# On-Premise Bandwidth Optimization Options

## Summary

Automox is the easiest-to-use, most-recommended, most efficient cloud-native solution for endpoint hardening--anywhere, in an instant. Being a cloud-native platform, Automox makes it possible to manage Windows, macOS, and Linux devices with one solution without purchasing physical hardware or installing a management application. As companies move to internet-based modern solutions, some of the challenges of legacy solutions are immediately solved, while others remain. The purpose of this document is to present the most common challenges, and provide guidance on how to utilize native technologies while working to preserve the intent of a cloud first, infrastructure-less solution.

### Solutions

#### Quality of Service (QoS)

Palo Alto Networks explains Quality of Service (QoS) as the following:

> "Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic. This enables the network administrator to assign the order in which packets are handled, and the amount of bandwidth afforded to that application or traffic flow…"
>
> "The QoS mechanisms for ordering packets and allotting bandwidth are queuing and bandwidth management respectively. Before they can be implemented however, traffic must be differentiated using classification tools. The classification of traffic according to policy allows organizations to ensure the consistency and adequate availability of resources for their most important applications.
>
> Traffic can be classified crudely by port or IP, or using a more sophisticated approach such as by application or user. The latter parameters allow for more meaningful identification, and consequently, classification of the data.
>
> Next, queuing and bandwidth management tools are assigned rules to handle traffic flows specific to the classification they received upon entering the network.
>
> The queuing mechanism allows for packets within traffic flows to be stored until the network is ready to process it. Priority Queuing (PQ) is developed to ensure the necessary availability and minimal latency of network performance for the most important batches of applications and traffic by providing an assigned priority and specific bandwidth to them based on their classification. This ensures the most important activities on a network are not starved of bandwidth by activities of lower priority. Applications, users, and traffic can be batched in up to 8 differentiated queues.

> Bandwidth management mechanisms measure and control traffic flows on the network to avoid exceeding its capacity and the resulting network congestion that occurs. Mechanisms for bandwidth management include traffic shaping, a rate limiting technique used to optimize or guarantee performance and increase usable bandwidth where necessary, and scheduling algorithms, which offer varied methods for providing bandwidth to specific traffic flows.” [1]

## Windows Delivery Optimization (DO)

Microsoft explains Delivery Optimization (DO) as the following:

> “Delivery Optimization is a new peer-to-peer distribution method in Windows 10. Windows 10 clients can source content from other devices on their local network that have already downloaded the updates or from peers over the internet. Using the settings available for Delivery Optimization, clients can be configured into groups, allowing organizations to identify devices that are possibly the best candidates to fulfill peer-to-peer requests.
>
> Windows Update, Windows Update for Business, and Windows Server Update Services (WSUS) can use Delivery Optimization. Delivery Optimization can significantly reduce the amount of network traffic to external Windows Update sources as well as the time it takes for clients to retrieve the updates.” [2]
>
> “Windows updates, upgrades, and applications can contain packages with very large files. Downloading and distributing updates can consume quite a bit of network resources on the devices receiving them. You can use Delivery Optimization to reduce bandwidth consumption by sharing the work of downloading these packages among multiple devices in your deployment. Delivery Optimization can accomplish this because it is a self-organizing distributed cache that allows clients to download those packages from alternate sources (such as other peers on the network) in addition to the traditional Internet-based servers. Delivery Optimization is a cloud-managed solution. Access to the Delivery Optimization cloud services is a requirement. This means that in order to use the peer-to-peer functionality of Delivery Optimization, devices must have access to the internet.” [3]

### DO Requirements and Supported Download Package Types

Requirements:

The following table lists the minimum Windows 10 version that supports Delivery Optimization [4]:

| **Device type** | **Minimum Windows version** |
|---|---|
| Computers running Windows 10 | 1511 |
| Computers running server core installations of Windows Server | 1709 |

| Device type | Minimum Windows version |
|---|---|
| IoT devices | 1803 |

Types of download packages supported by delivery optimization

| Download package | Minimum Windows version |
|---|---|
| Windows 10 updates (feature updates and quality updates) | 1511 |
| Windows 10 drivers | 1511 |
| Windows Store files | 1511 |
| Windows Store for Business files | 1511 |
| Windows Defender definition updates | 1511 |
| Microsoft 365 Apps and updates | 1709 (for more information, see Delivery Optimization and Microsoft 365 Apps) |
| Win32 apps for Intune | 1709 |
| XBox Game Pass games | 2004 |
| MSIX apps (HTTP downloads only) | 2004 |
| Configuration Manager Express updates | 1709 + Configuration Manager version 1711 |
| Edge browser installs and updates | 1809 |
| Dynamic updates | 1903 |

How Microsoft users Delivery Optimization

> “At Microsoft, to help ensure that ongoing deployments weren't affecting our network and taking away bandwidth for other services, Microsoft IT used a couple of different bandwidth management strategies. Delivery Optimization, peer-to-peer caching enabled through Group Policy, was piloted and then deployed to all managed devices using Group Policy. Based on recommendations from the Delivery Optimization team, we used the "group" configuration to limit sharing of content to only the devices that are members of the same Active Directory domain… More than 76 percent of content came from peer devices versus the Internet. [5]

## DO: Frequently Asked Questions

> “Does Delivery Optimization work with WSUS?: Yes. Devices will obtain the update payloads from the WSUS server, but must also have an internet connection as they communicate with the Delivery Optimization cloud service for coordination.

Which ports does Delivery Optimization use?: Delivery Optimization listens on port 7680 for requests from other peers by using TCP/IP. The service will register and open this port on the device, but you might need to set this port to accept inbound traffic through your firewall yourself. If you don't allow inbound traffic over port 7680, you can't use the peer-to-peer functionality of Delivery Optimization. However, devices can still successfully download by using HTTP or HTTPS traffic over port 80 (such as for default Windows Update data).

If you set up Delivery Optimization to create peer groups that include devices across NATs (or any form of internal subnet that uses gateways or firewalls between subnets), it will use Teredo. For this to work, you must allow inbound TCP/IP traffic over port 3544. Look for a "NAT traversal" setting in your firewall to set this up.

Delivery Optimization also communicates with its cloud service by using HTTP/HTTPS over port 80.

What are the requirements if I use a proxy?: For Delivery Optimization to successfully use the proxy, you should set up the proxy by using Windows proxy settings or Internet Explorer proxy settings. For details see Using a proxy with Delivery Optimization. Most content downloaded with Delivery Optimization uses byte range requests. Make sure your proxy allows byte range requests. For more information, see Proxy requirements for Windows Update.

What hostnames should I allow through my firewall to support Delivery Optimization?:

For communication between clients and the Delivery Optimization cloud service: *.do.dsp.mp.microsoft.com.

For Delivery Optimization metadata:

- *.dl.delivery.mp.microsoft.com
- *.emdl.ws.microsoft.com

For the payloads (optional):

- *.download.windowsupdate.com
- *.windowsupdate.com

Does Delivery Optimization use multicast?: No. It relies on the cloud service for peer discovery, resulting in a list of peers and their IP addresses. Client devices then connect to their peers to obtain download files over TCP/IP.

How does Delivery Optimization deal with congestion on the router from peer-to-peer activity on the LAN?: Starting in Windows 10, version 1903, Delivery Optimization uses LEDBAT to relieve such congestion. For more details see this post on the Networking Blog.

How does Delivery Optimization handle VPNs? Delivery Optimization attempts to identify VPNs by checking the network adapter type and details and will treat the connection as a VPN if the adapter description contains certain keywords, such as "VPN" or "secure."

If the connection is identified as a VPN, Delivery Optimization will suspend uploads to other peers. However, you can allow uploads over a VPN by using the Enable Peer Caching while the device connects via VPN policy.

If you have defined a boundary group in Configuration Manager for VPN IP ranges, you can set the DownloadMode policy to 0 for that boundary group to ensure that there will be no peer-to-peer activity over the VPN. When the device is not connected via VPN, it can still leverage peer-to-peer with the default of LAN.

With split tunneling, make sure to allow direct access to these endpoints:

Delivery Optimization service endpoint:

- https://*.prod.do.dsp.mp.microsoft.com

Delivery Optimization metadata:

- http://emdl.ws.microsoft.com
- http://*.dl.delivery.mp.microsoft.com

Windows Update and Microsoft Store backend services and Windows Update and Microsoft Store payloads

- http://*.windowsupdate.com>
- https://*.delivery.mp.microsoft.com
- https://*.update.microsoft.com
- https://tsfe.trafficshaping.dsp.mp.microsoft.com " [6]

## Troubleshooting

Common problems and solutions can be found here: Troubleshooting

## Caching

### Content Caching (macOS)

Content Caching allows a Mac administrator to set up a single or multiple macOS devices to download software updates to this device and then distribute them to all other macOS devices without downloading the software updates again for each device from the internet. Content caching will also give you the flexibility to choose what content gets cached as well.

How do I set up Content Caching?

Setting up content caching on the host and peer devices is easy to follow in the Apple guide on how to do this.

Why would I want to set up Content Caching?

Content Caching can be helpful in environments where internet bandwidth is limited. Deploying a Patch Policy via Automox to all devices in a centralized location can cause saturation to your local network, and can slow it down for your end-users.

When do I want to set up Content Caching?

You should want to set up Content Caching if you have multiple macOS devices into a centralized location, in most cases this will be a corporate office. Setting up one or more hosts will allow any macOS devices in the same subnet (or in some cases, the same Public IP address) to pull cached content from those host devices. You can also set up Content Caching for macOS devices that are on the go, that way if they can't see the host device it will update the operating system from the internet instead. Content Caching does not need to be set up for organizations that have a fully remote staff. Content Caching is also not recommended to be used over a VPN.

Requirements to setup Content Caching:

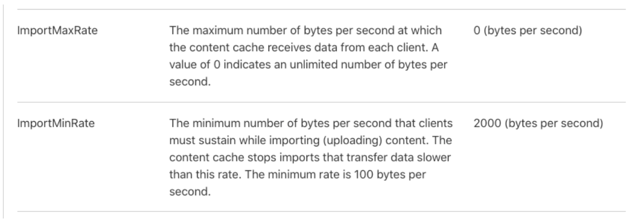
- A Mac device running macOS 10.13.5 or higher
    - Apple recommends any device running OS X 10.8.2; however, at the time this article is written, Automox only supports macOS 10.13+.
    - You can also set up multiple macOS host devices to distribute content to specific devices, if necessary.
- The macOS device connected to the internet.
    - It is recommended to hardwire a device with ethernet if possible.
    - It is also recommended to disable any other connections on the device.
    - A 1 GB ethernet connection or greater is recommended.
- Line-of-sight to devices that will download software updates from the host device.
    - This can also be accomplished with multiple subnets, as long as those devices have the same Public IP address.
- Other Best Practices provided by Apple:
    - Allow all Apple push notifications.
    - Don't use manual proxy settings.
    - Don't proxy client requests to content caches.
    - Bypass proxy authentication for content caches.
    - Specify a TCP port for caching. (See Port key in Configure advanced content caching settings on Mac.)
    - Manage inter-site caching traffic.
    - Block rogue cache registration.
    - Use a static public IP address for content caches

Bandwidth Limiting

Ensure that your local network can handle passing data to multiple devices before setting up content caching. While your local network bandwidth may be high, it is good to remember that each macOS software update is usually around 3 GBs or more, and multiple devices receiving this update simultaneously will saturate your local network. It is also good to note that Content Caching is not useful if you are supporting a largely remote environment, as bandwidth may not be as much of a concern.

If you want to deploy cached content to local machines, you may use this guide from Apple to modify the existing com.apple.AssetCache plist to help with limiting bandwidth on your local network. The defaults write command can accomplish this, or an MDM that can deploy configuration profiles.

It is recommended to add these plist strings to com.apple.AssetCache to help with bandwidth limiting:



| | | |
|---|---|---|
| ImportMaxRate | The maximum number of bytes per second at which the content cache receives data from each client. A value of 0 indicates an unlimited number of bytes per second. | 0 (bytes per second) |
| ImportMinRate | The minimum number of bytes per second that clients must sustain while importing (uploading) content. The content cache stops imports that transfer data slower than this rate. The minimum rate is 100 bytes per second. | 2000 (bytes per second) |

Plist strings to add to the "com.apple.AssetCache" plist

Considerations:

Cached content is stored in the boot drive of the host machine. If your boot drive free space gets too full, old cached content that is rarely used will be deleted in place of newer versions. The AllowCacheDelete plist string is enabled by default to clear old cached content.

After you set up Content Caching, peer devices may take some time to discover the host device. While Apple does not publish how long this takes, restarting the peer machine may help discover the host device quicker.

Helpful Links:

- What is content caching on Mac?
- Set up content cache clients, peers, or parents on Mac
- Use multiple content caches on Mac
- Content types supported by content caching in macOS
- Configure advanced content caching settings on Mac (Plist Modification)

## Considerations

Set up Delivery Optimization for Windows 10 updates

Delivery Optimization reference

Blog - Michael Niehaus (details unreferenced elsewhere)

## Best Practices

## Delivery Optimization

We have a few examples of how Delivery Optimization settings can be configured to increase peer sharing and throttle network bandwidth.  These are provided as a fully functional example, but consider what settings are most appropriate for your environment.

**Suggested for 1803 and later:**

- Download Mode: LAN (1)
- Group ID : (GUID per location.  Only needed with specific Download modes)***
- Select the source of Group IDs : (The options set in this policy only apply to Group (2) download mode. If Group (2) isn't set as Download mode, this policy will be ignored.)***
- Absolute Max Cache Size: 30 GB
- Allow uploads while the device is on battery while under set Battery level: 40
- Delay background download from http (in secs): 600 (10 min)**
- Delay Foreground download from http (in secs): 600 (10 min)**
- Max Cache Age: 2592000 (30 days)Maximum Download Bandwidth (in KB/s): 500 (500 KB/s = 4 mbit)*
- Minimum Peer Caching Content File Size (in MB): 1
- Minimum RAM (inclusive) allowed to use Peer Caching (in GB): 2

*The Maximum Download Bandwidth setting was removed in version 2004, and replaced with new settings for throttling traffic based on Foreground or Background channels.

**NOTE: As of March 31 2021, Automox leverages the Foreground channel to download updates. There is work to change the channel used for downloading updates to the background channel. Suggestion is to delay the background channel traffic only and not delay the foreground channel once Automox switches its channel use.

***Specific to Download Mode and Group settings. Only needed in association with specific selections.

**Suggested for 2004 and later:**

- Settings defined for 1803 and later
- Maximum Foreground Download Bandwidth (in KB/s): 500*
- Maximum Background Download Bandwidth (in KB/s): 500*

*NOTE: As of March 31 2021, Automox leverages the Foreground channel to download updates. There is work to change the channel used for downloading updates to the background channel. Suggestion is to throttle the background channel traffic only and not throttle the foreground channel once Automox switches its channel use.

https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization-reference#maximum-foreground-download-bandwidth-in-kbps

### Considerations per environment:

- Download Mode - There are several options for different environments. Common options are:
  - 1 for LAN. Optionally add the “Select a method to restrict peer selection = 1” settings to further restrict sharing to other devices on the same subnet mask. This can be useful in large WAN environments with a centralized internet egress point to ensure devices share within their subnets only.
  - 2 - Group. There are extensive options when utilizing Active Directory Sites, DHCP, DNS suffix, or Azure groups are utilized. You can also define a custom GUID to define your group. Please see the options available in the Microsoft documentation here: https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization-reference#select-the-source-of-group-ids
  - 3 - Internet. This is ideal for devices that are always remote.
- GroupID - Only relevant with specific download modes
- Select the source of Group IDs - The options set in this policy only apply to Group (2) download mode. If Group (2) isn't set as Download mode, this policy will be ignored.
- Select a method to restrict Peer Selection - option to filter peer selection by subnet mask when selecting LAN or Group Download Mode
- Delay background download from http (in secs) - discuss your installation expectations. The scenario above forces clients to leverage peer sharing by delaying fall back to downloading content directly from the internet for 10 minutes.
- Maximum Foreground and Background Download Bandwidth - discuss with the networking team to optimize settings. This could be specific to a specific office as an example should there be a high client count and\or low available bandwidth.
- Minimum Peer Caching Content File Size (in MB). We suggest lowering the minimum file size to share to encourage a higher peer-to-peer sharing percentage.
- Minimum RAM (inclusive) allowed to use Peer Caching (in GB). We recommend setting the minimum RAM requirement from the default of 4GB in environments where virtual devices or automated RAM allotment solutions are in place. If a device has less than the defined minimum RAM amount, DO will not honor the assigned configurations.

### Automox and Delivery Optimization

To propagate peer-to-peer content sharing, consider staging updates prior to scheduled production patch policy time. This would match up well with a pilot patch policy run a day or so before production patch policies are scheduled (or within an appropriate amount of time to ensure the patches distributed earlier would match those needed at the production policy run time).

