# Intel vPro® Enablement

## User Guide

*November 2020*

*Intel Confidential*

Document Number: 633631-0.5

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

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

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

The products described 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.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

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 product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

No product or component can be absolutely secure.

Intel, the Intel logo, 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.

# Contents



# Figures



# Tables

# Revision History

| Date | Revision | Description |
|---|---|---|
| November 2020 | 0.5 | Initial release. |

§

# 1.0 Introduction

Intel® vPro Platform is the sum of hardware, BIOS extensions and applications that deliver solutions for a robust and reliable applications.

This doc will introduce how to enable Intel vPro® step by step.

## 1.1 Terminology

**Table 1. Terminology**

| Term | Description |
|---|---|
| BIOS | Basic Input Output System |
| TXT | Trusted Execution Technology |
| BVT | Brand Verification Tool |
| TPM | Total Productive Maintenance |

## 1.2 Reference Documents

**Table 2. Reference Documents**

| Document | Document No./Location |
|---|---|
| TPM 2 Provisioning Tool for Intel Trusted Execution Technology for the OEM | 563989 |

# 2.0 Intel vPro® Function Enablement

This chapter will introduce Intel vPro® function enablement steps, including Hardware configuration, BIOS/MEBx Configuration, Intel® TXT TPM Provisioning, BVT, and IOTG recommended remote management tools.

## 2.1 Hardware Configuration

- Intel® Core™ xxxx vPro™ processor supporting the following features:

  o Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture (Intel®
  VT-x)
  o Intel® VT for Directed I/O (Intel® VT-d)
  o Intel® Trusted Execution Technology (Intel® TXT)
  o Intel® Software Guard Extensions (Intel® SGX)

- Intel® xxxx chipset supporting the following features:

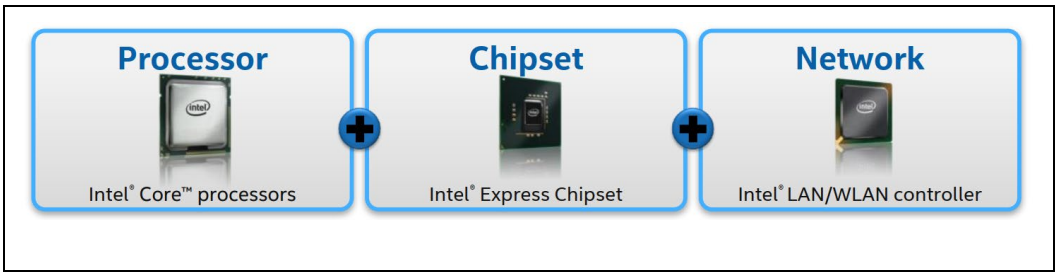
  o Intel® VT for Directed I/O (Intel® VT-d)
  o Intel® Trusted Execution Technology (Intel® TXT)

- Intel® Ethernet Connection I219-LM (Wired LAN is optional or required by vPro SKU)

- Wireless Network Adapters

- A discrete TPM 2.0 Trusted Platform Module (TPM) is required. The TPM must be provisioned for Intel® TXT
  and locked prior to final testing.

**Figure 1. Hardware Required Configuration**



## 2.2 MEBx Configuration

Press CTRL+P (/w Keyboard) during system cold boot or system reset, select MEBx login, 1st time login password is “admin” and changed to desired password.

Select Intel® AMT Configuration, set User Consent to “NONE”, select Active Network Access, then exit MEBx.

