Executive Summary

The Intel vPro® platform, which spans Intel® Core™ 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® Endpoint Management Assistant to validate its functionality and evaluate its ease of use in managing Intel® Core™ vPro® 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.1 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. The same study showed that productivity is a key issue for 75 percent of IT managers. 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® Active Management Technology (Intel® AMT) is an option you can configure on Intel vPro® 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® platform**—The technology platform within select client computers and Internet-of-Things (IoT) devices that enables easy, cost-effective management
- **Intel® Active Management Technology (Intel® 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-on³
- **Intel® Endpoint Management Assistant (Intel® EMA)**—Software that eases the configuration of Intel Active Management Technology, both inside and outside the corporate firewall, and provides a cloud-based portal using Intel Active Management Technology endpoint-management features
Intel® Endpoint Management Assistant: What Is It?

Configured correctly, Intel® Active Management Technology (Intel® AMT) in the Intel vPro® 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. 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® Endpoint Management Assistant (Intel® 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® (AWS®), Microsoft® Azure®, and Google Cloud Platform™

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® Endpoint Management Assistant (Intel® EMA) 1.3.1 (prerelease version) hosted in Microsoft® Azure® using Windows Server® 2016 with Microsoft® SQL Server® 2016 Developer edition. After setting up the Intel Endpoint Management Assistant tenant and creating an Intel® Active Management Technology (Intel® 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® PowerShell® 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). 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® Endpoint Management Assistant (Intel® 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® Active Management Technology (Intel® AMT) on endpoints equipped with the Intel vPro® 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® System Center Configuration Manager, Ivanti® Unified Endpoint Manager, and KACE® Systems Management Software.

For More Information

- For more information about Intel® Active Management Technology (Intel® AMT), visit www.intel.com/amt.
- For specific tools and guidance on implementing Intel® Active Management Technology (Intel® 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
The following steps describe how we configured the test environment. Note that we used Intel® Endpoint Management Assistant (Intel® 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® Active Management Technology Profile

An Intel® Active Management Technology (Intel® 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**.

---

**Figure 3.** Configuration details for the hotspot environment
b. Fill out the **General** tab.

c. Keep the default settings for the **Power States** tab.
d. Under the **Management Interfaces** tab, select the check boxes for all options except requiring consent under KVM redirection.

e. Under the **FQDN Source** tab, select **Shared with host OS**.
f. Under the **IP Address** tab, leave the default **From the DHCP server** selected.

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

![Wired 802.1X Configuration](image)

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® Endpoint Management Assistant (Intel® 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**.

![Endpoint Group Setup](image)

c. Click **Generate agent installation files**.
d. On the **Intel® AMT auto-setup** screen, select the check box to enable Intel® Active Management Technology (Intel® AMT) auto-setup, enter an administrator password in the appropriate field, and then click **Save**.

![Intel AMT auto-setup screen](image)

3. Create Users

Create Intel® Endpoint Management Assistant (Intel® 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**.
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.

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.
b. Select **Windows (64-bit) Service**—this installs the Intel® Endpoint Management Assistant (Intel® 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® Active Management Technology (Intel® AMT) configured automatically.

c. Click both **Download** buttons to download the agent and the agent policy, and then click **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.

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.
Appendix B: Use-Case Step Details

Prowess Consulting validated all the management functions described in this section. Basic Intel® Active Management Technology (Intel® AMT) management functions for a given endpoint can be accessed simply from the Endpoints tab in Intel® Endpoint Management Assistant (Intel® 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® AMT
- Remote file search
- View desktops
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.

**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).
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.

Help-Desk Functionality

Prowess examined five different kinds of help-desk functionality administered through Intel® Endpoint Management Assistant (Intel® 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.

TERMINAL ACCESS

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

PROCESS ACCESS AND REVIEW

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

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

---

### API-Based Management Using Intel® Endpoint Management Assistant (Intel® EMA)

Prowess also validated management functionality using the Intel® Endpoint Management Assistant (Intel® EMA) API through the Postman® 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® Active Management Technology (Intel® AMT) configuration, and Intel EMA administration
- **EMAJavaScriptLibrariesGuide.pdf**: Addresses in-band functionalities shown in the tabs—Desktop, Terminal, Files, Processes, and WMI
<table>
<thead>
<tr>
<th>Function</th>
<th>API call</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerOn</td>
<td>/api/v1/endpointOOBOperations/Single/PowerOn</td>
</tr>
<tr>
<td>Sleep_Light</td>
<td>/api/v1/endpointOOBOperations/Single/Sleep/Light</td>
</tr>
<tr>
<td>Sleep_Deep</td>
<td>/api/v1/endpointOOBOperations/Single/Sleep/Deep</td>
</tr>
<tr>
<td>PowerOff_Hard</td>
<td>/api/v1/endpointOOBOperations/Single/PowerOff/Hard</td>
</tr>
<tr>
<td>Hibernate</td>
<td>/api/v1/endpointOOBOperations/Single/Hibernate</td>
</tr>
<tr>
<td>PowerOff_Soft</td>
<td>/api/v1/endpointOOBOperations/Single/PowerOff/Soft</td>
</tr>
<tr>
<td>MasterBusReset</td>
<td>/api/v1/endpointOOBOperations/Single/MasterBusReset</td>
</tr>
<tr>
<td>PowerOff_SoftGraceful</td>
<td>/api/v1/endpointOOBOperations/Single/PowerOff/SoftGraceful</td>
</tr>
<tr>
<td>PowerOff_HardGraceful</td>
<td>/api/v1/endpointOOBOperations/Single/PowerOff/HardGraceful</td>
</tr>
<tr>
<td>MasterBusReset_Graceful</td>
<td>/api/v1/endpointOOBOperations/Single/MasterBusReset/Graceful</td>
</tr>
</tbody>
</table>

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

The Intel® Endpoint Management Assistant (Intel® 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.

```powershell
<# .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/endpointOOBOperations/Single/Hibernate"
This is the Intel EMA API Endpoint URI to hibernate an individual system.
See the Intel EMA Swagger for additional URIs #>
```
-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], WebException

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 $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 = @{ }
$headers.Add("Authorization", "($($token.token_type) $($token.access_token))")
# 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/endpoint0OB0Operations/Single/PowerCycle/OffSoft`.

With the command issued, the endpoint was powered down.

---


3 Keyboard, video, and mouse (KVM) remote control is only available with Intel® Core™ vPro® processors with active integrated graphics. Discrete graphics are not supported. For more information, visit www.intel.com/amt.

4 Our understanding is that Intel® Endpoint Management Assistant (Intel® 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.