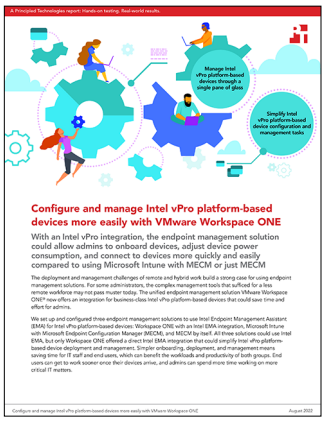

The science behind the report:

Configure and manage Intel vPro platform-based devices more easily with VMware Workspace ONE

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report **Configure and manage Intel vPro platform-based devices more easily with VMware Workspace ONE**.

We concluded our hands-on testing on July 12, 2022. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on July 8, 2022 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to **http://facts.pt/calculating-and-highlighting-wins**. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: Results of our testing

Task	VMware Workspace ONE for Intel vPro via integration with Intel EMA	Hybrid management using Microsoft Intune and Microsoft Endpoint Configuration Manager (MECM)	MECM only
Number of steps to import the Intel Endpoint Management Assistant (EMA) enrollment package	10	39	41

System configuration information

Table 2: Detailed information on the system we tested

System configuration information	15x Lenovo® ThinkPad® T14s Gen 3
Processor	
Vendor	Intel®
Model number	Core® i7-1270P vPro
Core frequency (GHz)	2.20
Number of cores	12
Cache size (MB) and type	18, Intel Smart Cache
Memory	
Amount (GB)	16
Type	LPDDR5-6400
Speed (MHz)	4,800
Integrated graphics	
Vendor	Intel
Model number	Iris Xe Graphics
Storage	
Amount (GB)	512
Type	PCIe SSD
Connectivity/expansion	
Wireless internet	Wi-Fi 6E AX211802.11AX
Bluetooth	5.2
USB	2x USB-A 3.2, 2x USB-C4.0
Thunderbolt	2x Thunderbolt 2
Video	1x HDMI 2.0b
Battery	
Size	14”
Type	IPS, Anti-Glare
Resolution	1920x1200
Touchscreen	Yes
Display	
Size (in.)	14
Type	IPS, Anti-Glare
Resolution	1920x1200
Touchscreen	Yes

System configuration information	15x Lenovo® ThinkPad® T14s Gen 3
Operating system	
Vendor	Microsoft
Name	Windows 10 Pro
Build number or version	19044.1620, 21H2
BIOS	
BIOS name and version	1.11
Dimensions	
Height (in.)	0.65
Width (in.)	12.50
Depth (in.)	8.93
Weight (lbs.)	2.7

Overview

For our testing, we configured one Intel EMA server shared by three different environments. We investigated how each environment interacted with the Intel EMA server. Our three environments included the following:

- A Workspace ONE UEM Console
- Configuration Manager - Local Configuration Manager server only
- Microsoft Intune (co-managed) - Intune and Configuration Manager connected
    - Note that we used the same Local Configuration Manager server for both the second and third environments. We first completed the work on the Configuration Manager environment and then enabled co-management for the Intune (co-managed) environment.

For each environment, we looked for existing integrations with the Intel EMA console and any functionality that existed between the environment and the Intel EMA server. We looked at Intel EMA agent installation, hardware-based power functionality, and KVM functionality. If a feature was not available, we relied on publicly available materials to research that feature's capabilities.

For the cloud infrastructure, we set up and configured the following:

- A VMware Workspace ONE UEM Console (provided by VMware)
- An active Microsoft Azure subscription with P2 licensing and five user accounts with individual EMS (five licenses)

For the local infrastructure, we set up and configured the following:

- An active directory server
- A deployment server to host our local Configuration Manager environment

For our systems under test, we setup and configured the following:

- Five laptops managed by VMware Workspace ONE
- Five laptops joined to the local domain and managed via Configuration Manager
- Five laptops joined to the Azure domain and managed via Intune

Completing general requirements

Creating an Intel EMA VM using the default template

1. Log into Azure.
2. From a web browser, navigate to **https://www.intel.com/content/www/us/en/download/19738/intel-endpoint-management-assistant-intel-ema-cloud-start-tool-for-azure.html.**
3. After an initial selection, Azure may prompt you to log in or sign up.
4. After logging in, Azure will take you to the server creation template.
5. Under Project details, enter your subscription and Resource group.
6. Under Instance details, select a region.
7. Enter the VM name.
8. Enter a username and password, and confirm the password.
9. Under Intel EMA configuration parameters, enter your Global Administrator username, Tenant Administrator username, and Intel EMA password.
10. Once completed, select review, and select create.

Setting up VMware Workspace ONE

Generating client credentials

To integrate Workspace One with the Intel EMA server, provide a Client ID and a Client Secret.

1. Download the Intel EMA API Sample Scripts package from **https://www.intel.com/content/www/us/en/download/19693/30076/intel-endpoint-management-assistant-intel-ema-api-sample-scripts.html.**
2. Extract the zip file, and in the PowerShell ISE, open the following PowerShell script:

```
PowerShell/Snippets/EMA_API-CreateOrDeleteClientCredentialsForTenant.ps1
```

3. Note the following variables:
    a. $emaServerURL is the URL of your EMA instance.
    b. $clientSecret is a complex secret that you create and must meet the following criteria:
        i. At least 12 characters and up to 255 characters
        ii. Contains at least one number
        iii. Contains both lowercase and uppercase alpha characters
        iv. Contains at least one special character
    c. $emaUsername and $emaPassword are credentials of a Tenant Administrator on the Intel EMA instance.
    d. To demonstrate deletion of existing client credentials, set $deleteCreds to $TRUE.
    e. If the Intel EMA instance uses Windows domain authentication, set $useADAuth to $TRUE.
4. The script demonstrates the REST API call used to generate client credentials. The results of the REST API call provide the Client ID, and the script writes to the console.
5. When done correctly, the output should look similar to the following:

    - PS C:\Users\EMADemo> C:\EMA_API-CreateOrDeleteClientCredentialsForTenant.ps1
    - Target Intel(R) EMA Server = https://ema.server.com
    - Retrieved Intel(R) EMA token.
    - Calling POST https://ema.server.com/api/latest/clientCredentials
    - Created Client Id: abcdabcd-12ab-34cd-56ef-abcd1234abcd

NOTE: Ensure that you remove the comment (#) from the beginning of the syntax.

Connecting VMware Workspace One to the Intel EMA instance

1. Log into Workspace One.
2. In the left pane, select Groups & Settings→Integrations.
3. On the Intel EMA/AMT tile, click Set up.
4. On the Intel EMA/AMT Integration Set Up, click Get Started.
5. On the Establish Integration with Intel EMA/AMT, select 2. Select the following Network Partner Credentials:

    - On Current setting, select Override.
    - On Server, enter your EMA server URL (ex., https://ema01.eastus2.cloudapp.azure.com), ensure SSL is enabled, and ensure the port is 443.
    - On API Version, select Latest.
6. Enter the Client ID you obtained from the previous section.
7. Enter your Client Secret.
8. For Child Permission, select Inherit or override.
9. To verify connection to the server, click Test Connection, and click Save Credentials and Connect.

Deploying the Intel EMA agent to enrolled Windows Devices through Workspace ONE

This is a verification step. Workspace ONE can deploy devices automatically based on Endpoint Groups.

1. Through your browser, log into your EMA server as the Tenant Administrator.
2. From the left icon menu, select Endpoint Group.
3. Click the down arrow of the Endpoint Group, and select Create Agent Files.
4. On the Generate Agent Installation Files page, select the platform you need. We chose Windows (64-bit) service.
5. Download the platform service and the policy file, and click Done.
6. Navigate to the two downloaded files, select the EMAAgent.exe and EMAAgent.msh files, and compress the files.
7. From your web browser, log into Workspace One.
8. In the left pane, select Resources, click the Apps drop-down menu, and select Native.
9. In the main pane, click the Add drop-down menu, and select Application file menu.
10. In the Add Application window, select the Organization Group ID. We used PTGroup.
11. For the Application File, click Upload, select the EMA zip file, and click Continue.
12. Under Details, select the Supported Processor Architecture that matches the file service you previously chose.
13. Select Deployment Options, and scroll down to How to Install.
14. On the Install Command, type `emaagent.exe -fullinstall`.
15. Under When To Call Install Complete, click Add.
16. For Criteria Type in the Add Criteria window, select File exists.
17. In Path, type `C:\Program Files\Intel\Ema Agent\emaagent.exe`, and click Add.
18. Click Files, and type `emaagent.exe -fulluninstall`.
19. Click Save & Assign.
20. In the Distribution window, provide a name, and provide an Assignment Group. We named our group PT Group.
21. For App Delivery Method, select Auto, and click Create.
22. In the Assignment screen, click Save.

Enrolling a device into Workspace ONE

1. From the client device, open a browser, and navigate to getwsone.com.
2. Install Workspace ONE Intelligent Hub. When the installation finishes, start Workspace ONE Intelligent Hub.
3. Enter the server URL, and select Next.
4. Enter the group ID, and select Next.
5. Enter the enrollment username and password.
6. Accept the terms of use.
7. Select Done.
8. Open Workspace ONE Intelligent Hub, and complete the enrollment.

Completing the Workspace ONE test cases

Deploying the provisioning package for existing endpoint groups

1. From the Workspace ONE UEM, select Groups & Settings.
2. Select Integrations.
3. Under the Intel Integration, click View.
4. Under Configuration, click Resync Endpoint Groups.
5. Click View.
6. Click Distribute.
7. Select the target application.
8. Click Assign.
9. On the Distribution screen, enter the following information, and click Create.
    - For Name, enter a name.
    - For Assignment Groups, select a group.
    - For the App Deliver option, select Auto.
    - Leave additional options as default.
10. On the Assignment Screen, click Save.

Managing WS1 systems through the WS1 Integration”

Powering off an out-of-band device

1. From the Workspace One UEM, navigate to Devices → List view.
2. Select the desired device, and select More Action.
3. Select OOB Power Off.

Powering on an out-of-band device

1. From the Workspace One UEM, navigate to Devices → List view.
2. Select the desired device, and select More Action.
3. Select OOB Power On.

Connecting to an out-of-band device via KVM through the Workspace ONE integration

1. In a web browser, log into Workspace ONE.
2. From the Workspace UEM, navigate to Devices→List view.
3. Select the desired device, select the More Action drop down menu, and select Remote KVM.
4. In the Remote KVM pop-up window, click OK.
5. If required, enter the Intel EMA server credentials, and click Log in.
6. Click Hardware Manageability.
7. In the left column, select Remote Desktop.
8. Click connect, and enter the User Consent Code that the target endpoint is displaying.

Setting up the Configuration Manager environment

We created two VMs, one named DC01 and another called Deployment. DC01 served as our active directory, and the Deployment hosted our Configuration Manager server infrastructure.

For our local environment, our Microsoft Endpoint Configuration Manager testing environment consisted of one server with VMware vSphere 7.0. We installed one Microsoft Windows Server 2022 Active Directory Server VM named DC0 with Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP) roles. We also installed a management server (site server VM) named Deployment with Microsoft Endpoint Configuration Manager version 2111 and Microsoft SQL Server 2019 Enterprise Evaluation Edition.

We created the following volumes on the DC01 VM:

- OS volume (40 GB)
- General sharing for CIFS (40 GB)

We used the following volumes on the Deployment VM (our Microsoft Endpoint Configuration Manager server):

- OS and Configuration Manager installation (300 GB thin-provisioned)
- Database (200 GB thin-provisioned)
- Logs (40 GB thin-provisioned)
- Backup (40 GB thin-provisioned)

After we installed Endpoint Manager, we installed the following roles to the VM:

- Component server
- Distribution point
- Service Connection point
- Fallback status point
- Management point
- Site server
- Site database server (database)
- Site database server (transaction log)

We used the following media to create our local Configuration Manager environment:

- Windows Server Installation Media -
- Microsoft Endpoint Configuration Manager 2203 - mu_microsoft_endpoint_configuration_manager_current_branch_version_2203_x86_x64_dvd_77e1425b
- SQL Server 2019 Enterprise Core - en_sql_server_2019_enterprise_core_x64_dvd_5e1ecc6b
- Windows 10 Enterprise x64

Configuring the Configuration Manager environment

Creating a Microsoft Windows 2019 VM template

1. From vCenter, boot the VM to the Windows Server 2019 installation media.
2. At the prompt to boot from the CD/DVD location, press any key.
3. Click Next.
4. Click Install now.
5. Click Windows Server 2019 Datacenter Edition (Desktop Experience), and click Next.
6. Select I accept the license terms, and click Next.
7. Click the OS drive, and click Next.
8. After installation, enter a password for the Administrator, and click Finish.
9. Boot to Windows, and log in.
10. Disable the firewall, IE enhanced security, and auto logoff with group policy objects.
11. Install VMware tools.
12. In your VM's hardware, ensure that you are using VMXNET3 for the Network Adapter and VMware Paravirtual for the SCSI controller.
13. Select Windows Update, patch to the latest updates, and disable Windows Update.
14. Use the following command to sysprep the device:

```
C:\Windows\System32\Sysprep.exe /generalize /oobe /shutdown /unattend
```

15. Close the server VM.
16. Clone and create DC01 and Deployment VMs, and add necessary disk space as outlined in the previous section.

Installing and configuring Active Directory and DNS on the DC01 VM

1. To install Windows remote tools on the Active Directory VM, open a PowerShell windows, and run the following command:

```
Install-WindowsFeature RSAT-ADDS
```

2. When the installation finishes, close PowerShell.
3. Open Server Manager.
4. On the Welcome screen, click Add roles and features.
5. At the initial Before you begin screen, click Next three times.
6. At the Server Roles screen, select Active Directory Domain Services.
7. In the pop-up window, click Add features.
8. Click Next three times.
9. Verify the roles are correct, and click Install.
10. Once installation finishes, close the Add roles and features wizard.
11. In Server Manager, click the flag at the top, and select Promote this server to a domain controller.
12. Select Add a new forest, enter a root domain name of your domain, and click Next. We chose the name test.local for ours.
13. On the Domain controller options screen, enter a password, and click Next.
14. On the DNS Options screen, click Next.
15. On the Additional Options screen, click Next.
16. On the Paths screen, click Next.
17. On the Review Options screen, click Next.
18. On the Prerequisites screen, verify all prerequisites have passed, and click Install.
19. Once Active Directory Domain Services finishes installing, click Finish, and restart the system.
20. To open DNS, type `dnsmgmt.msc` in a command prompt.
21. Traverse the DNS entries to reverse lookup, right-click, and select new zone.
22. Select primary zone, and click Next
23. Click To all DNS servers running on domain controllers in this forest, and click Next.
24. Click IPv4 Reverse lookup, and click Next.
25. Enter an appropriate IP address range. For example, 192.168.0.x.
26. Select Allow only secure updates, click Next, and click Finish.
27. Configure Active Directory users and Computers, and edit the Domain Administrator account to never expire.

Installing DHCP on the DC01 VM

1. Open Server Manager.
2. On the Welcome screen, click Add roles and features.
3. At the initial Before you begin screen, click Next three times.
4. At the Server Roles screen, select DHCP Server.
5. On the pop-up window, click Add features.
6. Click Next three times.
7. Verify the wizard will install the desired role, and click Install.
8. Once installation finishes, close the Add roles and features wizard.
9. At the top of the screen in Server Manager, click the flag, and select Complete DHCP configuration.
10. In the DHCP Post-Install configuration wizard window, click Next.
11. At the Authorization screen, click Commit.
12. At the Summary screen, click Close.

Configuring DCHP on the DC01 VM

1. In Administrative Tools, open the DHCP service.
2. Expand test.local, right-click IPv4, and select New Scope.
3. In the New Scope Wizard window, click Next.
4. At the scope name screen, name the scope Laptops, and click Next.
5. In the IP Address Range, enter the desired scope settings for your network.
6. Click Next four times.
7. At the Router screen, enter the gateway address that the clients will use, and click Next.
8. Click Next three times.
9. At the Completing the New Scope Wizard screen, click Finish.
10. With the administrator@test.local account as an administrator, join the Configuration Manager, and add the Deployment VM to the test.local domain.
11. Using the administrator@test.local user, log into the target server.

Creating the system management container

1. On the Active Directory VM, open a command window, and run ADSI edit.
2. On the toolbar, click Action → Connect to….
3. To accept the defaults, click OK.
4. Under Default Naming Context → DC=test, DC=local, right-click the System container, and click New → Object….
5. Select Container, and click Next.
6. Under Value, enter System Management, click Next, and click Finish.

Setting permissions for Configuration Manager on the DC01 VM

1. Open Active Directory Users and Computers.
2. On the toolbar, select View, and click Advanced features.
3. Under test.local → System, right-click System Management, and click Delegate control.
4. Click Next.
5. Click Add.
6. Click Object types, click Computers, and click OK.
7. Enter the computer account for the Endpoint Configuration Manager server as an object name, add the domain administrator account, and click OK.
8. Click Next.
9. Select Create a custom task to delegate, and click Next.
10. Choose This folder, existing objects…, and click Next.
11. Click Full Control, and click Next.
12. Click Finish.

Extending the AD schema on the DC01 VM

To publish key information in a secure location where clients can easily access it, we needed to extend the Active Directory schema for Configuration Manager. The extended schema helps process deploying and setting up clients and additional services that the Configuration Manager site system roles provide.

1. Extract the contents of Configuration Manager installation media to the Active Directory VM DC01.
2. From the installation media, navigate to \SMSSETUP\BIN\X64, right-click extadsch, and run as administrator.
3. To confirm if the operation was successful, review extadsch.log at the root of the system drive. If it was successful, the log will include, "Successfully extended the Active Directory schema."

Installing required roles

1. Log onto the Endpoint Configuration Manager server as administrator.
2. Create a deployment share at the root of the installation drive with read and write permissions for everyone. We named our deployment share.
3. Verify that the share is accessible.
4. In an elevated PowerShell terminal, run the following commands:

```
Set-ExecutionPolicy Unrestricted
Import-module ServerManager
Add-WindowsFeature Web-Common-Http,Web-Static-Content,Web-Default-Doc,Web-Dir-Browsing,Web-Http-
Errors,Web-Http-Redirect,Web-Asp-Net,Web-Net-Ext,Web-ASP,Web-ISAPI-Ext,Web-ISAPI-Filter,Web-Http-
Logging,Web-Log-Libraries,Web-Request-Monitor,Web-Http-Tracing,Web-Basic-Auth,Web-Windows-Auth,Web-
Url-Auth,Web-Filtering,Web-IP-Security,Web-Stat-Compression,Web-Mgmt-Tools,Web-WMI,RDC,BITS -Restart
```

Installing the Windows 10 ADK on the Deployment VM

For additional information around the Windows ADK, review the documentation at **https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install**. The site lists the latest versions for the following installations.

1. Download the Windows Assessment and Deployment Kit for Windows 10 from `https://go.microsoft.com/fwlink/?linkid=2165884`.
2. Click the executable adksetup.exe.
3. Click Next twice.
4. Accept the licensing agreement.
5. On the Select the features you want to install screen, select the following features, and click install:
   - Deployment Tools
   - Imaging and Configuration Designer (ICD)
   - Configuration Designer
   - User State Migration Toll (USMT)
6. Using the provided link, download the Windows PE add-on for the ADK.
7. Specify Location, and click Next.
8. Select the following features to install:
   - Deployment Tools
   - Imaging and Configuration Designer (ICD)
   - Configuration Designer
   - User State Migration Tool (USMT)
9. Click next, and click Close.

Installing the Windows Assessment and Deployment Kit Windows Preinstall Environment Add-ons – Windows 10 on the deployment VM

1. Download the adkwinpesetup.exe file from **https://docs.microsoft.com/en-us/windows-hardware/get-started/adk-install**.
2. Run adkwinpesetup.exe.
3. Accept the default locations, and click Next.
4. Select Windows Preinstallation Environment (PE), click Install, and click Close.

Installing SQL 2019 on the Deployment VM

1. Log into the Configuration Manager VM, named Deployment, as administrator@test.local.
2. Attach the installation media for SQL 2019 Enterprise Core, and run the setup.exe file.
3. From the menu on the left in the SQL Server Installation Window, select Installation, and select New SQL Server stand-alone installation or add features to an existing installation.
4. In the SQL Server 2016 Setup Window, select product key.
5. On the License Terms page, accept the terms, and click Next.
6. On the Microsoft Update screen, select Use Microsoft Update to check for updates, and click Next.
7. On the Feature Selection screen, under Instances Features, select Database Engine Services, select locations for your instance root and Shared Features directory, and click Next. We used our data volume.
8. On the Instance Configuration screen, select Default Instance, and leave the default instance ID.
9. On the Server Configuration screen, set Startup Type to Automatic for all four services. Select Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service.
10. Select Collation.
11. On Collation, verify that the Database Engine is set to SQL_Latin1_General_CP1_CI_AS, and click Next.
12. On Database Engine Configuration screen, select mixed authentication mode.
13. Under Specify SQL Server administrators, click Add Current User, and click Add.
14. Add the Configuration Manager Admins group, and click OK.
15. On the Data Directories tab, verify that wizard lists the additional data drive as the data root directory.
16. On TempDB, type the following settings:
    - Number of files: `1`
    - Initial size (MB): `1024`
    - Autogrowth (MB): `512`
    - Data directories: [use default]
    - Initial size of TempDB log file (MB): `1024`
    - Autogrowth (MB): `512`
    - Log directory: [use default]
17. On Memory, select Recommended. For Min Server Memory (MB), type `8192`, and for Max Server Memory (MB), type `16384`.
18. Click Next.
19. On the Ready to Install screen, review your settings, and click Install.
20. Click Next.
21. At the Ready to Install, run the SP2CU6 SQL server update.
22. Run Windows updates.

Installing Report Viewer and the SQL Server Management Studio on the deployment VM

1. Download the Report Viewer from **https://www.microsoft.com/en-US/download/confirmation.aspx?id=6442,** and install using all defaults.
2. In the SQL Server Installation Center, select Install SQL Server Management Studio.
3. Click the link to Download SQL Server Management Studio (SSMS).
4. From your Downloads folder, run SSMS-Setup-ENU.exe.
5. In the Microsoft SQL Server Management Studio installation wizard, click Install.
6. To restart your server after the installation completes, click Restart.

Changing SQL service to start as local system

1. Open SQL Server Configuration Manager.
2. Under SQL Service Services, right-click the SQL Server instance, and click Properties.
3. For Log on as, select Built-in account, and Local System. Click OK, and click Restart.

Installing WSUS role on the Deployment VM

1. Open Server Manager.
2. Click Add Roles and Features.
3. Select Windows Server Update Services, and click Next.
4. Uncheck WID Connectivity, select SQL Server Connectivity, and click Next.
5. Select an appropriate directory for Windows updates. We used \\deploy\wsusupdates\.
6. On the database instance selection screen, enter the database server name, and click Check Connection. Ensure you see the Successfully connected to server message, and click Next.
7. Click Install.
8. Click Close.

Installing Endpoint Configuration Manager update 2203 on the Deployment VM

1. Sign into the Endpoint Configuration Manager VM using the administrator@test.local account.
2. Attach the Configuration Manager update 2002 Installation media to the management server.
3. Open splash.hta.
4. Click Install.
5. Read the Before You Begin section, and click Next.
6. Choose Install a primary site.
7. Choose Use typical options.
8. Enter the product key, enter a Software Assurance Date, and click Next.
9. Select to accept the License Terms, and click Next.
10. Enter a path for the prerequisite file downloads, and click Next. We used User\Downloads\ConfigMgr.
11. Select a language, and click Next for both server and client.
12. On the Site and Installation Settings screen, enter a site code for the primary site and site name, and click Next.
13. On the Primary Site Installation screen, select Install the primary site as a stand-alone site, and click Next.
14. On the Database Information screen, leave the defaults, and click Next.
15. On the Database Information screen, click Next.
16. On the SMS Provider Settings screen, click Next.
17. On the Client Computer Communications Settings screen, select Configure the communication method on each site system role, select Clients will use HTTPs when they have a valid PKI certificate…, and click Next.
18. On the Site System Roles screen, select HTTP for client connections for both the management and distribution points, and click Next.
19. On the Diagnostic and Usage Data screen, click Next.
20. On the Service Connection Point Setup screen, click Next.
21. On the Settings Summary screen, click Next.
22. Click Install.

Enabling Active Directory System Discovery for Endpoint Configuration Manager

1. In the Configuration Manager console, navigate to Administration→Hierarchy Configuration→Discovery Method, and right-click Active Directory System Discovery and select Properties.
2. On the Active Directory System Discovery Properties screen, click Enable Active Directory System Discovery.
3. Next to Active Directory containers, click the Star.
4. In the Active Directory Container menu, for Path, click Browse. Select the top-level Active Directory object, and click OK.
5. Check Discover objects within AD group.
6. Select Use the Computer account of this site server, and click OK.
7. Click OK.
8. In the pop-up window, click Yes.

Setting up a Boundary Group

1. Under Hierarchy Config, select Boundaries Groups.
2. In Action, right-click and select Create Boundary Groups.
3. Click add, click the checked the server's name, and click OK twice.
4. Enter a name, and click Reference.
5. Enable Use Boundary group for site assignment.
6. Under Hierarchy Config, select Boundaries.
7. In Action, right-click and select Create Boundaries.
8. Click Type, and select AD site.
9. Click browse, and select the Default AD site name.
10. In description, provide a brief detail. We typed `Site Boundary`.
11. Click Boundary Groups.
12. Click Add.
13. Select the Boundary group, and click OK twice.

Adding a device to the domain

1. From the Start menu on the client device, type and select `This PC`.
2. On the toolbar, click Computer, and select System properties.
3. Scroll down, and select Rename this PC (advanced).
4. Under Computer Name, click Change.
5. Enter the desired computer name, and select Domain, and enter the domain name.
6. Enter the domain admin credentials, and click Okay twice.
7. Restart the device.
8. In the toolbar of the Configuration Manager Console on the Deployment server, navigate to Admininistration, Hierarchy Configuration, Discovery Method, and click Run Full Discovery Now.
9. Complete steps 1 through 8 for each of the five devices for the Configuration Manager environment.

Configuring automatic client push for discovered computers

1. Launch the Configuration Manager Console, and navigate to Administration → Site Configuration → Sites.
2. In the Sites list, select the site for which you want to configure site-wide client push.
3. On the top ribbon, click on Client Installation Settings, and click Client Push Installation.
4. On the Client Push Installation Properties window, click General, and enable automatic site-wide client push installation.
5. Under System types, select Servers and Workstation.
6. Click Accounts, click the star, and select New Account.
7. Add the domain admin/admin group, and click Apply and OK.
8. After a few minutes, open task manager, and under Process, verify that ccmsetup.exe is running.
9. Navigate to Assets and Compliance → Devices → All Systems, and verify that the client machines have the configuration manager client (Yes in the Client column).

Installing Endpoint Configuration Manager clients using client push installation wizard

1. Click Assets and Compliance → Devices → All Systems.
2. Right-click the device, and click Install Client.
3. On the Install Configuration Manager Client wizard, click Next.
4. Click Install the client software from a specified site, and click Next.
5. On the completion screen, click close.

Completing Configuration Manager test cases

Creating and deploying the Intel EMA Agent application using Endpoint Configuration Manager

1. Through your browser, log into your EMA server as the tenant administrator.
2. From the left icon menu, select Endpoint Group.
3. Click the down arrow of the Endpoint Group, and select Create Agent Files.
4. On the Generate Agent Installation Files page, select the platform you need.
5. Download both the platform service and the policy file, and click done.
6. In Configuration Manager, navigate to Software Library → Overview → Application Management → Application.
7. Click Create Application.
8. Select Manually specify the application information, and click Next.
9. On the General Information screen, enter the application details, and click Next.
10. On the Software Center screen, enter any details you want to be displayed in Software Center, and click Next.
11. On the Deployment type screen, click Add.
12. For deployment type, select script installer, and click Next.
13. Give the deployment type a name, and click Next.
14. On the content screen, enter the content location.
15. Under Specify the command used to install the content, enter the following install command in the installation program:

```
emaagent.exe -fullinstall
```

16. Enter the following command in the Uninstall program section, and click Next:

```
emaagent.exe -fulluninstall
```

17. On the Detection Method page, click Add Clause.
18. For Setting type, choose File System, and for Type, select File.
19. Enter the Path for the file.
20. For File or Folder name, type `emaagent.exe`.
21. Select The file system setting must satisfy the following rule to indicate the presence of this application:
    - Property: Version
    - Operator: Equals
    - Value: 1.7.0.4
22. To close the Detection Rule dialog box, click OK, and click Next.
23. On the User Experience page, click Next.
24. On the requirement page, click Next.
25. On the dependencies page, click Next.
26. On the Summary page, click Next, and click Close on the Completion page.
27. On the Deployment Types page, click Next.
28. On the Summary page, click Next, and click Close on the Completion page.
29. From Applications, select the Intel EMA Agent application you just created. In the ribbon above, select Distribute Content.
30. After the distribute content wizard appears, click Next.
31. Review the content to distribute, and click Next.
32. On the Specify the Content destination page, click Add.
33. Select the Distribution Point (deployment.test.local), click OK, and click Next.
34. Review the summary, click Next, and click Close.
35. Select Intel EMA Agent, and in the ribbon, click Deploy.
36. In the wizard, click browse beside the Collection, choose Device Collections (Temp), click OK, and click Next.
37. For Action in Deployment Settings, choose Install, and for Purpose, choose Required for automatic installation.
38. On the scheduling screen, select As soon as possible after the available time, and click Next.
39. On the User Experience Screen, Click Next.
40. On the Alert Screen, Click Next.
41. Review the summary, and click Finish. After a few minutes, the Application will deploy successfully on the client.

Configuring Intune

Adding the E5 and P2 licenses

1. Using the admin account, log into Azure.
2. Under Azure services, select Azure Active Directory.
3. Navigate to License.
4. Under Manage, select All products, and click +Try/Buy.
5. Select the free trial Enterprise Mobility + Security E5, and click Activate.
6. Complete steps 1 through 4 again, select the free trial Azure AD Premium P2, and click Activate.

Adding Intune and configuring the MDM scope

1. In the left pane under Azure Services, select Azure Active Directory, and click Mobility (MDM and MAM).
2. Click +Add application.
3. Select Microsoft Intune, and click Add.
4. Click Microsoft Intune.
5. On the Configure page, configure the following, and click Save:
    - MDM user scope: All
    - MAM user scope: All

Adding users

1. From the Azure portal, under azure services, select Azure Active Directory.
2. In the left pane under Manage, select Users.
3. Click + New user, and click Create new user.
4. In the first block, enter a username, and after @ in the block, enter the proper domain name.
5. For Name, enter the desired name as required, and select your Password options. If you choose Auto-generate Password, check Show Password, copy to the password to the clipboard, store it somewhere safe, and click Create.

Managing licensing on the target users.

1. Under Users, select the recently created user.
2. In the left pane, under Mange select Licenses, click +Assignments, select both Azure Active Directory Premium P2 and Enterprise Mobility + Security E5, and click Save.

Enrolling endpoints

1. From the device, power on, and configure Windows to connect to a network with internet access.
2. Open the Microsoft Store, and in the search bar, type `company portal`.
3. To install Company Portal, click Get, and click Launch.
4. When prompted, sign in using the User account credentials created in Azure.
5. Uncheck Allow my organization to manage my device, and click OK.
6. Enter the computer Password, press Enter, and click Done.
7. Click This device hasn't been set up for corporate use yet. To begin setup, select the message.
8. On the Set up your device screen, click Next.
9. On the Connect to work screen, click Connect.
10. On the Set Up a work or school account, verify the user account, and click Next.
11. Once the Company Portal app finishes adding the device, select Got It.
12. Click Next, and click done.
13. Enroll the four additional devices by completing steps 1 through 12 four more times.

Configuring co-management for Configuration Manager and Intune

Installing Azure AD Connect

1. On the Active Directory server, download Microsoft Azure Active Directory Connect from **https://www.microsoft.com/en-us/download/details.aspx?id=47594.**
2. In the Microsoft Azure Active Directory Connect installation tool, click I agree to the license terms and privacy notice, and click Continue.
3. Click Use Express Settings.
4. On the Connect to Azure AD screen, enter your Azure administrator's username and password, click Next, and complete the sign-in request.
5. On the Connect to AD DS screen, enter your local domain administrator username and password, and click Next.
6. On the Azure AD sign-in screen, select Continue without matching all UPN suffixes to verified domains. Click Next.
7. Click Install.

Configuring device options in Azure AD Connect

1. Open Azure AD Connect.
2. Click Configure.
3. Select Configure Device options, and click Next.
4. Under Device Options, select Configure Hybrid Azure AD join, and click Next.
5. On the Device operating systems page, select Windows 10 or later domain-joined devices. Click Next.
6. On the SCP configuration page, select the test.local forest. For Authentication Service, select Azure Active Directory. Click Add, and enter the credentials for the domain administrator. Click Next.
7. On the Ready to Configure page, click Configure.
8. Click Exit once the wizard presents the option.
9. Configuring Device Options in Azure AD Connect.

Configuring device options in Azure AD Connect

1. In the Configuration Manager Console, under Administration, Cloud Services, Cloud Attach, select Configure Cloud Attach.
2. In the Cloud Attach Configure Wizard, click Sign In. Enter the Azure global administrator credentials. Use the default settings, and click Next.
3. Accept the Create AAD application prompt.
4. Click Next.

Configuring device options in Azure AD Connect

1. In the Configuration Manager Console, under Administration, Overview, Updates and Servicing, and Console Exensions, right-click the WebView2 extension, and click Install.
2. In the pop-up, click OK.

Completing the Intune test cases

Preparing the Intel EMA agent for distribution with Intune

For this portion, we purchased subscriptions for Microsoft Enterprise Mobility + Security E5, which provided us with access to Azure AD and Intune. We then created a security group and assigned devices to that security group. IT administators must join or register devices to Azure Active Directory (Azure AD) and auto enroll them. The Intune management extension supports devices that are Azure AD joined, Azure AD registered, hybrid domain joined, or group policy enrolled.

Before you can add a Win32 app to Microsoft Intune, you must prepare the app by using the **Microsoft Win32 Content Prep Tool**. Download it to the Deployment Server.

1. Through your browser, log into your Intel EMA server as the tenant administrator.
2. From the left icon menu, select Endpoint Group.
3. Click the down arrow of the Endpoint Group, and select Create Agent Files.
4. On the Generate Agent Installation Files page, select the platform you need.
5. Download both the platform service and the policy file, and click done.
6. Log into the Deployment server, and open PowerShell as administrator.
7. Run the IntuneWinAppUtil.exe by either navigating to the location where you downloaded the file or enter the directory location, such the following:

```
C:\Users\administrator.TEST\Downloads\Microsoft-Win32-Content-Prep-Tool-master\IntuneWinAppUtil.exe
```

8. Type the following information for Setup folder, Setup File, and Output folder:
   - Setup Folder: `EMAAgent`
   - Setup file: `emaagent.exe`
   - Output Folder: `EMAAgent`
9. When asked Do you want to specify catalog folder (Y/N)?, select N, and press Enter. Wait until emaagent.intunewin appears in the Intel EMA Agent folder.
10. Through your browser, log into your Intel EMA server as the tenant administrator.
11. From the left icon menu, select Endpoint Group.
12. Click the down arrow of the Endpoint Group, and select Create Agent Files.
13. On the Generate Agent Installation Files page, select the platform you need.
14. Download both the platform service and the policy file, and click done.
15. Sign into the **Microsoft Endpoint Manager admin center**.
16. Navigate to Apps→All apps, and click Add.
17. In Select app type, under the other app types, select Windows app (Win32).
18. Click Select. The Add app steps should appear.
19. In Add app, click Select app package file.
20. In App package file, select the browse button. Navigate to and select emaagent.intunewin. The following app details should appear:
    - Enter Publisher name: Intel
    - Feature App: Yes
21. To display the Program page, select Next.
22. On the Program page, configure the following app installation and removal commands for the app:
    - Install: `install.cmd`
    - Uninstall: `uninstall.cmd`
    - Install behavior: `System`
23. Click Next.
24. In Requirements, type the following for operating system architecture and minimum operating system:
    - Operating System Architecture: `64-bit`
    - Minimum Operating System: `Windows 10 1607`
25. To display the Add a Requirement rule pane, select Add.

26. In the Requirement rule pane, type the following information, and click Okay:
    - For Requirement type, select File.
        - For Path, we typed `C:\Program Files\intel\ema agent\emaagent.exe`.
        - For file or folder, type `emaagent.exe`.
        - For property, select File or Folder exists.
27. Click Next.
28. On the Detection rule page, select Manually configure detection rules, and click Add.
29. Type the following for the Detection rule:
    - Rule Type: `File`
    - Path: `C:\Program Files\intel\ema agent\emaagent.exe`
    - File or Folder: `emaagent.exe`
    - Detection method: `File or Folder exists`
30. Click OK, and click Next.
31. On the Dependencies section, click Next.
32. On the Supersedence section, click Next.
33. Under Required on the Assignment section, click Add group.
34. Select the group that the client device is in, and click Next.
35. On the Review + Create section, review your details, and click Create.

Managing hybrid and MECM systems using Intel EMA

Admins must complete all hardware-based management tasks from the Intel EMA console.

Powering on an out-of-band device

1. In a web browser, navigate to the Intel EMA console.
2. Enter the tenant credentials, and click Log in.
3. In the left column, select the Endpoint icon to navigate to the enrolled endpoints.
4. Select the desired device, and at the far right, click view.
5. Click Hardware Manageability.
6. In the left column, select Remote Desktop.
7. In the right corner, select Power Actions→Power On.

Powering off an out-of-band device

1. In a web browser, navigate to the Intel EMA console.
2. Enter the tenant credentials, and click Log in.
3. In the left column, select the Endpoint icon to navigate to the enrolled endpoints.
4. Select the desired device, and at the far right, click view.
5. Click Hardware Manageability.
6. In the left column, select Remote Desktop.
7. In the right corner, select Power Actions→Power Off.

Connecting to an out-of-band device via KVM

1. In a web browser, navigate to the Intel EMA console.
2. Enter the tenant credentials, and click Log in.
3. In the left column, select the Endpoint icon to navigate to the enrolled endpoints.
4. Select the desired device, and at the far right, click view.
5. Click Hardware Manageability.
6. In the left column, select Remote Desktop.
7. Click connect, and enter the User Consent Code that the target endpoint is displaying.

Read the report at https://facts.pt/d81CmFQ

This project was commissioned by VMware.

Principled Technologies®

Facts matter.®