

DaaS 3 - Acceptance Checklist



Summary

Evolve IP requires the following best practices be implemented with DaaS, ensuring best user experience and supportability. As the client administrator, you are responsible to understand and implement all or some of the policies below, based on your specific requirements.

Evolve IP service delivery requires that the following be setup, configured and tested prior to entering a UAT phase of the project. Long term Evolve IP support and SLA's will be contingent upon the client environment being in compliance with the following recommendations and best practices.

Recommended Best Practices and Policies:

Disabling Windows Feature Updates

A feature update is when Windows 10 version 1903 is upgraded to the next feature release of Windows 10 1909. This update process can impact performance and functionality of your desktops for many reasons such as 3rd party vendors who needs to test the update from Microsoft before they will deploy their own update. Disabling the Windows feature update reduces the impact of this process and maintains the stability of your DaaS platform.

Applications and Load Over Time - Memory Requirements Will Grow

Memory resources are a driving factor in the performance of your DaaS seat. It is important to recognize that over time as you add new applications that were not part of the initial design requirements, less free memory (RAM) can constrain performance. Specifically, Real Time Audio Video collaboration tools will see a performance decrease as memory is consumed by additional applications. See the Real Time Audio Video Collaboration Tools section below for more details.

It is recommended that before you add new applications or software to check with Evolve IP to see if any changes to the DaaS seat resources are necessary.

Real Time Audio Video Collaboration Tools

Real Time Audio Video (RTAV) collaboration has become a standard tool for every business. It is important to recognize that the manufacturer's recommendation to use RTAV tools like Microsoft Teams and Zoom is to run them locally from the users endpoint. Evolve IP deploys our vendor's RTAV optimizations in order to provide the best RTAV possible outside of running from the local endpoint. RTAV will have performance and feature limitations running in DaaS when compared to running them from your local machine. We have detailed our experience with RTAV in virtualized environments [here](#) for your reference to help you select the best DaaS seat option.

Group Policy Objects

GPOs are settings within Microsoft's OS that define what a system will look like and how it will behave for a defined group of users. For example, GPOs enable control over a user's ability to access restricted files, run 3-D graphics, deploy new software, run background processes and limit a user's access to applications like the payroll software.

Evolve IP has provided the following GPOs to provide the best user experience:

Performance Optimization GPOs

Microsoft Teams Optimization

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Microsoft Teams Optimization
2. Evolve IP can provide the needed admx/adml files if these options are missing.
 - a. The ADMX files would get copied into your "Policy Definitions" folder
 - b. The ADML files would get copied into your "Policy Definitions\en-US" folder
3. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative Templates -> VMware View Agent Configuration VMware HTML5 Features VMware WebRTC Redirection Features**
 - i. Enable Media Optimization for Microsoft Teams
 1. Enabled

IE Graphics Optimization

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - IE Graphics Optimization
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **User Configuration -> Preferences -> Windows Settings -> Registry**
 - i. Action: Create
 - ii. Hive: HKEY_CURRENT_USER
 - iii. Key Path: Software\Microsoft\Internet Explorer\Main
 - iv. Value Name: UseSWRender
 - v. Value Type: REG_DWORD
 - vi. Value Data: 00000001
 - vii. Base: Hexadecimal

Chrome Graphics Optimization

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Chrome Graphics Optimization
2. Evolve IP can provide the needed admx/adml files
 - a. Copy CHROME.ADMX into your "Policy Definitions" folder
 - b. Copy CHROME.ADML into your "Policy Definitions\en-US" folder
3. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative Templates -> Google - > Google Chrome**
 - i. Use hardware acceleration when available: Disabled

Chrome - Disable Software Reporter Tool

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Chrome Disable Software Reporter Tool
2. *Right-click the GPO that you created for the group policy settings and select Edit.*
 - a. **Computer Configuration -> Preferences -> Windows Settings -> Registry**
 - i. Registry Key 1:
 1. Action: Create
 2. Hive: HKEY_LOCAL_MACHINE
 3. Key Path: Software\Policies\Google\Chrome
 4. Type: DWORD
 5. Name: ChromeCleanupEnabled
 6. Value: 0
 - ii. Registry Key 2:
 1. Action: Create
 2. Hive: HKEY_LOCAL_MACHINE
 3. Key Path: Software\Policies\Google\Chrome
 4. Type: DWORD
 5. Name: ChromeCleanupReportingEnabled
 6. Value: 0

Office 2016/2019/365 Graphics Optimization

1. **NOTE: This GPO is version specific. If using an older version of office, the appropriate ADMX/ADML files would be required.**
2. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Office 2016/2019/365 Graphics Optimization
3. Evolve IP can provide the needed admx/adml files
 - a. Copy all office ADMX files into your "Policy Definitions" folder
 - b. Copy all office ADML files into your "Policy Definitions\en-US" folder
4. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **User Configuration -> Policies -> Administrative Templates -> Microsoft Office 2016 -> Miscellaneous**
 - i. Do not use hardware graphics acceleration: Enabled

