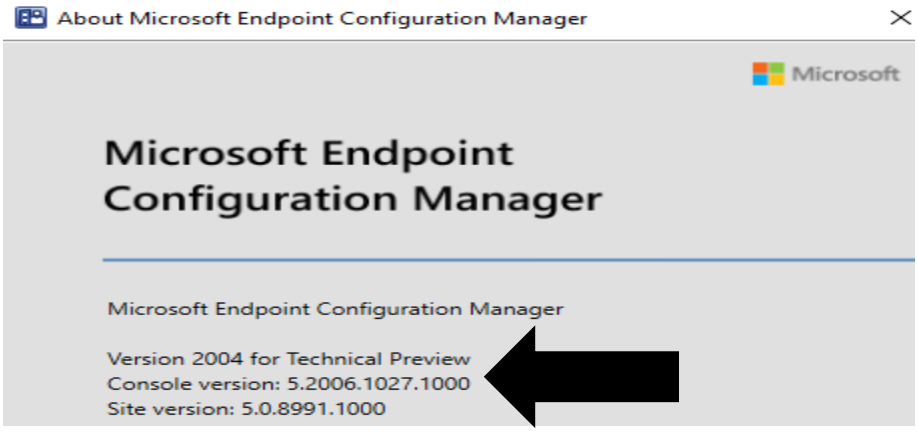
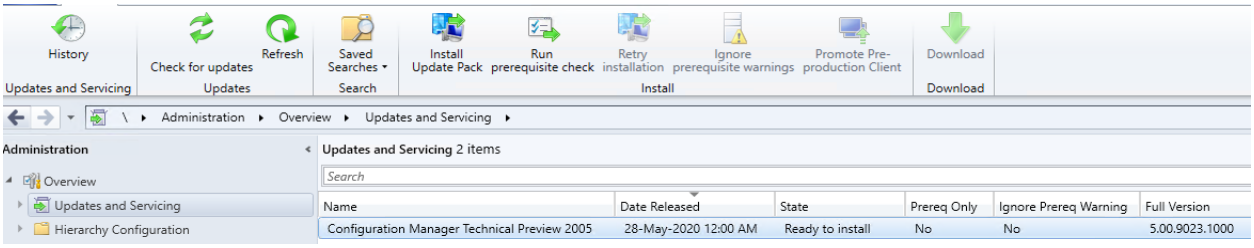
Installing Technical Preview 2005

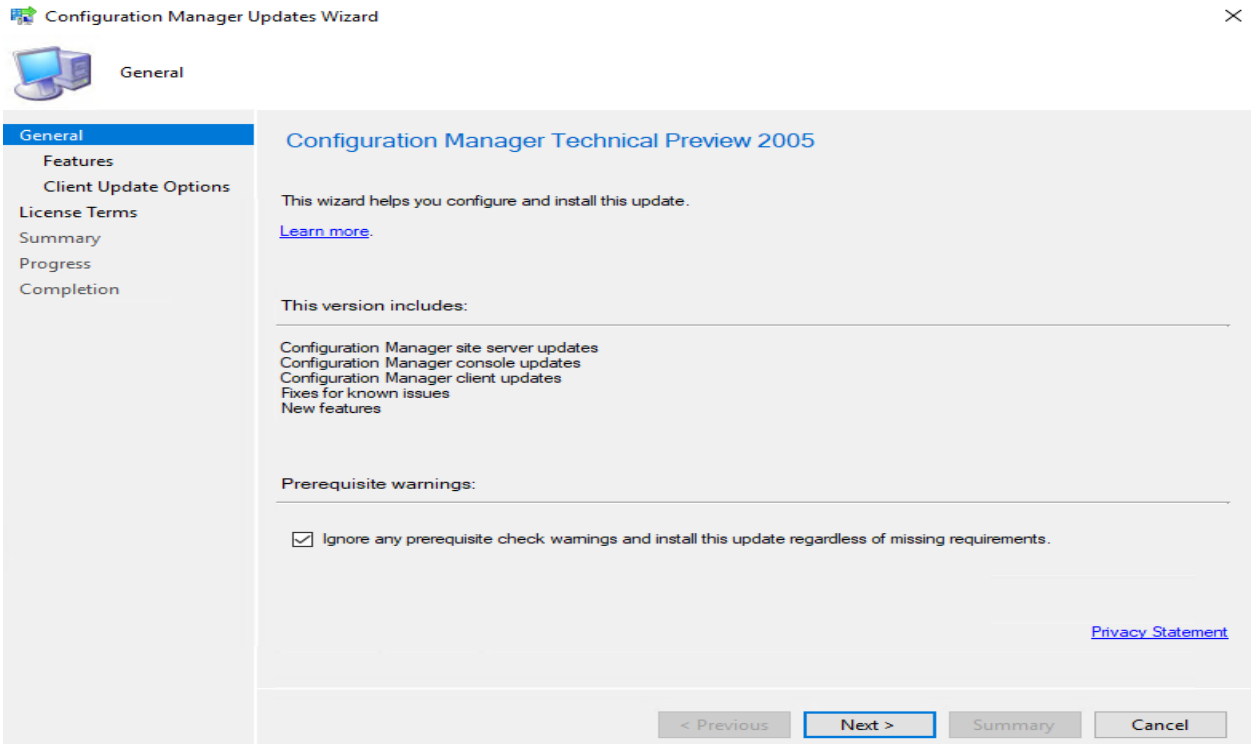
In this post, I will show you how to install TP2005 and explore new features. I am currently running TP2004. Will upgrade to TP2005 within the console.

