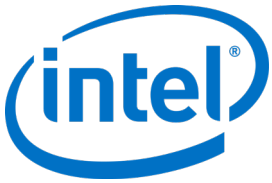


Intel® Manageability Commander (Intel® MC)

User Guide

Intel® MC Version 2.1

April 2020

Legal Disclaimer

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses. Check with your system manufacturer or retailer or learn more at http://www.intel.com/technology/vpro.

Intel, Intel vPro, Intel AMT, Intel EMA, and the Intel logo, are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Contents

1 Introduction 1

2 Installing and Uninstalling 2

2.1 Microsoft* SCCM Integration 3
2.2 Uninstallation 3

3 Migrating Data from Intel® MC 1.0 4

3.1 Exporting Computers from Intel® MC 1.0 4
3.2 Importing Computers into Intel® MC 2.0 and later 4

4 Managing Your Computers 5

4.1 Adding Systems 5
4.2 System Status 6
4.2.1 Remote Secure Erase 6
4.3 Remote Desktop 6
4.4 Serial-over-LAN (SOL) 7
4.5 Network Settings 8
4.6 Security Settings 8
4.7 User Accounts 8
4.8 Alarm Clocks 8
4.9 Event Log 9
4.10 Audit Log 10
4.11 Hardware Information 10
4.12 System Power 10
4.13 Storage Redirection 11

5 Command Line Support 12

6 Certificate Checking 13

6.1 Support for Isolated Networks 13

7 Troubleshooting 14

1 Introduction

Intel® Manageability Commander (Intel® MC) is a lightweight console used to connect with and utilize the features of Intel® Active Management Technology (Intel® AMT). Through this software, users will be able to connect to activated Intel® AMT devices and perform functions such as power control, remote desktop, hardware inventory, remote terminal, and more.

Additionally, this software will integrate with Microsoft* System Center Configuration Manager (SCCM) version 1511 and later. When deployment wake events are triggered in SCCM, Intel® MC will also attempt to perform an Intel® AMT power-on action. You can manually power on collections in SCCM by right-clicking them in Intel® MC.

You can also launch Intel® MC on a per-system basis by right-clicking the specific system in SCCM. The resulting context menu lets you use Intel® MC to remotely power on supported Intel® AMT client systems directly from SCCM.

2 Installing and Uninstalling

As a stand-alone application, Intel® MC can be installed on the following operating systems:

- Microsoft* Windows* 7
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows Server* 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

To install Intel® MC:

1. Download the latest Intel® MC installer package from the Download Center at http://downloadcenter.intel.com.
2. Double-click the download file to open it, then double-click **IMCInstaller<*version*>.msi** to launch the Intel® MC installer.
3. Accept the license agreement.
4. If you are installing Intel® MC on a system on which Microsoft* SCCM is installed, the installer automatically adds the Microsoft SCCM Console Extension subcomponent to the installation (see Section 2.1, Microsoft* SCCM Integration).
5. Click **Install** to install Intel® MC (and the Microsoft SCCM Console Extension if applicable). Although the Intel® MC installer supports installing to different location, it is recommended to use the default location for security reasons.
6. Follow the installer prompts, then click **Finish** to complete the Intel® MC installation.
7. Once the Intel® MC installation completes, follow the steps below to install the required **electron** subcomponent. Note that the Intel® MC desktop icon and start menu shortcut will not work until electron is installed.

To install electron (required):

Note: Intel® MC is tested and verified only with version 8.0.3 of electron (for Win32 and IA32). Use this version for both 32 bit and 64 bit platforms. Other versions of electron are not tested or supported.