Peer-to-peer content sharing via DO becomes more effective when there are 10 or more peers within a group. DO content sharing breaks up content into small portions, allowing peer connections to 10s - 100s of other devices at a time. Updates are not shared as a full patch, rather as smaller bits of content. This concept is important when considering a staging strategy.

## GPO and Registry Information

### Download Mode - DODownloadMode

Specifies the download method that Delivery Optimization can use in downloads of Windows Updates, Apps and App updates.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DODownloadMode
Value Type: REG_DWORD
Value: The following list shows the supported values:

- 0 = HTTP only, no peering.
- 1 = HTTP blended with peering behind the same NAT.
- 2 = HTTP blended with peering across a private group. Peering occurs on devices in the same Active Directory Site (if exist) or the same domain by default. When this option is selected, peering will cross NATs. To create a custom group use Group ID in combination with Mode 2.
- 3 = HTTP blended with Internet Peering.
- 99 = Simple download mode with no peering. Delivery Optimization downloads using HTTP only and does not attempt to contact the Delivery Optimization cloud services.
- 100 = Bypass mode. Do not use Delivery Optimization and use BITS instead.

### Group ID - DOGroupId

Group ID must be set as a GUID. This policy specifies an arbitrary group ID that the device belongs to.

Use this if you need to create a single group for Local Network Peering for branches that are on different domains or are not on the same LAN.
**Note**: this is a best effort optimization and should not be relied on for an authentication of identity.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:

SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DOGroupId
Value Type: REG_SZ

**Note**: You can generate a GUID easily with PowerShell: [guid]::NewGuid()

### Select the source of Group IDs - DOGroupIdSource

Set this policy to restrict peer selection to a specific source.When set, the Group ID will be assigned automatically from the selected source. If you set this policy, the GroupID policy will be ignored.

The options set in this policy only apply to Group (2) download mode. If Group (2) isn't set as Download mode, this policy will be ignored.

For option 3 - DHCP Option ID, the client will query DHCP Option ID 234 and use the returned GUID value as the Group ID.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DOGroupIdSourceValue Type: REG_DWORD
Value: Options available are:

- 1 = AD Site.
- 2 = Authenticated domain SID.
- 3 = DHCP Option ID.
- 4 = DNS Suffix.
- 5 = AAD Tenant ID.

### Select a method to restrict Peer Selection - DORestrictPeerSelectionBy

Set this policy to restrict peer selection via selected option.

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DORestrictPeerSelectionByValue Type: REG_DWORD
Value: Options available are:

- 1 = Subnet mask (more options will be added in a future release).

Option 1 (Subnet mask) applies to both Download Mode LAN (1) and Group (2).

Absolute Max Cache Size (in GB) - DOAbsoluteMaxCacheSize

Specifies the maximum size in GB of Delivery Optimization cache.This policy overrides the DOMaxCacheSize policy.

The value 0 (zero) means "unlimited" cache; Delivery Optimization will clear the cache when the device runs low on disk space.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE|
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DOAbsoluteMaxCacheSize
Value Type: REG_DWORD
Default Value: 10
Min Value: 0
Max Value: 4294967295
The default value is 10 G

**Delay background download from http (in secs) - DODelayBackgroundDownloadFromHttp**

This policy allows you to delay the use of an HTTP source in a background download that is allowed to use P2P.

After the max delay has reached, the download will resume using HTTP, either downloading the entire payload or complementing the bytes that could not be downloaded from Peers.

Note that a download that is waiting for peer sources, will appear to be stuck for the end user.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:

SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DODelayBackgroundDownloadFromHttp
Value Type: REG_DWORD
Default Value: 0
Min Value: 0
Max Value: 4294967295
The default value is 0 (no delay)

### Delay Foreground download from http (in secs) - DODelayForegroundDownloadFromHttp

This policy allows you to delay the use of an HTTP source in a foreground (interactive) download that is allowed to use P2P.

After the max delay has reached, the download will resume using HTTP, either downloading the entire payload or complementing the bytes that could not be downloaded from Peers.

Note that a download that is waiting for peer sources, will appear to be stuck for the end user.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DODelayForegroundDownloadFromHttp
Value Type: REG_DWORD
Default Value: 0
Min Value: 0
Max Value: 4294967295
The default value is 0 (no delay)

### Maximum Download Bandwidth (in KB/s) - DOMaxDownloadBandwidth

Specifies the maximum download bandwidth in KiloBytes/second that the device can use across all concurrent download activities using Delivery Optimization.

