Legal Information

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A “Mission Critical Application” is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL’S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS’ FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENCE IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm.

This Intel® Manageability Commander (“Software”) is furnished under license and may only be used or copied in accordance with the terms of that license. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. The Software is subject to change without notice, and should not be construed as a commitment by Intel Corporation to market, license, sell or support any product or technology. Unless otherwise provided for in the license under which this Software is provided, the Software is provided AS IS, with no warranties of any kind, express or implied. Except as expressly permitted by the Software license, neither Intel Corporation nor its suppliers assumes any responsibility or liability for any errors or inaccuracies that may appear herein. Except as expressly permitted by the Software license, no part of the Software may be reproduced, stored in a retrieval system, transmitted in any form, or distributed by any means without the express written consent of Intel Corporation.

Intel, Intel vPro, and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.
Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

3rd Party marks and/or logos and copying should be respected.

* Other names and brands may be claimed as the property of others. Copyright © 2015-2016, Intel Corporation. All rights reserved.
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 to 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 SCCM deployment wake events are triggered in SCCM, Intel® Manageability Commander will also attempt to perform an Intel® AMT power on action. Collections in SCCM can be manually powered on using Intel® Manageability Commander using the collection right click context menu. Intel® Manageability Commander can be launched on a per system basis by using the right click system context menu to get access to all of the supported Intel® AMT features directly from SCCM.
2. Installing / Uninstalling


2.1 Microsoft* SCCM Integration

When installing Intel® Manageability Commander as a plug-in to Microsoft SCCM, during installation, the following screen will be presented.

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

The Intel® Manageability Commander SCCM wake service will install the Intel® Manageability Commander Partner Notification File Service that will watch for changes with the partner notification file that is modified when a SCCM scheduled task executes wake-on-LAN. This can only be checked when Intel® Manageability Commander is installed on a SCCM primary site and when wake-on-LAN is enabled for scheduled tasks. Additionally, a Kerberos user account that has rights to the “Remote Control” realm for Intel® AMT must be provided during the installation of the Intel® Manageability Commander Partner Notification File Service.

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.

2.2 Uninstallation

To remove Intel® Manageability Commander, go to Control Panel, Programs, Uninstall a program. Find Intel® Manageability Commander in the list of installed programs. Right mouse button click Intel® Manageability Commander and click the Uninstall option.
3. Product Features

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

3.1 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 either use the file menu to “Add Intel AMT Computer...” or right click in the middle of the interface to “Add Computer...”. A dialog box will appear and the system specific connection information will need to be filled in.

The Friendly Name field can be anything the user wants and is not required. The Friendly Name is the name that will be shown in the interface if it is populated.

The Group Tag currently just provides an area for metadata about the system and is not required to be filled in.

The Hostname is required to be filled in and is how Intel® Manageability Commander finds the system. This can either be a Fully Qualified Domain Name (FQDN) or an IP address.

The Auth / Security field tells Intel® Manageability Commander what security needs to be 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. For Kerberos, an Active Directory Token Request FQDN must be supplied. This FQDN is the name of the system that Active Directory knows. This can be different then the hostname. Additionally, the token request FQDN must be followed by the AMT port number in this format: <FQDN>:<Port Number>. For TLS, port 16993 must be used. For Non-TLS, port 16992 must be used.

3.2 System Status

This page of Intel® Manageability Commander shows an overview of the AMT settings on the device, the ability to change some of these settings, the ability to perform power control changes as well as run pre-defined ME Scripts. Any text that is shown in a blue color can be clicked on and used to change that setting. This textual indication for setting changes is used throughout the user interface.
3.3 Remote Desktop

This feature utilizes the hardware keyboard, video, mouse capability of Intel® AMT to provide out of band remote control of the device. If there are features of Intel® AMT that are currently disabled and would prevent Remote Desktop from functioning, a warning message will be displayed on the screen.

![Remote Desktop Warning Message]

Clicking this message will show the user which features are required to make KVM function properly and will allow the user to make the necessary changes.

The Remote Desktop page will also allow the user to control power actions, boot to remote boot devices, optimize the KVM connection settings, and adjust the viewing window size.

3.4 Serial-over-LAN

This feature allows the user to utilize a remote terminal console to AMT. This allows connectivity at the command line level to interact with the device. Similar to Remote Desktop, if there are features of Intel® AMT that are currently disabled and would prevent Serial-over-LAN from functioning, a warning message will be displayed on the screen.