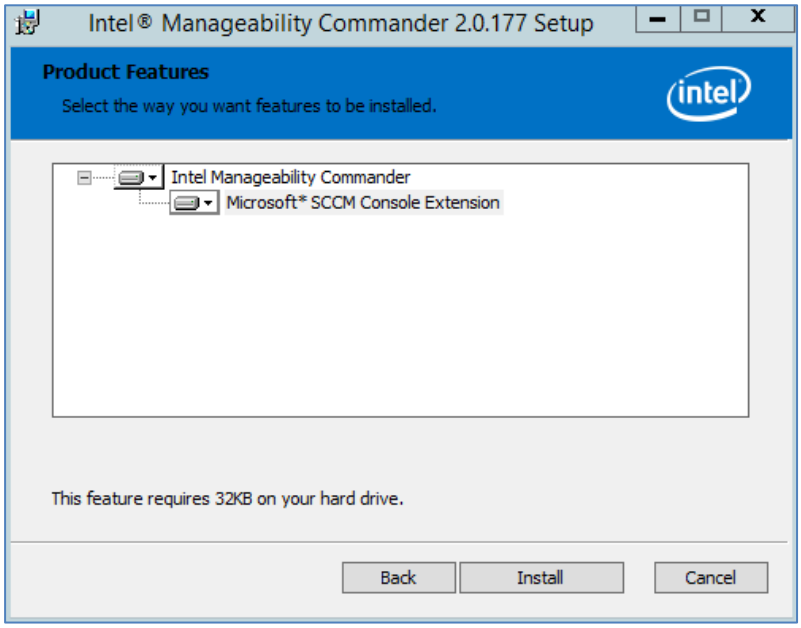
1. In a web browser, go to https://github.com/electron/electron/releases/tag/v8.0.3.
2. Scroll down and select **electron-v8.0.3-win32-ia32.zip** (see note above). The file is downloaded to your system.
3. Open the zip file and copy all files and subfolders to your Intel® MC installation folder (by default this is **c:/Program Files (x86)/Intel/Intel Manageability Commander**). Now the Intel® MC desktop icon and start menu shortcut will work.

To launch Intel® MC:

Once you finished installing Intel® MC and electron, use the Intel® MC desktop icon or start menu shortcut to launch Intel® MC.

2.1 Microsoft* SCCM Integration

When installing Intel® MC as a plug-in to Microsoft* SCCM, during installation, the following installer panel appears:



Selecting the "Microsoft* SCCM Console Extension" will install Intel® MC on the local system and will add the right-click context menus into the Microsoft* SCCM console. This extension can be installed anywhere that the Microsoft* SCCM console is installed to enable Intel® MC to launch directly from Microsoft* SCCM.

If Microsoft* SCCM is configured to support Partner Notifications, then the Intel® MC Microsoft* SCCM Console Extension will also install a service that will watch for changes to the partner notification files that are modified when a Microsoft* SCCM-scheduled task executes Wake-on-LAN. This component can be selected only when Intel® MC is installed on a Microsoft* SCCM primary site, and when Wake-on-LAN is enabled for scheduled tasks.

Once installation of Intel® MC has been completed on a Microsoft* SCCM primary site, the SMS_EXECUTIVE service must be restarted so that Intel® MC features will show up in Microsoft* SCCM. Additionally, if the Microsoft* SCCM console was open during Intel® MC installation, then the Microsoft* SCCM console will need to be closed and re-opened.

2.2 Uninstallation

To remove Intel® MC, go to **Settings, Apps & features**. Find **Intel® Manageability Commander** in the list of installed programs. Click **Intel® Manageability Commander**, then click the **Uninstall** option.

3 Migrating Data from Intel® MC 1.0

Note: The computer list must be exported from Intel® MC 1.0 before Intel® MC 2.x is installed. Once version 2.x is installed, the data from Intel® MC 1.0 will not be accessible from version 2.x.

Intel® MC 1.0 supports exporting the list of computers that it knows about, so that the connection information can be used on a different installation of Intel® MC. To protect this information, Intel® MC 1.0 requires the file to be encrypted prior to exporting.

3.1 Exporting Computers from Intel® MC 1.0

When you select **Save Computers** from the **File** menu, a dialog box prompts you for a password and location to save the exported connection information in a file.

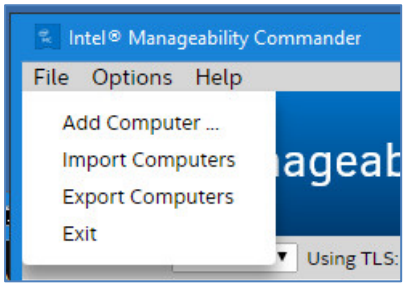
The password requirements are as follows:

- Must be least 8 characters long
- Must contain at least 1 upper case character
- Must contain at least 1 number
- Must contain at least 1 special character
- Cannot contain any Unicode characters

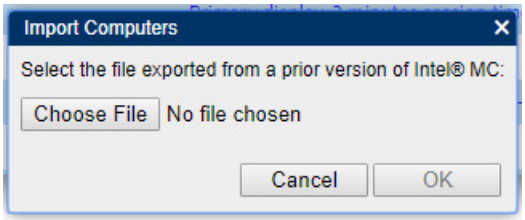
The exported computer list is saved as an .imc file.

