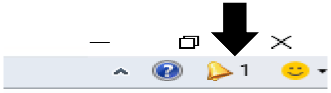
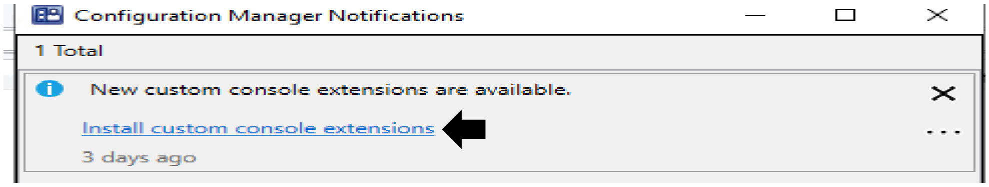
NEW FEATURES IN CURRENT BRANCH 2010 – CONFIGURATION MANAGER

In this post we will review new features released with CB2010. We will test them within the lab. Here we go..

Community Hub - **Community hub on Windows Server operating systems** - You can now display the Community hub on Windows Server operating systems. The Configuration Manager console will notify you to install the console extension to enable Windows Server 2012 and later to load the Community hub.





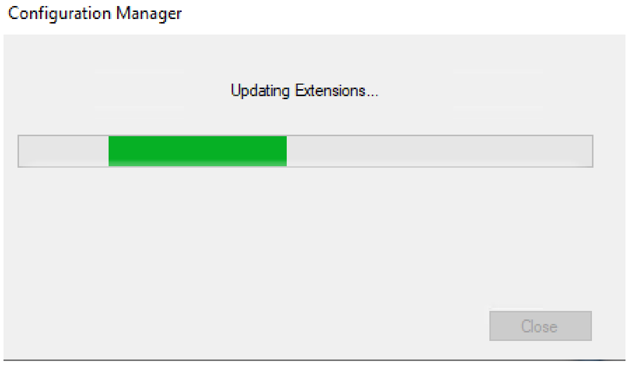
Configuration Manager Notifications

1 Total

New custom console extensions are available.

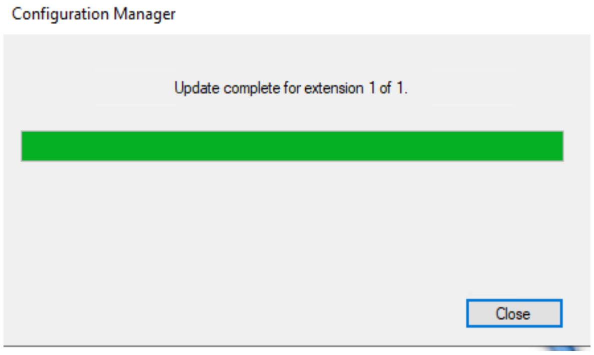
Install custom console extensions

3 days ago



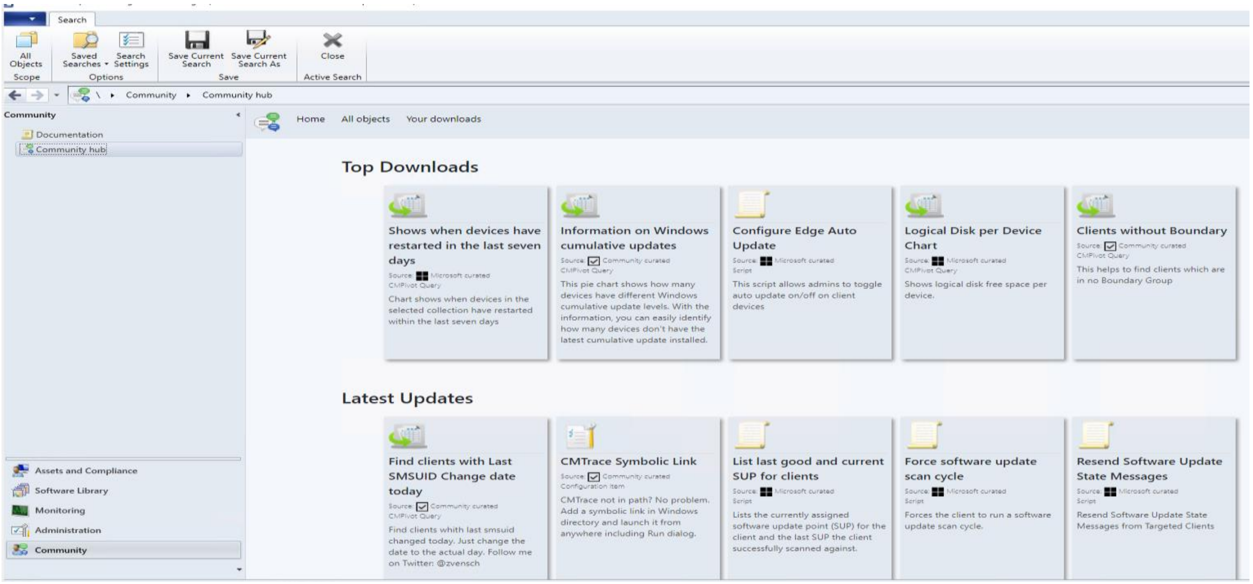
Configuration Manager

Updating Extensions...



Configuration Manager

Update complete for extension 1 of 1.