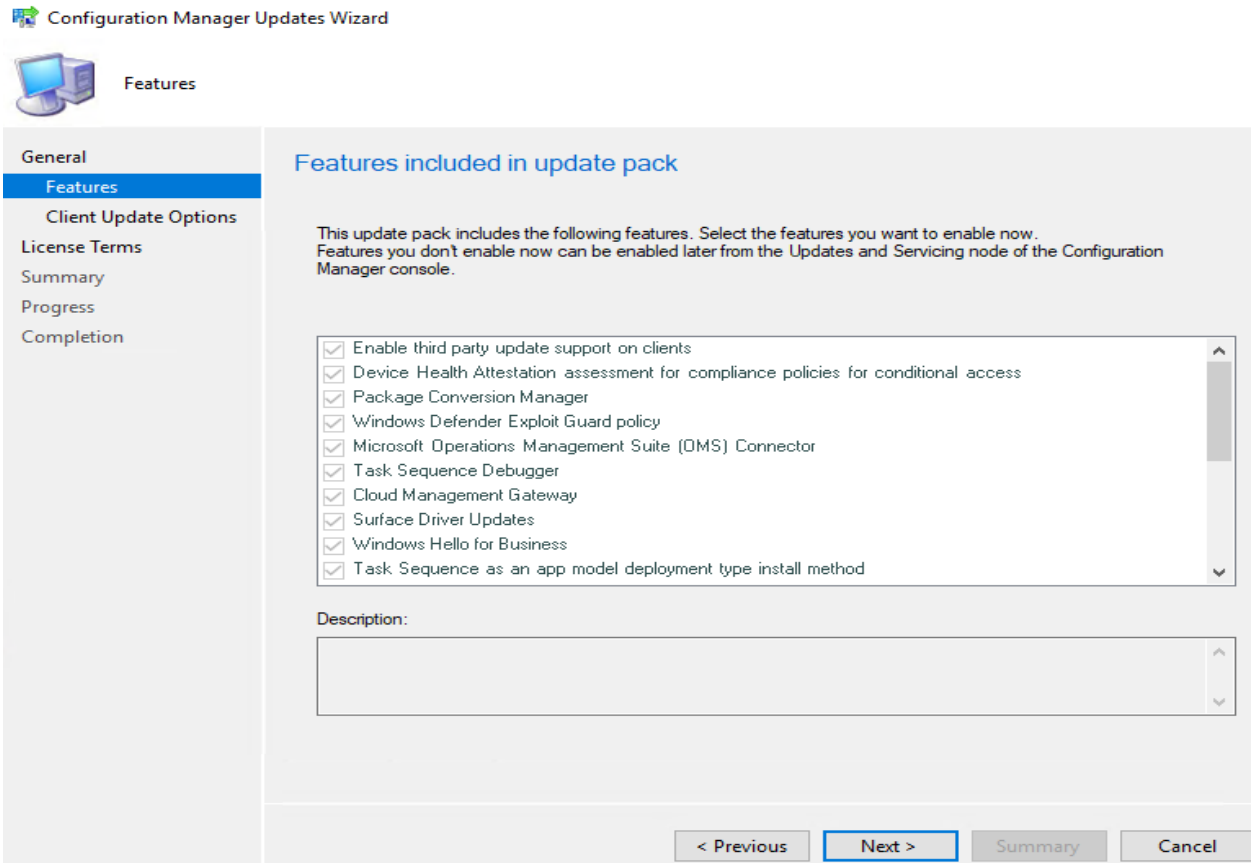


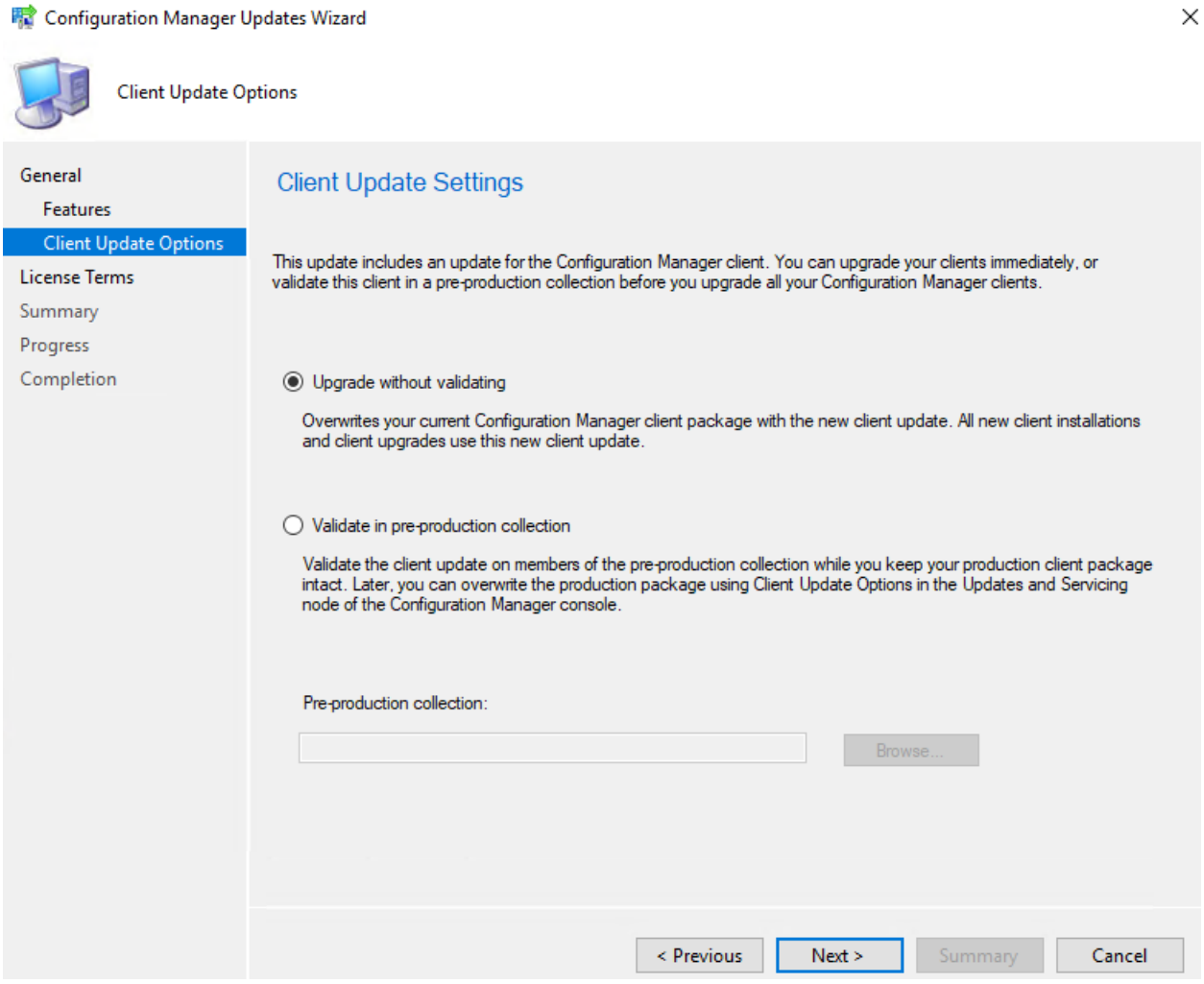
Visit these links for more info on Tp2005

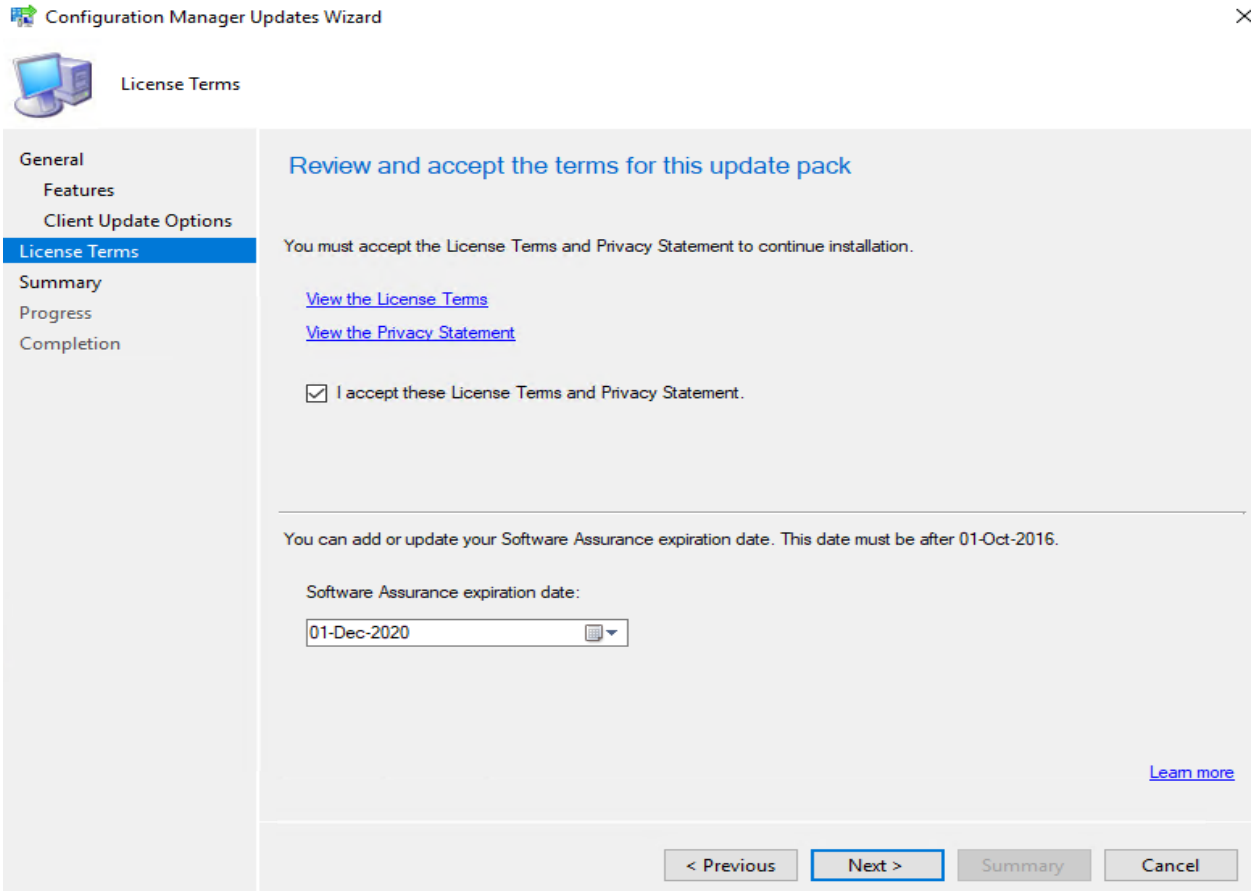
https://docs.microsoft.com/en-us/mem/configmgr/core/get-started/2020/technical-preview-2005?WT.mc_id=twitter
https://techcommunity.microsoft.com/t5/configuration-manager-blog/perform-real-time-management-in-mem-admin-center-with/ba-p/1428015

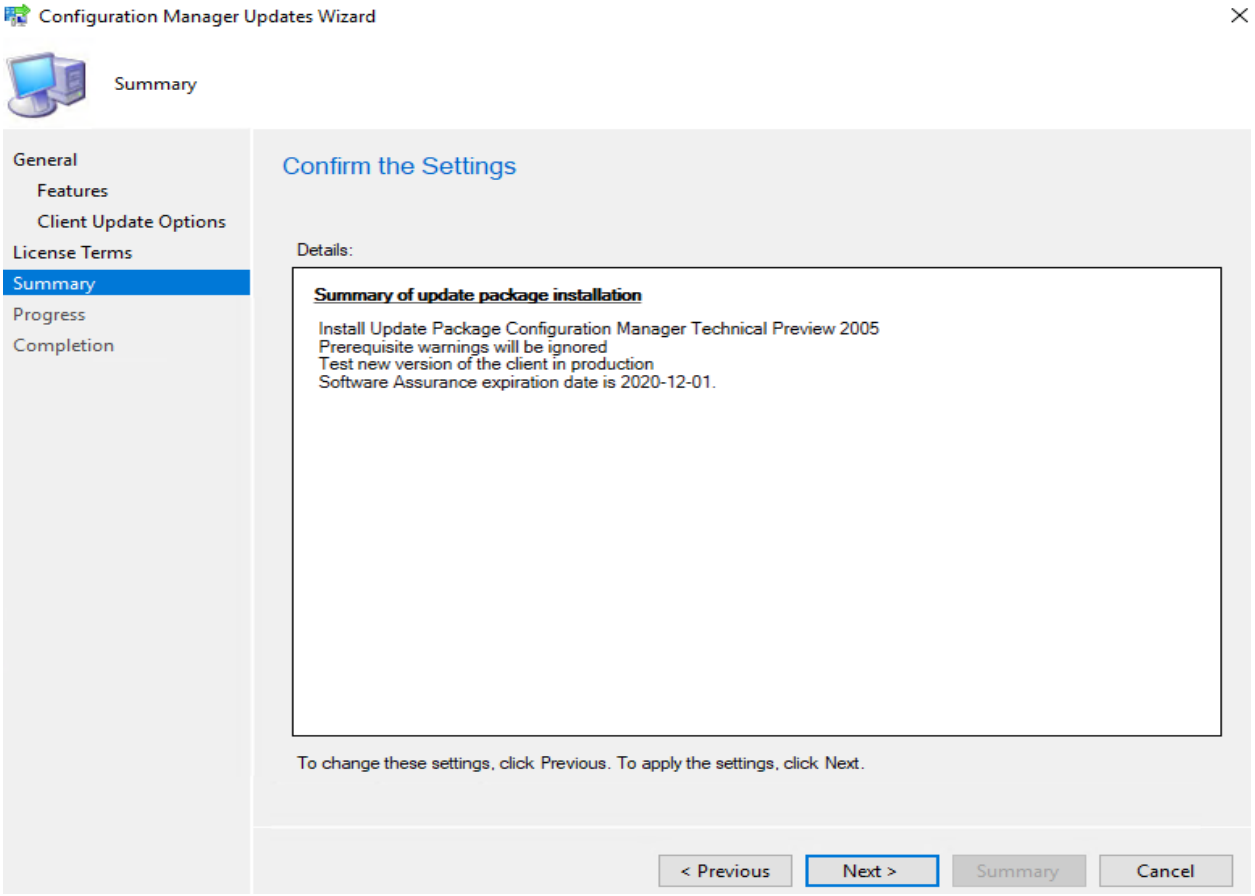


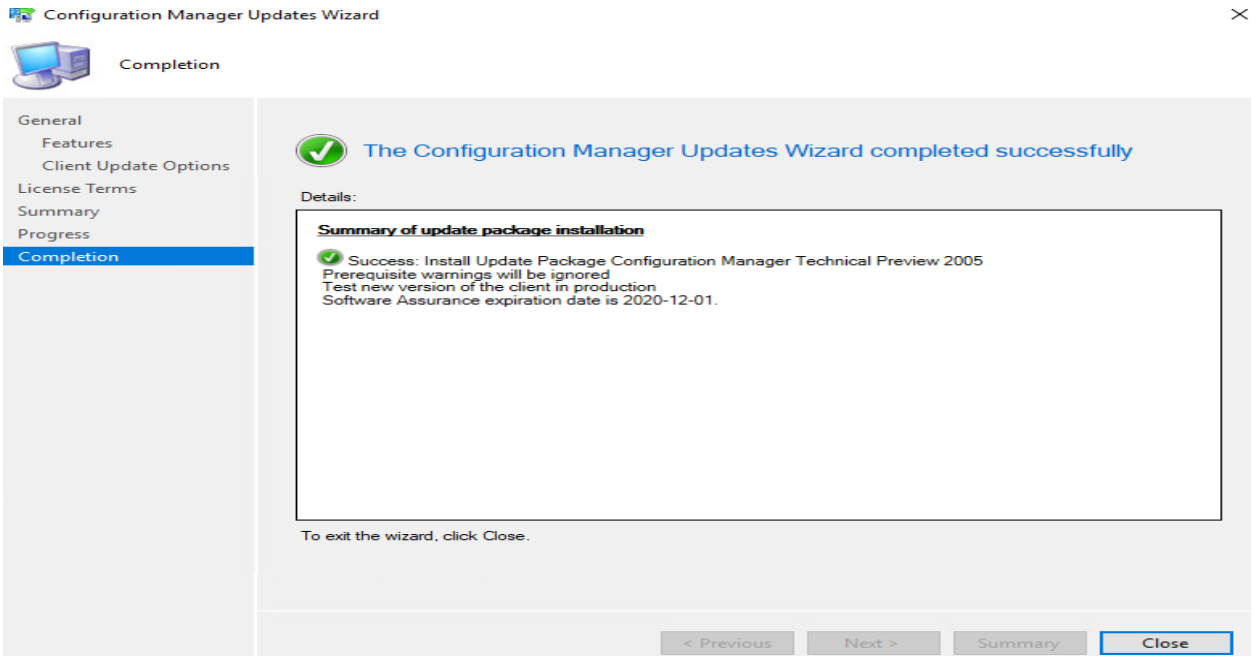


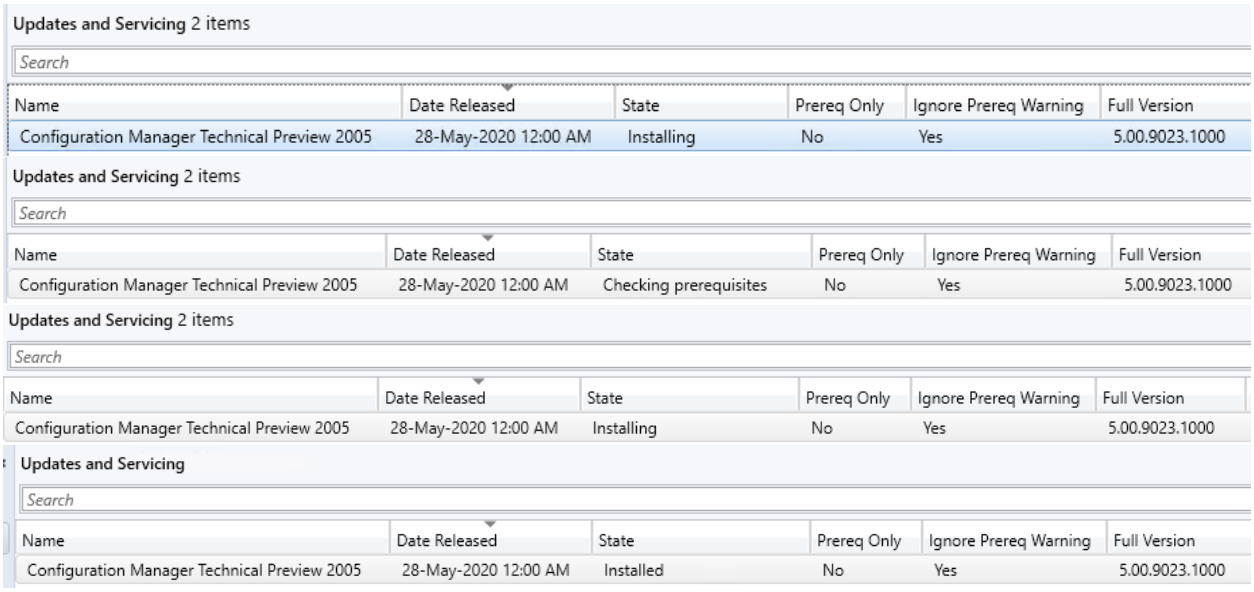

Configuration Manager Updates Wizard
Features
General
Features
Client Update Options
License Terms
Summary
Progress
Completion
Features included in update pack
This update pack includes the following features. Select the features you want to enable now.
Features you don't enable now can be enabled later from the Updates and Servicing node of the Configuration Manager console.
Enable third party update support on clients
Device Health Attestation assessment for compliance policies for conditional access
Package Conversion Manager
Windows Defender Exploit Guard policy
Microsoft Operations Management Suite (OMS) Connector
Task Sequence Debugger
Cloud Management Gateway
Surface Driver Updates
Windows Hello for Business
Task Sequence as an app model deployment type install method
Description:
< Previous
Next >
Summary
Cancel

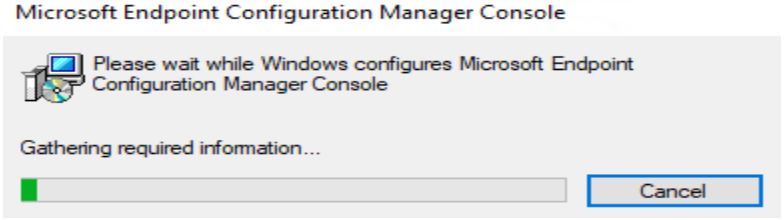

Configuration Manager Updates Wizard
Client Update Options
General
Features
Client Update Options
License Terms
Summary
Progress
Completion
Client Update Settings
This update includes an update for the Configuration Manager client. You can upgrade your clients immediately, or validate this client in 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

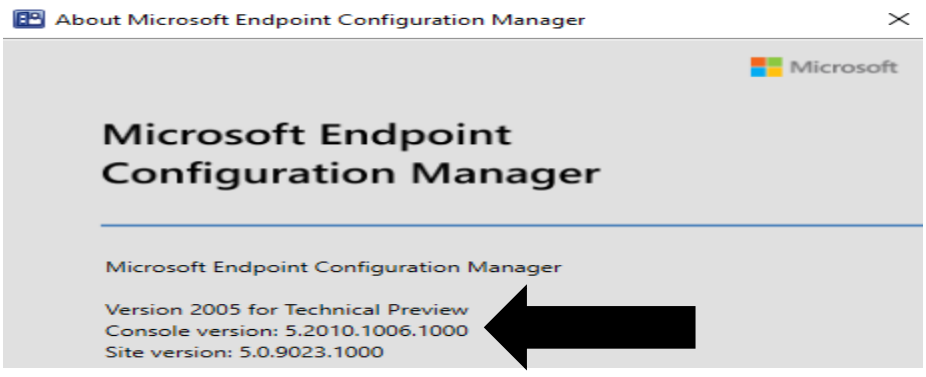

Configuration Manager Updates Wizard
License Terms
General
Features
Client Update Options
License Terms
Summary
Progress
Completion
Review and accept the terms for this update pack
You must accept the License Terms and Privacy Statement to continue installation.
View the License Terms
View the Privacy 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


Configuration Manager Updates Wizard
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 2005
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

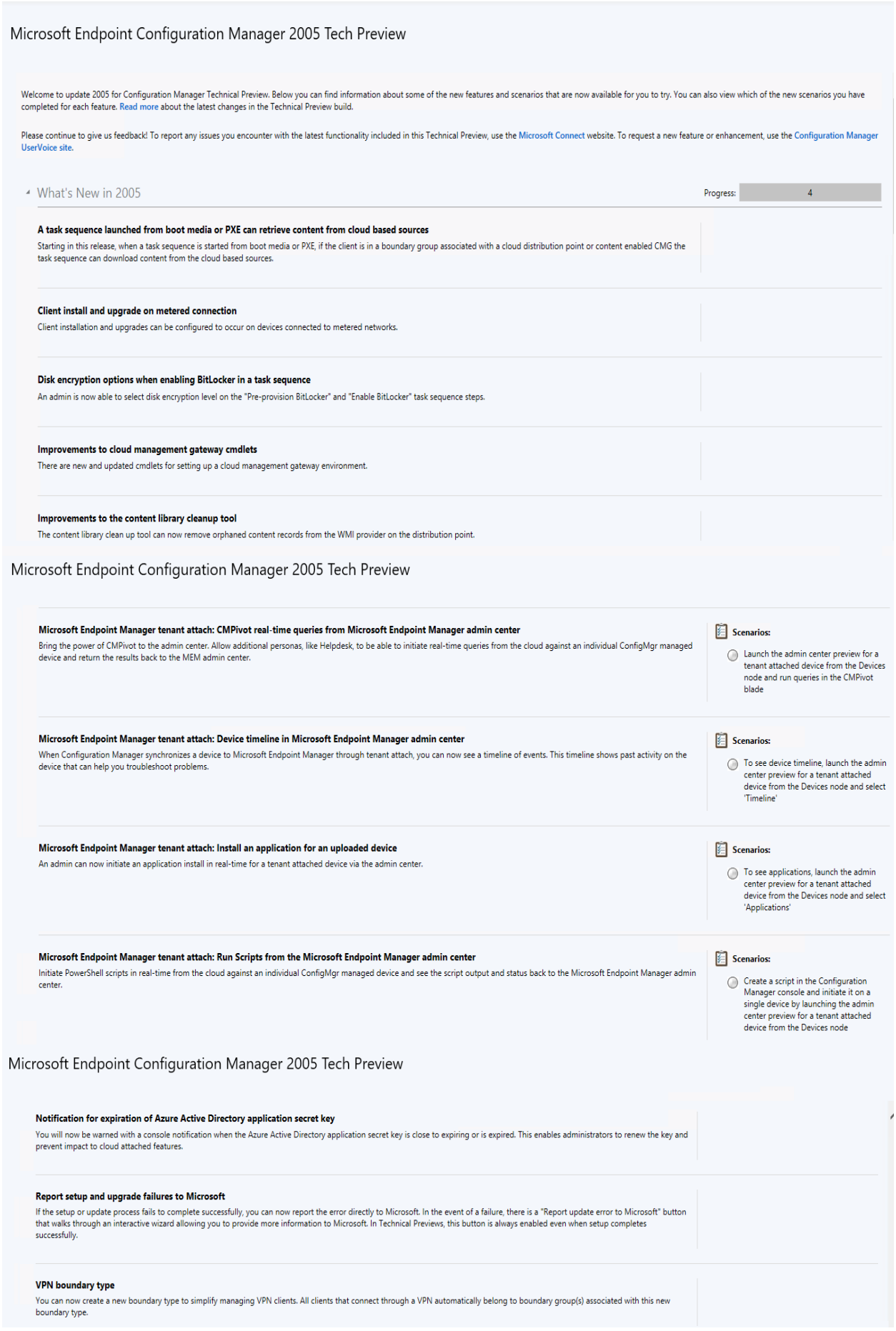

Configuration Manager Updates Wizard
Completion
General
Features
Client Update Options
License Terms
Summary
Progress
Completion
The Configuration Manager Updates Wizard completed successfully
Details:
Summary of update package installation
Success: Install Update Package Configuration Manager Technical Preview 2005
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
Configuration Manager Technical Preview 2005
28-May-2020 12:00 AM
Installing
No
Yes
5.00.9023.1000
Updates and Servicing 2 items
Search
Name
Date Released
State
Prereq Only
Ignore Prereq Warning
Full Version
Configuration Manager Technical Preview 2005
28-May-2020 12:00 AM
Checking prerequisites
No
Yes
5.00.9023.1000
Updates and Servicing 2 items
Search
Name
Date Released
State
Prereq Only
Ignore Prereq Warning
Full Version
Configuration Manager Technical Preview 2005
28-May-2020 12:00 AM
Installing
No
Yes
5.00.9023.1000
Updates and Servicing
Search
Name
Date Released
State
Prereq Only
Ignore Prereq Warning
Full Version
Configuration Manager Technical Preview 2005
28-May-2020 12:00 AM
Installed
No
Yes
5.00.9023.1000


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
Microsoft Endpoint Configuration Manager
Microsoft Endpoint Configuration Manager
Version 2005 for Technical Preview
Console version: 5.2010.1006.1000
Site version: 5.0.9023.1000

Below are new features in TP2005



NEW FEATURES:

1. A task sequence launched from boot media or PXE can retrieve content from cloud based sources – Starting in this release, when a task sequence is started from boot media or PXE, if the client is in a boundary group associated with a cloud distribution point or content enabled CMG the task sequence can download content from the cloud based sources.

Task sequence media support for cloud-based content

Even though there are more remote devices to manage these days, you may still have business processes to recover devices using task sequence media. For example, you send a USB key to a remote user to reimage their device. Or a remote office that has a local PXE server, but devices mainly connect to your main network over the internet. Instead of further taxing the VPN to download large OS deployment content, boot media and PXE deployments can now get content from cloud-based sources. For example, a cloud management gateway (CMG) that you enable to share content.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. Enable the following client setting in the **Cloud Services** group: **Allow access to cloud distribution point**. Make sure the client setting is deployed to the target clients. For more information, see the following articles:
   - How to configure client settings
   - About client settings - Cloud services
2. For the boundary group that the client is in, associate the content-enabled CMG or cloud distribution point site systems. For more information, see Configure a boundary group.
3. On the same boundary group, enable the following option: **Prefer cloud based sources over on-premise sources**. For more information, see Boundary group options for peer downloads.
4. Distribute the content referenced by the task sequence to the content-enabled CMG or cloud distribution point.
5. Start the task sequence from boot media or PXE on the client.

When the task sequence runs, it will download content from the cloud-based sources. Review **smsts.log** on the client.

2. Client install and upgrade on metered connection – Client installation and upgrades can be configured to occur on devices connected to metered networks.

Previously, if the device was connected to a metered network, new clients wouldn't install. Existing clients only upgraded if you allowed all client communication. For devices that are frequently roaming on a metered network, they would be unmanaged or on an older client version. Starting in this release, client install and upgrade both work when you set the client setting **Client communication on metered internet connections** to **Allow**.

To define the behavior for a new client installation, there's a new ccmsetup parameter **/AllowMetered**. When you allow client communication on a metered network for ccmsetup, it downloads the content, registers with the site, and downloads the initial policy. Any further client communication follows the configuration of the client setting from that policy.

If you reinstall the client on an existing device, it uses the following priority to determine its configuration:

1. Existing local client policy
2. The last command line stored in the Windows registry
3. Parameters on the ccmsetup command line

For more information, see the following articles:

- About client settings
- About client installation parameters and properties

Known issue with install and upgrade on metered connections

If you configure the client setting to **Limit**, the client won't install or upgrade. To work around this issue, configure the client setting to **Allow**.

3. Disk encryption options when enabling BitLocker in a task sequence - An admin is now able to select disk encryption level on the "Pre-provision BitLocker" and "Enable BitLocker" task sequence steps.

Based on your UserVoice feedback, you can now specify the **Disk encryption mode** on the Enable BitLocker and Pre-provision BitLocker task sequence steps. By default, the steps continue to use the default encryption method for the OS version. Use the new setting to select one of the following encryption algorithms: AES_128, AES_256, XTS_AES256, or XTS_AES128.

If the step runs on a version of Windows that doesn't support the specified algorithm, it falls back to the OS default. In this circumstance, the task sequence engine sends status message 11911.

If you use the following PowerShell cmdlets to configure these task sequence steps, use the new **EncryptionMethod** parameter:

- Set-CMTSStepEnableBitLocker
- New-CMTSStepEnableBitLocker
- Set-CMTSStepOfflineEnableBitLocker
- New-CMTSStepOfflineEnableBitLocker

4. Improvements to cloud management gateway cmdlets - There are new and updated cmdlets for setting up a cloud management gateway environment.

With more customers managing remote devices now, this release includes several new and improved Windows PowerShell cmdlets for the cloud management gateway (CMG). You can use these cmdlets to automate the creation, configuration, and management of the CMG service and Azure Active Directory (Azure AD) requirements.

> ⓘ **Note**
>
> While some of the new cmdlets might work with other Azure services, they're only tested with the **Cloud management** connection to support the CMG.

For example, an Azure administrator first creates the two required apps in Azure Active Directory (Azure AD). Then you write a script that uses the following cmdlets to deploy a CMG:

1. **Import-CMAADServerApplication**: Create the Azure AD server app definition in Configuration Manager.
2. **Import-CMAADClientApplication**: Create the Azure AD client app definition in Configuration Manager.
3. Use **Get-CMAADApplication** to get the app objects, and then pass to **New-CMCloudManagementAzureService** to create the Azure service connection in Configuration Manager.
4. **New-CMCloudManagementGateway**: Create the CMG service in Azure.
5. **Add-CMCloudManagementGatewayConnectionPoint**: Create the CMG connection point site system.

For more information about the CMG, see Plan for the cloud management gateway.

For more information on using PowerShell with Configuration Manager, see Get started with Configuration Manager cmdlets.

You can continue to use the following existing CMG cmdlets:

- Add-CMCloudManagementGatewayConnectionPoint
- Get-CMCloudManagementGateway
- Get-CMCloudManagementGatewayConnectionPoint
- New-CMCloudManagementGateway
- Remove-CMCloudManagementGateway
- Remove-CMCloudManagementGatewayConnectionPoint
- Set-CMCloudManagementGateway
- Set-CMCloudManagementGatewayConnectionPoint
- Start-CMCloudManagementGateway
- Stop-CMCloudManagementGateway

5. Improvements to the content library cleanup tool - The content library clean up tool can now remove orphaned content records from the WMI provider on the distribution point.

If you remove content from a distribution point while the site system is offline, an orphaned record can exist in WMI. Over time, this behavior can eventually lead to a warning status on the distribution point. To mitigate the issue in the past, you had to manually remove the orphaned entries from WMI. Making a mistake during this process could cause more severe issues with the server.

The content library cleanup tool in delete mode could remove orphaned files from the content library. It can now also remove orphaned content records from the WMI provider on a distribution point. Run the tool with the `/delete` parameter for both use cases.

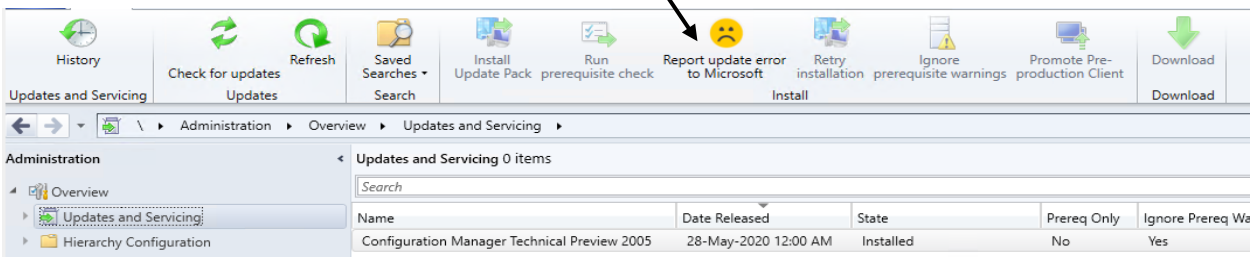
6. Notification for expiration of Azure Active Directory application secret key - You will now be warned with a console notification when the Azure Active Directory application secret key is close to expiring or is expired. This enables administrators to renew the key and prevent impact to cloud attached features.

Based on your UserVoice feedback, if you Configure Azure services to cloud-attach your site, the Configuration Manager console now displays notifications for the following circumstances:

- One or more Azure AD app secret keys will expire soon
- One or more Azure AD app secret keys have expired

To mitigate both cases, use the in-console action to Renew secret the key.

7. Report setup and upgrade failures to Microsoft - If the setup or update process fails to complete successfully, you can now report the error directly to Microsoft. In the event of a failure, there is a "Report update error to Microsoft" button that walks through an interactive wizard allowing you to provide more information to Microsoft. In Technical Previews, this button is always enabled even when setup completes successfully.



8. VPN boundary type - You can now create a new boundary type to simplify managing VPN clients. All clients that connect through a VPN automatically belong to boundary group(s) associated with this new boundary type

To simplify managing remote clients, you can now create a new boundary type for VPNs.

Previously, you had to create boundaries for VPN clients based on the IP address or subnet. This configuration could be challenging or not possible because of the subnet configuration or the VPN design.

Now when a client sends a location request, it includes additional information about its network configuration. Based upon this information, the server determines whether the client is on a VPN. All clients that connect through a VPN automatically belong to the boundary group associated with this new boundary type.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, go to the **Administration** workspace. Expand **Hierarchy Configuration**, and then select the **Boundaries** node.
2. In the ribbon, select **Create Boundary**.
3. Specify a **Description**, for example `VPN boundary`.
4. For the **Type**, select **VPN**. There are currently no additional configurations for this boundary type. Select **OK** to save and close.
5. Create a boundary group that includes this new VPN boundary. For more information, see Create a boundary group.

Known issues for VPN boundary

- You can only create one VPN boundary.
- The **Boundary** value in the console list is always `AUT:1`.
- The VPN detection logic may vary with different VPN solutions. If it doesn't work with your VPN, file a frown. Share details of your implementation to help improve the detection logic.

Lab Exercise – These new features (9 to 12) require Azure and Admin Center installed. I do not have Azure – Hence, I cannot complete these lab exercise.

9. Microsoft Endpoint Manager tenant attach: CMPivot real-time queries from Microsoft Endpoint Manager admin center - Bring the power of CMPivot to the admin center. Allow additional personas, like Helpdesk, to be able to initiate real-time queries from the cloud against an individual ConfigMgr managed device and return the results back to the MEM admin center.

Use CMPivot from the admin center preview

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace and select the **Devices** node.
2. Right-click on a device that's been uploaded to Microsoft Endpoint Manager.
3. In the right-click menu, select **Start** > **Admin Center Preview** to open the preview in your browser.
4. Select **CMPivot**, type your query in the script pane, then click **Run**.

10. Microsoft Endpoint Manager tenant attach: Device timeline in Microsoft Endpoint Manager admin center - When Configuration Manager synchronizes a device to Microsoft Endpoint Manager through tenant attach, you can now see a timeline of events. This timeline shows past activity on the device that can help you troubleshoot problems.

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace and select the **Devices** node.
2. Right-click on a device that's been uploaded to Microsoft Endpoint Manager.
3. In the right-click menu, select **Start** > **Admin Center Preview** to open the preview in your browser.
4. Click on **Timeline**. By default, you're shown events from the last 24 hours.

- Use the **Filter** button to change the **Time range**, **Event levels**, and **Provider name**.
- If you click on an event, you'll see the detailed message for it.
- The device sends events once a day to the admin center. Select **Refresh** to reload the page and have the device send new uncollected events to the admin center preview. You'll need to select **Refresh** again after a few minutes to see the newly collected events.

11. Microsoft Endpoint Manager tenant attach: Install an application for an uploaded device - An admin can now initiate an application install in real-time for a tenant attached device via the admin center.

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace and select the **Devices** node.
2. Right-click on a device that's been uploaded to Microsoft Endpoint Manager.
3. In the right-click menu, select **Start** > **Admin Center Preview** to open the preview in your browser.
4. Go to **Applications** in the admin center preview.
5. Select the application and click **Install**.

12. Microsoft Endpoint Manager tenant attach: Run Scripts from the Microsoft Endpoint Manager admin center - Initiate PowerShell scripts in real-time from the cloud against an individual ConfigMgr managed device and see the script output and status back to the Microsoft Endpoint Manager admin center.

1. In the Configuration Manager console, go to the **Assets and Compliance** workspace and select the **Devices** node.
2. Right-click on a device that's been uploaded to Microsoft Endpoint Manager.
3. In the right-click menu, select **Start** > **Admin Center Preview** to open the preview in your browser.
4. Select **Scripts**, then select one of your scripts. If needed, you can search by script name.
5. Click **Run script** from the page that appears on the right.

- You'll be notified your script has started. The **Run script** button will be disabled until it's complete.
- The **State** column is only valid while you're on the page. The state is reset to `Ready` if you navigate to another page.

6. When the script completes, the results will show in the **Output** pane. You can copy the text of the script output.

Thanks!

Ram Lan
30th May 2020