White Paper

Intel vPro® Platform
IT Professional Guide

For IT: A How-to Guide to the Intel vPro Platform

Table of Contents

Get the most out of your investment in the Intel vPro platform.

The Intel vPro platform integrates a suite of transformative technologies that have received extra tuning and testing for demanding business workloads. Rigorous validation by Intel and industry leaders helps ensure that every device built on the Intel vPro platform sets the standard for business. With each component and technology designed for professional grade, IT can be confident in one validated solution that brings together business-class performance, hardware-enhanced security, modern remote manageability, and PC fleet stability.

But how do you know if you're getting all the benefits of the Intel vPro platform? What actions do you need to take to enable and activate all the features of the platform that you want? In some cases, there is nothing you need to do beyond choosing the right versions of products from device manufacturers and ISVs who have already built the benefits of the Intel vPro platform into their solutions. In other cases, such as with remote device-management functionality, you can extract much more value from the platform by enabling or activating technologies that are part of the Intel vPro platform.

This guide provides an overview of your options and a roadmap for how to get started using Intel® Endpoint Management Assistant (Intel EMA) to take advantage of Intel Active Management Technology (Intel AMT).

Out-of-the-box benefits

First, pick the low-hanging fruit by taking advantage of the many benefits available with little or no IT action required.

Performance

Business-class performance is built right in. You don't need to do anything to gain the advantages of long battery life, support for Wi-Fi 6 on your laptops, or CPU/graphics processing unit (GPU) optimizations to support artificial intelligence (AI). New AI and machine learning (ML) algorithms in security, collaboration, and system optimization are demanding a large amount of CPU and GPU usage, which impacts performance, battery life, and responsiveness. Intel vPro platform technologies such as Intel Deep Learning Boost (Intel DL Boost) enable software makers to use AI and ML for all kinds of purposes—from visual noise reduction to memory scanning for ransomware—without users experiencing a degradation of performance.

Stability

Another benefit of the Intel vPro platform that is ripe for the picking is PC fleet stability. Rigorous testing by Intel of the various hardware components in your PCs help ensure that all brands of devices built on the Intel vPro platform deliver a reliable and stable foundation for smoother fleet management and refresh cycles on a global scope.

Moreover, the Intel Stable IT Platform Program (Intel SIPP) is designed to ensure that each Intel vPro platform release will be supported and available—globally and in quantity—for at least 15 months. This means that when you upgrade to a newly released Intel vPro platform generation, you can rest assured that you'll be able to acquire more of the same hardware for your fleet throughout the buying cycle, from anywhere in the world. This assurance includes not just the CPU, but also complementary Intel vPro technology–enabled PC components such as chipsets, Wi-Fi adapters, and Ethernet adapters. Intel also validates multiple versions of Windows with production-validated drivers on any given generation of the platform. This can help you better manage operating system (OS) transitions and take advantage of extended support from Microsoft for any given OS release.

Security

Most Intel vPro platform security features are part of Intel Hardware Shield, implemented by OEMs, ISVs, or partners, and they require little to no IT action. These features include Intel Secure Key, Intel BIOS Guard, Intel Runtime BIOS Resilience, Intel Total Memory Encryption (Intel TME), and accelerated memory scanning (AMS) with Intel Threat Detection Technology (Intel TDT). Intel Virtualization Technology (Intel VT) also includes security capabilities, and it is turned on by default on the Intel vPro platform, although third-party tools are needed in order to make full use of its capabilities. Such tools include HP Sure Click, Lenovo ThinkShield, and Dell SafeBIOS, for example.

Some Intel vPro platform security features are available only in specific ISV or OEM products or versions that support them, and these features might not be enabled by default, as shown in Table 1.

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
Protection against return-, jump-, and call-oriented programming (ROP/JOP/COP) attacks	Intel Control-flow Enforcement Technology (Intel CET)	11th Generation Intel® Core™ vPro® processors and a new enough version of Windows 10 Enterprise (10/2004 20H1: 19041.662+ and 10/2004 20H2: 19042.662+)
Detect ransomware and crypto-mining attack behavior and improve performance through GPU offloading	Intel TDT	8th Generation Intel Core vPro processor or newer and an endpoint detection and response (EDR) solution that supports Intel TDT, including Microsoft Defender Antivirus, 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 BIOS before the option appears in Windows (see figure 1)

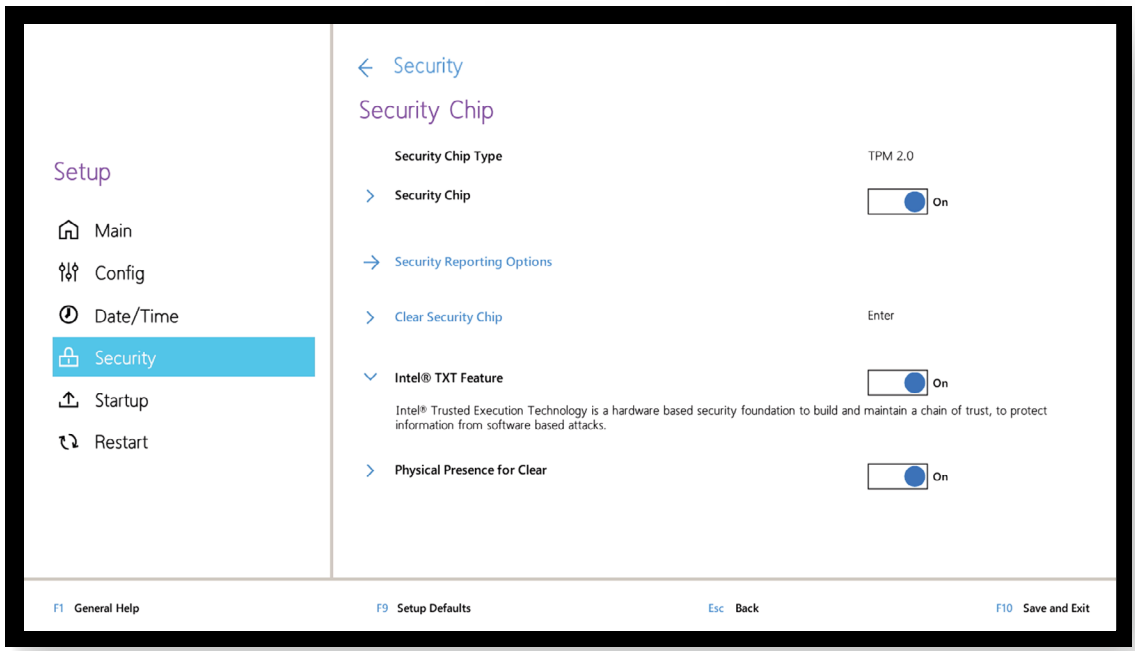

Figure 1. Cryptographic verification of the OS launch environment is done by enabling Intel TXT, shown here (details vary by OEM)

Maximize remote manageability

IT departments have scrambled to support the sudden surge in remote workers. Now you need to prepare your infrastructure for the likelihood that the new hybrid workforce reality will be permanent. With an estimated 70 percent of the workforce expected to be working remotely at least five days per month by 2025, remote manageability of your PC fleet will be critical into the foreseeable future.[1]

Intel vPro platform hardware and firmware provide a comprehensive set of remote-manageability capabilities named Intel AMT. Intel AMT is the only solution with remote remediation to 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:

- 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 Intel vPro platform–based PCs, you might already be taking advantage of Intel AMT manageability features. There are also Intel software tools that can help you provision, set up, and manage PCs using Intel AMT. Intel Manageability Commander and MeshCommander are consoles for managing devices with Intel AMT on premises. MeshCentral2 is the open source, multi-platform, self-hosted, feature-packed website for remote device management. 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 into 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 by using Intel EMA. Intel Management Engine (Intel ME) version 11.8 or newer is needed for out-of-band management.

Intel EMA is readily downloadable software 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 the Intel vPro platform. Intel EMA allows you to remotely cycle power via Intel AMT on a PC over a wired or Wi-Fi connection from the cloud to upgrade or patch software on a device 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. The 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 remotely and more securely manage devices. The starting point for installing on premises is an installation .exe file and a familiar installation wizard. Intel provides complete instructions for on-premises installation here.

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:

- Deployment guide for Amazon Web Services
- Deployment guide for Microsoft Azure
- Deployment guide for Google Cloud Platform

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 configure network security groups with security rules.
4. Deploy an Azure SQL Database instance and add to the existing virtual network.
5. Deploy a Windows Server 2019 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 2019 Datacenter VM, using the existing Azure SQL Database as the database endpoint.

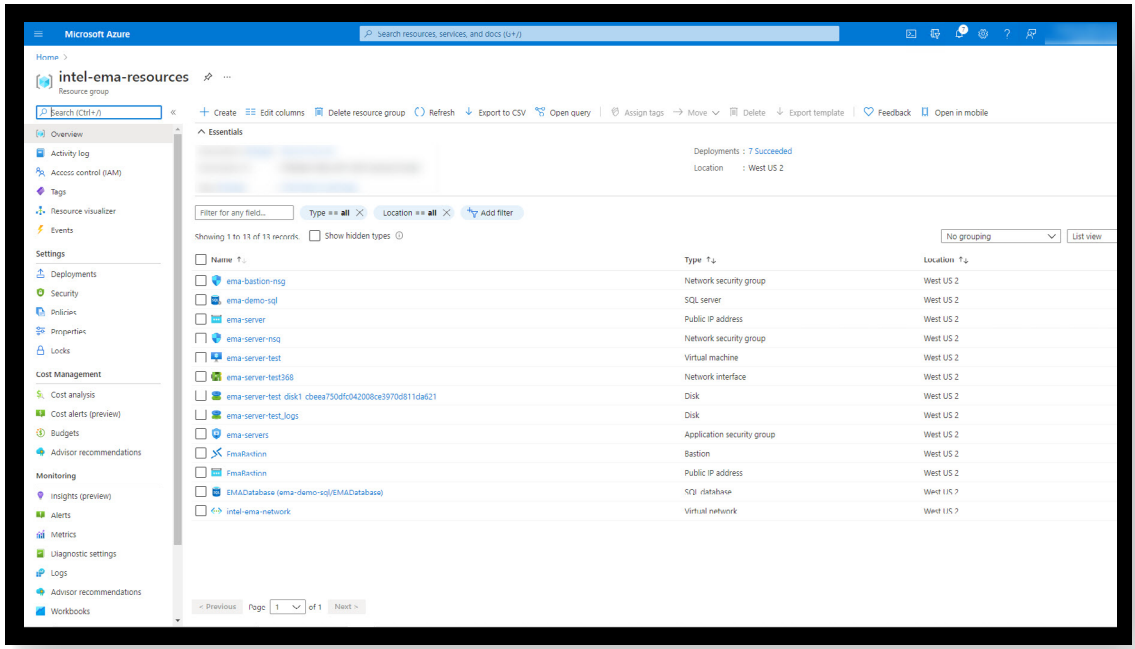

Figure 2. Example of an installed Intel EMA environment on Azure

Note that Intel's Cloud Start Tool can create a VM in Azure with all necessary background services and Intel EMA automatically installed in a default configuration. This 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'll 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'll create endpoint groups within tenants and the user accounts for the users who can manage them. Then you'll 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 IP address of your Intel EMA VM, and log in with the admin user credentials. (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'll 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. Then you can 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.

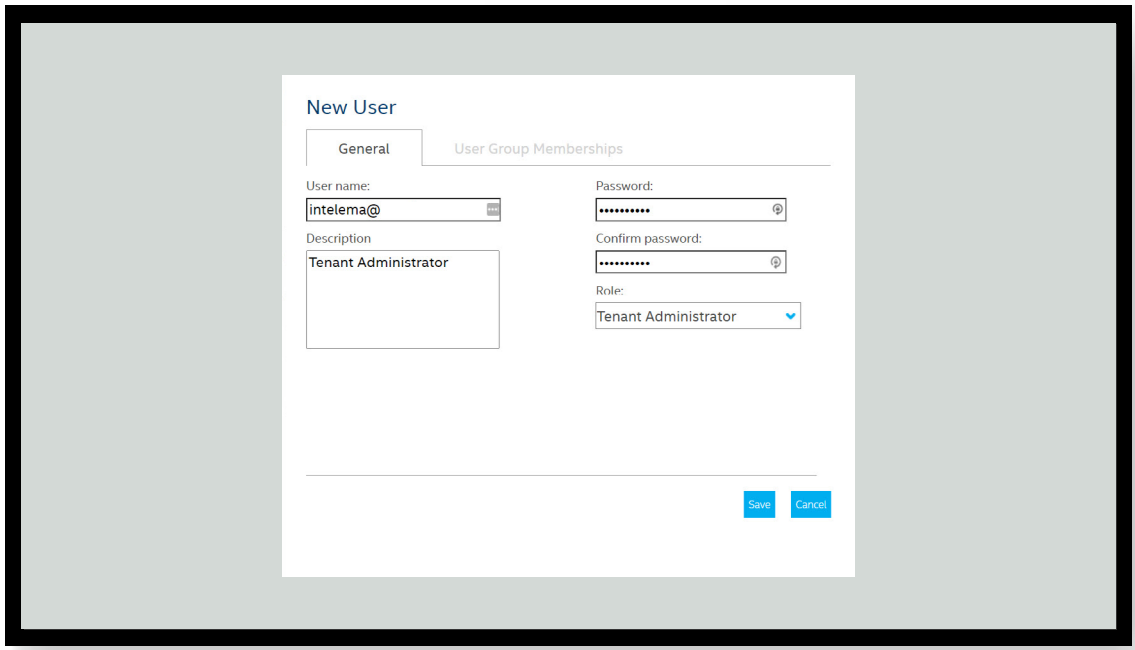

Figure 3. Add users to your Intel EMA tenant, starting with a Tenant Administrator

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 select all the features.
5. It's important to complete the Wi-Fi section if you'll be supporting employees working from home. In the Wi-Fi section, be sure the boxes for both **Synchronize with the host platform WiFi profiles** and **Enable WiFi connection in all system power states (S1-S5)** are selected, and then click **Save**.

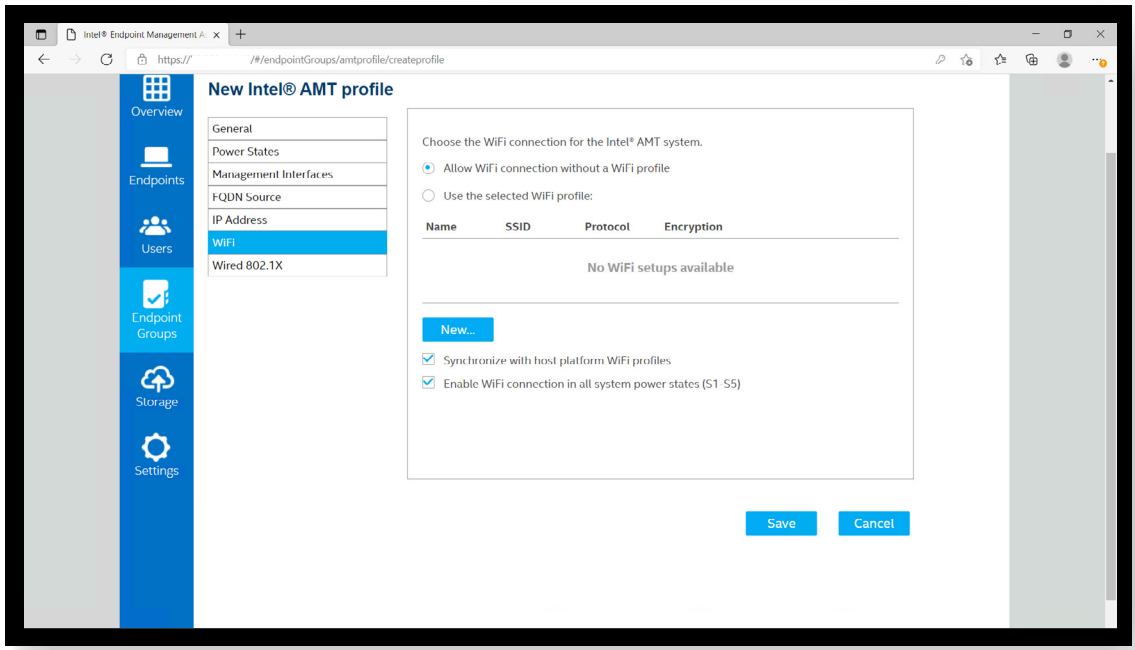

Figure 4. When creating an Intel AMT profile, be sure to complete the Wi-Fi section so you can support employees working remotely

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** check box and make sure it shows your Intel AMT profile and host-based provisioning (HBP) as the activation method.
5. Fill in the **Administrator Password**, and then click **Save**.

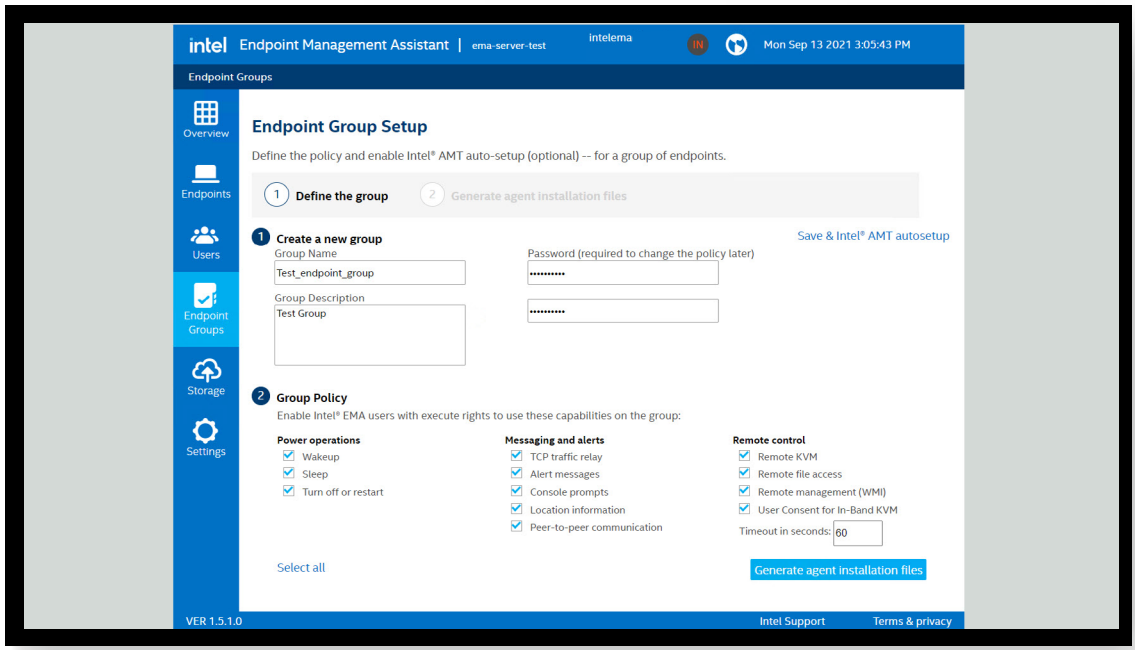

Figure 5. Enable Intel EMA users with execute rights on endpoints in an endpoint group

Generate and install agent installation files

After you've created an endpoint group and defined the group policy for that group, you'll 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'll need those two files together—EMAAgent.exe and EMAAgent.msh—in order 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.

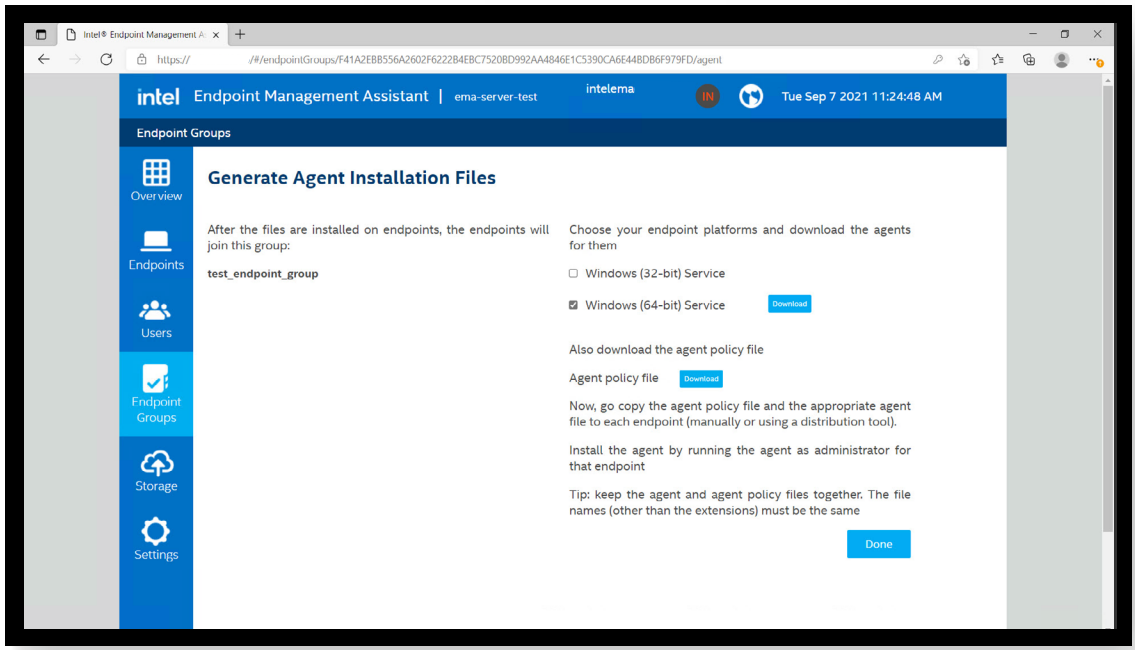

Figure 6. Download the two files you'll need to install the Intel EMA agent on each endpoint machine in the endpoint group

Common management tasks with Intel EMA

You can use Intel EMA for help-desk functionality and IT-task automation. You can use it to reimage a device remotely, and you can 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 that can be valuable to your help-desk operations.

The **General** tab gives you all kinds of information about the chosen endpoint machine, and it lets you control that machine's power state, search its files, provision Intel AMT, mount 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 when the remote OS is up and running. You'll want to explore this section to discover all the ways it can enhance your ability to provide support remotely, just as if you were deskside.

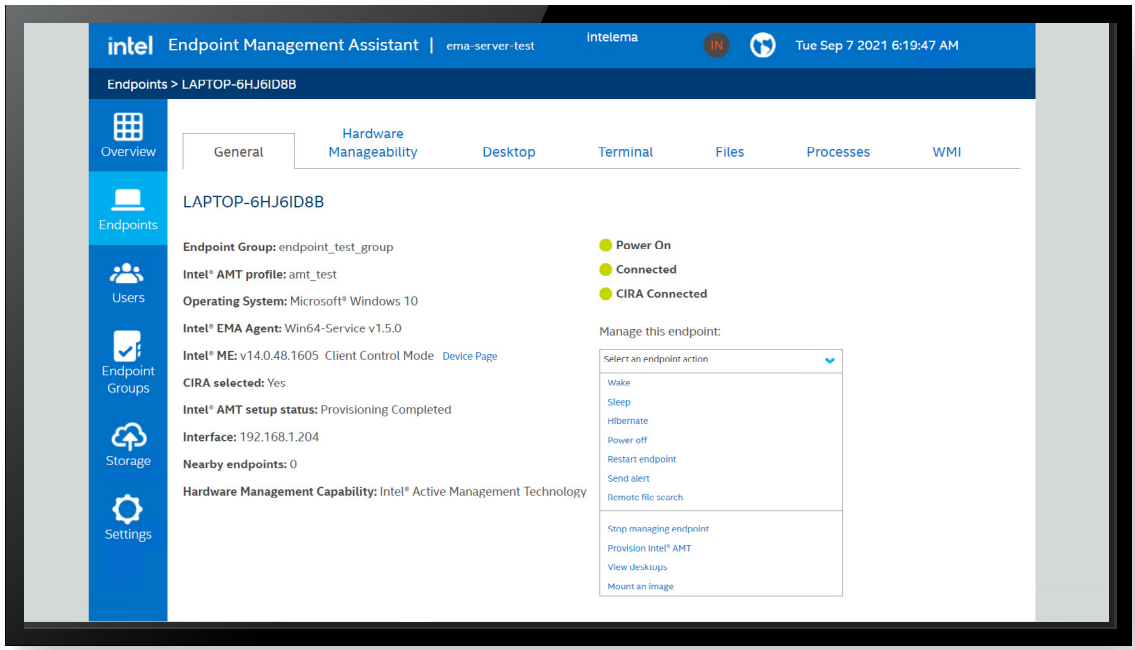

Figure 7. Explore the **Endpoints** section to discover how Intel EMA can enhance your remote support operations

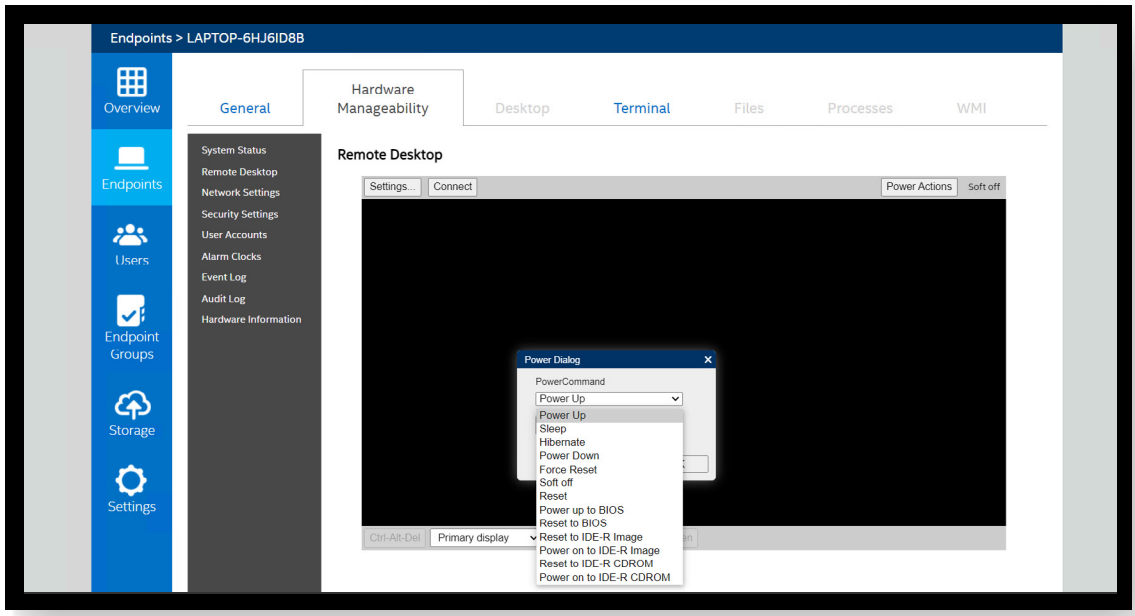

Figure 8. The Hardware Manageability tab provides access to out-of-band Intel AMT functions such as Power Actions

Reimage a device remotely

One remote capability worth special attention is reimaging a device. Whether 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 save your IT department substantial time by eliminating 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**.

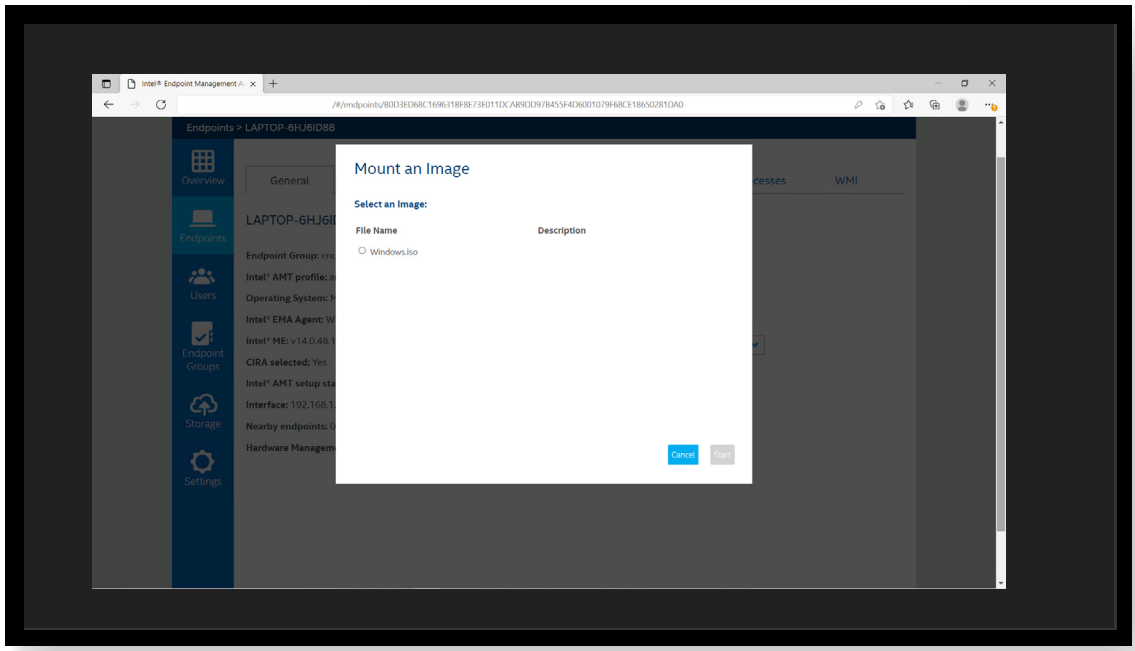

Figure 9. Mount an image to reinstall Windows on a device, wherever that device is located

Monitor the Intel EMA server log

To access the Intel EMA server log, you'll 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 **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.

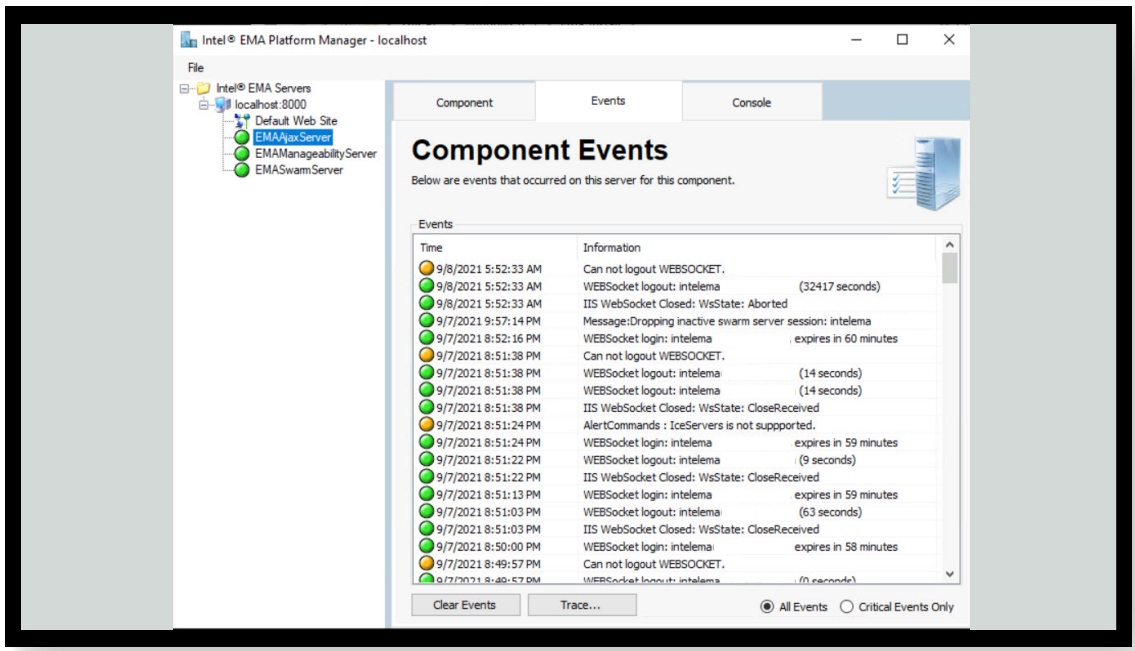

Figure 10. Monitor server events in real time and trace events on server components to troubleshoot issues

Conclusion

The Intel vPro platform brings a wide range of benefits to your company. Many performance, stability, security, and manageability advantages of the Intel vPro platform are already built into the products you buy from device manufacturers and software vendors. You can get even better security and manageability by deploying Intel EMA to take full advantage of the Intel AMT built into Intel vPro platform devices.

Want to learn more? Talk to our experts.

[1] Vox. "How remote work is quietly remaking our lives." October 2019. vox.com/recode/2019/10/9/20885699/remote-work-from-anywhere-change-coworking-office-real-estate.

Printed in USA 1021/RR/PRW/PDF Please Recycle 348687-001US