Top Downloads

Shows when devices have restarted in the last seven days
Source: Microsoft curated
CMPivot Query
Chart shows when devices in the selected collection have restarted within the last seven days

Information on Windows cumulative updates
Source: ☑ Community curated
CMPivot Query
This pie chart shows how many devices have different Windows cumulative update levels. With the information, you can easily identify how many devices don't have the latest cumulative update installed.

Configure Edge Auto Update
Source: Microsoft curated
Script
This script allows admins to toggle auto update on/off on client devices

Logical Disk per Device Chart
Source: Microsoft curated
CMPivot Query
Shows logical disk free space per device.

Clients without Boundary
Source: ☑ Community curated
CMPivot Query
This helps to find clients which are in no Boundary Group

Latest Updates

Find clients with Last SMSUID Change date today
Source: ☑ Community curated
CMPivot Query
Find clients whith last smsuid changed today. Just change the date to the actual day. Follow me on Twitter: @zvensch

CMTrace Symbolic Link
Source: ☑ Community curated
Configuration item
CMTrace not in path? No problem. Add a symbolic link in Windows directory and launch it from anywhere including Run dialog.

List last good and current SUP for clients
Source: Microsoft curated
Script
Lists the currently assigned software update point (SUP) for the client and the last SUP the client successfully scanned against.

Force software update scan cycle
Source: Microsoft curated
Script
Forces the client to run a software update scan cycle.

Resend Software Update State Messages
Source: Microsoft curated
Script
Resend Software Update State Messages from Targeted Clients

Microsoft Endpoint Manager tenant attach - Troubleshooting portal lists a user's devices based on usage - -The troubleshooting portal in Microsoft Endpoint Manager admin center allows you to search for a user and view their associated devices. Starting in this release, tenant attached devices that are assigned user device affinity automatically based on usage will now be returned when searching for a user.

Enhancements to applications in Microsoft Endpoint Manager admin center - We've made improvements to applications for tenant attached devices. Administrators can now do the following actions for applications in the Microsoft Endpoint Manager admin center:

Uninstall an application
Repair installation of an application
Re-evaluate the application installation status
Reinstall an application has replaced Retry installation

Cloud-attached management - Cloud management gateway with virtual machine scale set for CSP - Cloud management gateway (CMG) deployments can now use a virtual machine scale set in Azure to support Cloud Solution Provider (CSP) subscriptions. This feature is currently pre-release. At this time, it's intended only for CSP customers that don't already have a CMG in another subscription.

Disable Azure AD authentication for onboarded tenants - You can now disable Azure Active Directory (Azure AD) authentication for tenants not associated with users and devices. When you onboard Configuration Manager to Azure AD, it allows the site and clients to use modern authentication. Currently, Azure AD device authentication is enabled for all onboarded tenants, whether or not it has devices. For example, you have a separate tenant with a subscription that you use for compute resources to support a cloud management gateway. If there aren't users or devices associated with the tenant, disable Azure AD authentication.

Additional options when creating app registrations in Azure Active Directory - You can now specify Never for the expiration of a secret key when creating Azure Active Directory app registrations.

Validate internet access for the service connection point - If you use Desktop Analytics or tenant attach, the service connection point now checks important internet endpoints. These checks help make sure that the cloud-connected services are available. It also helps you troubleshoot issues by quickly determining if network connectivity is a problem.

Desktop Analytics - Support for new Windows 10 diagnostic data levels -Microsoft is increasing transparency by categorizing the diagnostic data that Windows 10 collects:

Basic diagnostic data is recategorized as Required
Full is recategorized as Optional

If you previously configured devices for Enhanced or Enhanced (Limited), in an upcoming release of Windows 10, they'll use the Required level. This change may impact the functionality of Desktop Analytics.

Support for Windows 10 Enterprise LTSC 2019 - The Windows 10 long-term servicing channel (LTSC) was designed for devices where functionality and features don't change over time. This servicing model prevents Windows 10 Enterprise LTSC devices from receiving the usual feature updates. It provides only quality updates to make sure that device security stays up to date. Some customers want to shift from LTSC to the semi-annual servicing channel, to have access to new features, services, and other major changes. You can now use Configuration Manager to enroll LTSC devices to Desktop Analytics. Once you enroll these devices, you can evaluate them in your deployment plans.

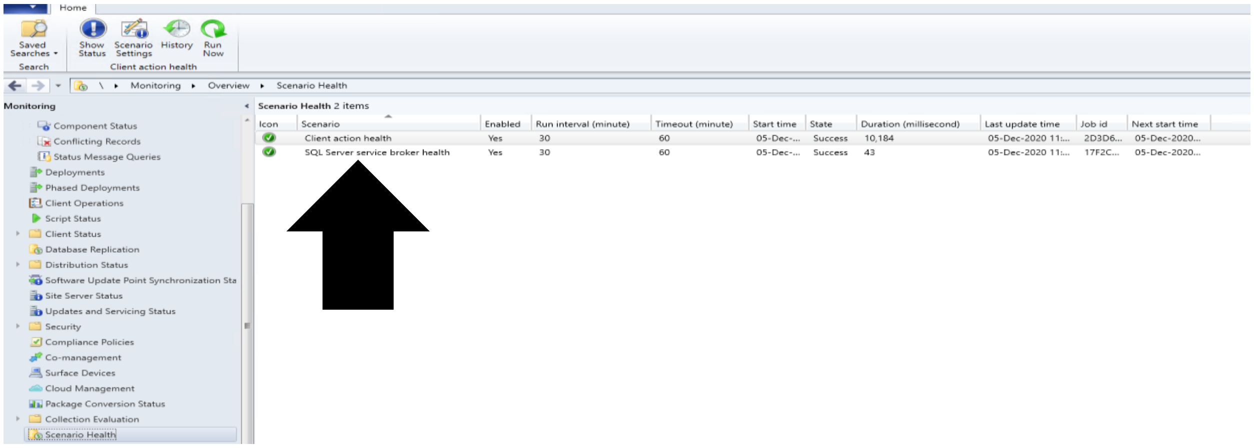
Site infrastructure - Monitor scenario health - Configuration Manager is complicated to troubleshoot. It's especially complex to understand system latency and the backlog between components. Cloud service-attached features increase that complexity.

You can now use Configuration Manager to monitor the health of end-to-end scenarios. It simulates activities to expose performance metrics and failure points. These synthetic activities are similar to methods that Microsoft uses to monitor some components in its cloud services. Use this additional data to better understand timeframes for activities. If failures occur, it can help focus your investigation.

This release includes the following two scenarios:

SQL Server Service Broker: The service broker is a required configuration for the site database. Many of the core subsystems in Configuration Manager use the service broker.

Client action health: Monitor the health of the fast channel used for client actions. If your environment is tenant attached with devices uploaded, this feature helps you see potential issues with client actions from the Microsoft Endpoint Manager admin center. You can also use this feature for on-premises client actions. For example, CMPivot, run scripts, and device wake-up.

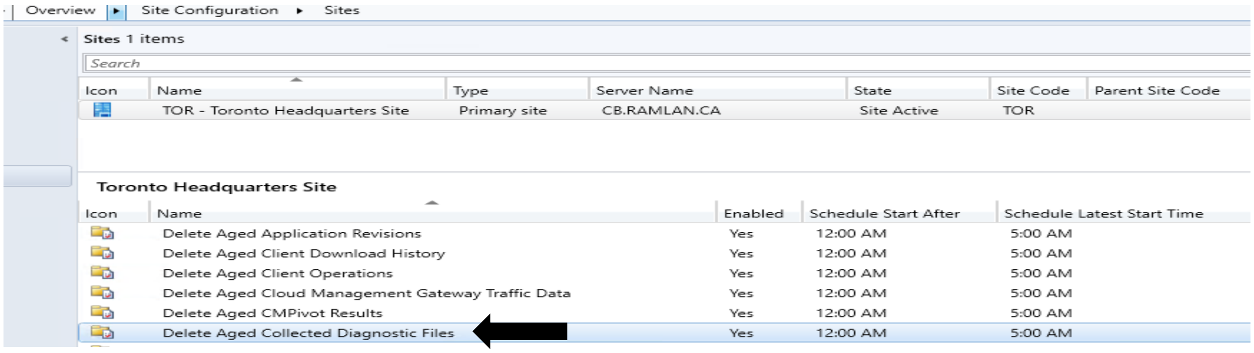


Scenario Health 2 items

Icon	Scenario	Enabled	Run interval (minute)	Timeout (minute)	Start time	State	Duration (millisecond)	Last update time	Job id	Next start time
✓	Client action health	Yes	30	60	05-Dec-...	Success	10,184	05-Dec-2020 11:...	2D3D6...	05-Dec-2020...
✓	SQL Server service broker health	Yes	30	60	05-Dec-...	Success	43	05-Dec-2020 11:...	17F2C...	05-Dec-2020...

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. If a failure occurs, the Report update error to Microsoft button is enabled. When you use the button, an interactive wizard opens allowing you to provide more information to us. In technical previews, this button is always enabled even when the setup completes successfully.

Delete Aged Collected Diagnostic Files task - You now have a new maintenance task available for cleaning up collected diagnostic files. Delete Aged Collected Diagnostic Files uses a default value of 14 days when it looks for diagnostic files to clean up. This task doesn't affect regular collected files. The new maintenance task is enabled by default.



Sites 1 items

Icon	Name	Type	Server Name	State	Site Code	Parent Site Code
	TOR - Toronto Headquarters Site	Primary site	CB.RAMLAN.CA	Site Active	TOR	

Toronto Headquarters Site

Icon	Name	Enabled	Schedule Start After	Schedule Latest Start Time
	Delete Aged Application Revisions	Yes	12:00 AM	5:00 AM
	Delete Aged Client Download History	Yes	12:00 AM	5:00 AM
	Delete Aged Client Operations	Yes	12:00 AM	5:00 AM
	Delete Aged Cloud Management Gateway Traffic Data	Yes	12:00 AM	5:00 AM
	Delete Aged CMPivot Results	Yes	12:00 AM	5:00 AM
	Delete Aged Collected Diagnostic Files	Yes	12:00 AM	5:00 AM

Improvements to the administration service - The Configuration Manager REST API, the administration service, requires a secure HTTPS connection. With the previous methods to enable HTTPS, enabling IIS on the SMS Provider was a prerequisite.

Starting in this release, you no longer need to enable IIS on the SMS Provider for the administration service. When you enable the site for enhanced HTTP, it creates a self-signed certificate for the SMS Provider, and automatically binds it without requiring IIS.

Client management - Wake machine at deployment deadline using peer clients on the same remote subnet - Wake on LAN (WoL) has always posed a problem in complex, subnetted networks. Good networking best practice reduces the size of broadcast domains to mitigate against the risk of broadcast traffic adversely affecting the network. The most common way to limiting network broadcast is by not allowing broadcast packets to be routed between subnets. Another option is to enable subnet directed broadcasts but most organizations don't allow the magic packet to traverse internal routers.

In version 1810, the introduction of peer wake-up allowed an administrator to wake a device or collection of devices, on demand using the client notification channel. Overcoming the need for the server to be in the same broadcast domain as the client.

This latest improvement allows the Configuration Manager site to wake devices at the deadline of a deployment. Instead of the site server issuing the magic packet directly, the site uses the client notification channel. It finds an online machine in the last known subnet of the target device. It then instructs the online client to issue the WoL packet for the target device.

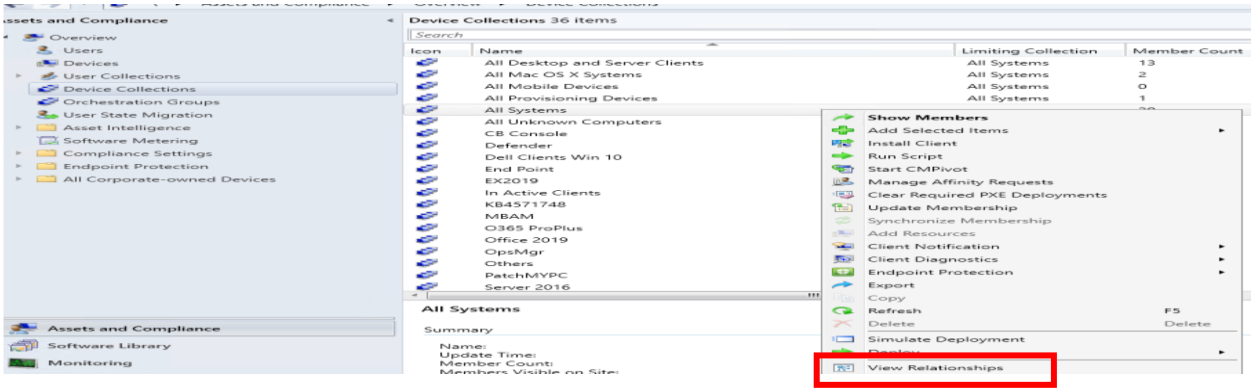
Improved Windows Server restart experience for non-administrator accounts - For a low-rights user on a device that runs Windows Server, by default they aren't assigned the user rights to restart Windows. When you target a deployment to this device, this user can't manually restart. For example, they can't restart Windows to install software updates.

Starting in this release, you can now control this behavior as needed. In the Computer Restart group of client settings, enable the following setting: When a deployment requires a restart, allow low-rights users to restart a device running Windows Server.

Collections - Collection query preview - You can now preview the query results when you're creating or editing a query for collection membership. Preview the query results from the query statement properties dialog. When you select Edit Query Statement, select the green triangle on the query properties for the collection to show the Query Results Preview window. Select Stop if you want to stop a long running query.

Collection evaluation view - We've integrated the functionality of Collection Evaluation Viewer into the Configuration Manager console. This change provides administrators a central location to view and troubleshoot the collection evaluation process.

View collection relationships - You can now view dependency relationships between collections in a graphical format. It shows limiting, include, and exclude relationships.



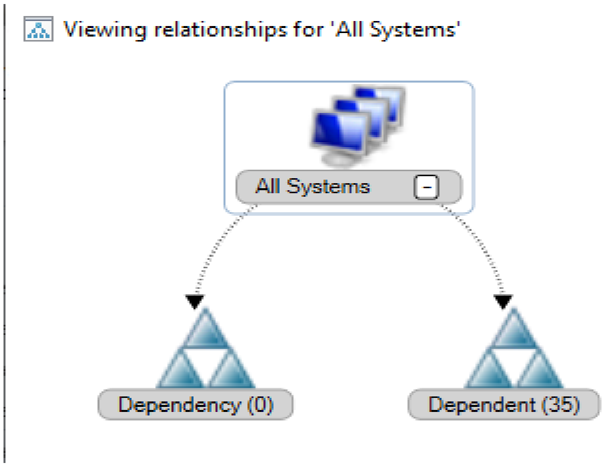
Device Collections 36 items

Icon	Name	Limiting Collection	Member Count
	All Desktop and Server Clients	All Systems	13
	All Mac OS X Systems	All Systems	2
	All Mobile Devices	All Systems	0
	All Provisioning Devices	All Systems	1
	All Systems		
	All Unknown Computers		
	CB Console		
	Defender		
	Dell Clients Win 10		
	End Point		
	EX2019		
	In Active Clients		
	KB4571748		
	MBAM		
	O365 ProPlus		
	Office 2019		
	OpsMgr		
	Others		
	PatchMYPC		
	Server 2016		

All Systems

Summary

Name:
Update Time:
Member Count:
Members Visible on Site:



Application management - 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.

OS deployment - Deploy an OS over CMG using bootable media - Starting in current branch version 2006, the cloud management gateway (CMG) supported running a task sequence with a boot image when you start it from Software Center. With this release, you can now use bootable media to reimage internet-based devices that connect through a CMG. This scenario helps you better support remote workers. If Windows won't start so that the user can access Software Center, you can now send them a USB drive to reinstall Windows.

Deploy a task sequence deployment type to a user collection- You can now deploy an application with a task sequence deployment type to a user-based collection. A user-targeted deployment still runs in the context of the local System account.

Manage task sequence size - Large task sequences cause problems with client processing. To further help manage the size of task sequences, this release continues to iterate on improvements.

Starting in this release Configuration Manager restricts actions for a task sequence that's greater than 2 MB in size. For example, the task sequence editor will display an error if you try to save changes to a large task sequence.

When you view the list of task sequences in the Configuration Manager console, add the Size (KB) column. Use this column to identify large task sequences that can cause problems.

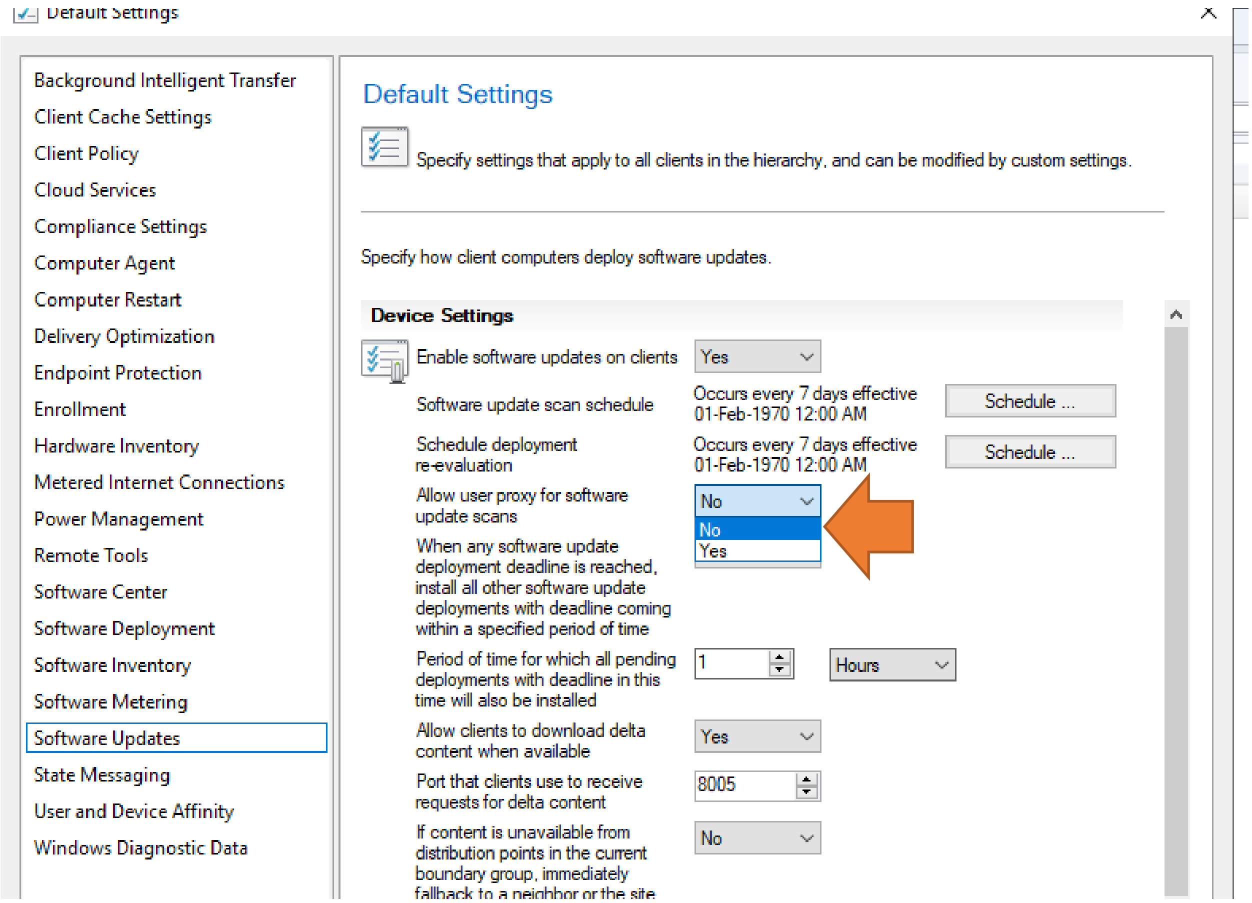
Analyze SetupDiag errors for feature updates - With the release of Windows 10, version 2004, the SetupDiag diagnostic tool is included with Windows Setup. If there's an issue with the upgrade, SetupDiag automatically runs to determine the cause of the failure. Configuration Manager now gathers and summarizes SetupDiag results from feature update deployments with Windows 10 servicing.

Improvements to task sequence performance settings - Starting in Configuration Manager version 1910, to improve the overall speed of the task sequence, you could activate the Windows power plan for High Performance. Starting in this release, you can now use this option on devices with modern standby and other devices that don't have that default power plan.

Protection- Improvements to BitLocker management -You can now manage BitLocker policies and escrow recovery keys over a cloud management gateway (CMG). This change also provides support for BitLocker management via internet-based client management (IBCM). There's no change to the setup process for BitLocker management. This improvement supports domain-joined and hybrid domain-joined devices.

Expanded Windows Defender Application Control management - Windows Defender Application Control enforces an explicit list of software allowed to run on devices. In this release, we've expanded Windows Defender Application Control policies to support devices running Windows Server 2019 or later.

Software updates - Enable user proxy for software update scans - Beginning with the September 2020 cumulative update, HTTP-based WSUS servers will be secure by default. By default, a client that scans for updates against an HTTP-based WSUS can't use a user proxy. If you still require a user proxy despite the security trade-offs, a new software updates client setting is available to allow these connections. For more information about the changes for scanning WSUS, see September 2020 changes to improve security for Windows devices scanning WSUS. To make sure that the best security protocols are in place, use the TLS protocol. This protocol helps to secure your software update infrastructure.



Default Settings

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

Specify how client computers deploy software updates.

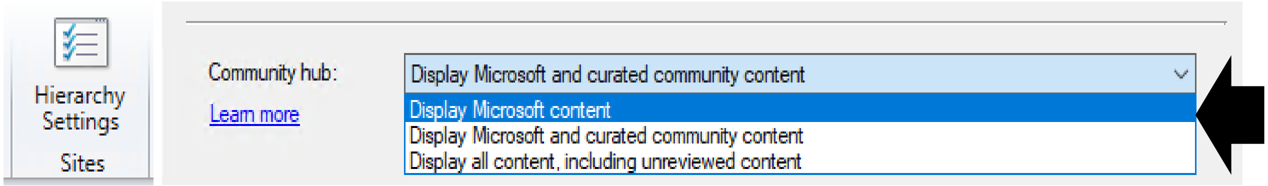
Device Settings

Enable software updates on clients	Yes	
Software update scan schedule	Occurs every 7 days effective 01-Feb-1970 12:00 AM	Schedule ...
Schedule deployment re-evaluation	Occurs every 7 days effective 01-Feb-1970 12:00 AM	Schedule ...
Allow user proxy for software update scans	No No Yes	
When any software update deployment deadline is reached, install all other software update deployments with deadline coming within a specified period of time		
Period of time for which all pending deployments with deadline in this time will also be installed	1	Hours
Allow clients to download delta content when available	Yes	
Port that clients use to receive requests for delta content	8005	
If content is unavailable from distribution points in the current boundary group, immediately fallback to a neighbor or the site	No	

Notifications for devices no longer receiving updates - To help you manage security risk in your environment, you'll be notified in-console about devices with operating systems that are past the end of support date. These devices may no longer receive security updates. Additionally, a new Management Insights rule was added to detect Windows 7, Windows Server 2008, and Windows Server 2008 R2 without Extended Security Updates (ESU).

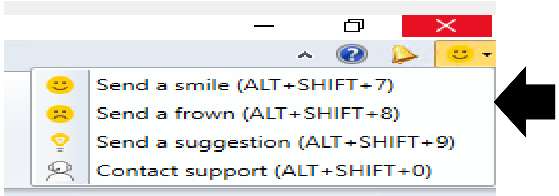
Immediate distribution point fallback for clients downloading software update delta content - There's a new client setting for software updates. If delta content is unavailable from distribution points in the current boundary group, you can allow immediate fallback to a neighbor or the site default boundary group distribution points. This setting is useful when using delta content for software updates since the timeout setting per download job is five minutes.

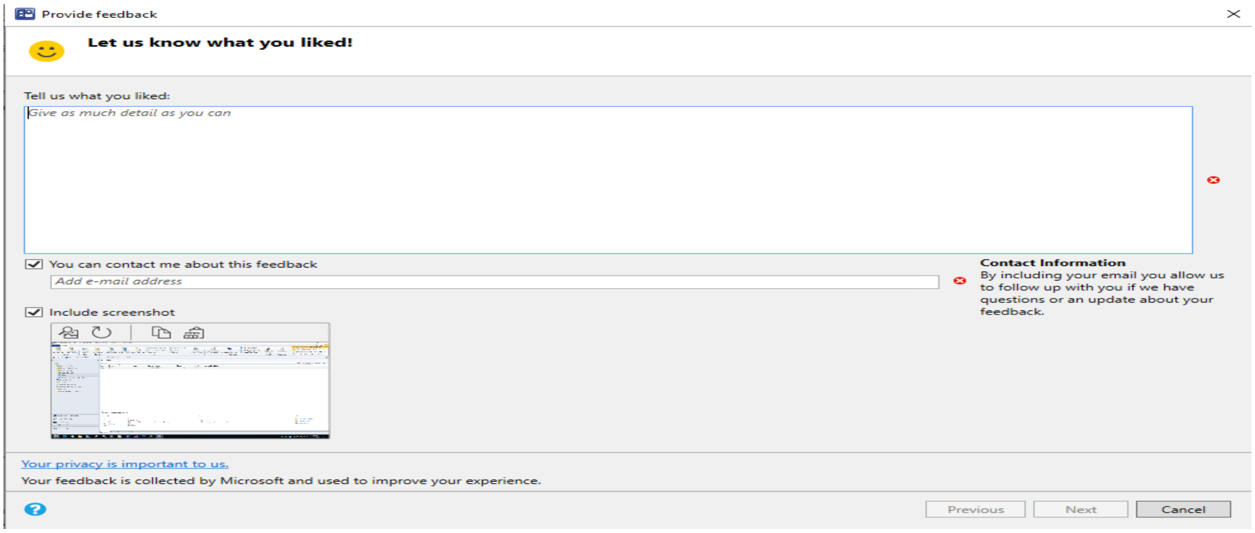
Configuration Manager console - Categorize Community hub content - Community hub content is grouped into a Microsoft, curated, or unreviewed category to allow admins to choose the types of content their environment displays. Admins can choose from the different categories of content that are provided in the Community hub to match their risk profile and their willingness to share and use content from those outside Microsoft and outside their own company.


Community hub: Display Microsoft and curated community content

Hierarchy Settings
Sites
Learn more
Display Microsoft content
Display Microsoft and curated community content
Display all content, including unreviewed content

Product feedback - The Configuration Manager console has a new wizard for sending feedback. The redesigned wizard improves the workflow with better guidance about how to submit good feedback.


Send a smile (ALT+SHIFT+7)
Send a frown (ALT+SHIFT+8)
Send a suggestion (ALT+SHIFT+9)
Contact support (ALT+SHIFT+0)


Provide feedback

Let us know what you liked!

Tell us what you liked:

Give as much detail as you can

☑ You can contact me about this feedback

Add e-mail address

Contact Information
By including your email you allow us to follow up with you if we have questions or an update about your feedback.

☑ Include screenshot

Your privacy is important to us.
Your feedback is collected by Microsoft and used to improve your experience.

Improvements to in-console notifications - You now have an updated look and feel for in-console notifications. Notifications are more readable and the action link is easier to find. Additionally, the age of the notification is displayed to help you find the latest information. If you dismiss or snooze a notification, that action is now persistent for your user across consoles.

Improvements to the Configuration Manager console - You can now copy discovery data from devices and users in the console. Copy the details to the clipboard, or export them all to a file. These new actions make it easier for you to quickly get this data from the console. For example, copy the MAC address of a device before you reimage it.

Various areas in the Configuration Manager console now use the fixed-width font Consolas. This font provides consistent spacing and makes it easier to read.

You now have an easier way to view status messages for objects. Select an object in the Configuration Manager console, and then select Show Status Messages from the ribbon.

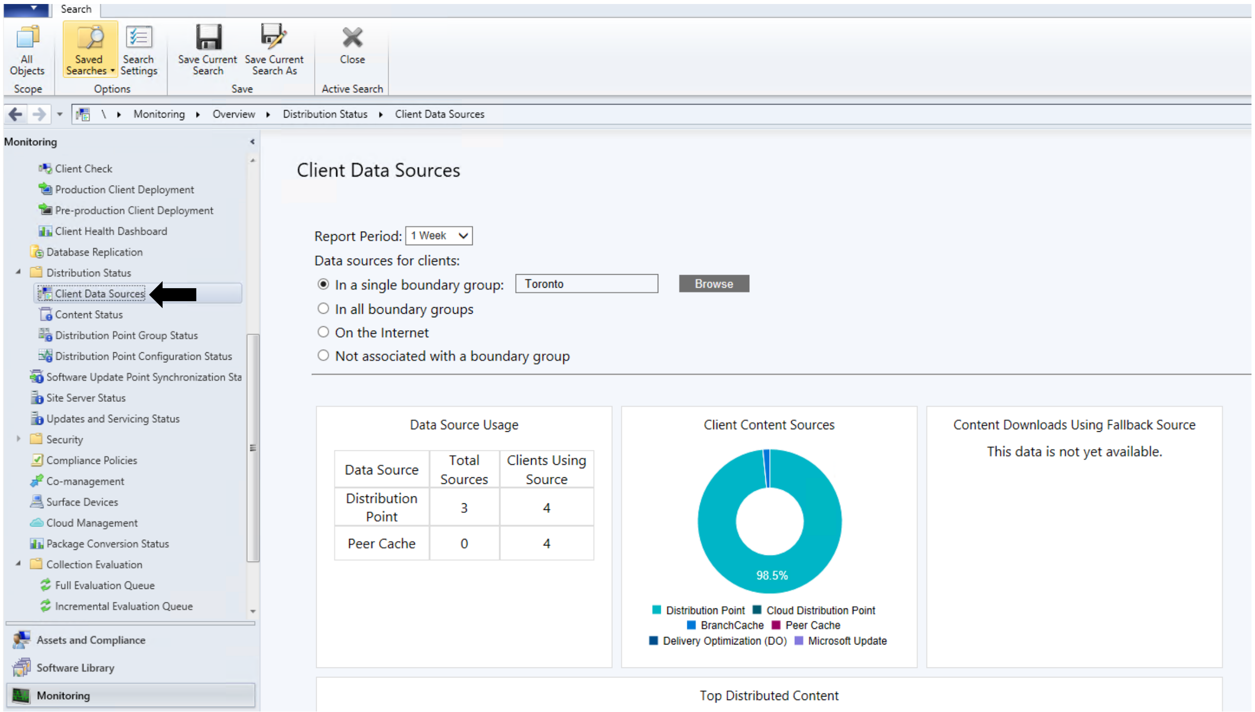
Now when you import an object in the Configuration Manager console, it imports to the current folder. Previously, Configuration Manager always put imported objects in the root node. This new behavior applies to applications, packages, driver packages, and task sequences.

To assist you when creating scripts and queries in the Configuration Manager console, you'll now see syntax highlighting and code folding, where available.

Content management - Improvements to client data sources dashboard - The client data sources dashboard now offers an expanded selection of filters to view information about where clients get content. These new filters include:

Single boundary group
All boundary groups
Internet clients
Clients not associated with a boundary group

The dashboard also includes a new tile for Content downloads using fallback source. This information helps you understand how often clients download content from an alternate source.