3.2 Importing Computers into Intel® MC 2.0 and later

To import the list of computers, select **Import Computers** from the **File** menu.



In the resulting dialog box, choose the .imc file that you want to load, type in the correct password if prompted, and click **OK**.



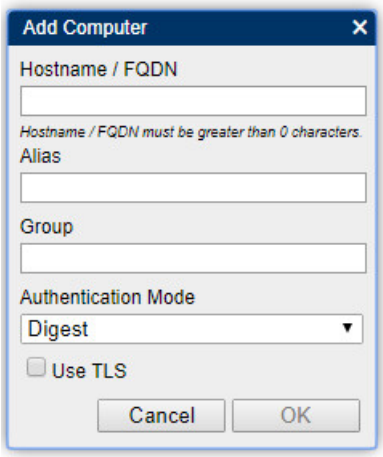
The list of computers will be imported.

4 Managing Your Computers

This section describes how to manage your computers with Intel® Manageability Commander.

4.1 Adding Systems

When Intel® MC is first launched, no systems are listed in the user interface. To add a new system, from the **File** menu, select **Add Computer**. A dialog box appears and prompts you for system-specific connection information.



Hostname/FQDN: The **Hostname** is required and is how Intel® MC finds the system. This can either be a fully-qualified domain name (FQDN), a simple hostname (with no domain), or an IP address. If transport layer security (TLS) is used to secure the connection, then the FQDN must be specified for the certificate verification to succeed. This version of Intel® MC supports TLS version 1.1 and later only. If the target Intel® AMT client system is configured to use TLS v1.0, then the connection attempt will fail with a "Timeout error," as a secure connection could not be established with Intel® MC.

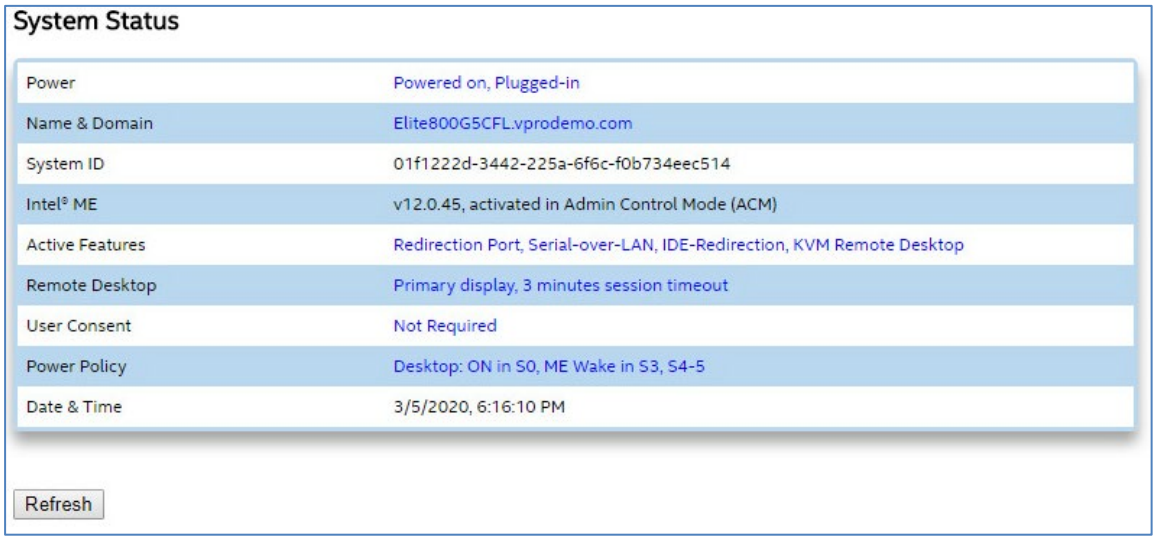
Alias: The **Alias** field can be any text and is not required. The **Alias** is the name that will be shown in the interface if it is populated. If no Alias is defined, the **Hostname** will be displayed.

