White Paper

Intel vPro®
IT Professional Guide

For IT: A How-to Guide to Intel vPro®

Table of Contents

Get the most out of your investment in devices using Intel vPro technologies.

Intel vPro integrates a suite of transformative technologies that can benefit demanding business workloads. Tuning, testing, and rigorous validation by Intel and industry leaders help ensure every device with Intel vPro sets the standard for business. With each component and technology designed for professional-grade devices, IT can be confident that devices equipped with Intel vPro bring together business-class performance, hardware-enhanced security, modern remote manageability, and PC fleet stability.

How do you know you are getting all the benefits of Intel vPro? What actions do you need to take to enable and activate all the features that you want? In some cases, you only need to choose from device manufacturers and ISVs who have already built the benefits of Intel vPro into their solutions. You can be assured that Intel vPro enables IT functionality and support, and is perfectly suited for the modern, hybrid work environment. With the remote device-management functionality of Intel vPro, you can extract even more value by providing device support both inside the corporate firewall and outside with cloud-based functionality via a cloud service provider (CSP).

This guide provides an overview of the benefits, a description of your options, and a roadmap to using Intel vPro Enterprise for Windows with particular emphasis on remote manageability using Intel® Endpoint Management Assistant (Intel® EMA) to take advantage of Intel® Active Management Technology (Intel® AMT).[1]

Out-of-the-box benefits

Many benefits available with Intel vPro are "out-of-the-box" and require little or no IT interaction.

Performance

With Intel vPro, business-class performance is built right in. Using the latest drivers and software versions ensures that you get the advantages of long battery life, support for Wi-Fi 6 on laptops, or CPU/graphics processing unit (GPU) optimizations that support artificial intelligence (AI) and machine learning (ML). Ever-growing requirements for AI and ML in memory handling, security and encryption, collaboration, and system optimization put huge demands on CPU and GPU usage, which can impact performance, battery life, and responsiveness. For intense workloads on laptops and high-power workstations, Intel® Core™ processors equipped with Intel® Deep Learning Boost (Intel® DL Boost) can improve device bandwidth and productivity with AI and ML-related tasks.

Stability

Another crucial benefit of Intel vPro is PC fleet stability. Rigorous testing by Intel of the various hardware components in laptops and desktops helps ensure all brands of devices built on Intel vPro technologies deliver a reliable and stable foundation for smoother fleet management and refresh cycles on a global scope.

The Intel® Stable IT Platform Program (Intel® SIPP) provides confidence with the aim that each new device built on Intel vPro will be supported and available—globally and in quantity—for at least 15 months. When you upgrade to a newly released device built on Intel vPro, you can be confident the same hardware for your fleet will be available throughout the buying cycle. This coverage includes not just the CPU, but also complementary Intel vPro technology–enabled PC components such as chipsets, Wi-Fi adapters, and Ethernet adapters. Intel provides production-validated drivers for multiple versions of Windows on any given generation of the platform, either through Windows Update or updating drivers through Device Manager. Intel SIPP can help you manage OS transitions and take advantage of extended support from Microsoft for any OS release.

Security

As organizations face increased exposure to cyber threats and risks, you can rely upon the security features of Intel vPro to help secure your environment. These features are part of Intel® Hardware Shield. While these features require implementation by OEMs, ISVs, or partners, activating additional Intel vPro security features requires little to no IT action. These features include Intel® BIOS Guard, Intel® Runtime BIOS Resilience, Intel® Total Memory Encryption (Intel® TME), and Intel® Threat Detection Technology (Intel® TDT) with Accelerated Memory Scanning (AMS) and targeted detection with Advanced Platform Telemetry. Read the white paper to learn more about the features of Intel Hardware Shield.

Intel® Virtualization Technology (Intel® VT) also includes security capabilities that can protect potential attack surfaces. Intel VT is turned on by default on devices equipped with Intel vPro (it might be listed as Intel VT-x on some BIOS screens), although third-party tools are needed to make full use of its capabilities. Such tools include HP Sure Click,[2] Lenovo ThinkShield,[3] and Dell SafeBIOS.[4]

Some Intel vPro security features are available only in specific ISV or OEM products or versions that support them. As these features might not be enabled by default, refer to Table 1 to review hardware-based security capabilities available in specific products or versions.

Table 1. Hardware-based security capabilities that are available only in specific products or versions, or which might not be enabled by default

Security benefit	Intel vPro technology	How to get it
Get protection against return-, jump-, and call-oriented programming (ROP/JOP/COP) attacks	Intel® Control-flow Enforcement Technology (Intel® CET)	11th Generation Intel Core processors or newer, Intel® Xeon® W (Workstation) processors, and the latest version of Windows 11 Enterprise (10/2021 21H2, 9/2022 22H2, 10/2023 23H2)
Detect ransomware and crypto-mining attack behavior and improve performance through GPU offloading	Intel TDT	8th Generation Intel Core processors or newer, Intel Xeon W (Workstation) processors, and an endpoint detection and response (EDR) solution that supports Intel TDT, including Microsoft Defender for Endpoint, SentinelOne Singularity, and BlackBerry Optics
Cryptographically verify the OS launch environment	Intel® Trusted Execution Technology (Intel® TXT)	Varies by OEM; you might need to enable Intel TXT in the BIOS before the option appears in Windows (see Figure 1 for an example)

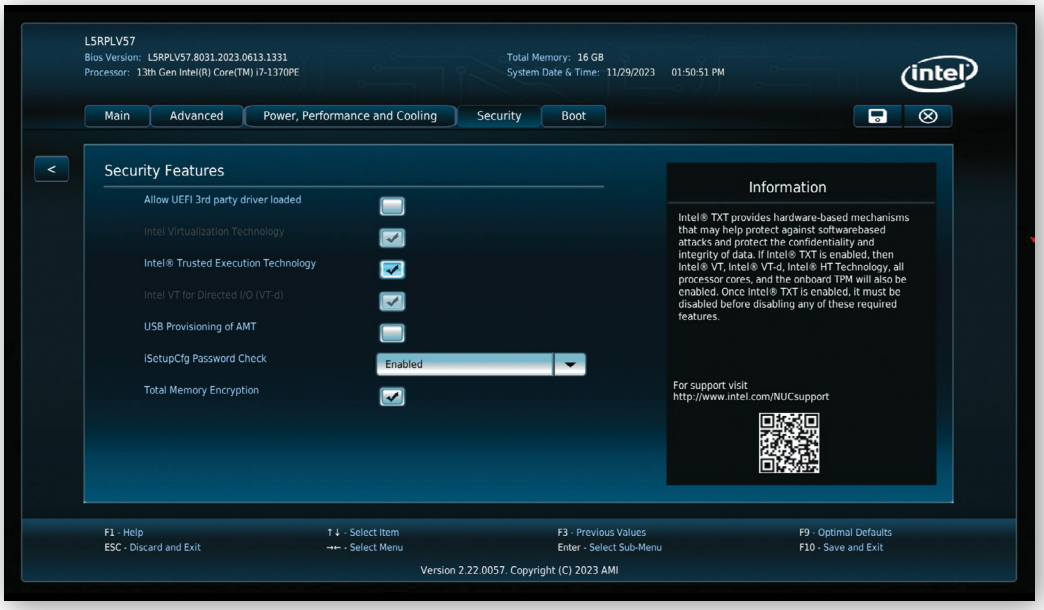

Figure 1. Cryptographic verification of the OS launch environment is done by enabling Intel TXT, shown here (details vary by OEM)

Manageability

The hybrid workplace is one of the biggest challenges facing IT administrators, with workers located both in the office and at various remote locations. IT administrators facing hybrid-work challenges can enable management connectivity to devices through Intel AMT and Intel EMA, which are built into devices with Intel vPro. The remainder of this paper provides detailed information on how to deploy remote manageability functionality through Intel AMT and Intel EMA.

Maximize remote manageability

IT departments have scrambled to support the sudden surge in remote workers, which can require preparing infrastructure for the new hybrid workforce reality. With an estimated 98 percent of workers wanting to work remote at least some of the time, remote manageability of your PC fleet will be critical into the foreseeable future.[5] Intel vPro provides a comprehensive set of remote-manageability capabilities through Intel AMT. Intel AMT can return your PCs to a known-good state, over wired and wireless connections, even when the OS is down.

Many system-management software vendors incorporate Intel AMT functionality into their products to varying degrees (which might require additional licenses or configurations), including:

- Microsoft Intune with Autopilot and Intel EMA
- VMware Workspace ONE
- Dell Client Command Suite
- Accenture Arrow
- CompuCom End-User Orchestrator
- Continuum
- ConnectWise
- Kaseya
- Ivanti
- Atos
- Lakeside
- Wortmann AG
- Terra

If you are using products like these with your devices equipped with Intel vPro, you might already be taking advantage of Intel AMT manageability features. Open AMT Cloud Toolkit provides open source, modular microservices and libraries for integration of Intel AMT.

For the most modern, cloud-enabled, out-of-band management of Windows devices located anywhere—including work-from-home Windows devices outside the firewall and connected over Wi-Fi—the premier manageability software you should consider is Intel EMA. You can incorporate Intel EMA within your existing IT support processes and use it to help automate a variety of IT tasks in a hybrid work environment.

How to harness the power of Intel AMT anywhere by using Intel EMA

This section surveys some of the top capabilities of Intel AMT, and it provides a roadmap for how to take advantage of those capabilities by using Intel EMA. Note that Intel® Management Engine (Intel® ME) version 11.8 or newer is needed for out-of-band management.

Intel EMA is readily downloadable software (see the next section for installation) that helps you set up and configure Intel AMT hardware and acts as a front end for utilizing Intel AMT, which is built into the hardware and firmware of devices equipped with Intel vPro. Some Intel EMA abilities include remotely cycling power via Intel AMT on a PC over a wired or Wi-Fi connection from the cloud, monitoring and controlling a remote laptop with keyboard, video, and mouse (KVM) control, or attaching a remote disk image to perform an upgrade or patch software in your employee's home office. Intel EMA is the software that lets you control Intel AMT.

How to install and configure Intel EMA

First, download the latest version of Intel EMA software. Intel EMA server software can be installed either on-premises or in the cloud. On-premises installations can be either inside the firewall to manage devices in the corporate environment, or beyond the firewall to more securely manage devices remotely. The starting point for installing on-premises is an installation .exe file and a familiar installation wizard. Download the complete installation guide.

Deployment procedures differ when you install the Intel EMA server in the cloud, depending on which cloud provider you use. Intel provides deployment guides for the three big cloud providers: Amazon Web Services, Microsoft Azure, and Google Cloud.

The following is a roadmap to installing on Azure as an example.

Installation example: Microsoft Azure

The high-level steps for installing the Intel EMA server on Azure are:

1. Create a new resource group in an existing Azure subscription.
2. Deploy an Azure application security group and configure as needed.
3. Deploy Azure Virtual Network, and then configure network security groups with security rules.
4. Deploy an Azure SQL Database instance, and then add it to the existing virtual network.
5. Deploy a Windows Server 2022 Datacenter Azure virtual machine (VM), add the VM to the existing virtual network, and configure Azure Bastion for remote desktop connectivity. If needed, deploy a load-balancing solution for an availability set.
6. Connect to Azure Active Directory (Azure AD) and Azure Active Directory Domain Services (Azure AD DS).
7. Deploy and configure Intel EMA on the Windows Server 2022 Datacenter VM using the existing Azure SQL database as the database endpoint.

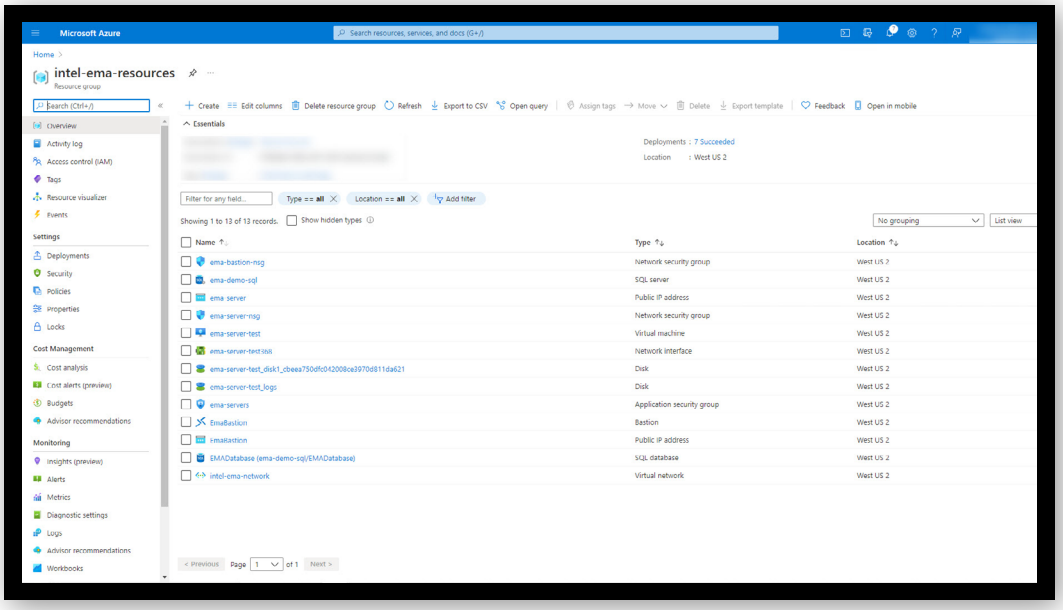

Figure 2. Example of an installed Intel EMA environment on Azure

Note that the Intel EMA Cloud Start Tool can create a VM in Azure with all necessary background services and Intel EMA automatically installed in a default configuration. The Intel EMA Cloud Start Tool for Azure allows you to start your evaluation or pilot process more quickly.

Getting started with Intel EMA

After your Intel EMA server is installed, whether on-premises or in the cloud, you will set up a tenant. A tenant is a usage space within the Intel EMA server that represents a business entity such as an organization or location within a company. One Intel EMA server can support multiple tenants.

You will create endpoint groups within tenants, in addition to creating the user accounts for the users who can manage those endpoint groups. Then you will create an Intel AMT profile, create an endpoint group with a group policy, and generate agent installation files to be installed on each device that will be governed by that group policy.

Open a browser window, enter the FQDN/hostname specified during server installation of your Intel EMA VM, and log in with the global admin user credentials configured during installation. (Note that you might need to log in from inside the firewall.)

Set up a tenant and create users

The first time you log in with the admin user credentials, you will see a Getting Started screen.

1. Click **Create a tenant**, give the new tenant a name and description, and then click **Save**.
2. On the left-side panel, click **Users**, and then click **New user** to create your first user, the tenant administrator.
3. You can then add more users as needed and, optionally, organize them into user groups. All users have access to all endpoints on a tenant, though a user group can be created that has read-only access.

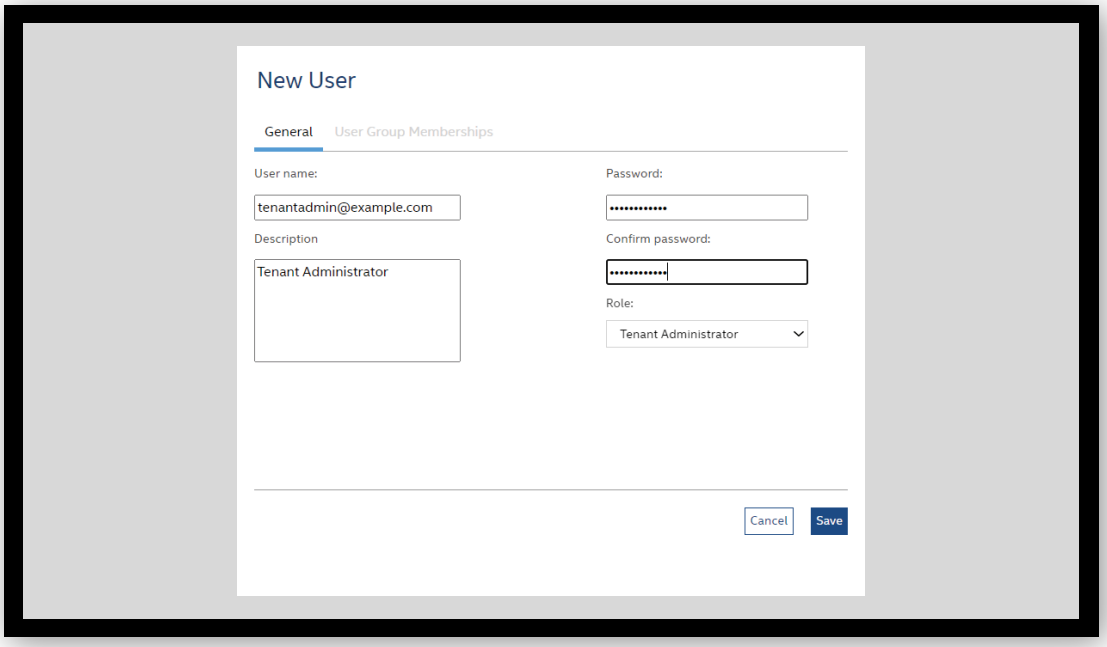

Figure 3. Add users to your Intel EMA tenant, starting with a tenant administrator

Create an Intel AMT profile

1. Log in to Intel EMA as the tenant administrator. On the left-side panel, click **Endpoint Groups**, and then click **Intel AMT Profiles** at the top.
2. Click **New Intel AMT Profile**.
3. In the **General** section, it is important to specify the profile name, client-initiated remote access (CIRA), and a nonresolvable domain name server (DNS) for the CIRA intranet domain suffix.
4. After you complete the General section, go to the **Management Interfaces** section, and then select all the features.
5. It's important to complete the Wi-Fi section if you will be supporting employees working from remote locations, such as their homes. In the Wi-Fi section, make sure that the **Synchronize with the host platform WiFi profies**, **Enable WiFi connection in all system power states (S1-S5)**, and **Enable WiFi profile sharing with UEFI BIOS** boxes are all selected, and then click **Save**.

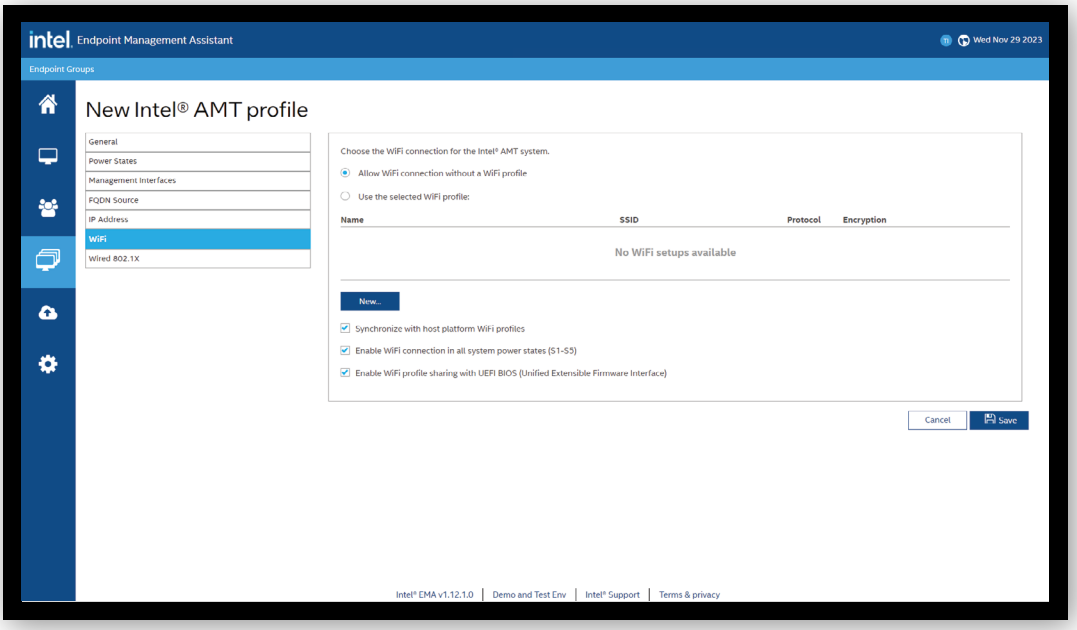

Figure 4. When creating an Intel AMT profile, be sure to complete the Wi-Fi section so you can support employees working remotely

Create endpoint groups

1. In the **Endpoint Groups** section, click **New endpoint group**.
2. Fill in the **Group Name**, **Group Description**, and **Password** fields, and then, under **Group Policy**, select all items.
3. Click **Save & Intel AMT autosetup**.
4. On the **Save & Intel AMT autosetup** screen, select the **Enabled** checkbox and make sure it shows your Intel AMT profile and host-based provisioning (HBP) as the activation method.
5. Fill in the **Administrator Password** field, and then click **Save**.

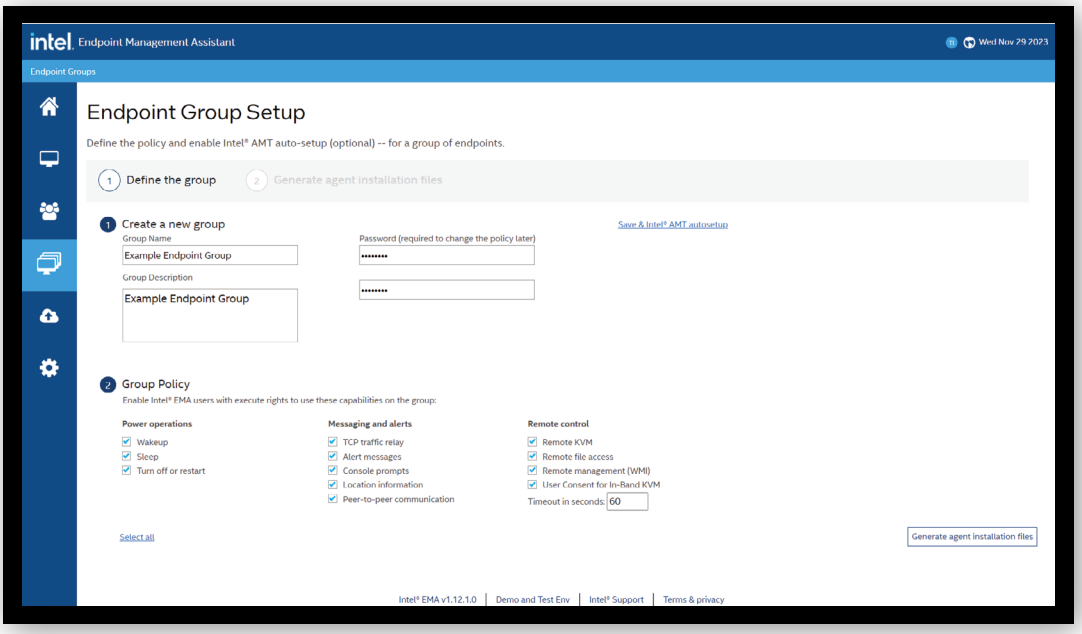

Figure 5. Enable Intel EMA users with execute rights on endpoints in an endpoint group

Generate and install agent installation files

After you have created an endpoint group and defined the group policy for that group, you will generate a file for installing the Intel EMA agent on each machine in the group.

1. Select the appropriate **Windows service** (almost always the 64-bit version), and then click **Download**.
2. Also click **Download** beside the **Agent policy** file.

You will need these two files together—EMAAgent.exe and EMAAgent.msh—to install the agent on each endpoint machine in the group. (Note: If you need to rename the files, rename them so that they still match.) For an evaluation, you can install the Intel EMA agent manually using the administrative command **emaagent.exe -fullinstall**. For production, you will most likely use the software distribution function from your systems management tool.

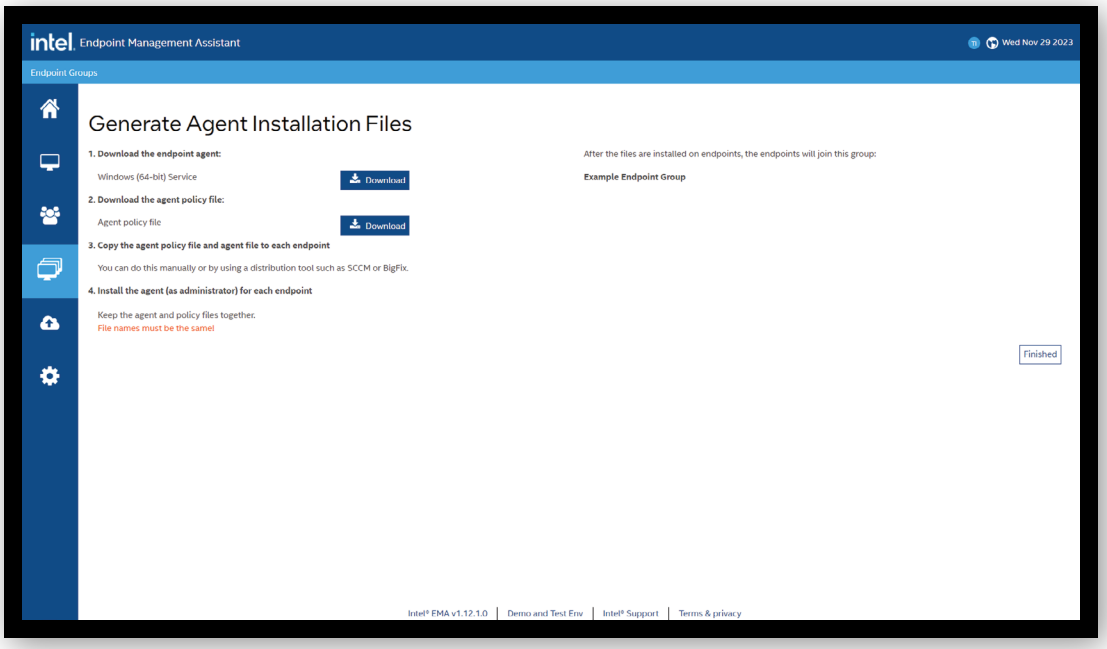

Figure 6. Download the two files you'll need to install the Intel EMA agent on each endpoint machine in the endpoint group

Common management tasks with Intel EMA

You can use Intel EMA for lifecycle management, including help-desk functionality and IT-task automation. Among the new features for remote manageability is Intel® Remote Platform Erase (Intel® RPE). You can use this technology to remotely reimage a device for repurposing, or you can delete the data stored on a device's storage drive and onboard memory if you wish to recycle the machine. You can also monitor the Intel EMA server log for visibility into Intel EMA server events.

Help-desk functionality

On the left panel of the Intel EMA screen, click **Endpoints** to access a range of functions for your help-desk operations.

The General tab provides information about the chosen endpoint machine. It allows control over that machine's power state, searching its files, provisioning Intel AMT, mounting an image, and more. The Hardware Manageability tab gives you access to Intel AMT out-of-band functions. The other tabs across the top of the Intel EMA screen (Desktop, Terminal, Files, Processes, and WMI) are for in-band functions that can be accessed when the remote OS is up and running. Endpoint functionality enhances your ability to provide support remotely, just as if you were at your desk.

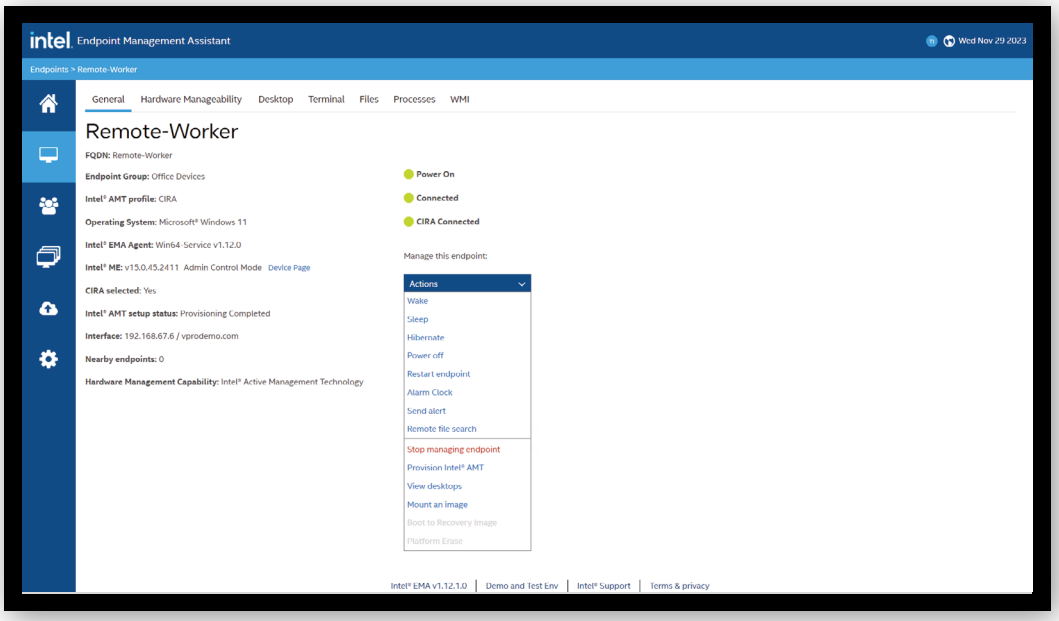

Figure 7. Explore the Endpoints section to discover how Intel EMA can enhance your remote support operations

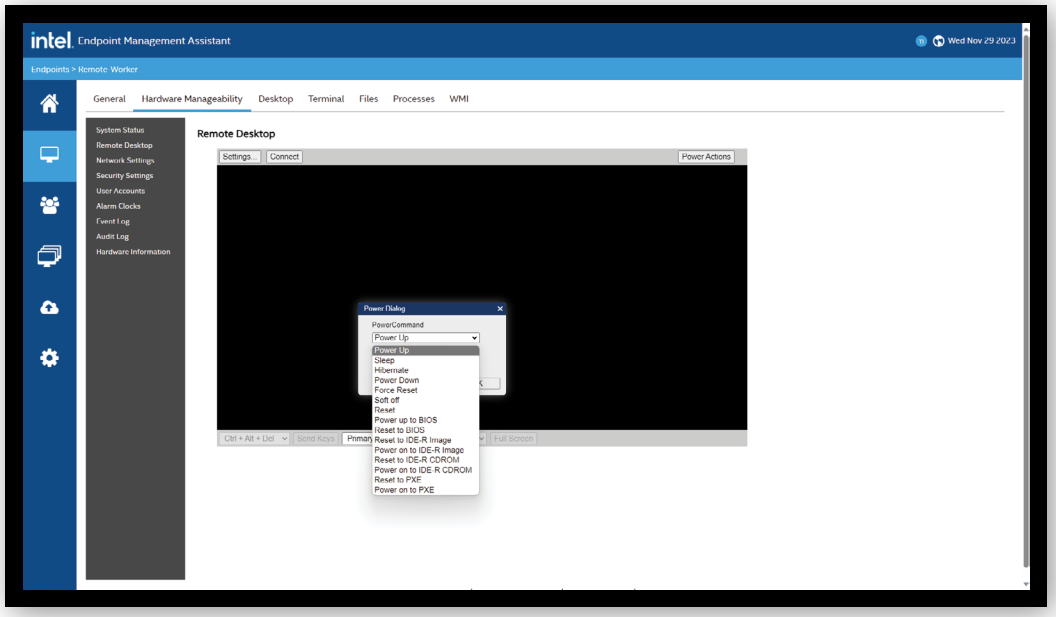

Figure 8. The Hardware Manageability tab provides access to out-of-band Intel AMT functions such as power actions

Lifecycle management actions

Intel EMA can do more than monitor endpoint machines. It also provides KVM-enabled remote operations without the machine being physically located with an IT technician. For inoperable or unresponsive machines, Intel EMA can remotely start a PC (as if the user pressed the power button), and it can mount and read a disk. This is especially useful if the machine will not boot or read from its solid state drive (SSD) or storage drive.

The USB Redirection (USBR) and One Click Recovery (OCR) features of Intel EMA allow you to mount a remote disk image (an .iso or .img file) to a managed endpoint via Intel AMT. Use this feature to mount a bootable image file and reboot a managed endpoint to a mounted image file. You can also browse the mounted image content from the console of the managed endpoint via KVM (note that the image must contain USB keyboard and mouse drivers for KVM interaction). Once you have mounted an image file, you can reboot the endpoint to the mounted image. OCR can initiate a recovery process on an endpoint to a last-known state (Intel AMT Out-of-Band [OOB] is required for this feature).

If you need to prepare a device for a new employee or reinstall Windows to fix a problem, the ability to mount a new image on a device wherever it might be, even over Wi-Fi, can eliminate the need for a physical IT presence. Be aware that an ISO file must be correctly formatted and can take hours to download. You can access this capability in the **Endpoints** section of Intel EMA, where you can click **Mount an image**.

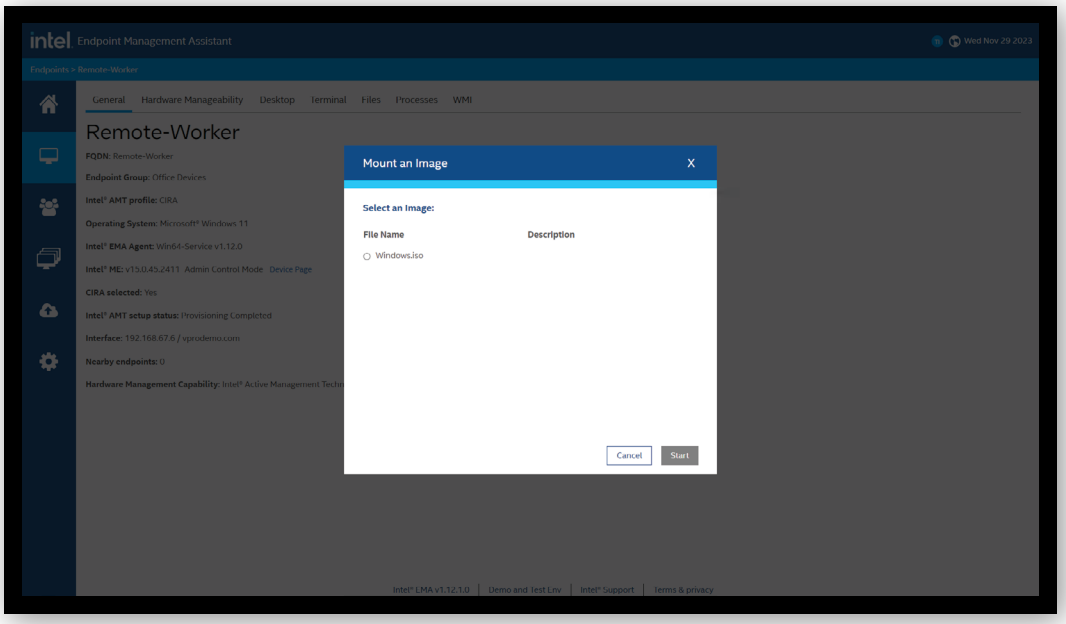

Figure 9. Mount an image to reinstall Windows on a device, wherever that device is located

Intel Remote Platform Erase (Intel RPE)

Intel RPE allows you to remotely erase all data and platform information, including (optionally) the platform's Intel AMT information. This feature is useful for end-of-life actions if a machine is to be retired, sold, or recycled. Note that Remote Secure Erase (RSE) is being deprecated. Additional information on Intel RPE can also be found in the Intel AMT Implementation and Reference Guide.

Table 2. Steps and features for Intel RPE

Three-step administrative process:	
1	Select a target system.
2	Select the items to be erased (such as an SSD or a Trusted Platform Module [TPM]).
3	Send the remote platform erase command.

What happens behind the scenes:

- Intel EMA locates target systems over the internet/intranet.
- A WS-Management command is sent to initiate Intel RPE on the next boot.
- The command is received by Intel AMT on an Intel vPro platform–based system.
- The remote platform erase is initiated. Data is erased from the selected items.

Monitor the Intel EMA server log

To access the Intel EMA server log, you will need to leave the Intel EMA application and launch the Intel EMA server installer on the Intel EMA server itself. A quick way to accomplish this is to launch **EMAServerInstaller.exe** and then click **Launch the Intel EMA Platform Manager**.

1. Log in to the **Intel EMA Platform Manager** using the administrator login that was created during installation of the Intel EMA server.
2. Click **localhost:8000**.
3. To see the event logs, click **Events**. You can choose at the bottom to see all events or only critical events. On the left, you can choose to view the events for the different server components (such as EMAAjaxServer, EMAManageabilityServer, and EMASwarmServer). Each component lets you trace its events in real time to help you with troubleshooting.

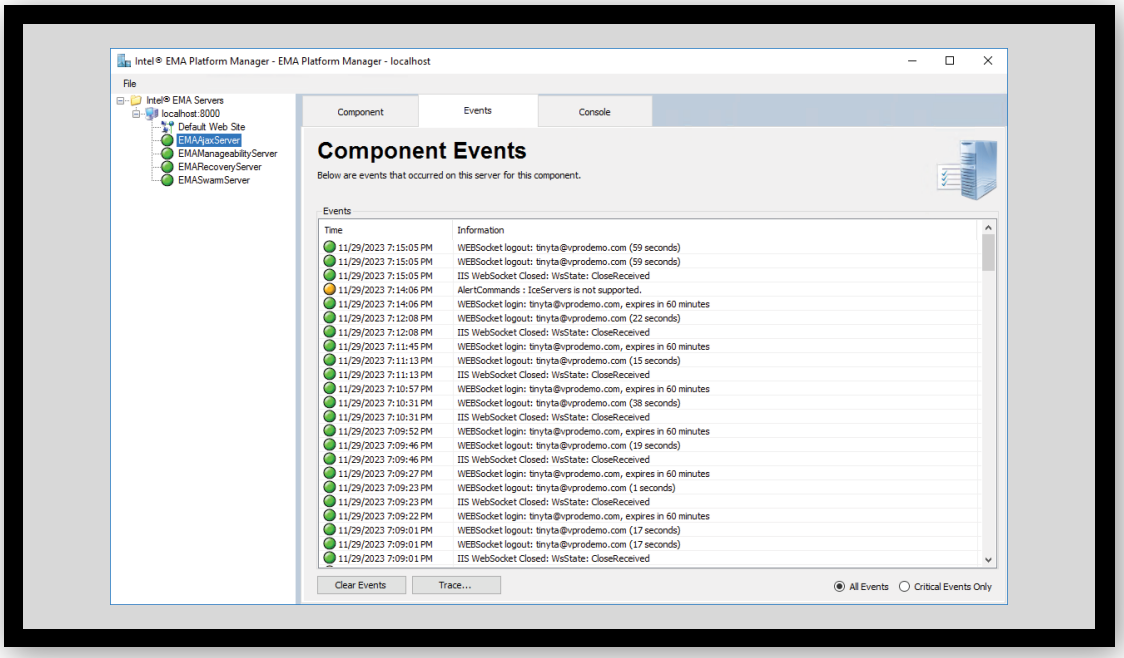

Figure 10. Monitor server events in real time and trace events on server components to troubleshoot issues

Additional features available with Intel EMA

Other features available through the Intel EMA console include:

- Remote file transfers*
- Remote command line*
- APIs to integrate Intel EMA or run as a stand-alone executable (the Intel EMA Agent console is available for download from the Intel EMA API)

*These features are only available in-band. Download the Intel EMA administration and usage guide for more information.

Conclusion

Intel vPro brings a wide range of benefits to your company. Many performance, stability, security, and manageability advantages of Intel vPro are available in the devices you buy from manufacturers and software vendors. These include features for enhanced business performance; greater stability for smooth fleet management; and important security features, such as Intel Hardware Shield, which protect against a growing number of cyber threats and risks.

Remember, you can get even better security and remote manageability by deploying Intel EMA to take full advantage of Intel AMT capabilities available with Intel vPro for Enterprise for Windows.

Want to learn more? Explore Intel vPro.

[1] Intel vPro Enterprise for Google Chrome does not have manageability features, while Intel vPro Essentials has Intel® Standard Manageability, a subset of Intel AMT.

[2] Intel. "Intel Virtualization Technologies Help Protect Endpoint Applications & Data without Impacting the User Experience." November 2022. intel.com/content/dam/www/central-libraries/us/en/documents/intel-virtualization-technologies-white-paper.pdf.

[3] Lenovo. "Flexible security to protect the workforce of the future." May 2021. https://techtoday.lenovo.com/sites/default/files/2023-01/Lenovo-IDG-REL-PTN-Nurture-General-Security-ThinkShield-Solutions-Guide-177-Solution-Guide-MS-Intel-English-WW.pdf.

[4] Dell Technologies. "Achieving pervasive security above and below the OS." delltechnologies.com/asset/en-us/products/security/industry-market/achieving-pervasive-security-above-and-below-the-os-whitepaper.pdf.

[5] Forbes. "Remote Work Statistics And Trends In 2024." June 2023. forbes.com/advisor/business/remote-work-statistics/.

Printed in USA 0624/RR/PRW/PDF Please Recycle 358530-002US