The default value 0 (zero) means that Delivery Optimization dynamically adjusts to use the available bandwidth for downloads.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10

RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DOMaxDownloadBandwidth
Value Type: REG_DWORD
Default Value: 0
Min Value: 0
Max Value: 4294967295
The default value is 0 (unlimited)

### Maximum Background Download Bandwidth (in KB/s) - DOMaxBackgroundDownloadBandwidth

Specifies the maximum background download bandwidth in KiloBytes/second that the device can use across all concurrent download activities using Delivery Optimization.

The default value 0 (zero) means that Delivery Optimization dynamically adjusts to use the available bandwidth for downloads.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DOMaxBackgroundDownloadBandwidth
Value Type: REG_DWORD
Default Value: 0
Min Value: 0
Max Value: 4294967295
The default value is 0 (unlimited)

### Maximum Foreground Download Bandwidth (in KB/s) - DOMaxForegroundDownloadBandwidth

Specifies the maximum foreground download bandwidth in KiloBytes/second that the device can use across all concurrent download activities using Delivery Optimization.

The default value 0 (zero) means that Delivery Optimization dynamically adjusts to use the available bandwidth for downloads.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DOMaxForegroundDownloadBandwidth
Value Type: REG_DWORD
Default Value: 0
Min Value: 0
Max Value: 4294967295
The default value is 0 (unlimited)

### Max Cache Age (in seconds) - DOMaxCacheAge

Specifies the maximum time in seconds that each file is held in the Delivery Optimization cache after downloading successfully.

The value 0 (zero) means "unlimited"; Delivery Optimization will hold the files in the cache longer and make the files available for uploads to other devices, as long as the cache size has not exceeded.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name:DOMaxCacheAge
Value Type: REG_DWORD
Default Value: 259200
Min Value: 0
Max Value: 4294967295
The default value is 3 days

### Allow uploads while the device is on battery while under set Battery level (percentage) - DOMinBatteryPercentageAllowedToUpload

Specify any value between 1 and 100 (in percentage) to allow the device to upload data to LAN and Group peers while on DC power (Battery).

The recommended value to set if you allow uploads on battery is 40 (for 40%). The device can download from peers while on battery regardless of this policy.

The value 0 means "not-limited"; The cloud service set default value will be used.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DOMinBatteryPercentageAllowedToUpload
Value Type: REG_DWORD
Default Value: 0
Min Value: 0
Max Value: 100
The default value is 0 (unlimited)

### Minimum RAM capacity (inclusive) required to enable use of Peer Caching (in GB) - DOMinRAMAllowedToPeer

Specifies the minimum RAM size in GB required to use Peer Caching.

For example if the minimum set is 1 GB, then devices with 1 GB or higher available RAM will be allowed to use Peer caching.

Recommended values: 1 GB to 4 GB.

Supported on: At least Windows 10 Server, Windows 10 or Windows 10 RT

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path:
SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization
Value Name: DOMinRAMAllowedToPeer
Value Type: REG_DWORD
Default Value: 4
Min Value: 1
Max Value: 100000
The default value is 4GB

# Index

## Sources

1. Delivery Optimization for Windows 10 updates - Windows Deployment
2. Optimize update delivery for Windows 10 updates (Windows 10) - Windows Deployment
3. Set up Delivery Optimization - Windows Deployment
4. Delivery Optimization reference - Windows Deployment
5. What is Quality of Service?
6. Quality of Service (QoS) Policy
7. What is content caching on Mac?
8. How to create a local mirror of the latest update for Red Hat Enterprise Linux 5, 6, 7, 8 without using Satellite server?
9. Create an Apache-based YUM/DNF repository on Red Hat Enterprise Linux 8
10. Repositories/Personal - Community Help Wiki
11. Setup Delivery Optimization (DO) for ConfigMgr Current Branch - Deployment Research

## References

[1] "What is Quality of Service? - Palo Alto Networks." https://www.paloaltonetworks.com/cyberpedia/what-is-quality-of-service-qos. Accessed 8 Mar. 2021.

[2] "Optimize Windows client update delivery - Microsoft Docs." 17 Feb. 2021, https://docs.microsoft.com/en-us/windows/deployment/update/waas-optimize-windows-10-updates. Accessed 9 Mar. 2021.

[3], [4], [5], and [6] reference the following: "Delivery Optimization for Windows 10 updates", https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization