Legal Disclaimer

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. Check with your system manufacturer or retailer or learn more at intel.com/AMT.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel® Active Management Technology requires activation and a system with a corporate network connection, an Intel Active Management Technology-enabled chipset, and network hardware and software. For notebooks, Intel Active Management Technology may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit intel.com/AMT.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

© 2018 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, and Intel vPro are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

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

Intel® Manageability Commander 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® Manageability Commander 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® Manageability Commander.

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

An exported computer list from Intel® Manageability Commander 1.0 can be imported into Intel® Manageability Commander 2.0.
2 Migrating Data from IMC 1.0

<table>
<thead>
<tr>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The computer list must be exported from Intel® Manageability Commander 1.0 before Intel® Manageability Commander 2.0 is installed. Once version 2.0 is installed, the data from Intel® Manageability Commander 1.0 will not be accessible from version 2.0.</td>
</tr>
</tbody>
</table>

Intel® Manageability Commander 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® Manageability Commander. To protect this information, Intel® Manageability Commander 1.0 requires the file to be encrypted prior to exporting.

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:
- Is at least 8 characters long
- Contains at least 1 upper case character
- Contains at least 1 number
- Contains at least 1 special character
- Cannot contain any Unicode characters

The exported computer list is saved as an .imc file.
To import the list of computers into Intel® Manageability Commander 2.0, select **Import Computers** from the **File** menu.

```
File   Options   Help
       Add Computer ...
       Import Computers
       Exit
```

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

![Import Computers dialog box]

The list of computers will be imported.
3 Installing/Uninstalling

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

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

3.1 Microsoft® SCCM Integration

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

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

If Microsoft® SCCM is configured to support Partner Notifications, then the Intel® Manageability Commander Microsoft® SCCM Console Extension will also install a service that will watch for changes to the partner notification files that are modified when an SCCM-scheduled task executes wake-on-LAN. This component can be selected only when Intel® Manageability Commander is installed on a SCCM primary site, and when wake-on-LAN is enabled for scheduled tasks.
Once installation of Intel® Manageability Commander has been completed on a Microsoft® SCCM primary site, the SMS_EXECUTIVE service must be restarted so that Intel® Manageability Commander features will show up in Microsoft® SCCM. Additionally, if the Microsoft® SCCM console was open during Intel® Manageability Commander installation, then the Microsoft® SCCM console will need to be closed and re-opened.

3.2 Uninstallation

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

This section describes the product features included with Intel® Manageability Commander.

4.1 Adding Systems

When Intel® Manageability Commander is first launched, there won't be any systems 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.

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.

The Hostname is required, and is how Intel® Manageability Commander 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® Manageability Commander 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® Manageability Commander.

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. It also supports both TLS and Non-TLS connection encryption. 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

This page of Intel® Manageability Commander shows an overview of the Intel® AMT settings on the device, and lets you change some of these settings, and perform power control changes. Any setting that is shown in blue on this page can be clicked to change that setting. This textual indication for setting changes is used throughout the user interface.
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.

4.4 Storage Redirection

The Storage Redirection feature enables mounting CD-ROM (.iso) and floppy (.img) images remotely to the target Intel® AMT system.

To start a storage redirection session, open the Storage Redirection dialog box, located on the remote desktop view, then select a valid image and click the OK button. A spinning progress icon will be visible on the remote desktop view while the redirection session is in progress.

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.
4.5 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.

![Intel® Manageability Commander](image)

This document and the information contained herein is proprietary and confidential and may not be duplicated, redistributed, or displayed to any other party without the expressed written permission of Intel®.
4.6 Event Log

The Event Log shows all Intel® AMT events. On this page, you can clear the log, save the log to a file, freeze the log so that the entry you are looking at doesn't scroll off the screen, and filter what events are shown on the page by typing in keywords.
4.7 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.
4.8 User Accounts

The User Accounts page lets you add multiple user accounts to Intel® AMT. Only digest accounts are supported through Intel® Manageability Commander. 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, or enable/disable it. If you don’t have permission to do some or any of these modifications for a particular user account, those options aren’t 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.
4.9 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.
To add an alarm, click the Add Alarm button on the Alarm Clocks page. An Alarm Clock dialog box appears.

![Alarm Clock Dialog Box](image)

You must provide all the required values to add an alarm clock to the system. If there are any issues with your settings or the Intel® AMT system, the dialog box will display an appropriate error message. You can add up to five alarm clocks per target system.

To delete an alarm clock, right-click on the specific alarm clock and select Delete from the resulting menu.
4.10 Remote Secure Erase

Intel® Remote Secure Erase allows you to erase all data from the SSD on a target PC.

![Remote Secure Erase Interface](image-url)
## 5 Command Line Support

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>Shows this help information</td>
</tr>
<tr>
<td>-r, --reset</td>
<td>Removes all stored application data and settings, thus resetting the application state</td>
</tr>
<tr>
<td>-h, --hostname=HOST</td>
<td>Specifies the FQDN of the remote system to immediately connect</td>
</tr>
<tr>
<td></td>
<td>A new system will be added to the list of managed systems if it does not already exist'</td>
</tr>
<tr>
<td>-u, --username=USER</td>
<td>The user name to use for Digest authentication with the remote system</td>
</tr>
<tr>
<td>-p, --password=PASS</td>
<td>Password for the Digest authtication user account'</td>
</tr>
<tr>
<td>-k, --kerberos</td>
<td>Specifies the use of Kerberos for authentication with the remote system</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>-t, --tls</td>
<td>Specifies the use of TLS for the connection</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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® Manageability Commander for the targeted Intel® AMT system. In addition, the Intel® Manageability Commander 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 document and the information contained herein is proprietary and confidential and may not be duplicated, redistributed, or displayed to any other party without the expressed written permission of Intel®.
This version of Intel® Manageability Commander 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® Manageability Commander via the “-list:<filepath>” command line switch. Intel® Manageability Commander will then read this JSON file and create representative computer objects that can be used with the 1:1 usages provided by Intel® Manageability Commander.
6 Certificate Checking

Intel® Manageability Commander 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® Manageability Commander 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® Manageability Commander will reject the connection and display an appropriate error message.
7 Troubleshooting

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


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