Secure and manage PCs better with new features of the Intel® vPro™ platform

Upgrading to new HP systems powered by 7th generation Intel® Core™ vPro™ processors can improve security and management

Whatever your business, it is imperative that your IT staff secures the confidential documents on your employees' PCs and protects against data and identity theft. You also need efficient ways to manage all those PCs. For organizations in need of new ways to secure and manage devices, the latest version of the Intel Core vPro platform offers a range of features and technologies.

In the Principled Technologies labs, we explored three new PCs from HP, all of which feature 7th generation Intel Core vPro processors: the HP EliteDesk 800 G3 Desktop Mini PC, the HP EliteDesk 800 G3 Tower PC, and the HP EliteBook x360 1030 G2. We also investigated three older HP systems powered by 3rd generation Intel Core vPro processors. We found that the new systems came packed with features that improve both security and management and were not present in the older systems.

Explore this paper to see how upgrading to new systems powered by 7th generation Intel Core vPro processors can help your business.

Boost security

with Intel Authenticate technology and HP Client Security

Manage PCs remotely

with USB-R storage redirect and wireless provisioning

And more

A more convenient experience for users and Microsoft® Windows® 10 Pro

Upgrade to gain key features

The new HP systems we tested were based on the latest version of the Intel vPro platform, a set of hardware and software technologies designed for enterprise-class laptops and desktops. They also used Intel® Active Management Technology (Intel® AMT). We provisioned the systems in our lab and looked at the Intel vPro platform technologies that can help IT administrators better manage PCs on their company network and can boost PC security. These include Intel® Authenticate technology, which adds hardware-hardened authentication factors to PCs to prevent unauthorized access; wireless provisioning, which lets administrators provision systems without cables; and USB-R storage redirection, which allows administrators to load and run a system image stored anywhere on their network on an Intel AMT-provisioned PC.

In the following sections, we'll look more closely at these features, which are available on systems powered by 7th generation Intel Core vPro processors, but not on those powered by 3rd generation Intel Core vPro processors.

The new HP systems we tested suit a variety of employee needs.

(Note: We have based the descriptions below on marketing material from HP; PT did not test system performance.)

HP EliteDesk 800 G3 Desktop Mini PC

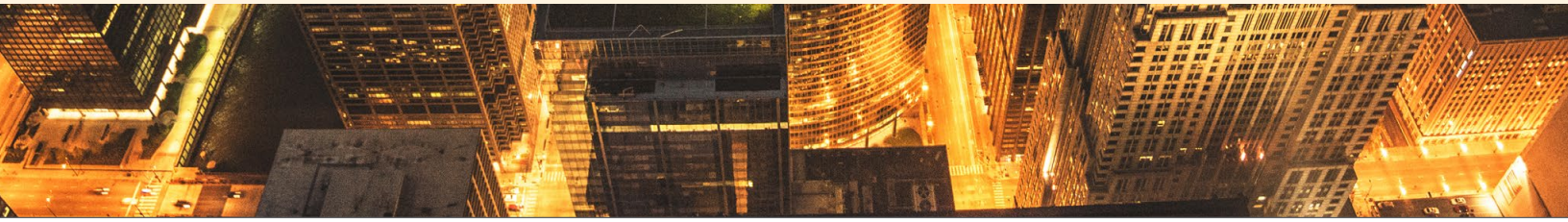
This is the smallest desktop offering from HP. The business-class PC is designed for the enterprise end-user and comes with new Intel Optane memory for large, speedy drives.

HP EliteDesk 800 G3 Tower PC

This VR-ready desktop comes with the option to increase performance even further with 91W processors, up to 64 GB of DDR4 memory, and high-end discrete graphics. It has five bays and four full-height slots, allowing for future expansion..

HP EliteBook x360 1030 G2

The EliteBook offers business-class performance and flexibility, letting users work in a variety of different modes suited to a variety of environments.



How the Intel vPro platform can help your business: Security

With Intel Authenticate technology, 7th generation Intel Core vPro processors offer an identity protection solution not included in 3rd generation Intel Core vPro processors:

Bluetooth® authentication and walk-away lock

We tested this feature on the three new HP systems, all of which had Intel Authenticate technology. Once our technician installed the Intel Authenticate app on a smart phone, the Intel Authenticate solution would not unlock the system unless it could detect that smartphone, which connects to the computer via Bluetooth. Additionally, when he took the phone more than three meters from the system, the screen locked automatically, preventing unauthorized access.

Protected PIN

All three new HP systems used Protected PIN. Each time our technician logged into a system, the numbers on the number pad appeared in a new, randomized sequence that was invisible to the OS. Even spyware cannot read or steal this type of PIN.

Fingerprint scan

The HP EliteBook x360 1030 G2 we tested was equipped with a fingerprint scanner. After our technician enrolled his fingerprint in HP Client Security, he could log into the system using his fingerprint. Through fingerprint scanning, Intel Authenticate technology ties an employee device to that person's very biology, greatly reducing the likelihood of unauthorized access.

Intel AMT Location

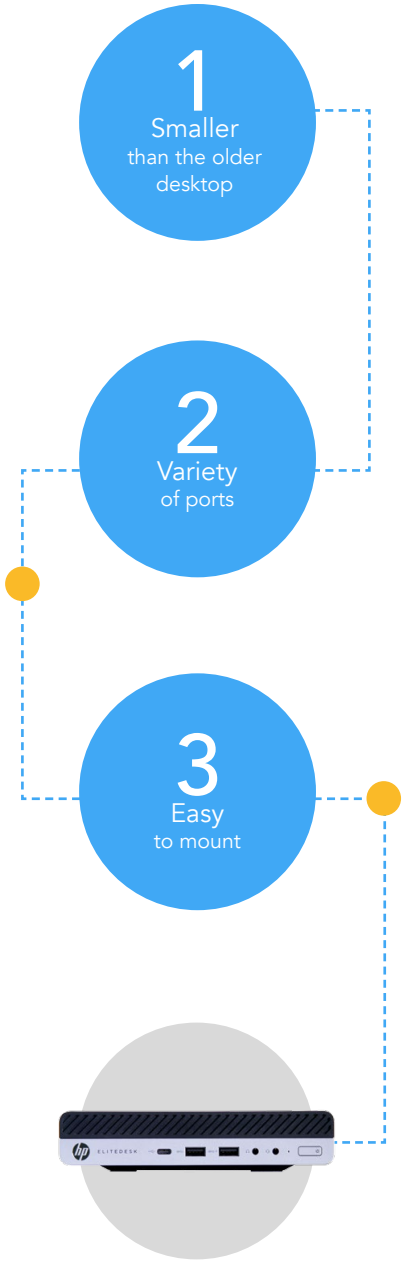
All three new systems had Intel AMT Environment Detection, which the Intel Authenticate solution can utilize to allow only systems that are connected to the corporate network to log on. After enrolling the AMT network logical location factor, our technician disconnected the system from the network and Intel Authenticate technology successfully blocked access to the system.

HP Client Security

HP Client Security lets users and admins customize each Intel Authentication factor in the HP Client Security Interface. Also, via the Device Permissions section, the administrator can specify access requirements for removable media. Our technician disabled the CD/DVD-ROM drives for standard users, while allowing them for administator accounts. IT can also disable Bluetooth or COM ports. Just in Time Authentication (JITA) helps prevent unauthorized users from running malicious software while users are away from their systems. When you insert a CD or removable storage device, the system presents a Windows notification. Only once a logged-in user clicks the notice will the system mount the media. Our technician configured these options, verified that USBs and CD-ROMs ran only with user approval, and set up Intel Authenticate factors using HP Client Security.

HP EliteDesk 800 G3 Desktop Mini PC

Here are just a few benefits companies can realize from the HP EliteDesk 800 G3 Desktop Mini PC:



HP EliteDesk 800 G3 Tower PC

Upgrading to the HP EliteDesk 800 G3 Tower PC can offer companies a number of benefits:

1. Takes up less space than the older desktop
2. HP Client Security features
3. Offers the option for comprehensive support plan

How the Intel vPro platform can help your business: Remote management

When your IT staff manages hundreds or even thousands of devices, routine tasks such as provisioning can eat up time that could be better spent on more strategic projects. The 7th generation Intel Core vPro processors include several remote management features that the 3rd generation Intel Core vPro processors did not:

Wireless provisioning

The wireless provisioning feature let our technician provision the HP EliteBook x360 1030 G2, which lacked a wired Ethernet connection, using no cables at all. This feature, which also works for desktops, allows the system to receive AMT commands via the wireless adapter. This lets admins perform certain management tasks on systems connected to the corporate network over Wi-Fi. Not having to worry about proximity to a wired network connection gives companies flexibility to place systems, especially desktops, in whatever location is most convenient.

USB-R storage redirection

This feature enables administrators to present remote drives to a PC as if they were connected by USB port. They can install disk images remotely, which saves them time on each PC. To boot to an image without USB-R storage redirection, an administrator must travel to the system and insert a CD or USB drive containing the image. With USB-R storage redirection, an admin need only open the Intel AMT management console to install that same image to the machine.

Intel Manageability Commander

Our technician installed Intel Manageability Commander on our management server. From the console, admins can control all of their AMT-provisioned machines—both old and new—from a single console. Once they have connected Intel Manageability Commander to the target system, they can view and configure settings, initiate KVM connections, edit network and security settings, and check audit and event logs to investigate the system's history.

Upgrade to a more convenient experience for your users

Intel vPro platform technologies don't just help your IT administrators—they also help your end users. For example, remote management means they don't have to worry about servicing their own PCs. Also, with biometrics and smart phone proximity, Intel Authenticate technology offers convenient ways for them to log into their PCs.

Available across the board

In the previous sections of this report, we've highlighted the features available to companies upgrading to the new HP systems powered by 7th generation Intel Core vPro processors. Here, we look at some features available on these systems as well as the HP systems powered by 3rd generation Intel Core vPro processors.

Remote push patches

Intel AMT has a built-in alarm feature that awakens PCs whenever your administrator is ready to push a patch to a set of systems.

Control employee PCs remotely

The Keyboard Video Mouse (KVM) Remote Control feature allows administrators to see a user's screen remotely and take control of the user's keyboard and mouse, without needing to be physically present.

System Defense

Administrators can monitor and take action on network traffic packets, and can limit network access for a suspect system.

Power control

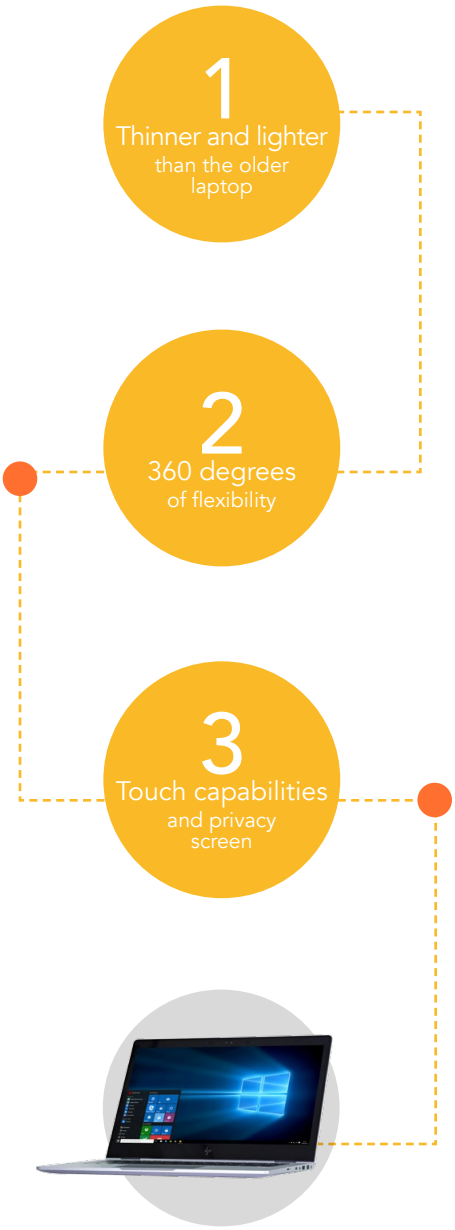
IT can remotely turn AC-powered machines off to save energy or on to service them.

Out-of-band management capabilities

This feature allows admins to control or remediate a PC when the OS is down, locked, or absent from a system. Even if the network connection is disabled in the OS, the administrator can continue issuing commands via Intel AMT.

HP EliteBook x360 1030 G2

Upgrading to this newer HP laptop system can deliver the following benefits.



Microsoft Windows 10 Pro

Upgrading to Windows 10 gives you access to the latest features from the popular business OS, including Windows Hello and touch functionality.

Conclusion

If your employees are using PCs powered by 3rd generation Intel Core vPro processors, you have much to gain by upgrading. Keeping employee computers—and the data on them—secure helps avoid potentially devastating data breaches. New HP systems powered by 7th generation Intel Core vPro processors have Intel Authenticate technology, which adds layers of security to these systems and, by extension, to your company. You also benefit when the IT staff tasked with managing the PCs throughout the organization have access to the efficiency-boosting remote management technologies available on these new systems. An investment in systems powered by 7th generation Intel Core vPro processors can be a smart business decision.

On April 24, 2017, we finalized the hardware and software configurations we tested. Updates for current and recently released hardware and software appear often, so unavoidably these configurations may not represent the latest versions available when this report appears. For older systems, we chose configurations representative of typical purchases of those systems. We concluded hands-on testing on May 2, 2017.

Appendix A: System configuration information

Notebook systems

System	HP EliteBook x360 1030 G2	HP EliteBook 2570p
Processor		
Vendor	Intel	Intel
Name	Core	Core
Model number	i7-7600U	i5-3320M
Core frequency (GHz)	2.80	2.60
Number of cores	2	2
Cache	4MB L3	3MB L3
Memory		
Amount (GB)	8	8
Type	DDR4	DDR3
Speed (MHz)	2,133	1,600
Integrated graphics		
Vendor	Intel	Intel
Model number	HD Graphics 620	HD Graphics 4000
Storage		
Amount (GB)	256	320
Type	SATA SSD	SATA HDD
Connectivity/expansion		
Wired internet	N/A	Intel 82579LM
Wireless internet	Intel Dual Band Wireless-AC 8265	Centrino® Advanced-N 6205
Bluetooth	4.0	4.0
USB	1 USB Type-C with Thunderbolt™, 2 x USB 3.1	1 x USB 3.0, 2 x USB 2.0
Thunderbolt	1	N/A
Video	1 x DisplayPort	1 x DisplayPort, 1 x VGA
Battery		
Type	Lithium-polymer	Lithium-ion
Size	Integrated	Integrated
Rated capacity (Wh)	57	62

System	HP EliteBook x360 1030 G2	HP EliteBook 2570p
Display		
Size (in.)	13.3	12.5
Type	FHD UWVA ultra slim	LED Backlight
Resolution	1,920 x 1,080	1,920×1,080
Touchscreen	Yes	No
Operating system		
Vendor	Microsoft	Microsoft
Name	Windows 10 Pro	Windows 7 Pro
Build number or version	15063	7601
BIOS		
BIOS name and version	HP P80 Ver. 92.04	HP F68ISB 40
Dimensions		
Height (in)	0.6	1.1
Width (in)	12.5	12.0
Depth (in)	8.6	8.2
Weight (lbs.)	2.8	3.6

Desktop systems

System	HP EliteDesk 800 G3 DM	HP Compaq Elite 8300 Ultra-Slim Desktop
Processor		
Vendor	Intel	Intel
Name	Core	Core
Model number	i5-7600T	i5-3470S
Core frequency (GHz)	2.70	2.90
Number of cores	4	4
Cache	6MB L3	6MB L3
Memory		
Amount (GB)	8	8
Type	DDR4	DDR3
Speed (MHz)	2,400	1,600
Integrated graphics		
Vendor	Intel	Intel
Model number	HD Graphics 630	HD Graphics 2500

System	HP EliteDesk 800 G3 DM	HP Compaq Elite 8300 Ultra-Slim Desktop
Storage		
Amount (GB)	256	320
Type	SATA SSD	SATA HDD
Connectivity/expansion		
Wired internet	Intel I219-LM	Intel 82579LM
Wireless internet	Intel Dual Band Wireless-AC 8265	NA
Bluetooth	Yes	NA
USB	1 x USB 3.1 Type-C, 4 x USB 3.1	6 x USB 2.0, 4 x USB 3.0
Thunderbolt	N/A	N/A
Video	2 x DisplayPort	1 x VGA, 1 x DisplayPort
Operating system		
Vendor	Microsoft	Microsoft
Name	Windows 10 Pro	Windows 7 Pro
Build number or version	15063	7601
BIOS		
BIOS name and version	HP P21 Ver 92.99	HP K01 Ver 02.99
Dimensions		
Height (in)	1.4	2.6
Width (in)	7.0	9.9
Depth (in)	6.9	10.0
Weight (lbs.)	2.7	6.8

Tower systems

System	HP EliteDesk 800 G3 Tower PC	HP Compaq Elite 8300 TWR
Processor		
Vendor	Intel	Intel
Name	Core	Core
Model number	i7-7700	i5-3470
Core frequency	3.60	3.20
Number of cores	4	4
Cache	8MB L3	6MB L3
Memory		
Amount (GB)	8	8
Type	DDR4	DDR3
Speed (MHz)	2,400	1,600

System	HP EliteDesk 800 G3 Tower PC	HP Compaq Elite 8300 TWR
Integrated graphics		
Vendor	Intel	N/A
Model number	HD Graphics 630	N/A
Discrete graphics		
Number of cards	N/A	1
Vendor	N/A	AMD
Model number	N/A	Radeon HD 6500
VRAM	N/A	1 GB
Storage		
Amount (GB)	256	1,000
Type	SATA SSD	SATA HDD
Connectivity/expansion		
Wired internet	Intel I219-LM	Intel 82579LM
Wireless internet	Intel Dual Band Wireless-AC 8265	NA
Bluetooth	4.0	NA
USB	4 x USB 2.0, 6 x USB 3.1, 1 USB Type-C 3.1	6 x USB 2.0, 4 x USB 3.0
Video	2 x DisplayPort	1 x DVI, 2 x DisplayPort, 1 x VGA
Operating system		
Vendor	Microsoft	Microsoft
Name	Windows 10 Pro	Windows 7 Pro
Build number or version	15063	7601
BIOS		
BIOS name and version	HP P01 00.42	HP K01 v02.51
Dimensions		
Height (in)	14.4	17.6
Width (in)	6.1	7.0
Depth (in)	14.6	17.5
Weight (lbs.)	21.8	24.7

Appendix B: How we tested

Our environment included a preexisting Active Directory® virtual machine (VM) and a second VM with Microsoft System Center Configuration Manager Server as a management VM. We also included a third VM as a root certificate authority. All three VMs used Windows Server® 2012 R2 Datacenter Edition and were joined to our local domain.

Enabling discovery

Configuring the management server to provision Intel Core vPro processor-powered systems

Creating Active Directory accounts for Intel AMT provisioning

1. Log into the Domain Controller using the domain\administrator account.
2. Open Active Directory Administrative Center.
3. Under test(local), click New→Group.
4. On the Create Group window, for Group name, use Kerberos Admins; for Group type, use security.
5. Add Kerberos Admins as a member of the Domain Admins group.
6. Add the computer account of the SCCM server to the Kerberos Admins security group.
7. Create an Organizational Unit for AMT managed systems. We used `AMT`
8. Create a security group called `AMT`
9. Add the Kerberos Admins group to the AMT security group.

Creating certificate templates for out-of-band (OOB) management

1. Log into Certificate Authority as domain\administrator.
2. Click Start→Administrative Tools→Certification Authority.
3. Right-click test-CA-CA, and click Properties.
4. On the General tab, click View Certificate.
5. On the Details tab, scroll to and select Thumbprint. Copy the 40-character code displayed in the details. You will add this information to the AMT BIOS later.
6. To close the Certificate Authority properties, click OK.
7. Expand the Certification Authority, and select Certificate Templates.
8. Right-click Certificate Templates, and select Manage.
9. In the list of available certificate templates, locate Web Server. Right-click the template, and select Duplicate Template.
10. Select Windows 2003 Enterprise, and click OK.
11. Change the template name for the AMT Provisioning certificate. We used `AMT Provisioning`
12. On the Subject Name tab, select Build from this Active Directory Information. Select Common Name, and choose the option UPN.
13. On the Security tab, add the security group created for the SCCM site server. We used the Kerberos Admin group. Add the Enroll permission for the security group. Ensure Domain Admins and Enterprise Admins have Enroll permissions.
14. On the Extensions tab, select Application Policies, and click Edit.
15. Click Add. Click New. Type `AMT Provisioning` for the name, and `2.16.840.1.113741.1.2.3` as the Object Identifier. Click OK.
16. Ensure AMT Provisioning and Server Authentication are listed, and click OK.
17. To close the template properties, click OK.
18. Right-click the AMT Web Server Certificate template, and select Duplicate Template.
19. Select Windows 2003 Enterprise, and click OK.
20. Change the template name for the AMT Web Server Certificate. We used `AMT Web Server Certificate Template`
21. On the General tab, choose the option Publish Certificate in Active Directory.
22. On the Subject Name tab, select Supply in the request.
23. On the Security tab, ensure Domain Admins and Enterprise Admins have Enroll permissions.
24. To close the template properties, click OK.
25. In Certification Authority, navigate to Certificate Templates.
26. For both the AMT Provisioning Template and the AMT Web Server Certificate Template, repeat the following steps:
    a. Right-click the central panel, and select New→Certificate Template to Issue.
    b. Select the AMT Provisioning Template.
    c. Click OK.
27. Log into the management server as domain\administrator.
28. Click Start→Run. Type `mmc`, and press Enter.
29. In the mmc console, click File→Add/Remove Snap-in…

30. Select Certificates, and click Add. Select Computer account. Click Next.
31. Select Local computer, and click Finish.
32. Click OK.
33. Expand Certificates (Local Computer)→Personal→Certificates.
34. In the right panel, click More Actions→All Tasks→Request a new certificate…
35. Click Next.
36. Accept the defaults, and click Next.
37. Select the new AMT Provisioning certificate. Click Enroll.
38. Click File→Add/Remove Snap-in…
39. Select Certificates, and click Add. Select Computer account. Click Next.
40. Select My user account, and click Finish.
41. Click OK.
42. Expand Certificates→Personal→Certificates.
43. In the right panel, click More Actions→All Tasks→Request a new certificate…
44. Click Next.
45. Accept the defaults, and click Next.
46. Select the new AMT Provisioning certificate. Click Enroll.
47. Click File→Add/Remove Snap-in…
48. Select Certificates, and click Add. Select My user account. Click Next.
49. Select Local computer, and click Finish.
50. Click OK.
51. Expand Certificates – Current User→Personal→Certificates.
52. From Certificates (Local)→Personal→Certificates, click and drag the certificate created using the AMT Provisioning template into Certificates – Current User→Personal→Certificates.
53. Click Close.

Installing Intel Setup and Configuration Software (SCS) 11.1

1. Download IntelSCS_11.1.zip from https://downloadcenter.intel.com/download/26505.
2. Extract the contents to `C:\IntelSCS_11.1`.
3. Browse to `C:\IntelSCS_11.1\IntelSCS\RCS`.
4. Run `IntelSCSInstaller.exe`.
5. At the Welcome screen, click Next.
6. Select I accept the terms of the license agreement, and click Next.
7. Check the Boxes for Remote Configuration Service (RCS), Database Mode, and Console.
8. Enter the credentials of the Domain account that will run the service. We used `test.local\administrator`. Click Next.
9. Select db.test.local as the location for the SCS database. This information may populate automatically. Select Windows Authentication, and click Next.
10. On the Create Intel SCS Database pop-up, click Create Database.
11. On the confirmation screen, click Close.
12. On the confirmation screen, leave the default Installation Folder, and click Install.
13. Once the installation is complete, click Next.
14. Click Finish.

Installing the provisioning certificate

1. Open MMC, and add the certificates snap-in, targeted at the local computer.
2. Navigate to Personal, Certificates.
3. Right-click the AMT Provisioning Certificate, and choose Open.
4. On the Details tab, click Copy to file.
5. On the Welcome screen, click Next.
6. On the Export Private Key screen, choose Yes, export the private key, and then choose Next.
7. On the Export File Format screen, check the boxes for Include all certificates in the certification path if possible and Export all extended properties. Click Next.
8. On the Password screen, enter a password to protect the private key.
9. On the File to Export screen, enter `C:\Install_Files\scs-prov-cert.pfx`, and click Next.
10. On the Completed screen, click Close.
11. From an elevated command prompt, run the following command:

```
RCSutils.exe /Certificate Add c:\Install_Files\scs-prov-cert.pfx  /RCSuser NetworkService net stop
rcsserver && net start rcsserver
```

12. To verify, run the following command, and make sure the expected certificate is listed:
```
RCSUtils.exe /certificate view /RCSuser NetworkService /log file C:\rcsout.txt
```

Setting up AMT provisioning with Intel SCS Remote Configuration Service

Creating the wireless configuration profile

1. On the management server, launch the Intel Setup and Configuration Console.
2. Click Profiles.
3. To construct a profile for deployment, click New.
4. For Profile Name, enter a description of the target clients. We used `wireless`. Click OK.
5. On the Getting Started Screen, choose Configuration / Reconfiguration.
6. On the Optional Settings screen, choose the options Active Directory Integration, Access Control List (ACL), Home Domains, Transport Layer Security (TLS), Network Configuration, WiFi Connection, and click Next.
7. On the AD Integration screen, browse for the OU created for the AMT managed devices. We used OU=AMT, DC=test, DC=local. Click Next.
8. On the Access Control List screen, click Add.
9. Select Active Directory User/Group. Click Browse.
10. Add Kerberos Admin, Domain Admins, or other administrative users groups. Click OK.
11. For Access Type, select Remote.
12. Choose the option for PT Administration. Click OK.
13. Click Next.
14. On the Home Domains screen, click Add…
15. In the Domain Properties Window, type the name of your domain. We used test.local. Click OK.
16. Click Next.
17. On the TLS screen, from the drop-down menu, select the Enterprise Certificate Authority, ca.test.local.
18. Select the Server Certificate Template to be used to generate certificates for the AMT devices. We selected AMTWebServerCertificate. Click Next.
19. On the Network Configuration Screen, select Allow WiFi connection with the following WiFi setups.
20. Click Add…
21. On the WiFi Setup screen, enter the information for your device. Our device used WPA and CCMP. Click OK when finished.
22. On the System Settings screen, choose the options Web UI, Serial Over LAN, IDE Redirection, and KVM Redirection.
23. Select Use the following password for all systems. Enter the password for use after provisioning is complete. We used `P@ssw0rd`
24. Enter the RFB Password for KVM sessions. We used `P@ssw0rd`
25. Enter the MEBX password. We used `P@ssw0rd`
26. Uncheck User Consent required before beginning KVM session, and click OK.
27. Check the box for the following options:
    a. Synchronize Intel AMT clock with operating system
    b. Enable Intel AMT to respond to ping requests
    c. Enable Fast Call for Help (within the enterprise network)
28. To edit IP and FQDN settings, click Set.
29. In the Network Settings window, select Use the following as the FQDN, and choose Primary DNS FQDN from the drop-down menu.
30. Choose the option that indicates the device and the OS will have the same FQDN (Shared FQDN).
31. Select Get the IP from the DHCP server.
32. Select Update the DNS directly or via DHCP option 81. Click OK.
33. Click Next.
34. Click Finish.

Adding the configurator to a shared folder

1. Create a shared folder called `amtshare`
2. Copy the file at C:\IntelSCS_11.1\IntelSCS\Configurator to the shared C:\amtshare folder.

Configuring the clients

Repeat the steps below for each system.

Reserving an IP address in DHCP

1. On the Domain Controller, run `dhcpmgmt.msc`.
2. Expand FQDN→IPv4→Scope, and click Reservations.
3. Click More Actions, and click New Reservation.
4. For Reservation Name, enter the host name of the target client.
5. Enter an IP address to reserve.
6. Enter the MAC address of the target client's Ethernet port.
7. Click Add.

Configuring policy on the target client

1. Log onto the target client using domain\administrator.
2. Download and apply applicable driver packages from the manufacturer's website.
3. Open Windows Firewall with Advanced Security.
4. Click Firewall Properties.
5. On the Domain Profile, Private Profile, and Public Profile tabs, set the Firewall state to Off. Click OK.
6. Set the host name and IP of each virtual machine.
7. Run `lusrmgr.msc`.
8. Select Groups.
9. Right-click Administrators, and click Properties.
10. Click Add.
11. Select Object Types, check the box for Computers, and click OK.
12. Type the hostname of the Configuration Manager server, click Check Names, and click OK.

Installing AMT tools on the management server

Installing the Manageability Commander Tool Mesh Edition

1. On the management server, download the tool from the following link: http://www.meshcommander.com/ManageabilityDeveloperToolKit.msi.
2. Run the installer, and complete using all defaults.

Adding systems to the Manageability Commander Tool Mesh Edition

1. Open the Manageability Commander Tool Mesh Edition.
2. Click File, click Add, and click Add Intel AMT Computer…
3. Enter the FQDN, username, and password for the target computer.

Installing the Intel Manageability Commander

1. Download the tool from the following link: https://downloadcenter.intel.com/download/26375/Intel-Manageability-Commander.
2. Run the installer, and complete using all defaults.

Adding systems to the Intel Manageability Commander

1. Open the Intel Mangeability Commander.
2. Click File, and click Add Intel AMT Computer…
3. In the Add Computer Window, give the computer a friendly name.
4. Enter the FQDN of the target system.
5. For Auth/Security, select Digest/TLS. Enter the username and password for the target device.

Installing certificates on target systems

1. On each target system, during boot, press Ctrl + P to enter the Intel Management Engine BIOS Extension (MEBx).
2. Enter the Intel Management Engine (ME) password. The default is `admin`.
3. Navigate to Intel ME General Settings, Remote Setup and Configuration, TLS PKI, and select Manage Hashes.
4. Press the insert key to add a certificate hash.
5. Enter a name for the hash.
6. Enter the 40-character thumbprint recorded before.
7. Exit the MEBx menu.

Provisioning a system with an Intel Core vPro processor (works for both wired and wireless systems)

1. Log into the target system.
2. Navigate to the amtshare folder on the configuration server, and copy the Configurator folder onto the desktop.
3. Open the target folder.
4. Click File, navigate to Open command prompt, and click Open command prompt as Administrator.
5. Run the following command in the elevated command prompt:
   ```
   ACUConfig.exe /Verbose /Output console ConfigViaRCSOnly cm.test.local wireless
   ```

Note: Configuration for our laptop varied from this because we used an internally generated certificate. To configure the system, we first manually input our configuration information into the pre-boot MEBx menu. We then ran the command as usual. This workaround is not necessary for users who purchase their certificates.

Booting to an image using IDE-R

1. On the Configuration Manager server, open the Intel Manageability Commander.
2. Select the target system, and click Connect.
3. Once Connected, select Remote Desktop.
4. On the Remote Desktop screen, click IDER.
5. On the Storage Redirection screen, next to .ISO file, click Choose File.
6. Select an ISO file, and click OK. We choose an ISO for Windows 10 x64 Multiple Editions disk.
7. For Start, select On Reset.
8. Click OK.
9. Click Power Actions.
10. On the Power Actions screen, select Reset to IDE-R CDROM.
11. While booting, press the space bar when prompted to boot to the target image.

Activating Intel Authenticate technology

Downloading the software

1. Download the IntelAuthenticate_SCCM_v2.1.zip from the following site https://downloadcenter.intel.com/download/26501/?v=t.
2. Unzip the files.

Adding required Hardware Inventory Classes

1. Open the Configuration Manager Console. In the Administration workspace, under Overview, select Client settings.
2. Right-click the Default Client Settings, and select Properties.
3. Select Hardware Inventory, and click Set Classes…
4. In the Hardware Inventory Classes window, click Import…
5. Navigate to the SCCMAddonfolder, select sms_def_SCSDiscovery.mof. Click OK.
6. On the Import Summary window, click Import. Then click OK twice.
7. Repeat steps 4 through 6 for the sms_def_AMT.mof file.

Creating the Intel Authenticate Profile

1. Navigate to \Intel_SCS_Framework\Profile Editor\ and run ProfileEditor.exe.
2. In the Profile Editor Window, click New.
3. Under signing certificate, click Select Signing Certificate.
4. Select a valid certificate from the certificate store. Click Select.
5. Under Authentications Factors, select Select Intel AMT Location, Bluetooth Proximity, Protected Fingerprint, and Protected PIN.

6. Select All selected factors. Note that we created multiple profiles to test the various authentication factors both individually and in combination.
7. Under Actions, select Enable OS Login. Select Protected Fingerprint and Protect PIN as factors that can be used for OS login.
8. Under Walk-Away Lock, select Enable Walk-Away Lock.
9. Click Save As… and give the .xml a name. We used AuthProfile.xml.

Installing the Intel Authenticate Plugin

1. In the Intel Authenticate folder, navigate to IntelSCS_SCCMAddon\SCCMAddon, and run SCCMAddon.exe.
2. On the License Agreement screen, click I agree to the license agreement, and click Next.
3. On the SCCM Settings screen, verify the settings, and click Next.
4. On the Select Components screen, click the button under path for each component, and set them as follows:
    a. Solutions Framework: \IntelAddons\Solutions Framework\ HostSolutionManagerInstaller.exe
    b. Platform Discovery —\IntelAddons\Platform Discovery\PlatformDiscovery.exe
    c. Intel AMT — \Configurator\ACUConfig.exe
5. Set all components to Install, and click Next.
6. On the Intel AMT screen, click Discover and Unconfigure. Click Next.
7. On the Intel Authenticate screen, click Discover, Unconfigure, and Configure.
8. Browse to select the .xml file. Navigate to the AuthProfile.xml created in the previous section.
9. On the Addon Packages screen, designate a shared location for the packages folder. Click Next.
10. Once complete, click Finish.

Automatically creating the Intel Authenticate Installer Package

1. Open an administrative command prompt in the \Intel_SCS_Components\AuthenticatePackage.
2. Enter the following command:

```
CreateAuthenticatePackage.exe -p
"C:\AddonPackagesFolder\AuthenticateInstallers"
```

Enabling the Task Sequences and deploying the Intel Authenticate software

1. In the Configuration Manager console, in the Software Library workspace, under Operating systems, select Task sequences.
2. Enable the Intel SCS: Platform Discovery task sequence by right-clicking its entry and selecting Enable. Do not continue until the Intel Authenticate: Exists collection has been populated in Device Collections.
3. Enable the Intel SCS: Solutions Framework Installation task sequence. Do not continue until the Intel SCS: Solutions Framework Not Installed collection is populated.
4. Enable the Intel Authenticate: Client Installation task sequence. Do not continue until the Intel Authenticate: Plugin Not Installed collection is populated.
5. Enable the Intel Authenticate: Installation task sequence. Do not continue until the Intel Authenticate: Plugin Available collection is populated.
6. Disable and reenable the Intel SCS: Platform Discovery task sequence. Do not continue until the Intel Authenticate: Plugin Available Collection is populated.
7. Enable the Intel Authenticate: Configuration task sequence.

Enrolling the authentication factors

1. Log into the target system.
2. Open the Intel Authenticate application.
3. On the Intel Authenticate screen, click Next.
4. On the Factors screen, click Next.
5. On the Enroll these factors screen, beside Protected Pin, click Enroll Factor.
6. On the Protected Pin screen, use the digital keypad to enter a PIN, and confirm the PIN.
7. Click Submit.
8. On the Protected Pin Successful Enrollment screen, click Return to home.
9. On the Enroll these factors screen, beside Bluetooth Proximity, click Enroll Factor.
10. On the target device, on the Bluetooth Proximity page, click Proceed.
11. Follow the directions listed to download the appropriate Intel Authenticate mobile application for your smart phone. We used an Android™ device. Once you have installed the app, go to the target device, and click The app is installed, Proceed.
12. On the smart phone, open Intel Authenticate. Click Make Discoverable. Agree to make device discoverable for 120 seconds.
13. On the Bluetooth Proximity screen, select your phone from the list of devices.
14. Once paired, verify that the number matches on both devices.
15. On the Enroll phone screen, click Proceed.

16. On the smart phone, enter the enrollment pin shown on the target laptop and click OK.
17. On the target laptop, click Return to home.

You may now log into the target device using the enrolled factors.

Enrolling the Intel AMT Location factor

1. Log into the target system
2. Open the Intel Authenticate application.
3. On the Intel Authenticate screen, click Next.
4. On the Factors screen, click Next.
5. On the Enroll these factors screen, next to Intel AMT Location, click Enroll Factor.
6. On the Fingerprint screen, click Enroll.
7. On the Fingerprint Enrollment screen, once complete, click Return to Home.

Enrolling the fingerprint factor on a laptop

1. Open HP Client Security.
2. Under Intel Client Security, select Fingerprints.
3. On the Fingerprints screen, click Add a fingerprint.
4. Enroll your first finger by placing the finger on the scanner multiple times until the message "Fingerprint is enrolled" shows below the blue bar.
5. Repeat step 4 with a second finger.
6. Open the Intel Authenticate application.
7. On the Intel Authenticate screen, click Next.
8. On the Factors screen, click Next.
9. On the Enroll these factors screen, next to Fingerprint, click Enroll Factor.
10. On the Fingerprint screen, click Enroll.
11. On the Fingerprint Enrollment screen, once complete, click Return to Home.

You may now log into the target device using the fingerprint factor.

HP Client Security

Configuring HP Client Security

1. Log into the system using an administrator account, and open HP Client Security.
2. In the HP Client Security Window, under Device Security, click Device Permissions.
3. Select the Administrators tab.
4. Next to Device Access Manager with Just In Time Authentication, click the toggle to Enable.
5. Under Removable Media, for CD/DVD-ROM drives, click the drop-down menu under Access, and select Allow – JITA Required.
6. For Removable storage, click the drop-down menu under Access, and select Allow – JITA Required.
7. Click the Standard Users tab.
8. Next to Device Access Manager with Just In Time Authentication, click the toggle to Enable.
9. Under Removable Media, for CD/DVD-ROM drives, click the drop-down menu under Access, and select Deny.
10. For Removable storage, click the drop-down menu under Access, and select Deny.

Administrator account

1. Log into the system with an administrator account.
2. Insert a portable USB drive. Verify that the device is not visible in File Explorer.
3. When the Device Access Manager notification appears, click the notification, and verify that the device is visible in File Explorer.
4. Insert a portable CD/DVD drive with any CD. Verify that the device is not visible in File Explorer.
5. When the Device Access Manager notification appears, click the notification, and verify that the device is visible in File Explorer.

Standard user account

1. Log into the system with a standard user account.
2. Insert a portable USB drive. Verify that the device is not visible in File Explorer.
3. Insert a portable CD/DVD drive with any CD. Verify that the device is not visible in File Explorer.

Appendix C: Intel Authenticate technologies availability

The following chart shows the availability of the four Intel Authenticate technologies across the six systems we tested.

		Bluetooth proximity	Intel AMT Location	Fingerprint scanner	Protected PIN
Notebook	HP EliteBook x360 1030 G2	✓	✓	✓	✓
	HP EliteBook 2570p	✗	✗	✗	✗
Desktop	HP EliteDesk 800 G3 DM	✓	✓	✗	✓
	HP Compaq Elite 8300 Ultra-Slim Desktop	✗	✗	✗	✗
Tower	HP EliteDesk 880 G3 Tower PC	✓	✓	✗	✓
	HP Compaq Elite 8300 TWR	✗	✗	✗	✗

The following screenshots show the results of our running the Intel Authenticate_Check tool to determine which Intel Authenticate technologies each system supported.

Notebook systems

HP EliteBook x360 1030 G2

```
PS C:\Users\administrator\Desktop\CheckTool> .\Authenticate_Check.exe /factors

####### Intel (R) Authenticate Factors Test 2.1.0.24 #######


 Factor:         Bluetooth Proximity (Android)
 Status:         Ready For Use

 Factor:         Bluetooth Proximity (iOS)
 Status:         Ready For Use

 Factor:         Intel AMT Location
 Status:         Supported

 Factor:         Fingerprint
 Status:         Supported
 Reason:         The Soft Fingerprint DLLPath registry key is missing. (This registry key, and the DLL to which it
                 points, are added when Intel Authenticate is installed.)

 Factor:         Protected PIN
 Status:         Ready For Use


Windows 10 (x64) (10.0.15063.296)

Note: For more detailed information, use the /v flag.

#################################################################
PS C:\Users\administrator\Desktop\CheckTool>
```

HP EliteBook 2570p

```
PS C:\Users\administrator\Desktop\CheckTool> .\Authenticate_Check.exe /factors

####### Intel (R) Authenticate Factors Test 2.1.0.24 #######


 Factor:         Bluetooth Proximity (Android)
 Status:         Not Supported
 Reason:         1. No Intel Network Adapter Card found or the driver is not installed
                 2. There is a problem with the Protected Transaction Display (see the Protected PIN factor for details)

 Factor:         Bluetooth Proximity (iOS)
 Status:         Not Supported
 Reason:         1. No Intel Network Adapter Card found or the driver is not installed
                 2. There is a problem with the Protected Transaction Display (see the Protected PIN factor for details)

 Factor:         Intel AMT Location
 Status:         Not Supported
 Reason:         The minimum supported version of Intel AMT is 11.0.15.1003.

 Factor:         Fingerprint
 Status:         Not Supported
 Reason:         A compatible Fingerprint sensor was not detected

 Factor:         Protected PIN
 Status:         Not Supported
 Reason:         1. This factor requires version 21.20.16.4481 or higher of the Intel Graphics Driver.
                 2. This factor requires version 11.6.0.1019 or higher of the Intel ME Software.
                 3. Failed to establish a session with the oath applet. Please try to restart the machine or reinstall
                 up to date "Intel(R) Management Engine" driver


Windows 7 (x64) (6.1.7601.65536)

Note: For more detailed information, use the /v flag.

########################################################################
PS C:\Users\administrator\Desktop\CheckTool>
```

Desktop systems

HP EliteDesk 800 G3 DM

```
PS C:\Users\administrator\Desktop\CheckTool> .\Authenticate_Check.exe /factors

####### Intel (R) Authenticate Factors Test 2.1.0.24 #######


 Factor:         Bluetooth Proximity (Android)
 Status:         Ready For Use

 Factor:         Bluetooth Proximity (iOS)
 Status:         Ready For Use

 Factor:         Intel AMT Location
 Status:         Supported

 Factor:         Fingerprint
 Status:         Not Supported
 Reason:         A compatible Fingerprint sensor was not detected

 Factor:         Protected PIN
 Status:         Ready For Use


Windows 10 (x64) (10.0.15063.296)

Note: For more detailed information, use the /v flag.

########################################################################
PS C:\Users\administrator\Desktop\CheckTool>
```

HP Compaq Elite 8300 Ultra-Slim Desktop

```
PS C:\Users\administrator\desktop\CheckTool> .\Authenticate_Check.exe /factors

####### Intel (R) Authenticate Factors Test 2.1.0.24 #######


 Factor:         Bluetooth Proximity (Android)
 Status:         Not Supported
 Reason:         1. No Intel Network Adapter Card found or the driver is not
                 installed
                 2. There is a problem with the Protected Transaction
                 Display (see the Protected PIN factor for details)

 Factor:         Bluetooth Proximity (iOS)
 Status:         Not Supported
 Reason:         1. No Intel Network Adapter Card found or the driver is not
                 installed
                 2. There is a problem with the Protected Transaction
                 Display (see the Protected PIN factor for details)

 Factor:         Intel AMT Location
 Status:         Not Supported
 Reason:         The minimum supported version of Intel AMT is 11.0.15.1003.

 Factor:         Fingerprint
 Status:         Not Supported
 Reason:         A compatible Fingerprint sensor was not detected

 Factor:         Protected PIN
 Status:         Not Supported
 Reason:         1. This factor requires version 21.20.16.4481 or higher of
                 the Intel Graphics Driver.
                 2. This factor requires version 11.6.0.1019 or higher of
                 the Intel ME Software.
                 3. Failed to establish a session with the oath applet.
                 Please try to restart the machine or reinstall up to date
                 "Intel(R) Management Engine" driver


Windows 7 (x64) (6.1.7601.65536)

Note: For more detailed information, use the /v flag.

##############################################################################
PS C:\Users\administrator\desktop\CheckTool>
```

Tower systems

HP EliteDesk 800 G3 Tower PC

```
PS C:\Users\administrator\Desktop\CheckTool> .\Authenticate_Check.exe /factors

####### Intel (R) Authenticate Factors Test 2.1.0.24 #######


 Factor:         Bluetooth Proximity (Android)
 Status:         Ready For Use

 Factor:         Bluetooth Proximity (iOS)
 Status:         Ready For Use

 Factor:         Intel AMT Location
 Status:         Supported

 Factor:         Fingerprint
 Status:         Not Supported
 Reason:         A compatible Fingerprint sensor was not detected

 Factor:         Protected PIN
 Status:         Ready For Use


Windows 10 (x64) (10.0.15063.296)

Note: For more detailed information, use the /v flag.

##############################################################################
PS C:\Users\administrator\Desktop\CheckTool>
```

HP Compaq Elite 8300 TWR

```
PS C:\Users\administrator\Desktop\CheckTool> .\Authenticate_Check.exe /factors

####### Intel (R) Authenticate Factors Test 2.1.0.24 #######


 Factor:         Bluetooth Proximity (Android)
 Status:         Not Supported
 Reason:         1. No Intel Network Adapter Card found or the driver is not installed
                 2. There is a problem with the Protected Transaction Display (see the
                 Protected PIN factor for details)

 Factor:         Bluetooth Proximity (iOS)
 Status:         Not Supported
 Reason:         1. No Intel Network Adapter Card found or the driver is not installed
                 2. There is a problem with the Protected Transaction Display (see the
                 Protected PIN factor for details)

 Factor:         Intel AMT Location
 Status:         Not Supported
 Reason:         The minimum supported version of Intel AMT is 11.0.15.1003.

 Factor:         Fingerprint
 Status:         Not Supported
 Reason:         A compatible Fingerprint sensor was not detected

 Factor:         Protected PIN
 Status:         Not Supported
 Reason:         1. This factor requires version 21.20.16.4481 or higher of the Intel
                 Graphics Driver.
                 2. This factor requires version 11.6.0.1019 or higher of the Intel ME
                 Software.
                 3. Failed to establish a session with the oath applet. Please try to
                 restart the machine or reinstall up to date "Intel(R) Management Engine"
                 driver


Windows 7 (x64) (6.1.7601.65536)

Note: For more detailed information, use the /v flag.

############################################################################
PS C:\Users\administrator\Desktop\CheckTool>
```

This project was commissioned by Intel Corp.

Principled Technologies®

Facts matter.®