Client Data Sources

Report Period: 1 Week

Data sources for clients:

● In a single boundary group: Toronto Browse
○ In all boundary groups
○ On the Internet
○ Not associated with a boundary group

Data Source Usage

Data Source	Total Sources	Clients Using Source
Distribution Point	3	4
Peer Cache	0	4

Client Content Sources

Content Downloads Using Fallback Source

This data is not yet available.

Top Distributed Content

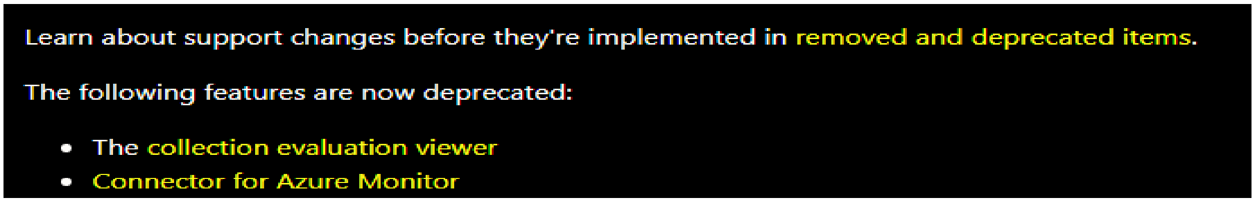
Improvements to the content library cleanup tool - If you remove content from a distribution point while the site system is offline, an orphaned record can exist in WMI. Over time, this behavior can eventually lead to a warning status on the distribution point. To mitigate the issue in the past, you had to manually remove the orphaned entries from WMI. The content library cleanup tool in delete mode can now remove these orphaned content records from WMI.

PowerShell - Update PowerShell help - You can now use the Update-Help cmdlet to get the latest information for the Configuration Manager PowerShell module. This content is the same as what's published on docs.microsoft.com for the ConfigurationManager module.

Support for PowerShell version 7 - The Configuration Manager PowerShell cmdlet library now offers support for PowerShell 7. For more information, see Get started with Configuration Manager cmdlets.

Improvements to cloud management gateway cmdlets - 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.

Depreciated Features



Learn about support changes before they're implemented in removed and deprecated items.

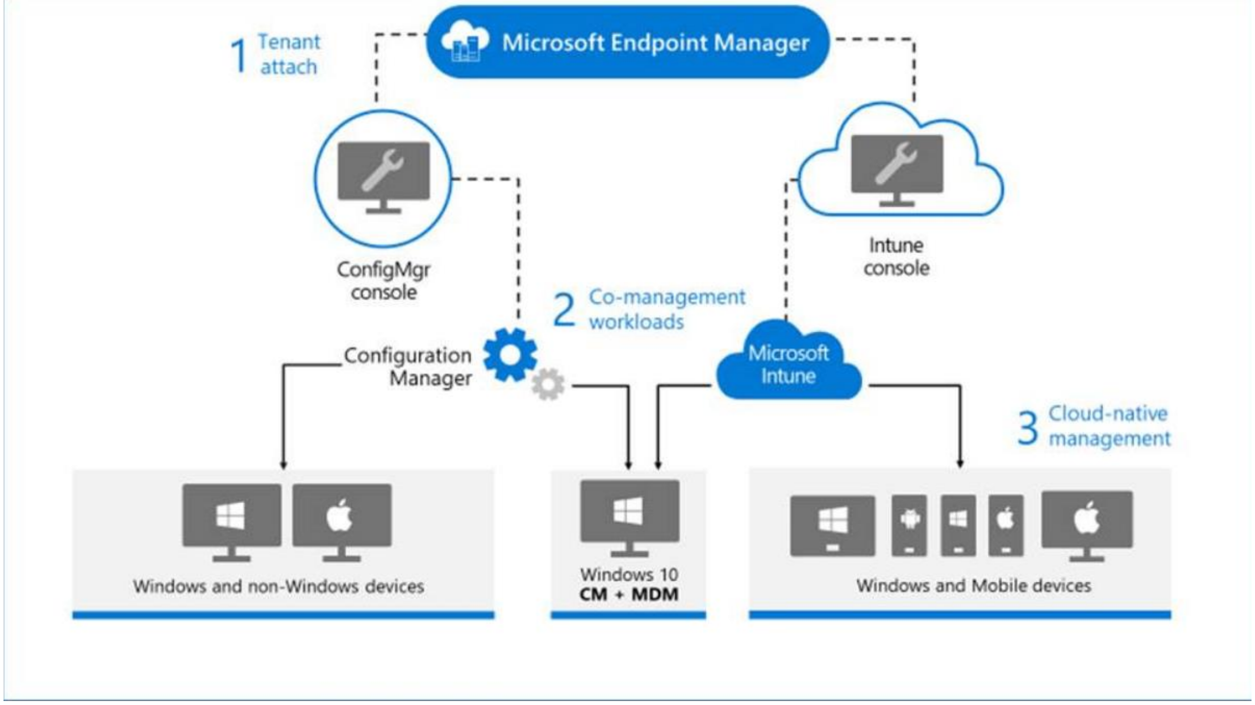
The following features are now deprecated:

- The collection evaluation viewer
- Connector for Azure Monitor

This concludes all the features in CB 2010

Thanks

Ram Lan
5th Dec 2020


1 Tenant attach
Microsoft Endpoint Manager
ConfigMgr console
Intune console
2 Co-management workloads
Configuration Manager
Microsoft Intune
3 Cloud-native management
Windows and non-Windows devices
Windows 10
CM + MDM
Windows and Mobile devices