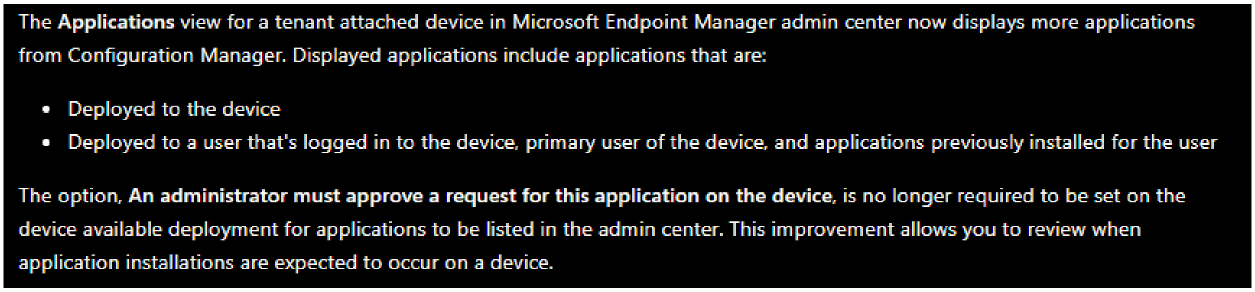
New Features in Current Branch 2103 – Configuration Manager

I will explore new features released in CB2103. Microsoft released this version on 5th April 2021. Here are the features.

Microsoft Endpoint Manager tenant attach - Display all applications for a device in Microsoft Endpoint Manager admin center.



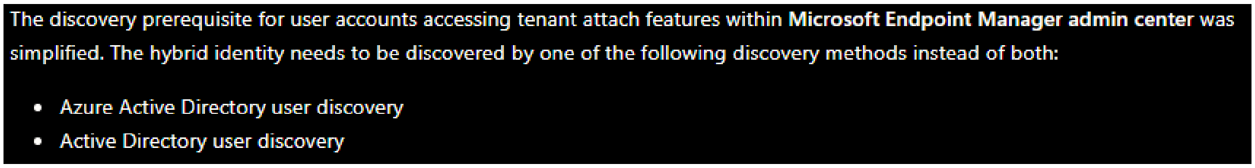
The **Applications** view for a tenant attached device in Microsoft Endpoint Manager admin center now displays more applications from Configuration Manager. Displayed applications include applications that are:

- Deployed to the device
- Deployed to a user that's logged in to the device, primary user of the device, and applications previously installed for the user

The option, **An administrator must approve a request for this application on the device**, is no longer required to be set on the device available deployment for applications to be listed in the admin center. This improvement allows you to review when application installations are expected to occur on a device.

Antivirus policy exclusions merge - When a tenant attached device is targeted with two or more antivirus policies, the settings for antivirus exclusions will merge before being applied to the client. This change results in the client receiving the exclusions defined in each policy, allowing for more granular control of antivirus exclusions.

User discovery prerequisite simplification -

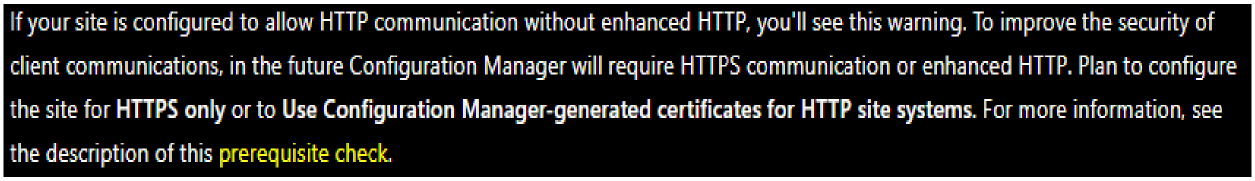


The discovery prerequisite for user accounts accessing tenant attach features within **Microsoft Endpoint Manager admin center** was simplified. The hybrid identity needs to be discovered by one of the following discovery methods instead of both:

- Azure Active Directory user discovery
- Active Directory user discovery

Application details - When tenant attach is enabled, the applications pane in the Microsoft Endpoint Manager admin center will show an Error Description if the application status is Failed.

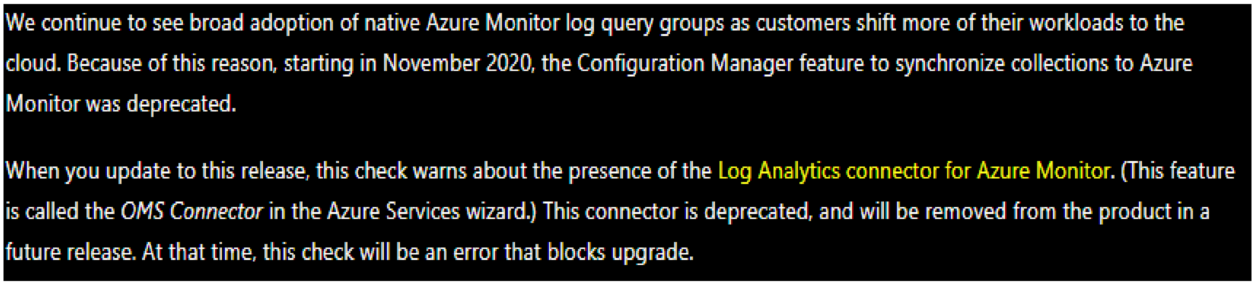
Enable the site for HTTPS-only or enhanced HTTP -