![Serial-over-LAN Warning Message]

Clicking this message will show the user which features are required to make Serial-over-LAN function properly and will allow the user to make the necessary changes.
Serial-over-LAN will also allow the user to control power actions, boot to remote boot devices, adjust the ASCII and terminal types, and resolution. Additionally, there are buttons that will support the escape key, backspace key, cut, copy, and paste.

3.5 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, Processor(s), Memory Stick(s), and Storage Media. The Save button will allow a user to save the information to a file that contains the Hardware Information presented on this page.

3.6 Event Log
The Event Log shows all Intel® AMT events. On this page, you can clear the log, save the log off 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.

3.7 Audit Log
The Audit Log is a special log that allows users with the auditor permission for Intel® AMT to review changes that other users have made to the Intel® AMT policy. This page has similar functionality as the Event Log in that it allows users to save the log to a file, clear the log, and filter the log based on keywords.

3.8 Network Settings
The Network Settings page allows users to see and modify the network settings of Intel® AMT. This page will list all Intel® AMT capable network interfaces on the device. In addition to being able to change the settings of the different interfaces, if the device has a wireless interface, users can add wireless profiles to Intel® AMT so that when the operating system of the device is offline, Intel® AMT will be able to connect to the network using the wireless interface. Intel® AMT supports multiple wireless profiles.

3.9 Internet Settings
The Internet Settings page allows for Intel® AMT Client Initiated Remote Access (CIRA) to be configured. When setting Environment Detection, Intel® AMT will look at the DNS suffix of the network it is currently on, and if it is different than what is listed here, it will attempt to establish a CIRA connection to the Management Presence Server (MPS). Users can specify the settings for different connection types and can add the connection information for the MPS that they are using.

3.10 Security Settings
The Security Settings page allows for certificate management for Intel® AMT. A user can change the settings for the Remote and Local TLS certificates to enable TLS, Mutual TLS, or disable TLS. Additionally, users can add and issue certificates to be used for TLS.

3.11 System Defense
System Defense is a feature where a user can configure Intel® AMT to monitor or block some or all of the network traffic coming in over the wired interface without blocking access to Intel® AMT itself. In the case where the OS has become infected, the system can still be remotely access and repaired without impacting other systems on the network. Intel® Manageability Commander supports defining multiple system defense filters and policies and applying those policies individually to the device.

3.12 User Accounts
The User Accounts page allows multiple user accounts to be added 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 grain permission handling.
4. 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 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 display the cert to users to manually verify. Invalid TLS certificates will cause Intel® Manageability Commander to display a red text saying “Invalid TLS”.

4.1. SCCM Integration

In order to run the Microsoft SCCM console extensions and the Intel® Manageability Commander Partner Notification File Service using the –ignoretls command, the user is required to add the following key-value pair in the registry:

Under: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intel\Intel Manageability Commander\Setup:
• ignoreTls = 1

In order to run the Microsoft SCCM console extensions and the Intel® Manageability Commander Partner Notification File Service using the –debug command, the user is required to add the following key-value pair in the registry:

Under: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intel\Intel Manageability Commander\Setup:
• debugMode = 1

5. Exporting the Computer List

Intel® Manageability Commander 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 or backed up. Among other connection information, the AMT digest password is stored in this file. In order to protect this information, Intel® Manageability Commander requires the file to be encrypted prior to exporting. When a user clicks the file menu and save computers, a dialog box will be presented to the user to enter in a password and file path to save the exported connection information.

The password requirements are:
• Be at least 8 characters long
• Contains at least 1 upper case character
• Contains at least 1 lower case character
• Contains at least 1 number
• Contains at least 1 special character
• Cannot contain any Unicode characters

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

To import the list of computers into another installation of Intel® Manageability Commander, click the file menu and select load computers. Choose the .imc file that you want to load and enter in the correct password for the .imc file. The list of computers and the connection information will be added to Intel® Manageability Commander.

6. Troubleshooting

To troubleshoot common issues with Intel® Manageability Commander, please see the support articles located at:
http://www.intel.com/content/www/us/en/support/software/manageability-products/intel-manageability-
For a reference to Intel® AMT and the Intel® AMT SDK, please go to the following link: