Lenovo ThinkStation

Intel® Active Management Technology

(Intel® AMT)

Table of Contents

Overview

Intel Active Management Technology (AMT) is a hardware-based feature in Intel vPro platforms that allows IT administrators to remotely manage, monitor, and secure devices, even when they are powered off or the operating system is unresponsive. AMT provides out-of-band management capabilities, meaning it operates independently of the device's OS, establishing a secure connection to the hardware over the network.

While vPro mainly applies to Intel Core i5, i7, and i9 processors designed for business use, certain Intel Xeon processors (like Xeon E and Xeon W for workstations) also support vPro features such as AMT, offering similar manageability and security functions.

By leveraging AMT, organizations can reduce operational costs, enhance security, and improve IT management efficiency, though some features may depend on the hardware configuration.

Key features of AMT include:

1. Remote Access and Control: Enables remote troubleshooting, diagnostics, and repairs without needing physical access. Note that some features, like Keyboard-Video-Mouse (KVM) remote control, require an integrated graphics processor (iGPU) and are not available on Intel Xeon CPUs.

2. Security Management: Provides secure device monitoring, threat detection, patch deployment, and policy compliance, along with features like remote wipe and data protection.

3. Power Management: Allows remote control of power states, scheduling of maintenance tasks, and improved energy efficiency across devices.

4. Inventory and Asset Management: Facilitates the collection of hardware and software inventory data to track devices in an organization.

This document will offer guidance on its basic configuration together with some high-level limitations.

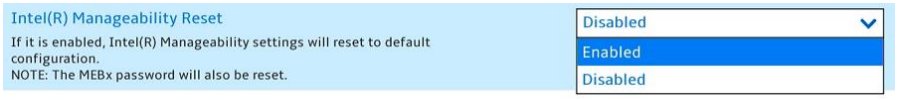
Section 1 – BIOS Configuration

For any new installation, it is recommended to reset the AMT feature to its default settings, regardless of whether the current password is known. This ensures that any existing configuration does not interfere with the installation process.

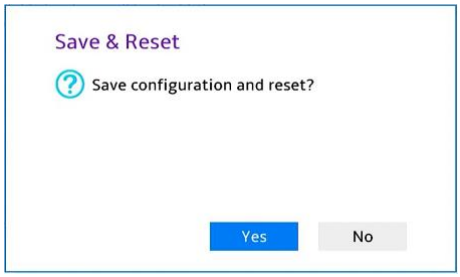
During POST, at the BIOS logo press **F1**

Navigate to **Advanced**, then **Intel® Manageability**,

Then Intel® Manageability Reset **Enabled**.



Then press **F10** to save and exit.

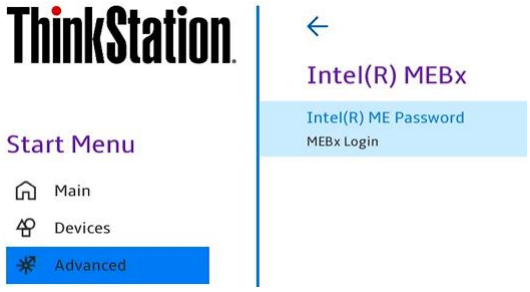


On reset notice the prompt stating that the Intel Management Engine is being “unconfigured”.

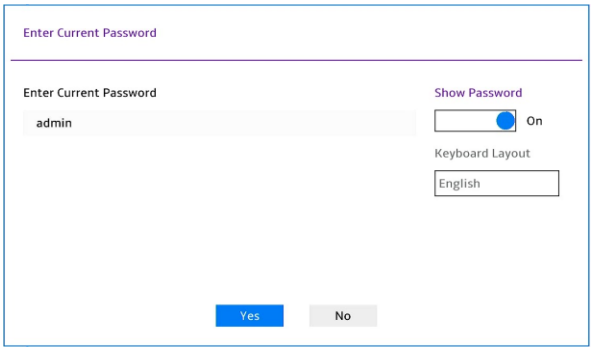
```
Found unconfigure of Intel(R) ME
Platform will continue with unconfiguration shortly...
```

When the Lenovo BIOS logo appears again, this time press **F12** to enter the **App menu**. Navigate to **Intel Management Engine BIOS Extension** or **Intel® MEBx,**

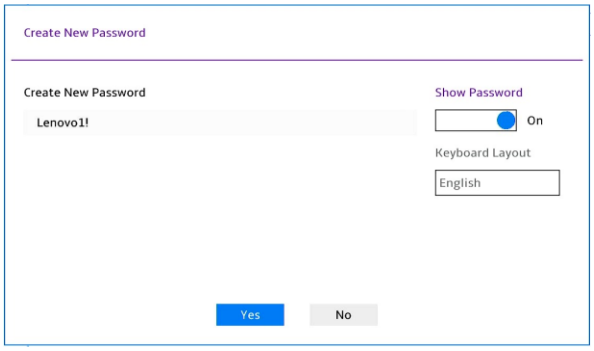
Select **Intel® ME Password -** MEBx Login,



Enter the now default password of ‘**admin’**



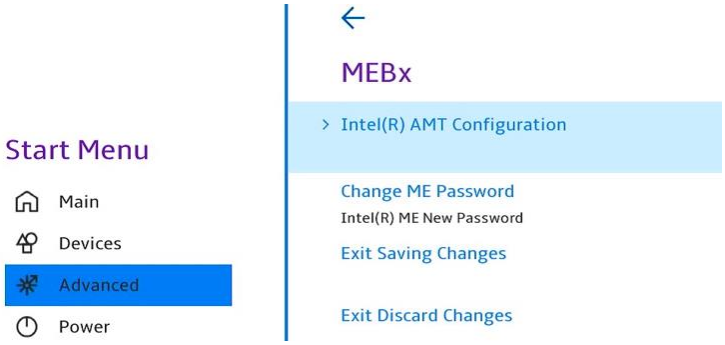
Set a new password. It must contain minimum 8 characters with upper, lowercase, 0-9, and one special character. **Do not** set the password to Lenovo1! As in this example!



If the new password doesn't meet the minimum criteria, there's no warning; it simply redirects you to re-enter the default password again.

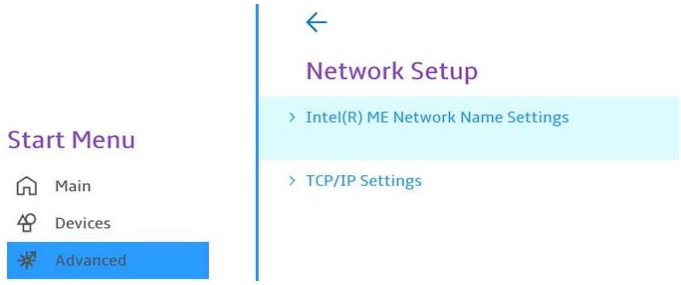
Once the password has been changed successfully you have access to the full AMT configuration menu,

Select **Intel® AMT Configuration**,

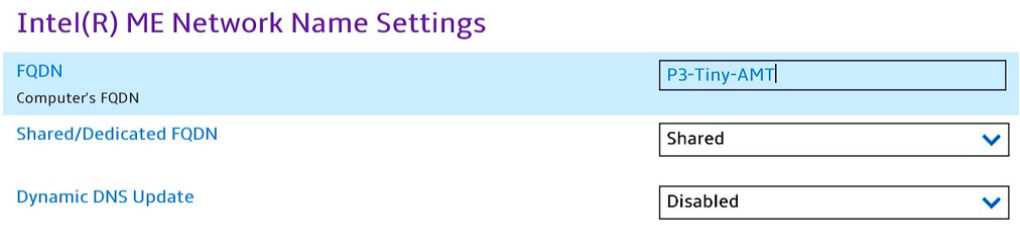


And change Network Access State to **Network Active**,

Then select **Network Setup**, followed by **Intel® ME Network Name Settings**,



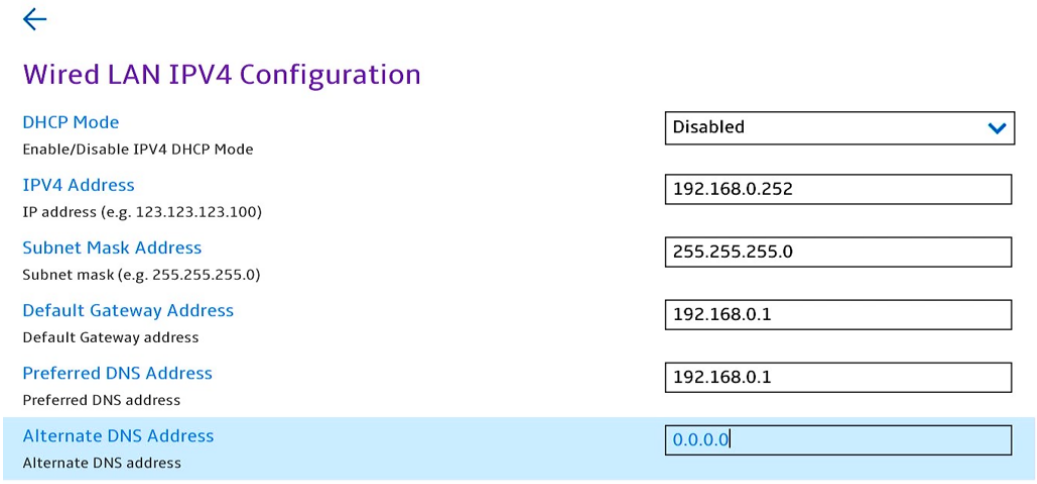
And enter a FQDN name, in this example P3-Tiny-AMT has been configured,



Return to the previous menu this time selecting **TCP/IP Settings** followed by **Wired LAN IPV4 Configuration.**

These are the network setting for the Intel® AMT not the host operating system. The two technologies share the same physical Intel network port, but this will be a separate ‘management’ address.

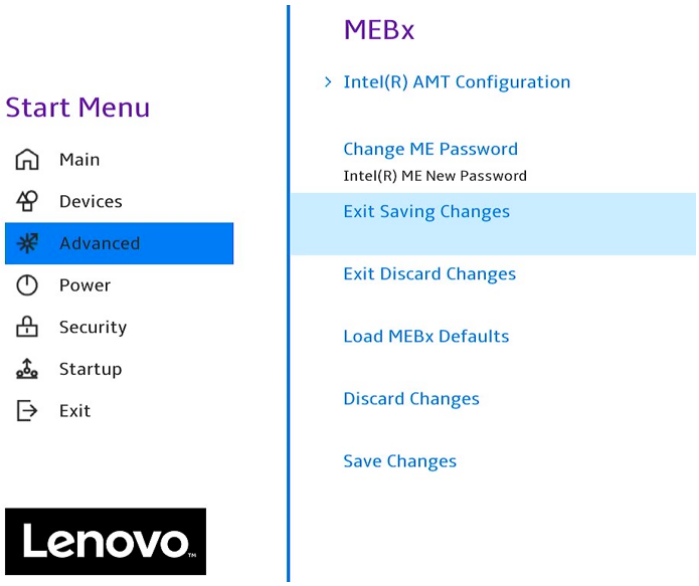
Your configuration will differ to that below.



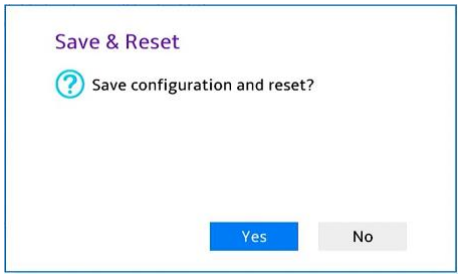
It is recommended to change DHCP mode to **Disabled** and configure a static management network address. Management networks don’t typically use DHCP, and a static address is advised to ensure it doesn’t change.

This network must be routable to the host system you wish to connect in from. If ICMP echo is permitted on your network, you can start a ping going via command line to this address to ensure it is active.

Escape (Esc) back to the 1st menu and, **Exit Saving Changes**,



Selecting **Yes** to the prompt,



Section 2 – Remoting in!

Intel's own Getting Started with Intel® Active Management Technology documentation states,

*"If you want access functions not supported with the **Intel AMT Web UI**, you need to use a remote management software from Intel **or third party with Intel AMT support**."*

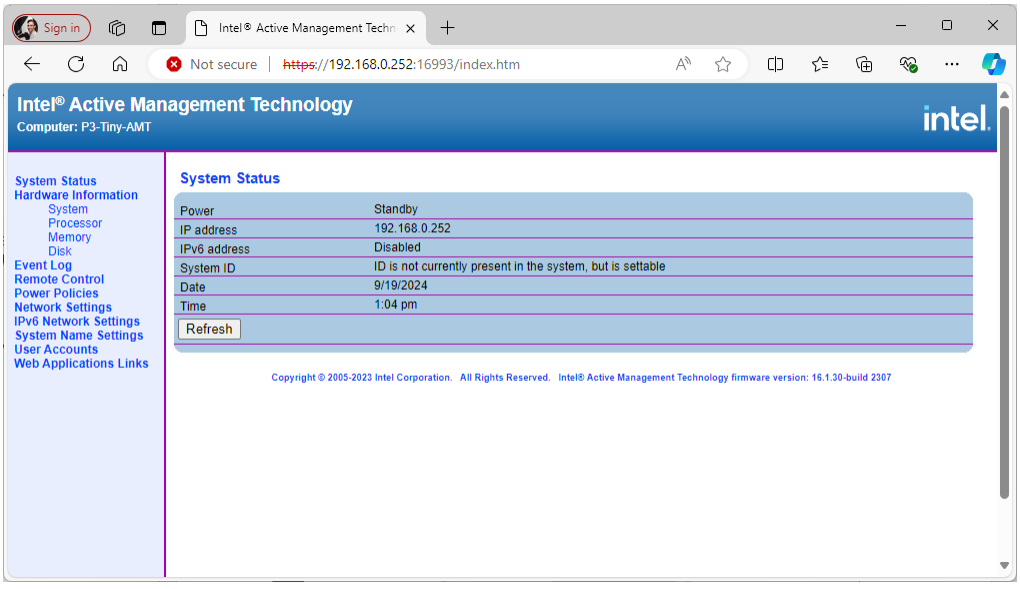
Intel AMT Web UI:

An administrator with user rights can remotely connect to the Intel AMT device via the Web UI by entering the URL of the device. Depending on whether TLS has been activated, the URL will change:

- Non-TLS - http:// <IP_or_FQDN>:16992
- TLS - https:// <IP_or_FQDN>:16993

You can also use a local connection using the host's browser for a non-TLS connection. Use either localhost or 127.0.0.1 as the IP address. Example: http://127.0.0.1:16992

Options available via the Intel AMT Web UI may only offer a subset of what's available with a dedicated desktop application. It offers no remote desktop capability.



Intel® Manageability Commander:

Please note from the outset IMC no longer supports self-signed certificates. A supported and paid for Vendor Certificates to Support Intel® AMT will be required.

Intel Manageability Commander is but one option and it can be downloaded from Intel.

Please view Intel's Getting Started guide for more detail if required.

After downloading and Installing Intel® Manageability Commander it still requires Electron, **a third-party component**, for Intel MC to be functional. You must download and unzip Electron to the folder where Intel MC has been installed. Details provided post install.

Then,

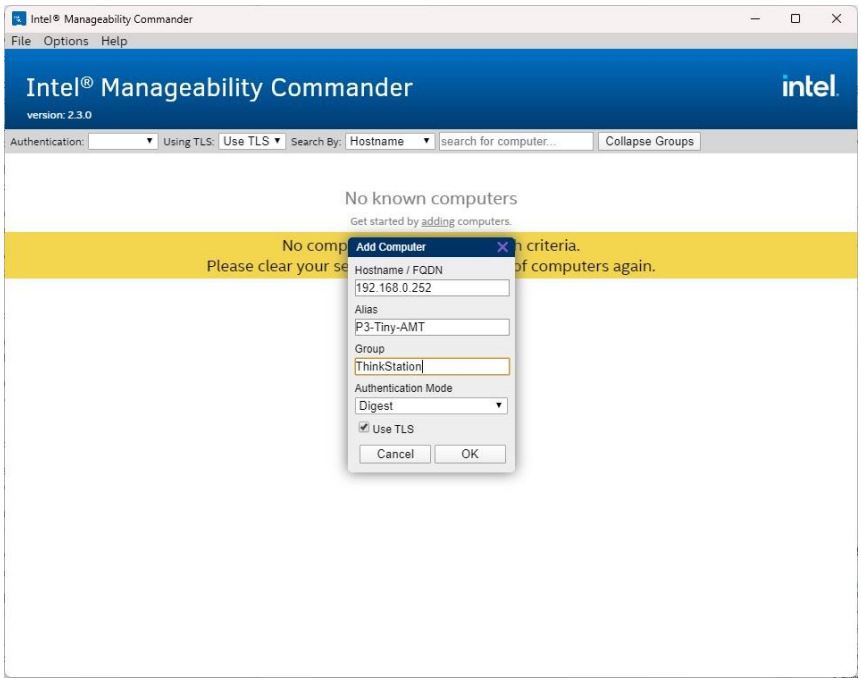
1. In a web browser, navigate to https://github.com/electron/electron/releases/tag/v8.5.5.

2. Scroll down and select 'electron-v8.5.5-win32-ia32.zip' (see note above). The file is downloaded to your system.

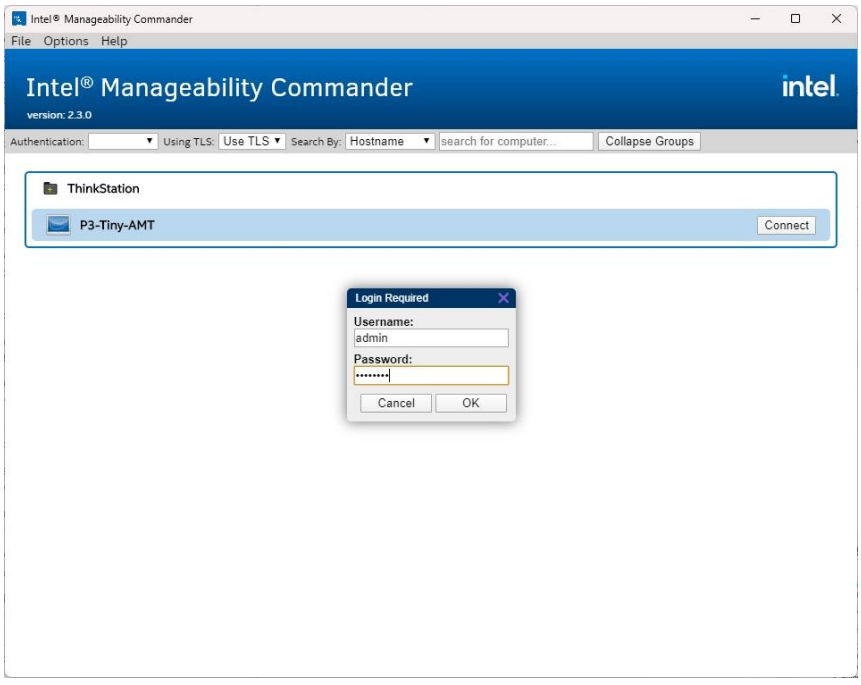
3. Open the zip file and copy all files and subfolders to your Intel MC installation folder (by default this is C:/Program Files (x86)/Intel/Intel Manageability Commander). Now the Intel MC desktop icon and start menu shortcut will work. Make sure that you copy these files to this installation folder and not into any subfolders that may be present in the Intel MC installation folder.

From within the Intel Manageability Commander interface click **File**, **Add Computer** from the top left menu and input the network details from Section 1.

Pay close attention to the Hostname / FQDN, not to be confused with the Alias. Change Authentication Mode to **Digest** and tick **Use TLS** click **OK**.



Once added click on the Connect button and input the username of admin and password set in Section 1.



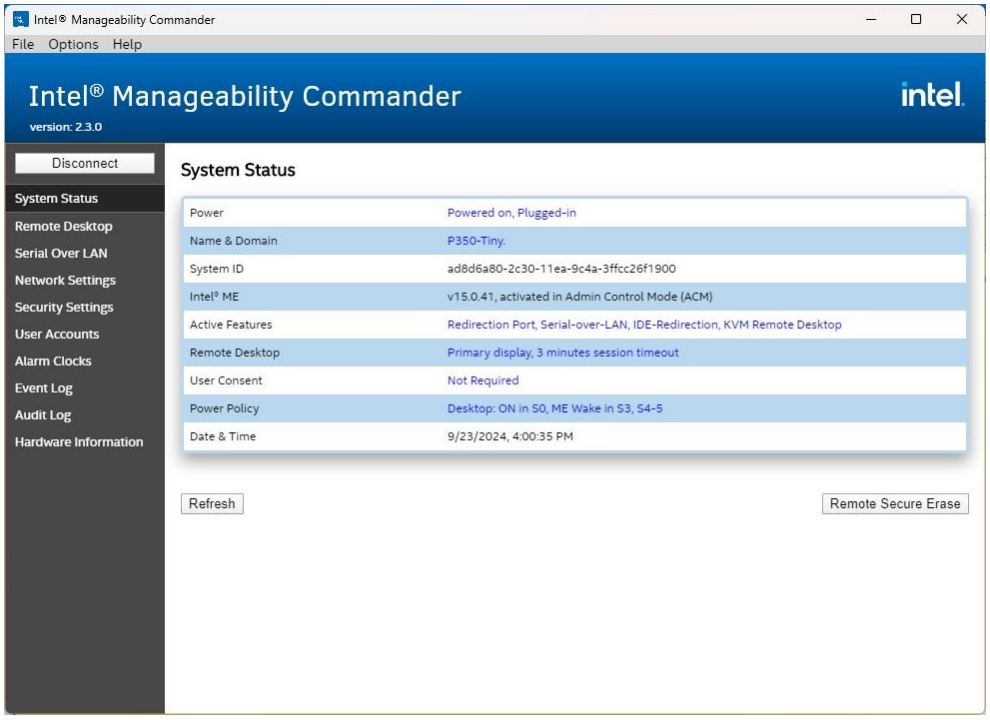
At this point you may receive the following error,

Intel introduced security updates to Intel® AMT (AMT16), and only pre-validated OEM Certificates with SHA256 are supported. Their hash is pre-installed into the BIOS firmware of vPRO-capable machines. Self-Certificates are not supported anymore.

For Vendor Certificates to support Intel® AMT, go to the bottom of this linked page.

The issue is documented in the following Intel forum thread in detail.

Once the connection is successfully established, the inventory will progressively populate on the left-hand side.

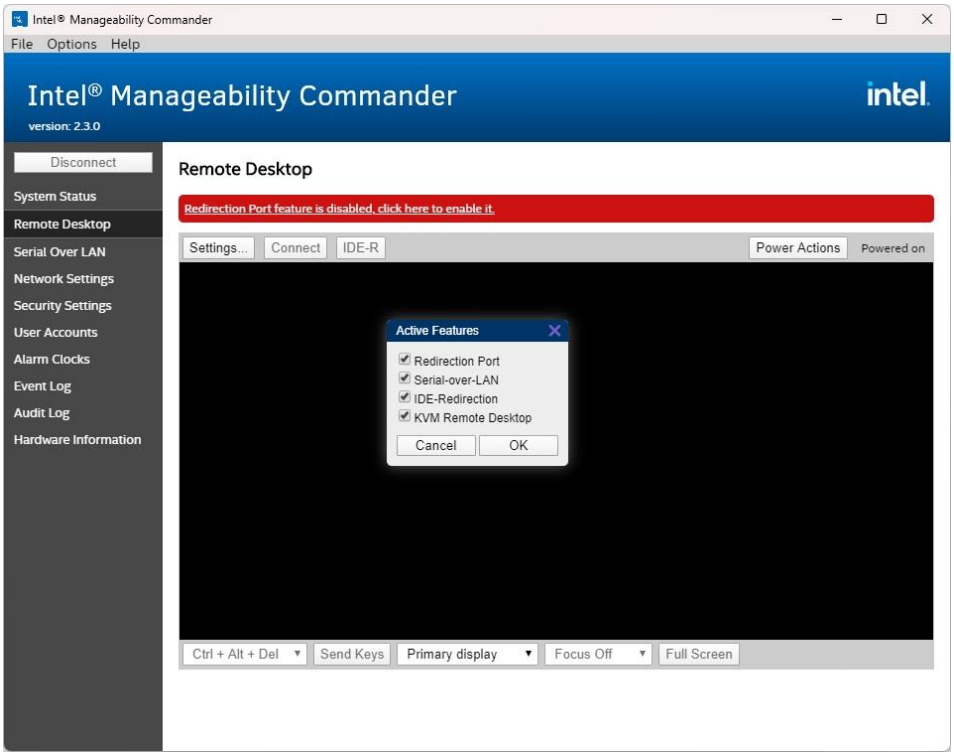


On a Xeon-based system without an integrated GPU (iGPU), the remote desktop feature is unavailable. This is because the desktop interface for remote sessions relies on the iGPU within the Intel® CPU.

On an Intel® Xeon® based system there are still many useful features, from remote hardware inventory to remote power on and reset.

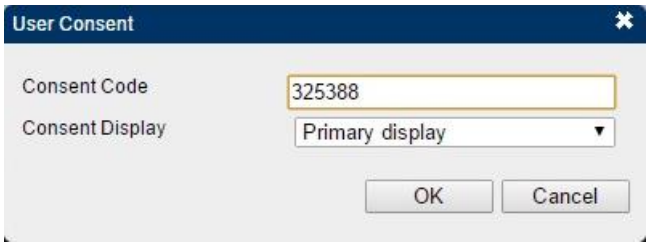
On an Intel® Core™ based system, one with an iGPU you have the addition of a Remote Desktop option with KVM functionality.

Before this feature is fully enabled you will need to click on the **RED** banner and enable both **Redirection Port** and **KVM Desktop.**



Then click **Connect.**

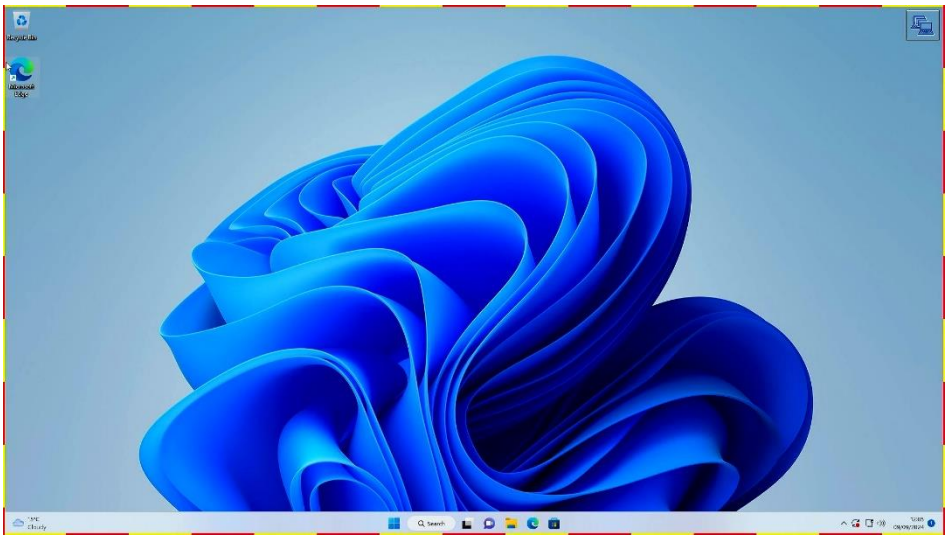
You are immediately prompted to input a **Consent Code**.



NB: User Consent can be modified and disabled in the BIOS so that it is not required. Change to User Opt-in NONE.

This code has just appeared on the user's desktop, and they need to provide you it to grant access to the user's desktop.

Once remotely connected to the user's desktop the user will see a flashing red and yellow border around the outside of the screen. This lets them know their action are possibly visible to others not in their immediate vicinity.



The purchasing and provisioning of a supported certificate from a trusted CA falls outside of the scope of this document. You may wish to use MeshCommander as an alternative to test remote functionality.

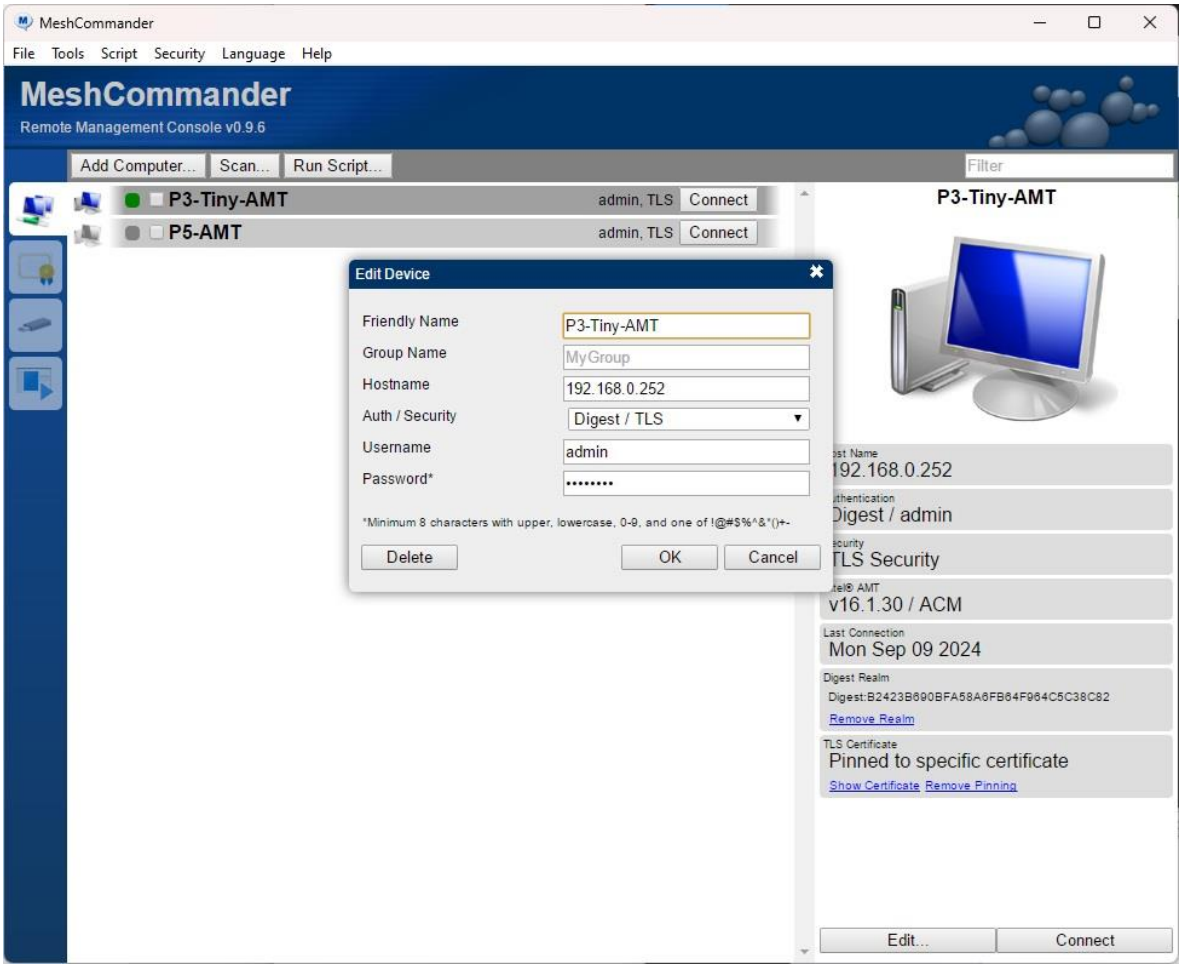
MeshCommander: (Self-Signed Supported)

MeshCommander is popular alternative to Intel Manageability Commander and can be used to test remote functionality without the need for a vendor certificate.

https://www.meshcommander.com/meshcommander

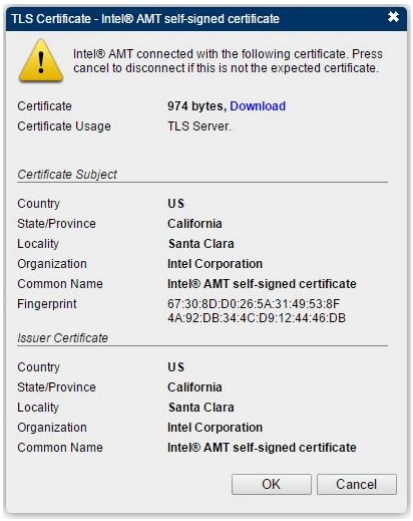
From within the MeshCommander interface click **Add Computer** on the top left and input the network details from Section 1.

Pay close attention to the Hostname / IP address, not to be confused with the friendly name. Change Auth / Security to **Digest / TLS** and input the **password**, also set in Section 1.



Then click on the **Connect** button to the right of your new entry.

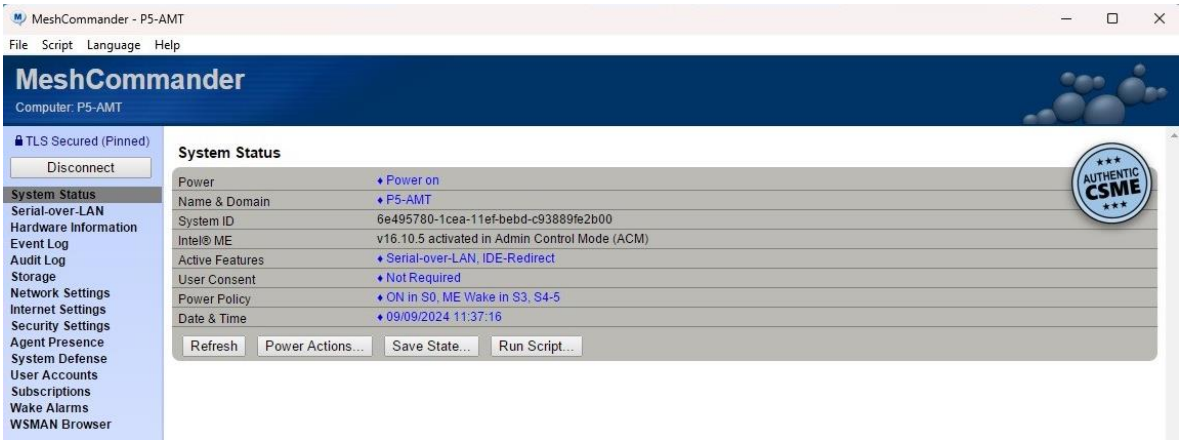
Accept the **self-signed**
TLS certificate when prompted,



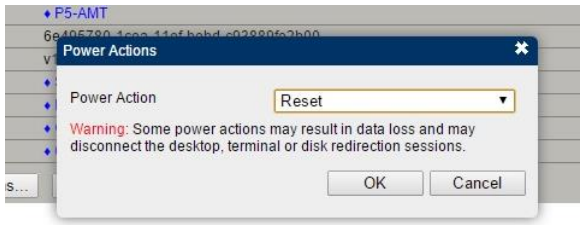
Once the connection is successfully established, the inventory will progressively populate on the left-hand side.

On a Xeon-based system without an integrated GPU (iGPU), the remote desktop feature is unavailable. This is because the desktop interface for remote sessions relies on the iGPU within the Intel® CPU.

Intel® Xeon® based system i.e. P5:



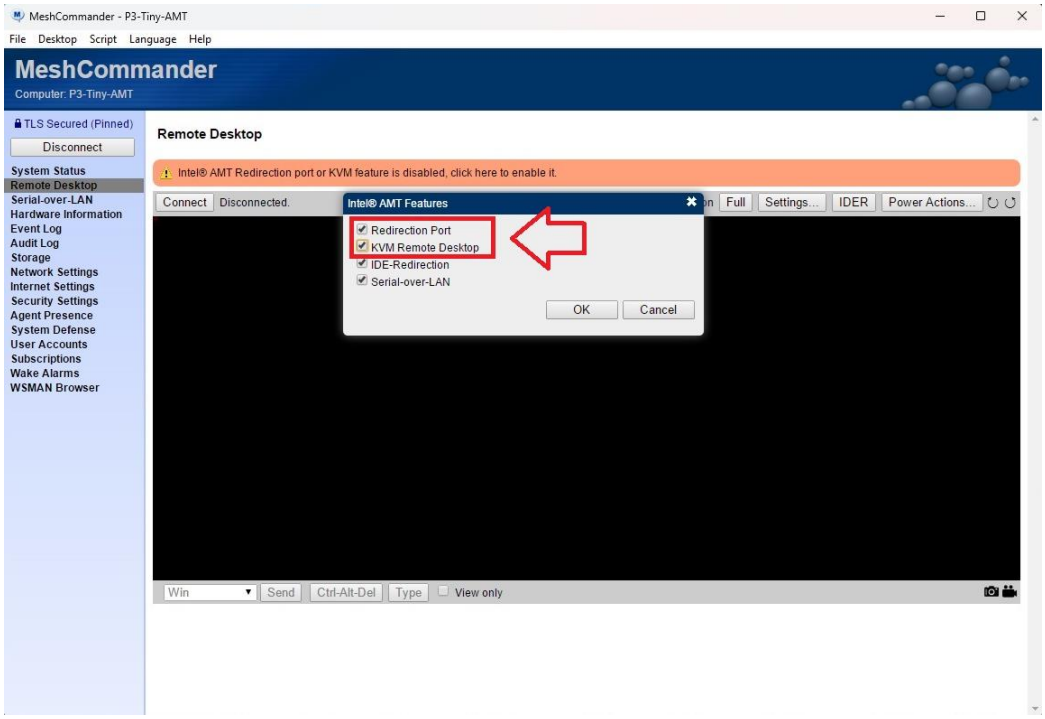
On an Intel® Xeon® based system there are still many useful features, from remote hardware inventory to remote power on and reset.



On an Intel® Core™ based system, one with an iGPU you have the addition of a Remote Desktop option with KVM functionality.

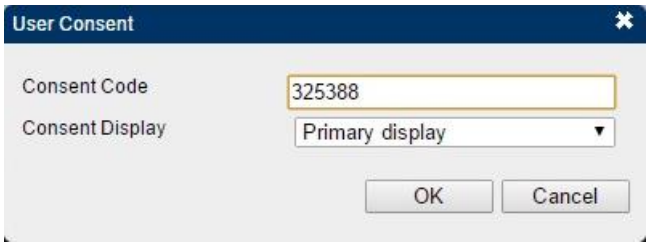
Before this feature is fully enabled you will need to click on the **ORANGE** banner and enable both **Redirection Port** and **KVM Desktop.**

Intel® Core™ based system i.e. P3 Tiny::



Then click **Connect.**

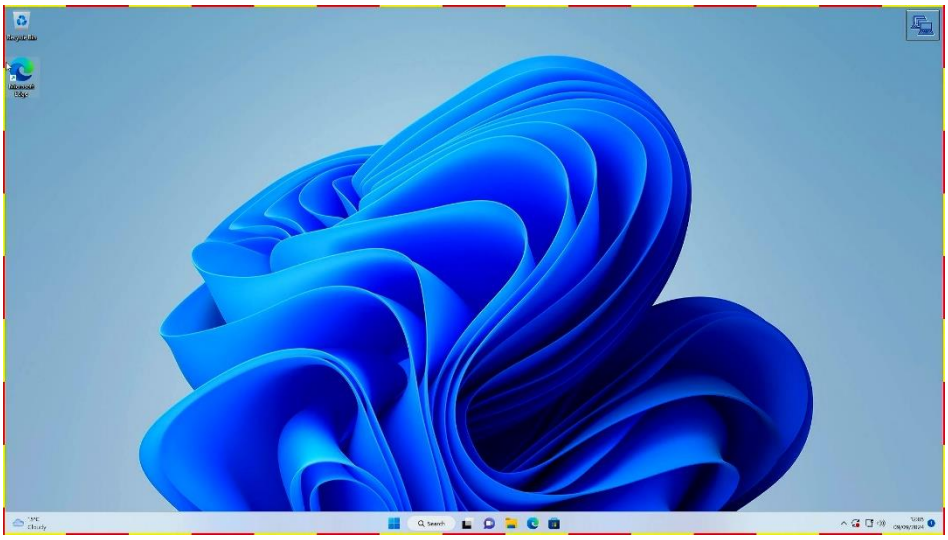
You are immediately prompted to input a **Consent Code**.



NB: User Consent can be modified and disabled in the BIOS so that it is not required. Change to User Opt-in NONE.

This code has just appeared on the user's desktop, and they need to provide you it to grant access to the user's desktop.

Once remotely connected to the user's desktop the user will see a flashing red and yellow border around the outside of the screen. This lets them know their action are possibly visible to others not in their immediate vicinity.

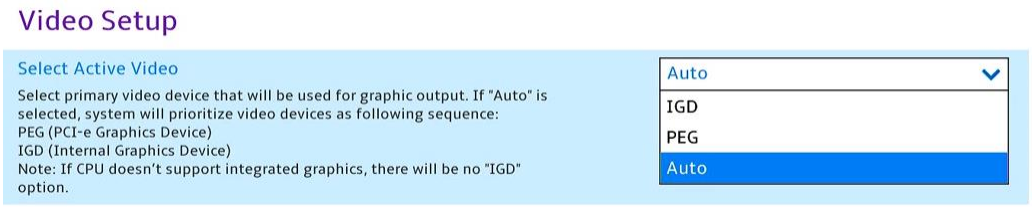


Section 3 – Considerations

Probably the most notable consideration when using Intel® AMT Remote Desktop in a workstation is the relationship between the Intel® iGPU (within the CPU) and any add-in discreet GPUs (Nvidia or AMD).

A remote desktop session will result in a black screen for the remote user if any of the following apply,

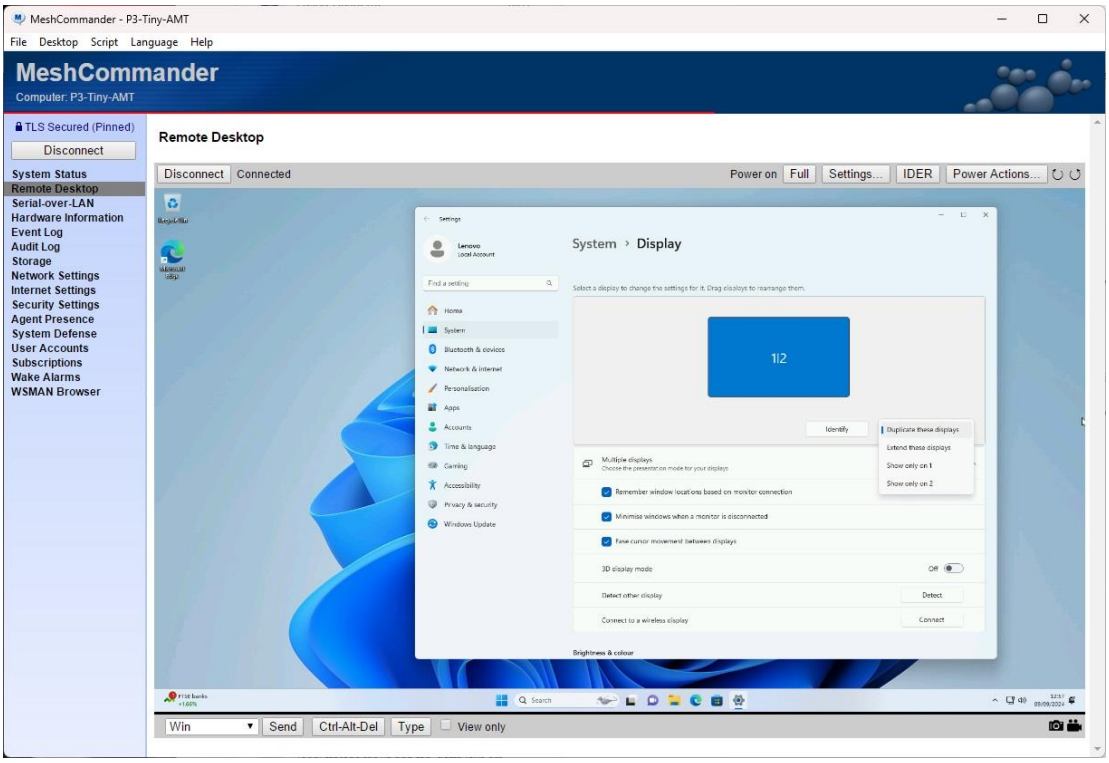
- If the iGPU or IGD (Internal Graphics Device) is disabled in the BIOS under video setup i.e. set to PEG (PCI-e Graphics Device)



- If the Intel® CPU has no iGPU or IGD (Internal Graphics Device)
- If the user has no display connected to the onboard iGPU video ports. The iGPU needs an active video connection to send to the remote viewer.

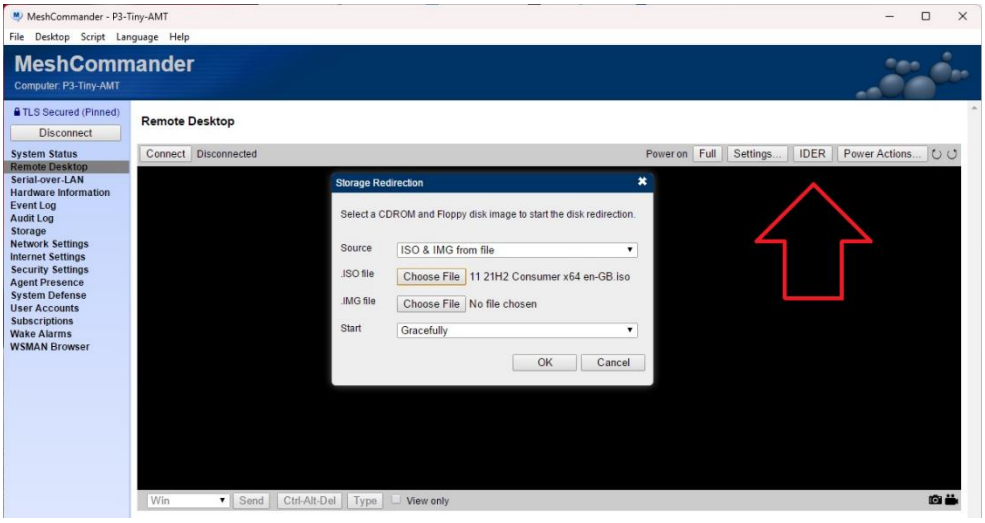
For most high-performance workstations, the primary display will be one connected to the add-in discreet GPU and not the onboard iGPU ports. In this scenario it may be necessary to duplicate the users display to a dummy display connected to the iGPU to ensure the Remote admin ‘sees’ the same desktop as the user.

By default, the additional admin session on the iGPU would appear as an extended desktop.

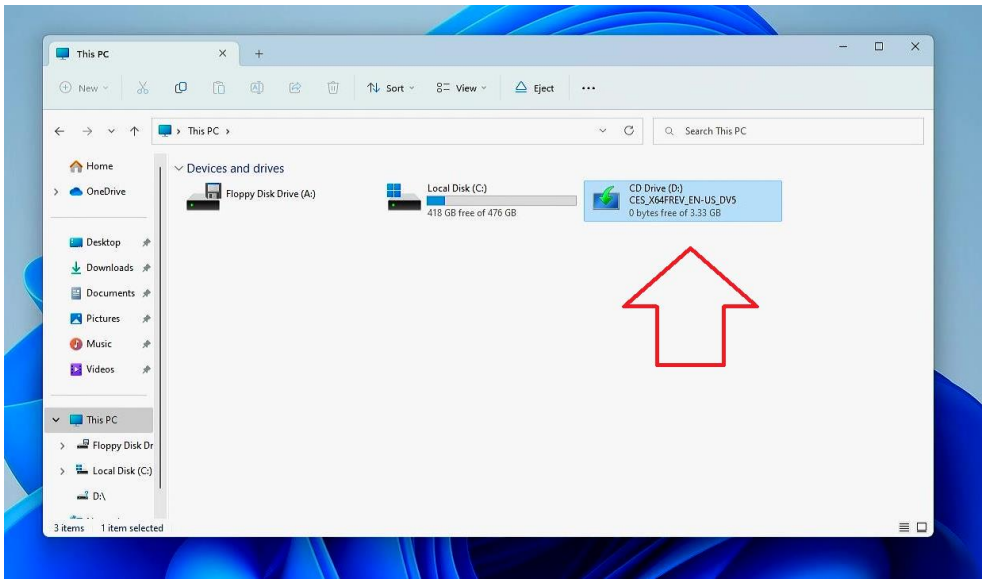


Section 4 – Appendix

It may be necessary to mount remote media or ISOs to the user's desktop. This is possible by clicking on the IDER button from within the Remote desktop section and browsing to the desired ISO file.



This file will then be mounted on the user's desktop as a regular CD-ROM,



While technically possible to perform a full installation of the operating system this way, in practice it is just too slow and unstable to be of meaningful benefit. Local media would be preferred.

Revision History

Version	Date	Author	Changes/Updates
v1.0	03/10/2024	Matthew R	Initial Release