If your site is configured to allow HTTP communication without enhanced HTTP, you'll see this warning. To improve the security of client communications, in the future Configuration Manager will require HTTPS communication or enhanced HTTP. Plan to configure the site for **HTTPS only** or to **Use Configuration Manager-generated certificates for HTTP site systems.** For more information, see the description of this prerequisite check.

https://docs.microsoft.com/en-us/mem/configmgr/core/servers/deploy/install/list-of-prerequisite-checks#enable-site-system-roles-for-https-or-enhanced-http

Deprecated Azure Monitor connector -

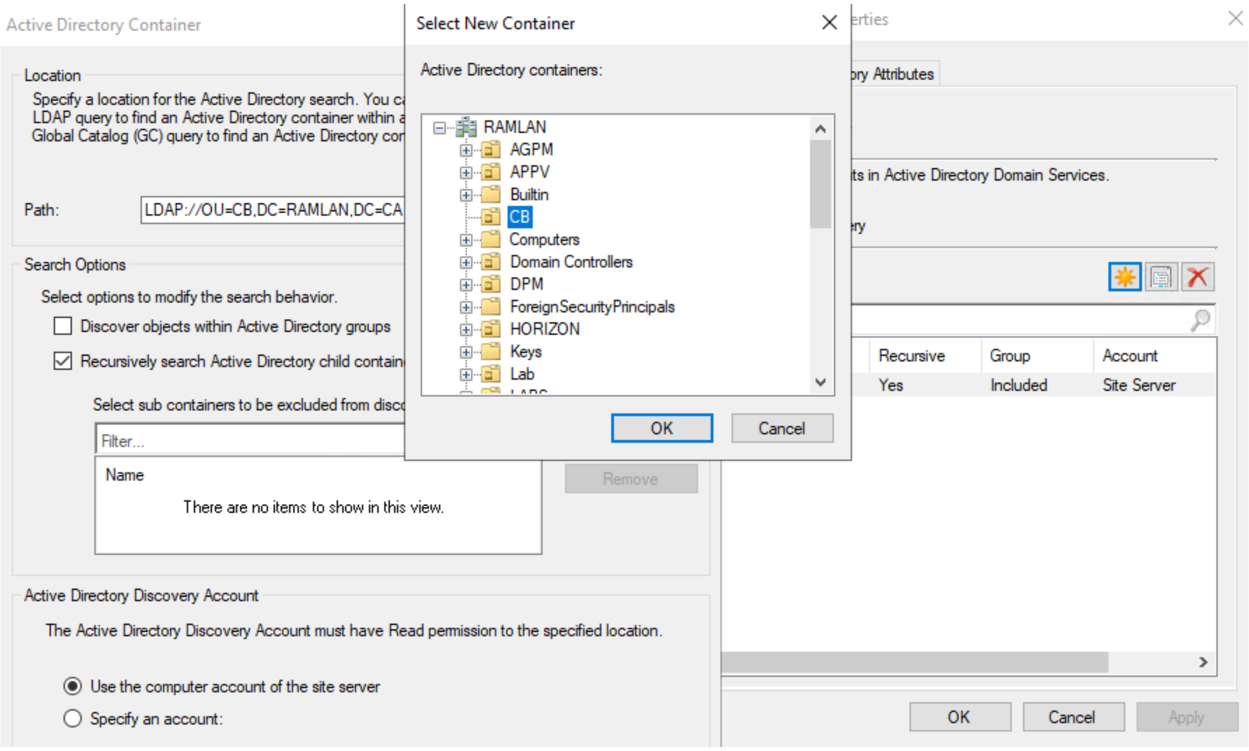


We continue to see broad adoption of native Azure Monitor log query groups as customers shift more of their workloads to the cloud. Because of this reason, starting in November 2020, the Configuration Manager feature to synchronize collections to Azure Monitor was deprecated.

When you update to this release, this check warns about the presence of the Log Analytics connector for Azure Monitor. (This feature is called the *OMS Connector* in the Azure Services wizard.) This connector is deprecated, and will be removed from the product in a future release. At that time, this check will be an error that blocks upgrade.

SQL Server Express version - If you have a secondary site that uses SQL Server Express edition, this check warns if the version is earlier than SQL Server 2016 with service pack 2 (13.0.5026.0).

Allow exclusion of organizational units (OU) from Active Directory User Discovery - You can now exclude OUs from Active Directory User Discovery.



Active Directory Container

Location

Specify a location for the Active Directory search. You c
LDAP query to find an Active Directory container within a
Global Catalog (GC) query to find an Active Directory cor

Path: LDAP://OU=CB,DC=RAMLAN,DC=CA

Search Options

Select options to modify the search behavior.

□ Discover objects within Active Directory groups

☑ Recursively search Active Directory child contain

Select sub containers to be excluded from disc

Filter...

Name
There are no items to show in this view.

Active Directory Discovery Account

The Active Directory Discovery Account must have Read permission to the specified location.

● Use the computer account of the site server

○ Specify an account:

Select New Container

Active Directory containers:

- RAMLAN
  - AGPM
  - APPV
  - Builtin
  - CB
  - Computers
  - Domain Controllers
  - DPM
  - ForeignSecurityPrincipals
  - HORIZON
  - Keys
  - Lab

erties

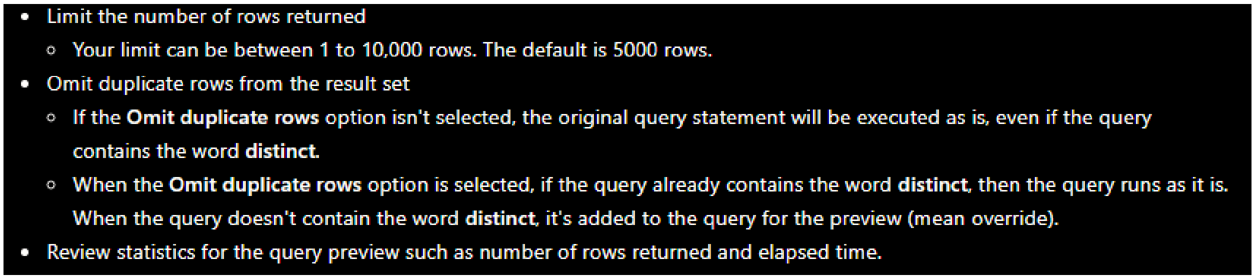
ry Attributes

ts in Active Directory Domain Services.

Recursive	Group	Account
Yes	Included	Site Server

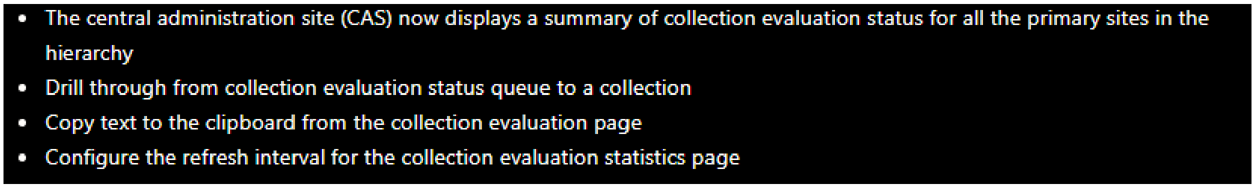
Improvements to the collection relationships viewer - Starting in version 2010, you can view dependency relationships between collections in a graphical format. The relationships for a collection were presented as two hierarchical trees, one for dependents and the other for dependencies. In this release, you can view both parent and child relationships together in a single graph. This change allows you to quickly see an overview of all the relationships of a collection at once and then drill down into specific related collections. It also includes other filtering and navigation improvements.

Improvements to query preview - You now have more options when using the collection query preview. The following improvements have been made to previewing collection queries:



- Limit the number of rows returned
  - Your limit can be between 1 to 10,000 rows. The default is 5000 rows.
- Omit duplicate rows from the result set
  - If the **Omit duplicate rows** option isn't selected, the original query statement will be executed as is, even if the query contains the word **distinct**.
  - When the **Omit duplicate rows** option is selected, if the query already contains the word **distinct**, then the query runs as it is. When the query doesn't contain the word **distinct**, it's added to the query for the preview (mean override).
- Review statistics for the query preview such as number of rows returned and elapsed time.

Improvements to collection evaluation view - The following improvements were made to the collection evaluation view:



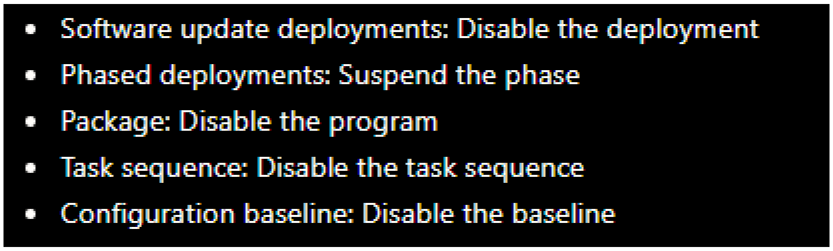
- The central administration site (CAS) now displays a summary of collection evaluation status for all the primary sites in the hierarchy
- Drill through from collection evaluation status queue to a collection
- Copy text to the clipboard from the collection evaluation page
- Configure the refresh interval for the collection evaluation statistics page

Change foreground color for Software Center branding - Software Center already provides various controls for you to customize the branding to support your organization's brand. For some customers, their brand color doesn't work well with the default white font color for a selected item. To better support these customers and improve accessibility, you can now configure a custom color for the foreground font.

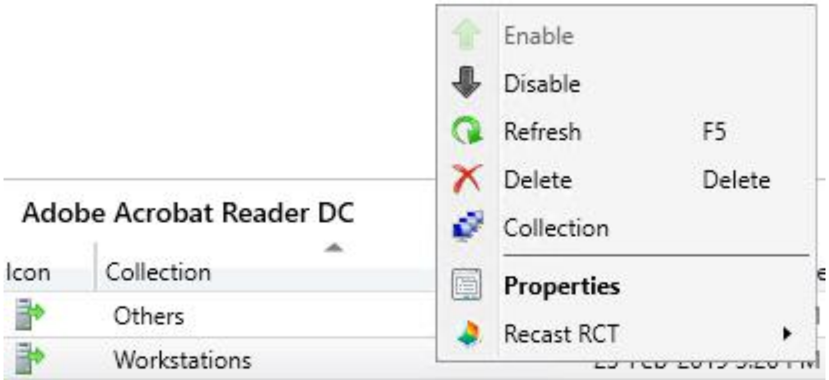
Improved user experience and security with Software Center custom tabs - Since current branch version 1906, you can add up to five custom tabs to Software Center. These custom tabs let you give your users easy access to common web apps and other sites. Previously, to display websites Software Center used the Windows built-in Internet Explorer browser control.

