



Optimizing UDS Enterprise in Windows 10

Deploying virtual desktops with Windows 10 requires making a planning and configuration that provides users with an optimized and secure virtual desktop platform.

This document describes a series of good practices related to Windows 10 configuration and characteristics that will allow you to optimize the performance and behavior of the virtual desktops deployed for your users.

The user configuration will be carried out on the Active Directory group policy objects, which have a direct influence on the user profile at the moment when said template source or golden image is loaded.

All other proposed configurations and modifications will be made on the virtual machine image defined as the source template, which subsequently will be used as the base for performing the deployment of virtual desktops. These are modifications in the system registry and modifications of operating system services.

One must take into account that most modifications in this document are recommended, and that it remains at the discretion of the system administrator whether or not to implement them, depending on the utility of the characteristic to be disabled. The character of the configuration type to be optimized, either recommended or mandatory, is indicated in the title of the corresponding section.

Of all of the modifications described in this document, some are generic and apply to all virtual desktop platforms, while others are exclusively for non-persistent virtual desktop platforms.

In no way are the proposed configurations and modifications necessary for the correct operation of a desktop virtualization platform; they simply optimize certain aspects of their operation. It is the responsibility of the system administrator to adopt changes and to make sure that the platform is operating correctly.

VirtualCable and the UDS Enterprise team are not responsible for any possible consequences to the stability of the system once the changes proposed in this document have been applied.



User configuration

Unlike machine configuration, user configuration cannot be applied to the base template on which the virtual desktops are going to be deployed. To make the changes in a centralized way, we recommend using the Group Policy Objects (GPO).

Recommended generic user configurations

Group Policy Objects: We recommend applying the following GPO configurations to any virtual desktop platform.

Element	Route	Explanation
Screen saver	Administrative Templates – Control Panel – Personalization Activate screen saver: Enabled Prevent changes in screen saver: Enabled Password protected screen saver: Enabled Screen saver activation time: 600 seconds Force specific screen saver: scrnsave.scr	Using complex screen savers consumes a large amount of resources. You can use the basic screen saver to ensure the virtual desktop without consuming resources

Virtual Machine (MV) or source template configuration

For the configurations described in this section that involve changes to the Windows registry, we recommend taking into account the possible implications when making said changes.

Incorrectly modifying the Windows registry can make the system unstable. We recommend creating a backup of the Windows registry before making any change to it.

For a correct optimization of the source virtual machine, there are a series of parameters that we can adjust in order to improve its performance.

The adjustments on the source virtual machine can be separated into three sections: system registry, group policy objects or GPO and Windows 10 services.



Recommended generic VM configurations

System registry: The following changes in the system registry are valid for any virtual desktop platform, persistent or non-persistent. These modifications will reduce the usage of virtual desktop resources in the hypervisor platform.

Configuration	Modification in the registry	Explanation
Deactivate "Last Access Timestamp"	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem] "NtfsDisableLastAccessUpdate"=dword:00000001	Increases speed when visualizing files
Reduce delay when showing the Menu	[HKEY_CURRENT_USER\Control Panel\Desktop] "MenuShowDelay"="150"	Reduce delay when showing the Windows menu. It provides a better user experience
Disable all visual effects except "Use of common tasks in folders" and "Use of visual styles in buttons and Windows"	[HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics] "MinAnimate"="0" [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced] "ListViewAlphaSelect"=dword:00000000 "TaskbarAnimations"=dword:00000000 "ListViewShadow"=dword:00000000 [HKEY_CURRENT_USER\Control Panel\Desktop] "DragFullWindows"="0" "FontSmoothing"="0" "UserPreferencesMask"=binary:90,12,01,80,10,00,00,00	Provides a better user experience
Hide "Hard Error Messages"	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows] "ErrorMode"=dword:00000002	It doesn't show error messages



Recommended VM configurations for non-persistent desktops

System Registry: These changes in the registry are recommended for non-persistent virtual desktops. As you can see in the chart below, the parameters are used to configure event registrations, log storage and disk defragmentation. These services aren't used in non-persistent virtual desktops.

Configuration	Modification in the registry
Disable Clear Page File at Shutdown	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management] "ClearPageFileAtShutdown"=dword:00000000
Disable Background Defragmentation	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction] "Enable"="N"
Disable Background Layout Service	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OptimalLayout] "EnableAutoLayout"=dword:00000000
Disable Bug Check Memory Dump	[HKLM\SYSTEM\CurrentControlSet\Control\CrashControl] "CrashDumpEnabled"=dword:00000000 "LogEvent"=dword:00000000
Disable Memory Dumps	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl] "CrashDumpEnabled"=dword:00000000 "LogEvent"=dword:00000000
Disable Mach. Acct. Password Changes	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters] "DisablePasswordChange"=dword:00000001
Redirect Event Logs	HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application] "File"="D:\EventLogs\Application.evtx" [HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security] "File"="D:\EventLogs\Security.evtx" [HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\System] "File"="D:\EventLogs\System.evtx"
Reduce Event Log Size to 64K	HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application] "MaxSize"=dword:00010000 [HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security] "MaxSize"=dword:00010000 [HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\System] "MaxSize"=dword:00010000



Group Policy Objects: We recommend applying the following GPO configurations to any virtual desktop platform. These configurations are enabled in Windows 10 by default, as it is not necessary to have these options enabled when deploying non-persistent virtual desktops based on templates since, apart from using resources, these configurations are useful when the virtual desktop remains in time.

Element	Route	Explanation
Error report	Administrative Templates – Windows Components – Windows Error Report Deactivate Windows Error Report: Enabled	Creates application dumps that are sent to Microsoft. It is advisable to deactivate it unless you have to troubleshoot in an application
Windows Update	Administrative Templates – Windows Components – Windows Updates Configure automatic updates: Disabled	Windows updates must be made on the source template
System restoration	Administrative Templates – System – System Restoration Turn off system restoration: Enabled	It is not necessary since the virtual desktops are going to be based on a source template

Recommended services configuration for non-persistent desktops

Services: Windows 10 includes a series of services activated by default. These services improve performance as the virtual desktop is kept in time. UDS Enterprise allows, among other functions, the publication of non-persistent virtual desktops. So, for this type of deployments, having these services active doesn't make much sense. We list the services which may be disabled below.

Configuración	Recomendación	Justificación
Background intelligence transfer service	Disabled	This service uses the inactive network bandwidth for services such as Windows Update. As you are going to deactivate services that depend on BITS, this service will be deactivated
Applications experience	Disabled	Automatically implements the software updates to the programs. This functionality does not tend to be necessary in a virtual desktop environment
Function discovery resource publication service	Disabled	This service publishes information from the desktop to the network so that others can find it. This functionality does not tend to be necessary in a virtual desktop environment
BitLocker encryption Service	Disabled	This functionality does not tend to be necessary in a virtual desktop environment



UDS Enterprise

Optimizing UDS Enterprise in Windows 10

www.udsenderprise.com

Service of the backup module to block-level	Disabled	Windows uses WBENGINE service to make backup and recovery operations. It is not necessary to enable this service
Computer browser service	Disabled	It maintains an updated list of computers on your network and supplies this list to computers designated as browsers. This functionality does not tend to be necessary in a virtual desktop environment
Home Group Listener	Disabled	Just like in most environments, virtual desktops will be linked to a domain, so the Home Group functionality is not necessary
Home Group Provider	Disabled	
Hyper-V data exchange service	Disabled	This functionality is not necessary
Hyper-V Guest Shutdown Service	Disabled	This functionality is not necessary
Hyper-V Heartbeat Service	Disabled	This functionality is not necessary
Remote Desktop's Hyper-V virtualization service	Disabled	This functionality is not necessary
Hyper-V Time Synchronization Service	Disabled	This functionality is not necessary
Hyper-V Volume Shadow Copy Requestor	Disabled	This functionality is not necessary
Parental control	Disabled	This functionality is not necessary
The problem reports and solutions control Panel support	Disabled	This service provides support to view, send, and delete problem reports of system level for the problem reports and solutions control panel. This functionality is not usually necessary in a virtual desktop environment
Host UPnP device	Disabled	Allows UPnP devices to be hosted in the computer. This functionality is usually not necessary in a virtual desktop environment
Windows error reporting service	Disabled	Allows to report errors when programs fail to operate or respond and provide existing solutions. It also allows to generate logs for diagnostic and repair services. This service is generally not necessary in a VDI environment
Volume shadow copy	Disabled	Manages and implements Volume Shadow Copies used for backup and other purposes. This service must be disabled
Writing pad and touch keyboard service	Disabled	Enables the functionality of pen and pen input panel of the handwriting and touch pad. This service is generally not necessary in VDI
SSDP Detection	Disabled	It detects devices and network services that use the SSDP detection Protocol, such as UPnP devices. This service is generally not necessary in a virtual desktop environment
Secure Socket Tunneling Protocol service	Disabled	It offers compatibility with the (SSTP) secure sockets tunnel Protocol to connect to remote computers using VPN. This service is generally not necessary in a virtual desktop environment



UDS Enterprise

Optimizing UDS Enterprise in Windows 10

www.udsenderprise.com

Windows Biometric Service	Disabled	Provides to the client application the ability to capture, compare, manipulate and store biometric data without direct access to any sample or biometric hardware
Windows Store Service (WSService)	Disabled	Provides infrastructure support for the Windows Store
Diagnostic service host	Disabled	Diagnostic Policy service uses the diagnostic service Host to host the diagnoses that must run in the context of local service
Host de sistema de diagnóstico	Disabled	El Servicio de directivas de diagnóstico usa el Host del servicio de diagnóstico para hospedar los diagnósticos que deben ejecutarse en un contexto de Servicio local
Host provider of detection of function	Disabled	The FDPHOST service hosting providers of detection of FD (functions detection) networks. This functionality is not usually necessary in a virtual desktop environment
Security center	Disabled	When this is disabled, the service does not report anti-virus, malware or firewall configuration problems. Since many of these elements are disabled in a virtual desktop environment, deactivating this service erases the messages shown to users
Superfetch	Disabled	Maintains and improves system performance over the course of time. Since the data of this service is stored with the operating system in non-persistent virtual desktop environments, this functionality is not necessary
Themes	Disabled	Allows the user to operate the desktop themes that include wallpapers and visual and sound effects that consume resources of the machine
IP Helper Application	Disabled	It provides tunnel connectivity using IPv6 transition technologies
The Microsoft iSCSI initiator service	Disabled	It administers the Internet (iSCSI) SCSI sessions. This service must be disabled
Microsoft software shadow copy provider	Disabled	Manages software-based volume snapshots taken by the volume shadow copy service. This functionality is not usually necessary in a virtual desktop environment
Offline files	Disabled	The offline files service performs maintenance activities on the offline files cache. This functionality is not usually necessary in a virtual desktop environment
Windows Defender	Disabled	Most organizations have their own anti-virus system. For this reason, this service should be disabled
Window media player network sharing service	Disabled	Unless the users are going to share elements by using Media Player, this service can be disabled
WWAN Automatic configuration	Disabled	This service manages connections and adapters embedded modules/data card (GSM and CDMA) mobile broadband by automatically configuring networks. This service is generally not necessary in a virtual desktop environment



WLAN Automatic configuration	Disabled	The WLANSVC service provides the logic to configure, detect, connect and disconnect from a network of wireless local area network (WLAN), as defined in the IEEE 802.11 standards. This service should be disabled
Windows Search	Disabled	Provides content indexing, cache search results for files, email, and other types of content and properties. This service must be disabled
Windows Update	Disabled	Enables the detection, download and installation of updates for Windows and other programs. This service must be disabled

Common configurations

These final configurations optimize the desktop by eliminating unnecessary elements. They are applied to different sections within the OS of the source machine. In the case of anti-viruses, we recommend consulting the manufacturer for these types of optimizations.

Configuration	Recommendation	Explanation
Startup animation	Disable with the following command bcdedit /set bootux disabled	Disables the animation, reduces the use of resources and speeds up the desktop startup process
Erase unused Windows components	Windows Media Center DVD Maker Tablet components	These components are not used in a centralized VDI environment
Paging file	Match the minimum and the maximum	Keeping the paging file at a single size prevents it from growing, thus avoiding a high use of IO
Disk cleanup	Erase unnecessary files	Cleans up unnecessary files
Disk defragmentation	Perform disk defragmentation	Disk defragmentation must be performed as the final step in the creation of the source template
Anti-virus	Optimize	Configures the anti-virus for scanning scripts and disabling automatic updates. The source template must be scanned before moving on to production

Support and professional services

VirtualCable sells UDS Enterprise through a subscription model, including product support and updates in segments based on number of users.

Additionally, VirtualCable offers a broad portfolio of professional services to install and configure UDS Enterprise and other virtualization technologies.

For further information visit www.udsenderprise.com or email us at info@udsenderprise.com