# PROWESS

# TESTING INTEL vPRO® PLATFORM-ENABLED CLIENT MANAGEMENT FROM THE CLOUD

Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) 1.3.1 shines in ease-of-use and efficiency tests conducted by Prowess Consulting.

# **Executive Summary**

The Intel vPro® platform, which spans Intel® Core<sup>™</sup> vPro® processors and Intel® Xeon® E3 and E5 processors, includes Intel® Active Management Technology (Intel® AMT). Platforms equipped with Intel® AMT can be managed remotely, regardless of power state or whether an operating system (OS) is functioning. Intel® Endpoint Management Assistant (Intel® EMA) is software that eases the configuration of Intel® AMT and provides a portal for cloud-based management of Intel vPro® platform–based devices on the network.

Engineers at Prowess Consulting undertook installation and testing of Intel<sup>®</sup> Endpoint Management Assistant to validate its functionality and evaluate its ease of use in managing Intel<sup>®</sup> Core<sup>™</sup> vPro<sup>®</sup> processor–based endpoint devices. We configured an environment to test various use-case scenarios with laptop and desktop machines on wired and wireless routers and public hot spots. We conducted two kinds of testing:

- Installing Intel® Endpoint Management Assistant in the test environment
- Performing a wide range of endpoint-management functions using both the graphical user interface (GUI) and the API

Both the installation and endpoint-management tests were carried out successfully. The processes were generally easy and efficient, with minor exceptions noted in the **Test Results** section of this paper.

## The Challenge of Modern Endpoint Management

Imagine that you're responsible for an enterprise IT organization managing 20,000 or so clients. (Perhaps you don't have to imagine very hard.) Your employees are away from their desks 50 to 60 percent of the time.<sup>1</sup> How do you connect to malfunctioning devices to see what users are seeing when they are outside your firewall? How do you update the operating systems on those devices or power cycle a system when it is no longer responding?

As more of the users you support work outside the firewall and access cloud-based services more than the intranet, management and support gets more complicated. You still need a centralized

management tool, but traditional means of using those tools can make it difficult to manage, secure, and update devices without complicating users' lives. This is particularly true when your users have high expectations for their technology (their personal devices "just work," and they expect the same from their work devices). According to a study conducted by Forrester Consulting, security issues are a primary concern for 81 percent of IT managers.<sup>2</sup> The same study showed that productivity is a key issue for 75 percent of IT managers.<sup>2</sup> These are likely issues you wrestle with as well.

Your current remote management solutions don't always keep up with the relentless change of technology. You need something that expands your management reach beyond the operating system on the systems you manage, but that also integrates with existing tools in the market.

#### In-Band Versus Out-of-Band Management

**In-band management** refers to endpoint management that relies upon a software agent running on the endpoint's OS. Such management technology cannot interact with the endpoint when the OS is off or malfunctioning.

**Out-of-band management** refers to management technology that interacts with an endpoint directly on the hardware layer below the OS. Such technology can power on or otherwise interact with endpoints even when their operating systems are not functioning.

Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) is an option you can configure on Intel vPro<sup>®</sup> platform–based devices to let you manage them out of band. That is how, for example, you can remotely power on a device that is off. But many IT organizations struggle with how to set up Intel AMT. How can you configure it quickly and easily? How can you be sure that Intel AMT is configured correctly and will not compromise security?

#### Overview of the Intel® Out-of-Band Endpoint-Management Technology Stack

The Intel® technology stack available with Intel vPro® platform-based devices includes:

- Intel vPro<sup>®</sup> platform—The technology platform within select client computers and Internet-of-Things (IoT) devices that enables easy, cost-effective management
- Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT)—The hardware and firmware included in Intel vPro platform—based devices that enhances remote endpoint management with out-of-band features such as power-on<sup>3</sup>
- Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA)—Software that eases the configuration of Intel Active Management Technology, both inside and outside the corporate firewall, and provides a cloudbased portal using Intel Active Management Technology endpoint-management features

# Intel<sup>®</sup> Endpoint Management Assistant: What Is It?

Configured correctly, Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) in the Intel vPro<sup>®</sup> platform has the potential to extend the reach of endpoint management for IT organizations of all sizes. The keyboard, video, and mouse (KVM) features in Intel Active Management Technology can simplify help-desk and troubleshooting tasks with end users, and the power on/off functionality of Intel Active Management Technology can make out-of-band (OOB) management easy and less intrusive for end users.<sup>3</sup> And Client Initiated Remote Access (CIRA) in Intel Active Management Technology helps secure management data from cloud-based endpoints. To make the capabilities of Intel Active Management Technology easy to incorporate into endpoint management, Intel provides Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA).

Intel Endpoint Management Assistant is designed to make Intel Active Management Technology easy to configure and use for managing devices equipped with Intel vPro technology, which in turn simplifies client management and can help reduce management costs.

### Extend the Reach of Endpoint Management Beyond the Endpoint OS

Intel® Endpoint Management Assistant (Intel® EMA) 1.3:

- Adds cloud-based endpoint management for Intel® Active Management Technology (Intel® AMT)
- Addresses Intel Active Management Technology configuration and use-case scenarios, such as client devices not on an intranet or on a home network
- Lowers the cost of endpoint operations through both in-band and out-of-band remote management
- Deploys in private- or public-cloud services such as Amazon Web Services<sup>®</sup> (AWS<sup>®</sup>), Microsoft<sup>®</sup> Azure<sup>®</sup>, and Google Cloud Platform<sup>™</sup>

# Prowess Put Intel Endpoint Management Assistant to the Test

Modernizing client management and making it easier to extract value from already-deployed devices with the Intel vPro platform would be a big win for IT shops of all sizes, so Prowess decided to put these claims to the test.

#### **Use-Case Scenarios**

To assess these claims about Intel Endpoint Management Assistant, we tested it in four use cases that reflect how IT organizations are expected to manage their modern client infrastructures:

- 1. Desktops on the corporate domain, behind the firewall
- 2. Laptops on corporate domain, behind the firewall
- 3. Laptops in home offices, connected to the internet via wired and wireless routers
- 4. Laptops connected to the internet via a known Wi-Fi® hotspot, such as a cell phone hotspot

### Test Configuration

We installed and configured Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) 1.3.1 (prerelease version) hosted in Microsoft<sup>®</sup> Azure<sup>®</sup> using Windows Server<sup>®</sup> 2016 with Microsoft<sup>®</sup> SQL Server<sup>®</sup> 2016 Developer edition. After setting up the Intel Endpoint Management Assistant tenant and creating an Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) configuration profile, we performed the following steps to set up and configure the hardware for testing:

- 1. Create an Intel AMT profile
- 2. Add wireless profiles to the AMT profile
- 3. Create an endpoint group
- 4. Create users
- 5. Create a user group
- 6. Generate agent-installation files
- 7. Install agent files on endpoints

For details about the test configuration used by Prowess, see Appendix A.

#### Management Tasks Tested

Once deployed, we subjected Intel Endpoint Management Assistant to a battery of tests that included the following management tasks performed both manually via the Intel Endpoint Management Assistant GUI and automatically using Windows<sup>®</sup> PowerShell<sup>®</sup> and the Intel Endpoint Management Assistant API:

- Basic management functions
- Automated power on (out of band)
- KVM (in and out of band)
- Help-desk functionality
- API-based management

For details about the steps taken by Prowess for these use cases, see Appendix B.

# Test Results

Testing included installation, configuration, and performance of device-management tasks.

#### Configuration

We successfully set up the test configuration as described in **Appendix A**. Installation went smoothly except for one early difficulty that we encountered involving permissions issues in Windows Server 2016 on an Azure virtual machine (VM).<sup>4</sup> Once that problem was resolved, the rest of the installation process worked as expected.

Note: We used the default ports (8080, 8000, and so on) for installation, but we would advise others to choose custom ports when they are supported in version 1.3.3.

### Management Tasks

All the use cases and endpoint-management functions described in **Appendix B** performed as expected in our tests. Management tasks were easy to access and use in the Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) GUI. API-based management also performed well, although we did find gaps in the pre-release documentation that made the API a little less easy to use. In particular, Intel provided assistance with authentication methods and, based on our experience, we expect those methods to be better documented in the release version.

#### Conclusion

Our testing demonstrates that Intel Endpoint Management Assistant provides IT administrators with a means to configure Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) on endpoints equipped with the Intel vPro<sup>®</sup> platform quickly and easily. Correctly configured, Intel Active Management Technology helps meet the needs of IT departments for modern manageability. Our testing indicates that Intel Endpoint Management Assistant lives up to Intel's claims about it providing simplified, cloud-based management that can complement the capabilities that organizations already use for endpoint management, including Microsoft<sup>®</sup> System Center Configuration Manager, Ivanti<sup>®</sup> Unified Endpoint Management Software.

#### For More Information

- For more information about Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT), visit **www.intel.com/amt**.
- For specific tools and guidance on implementing Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT), visit www.intel.com/implementamt.

# Appendix A: Test Configuration Details

The Prowess test environment consisted of six managed endpoints: four desktop and two mobile systems using host-based configuration. Figure 1 details the layout of the test environment.



Figure 1. Prowess Consulting's primary test configuration for Intel® Endpoint Management Assistant (Intel® EMA)



Figure 2. Configuration details for the home office test environment



#### Figure 3. Configuration details for the hotspot environment

The following steps describe how we configured the test environment. Note that we used Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) pre-release version 1.3.1. Be sure to refer to the documentation for the version you are installing for the most up-to-date instructions.

#### 1. Create an Intel<sup>®</sup> Active Management Technology Profile

An Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) profile defines the configuration that will be used to provision Intel AMT.

a. On the **Endpoints Groups** panel, click the **Intel® AMT Profiles** tab, and then click **New Intel® AMT Profile**.

Endpoint 0	Groups				
Overview Endpoints	Endpoint group Manage endpoints by placing the and optionally an associated Intr Endpoint Groups	em into an endpoint group wi l® AMT autosetup. Intel® AMT Profiles	here they will share a comm	non set of permissions	Summary view
area and a construction of the second	Search profile names and description	an Q	Manage WiFi profiles	Manage 802.1X profiles	New Intel <sup>®</sup> AMT Profile
	Profile Name		Description		
Endpoint	EPHA HEST		Test APT1 Profil	H.	view
Settings					
	Previous		Page 1 of 1		Next

#### b. Fill out the **General** tab.

Power States         EMA_test         Test Att Profile           Management Interfaces         FOM Source              •             Use Client Initiated Remote Access (CIRA)             Tip: If the computer is behind an HTTP proxy, use TLS security instead.             CIRA intranet suffic:             Emaster com             CIRA Proxy Settings             Domain suffix             Proxy address             Port             No settings added		Profile Name	Profile Description	0
Management Interfaces         FODM Source         IP Address         WRFi         Clink Intranet suffice         Enables computer is behind an HTTP proxy, use TLS security instead.         Clink Intranet suffice         Enables com         Clink A Proxy Settings         Domain suffix       Proxy address         No settings added	Power States	EMA_test	Test ANT Profile	•
FQDN Source         IP Address           IP Address         Tip: If the computer is behind an HTTP proxy, use TLS security instead.           ViRel         CIRA intranet suffic:           Wried 802.1X         Enable Computer is behind an HTTP proxy, use TLS security instead.           CIRA intranet suffic:         Enable Computer is behind an HTTP proxy, use TLS security instead.           CIRA intranet suffic:         Enable Computer is behind an HTTP proxy, use TLS security instead.           CIRA intranet suffic:         Enable Computer is behind an HTTP proxy, use TLS security instead.           CIRA intranet suffic:         Enable Computer is behind an HTTP proxy, use TLS security instead.           CIRA intranet suffic:         Enable Computer is behind an HTTP proxy, use TLS security instead.           CIRA intranet suffic:         Enable Computer is behind an HTTP proxy address           Domain suffix         Proxy address         Port         Address	Management Interfaces			
IP Address VAGress VAGR VAGR VAGR VAGR VAGR VAGR VAGR VAGR	FQDN Source			
WGFI         CIRA intracet suffice           Wired 802.1X         CIRA intracet suffice           CIRA intracet suffice         CIRA Proxy Settings           CIRA Proxy Settings         Domain suffix           Proxy address         Port           No settings added	P Address	Use Client Initiated Remo	te Access (CIRA)	and
Wired 802.1X CIRA Intranet Suffic: Emaint com CIRA Proxy Settings Domain suffix Proxy address Port Art No settings added	WiFi	The trace computer is bern	nu an err re proxy, use rits secondy inst	CIRC.
CIRA Proxy Settings Domain suffix Proxy address Port Ad No settings added	Wired 802.1X	CIRA intranet suffix: Ematest.com		
No settings added		CIRA Proxy Settings Domain suffix Pro	xy address Port	Add
			No settings added	
O Use TLS security		O Use TLS security		

c. Keep the default settings for the **Power States** tab.

General Power States Management Interfaces FQDN Source IP Address WiFi WiFed 802.1X	Choose the power states when Intel® AMT manageability features will be available on the system      Any time the system is connected to power (recommended)      Manageability features will be available in all system power states (50-55)      Only when the system's operating system is running

d. Under the **Management Interfaces** tab, select the check boxes for all options except requiring consent under KVM redirection.

Overview	New Intel® AMT profile	e
Endpoints Users Users Endpoint Groups Settings	General Power States Management Interfaces FQDN Source IP Address WiFi Wifed 802.1X	Select the interfaces you want to open on the Intel <sup>4</sup> AMT system.         ✓       KVM redirection          □       Requires user consent before beginning the KVM session         Timeout for user consent metric (seconds)         ✓       Web-based user interface          ✓       Serial over LAN          ✓       IDE/JUSB redirection
		Save Cancel

e. Under the FQDN Source tab, select Shared with host OS.

Endpoint	Groups	
	New Intel® AMT profi	
Endpoints Users Endpoint Croups Settings	General. Power States Management Interfaces IP Address WiFi Wired 802.1X	Specify the source of the FQDN that will be sent in the Intel <sup>®</sup> AMT device.  Shared with host OS On-board connection-specific DNS ONS lookup Primary DNS
		Save Cancel

f. Under the **IP Address** tab, leave the default **From the DHCP server** selected.

Nerview Indpoints Users Ndpoint Groups Settings	General Power States Management Interfaces FODM Source IP Address WiFel WiFel B02.1X	Select the source for the IP address that will be sent to the Intel <sup>®</sup> AMT system.  From the DHCP server Use a static IP address from host.
		Save Cancel

g. Under the WiFi tab, select Use the selected WiFi profile: and then click New. Fill out the form for the Wi-Fi profile name, SSID, security type, encryption, and security key. Click Save. Select that profile and make sure that Enable WiFi connection in all system power states (S1-S5) is checked.

General Power States	Cho	oose the Wil	Fi connection f	or the Intel® AM	4T system.		
Management Interfac	es O	Allow WiFi	connection wit	thout a WiFi pro	ofile		
FQDN Source	۲	Use the set	lected WiFi pro	ofile:			
IP Address	Na		CCID	Protocol	Encruption		
WiFi		EMA test	ProweccAP	WPA2PSK	ткір	Edit	Delete
Wired 802.1X		Condition.	rioweaper	HIPSEP SIL	THUP	Lun	Detette
it							
		New					
		Synchroniz	e with host pla	atform WiFi pro	files		
		Enable WiF	i connection in	n all system pov	wer states (S1-S	(5)	
ne the WiFi profile profile name:	[			,	<		
ne the WiFi profile profile name: I:				) ]	<		
ne the WiFi profile profile name: ): irity type:	WPAPSK		×.	)	K		
ne the WiFi profile profile name: ): urity type: yption:	WPAPSK		v v	) ]	<		
ne the WiFi profile profile name: :: rrity type: yption: rrity key:	WPAPSK TKIP		<b>v</b>	)	¢		
ne the WiFi profile profile name: t: rity type: yption: rity key: 1X setup:	WPAPSK TKIP	2	> >	)	¢		
ne the WiFi profile profile name: I: Irity type: yption: Irity key: 1X setup:	WPAPSK TKIP	0	> >	) ] ]	(		
ne the WiFi profile profile name: ): irity type: yption: irity key: 1X setup: if: profile can be used in ilee:	WPAPSK TKIP None V	Dorofiles. C	▼ ▼	] ] affect these	¢		
ne the WiFi profile profile name: :: :rity type: yption: urity key: 1X setup: Fi profile can be used in les:	WPAPSK TKIP None V	a) profiles. C	▼ ▼	) ] affect these			
ne the WiFi profile i profile name: i: irity type: yption: irity key: iX setup: iFi profile can be used in les:	WPAPSK TKIP None V	3) arofiles, C.	hanges will	] ] affect these	¢		

h. Under the Wired 802.1X tab, leave the default settings.

New Intel® AMT prof	file
General	
Power States	Choose the wired 802.1X setup for the Intel® AMT system.
oints Management Interfaces	Name Protocol
FQDN Source	
IP Address	No setups available
ers WiFi	
Wired 802.1X	
noint .	
ups	
5	· · · · · · · · · · · · · · · · · · ·
ings	New
	TRU West
	Save Cancel

i. Click **Save** at the bottom of the screen.

#### 2. Create Endpoint Groups

Endpoint groups allow for the grouping of endpoints into buckets.

- a. In Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA), on the **Endpoint Groups** panel, under **Endpoint Groups**, click **New endpoint group**.
- b. Under Group Policy, select all capabilities except for User Consent for In-Band KVM.

U verview	Endpoint Group Setup				
	Define the policy and enable Intel® A	MT auto-setup	(optional) for a group of endp	points.	
ndpoints	1 Define the group	Generate age	nt installation files		
~	1 Create a new group				Save & Intel® AMT autosetu
Users	Group Name		Password (required to change the	policy later)	
	IntelEMA_Test				
1	Group Description				
ndpoint	Test Group				
<b>O</b> iettings	2 Group Policy				
	Enable Intel® EMA users with exec	ute rights to use	these capabilities on the group:		
	Power operations	Mes	saging and alerts	Rem	ote control
	Wakeup	~	TCP traffic relay		Remote KVM
	Sleep	2	Alert messages		Remote file access
	<ul> <li>Turn off or restart</li> </ul>	~	Console prompts	M	Remote management (WMI)
		M	Location information		User Consent for In-Band KVM
		×	Peer-to-peer communication		
	Select all			1	Generate agent installation files

c. Click Generate agent installation files.

d. On the **Intel® AMT autosetup** screen, select the check box to enable Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) auto-setup, enter an administrator password in the appropriate field, and then click **Save**.

Endpoint G	Groups		
Merview 1	Intel® AMT autosetup (IntelEMA_Test)		
	After setting up, any endpoint joining this group and supporting Intel® AMT will automatically be activated. Need to have at least 1 Intel® AMT profile.		
	Enabled		
	Intel® AMT profile: EMA Test		
PETD	Activation Method: Host Based Provisioning (HBP) 💙 👩		
-	Administrator Password: 🔤 🔲 display		
dpoint roups			
~			
ttings			
		_	_
		Save	Cancel

#### 3. Create Users

Create Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) users, and then assign permissions and endpoint groups.

- a. On the Users panel, under the Users tab of the Manage Users section, click New User.
- b. Supply a descriptive **User name** and **Description**, select **Endpoint Group User** for the **Role**, and then click **Save**.

Users	New User					
Manage individual	General	User Group	Memberships		the user to a use	
Intel EMT	User name:		Role:			
	EMA_test_user@	test.com	Endpoint Group User	~		
Search	Description					
User name	Test Endpoint Us	er				
Intelemal Ostratient.co					Group User	
intelema 4@stratient.co					Group User	
Intelematignstratient.co					dmentstrator	0
Intelema@stratient.com					dmunistrator	
Intelema2@stratient.co					Group User	•
			8	ave Cancel		

### 4. Create User Groups

Create a new user group to assign users to an endpoint group.

- a. On the Users panel, under the Users tab of the Manage Users section, click New Group.
- b. Select the users and endpoint groups to add to the user group, and then click Save.

Users	G	eneral Members	Endpoint (	Groups		nrivileges for the endpoint
group.	Select t	he user groups where this user is a	member:			humeRes for the endron
Intel EMT		Endpoint Groups		Can Execute	Read Only	
(Berns		IntelTestGroup1				
Search		IntelEMATest				New Group
Name		IntelEMATest2				
EmaTestGroupT		IntelEMA_Test			۲	0
		Previous Page	1 of 1	N	lext.	
				s	Cancel	

#### 5. Generate Agent-Installation Files

For each endpoint group, generate the installation files that will be installed on the client endpoints.

a. On the Endpoint Groups panel, under the Endpoint Groups tab, select Create Agent
 Files for the appropriate endpoint group.

v	Endpoint group			
	Manage endpoints by placing t and optionally an associated In	hem into an endpoint group where t tel® AMT autosetup.	hey will share a common set of permission	ons Summary view
s	Endpoint Groups	Intel® AMT Profiles		
	Search endpoint groups	Q		New endpoint group
	Name		Endpoint Count	
	IntelTestGroup1		0	
	IntelEMATest		6	•
	IntelEMATest2		0	•
	IntelEMA_Test		0	View Configuration View Endpoints Create Agent Files
			Page 1 of 1	

- b. Select Windows (64-bit) Service—this installs the Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) agent background service, a light agent that runs in a 4 MB footprint. The "console" option allows for agentless installation. The application will run only until the system is rebooted; however, all agent-based in-band functions are disabled on the Intel EMA console. The agent will communicate with the Intel EMA server and get Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) configured automatically.
- c. Click both **Download** buttons to download the agent and the agent policy, and then click **Done**.

Generate Agent Installation Files	
After the files are installed on endpoints, the endpoints will join this group:	Choose your endpoint platforms and download the agents for them
IntelEMA_Test	Windows (32-bit) Console
	Windows (32-bit) Service
	Windows (64-bit) Console
	Windows (64-bit) Service
	Also download the agent policy file
	Agent policy file Develop
	Now, go copy the agent policy file and the apporpriate agent file to each endpoint (manually or using a distribution tool).
	Install the agent by running the agent as administrator for that endpoint
	Tip: keep the agent and agent policy files together. The file names (other than the extensions) must be the same
	Done

### 6. Install Agent Files on Endpoints

The agent software must be installed on the client endpoint in order to access the client using Intel Endpoint Management Assistant. This cannot be done using Intel Endpoint Management Assistant. To install the agent:

### Installation from a Graphical User Interface (GUI)

This is how we installed from a CLI for our testing. In a production environment, the process would likely be automated using software delivery tools.

- 1. Transfer the files generated previously to the target computer(s). These files will be named EMAAgent.exe and EMAAgent.msh.
- 2. Run the **EMAAgent.exe** application with administrator privileges to open the installer.

Intel(R) EMA Agent Installer	
Click the buttons below to install or un installed, the EMA agent runs as a bac The agents facilitate computer manage	install the peer-to-peer EMA agent. When kground service, linking up to other computers. ement and other applications.
Installation Information	
Current Service Status	Running
New Service Version	v0.4.35, 64bit
New Trusted Policy	IntelEMATest2
New Trusted Hash	87501DE1B1046453967D50651AA3243C
Install / Update Uninstall	stall Save EULA Close

- 3. Click Install/Update. The application will close when it is done.
- 4. To test the install, browse to **http://localhost:16990** to see the agent status and information on its connection to the server.

#### Installation from a Command-Line Interface (CLI)

This is how we installed from a CLI for our testing. In a production environment, the process would likely be automated using software delivery tools.

- 1. Transfer the files generated previously to the target computer(s). These files will be named EMAAgent.exe and EMAAgent.msh.
- 2. Using Command Prompt with administrator privileges, locate the files transferred previously.
- 3. Run EMAAgent.exe with the -fullinstall option, this will perform a silent installation.

Administrator: Command Prompt	
Microsoft Windows [Version 10.0.18362.239] (c) 2019 Microsoft Corporation. All rights reserved.	
C:\WINDOWS\system32>cd c:\ema	
c:\EMA≻emaagent.exe -fullinstall EmaAgent installed Started EmaAgent c:\EMA>	

# Appendix B: Use-Case Step Details

Prowess Consulting validated all the management functions described in this section. Basic Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) management functions for a given endpoint can be accessed simply from the Endpoints tab in Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA). Other management functions are accessed differently, as described below.

### **Basic Management Functions**

From the **Endpoints** panel, select the endpoint you wish to access, and then expand the **Select an endpoint action** drop-down menu for the following management tasks:

- Wake
- Sleep
- Hibernate
- Power off
- Restart endpoint
- Send alert
- Stop managing endpoint
- Provision Intel<sup>®</sup> AMT
- Remote file search
- View desktops

Intel	EMT							
M	anaged Endpoi	nts	Intel®	AMT Discovery				
s These e	endpoints have	Intel®	EMA agent ir	nstalled and can be	managed by	Intel® EMA.	Search (name or	model)
Filte	f Clear Filters	End	points			COLINING	Select an endpoint action	•
► End	point Group IntelEMATest		Name	Endpoint Group	Connection	Intel® AMT Version	Hibernate Power off	
Y Con	nection		intelema6	IntelEMATest	Connected	v11.8.65	Restart endpoint	
	Connected		intelema5	IntelEMATest	Not Connected	v11.8.65	Send alert	
Y Pow	er State		IntelEMA4	IntelEMATest	Connected	v12.0.35	Nemore me search	
	On		IntelEMA2	IntelEMATest	Not Connected	v12.0.35	Stop managing endpoint Provision Intel <sup>®</sup> AMT	
🛩 Intel	* AMT Status		IntelEMA1	IntelEMATest	Connected	v12.0.6	View desktops	
	Provisioned		intelema3	IntelEMATest	Connected	v12.0.35	Provisioned	8/14/2019, 4:24: vie
ar Intel	Not provisioned							
	v11.8.65							
	v12.0.35							
	v12.0.6							
				10	Dama	1 of 1		Maxt

You can also execute these management tasks for multiple endpoints from the **Endpoints** panel by selecting the endpoints you wish to access, expanding the **Select an endpoint action** drop-down menu, and then selecting the management function you wish to execute.

	Managed Endpol	nts	Intel <sup>®</sup> /	AMT Discovery				
s	These endpoints have	Intel <sup>®</sup>	EMA agent ir	nstalled and can be	e managed by	Intel® EMA.	Search (name or model)	
	Filter Clear Filters	End	points Name	Endpoint Group	Connection	Intel <sup>®</sup> AMT	Select an endpoint action Wake Sleep Hibemate	
it	Connection Connected Not Connected		intelema6 intelema5	IntelEMATest	Connected Not Connected	Version v11.8.65 v11.8.65	Power off Restart endpoint Send alert Demote file search	
s	Power State     On     Intel <sup>®</sup> AMT Status	NN	IntelEMA4 IntelEMA2	IntelEMATest	Connected Not Connected	v12.0.35 v12.0.35	Stop managing endpoint Provision Intel® AMT	
	Provisioned Not provisioned  Intel <sup>®</sup> AMT Version V11.8.65		intelema3	IntelEMATest	Connected	v12.0.35	Provisioned 8/14/2011	9, 4:24: <b>vi</b>

### Automated Power on (Out of Band)

From the **Endpoints** panel, click **View**, and then click **Intel® AMT** > **Alarm Clocks** > **Add Alarm**. Here you can set up to five alarms and specify intervals, but please be aware that the time is Coordinated Universal Time (UTC).

Endpoints	> intelema6									
Overview	General	Intel® AMT	Desktop	Termir	nal	Files	Processes	WMI		
	System Status	Alarm Clocks								
Endpoints	Nemote Deatrop Network Settings User Accounts Alarm Clocks Event Log Audit Log	Manage the Intel® AMT also No Alarm Clocks are prese Add Alarm Refres	arm clocks for this computer Int h	clocks for this computer						
area and a construction of the second	haroware information									
Endpoint			Alarm Clock			×				
Groups			AMT Date & Time	08/14/2019,	04:48:38 PM					
~			Start Date *	MM DD	YYYYY					
$\mathbf{Q}$			Start Time **	НН	MM					
Settings			Delete On Completio	n Yes 🖲						
			Inflorval * Start Data & Time is relative ** Military Time format (24hrs	Days e to the AV/T Syster el	Hours Date & Time	Minutes				
			Alarm Name must be betwee	en 1 and 32 charbol	Canad					
			L		Gancel	OK				

### KVM (Out of Band)

Connect to a given endpoint from the **Endpoints** panel under **Intel® AMT** > **Remote Desktop**. Accept the default remote desktop settings, and then click **Connect**.

Note: Out-of-band KVM is not available via APIs.

General	Intel® AMT	Desktop	Terminal	Files	Processes	WMI
System Status	Remote Desktop					
Network Settings	Settings Disconnec	t				Powered on Power Actions
Alarm Clocks Event Log Audit Log Hardware Information	ж.					
			∙ Working 15% o Don't turn of	on updates complete f your computer		
	Ctrl-Alt-Del Full Scree	m			(57) Focus	s Off • Primary display •
	General System Status Remote Deaktop Network Settings Alarm Clocks Even Log Hardware Information	General Intel <sup>#</sup> AMT System Statis Remote Desktop Network Stering User Accounts Alum Clocks Event Log Hardware Information Ctri-AR-Del Full Screet	General         Intel® AMT         Desktop           System Status Remote Desktop Network Servings User Accounts Alarm Clocks Feet Log Hardware Information         Remote Desktop         Settings         Disconnect	General         Intel® AMT         Desktop         Terminal           Sented Desktop         Remote Desktop         Sentings         Disconnect           Marm Clocks Evert Lig         Sentings         Disconnect         Working 15%           Hurdware Information         Ctri-Ak-Det         Full Screen         Ctri-Ak-Det         Full Screen	General     Intel <sup>4</sup> AMT     Desktop     Terminal     Files       System Statis Remote Desktop     Remote Desktop     Remote Desktop     Remote Desktop       Network Stering Var Accounts Aturn Clock Poert Cig Net Use Networks reinformation     Disconnect     Vorking on updates 15% complete       Don't turn off your computer     Cet-Att-Del     Full Screen	General     Intel® AMT     Desktop     Terminal     Files     Processes       Remote Desktop     Remote Desktop     Remote Desktop     Remote Desktop     Remote Desktop       Network Steinings User Accounts     Disconnect     Remote Desktop     Remote Desktop       Network Steinings     Disconnect     Remote Desktop     Remote Desktop       Working on updates     15% complete     Don't turn off your computer       On't turn off your computer     Ctti-AB-Del     Full Streen     Ctti-AB-Del

### Help-Desk Functionality

Prowess examined five different kinds of help-desk functionality administered through Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA):

- Audit log review
- Terminal access
- File access
- Process access and review
- Windows Management Instrumentation (WMI) queries

Brief steps for each type are listed below.

#### **AUDIT LOG REVIEW**

From the **Endpoints** panel, click **Intel® AMT** > **Audit Log** > **Click here to load the audit log**. This is a log of what Intel® Active Management Technology (Intel® AMT) actions have been performed on the client system and by which Intel AMT user.

General	Intel® AMT	Desktop	Terminal	Files	Processes	WMI
System Status	Audit Log					
Remote Desktop	Settings					
Network Settings	State		Enabled NoKey			
Alarm Clocks	Storage		21 records) 99 % free			
Event Log	Overwrite Policy		Wraps when full			
Audit Log Hardware Information	Details					
	Refresh					search for event
	Time		Initiator	Action		
	1/25/2010 426/10 PM		\$50s4dmin, 127.0.0.1	Network Time, Intel	PIE Time Set, 1/9/2019, 4:4.	3.12 MM
	7/20/2010 4:36:19 PM		\$50x4dmin, 127.0.0.1	Network Time, Intel	- ME Time Set, 1/25/2019, 33	21.00 PM
	7/37/2019, 6/23/45 PM		\$50xAdmin, 127.0.0.1	Network Time, Intel	ME Time Set, 7/9/2019, 7:2.	7.38.044
	7/23/2010 0:05/23 PM		\$50x4dmin, 127.0.0.1	Network Time, Intel	ME Time Set, 7/23/2019, 8:	06:15 04
	7/25/2010, 9:06:23 PM		\$50x4dmin, 127.0.0.1	Security Admin AC	Access with Invalid Condenti	als Invalid ME area
	7/31/2010 2-23-57 PM		Local	Liter Ont-In Events	Ontale Policy Chaose From I	CVM to None
	7/31/2019 2:24:17 PM		Local	Security Admin Do	visioning Started	and to have
	8/2/2019 6:45:11 PM	_	Local	Security Admin, Pro	provisioning Started MER-	
	8/2/2019 6:45:33 PM		Local	Liser Ont-In Fuents	Ont-In Policy Change From I	WM to None
	8/2/2019 6:50:18 PM		Local	Security Admin Dro	visioning Started	and to redifie
	8/2/2019, 11:50:40 AM		admin 127.0.0.1	Security Admin ACI	Entry Added EMA-user	
	8/2/2019, 11:50:41 AM		admin, 127.0.0.1	Redirection Manage	KVM Enabled	
	8/2/2019, 11:50:44 AM		admin. 127.0.0.1	Security Admin. TLS	Trusted Root Certificate Add	ied
	8/2/2019, 11:50:48 AM		admin. 127.0.0.1	Security Admin. TLS	Trusted Root Certificate Add	led
	8/2/2019, 11:50:53 AM		admin, 127.0.0.1	Wireless Configurat	ion, #3	
	8/3/2019, 11:49:12 AM		\$\$OsAdmin, 127.0.0.1	Network Time, Intel	<sup>9</sup> ME Time Set, 8/3/2019, 6:49	9:12 PM
	8/4/2019, 10:26:35 PM		admin, 172.17.40.202	Redirection Manage	r, KVM Session Started	
	8/4/2019, 10:26:57 PM		admin, 172.17.40.202	Redirection Manage	r, KVM Session Ended	
	8/14/2019, 4:51:58 PM		admin, 172.17.40.202	Redirection Manage	r, KVM Session Started	
	8/14/2019, 4:52:51 PM		admin, 172.17.40.202	Redirection Manage	r, KVM Session Ended	

#### **TERMINAL ACCESS**

From the **Endpoints** panel, click the **Terminal** tab. Click **Start Terminal**. Type **cmd** to start a command prompt.

General	Intel® AMT	Desktop	Terminal	Files	Processes	WMI
IntelEMA1	Disconnect					
	0mMicrosoft	Windows [V	ersion 10.0.17134.	950]		
	(c) 2018 Mi	crosoft Cor	poration. All righ	ts reserved.		
	C:\Program	Files\Intel	\EMA Agent>dir			
	Volume in	drive C is	Windows			
	Volume Ser	ial Number	is 54E3-4C96			
	Directory	of C:\Progr	am Files\Intel\EMA	Agent		
	, , ,					
	09/03/2019	11:07 AM	<dir> .</dir>			
	09/03/2019	11:07 AM	<dir> .</dir>			
	05/20/2019	11:56 AM	2,844,816 Er	maAgent.exe		
	09/03/2019	11:07 AM	12,169 E	maAgent.log		
	05/20/2019	11:50 AM	5,600 E	maAgent.msn		
	09/03/2019	11:07 AM	32.768 m	ash.dh		
	03/03/2013	5 File(	s) 2,893,569	ovtes		
		2 Dir(s	) 225,690,787,840	bytes free		
	C:\Program	Files\Intel	FMA Agent>			
	C+ (F) Ogi alli	Liles (inter	Terre ABerres			

#### **FILE ACCESS**

From the **Endpoints** panel, click the **Files** tab. This allows for full folder navigation and allows you to upload, download, rename, and even delete files on the client system.

General	Intel <sup>®</sup> AMT	Desktop	Terminal	Files	Processes	WMI
IntelEMA1	Disconnect					
Top Up S	elect All New Folder	Rename Delete	Upload Download	Refresh	Show Hidden Files	Sort by name ↑
			Drives- C:\			
Drivers					7/2	4/2019 12:55:21 PM
PerfLogs	Files				3/	4/2019 12:06:50 PM
🗌 🕌 Program I	Files (x86)				7/	24/2019 1:10:11 PM
Users	5				7/2	4/2019 12:59:22 PM 31/2019 7:56:39 AM
U Windows					7/	24/2019 1:08:06 PM
U S Windows	10Upgrade				7/2	3/2019 12:04:57 PM

#### **PROCESS ACCESS AND REVIEW**

From the **Endpoints** panel, click **Processes** > **View Processes**. From this page, you are able to start and terminate Windows services.

Endpoints	> IntelEM	IA1				
Overview	G	eneral Intel® AMT	Desktop Terminal	Files	Processes	WMI
	IntelE	MA1 Disconnect				
Endpoints		inate Launch	Refresh		Search	Q
		Process		ID		
Users		System Idle Process		0		
		System		4		
× 6		Registry		144		
Endpoint		smss.exe		492		
Groups		CS/SS.exe		688		
0		wininit.exe		776		
Settings		csrss.exe		784		
		services.exe		848		
		lsass.exe		868		
		winlogon.exe		928		
		sychost.exe		348		
		sychost.exe		552		
		WUDFHost.exe		568		
		fontdrvhost.exe		788		
		fontdrvhost.exe		996		
		Previous	Page 1	of 11		Next

#### **WMI QUERIES**

From the Endpoints panel, click the WMI tab. Enter your WMI query, and then click Execute.

Type: WMI nu WMI Query ROOTN WMI response: source = 6: Got WMI response, length Caption , ProcessId	hamespace: '\CIMV2 i395F079FE0BA46F68BAEBA i = 4461 bytes, 2 colum	WMI select query: SELECT Caption,ProcessId FROM Win32_Process AS697ECS0DBA8054BC4945B69CD380F7BF19F46304, rId = 0
Type: WMI n WMI Query ROOT WMI response: source = 6: Got WMI response, length Caption , ProcessId	namespace: \CIMV2 \395F079FE0BA46F68BAE8A ı = 4461 bytes, 2 colum	WMI select query:           SELECT Caption,Processid FROM Win32_Process           x5697EC500BA8054BC4945B69CD380F78F19F46304, rld = 0
WMI Query  ROOT WMI response: source = 6: Got WMI response, length Caption , ProcessId	CCIMV2 3395F079FE0BA46F68BAE8A = 4461 bytes, 2 colum	SELECT Caption,ProcessId FROM Win32_Process
WMI response: source = 6: Got WMI response, length Caption , ProcessId	395F079FE0BA46F68BAE8A 1 = 4461 bytes, 2 colum	A5697EC5DD8A8054BC4945B69CD380F78F19F46304, rId = 0
, Aggistry, 120 Registry, 120 Smss.exe, 436 crss.exe, 676 wininit.exe, 760 crss.exe, 784 services.exe, 840 leass.exe, 852 winlogon.exe, 924 svchost.exe, 484 fontdrvhost.exe, 484 fontdrvhost.exe, 484 kUDFHost.exe, 1100 svchost.exe, 1100 svchost.exe, 1156 kUDFHost.exe, 1222		

# API-Based Management Using Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA)

Prowess also validated management functionality using the Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) API through the Postman<sup>®</sup> API-development environment.

#### **Useful References**

In addition to Table 1 below, you may wish to refer to the following documents in the Intel Endpoint Management Assistant documentation:

- **EMAAPIguide.pdf:** Addresses RESTful APIs for out-of-band functions, Intel<sup>®</sup> Active Management Technology (Intel<sup>®</sup> AMT) configuration, and Intel EMA administration
- **EMAJavaScriptLibrariesGuide.pdf:** Addresses in-band functionalities shown in the tabs—Desktop, Terminal, Files, Processes, and WMI

#### Table 1. Intel® Endpoint Management Assistant APIs

Function	API call
PowerOn	/api/v1/endpointOOBOperations/Single/PowerOn
Sleep_Light	/api/v1/endpointOOBOperations/Single/Sleep/Light
Sleep_Deep	/api/v1/endpointOOBOperations/Single/Sleep/Deep
PowerCycle_OffSoft	/api/v1/endpointOOBOperations/Single/PowerCycle/OffSoft
PowerOff_Hard	/api/v1/endpointOOBOperations/Single/PowerOff/Hard
Hibernate	/api/v1/endpointOOBOperations/Single/Hibernate
PowerOff_Soft	/api/v1/endpointOOBOperations/Single/PowerOff/Soft
PowerCycle_OffHard	/api/v1/endpointOOBOperations/Single/PowerCycle/OffHard
MasterBusReset	/api/v1/endpointOOBOperations/Single/MasterBusReset
PowerOff_SoftGraceful	/api/v1/endpointOOBOperations/Single/PowerOff/SoftGraceful
PowerOff_HardGraceful	/api/v1/endpointOOBOperations/Single/PowerOff/HardGraceful
MasterBusReset_Graceful	/api/v1/endpointOOBOperations/Single/MasterBusReset/Graceful
PowerCycle_OffSoftGraceful	/api/v1/endpointOOBOperations/Single/PowerCycle/OffSoftGraceful
PowerCycle_OffHardGraceful	/api/v1/endpointOOBOperations/Single/PowerCycle/OffHardGraceful

#### API-BASED MANAGEMENT TESTING USING INTEL® ENDPOINT MANAGEMENT ASSISTANT (INTEL® EMA)

The Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) was deployed using the "Use Domain Authentication" method. Here we encountered a complication regarding the way in which the authentication method was passed to the Intel EMA server to receive a token. This issue was resolved with Intel assistance and the resolution is expected to be documented in version 1.3.3.

Prowess tested the REST calls using PowerShell and Postman.

<#

.SYNOPSIS

This PowerShell script gets the authentication token from the Intel Endpoint Management Assistant for use in various REST based calls.

.PARAMETER creds

.PARAMETER emaUsername The Intel EMA Tenant Admin

.PARAMETER emaPassword The Intel EMA Tenant Admin password

.PARAMETER emaServer The Intel EMA Server URL

```
.PARAMETER emaCmdApi = "/api/v1/endpoint00B0perations/Single/Hibernate"
This is the Intel EMA API Endpoint URI to hibernate an individual system.
See the Intel EMA Swagger
for additional URIs
#>
```

```
$psCreds = New-Object System.Management.Automation.PSCredential
-ArgumentList $emaUsername, $emaPasswordSecure
$creds = @{username = $emaUsername; password =
$psCreds.GetNetworkCredential().Password; grant_type = "password" }
# This command runs the OAuth authentication method
Invoke-RestMethod -Uri "$emaServer/api/token" -Method Post -Body $creds
# By using this method to create the token request call, this error was
received:
Invoke-RestMethod : {"error":"unsupported_grant_type","error_
description":"Standard OAuth authorization grant is
disabled. Please use getUsingWindowsCredentials URI to get an Access
Token."}
At EMA_Power_PSscript.ps1:80 char:14
+ ...
       $token = Invoke-RestMethod -Uri "$emaServer/api/token" -Method Pos
. . .
                  + CategoryInfo
                           : InvalidOperation: (System.Net.
HttpWebRequest:HttpWebRequest) [Invoke-RestMethod], WebExc
   eption
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.
PowerShell.Commands.InvokeRestMethodCommand
Invoke-RestMethod :
Bad Request
Bad Request
HTTP Error 400. The request is badly formed.
<# In reading this error, it was determined that the correct URI to pass was</p>
$emaServer/api/v1/accessTokens/getUsingExistingToken. However, a token was
still unable to be issued by using that URI and the previous body method.
With the help of Intel, it was noted that the credentials needed to be
passed with NTLM. #>
# The updated PowerShell command in turn was updated as follows:
$creds = Get-Credential
$token = Invoke-RestMethod -Uri
"$emaServer/api/v1/accessTokens/getUsingWindowsCredentials" -Method Get
-Credential $creds
$headers = Q{}
$\phi addrs.Add("Authorization", "$($token.token_type) $($token.access_token)")
```

```
23 | 🛐
```

```
# Once the token was issued, it was used to create the header and further
used for future API calls.
# To get the current Intel® Active Management Technology (Intel® AMT)
profiles, run:
Invoke-RestMethod -Uri "$emaServer/api/v1/amtProfiles" -Method Get
-ContentType "application/json" -Headers $headers
# To get the endpoint ID, run:
$endpoints = Invoke-RestMethod -Uri "$emaServer/api/v1/endpoints" -Method
Get -Headers $headers
$emaEndpointId = $endpoint.EndpointId
# To hibernate a single endpoint, run:
$body = ConvertTo-Json -InputObject @{endpointId = $emaEndpointId }
Invoke-RestMethod -Uri "$emaServer$emaCmdApi" -Method Post -ContentType
"application/json" -Headers $headers -Body $body
```

Using Postman, the authorization method was set to NTLM Authentication.



Once the bearer token was provided, the **Bearer Token** authorization method was used. This REST call gets the endpointGroups.



Using Postman, the endpoint power functionality was controlled by first retrieving the endpoint ID by using a REST call with GET api/v1/endpoints.



After retrieving the endpoint ID, a POST command was sent to api/v1/ endpoint00B0perations/Single/PowerCycle/OffSoft.



With the command issued, the endpoint was powered down.

- <sup>1</sup> GlobalWorkplaceAnalytics.com. "Telecommuting Trend Data." July 2018. https://globalworkplaceanalytics.com/telecommuting-statistics.
- <sup>2</sup> Forrester. "The Total Economic Impact<sup>™</sup> of the Intel vPro Platform." December 2018. Study commissioned by Intel and conducted by Forrester
- Consulting. www.intel.com/content/www/us/en/business/enterprise-computers/vpro-platform-tei-case-study.html. The study surveyed 256 IT
- managers at mid-sized organizations (100–1,000 employees) using Intel vPro<sup>®</sup> platforms in US, UK, Germany, Japan, and China. <sup>3</sup> Keyboard, video, and mouse (KVM) remote control is only available with Intel<sup>®</sup> Core<sup>™</sup> vPro<sup>®</sup> processors with active integrated
- graphics. Discrete graphics are not supported. For more information, visit www.intel.com/amt.
- <sup>4</sup> Our understanding is that Intel<sup>®</sup> Endpoint Management Assistant (Intel<sup>®</sup> EMA) version 1.3.3 will handle domain authentication differently, so this should not be an issue.



The analysis in this document was done by Prowess Consulting and commissioned by Intel.

Results have been simulated and are provided for informational purposes only. Any difference in system hardware or software design of configuration may affect actual performance.

Prowess and the Prowess logo are trademarks of Prowess Consulting, LLC.

Copyright © 2019 Prowess Consulting, LLC. All rights reserved.

Other trademarks are the property of their respective owners.