Starting in this release, Software Center can now use the Microsoft Edge WebView2 browser control. The WebView2 browser control provides improved security and user experience. For example, more websites should work with these custom tabs without displaying script errors or security warnings.

Disable application deployments - You can now disable application deployments. Other objects already have similar behaviors:

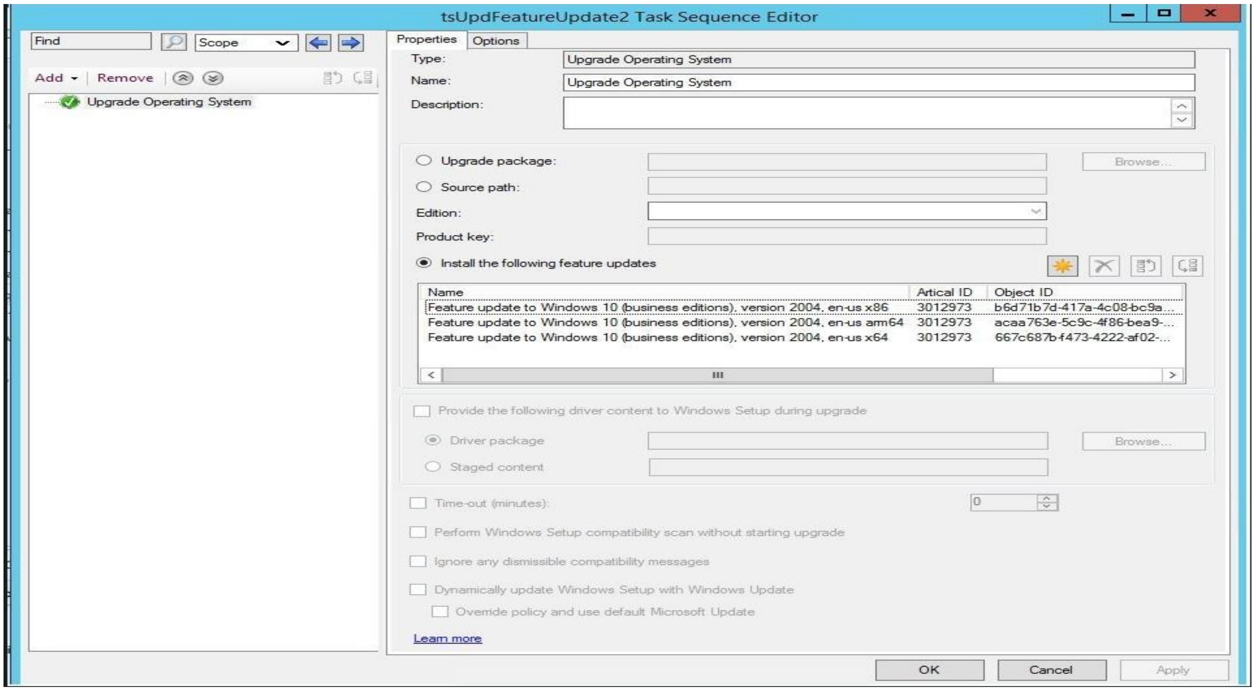


- Software update deployments: Disable the deployment
- Phased deployments: Suspend the phase
- Package: Disable the program
- Task sequence: Disable the task sequence
- Configuration baseline: Disable the baseline



Windows 10 Servicing dashboard changes - We've simplified the Windows 10 Servicing dashboard to make it more relevant. The new Quality Update Versions chart displays the top five revisions of Windows 10 across your devices. The Latest Feature Update chart shows the number of devices that installed the latest feature update. The Windows 10 Usage chart, showing the distribution of Windows 10 major releases, was renamed to Feature Update Versions. Servicing plan and Windows 10 ring information were removed from the dashboard.

Deploy a feature update with a task sequence - You can now upgrade a client's Windows OS by using a feature update deployed with a task sequence. This integration combines the simplicity of Windows servicing with the flexibility of task sequences. Servicing uses content that you synchronize through the software update point. This process simplifies the need to manually get, import, and maintain the Windows image content used with a standard task sequence to upgrade Windows. The size of the servicing ESD file is generally smaller than the OS upgrade package and WIM image file. You can also use Windows features such as Dynamic Update and Delivery Optimization.



Type: Upgrade Operating System

Name: Upgrade Operating System

Description:

○ Upgrade package:

○ Source path:

Edition:

Product key:

● Install the following feature updates

Name	Artical ID	Object ID
Feature update to Windows 10 (business editions), version 2004, en-us x86	3012973	b6d71b7d-417a-4c08-bc9a...
Feature update to Windows 10 (business editions), version 2004, en-us arm64	3012973	acaa763e-5c9c-4f86-bea9-...
Feature update to Windows 10 (business editions), version 2004, en-us x64	3012973	667c687b-f473-4222-af02-...

□ Provide the following driver content to Windows Setup during upgrade

● Driver package

○ Staged content

□ Time-out (minutes): 0

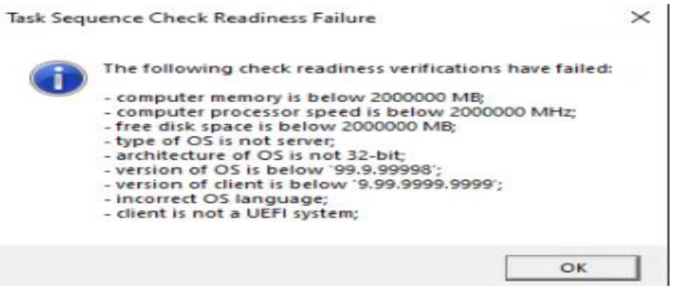
□ Perform Windows Setup compatibility scan without starting upgrade

□ Ignore any dismissible compatibility messages

□ Dynamically update Windows Setup with Windows Update

□ Override policy and use default Microsoft Update

Task sequence error shows more check readiness details - The task sequence progress can now display more information about readiness checks. If a task sequence fails because the client doesn't meet the requirements configured in the Check readiness task sequence step, the user can now see more details about the failed prerequisites.



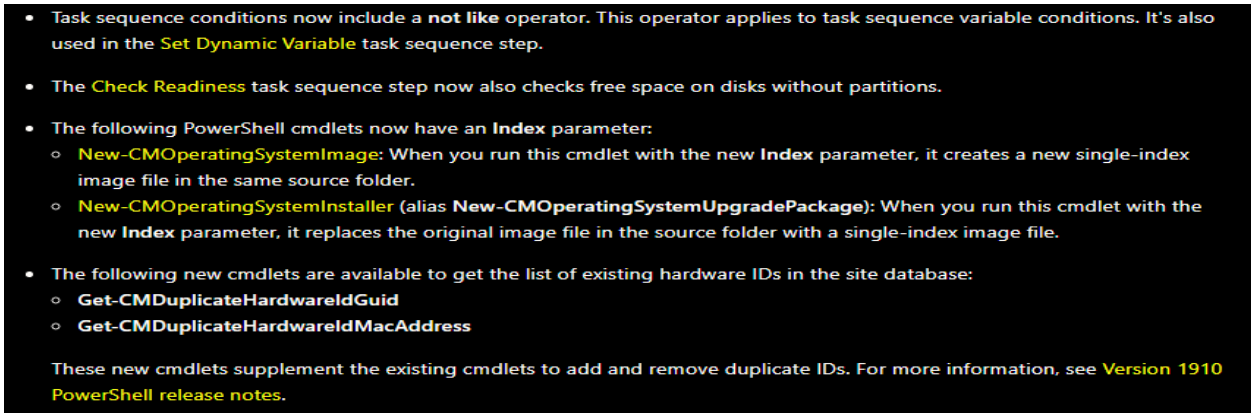
Task Sequence Check Readiness Failure

The following check readiness verifications have failed:

- computer memory is below 2000000 MB;
- computer processor speed is below 2000000 MHz;
- free disk space is below 2000000 MB;
- type of OS is not server;
- architecture of OS is not 32-bit;
- version of OS is below '99.9.99998';
- version of client is below '9.99.9999.9999';
- incorrect OS language;
- client is not a UEFI system;

Encryption algorithm to capture and restore user state - The task sequence steps to Capture User State and Restore User State always encrypt the USMT state store. Previously, Configuration Manager configured USMT to use the 3DES algorithm. Starting in this release, both steps now use the highest supported encryption algorithm, AES 256.

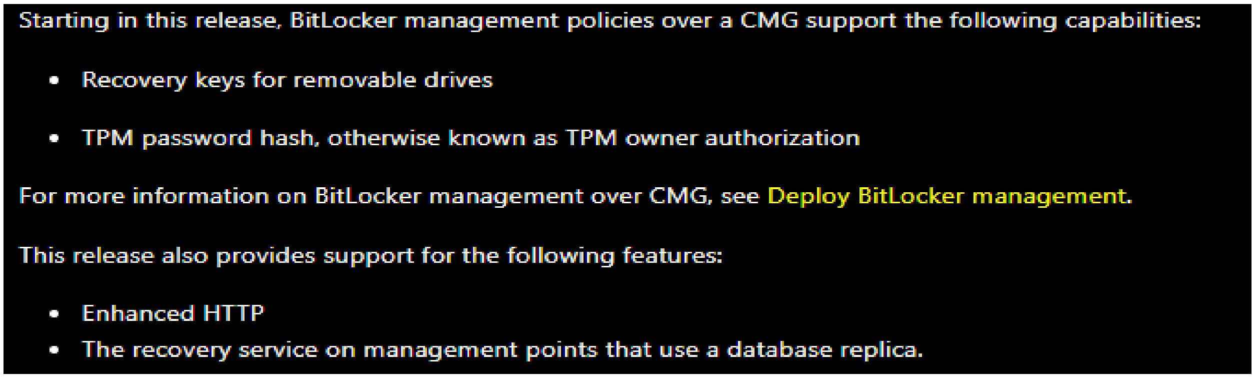
Improvements to OS deployment - This release includes the following improvements to OS deployment:



- Task sequence conditions now include a **not like** operator. This operator applies to task sequence variable conditions. It's also used in the Set Dynamic Variable task sequence step.
- The Check Readiness task sequence step now also checks free space on disks without partitions.
- The following PowerShell cmdlets now have an **Index** parameter:
  - New-CMOperatingSystemImage: When you run this cmdlet with the new **Index** parameter, it creates a new single-index image file in the same source folder.
  - New-CMOperatingSystemInstaller (alias **New-CMOperatingSystemUpgradePackage**): When you run this cmdlet with the new **Index** parameter, it replaces the original image file in the source folder with a single-index image file.
- The following new cmdlets are available to get the list of existing hardware IDs in the site database:
  - **Get-CMDuplicateHardwareIdGuid**
  - **Get-CMDuplicateHardwareIdMacAddress**

  These new cmdlets supplement the existing cmdlets to add and remove duplicate IDs. For more information, see Version 1910 PowerShell release notes.

Improvements to BitLocker management - In current branch version 2010, you can manage BitLocker policies and escrow recovery keys over a cloud management gateway (CMG). This support included a couple of limitations.



Starting in this release, BitLocker management policies over a CMG support the following capabilities:

- Recovery keys for removable drives
- TPM password hash, otherwise known as TPM owner authorization

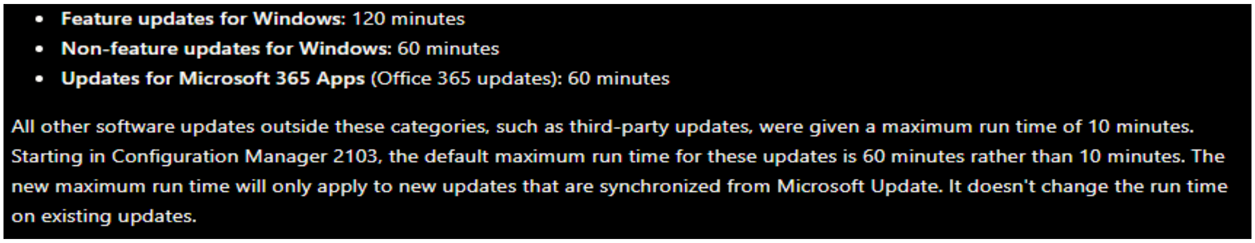
For more information on BitLocker management over CMG, see Deploy BitLocker management.

This release also provides support for the following features:

- Enhanced HTTP
- The recovery service on management points that use a database replica.

Approved scripts for orchestration groups - You can now select from scripts that have already been approved when configuring pre and post-scripts for an orchestration group. When in the Create Orchestration Group Wizard, you'll see a new page called Script Picker. Select your pre and post scripts from your list of scripts that are already approved. You can still add scripts manually on the pre and post-script pages. Additionally, you can also edit scripts that you pre-populated from the Script Picker.

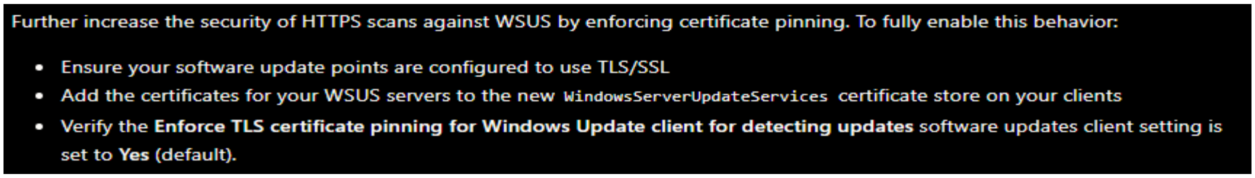
Change default maximum run time for software updates - Configuration Manager sets the following maximum run time for these categories of software updates:



- **Feature updates for Windows:** 120 minutes
- **Non-feature updates for Windows:** 60 minutes
- **Updates for Microsoft 365 Apps** (Office 365 updates): 60 minutes

All other software updates outside these categories, such as third-party updates, were given a maximum run time of 10 minutes. Starting in Configuration Manager 2103, the default maximum run time for these updates is 60 minutes rather than 10 minutes. The new maximum run time will only apply to new updates that are synchronized from Microsoft Update. It doesn't change the run time on existing updates.

TLS certificate pinning for devices scanning HTTPS-configured WSUS servers -



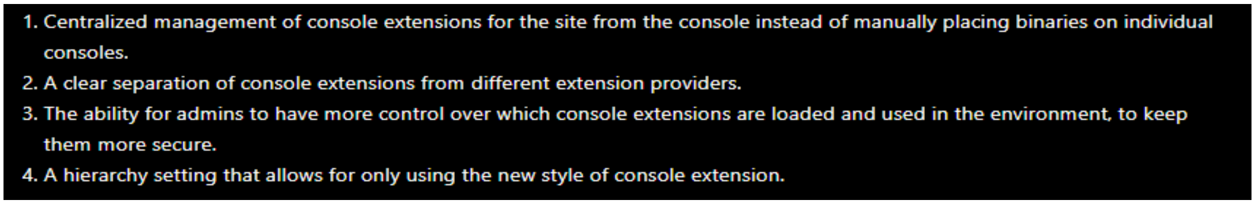
Further increase the security of HTTPS scans against WSUS by enforcing certificate pinning. To fully enable this behavior:

- Ensure your software update points are configured to use TLS/SSL
- Add the certificates for your WSUS servers to the new `WindowsServerUpdateServices` certificate store on your clients
- Verify the **Enforce TLS certificate pinning for Windows Update client for detecting updates** software updates client setting is set to **Yes** (default).

Download Power BI report templates from Community hub - Community hub now supports contributing and downloading Power BI report template files. This integration allows administrators to easily share and reuse Power BI reports. Contributing and downloading Power BI report template is also available for current branch versions of Configuration Manager.

Access the top queries shared in the Community hub from CMPivot - You can now access the top CMPivot queries shared in the Community hub from on-premises CMPivot. By leveraging pre-created CMPivot queries shared by the broader community, CMPivot users gain access to a wider variety of queries. On-premises CMPivot accesses the Community hub and returns a list of the top downloaded CMPivot queries. Users can review the top queries, customize them, and then run on-demand. This improvement gives a wider selection of queries for immediate usage without having to construct them and also allows information sharing on how to build queries for future reference.

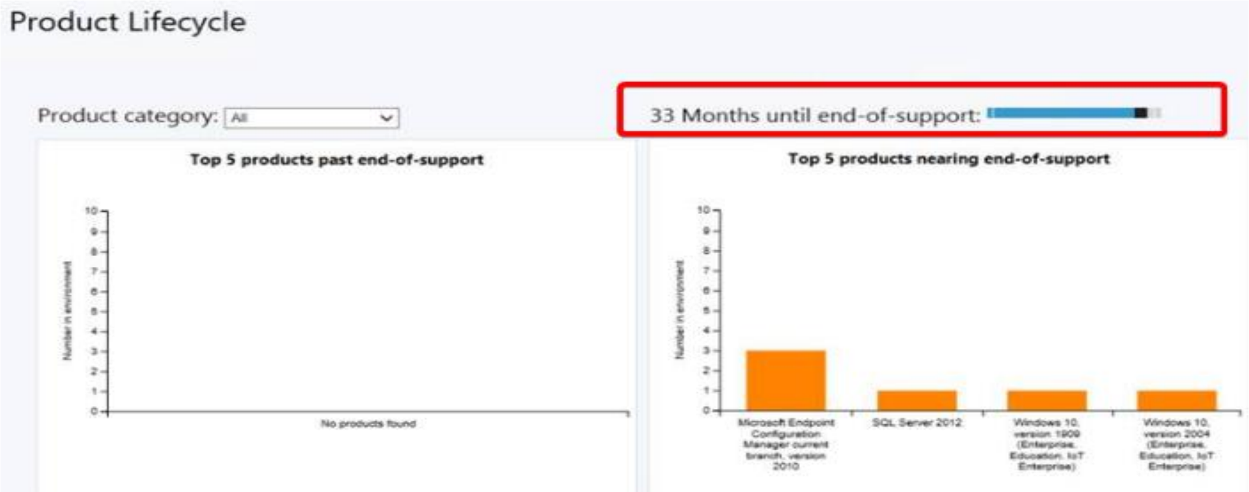
Centralized management of console extensions - Configuration Manager now supports a new style of console extensions that have the following benefits:



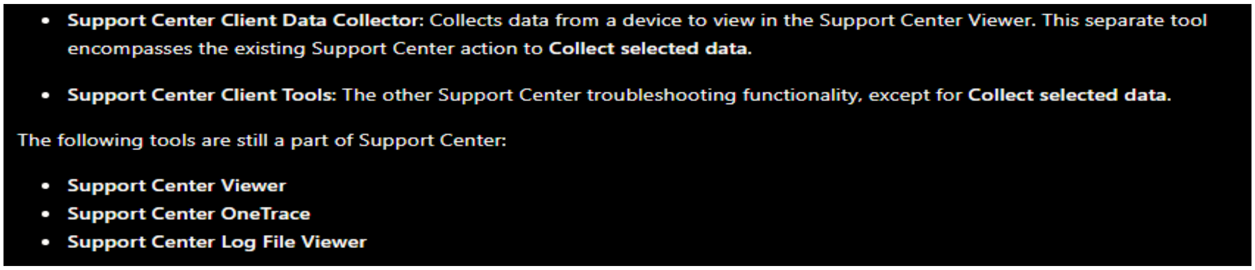
1. Centralized management of console extensions for the site from the console instead of manually placing binaries on individual consoles.
2. A clear separation of console extensions from different extension providers.
3. The ability for admins to have more control over which console extensions are loaded and used in the environment, to keep them more secure.
4. A hierarchy setting that allows for only using the new style of console extension.

Add a report as a favorite - Configuration Manager ships with several hundred reports by default, and you may have added more to that list. Instead of continually searching for reports you commonly use, you can now make a report a favorite. This action allows you to quickly access it from the new Favorites node.

Improvements to the product lifecycle dashboard - This release includes improvements to the product lifecycle dashboard to make it more actionable for you.


Product Lifecycle
Product category: All
33 Months until end-of-support:
Top 5 products past end-of-support
Number in environment
0
1
2
3
4
5
6
7
8
9
10
No products found
Top 5 products nearing end-of-support
Number in environment
Microsoft Endpoint Configuration Manager current branch, version 2010
SQL Server 2012
Windows 10, version 1909 (Enterprise, Education, IoT Enterprise)
Windows 10, version 2004 (Enterprise, Education, IoT Enterprise)

Improvements to Support Center - Support Center is now split into the following tools:

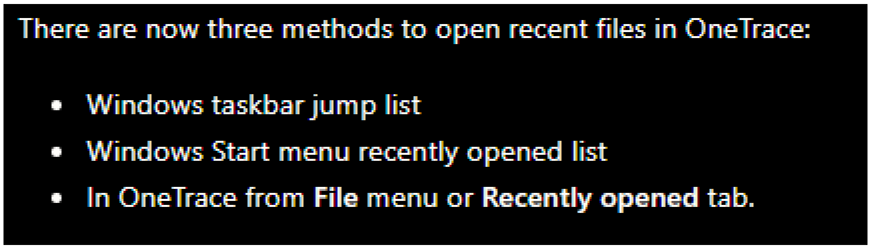


- **Support Center Client Data Collector:** Collects data from a device to view in the Support Center Viewer. This separate tool encompasses the existing Support Center action to **Collect selected data**.
- **Support Center Client Tools:** The other Support Center troubleshooting functionality, except for **Collect selected data.**

The following tools are still a part of Support Center:

- **Support Center Viewer**
- **Support Center OneTrace**
- **Support Center Log File Viewer**

OneTrace support for jump lists - Support Center OneTrace now supports jump lists for recently opened files. Jump lists let you quickly go to previously opened files, so you can work faster.



There are now three methods to open recent files in OneTrace:

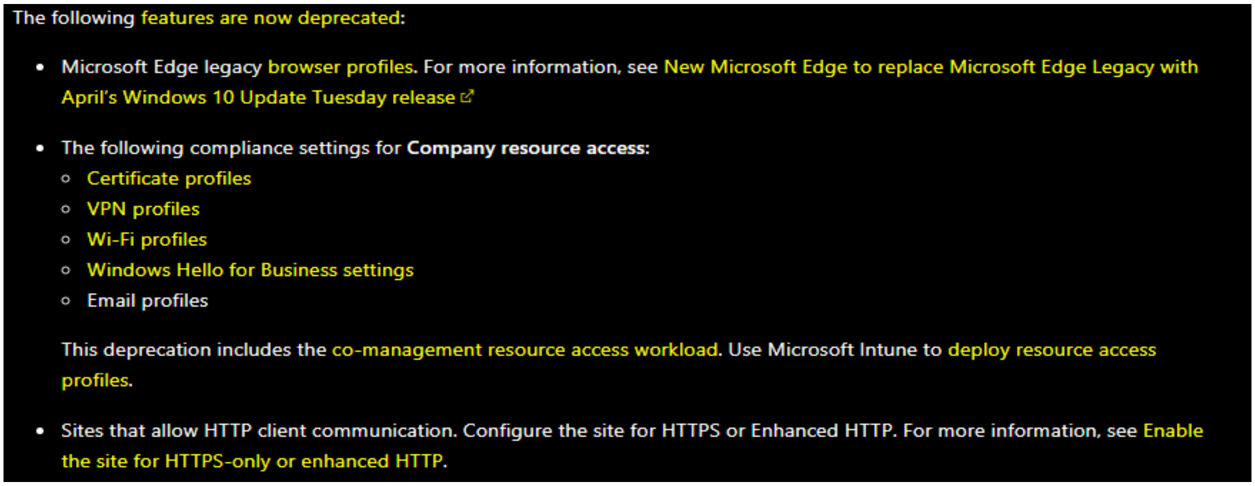
- Windows taskbar jump list
- Windows Start menu recently opened list
- In OneTrace from **File** menu or **Recently opened** tab.

Known issue with updateable PowerShell help - Starting in version 2010, you could use the Update-Help cmdlet to download the latest information for the Configuration Manager PowerShell module.

Because of a change in how the updateable content is structured and published with the release of version 2103, don't use Update-Help on a version 2010 site. Update the site to version 2103, and then update the local help content.

The cmdlet will successfully download content on a version 2010 console, but Get-Help will only return default usage information. Before the release of version 2103, if you used Update-Help with a version 2010 site, you can continue to use Get-Help now.

Depreciated Features – These are the following:



The following features are now deprecated:

- Microsoft Edge legacy browser profiles. For more information, see New Microsoft Edge to replace Microsoft Edge Legacy with April's Windows 10 Update Tuesday release
- The following compliance settings for **Company resource access:**
  - Certificate profiles
  - VPN profiles
  - Wi-Fi profiles
  - Windows Hello for Business settings
  - Email profiles

  This deprecation includes the co-management resource access workload. Use Microsoft Intune to deploy resource access profiles.
- Sites that allow HTTP client communication. Configure the site for HTTPS or Enhanced HTTP. For more information, see Enable the site for HTTPS-only or enhanced HTTP.

This concludes new features.

Thanks

Ram Lan
7th April 2021