**Figure 2. User Consent**

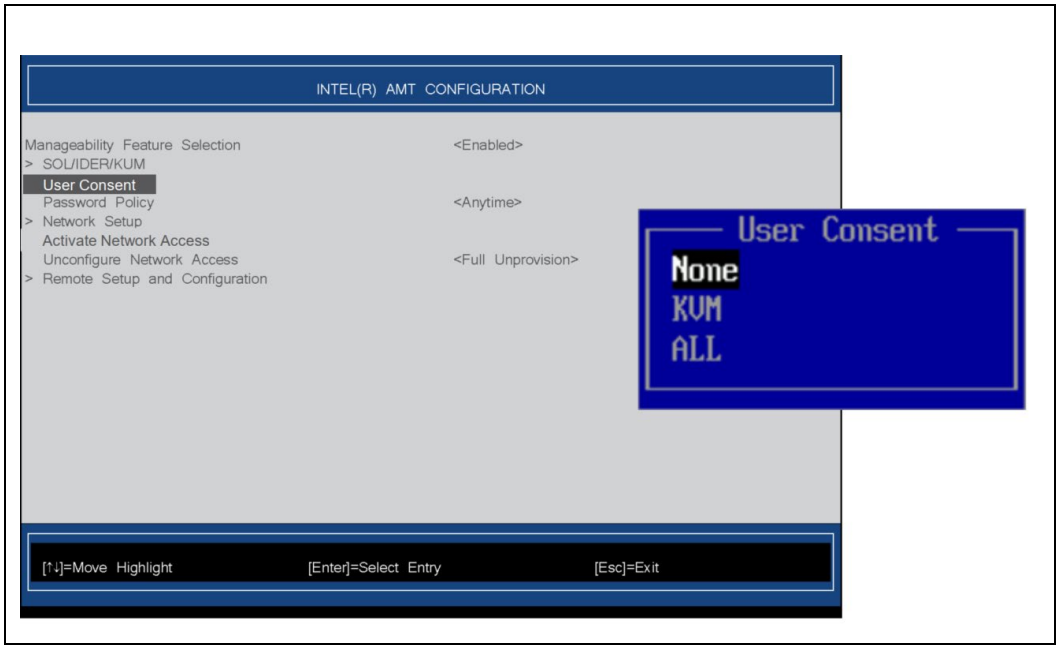
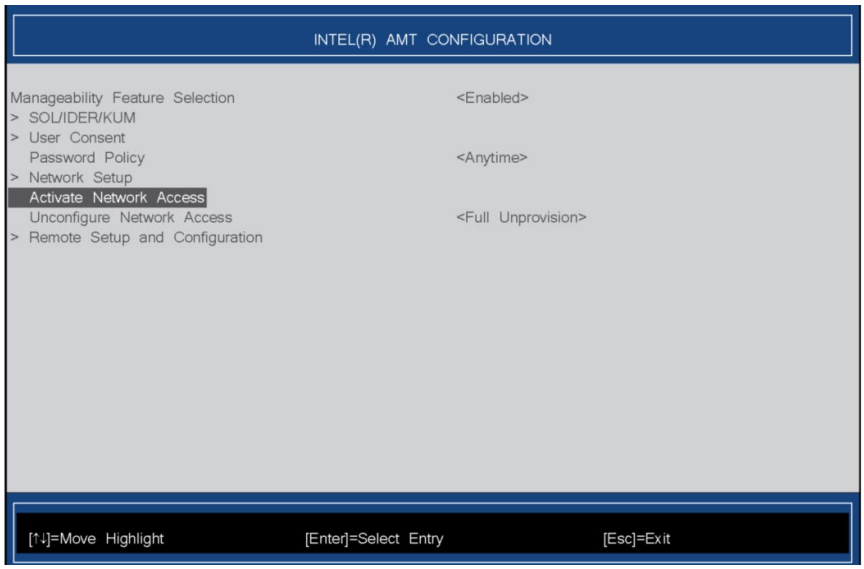


**Figure 3. Active Network Access**

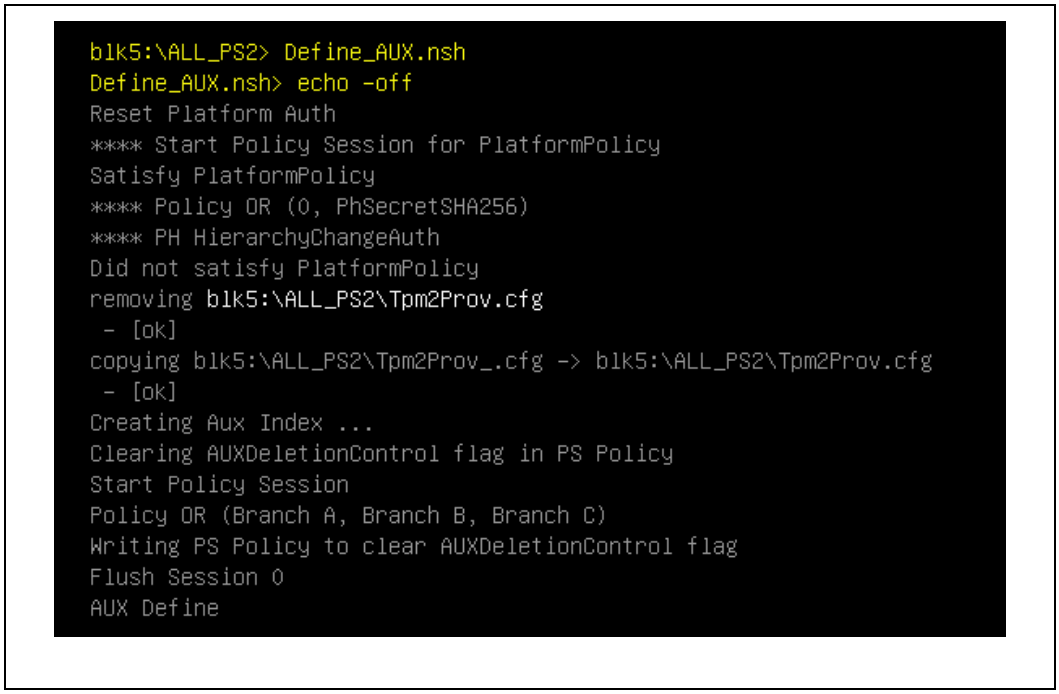



## 2.3 TPM 2.0 Provisioning

Download RDC no.563989 Tpm2ProvTool toolkit and execute following TPM 2.0 Provisioning Tool Guide to provision a TPM for use with Intel® TXT.

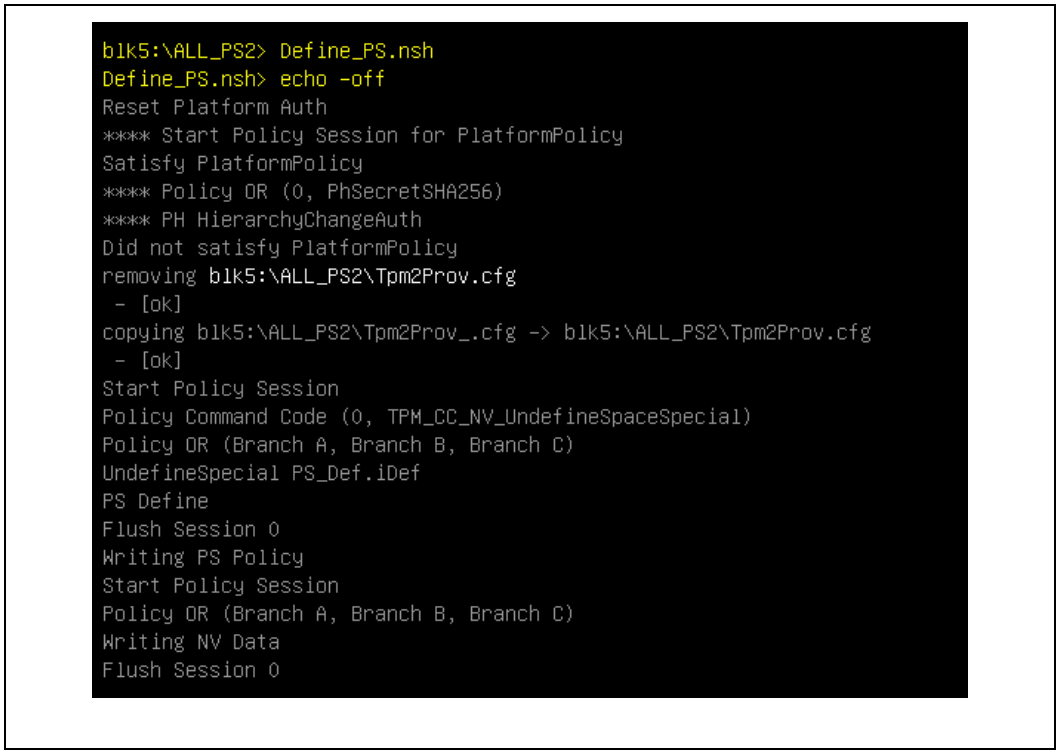
- Disable TXT in BIOS Setup and reboot
- Boot to EFI64 shell with access to the provisioning tools
- Run Define_AUX.nsh to define the AUX index

