switch can be used to store plaintext credentials.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Write-AMTCredential –Full

```
        ------------------------ EXAMPLE 1 -------------------------
    C:\PS>Write-AmtCredential
        ------------------------ EXAMPLE 2 -------------------------
    C:\PS>$AMTCredential = Write-AmtCredential   (will assume the digest account
"admin")
        ------------------------ EXAMPLE 3 -------------------------
    C:\PS>$AMTCredential = Get-Credential

    Write-AmtCredential –Username $AMTCredential.Username –Password
$AMTCredential.Password
```

5.11 Informational Cmdlets

This section describes the cmdlets that directly communicate with the client's Intel AMT firmware to return information about the client system.

5.11.1 Get-AMTAccessMonitor

NAME

Get-AMTAccessMonitor

SYNOPSIS

Returns Intel AMT access events

SYNTAX

Get-AMTAccessMonitor [-ComputerName] <String[]> [-Username <String>] [-Password <String>] [-TLS] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet returns the Intel AMT access events from clients that have Intel AMT firmware version 3.2 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTAccessMonitor –Full

```
        ------------------------ EXAMPLE 1 -------------------------
    C:\PS>Get-AMTAccessMonitor -computername:vProClient
```

```
      ComputerName : vProClient
      TimeStamp    : 1/01/2011 11:46:55 PM
      Message      : AMT Provisioning Started
      Location     :
      User         :




      ------------------------ EXAMPLE 2 --------------------------

      C:\PS>Get-AMTAccessMonitor vProClient -Credential $amtcred - TLS | Format-Table


      ComputerName        TimeStamp              Message              Location        User
      ------------        ---------              -------              --------        ----
      vProClient          1/01/2011 11:46:55 PM  AMT Provisioning Sta...
```

5.11.2   Get-AMTEventLog

NAME

Get-AMTEventLog

SYNOPSIS

Returns the Intel AMT event log

SYNTAX

Get-AMTEventLog [-ComputerName] <String[]> [-Username <String>] [-Password <String>] [-TLS] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet returns the Intel AMT event log from clients that have Intel AMT firmware version 3.2 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTEventLog –Full

```
      ------------------------ EXAMPLE 1 --------------------------
      C:\PS>Get-AMTEventLog -computername:vProClient


      ComputerName : vProClient
      Severity     : 8
      TimeStamp    : 2010/01/01 7:28:20 AM
      Source       : BIOS
      Message      : Starting operating system boot process



      ------------------------ EXAMPLE 2 --------------------------

      C:\PS>Get-AMTEventLog -computername:vProClient | Format-Table
```

```
ComputerName      Severity    TimeStamp                     Source      Message
------------      --------    ---------                     ------      -------
vProClient              8     2010/01/01 7:28:20 AM         BIOS        Starting
```

5.11.3 Get-AMTFirmwareVersion

NAME

Get-AMTFirmwareVersion

SYNOPSIS

Returns the core Intel AMT firmware version

SYNTAX

Get-AMTFirmwareVersion [-ComputerName] <String[]> [-Username <String>] [-Password <String>] [-TLS] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet returns the Intel AMT core firmware version from clients that have Intel AMT firmware version 3.2 or higher.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTFirmwareVersion –Full

```
------------------------- EXAMPLE 1 -------------------------
C:\PS>Get-AMTFirmwareVersion –computername:vProClient

ComputerName              Property                      Value
------------              --------                      -----
vProClient                AMT FW Core Version           7.1.3.1053
```

5.11.4 Get-AMTHardwareAsset

NAME

Get-AMTHardwareAsset

SYNOPSIS

Shows hardware information about the system

SYNTAX

 Get-AMTHardwareAsset [-ComputerName] <String[]> [[-Port] <String>] [-Username <String>] [-Password <String>] [-TLS][-TextOutput] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet returns the hardware information from clients that have Intel AMT firmware version 3.2 or higher.

Use the -TextOutput switch to show the data in a text only tree format.

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTHardwareAsset –Full

```
------------------------- EXAMPLE 1 --------------------------

C:\PS>get-AMTHardwareAsset vProClient.vprodemo.com -Credential $AMTCredential


ComputerName                    PSParentPath                    Name
Value
------------                    ------------                    ----
-----
    vProClient.vprodemo.com     \HardwareAssets\BIOS\Prima... Version
1.16
    vProClient.vprodemo.com     \HardwareAssets\BIOS\Prima... ReleaseDate
2010/10/21 12:00:00 AM
    vProClient.vprodemo.com     \HardwareAssets\BIOS\Prima... Manufacturer
American Megatrends Inc.
    vProClient.vprodemo.com     \HardwareAssets\Cpu\CPU 0       CPUStatus
CPU Enabled
    vProClient.vprodemo.com     \HardwareAssets\Cpu\CPU 0       CurrentClockSpeed
2700
    vProClient.vprodemo.com     \HardwareAssets\Cpu\CPU 0
ExternalBusClockSpeed           100
    vProClient.vprodemo.com     \HardwareAssets\Cpu\CPU 0       Family
Intel(R) Core(TM) i7 proc
    e...
    vProClient.vprodemo.com     \HardwareAssets\Cpu\CPU 0       MaxClockSpeed
2700
    vProClient.vprodemo.com     \HardwareAssets\Cpu\CPU 0       UpgradeMethod
ZIF Socket
    vProClient.vprodemo.com     \HardwareAssets\Cpu\CPU 0       Manufacturer
Intel(R) Corporation
    vProClient.vprodemo.com     \HardwareAssets\Cpu\CPU 0       Version
Intel(R) Core(TM) i7-2620
    M...




------------------------- EXAMPLE 2 --------------------------

    C:\PS>Get-AMTHardwareAsset -ComputerName vProClient.vProDemo.com -Credential
$AMTCredential | Where-Object -FilterS
    c#ript {$_.PSPath -like "*BIOS*"}


ComputerName                    PSParentPath                    Name
Value
------------                    ------------                    ----
-----
    vProClient.vprodemo.com     \HardwareAssets\BIOS\Prima... Version
1.16
```

```
    vProClient.vprodemo.com            \HardwareAssets\BIOS\Prima... ReleaseDate
2010/10/21 12:00:00 AM
    vProClient.vprodemo.com            \HardwareAssets\BIOS\Prima... Manufacturer
American Megatrends Inc.

    Displays only the results that contain "BIOS" in their path




    ------------------------ EXAMPLE 3 --------------------------

    C:\PS>Get-AMTHardwareAsset -ComputerName vProClient.vProDemo.com -Credential
$AMTCredential | Where-Object -FilterS
    c#ript {$_.PSPath -like "*BIOS*"} | format-list


    ComputerName : vProClient.vprodemo.com
    PSParentPath : AmtSystem::\HardwareAssets\BIOS\Primary BIOS
    Name         : Version
    Value        : 1.16

    ComputerName : vProClient.vprodemo.com
    PSParentPath : AmtSystem::\HardwareAssets\BIOS\Primary BIOS
    Name         : ReleaseDate
    Value        : 2010/10/21 12:00:00 AM

    ComputerName : vProClient.vprodemo.com
    PSParentPath : AmtSystem::\HardwareAssets\BIOS\Primary BIOS
    Name         : Manufacturer
    Value        : American Megatrends Inc.

    Displays only the results that contain "BIOS" in their path and formatted into
a list.




    ------------------------ EXAMPLE 4 --------------------------

    C:\PS>Get-AMTHardwareAsset -ComputerName vProClient -Credential $AMTCredential
-TextOutput


    vProClient BIOS
    vProClient  BIOS:Primary BIOS
        Version............. 1.16
        ReleaseDate......... 2010/10/21 12:00:00 AM
        Manufacturer........ American Megatrends Inc.
    vProClient Cpu
    vProClient  Cpu:CPU 0
        CPUStatus........... CPU Enabled
        CurrentClockSpeed... 2700
        ExternalBusClockSpeed 100
        Family.............. Intel(R) Core(TM) i7 processor
        MaxClockSpeed....... 2700
        UpgradeMethod....... ZIF Socket
        Manufacturer........ Intel(R) Corporation
        Version............. Intel(R) Core(TM) i7-2620M CPU @ 2.70GHz

    Displays results formatted as text.
```

5.11.5   Get-AMTPowerState

NAME

Get-AMTPowerState

SYNOPSIS

Returns the system power state

SYNTAX

Get-AMTPowerState [-ComputerName] <String[]> [[-Port] <String>] [-Username <String>] [-Password <String>] [-TLS] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION

This cmdlet returns the system power state from clients that have Intel AMT firmware version 3.2 or higher.

For more details, review the Windows PowerShell integrated help by typing:

   Get-Help Get-AMTPowerState –Full

```
------------------------- EXAMPLE 1 -------------------------

C:\PS>Get-AMTPowerState -computername:vproclient.vprodemo.com


Computer Name                   Power State ID         Power State Description
-------------                   -------------          -----------------------
vproclient.vprodemo.com                   2            On (S0)




------------------------- EXAMPLE 2 -------------------------

C:\PS>Get-AMTPowerState -computername:vproclient.vprodemo.com -credential
$AMTCredential -TLS


Computer Name                   Power State ID         Power State Description
-------------                   -------------          -----------------------
vproclient.vprodemo.com                   2            On (S0)
```

5.12 Intel Fast Call for Help

This section describes the cmdlets that allow configuration of an environment that supports Intel Fast Call for Help. Once the MPS proxies are setup using set-AMTMPS clients can be added to the MPS interface with set-AMTMPSCclient. Afterwards all AMT cmdlets will transparently route to the client through the MPS interface.

- Setup proxy information with set-AMTMPS
- Identify when client connects to MPS.
- Add client with set-AMTMPSClient
- Call cmdlets with no change.

5.12.1 Get-AMTMPSStatus

NAME

Get-AMTMPSStatus

SYNOPSIS

Returns the status of the Intel Fast Call for Help Management Presence Server (MPS) interface settings

SYNTAX

Get-AMTMPSStatus [<CommonParameters>]

DESCRIPTION

Returns the status of the Intel Fast Call for Help Management Presence Server (MPS) interface settings

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Get-AMTMPSStatus –Full

```
-------------------------- EXAMPLE 1 --------------------------
get-AMTMPSStatus

HTTPProxy              SOCKSProxy              Client        Enabled
---------              ----------              ------        -------
HTTP Proxy address     SOCKS Proxy address                   True
```

5.12.2 Set-AMTMPS

NAME

Set-AMTMPS

SYNOPSIS

Set proxy information for the Intel Fast Call for Help Management Presence Server (MPS) interface

SYNTAX

Set-AMTMPS [-HTTPProxy] <String[]> [-SOCKSProxy] <String[]>
[<CommonParameters>]

DESCRIPTION

Set proxy information for the Intel Fast Call for Help Management Presence Server
(MPS) interface

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Set-AMTMPS –Full

```
-------------------------- EXAMPLE 1 --------------------------
set-AMTMPS –HTTPProxy HTTPProxy –SOCKSProxy SocksProxy

HTTPProxy            SOCKSProxy          Client        Enabled
---------            ----------          ------        -------
HTTP Proxy address   SOCKS Proxy address               True
```


5.12.3   Set-AMTMPSClient

NAME

Set-AMTMPSClient

SYNOPSIS

Add and remove clients from the Intel Fast Call for Help Management Presence Server
(MPS) interface

SYNTAX

Set-AMTMPSClient [-action] <String[]> [-hostname] <String[]>
[<CommonParameters>]

The valid parameters for –action are {add, remove}

DESCRIPTION

Add and remove clients from the Intel Fast Call for Help Management Presence Server
(MPS) interface

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Set-AMTMPSClient –Full

```
-------------------------- EXAMPLE 1 --------------------------
set-AMTMPSClient -action add -hostname DemoClient

Added DemoClient to MPS client list


-------------------------- EXAMPLE 2 --------------------------
set-AMTMPSClient -action remove -hostname DemoClient

Removed DemoClient from MPS client list
```

5.12.4 Clear-AMTMPS

NAME

Clear-AMTMPS

SYNOPSIS

Clears the Intel Fast Call for Help Management Presence Server (MPS) interface settings

SYNTAX

Clear-AMTMPS [<CommonParameters>]

DESCRIPTION

Clears the Intel Fast Call for Help Management Presence Server (MPS) interface settings

For more details, review the Windows PowerShell integrated help by typing:

Get-Help Clear-AMTMPS –Full

```
-------------------------- EXAMPLE 1 --------------------------
clear-AMTMPS

MPS settings cleared
```

6   AMTSystem PowerShell Drive Provider

Microsoft has added the concept of a Windows PowerShell drive to Windows PowerShell version 2.0. These drives are information stores that can be accessed like a file system drive. Many drives are created automatically, such as the Registry (HKCU: and HKLM:), the certificate store (Cert:) and the Environment (ENV:)

http://technet.microsoft.com/en-us/library/dd315335.aspx

Intel has created a PowerShell Drive provider called AMTSystem that allows a remote Intel vPro technology enabled client to be accessed like a drive. This powerful feature allows the remote system's Intel vPro technology settings to easily be listed, accessed and changed.

Map a New-PSDrive called "AMT" to a remote system with Intel vPro technology. To do so, run the following command from the PowerShell console:

 New-PSDrive -Name AMT -PSProvider amtsystem -Root "\" –ComputerName vproclient.vprodemo.com -Credential $myPScredential

If your AMT client is configured in TLS mode (TLS encrypted traffic over AMT Port 16993), add the –TLS switch to the command.

Type **Get-PSDrive** to list the available drives
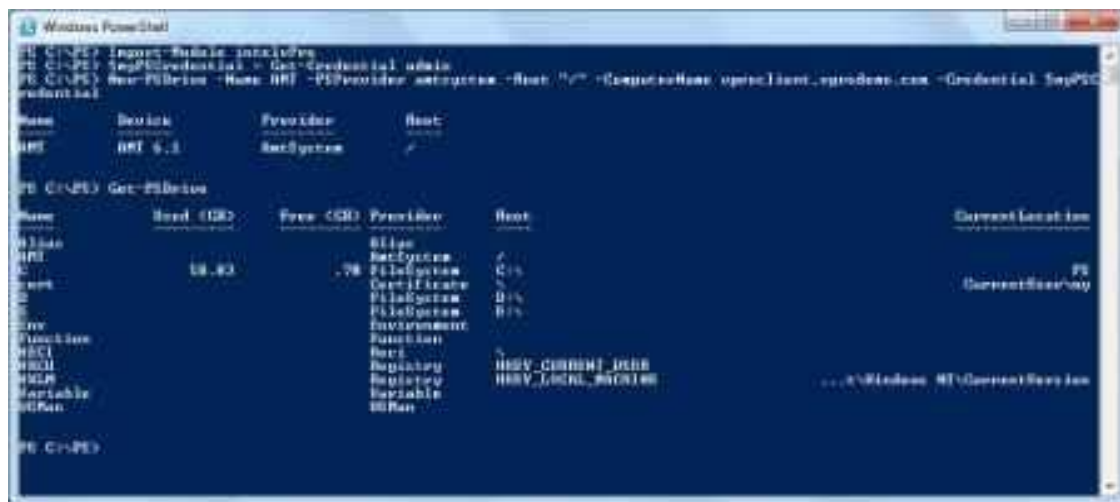
Now that the AMT PowerShell Drive is mapped, browse and navigate the remote system in a similar fashion as a normal file system drive:
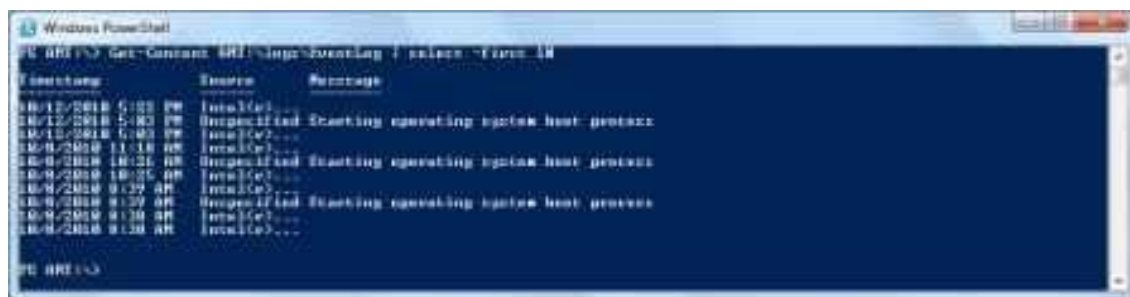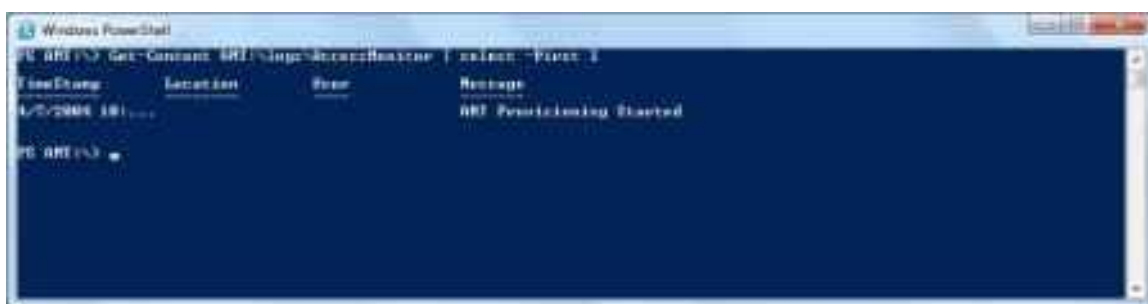
cd AMT:

dir
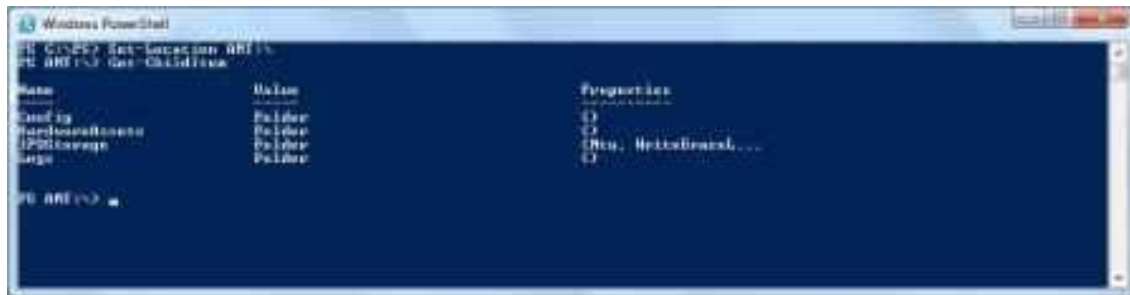
What can be done with this newly mapped drive? To display the AMT Event log:

Get-Content AMT:\logs\EventLog

And the same for the AMT Access Monitor (Audit Log):

Get-Content AMT:\logs\AccessMonitor

We can enumerate the system Hardware Inventory and dump the data to a file for auditing purposes:

Get-ChildItem -Recurse AMT:\HardwareAssets | Out-File C:\PS\HWInv.txt

If that is too much info focus on the BIOS items only:
Get-ChildItem -Recurse AMT:\HardwareAssets\BIOS

To turn IDE-R on:
Set-Item AMT:\Config\Redirection\IderEnabled -value "True"

To turn KVM User consent off:
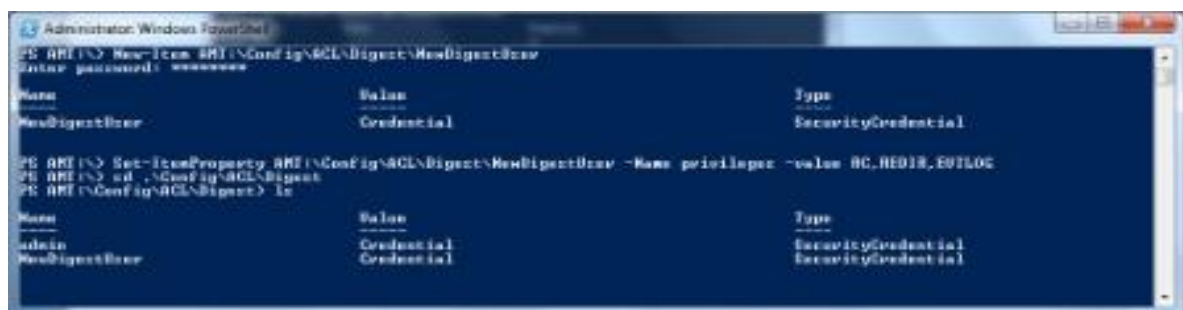**Set-Item AMT:\Config\KVM\UserConsent -value "False"**

To change the AMT hostname:
Set-Item AMT:\Config\etc\Hosts\HostName "NewHostName"

Add a new user and give them rights:
New-Item AMT:\Config\ACL\Digest\NewDigestUser -Password P@ssw0rd
Set-ItemProperty AMT:\Config\ACL\Digest\NewDigestUser -Name Privileges -Value RC,REDIR,EVTLOG
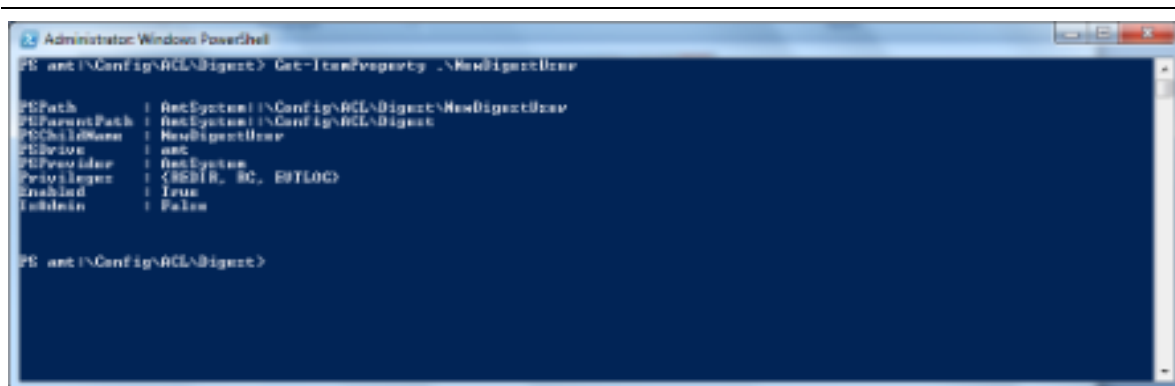
Check the properties of the newly added user:
Get-ItemProperty NewDigestUser

A   Appendix A: QuickStart Guide

This appendix provides minimal information to quickly install setup and use the Intel vPro Technology Module for Microsoft Windows PowerShell.

A.1   Download the Module

Download the latest version of the module from www.intel.com/go/powershell

A.2   Install the Module

Start setup.exe for the version of windows you are running.

NOTE

The installer must be run from an account with administrative rights.

A.3   Set Execution Level

Open a PowerShell console as an administrator and type
   Set-ExecutionPolicy RemoteSigned

A.4   Set Credentials

In the PowerShell console type
   $AMTCred = get-credential

A.5   Run Cmdlets

Now use cmdlets to manage the Intel vPro technology enabled client.
   Get-AMTPowerState "ComputerName" –Credential $AMTCred
   Invoke-AMTPowerManagement "ComputerName" –Credential $AMTCred – Operation PowerOn
   Invoke-AMTGUI "ComputerName" –Credential $AMTCred

B Appendix B: General Cmdlet and Function Methodology

This appendix provides further information on the methodology used in developing the cmdlets and functions for the Windows PowerShell Module for Intel vPro Technology.

B.1 Verb-Noun Pair Compliance

The Windows PowerShell Module for Intel vPro Technology actively complies with Windows PowerShell verb-noun pair convention for the names of cmdlets and functions. The verb part of the name identifies the action that the cmdlets and functions perform. The noun part of the name identifies the entity on which the action is performed. For more information on the Windows PowerShell verb-noun methodology, please visit the following link.

http://msdn.microsoft.com/en-us/library/ms714428(VS.85).aspx

B.2 Cmdlet and Function Parameters

With every Windows PowerShell Module for Intel vPro Technology cmdlets and functions, there is a consistent set of parameters that all the cmdlets use.

Table 2: Cmdlet and Function Parameters

Parameter	Description	Positional Input	Pipeline Input	Required
ComputerName	Managed Client hostname, FQDN, IP address, or array of the previous	Yes	ByValue, ByPropertyName	True
TLS	Switch to specify if TLS should be used to communicate with the client. 16992 for non-TLS, 16993 for TLS. Default is 16992 if TLS is not specified.	No	ByPropertyName	False
Username	Digest or Kerberos User to authenticate with	No	ByPropertyName	False
Password	Password for Digest	No	ByPropertyName	False

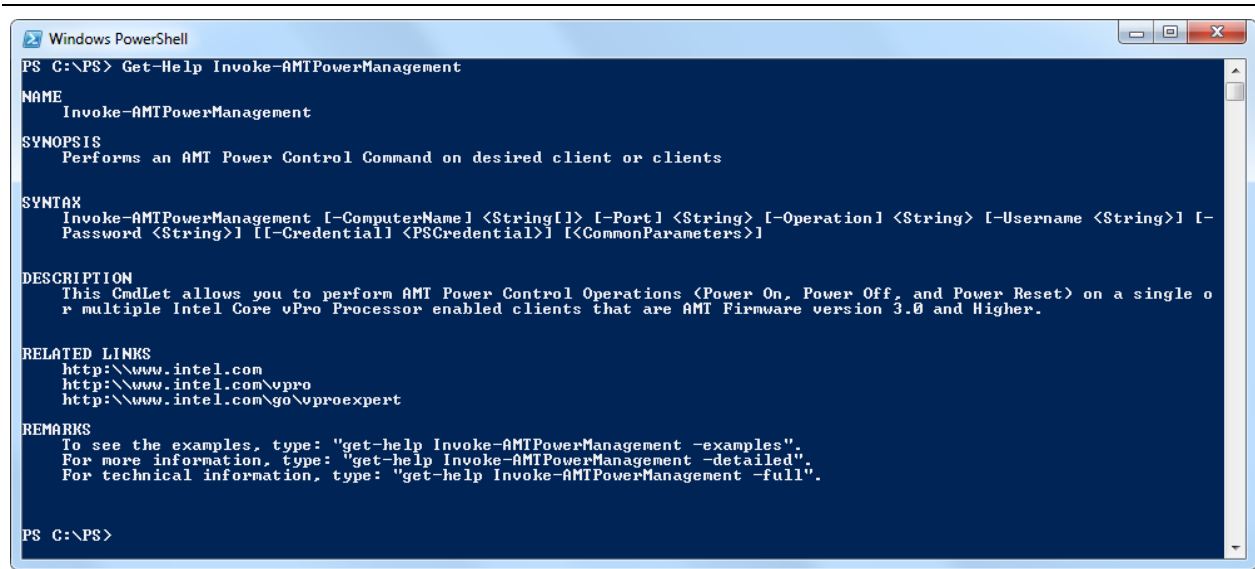|	or Kerberos User			
Credential	Preferred mechanism for authentication using PS-Credential	Yes	ByPropertyName	False

Although it may not exist in every cmdlet and function the following parameters are consistently used:

Parameter	Description	Positional Input	Pipeline Input	Required
Operation	Typically a sub operation of the cmdlets or functions	Yes	ByPropertyName	True

The Windows PowerShell Get-Help command can be used on the desired cmdlets and functions show any additional parameters that may be optional or required.

B.3   Cmdlets and Functions Integrated Help

Each Windows PowerShell Intel vPro Module cmdlet and function support the **Get-Help** command. Example use of the Get-Help command is the following:


```
Windows PowerShell

PS C:\PS> Get-Help Invoke-AMTPowerManagement

NAME
    Invoke-AMTPowerManagement

SYNOPSIS
    Performs an AMT Power Control Command on desired client or clients

SYNTAX
    Invoke-AMTPowerManagement [-ComputerName] <String[]> [-Port] <String> [-Operation] <String> [-Username <String>] [-
    Password <String>] [[-Credential] <PSCredential>] [<CommonParameters>]

DESCRIPTION
    This CmdLet allows you to perform AMT Power Control Operations (Power On, Power Off, and Power Reset) on a single o
    r multiple Intel Core vPro Processor enabled clients that are AMT Firmware version 3.0 and Higher.

RELATED LINKS
    http:\\www.intel.com
    http:\\www.intel.com\vpro
    http:\\www.intel.com\go\vproexpert

REMARKS
    To see the examples, type: "get-help Invoke-AMTPowerManagement -examples".
    For more information, type: "get-help Invoke-AMTPowerManagement -detailed".
    For technical information, type: "get-help Invoke-AMTPowerManagement -full".


PS C:\PS>
```

Figure 3: Module Help

By using the **Full**, **Detailed**, and **Examples** parameters with Get-Help more detailed information on the cmdlet and function and how to use it is provided.