Microsoft Edge Graphics Optimization

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 – Microsoft Edge Graphics Optimization
2. Evolve IP can provide the needed admx/adml files. [Download Microsoft Edge for Business - Microsoft](#)
 - a. Copy msedge.admx, msedgeupdae.admx, and msedgewebview2.admx into your "Policy Definitions" folder
 - b. Copy msedge.adml, msedgeupdae.adml, and msedgewebview2.adml into your "Policy Definitions\en-US" folder
3. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative -> Microsoft Edge**
 - b. User Hardware Acceleration when available
 - i. Disabled

Windows 10 & Update GPOs

Windows 10 Device Registration

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Windows 10 Device Registration
2. Evolve IP can provide the needed admx/adml files if these options are missing.
 - a. The ADMX files would get copied into your "Policy Definitions" folder
 - b. The ADML files would get copied into your "Policy Definitions\en-US" folder
3. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Device Registration**
 - i. Register domain-joined computers as devices
 1. Enabled
 - b. **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Update**
 - i. Do not connect to any Windows Update Internet Locations
 1. Disabled

Disable Peer to Peer Windows Updates

1. Create new GPO under the OU with the desktops in it with the name: Evolve IP- DaaS 3 - Windows Update Delivery Optimization
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Delivery Optimization**
 - i. Edit Download Mode
 1. Enabled
 2. HTTP only (0)

Allow Windows Store Apps to Auto Update

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Windows Store Apps
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Preferences -> Windows Settings -> Registry**
 - i. Action: Delete
 - ii. Hive: HKEY_LOCAL_MACHINE
 - iii. Key Path: Software\Policies\Microsoft\WindowsStore
 - iv. Value Name: AutoDownload

DaaS Windows Updates

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Windows Updates
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration Policies Administrative Templates Windows Components Windows Updates Windows Updates for Business**
 - i. Select when Preview Builds and Feature Updates are received: Enabled
 1. Select the Windows readiness level for the updates you receive: Semi-annual Channel
 2. After a Preview Build or Feature Update is released, defer receiving it for this many days:
366

RMM Windows Firewall Exceptions

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Windows Firewall
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration** **Policies** **Administrative**
Templates **Network** **Network Connections** **Windows**
Defender Firewall **Domain Profile**
 - i. Windows Defender Firewall: Allow inbound file and printer sharing exception : Enabled
 1. Allow unsolicited incoming messages from these IP addresses: 10.200.1.0/24
 - ii. Windows Defender Firewall: Allow ICMP exceptions: Enabled
 1. Options: Allow inbound echo request
 - iii. Windows Defender Firewall: Allow inbound remote administration exception: Enabled
 1. Allow unsolicited incoming messages from these IP addresses: 10.200.1.0/24

User Group Policy Loopback

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - User Group Policy Loopback
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative**
Templates -> System -> Group Policy
 - i. Configure user Group Policy Loopback processing mode:
Enabled
 1. Mode: Merge
3. **Ensure this GPO is processed last.**

User Experience GPOs

Turn Off Display

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Turn Off Display
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Administrative Templates -> System -> Power Management -> Video and Display Settings**
 - i. Turn Off the Display (Plugged In): Enabled
 - ii. Turn Off the Display (seconds): 0

PCoIP - Clipboard Redirection & vSphere Console Access

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 – PcoIP
2. Evolve IP can provide the needed admx/adml files
 - a. Copy PCOIP.ADMX into your "Policy Definitions" folder
 - b. Copy PCOIP.ADML into your "Policy Definitions\en-US" folder
3. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative -> Classic -> PCoIP Session Variables -> Overridable Administrator Defaults**
 - i. Enable access to a PCoIP session from a vSphere console
 1. Enabled
 - ii. Configure Clipboard Redirection
 1. Enabled
 2. Enabled in both directions

Blast - Screen Blanking & Clipboard Redirection

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 – Blast
2. Evolve IP can provide the needed admx/adml files
 - a. Copy VDM_BLAST.ADMX into your "Policy Definitions" folder
 - b. Copy VDM_BLAST.ADML into your "Policy Definitions\en-US" folder
3. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative -> Classic -> VMware Blast**
 - i. Screen Blanking
 1. Disabled
 - ii. Configure Clipboard Redirection
 1. Enabled
 2. Enabled in both directions

Outlook - Cached Mode Enabled

1. Create new GPO Under the OU with the desktops in it with the name:
Evolve IP - DaaS 3 - Outlook Cached Mode.
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **User Configuration -> Policies -> Administrative Templates**
Microsoft Outlook 2016 Account Settings Exchange Cached Exchange Mode
 - b. Set Cached Exchange Mode Sync Settings to enabled and 3 months unless customer requests longer duration
 - c. Set Use Cached Exchange Mode for new and existing Outlook profiles to enabled.
 - d. **User Configuration -> Policies -> Administrative Templates**
Microsoft Outlook 2016 Outlook Options Delegates
 - e. Set Disable shared mail folder caching to enabled

Prevent Bing as Default Search Engine

1. Download and install the latest *Microsoft Office 365 Group Policy Templates* (ADMX and ADML files)
 - a. <https://www.microsoft.com/en-us/download/details.aspx?id=49030>
2. Create new GPO Under the OU with the desktops in it with the name: Evolve IP - DaaS 3 - Disable Bing
3. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **Computer Configuration -> Policies -> Administrative Templates -> Microsoft Office 2016 (Machine) -> Updates**
 - b. Look through the list of policies and double-click on the ***Don't install extension for Microsoft Search in Bing that makes Bing the default the search engine*** option.
 - c. Select **Enabled** and then press **Apply** followed by **OK** to configure the policy.

Folder Redirection

1. Create new GPO Under the OU with the desktops in it with the name: Evolve IP - DaaS 3 - Folder Redirection
2. Right-click the GPO that you created for the group policy settings and select Edit.
 - a. **User Configuration -> Policies -> Windows Settings -> Folder Redirection**
 - i. Favorites (right click the folder)
 1. Setting: Basic (Redirect everyone's folder to the same location)
 2. Target Folder Location: Create a folder for each user under the root path
 3. Root Path: \\server\share
 4. Options:
 - a. Grant user exclusive rights to Favorites: Disabled
 - b. Move the Contents of Favorites to the new location: Enabled
 - c. Also apply redirection policy to Windows 2000 server, Windows...: Disabled
 - d. Policy Removal Behavior: Leave Contents

ii. Desktop

1. Setting: Basic (Redirect everyone's folder to the same location)
2. Target Folder Location: Create a folder for each user under the root path
3. Root Path: \\server\share
4. Options:
 - a. Grant user exclusive rights to Desktop: Disabled
 - b. Move the Contents of Desktop to the new location: Enabled
 - c. Also apply redirection policy to Windows 2000 server, Windows...: Disabled
 - d. Policy Removal Behavior: Leave Contents

iii. Documents

1. Setting: Basic (Redirect everyone's folder to the same location)
2. Target Folder Location: Create a folder for each user under the root path
3. Root Path: \\server\share
4. Options:
 - a. Grant user exclusive rights to Documents: Disabled
 - b. Move the Contents of Documents to the new location: Enabled
 - c. Also apply redirection policy to Windows 2000 server, Windows...: Disabled
 - d. Policy Removal Behavior: Leave Contents

iv. Downloads

1. Setting: Basic (Redirect everyone's folder to the same location)
2. Target Folder Location: Create a folder for each user under the root path
3. Root Path: \\server\share
4. Options:
 - a. Grant user exclusive rights to Downloads: Disabled
 - b. Move the Contents of Downloads to the new location: Enabled
 - c. Also apply redirection policy to Windows 2000 server, Windows...: Disabled
 - d. Policy Removal Behavior: Leave Contents

v. Music

1. Setting: Follow the Documents Folder

vi. Videos

1. Setting: Follow the Documents Folder

vii. Pictures

1. Setting: Follow the Documents Folder

File Exclusions for Anti Virus

File Exclusions for Anti Virus

File Exclusions for Anti Virus:

C:\Windows\system32\wbem\wmiprvse.exe
C:\Program Files\Citrix\User Profile Manager\UserProfileManager.exe
C:\Program Files\Citrix\Server Resource Management\Memory Optimization
Management\Program\CtxSFOSvc.exe
C:\Windows\system32\taskmgr.exe
\${WinDir}\SoftwareDistribution\Datastore\DataStore.edb
\${WinDir}\SoftwareDistribution\Datastore\Logs\Edb*.jrs
\${WinDir}\SoftwareDistribution\Datastore\Logs\Edb.chk
\${WinDir}\SoftwareDistribution\Datastore\Logs\Tmp.edb
\${windir}\Security\Database*.edb
\${windir}\Security\Database*.sdb
\${windir}\Security\Database*.log
\${windir}\Security\Database*.chk
\${windir}\Security\Database*.jrs
\${windir}\Security\Database*.xml
\${windir}\Security\Database*.csv
\${windir}\Security\Database*.cmtx
pcoip_server_win32.exe
wssm.exe
VMBlastS.exe
wsnm_jms.exe
vmwareviewclipboard.exe*
outlook.exe*
excel.exe
splwow64.exe
vmtoolsd.exe
C:\Program Files (x86)\VMware\VMware DaaS Agent\service\DaaSAgent.exe

Local Horizon View Client

Local Horizon View Client

Thick Client Requirements:

Minimum Version to support Teams Optimization is v2012 Build 8.1

Thin Client Requirements:

If using a Wyse 5030: The Firmware version must be v8.6_412_3040 in order for Teams Optimization to function

RMM Checks

RMM Checks

RMM allows you to set up periodic checks to ensure optimal performance. We recommend setting these checks for after hours in order to reduce load on the platform. Using any RMM scheduled task. Preexisting IT policies should be reevaluated prior to deploying automated

Client Signature: _____

Date: _____