**Figure 4. Run Define_AUX.nsh**



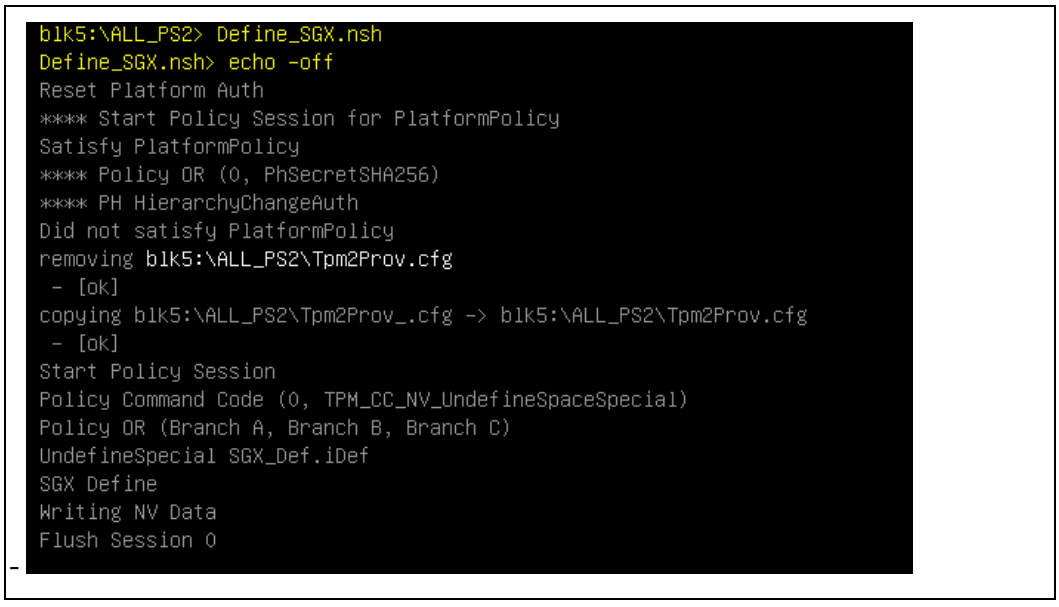

- Run Define_PS.nsh to define the PS index

**Figure 5. Run Define_PS.nsh**




- Run Define_SGX.nsh to define the SGX index

**Figure 6. Run Define_SGX.nsh**



- For PS2 attribute only: Run Lock_PS2.nsh to write-protect the PS2 data

**Figure 7. Run Lock_PS2.nsh**

```
blk5:\ALL_PS2> Lock_PS2.nsh
Lock_PS2.nsh> echo -off
Reset Platform Auth
**** Start Policy Session for PlatformPolicy
Satisfy PlatformPolicy
**** Policy OR (0, PhSecretSHA256)
**** PH HierarchyChangeAuth
Did not satisfy PlatformPolicy
removing blk5:\ALL_PS2\Tpm2Prov.cfg
 - [ok]
copying blk5:\ALL_PS2\Tpm2Prov_.cfg -> blk5:\ALL_PS2\Tpm2Prov.cfg
 - [ok]
Lock PS (for PS2 index only)
```

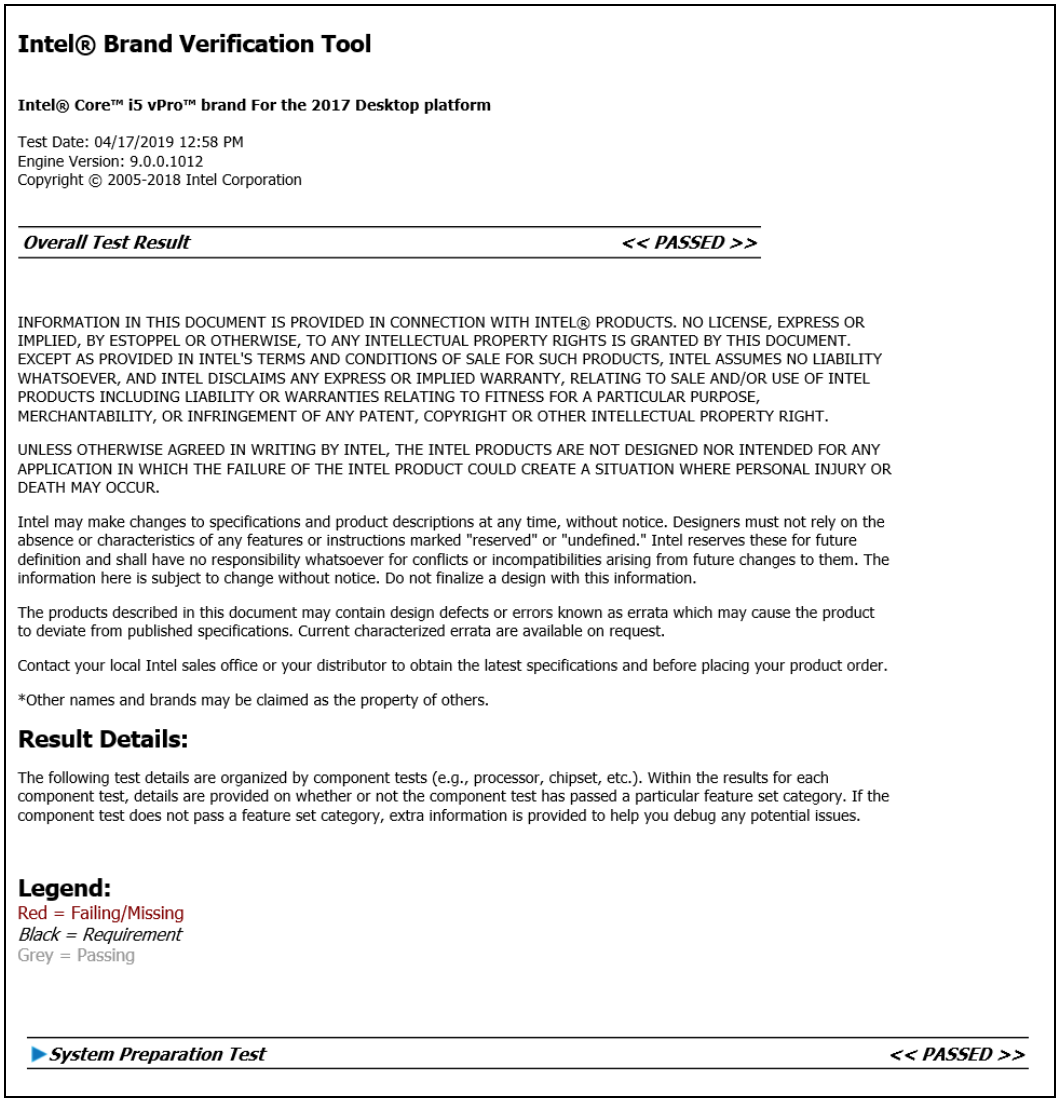
- Enable TXT in BIOS Setup

## 2.4 BVT (Brand Verification Tool)

Download BVT tool from link http://www.intel.com/go/bvt, following 'Support Platform PDF' check your HW/SW configurations and run bvt-package-vxxxx.exe.

For failed items, you can expand Red color branch to check detailed information.

**Figure 8. BVT Test Report**



**Intel® Brand Verification Tool**

**Intel® Core™ i5 vPro™ brand For the 2017 Desktop platform**

Test Date: 04/17/2019 12:58 PM
Engine Version: 9.0.0.1012
Copyright © 2005-2018 Intel Corporation

***Overall Test Result*** ***<< PASSED >>***

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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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.

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

**Result Details:**

The following test details are organized by component tests (e.g., processor, chipset, etc.). Within the results for each component test, details are provided on whether or not the component test has passed a particular feature set category. If the component test does not pass a feature set category, extra information is provided to help you debug any potential issues.

**Legend:**
Red = Failing/Missing
*Black = Requirement*
Grey = Passing

▶ ***System Preparation Test*** ***<< PASSED >>***

**NOTE:** BVT report, check failing with red item

## 2.5 IOTG Recommended Management Tool

- Download MeshCommander and install the MeshCommander tool on the console PC, to verify AMT features.

  Download link:
  http://info.meshcentral.com/downloads/mdtk/meshcommander.msi

**Figure 9. MeshCommander Tool**

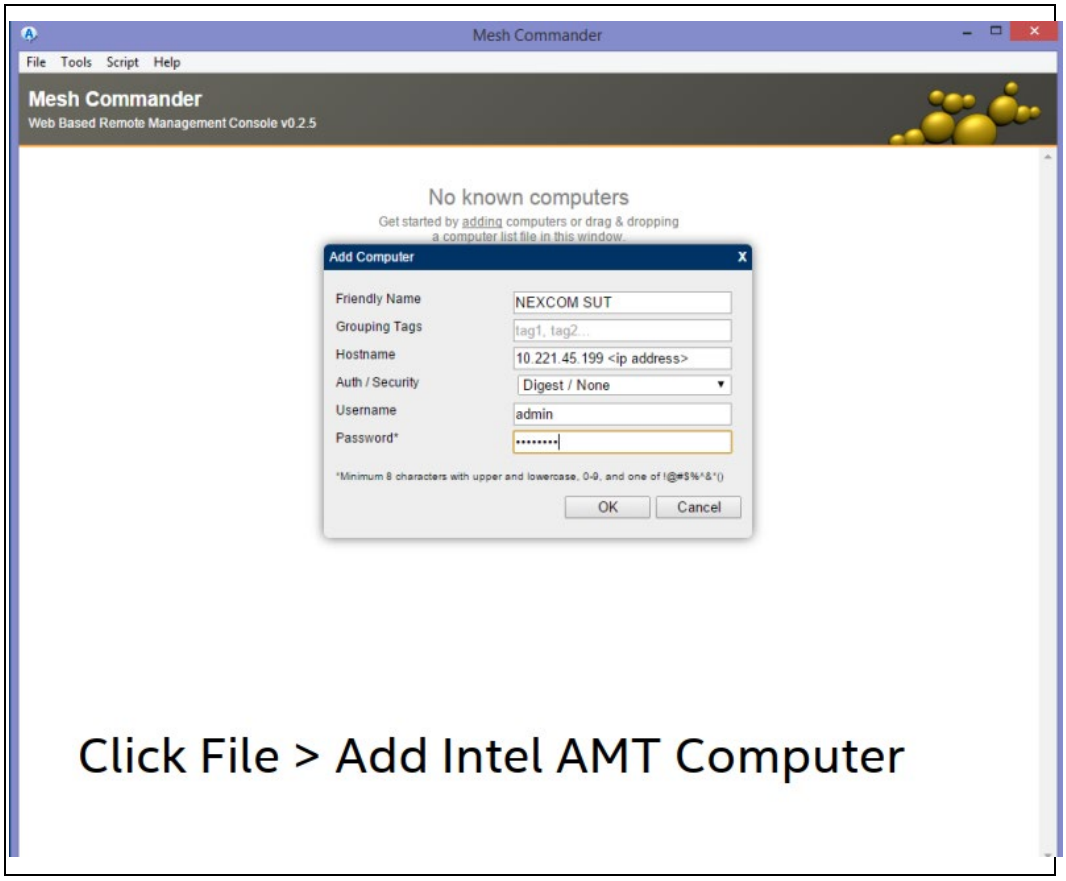
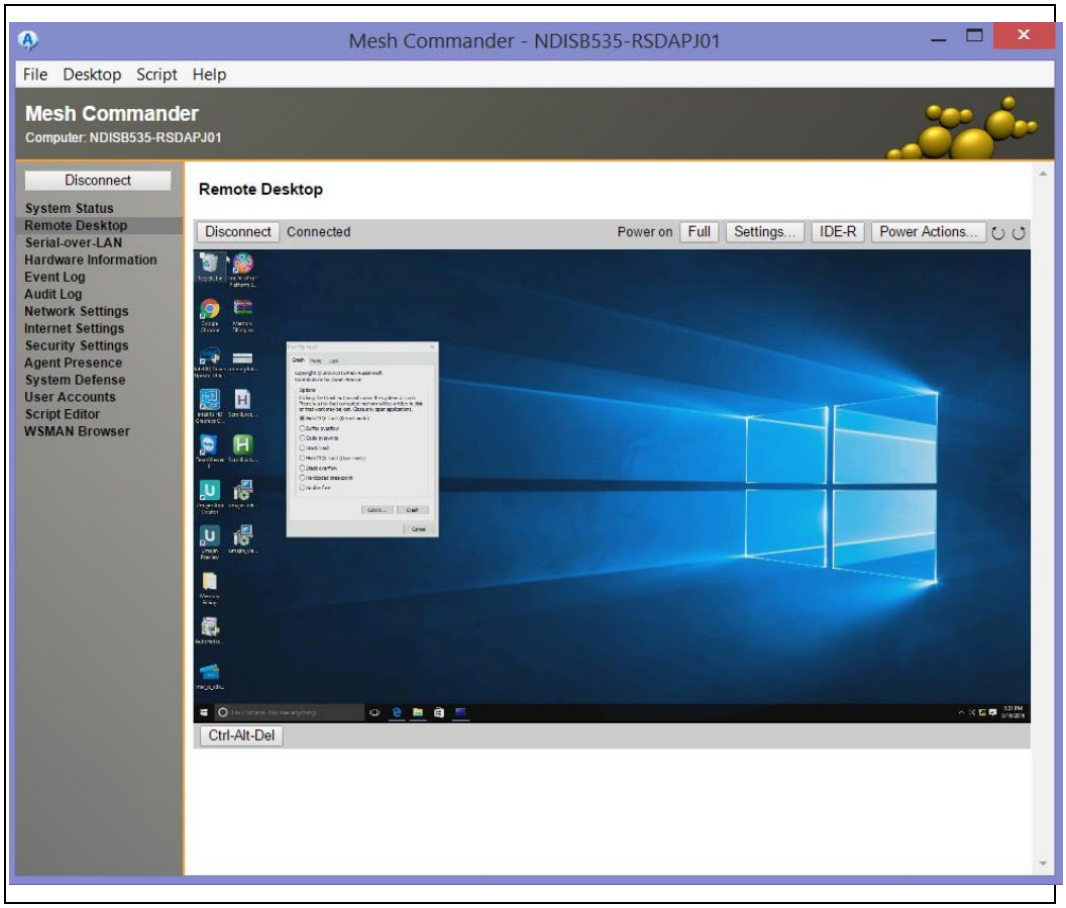


**Figure 10. KVM to Connect Remote Desktop**




§