Group: The **Group** field can be any text and is not required. It can be used to group systems together under a group name.

Authentication Mode: The **Authentication Mode** field specifies the type of security used to connect to the Intel® AMT system. The software supports both Digest and Kerberos authentication methods. For Digest, a system-specific Intel® AMT user name and password must be supplied to authenticate to the Intel® AMT system.

4.2 System Status

The System Status screen displays various information about the currently connected system.



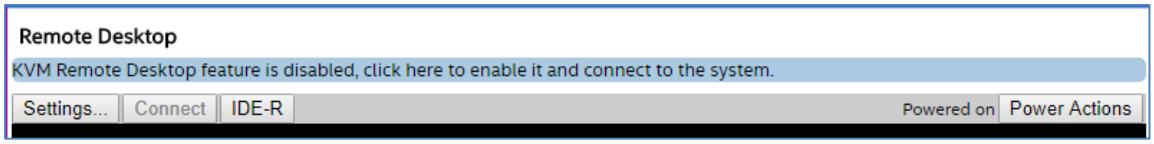
4.2.1 Remote Secure Erase

Remote Secure Erase allows you to remotely erase the hard drive on a managed system. Follow instructions and prompts on this screen.

4.3 Remote Desktop

This feature utilizes the hardware keyboard, video, mouse capability of Intel® AMT to provide out-of-band remote control of the device. The Remote Desktop page also lets you to control power actions, boot to remote boot devices, optimize the KVM connection settings, and adjust the viewing window size.

If there are features of Intel® AMT that are currently disabled and prevent Remote Desktop from functioning, a warning message will appear.



Click this message to view and change the settings as required to make the Remote Desktop function properly

The Remote Desktop feature requires that both the "Redirection Port" and "KVM Remote Desktop" features be enabled.

The following settings available on this window control how the Remote Desktop session is managed.

Settings	• **Image Encoding:** Sets the remote desktop display (from highest compression to lowest): RLE8, RLE16, RAW8, RAW16. These compression settings can be changed from the "Settings" button on the Remote Desktop page if the session cannot be established with the remote device or if the display is slow to update. For example, if the remote desktop is using a high display resolution with a high color depth, then changing these Remote Desktop

	"Image Encoding" setting could produce a better experience. • **Show Local Mouse Cursor:** Causes the local mouse cursor – of the system where Intel® MC is running – to display on top of the Remote Desktop window. You will see both the local and remote mouse cursor in the window. You may choose to hide the local mouse cursor if there is latency between their respective movements on the display or if the mapping is not one-to-one. • **Limit Frame Rate:** reduces the refresh rate of the remote image display, which can be useful if there is insufficient network bandwidth to smoothly show the remote desktop display.
Connect/Disconnect	Connects to the current system for remote desktop access. Use **Disconnect** to disconnect.
IDE-R	See Section 4.13, Storage Redirection later in this document.
Ctrl-Alt-Del	Sends the three-button keyboard combination to the remote system. If this keyboard combination were physically pressed, then the local system would capture this input instead of the intended remote device.
Primary display	Drop-down list of the active display devices of the remote system. This can be "Primary display", "Secondary display", or "3rd display". Changing this selection will change which of the remote device's displays are shown in the Remote Desktop window.
Focus Off	Drop-down list that controls what area of the remote display is updated. The "Focus Off" option forces the entire desktop area to be updated with every frame that transmitted from the remote device. The "Large Focus" and "Small Focus" can be used where there is limited network bandwidth or high latency to force only the area around the mouse cursor – large or small area, respectively – to be updated instead of the whole desktop area.
Full Screen	The Remote Desktop feature also provides support for full screen and display rotation from buttons at the bottom of this window

4.4 Serial-over-LAN (SOL)

Serial-over-LAN (SOL) allows the serial character stream of the serial port to be redirected over a LAN connection. This is useful in enabling console redirection for the BIOS and EFI, as well as the operating system (text based) on remotely managed systems.

Connect	Connect to the remote system.

Power Actions	Displays dialog to perform power actions (power up, power down, sleep, etc.) on the remote system.
IDE-R	See Section 4.13, Storage Redirection.
Start Capture	Records all data sent and received to a binary file on disk. This can be useful for diagnostic or auditing purposes after the session has been terminated
Bottom row buttons	Send these controls to the remote system.

4.5 Network Settings

The Network Settings page allows you to see and modify the network settings of Intel® AMT. This page lists all Intel® AMT-capable network interfaces on the device. If the device has a wireless interface, you can add wireless profiles to Intel® AMT so that when the operating system of the device is offline, Intel® AMT can connect to the network using the wireless interface. Intel® AMT supports multiple wireless profiles.

Editable settings are shown in blue. To change an editable setting, do the following:

1. Click the setting value, shown in blue.
2. In the dialog displayed, select the desired value for the setting and click **OK**.

4.6 Security Settings

The Security Settings page allows you to manage the Intel® AMT certificates for this computer. Use the **Add** button to apply an existing local Intel® AMT certificate (from a file on disk) to the remote computer.

Note: Intel® MC does not support creating new certificates.

4.7 User Accounts

The User Accounts page lets you add multiple user accounts to Intel® AMT. Only digest accounts are supported through Intel® MC. Each account can be assigned one or more Intel® AMT realms to allow for fine-grained permission handling.

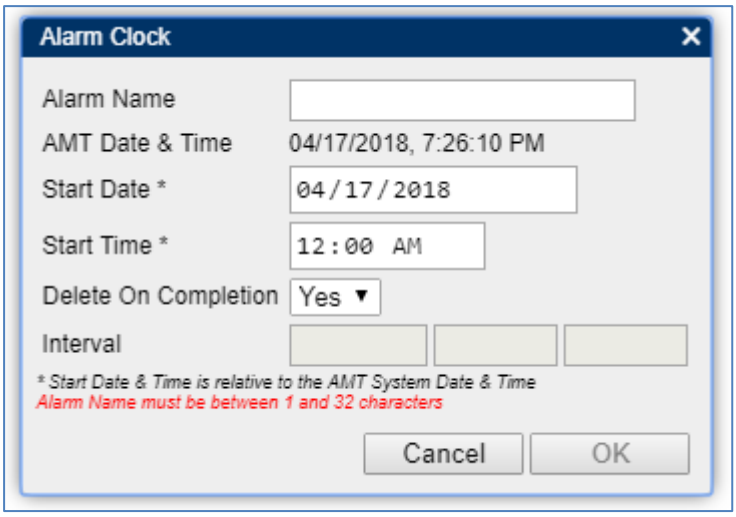
Right-click on a user account to edit, delete, enable, or disable it. If you don't have permission to do some or any of these modifications for a user account, those options will not be available. A maximum of 13 user accounts can be added to a system; once the user accounts count reaches 13, the **Add Account** button becomes disabled.

4.8 Alarm Clocks

The Alarm Clocks page lets you set alarm clocks on the target system for waking up the system at a specific time or time intervals. The Alarm Clock page displays currently active alarms with name and activation time, or displays "No Alarm Clocks are present" if there are no active alarms on the target Intel® AMT system. You can add up to five alarm clocks per target system.

To add an alarm clock:

1. Click **Add Alarm** button on the Alarm Clocks page.
2. Enter or select all required values on the **Alarm Clock** dialog.
3. Click **OK**.



To delete an alarm clock, right-click on the specific alarm clock and select **Delete** from the resulting menu.

4.9 Event Log

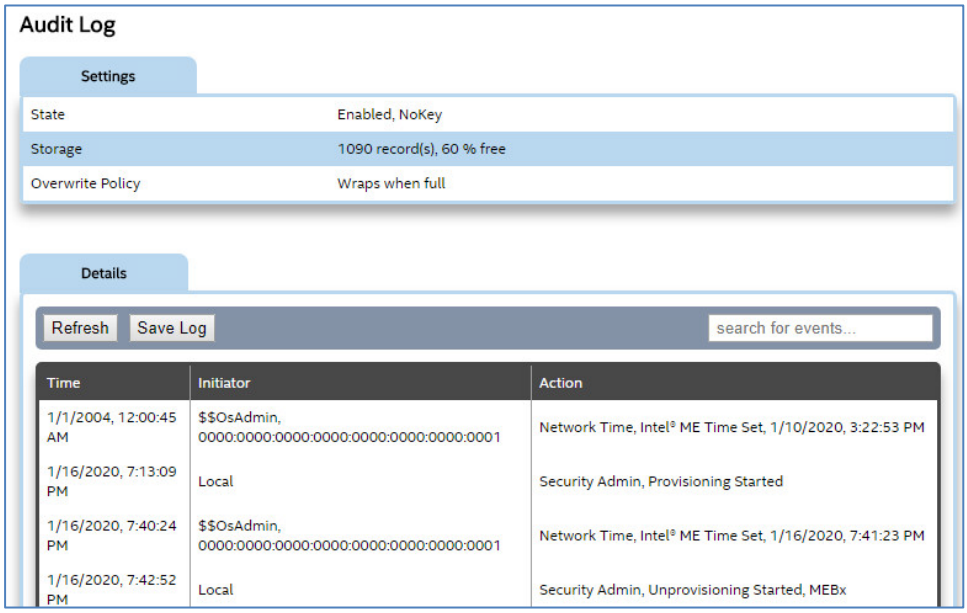
The Event Log shows all Intel® AMT events of the system you are connected to.

Refresh	Refresh the log display.
Clear Log	Clear the current log display.
Save Log	Save the current log display to file.
Freeze Log	Freeze the log so that the entry you are looking at does not scroll off the screen
Search for events	Filter which events are shown on the page by typing in keywords.

4.10 Audit Log

The Audit Log page allows you to review changes that other users have made to the Intel® AMT policy. The **Settings** tab is automatically populated when you select **Audit Log** from the navigation pane at left.

To view the actual Audit Log records, click on **Click here to load the audit log** under **Details** (this can take a little while to load).



Refresh	Refresh the log display.
Save Log	Save the current log display to file.
Search for events	Filter which events are shown on the page by typing in keywords.

Note: This version of Intel® MC does not support enabling the Audit Log feature of the remote Intel® AMT device. It only supports the viewing of the Audit Log entries.

4.11 Hardware Information

The Hardware Information page provides a list of hardware that Intel® AMT has access to read from the BIOS. This includes information about the OEM platform, baseboard, BIOS, processors, and storage media, including USB drives.

4.12 System Power

System power is available from the Remote Desktop page and the Serial Over LAN page. It is not a menu choice in the navigation pane at left.

To change system power settings:

1. Select either **Remote Desktop** or **Serial Over LAN** from the navigation pane at left.
2. Click the **Power Actions** button.
3. From the **PowerCommand** drop-down list, select the desired power action (power up, power down, sleep, hibernate, etc.). If you select **Only Show Valid Commands**, only power commands that are

valid based on the current system's power state are displayed. This can take a little time for Intel® MC to query the remote system's Intel® AMT.

4. Click **OK**.

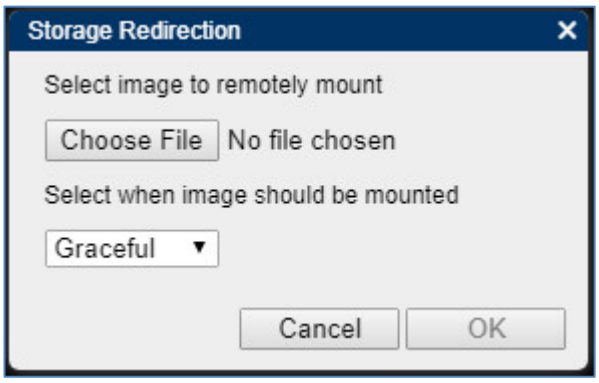
4.13 Storage Redirection

Storage Redirection is available from the Remote Desktop page and the Serial Over LAN page. It is not a menu choice in the navigation pane at left.

The Storage Redirection feature enables mounting CD-ROM (.iso) and floppy (.img) images remotely to the target Intel® AMT system. In order to use this feature, both the "Redirection Port" and "IDE-Redirection" features must be enabled on the remote device, which can be accessed from the "System Status" page under "Active Features".

To start a storage redirection session:

1. Select **Remote Desktop** or **Serial Over LAN** from navigation pane at left.
2. Click **IDE-R**.
3. In the **Storage Redirection** dialog box select a valid image and click **OK**.



After mounting an image, you can boot into the image. Options to boot and reset to remote images appear in the **Power Command** dialog box when a storage redirection session is active.

5 Command Line Support

The following table lists the command line switches supported by Intel® MC.

Option	Description
`--help`	Shows this help information.
`-r, --reset`	Removes all stored application data and settings, thus resetting the application state.
`-h, --hostname=`*`HOST`*	Specifies the FQDN of the remote system to immediately connect. A new system will be added to the list of managed systems if it does not already exist'
`-u, --username=`*`USER`*	The user name to use for Digest authentication with the remote system.
`-p, --password=`*`PASS`*	Password for the Digest authentication user account.
`-k, --kerberos`	Specifies the use of Kerberos for authentication with the remote system. This option is only used when the system specified with -h does not already exist in the list of managed systems and a new one is being created.
`-t, --tls`	Specifies the use of TLS for the connection. This option is only used when the system specified with -h does not already exist in the list of managed systems and a new one is being created.

To connect to a system using Digest authentication without TLS:

```
imc.exe --hostname=testSystem.demo.com --username=admin --password=P@ssw0rd
```

To connect to a system using Kerberos and TLS:

```
imc.exe --hostname=testSystem.demo.com –kerberos --tls
```

The Microsoft* SCCM extension uses these command line switches to automate launching Intel® MC for the targeted Intel® AMT system. In addition, the Intel® MC Microsoft* SCCM extension with Partner Notification support uses a special command line switch for passing the file that contains the list of systems to remotely power on: '**`--s0List=`*`FILEPATH`***'. This file is a JSON-formatted file that contains the FQDNs to use for the remote power on operation.

This version of Intel® MC also provides support for importing the list of computers that Intel® Setup and Configuration Service (Intel® SCS), version 12 and later, manages. Intel® SCS will export a list of computers to a JSON file that is then passed on to Intel® MC via the "**`-list:<`*`filepath`*`>`**" command line switch. Intel® MC will then read this JSON file and create representative computer objects that can be used with the 1:1 usages provided by Intel® MC.

6 Certificate Checking

Intel® MC automatically verifies that certificates, used in TLS, chain down to a root in the Windows Computer Account Trusted Root certificate store of the machine from which it is run. Additionally, the Intel® MC will verify that the DNS name or Subject Name in the certificate matches the host name of the Intel® AMT device. Just like in web browsers, the machine will automatically connect and display a lock indicating that the connection is secured via TLS. If the certificate cannot chain to a root in the certificate store, then Intel® MC will reject the connection and display an appropriate error message.

6.1 Support for Isolated Networks

As part of the TLS certificate chain verification process, Intel® MC will attempt to pull the latest certificate revocation lists (CRLs) from various distribution points (CDP). However, in many enterprise network environments the management console is contained within a DMZ but certificates in the TLS chain are from external CAs.

In this scenario, the TLS connection establishment will timeout with an error before Intel® MC is able to fully validate the TLS certificate chain. This is because the system running Intel® MC is unable to reach the CRL CDPs in a timely manner. There are two (2) workarounds available for this scenario:

1. Create a CRL CDP in the DMZ. Specifics on how to do this are outside the scope of this user guide. However, the following are online resources that should be helpful:
    - https://blogs.technet.microsoft.com/nexthop/2012/12/17/updated-creating-a-certificate-revocation-list-distribution-point-for-your-internal-certification-authority/
    - https://techcommunity.microsoft.com/t5/Configuration-Manager-Archive/How-to-Publish-the-CRL-on-a-Separate-Web-Server/ba-p/272748
2. Launch Intel® MC will the command line switch '**`--limitcrl`**'. This will limit the time Intel® MC waits for retrieving the CRLs from unreachable CDPs.
    - This flag does not persist across Intel® MC usages. By default, Intel® MC will not place any time limits on connecting to CRL CDPs.
    - You will need to use this flag each time you want to launch Intel® MC for usages within an isolated network environment.

7 Troubleshooting

To troubleshoot common issues with Intel® MC, please see the support articles located at

> http://www.intel.com/content/www/us/en/support/software/manageability-products/intel-manageability-commander.html

For a reference to Intel® AMT and the Intel® AMT SDK, please go to the following link:

> https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm