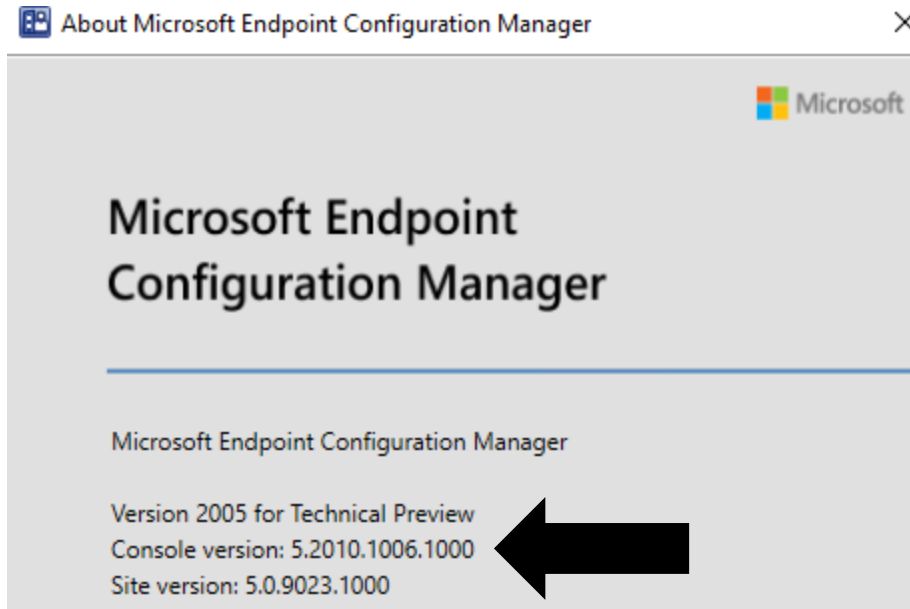


Installing Technical Preview 2006

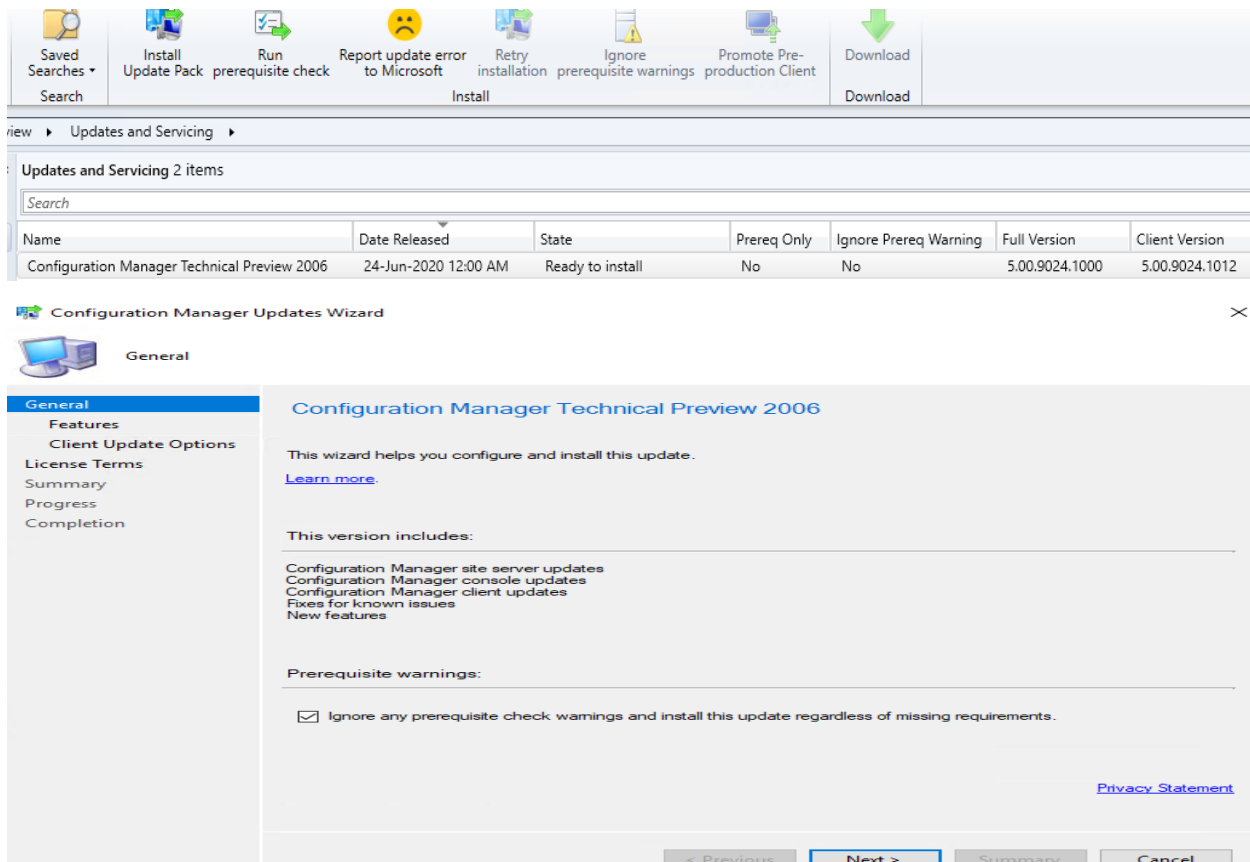
In this post, I will show you how to install TP2006 and explore new features. I am currently running TP2005. Will upgrade to TP2006 within the console.



Visit these links for more info on TP2006

https://techcommunity.microsoft.com/t5/configuration-manager-blog/view-configmgr-apps-in-company-portal-using-configuration/ba-p/1490858?utm_source=dlvr.it&utm_medium=twitter

<https://docs.microsoft.com/en-us/mem/configmgr/core/get-started/2020/technical-preview-2006>





Client Update Options

General

Features

Client Update Options

License Terms

Summary

Progress

Completion

Client Update Settings

This update includes an update for the Configuration Manager client. You can upgrade your clients immediately, or validate this client in a pre-production collection before you upgrade all your Configuration Manager clients.

☒ Upgrade without validating

Overwrites your current Configuration Manager client package with the new client update. All new client installations and client upgrades use this new client update.

☐ Validate in pre-production collection

Validate the client update on members of the pre-production collection while you keep your production client package intact. Later, you can overwrite the production package using Client Update Options in the Updates and Servicing node of the Configuration Manager console.

Pre-production collection:

[Browse...](#)

< Previous

Next >

Summary

Cancel



License Terms

General

Features

Client Update Options

License Terms

Summary

Progress

Completion

Review and accept the terms for this update pack

You must accept the License Terms and Privacy Statement to continue installation.

[View the License Terms](#)[View the Privacy Statement](#)

☒ I accept these License Terms and Privacy Statement.

You can add or update your Software Assurance expiration date. This date must be after 01-Oct-2016.

Software Assurance expiration date:

01-Dec-2020 

[Learn more](#)

< Previous

Next >

Summary

Cancel



Summary

General

Features

Client Update Options

License Terms

Summary

Progress

Completion

Confirm the Settings

Details:

Summary of update package installation

Install Update Package Configuration Manager Technical Preview 2006
Prerequisite warnings will be ignored
Test new version of the client in production
Software Assurance expiration date is 2020-12-01.

To change these settings, click Previous. To apply the settings, click Next.

< Previous

Next >

Summary

Cancel



Completion

General

Features

Client Update Options

License Terms

Summary

Progress

Completion

**The Configuration Manager Updates Wizard completed successfully**

Details:

Summary of update package installation

✓ Success: Install Update Package Configuration Manager Technical Preview 2006
Prerequisite warnings will be ignored
Test new version of the client in production
Software Assurance expiration date is 2020-12-01.

To exit the wizard, click Close.

< Previous

Next >

Summary

Close

Updates and Servicing 2 items						
Search						
Name	Date Released	State	Prereq Only	Ignore Prereq Warning	Full Version	Client Version
Configuration Manager Technical Preview 2006	24-Jun-2020 12:00 AM	Installing	No	Yes	5.00.9024.1000	5.00.9024.1012

Updates and Servicing 2 items						
Search						
Name	Date Released	State	Prereq Only	Ignore Prereq Warning	Full Version	Client Version
Configuration Manager Technical Preview 2006	24-Jun-2020 12:00 AM	Checking prerequisites	No	Yes	5.00.9024.1000	5.00.9024.1012

Updates and Servicing 2 items						
Search						
Name	Date Released	State	Prereq Only	Ignore Prereq Warning	Full Version	Client Version
Configuration Manager Technical Preview 2006	24-Jun-2020 12:00 AM	Installing	No	Yes	5.00.9024.1000	5.00.9024.1012

Configuration Manager



A new version of the console is available (5.2010.1022.1000). Click OK to close the console and install the new version now. Click Cancel to continue working with the old console (5.2010.1006.1000). Working in the old console might corrupt data.

OK

Cancel

Microsoft Endpoint Configuration Manager Console



Please wait while Windows configures Microsoft Endpoint Configuration Manager Console

Gathering required information...



Cancel

About Microsoft Endpoint Configuration Manager



Microsoft Endpoint Configuration Manager

Microsoft Endpoint Configuration Manager

Version 2006 for Technical Preview
Console version: 5.2010.1022.1000
Site version: 5.0.9024.1000



Microsoft Endpoint Configuration Manager 2006 Tech Preview

Welcome to update 2006 for Configuration Manager Technical Preview. Below you can find information about some of the new features and scenarios that are now available for you to try. You can also view which of the new scenarios you have completed for each feature. [Read more](#) about the latest changes in the Technical Preview build.

Please continue to give us feedback! To report any issues you encounter with the latest functionality included in this Technical Preview, use the [Microsoft Connect](#) website. To request a new feature or enhancement, use the [Configuration Manager UserVoice site](#).

What's New in 2006

Client install and upgrade on metered connection

Client installation and upgrades can be configured to occur on devices connected to metered networks.

Directly link to Configuration Manager Community hub items

Ability to easily navigate to and reference items in the Configuration Manager console Community hub node by merely following a link.

Import previously created Azure AD application during tenant attach onboarding

During a brand new onboarding to cloud attach an admin can specify a previously created application during onboarding to tenant attach.

Improvements to available apps via CMG

An internet-based device that isn't joined to Azure Active Directory (Azure AD) and communicates via a cloud management gateway (CMG) can now get apps deployed as available to users.

Improvements to Company Portal Integration

You can now control whether Software Center or the Company Portal sends user notifications on co-managed devices.

Microsoft Endpoint Configuration Manager 2006 Tech Preview

Improvements to managing device restarts

You can now configure client settings to prevent devices from automatically restarting when a deployment requires it. By default, Configuration Manager can still force devices to restart.

Improvements to task sequences over cloud management gateway

A workgroup client communicating via cloud management gateway using token authentication can now run task sequences.

Intranet clients can use a CMG software update point

Intranet clients can now access a CMG software update point when it's assigned to the boundary group.

Management Insights rules to optimize for remote workers

We have added new rules in Management Insights to help you create better experiences for remote workers and reduce load on your infrastructure.

Windows 10 Enterprise multi-session platform support

The 'Windows 10 Enterprise multi-session' platform is now available in the list of supported OS versions on objects with requirement rules or applicability lists.

Wipe and Load OSD task sequence initiated from software center can be run over cloud management gateway

It is now supported to run a wipe and load task sequence from software center whilst a client is communicating with a CMG.

Microsoft Endpoint Configuration Manager (Connected to 1P1 - Technical Preview - North America) (Evaluation, 90 days left)

Home

History Check for updates Refresh Saved Searches Install Update Pack prerequisite check Run prerequisite check Report update error to Microsoft Retry installation Ignore prerequisite warnings Promote Pre-production Client Download

Updates and Servicing Administration Overview Updates and Servicing 1 items


Name	Date Released	State	Prereq Only	Ignore Prereq Warning	Full Version	Client Version
Configuration Manager Technical Preview 2006	24-Jun-2020 12:00 AM	Installed	No	Yes	5.00.9024.1000	5.00.9024.1012

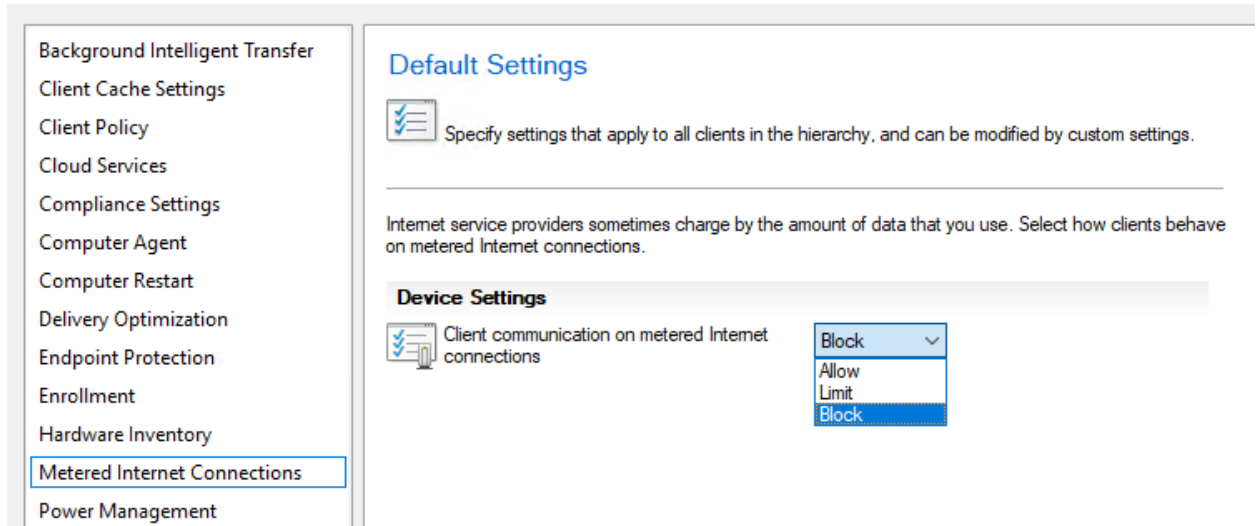
Features 20 items

Name	Feature Type	Status	Description
Azure Active Directory user group discovery	Release	On	Cloud-enable your...
Cloud Management Gateway	Release	On	Provides a simple...
PFX Create	Release	On	Create and deploy...
Task Sequence as an app model deployment type install method	Release	On	An admin is now a...
Task Sequence Debugger	Release	On	The Task Sequenc...
Synchronize collection membership results to Azure Active Directory groups	Release	On	You can now enab...
Enable third party update support on clients	Release	On	Enables configurat...
Windows Hello for Business	Release	On	Admin can target...
Windows Defender Exploit Guard policy	Release	On	You can control W...
Surface Driver Updates	Release	On	Manage Surface D...
Microsoft Operations Management Suite (OMS) Connector	Release	On	Sync data such as...
BitLocker Management	Release	On	Ability to manage...
Create and run scripts	Release	On	Create and run Po...
Package Conversion Manager	Release	On	Package Conversio...
Approve application requests for users per device	Release	On	User-based applic...
Orchestration Group	Release	On	Control settings fo...
Conditional access for managed PCs	Release	On	To help secure Offi...
Device Health Attestation assessment for compliance policies for conditional access	Release	On	Use Device Health...
VPN for Windows 10	Release	On	You can use Micro...
Application Groups	Release	On	Create a group of...

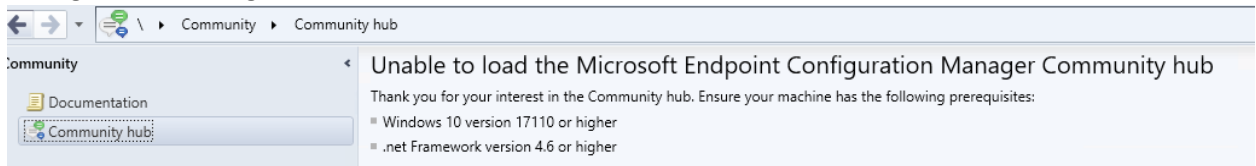
NEW FEATURES:

1. **Client install and upgrade on metered connection** - Starting in Configuration Manager technical preview version 2005, you could install and upgrade the client when you allowed client communication on a metered connection. You can now also configure the client setting Client communication on metered internet connections to Limit. This option reduces the client communication on a metered network, but now still allows the client to stay current.

 Default Settings



2. **Directly link to Configuration Manager Community hub items** - You can now easily navigate to and reference items in the Configuration Manager console Community hub node with a direct link. The intention for this feature is for easier collaboration and being able to share links to Community hub items with your colleagues. Currently, you'll see these links shared by the Configuration Manager team and in the documentation.



3. **Import previously created Azure AD application during tenant attach onboarding -**

During a new onboarding, an administrator can specify a previously created application during onboarding to tenant attach. From the **Tenant onboarding** page in the **Co-management Configuration Wizard**, select **Optionally import a separate web app to synchronize Configuration Manager client data to Microsoft Endpoint Manager admin center**. This option will prompt you to specify the following information for your Azure AD app:

- Azure AD tenant name
- Azure AD tenant ID
- Application name
- Client ID
- Secret key
- Secret key expiry
- App ID URI

4. Improvements to available apps via CMG -

An internet-based, domain-joined device that isn't joined to Azure Active Directory (Azure AD) and communicates via a cloud management gateway (CMG) can now get apps deployed as available. The Active Directory domain user of the device needs a matching Azure AD identity. When the user starts Software Center, Windows prompts them to enter their Azure AD credentials. They can then see any available apps.

Configure the following prerequisites to enable this functionality:

- Windows 10 device
 - Joined to your on-premises Active Directory domain
 - Communicate via CMG
- The site has discovered the user by both **Active Directory** and **Azure AD user discovery**

5. Improvements to Company Portal Integration - The Company Portal is now the cross-platform app portal experience for Microsoft Endpoint Manager. You can now use a preview version of the Company Portal on co-managed devices. By configuring co-managed devices to also use the Company Portal, you can provide a consistent user experience on all devices. This preview version of the Company Portal supports the following actions:

Launch the Company Portal app on co-managed devices and sign in with Azure Active Directory (Azure AD) single sign-on (SSO).

View available and installed Configuration Manager apps in the Company Portal alongside Intune apps.

Install available Configuration Manager apps from the Company Portal and receive installation status information.

Prerequisites for Company Portal preview


- Contact the Company Portal preview team to get started: cppreview@microsoft.com
- Windows 10, version 1803 or later:
 - Enrolled to **co-management**
 - Access to **internet endpoints for Intune**
- The user accounts that sign in to these devices require the following configurations:
 - An Azure AD identity
 - Assigned an Intune license

6. **Improvements to managing device restarts** - You can now configure client settings to prevent devices from automatically restarting when a deployment requires it. By default, Configuration Manager can still force devices to restart.

Default Settings


Background Intelligent Transfer
Client Cache Settings
Client Policy
Cloud Services
Compliance Settings
Computer Agent
Computer Restart
Delivery Optimization
Endpoint Protection
Enrollment
Hardware Inventory
Metered Internet Connections
Power Management
Remote Tools
Software Center
Software Deployment
Software Inventory
Software Metering
Software Updates
State Messaging
User and Device Affinity
Windows Diagnostic Data

Default Settings

 Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Specify restart behavior on client computers.

Device Settings

 Configuration Manager can force a device to restart


Specify the amount of time after the deadline before a device gets restarted (minutes)

Specify the amount of time that a user is presented a final countdown notification before a device gets restarted (minutes)

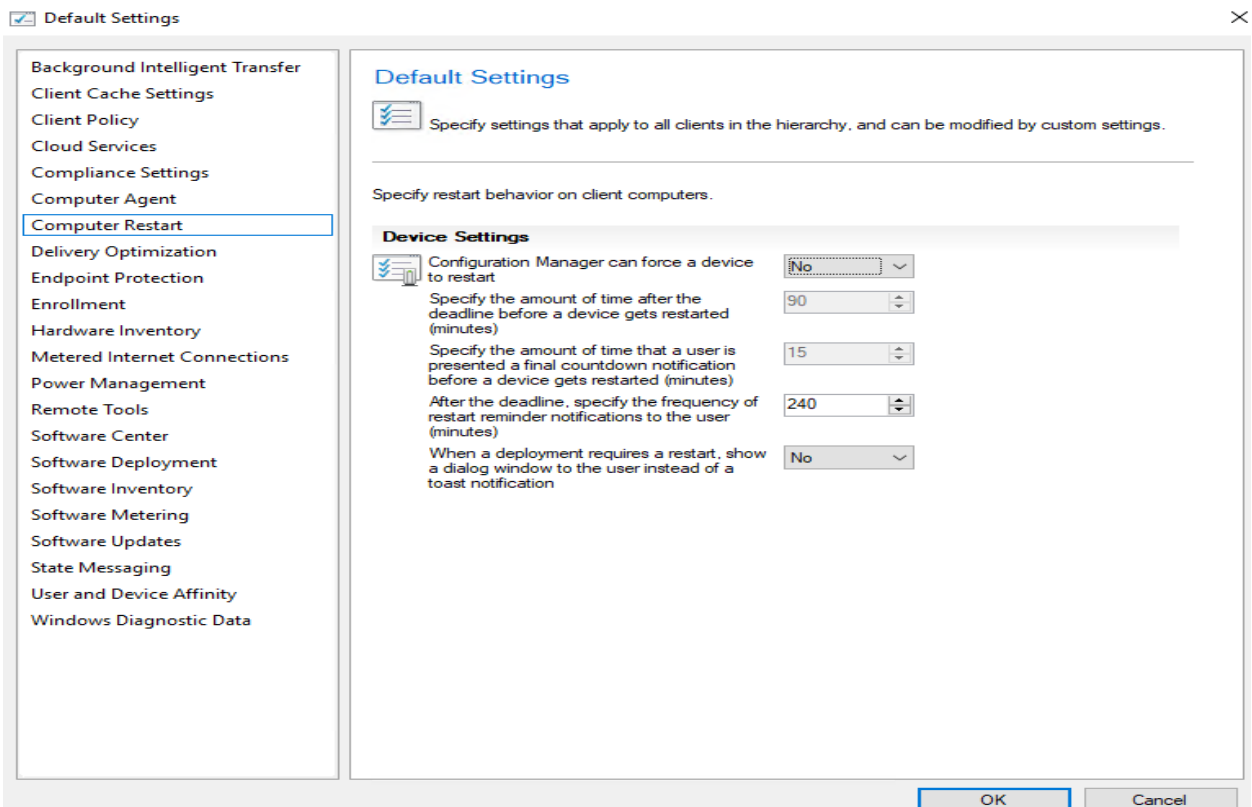
After the deadline, specify the frequency of restart reminder notifications to the user (minutes)

When a deployment requires a restart, show a dialog window to the user instead of a toast notification

Configuration Manager

 Updates may not be fully installed and additional software installations may not occur until a restart is triggered by the user.

Are you sure you want to disable this setting?



Try it out!

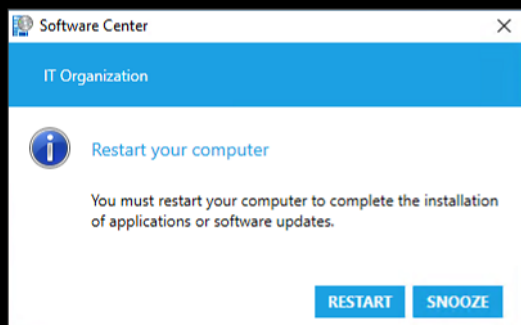
Try to complete the tasks. Then send [Feedback](#) with your thoughts on the feature.

1. In the **Computer Restart** group of client settings, disable the following new option: **Configuration Manager can force a device to restart**. When you disable this setting, you can't specify the amounts of time after the deadline that the device is restarted or the user is presented a final countdown notification.
2. For the purposes of testing the behavior, change the frequency of the following setting to 2 minutes: **After the deadline, specify the frequency of restart reminder notifications to the user (minutes)**.
3. **Deploy an app** that requires a restart. Make the deployment required with an immediate deadline.

Tip

For the purposes of testing, on the app deployment type properties, go to the **Return Codes** tab. For return code value 0, change the **Code Type** to **Hard Reboot**.

Wait or force the client to receive the updated client settings and app deployment policies. After the app installs successfully, you'll see the following notification:



If you **Snooze** this notification, it will show again based on how you configure the frequency of restart reminder notifications. The device won't restart until you select **Restart** or manually restart Windows.

To help troubleshoot, use the `rebootcoordinator.log` and `SCNotify.log` files.

7. **Improvements to task sequences over cloud management gateway** - A workgroup client communicating via cloud management gateway using token authentication can now run task sequences.

This release includes the following improvements to deploy task sequences to devices that communicate via a cloud management gateway (CMG):

- Support for OS deployment: With a task sequence that uses a boot image to deploy an OS, you can deploy it to a device that communicates via CMG. The user needs to start the task sequence from Software Center.
- This release fixes the two **known issues** from Configuration Manager current branch version 2002. You can now run a task sequence on a device that communicates via CMG in the following circumstances:
 - A workgroup device that you register with a **bulk registration token**
 - You configure the site for **Enhanced HTTP** and the management point is HTTP

Known issue with OS deployment via CMG

If there's an **Install Application** step in an OS deployment task sequence to a client via CMG, it fails to download the app policy. To work around this issue, disable this step in the task sequence. Deploy the app separately from the task sequence.

8. **Intranet clients can use a CMG software update point** - Intranet clients can now access a CMG software update point when it's assigned to the boundary group.

Intranet clients can now access a CMG software update point when it's assigned to the boundary group. Admins can allow intranet devices to scan against a CMG software update point in the following scenarios:

- When an internet machine connects to the VPN, it will continue scanning against the CMG software update point over the internet.
- If the only software update point for the boundary group is the CMG software update point, then all intranet and internet devices will scan against it.

9. **Management Insights rules to optimize for remote workers** - We have added new rules in Management Insights to help you create better experiences for remote workers and reduce load on your infrastructure.

Management Insights

Top 10 Applicable Insight Rules				
Filter				
Insight Name	Group	Priority	Last Change	Status
Client settings aren't configured to allow clients to download delta content	Software Updates	Critical	26-Jun-2020 1:07 PM	Action Needed
Distribution points not serving content to clients	Proactive Maintenance	Recommended	26-Jun-2020 1:07 PM	Action Needed
Unused boot images	Proactive Maintenance	Recommended	26-Jun-2020 1:07 PM	Action Needed
Enable devices to be hybrid Azure Active Directory joined	Cloud Services	Recommended	26-Jun-2020 1:07 PM	Action Needed
Assess co-management readiness	Cloud Services	Recommended	26-Jun-2020 1:07 PM	Action Needed
Upgrade Readiness will be retired soon. Check out the new Desktop Analytics service	Cloud Services	Recommended	26-Jun-2020 1:07 PM	Action Needed
Unused boot images	Operating System Deployment	Recommended	26-Jun-2020 1:07 PM	Action Needed
Enable cloud management gateway	Cloud Services	Recommended	26-Jun-2020 9:42 PM	Action Needed
Target Endpoint security policies from Microsoft Endpoint Manager admin center	Cloud Services	Recommended	26-Jun-2020 9:42 PM	Action Needed
Define VPN boundary groups	Optimize for remote workers	Recommended	26-Jun-2020 9:42 PM	Action Needed

This release adds a new group of **management insights**, **Optimize for remote workers**. These insights help you create better experiences for remote workers and reduce load on your infrastructure. The insights in this release primarily focus on VPN:

- **Define VPN boundary groups:** Create a VPN boundary and associate it to a boundary group. Associate VPN-specific site systems to the group, and configure the settings for your environment. This insight checks for at least one boundary group with at least one VPN boundary in it. From the properties of this insight, select **Review Actions** to go to the **Boundary Groups** node. For more information, see **VPN boundary type**.
- **Configure VPN connected clients to prefer cloud based content sources:** To reduce traffic on the VPN, enable the boundary group option to **Prefer cloud based sources over on-premises sources**. This option allows clients to download content from the internet instead of distribution points across the VPN. For more information, see **Boundary group options**.
- **Disable peer to peer content sharing for VPN connected clients:** To prevent unnecessary peer-to-peer traffic that likely doesn't benefit the remote clients, disable the boundary group option to **Allow peer downloads in this boundary group**. For more information, see **Boundary group options**.

Create Boundary

General | **Boundary Groups**

Configure settings for this boundary

Description:

Type: **VPN**

Network: **VPN**

Subnet mask:

Subnet ID:

NOTE: The Network and Subnet mask values are used to calculate the Subnet ID and are not saved.

OK Cancel Apply

This release improves upon the new VPN boundary type first introduced in **technical preview version 2005**. You can now create more than one VPN boundary, and can detect the connection by the VPN name or description. When you open the **Create Boundary** page, and select the **VPN** type, choose one of the following options:

- **Auto detect VPN:** This option is the same behavior as before. The boundary value in the console list will be **AUT:1**. It should detect any VPN solution that uses the point-to-point tunneling protocol (PPTP). If it doesn't detect your VPN, use one of the other options.
- **Connection name:** Specify the name of the VPN connection on the device. It's the name of the network adapter in Windows for the VPN connection. Configuration Manager matches the first 251 characters of the string, but doesn't support wildcard characters or partial strings. The boundary value in the console list will be **NAM:<name>**, where **<name>** is the connection name that you specify.

For example, you run the `ipconfig` command on the device, and one of the sections starts with: `PPP adapter ContosoVPN: .` Use the string `ContosoVPN` as the **Connection name**. It displays in the list as **NAM:ContosoVPN**.

- **Connection description:** Specify the description of the VPN connection. Configuration Manager matches the first 251 characters of the string, but doesn't support wildcard characters or partial strings. The boundary value in the console list will be **DES:<description>**, where **<description>** is the connection description that you specify.

For example, you run the `ipconfig /all` command on the device, and one of the connections includes the following line: `Description : ContosoMainVPN`. Use the string `ContosoMainVPN` as the **Connection description**. It displays in the list as **DES:ContosoMainVPN**.

In every case, the device needs to be connected to the VPN for Configuration Manager to associate the client in that boundary.

10. **Windows 10 Enterprise multi-session platform support** - The 'Windows 10 Enterprise multi-session' platform is now available in the list of supported OS versions on objects with requirement rules or applicability lists.

The **Windows 10 Enterprise multi-session** platform is available in the list of supported OS versions on objects with requirement rules or applicability lists.

For more information on Configuration Manager's support for Windows Virtual Desktop, see [Supported OS versions for clients and devices](#).

📘 **Note**

If you previously selected the top-level **Windows 10** platform, this action automatically selected all child platforms. This new platform isn't automatically selected. If you want to add **Windows 10 Enterprise multi-session**, manually select it in the list.

11. **Wipe and Load OSD task sequence** initiated from software center can be run over cloud management gateway - It is now supported to run a wipe and load task sequence from software center whilst a client is communicating with a CMG.
12. **Tenant Attach:** Improvements to Configuration Manager actions in Microsoft Endpoint Manager admin center - This release introduces some improvements to the administration of Configuration Manager devices in Microsoft Endpoint Manager admin center. Improvements include:

- Configuration errors now include links to documentation to help you troubleshoot.
- User available applications now appear in the **Applications** node for a ConfigMgr device.
 - The application list includes applications deployed to a user currently logged on to the device.
 - Multi-user session scenarios aren't supported.
 - Azure AD joined devices aren't currently supported, only AD joined devices.

To deploy an application to a user, install the latest version of the Configuration Manager client, then follow the instructions in [Tenant attach: Install an application from the admin center](#).

13. **CMG support for endpoint protection policies** - While the cloud management gateway (CMG) has supported endpoint protection policies, devices required access to on-premises domain controllers. Starting in this release, clients that communicate via a CMG can immediately apply endpoint protection policies without an active connection to Active Directory.

This concludes TP2006

Thanks

Ram Lan

27th June 2020