Gallagher Command Centre

Visitor Management Kiosk Hardened Installation

Technical Document

Copyright © Gallagher Group Limited

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2025. All rights reserved.

Contents

1 Introduction 4
2 Prerequisites 4
3 Implications 4
4 Procedure 4
5 Configure Windows Accounts 5
6 Prepare and deploy Visitor Management Kiosk 5
7 Disable Boot Options 6
8 Enable Windows Embedded Shell Launcher 6
9 Set custom shell 6
10 Configure Windows Automatic Logon (optional) 8
11 Configure Command Centre Automatic Logon (optional) 9
12 Preventing installation of all devices (optional) 9
Appendix A - Physical Security Considerations 11
Appendix B - Shell Removal 12

Copyright © Gallagher Group Limited

1 Introduction

This document describes the process for configuring a Microsoft Windows 10 or 11 system to boot into the Visitor Management Kiosk application as its shell, automatically logging on with a specified windows user account and Command Centre operator account.

The final configuration will have two windows accounts:

1. Low privilege Kiosk operator account.
2. Local administrative configuration account.

It is recommended that this configuration be utilised in combination with a secure Kiosk enclosure to ensure best security.

IMPORTANT:
The VM Kiosk application runs on a supported Microsoft Windows environment.
It is the site installers responsibility to ensure the implemented solution meets the sites requirements by researching, implementing and regularly reviewing the kiosk environment to ensure hardening against break outs. This document gives examples of how hardening can be achieved.

2 Prerequisites

The following software is required.

- Gallagher Command Centre.
- Gallagher Visitor Management Kiosk.
- Microsoft Windows 10/11 Enterprise or Education edition.
- A Gallagher Command Centre Division configured for Visitor Management including Kiosk features.

3 Implications

Once implemented, a physical keyboard and mouse will be required to login into the Kiosk PC with an administrative account.

The Visitor Management Kiosk software will be executed as the windows shell, there will be no UI elements from the standard Windows explorer interface available.

Ensure that the configuration works before applying the hardening. Also ensure that all settings, for example screen resolution, etc are set as per preference, before applying the hardening. Once the hardening has been applied these setting will not be available.

4 Procedure

1. Configure Windows Accounts.
2. Prepare and deploy Visitor Management Kiosk.
3. Disable Boot Options:
    - F8 Boot Key
    - F10 Boot Key
    - Boot UI
4. Enable Windows Embedded Shell Launcher.
5. Set custom shell.
6. Configure Windows Automatic Logon. (optional)
7. Configure Command Centre Automatic Logon. (optional)

Copyright © Gallagher Group Limited

5 Configure Windows Accounts

Complete the steps below on a clean install of Windows 10 or 11 Enterprise or Education edition.

1. Log into windows with an account with administrative rights.
2. Open the Computer Management console and navigate to Local User and Groups > Users.
3. Select each of the user accounts, including the Built-in user accounts and set a strong complex password on each of them.
4. Remove or disable any non-essential windows user accounts from the system, this process should include disabling the all the built-in user accounts.
5. Ensure you have a windows account configured with local administrative rights, this account will be used when preforming administrative functions on the Gallagher Visitor Management Kiosk.
6. Create a new windows account for Gallagher Visitor Management Kiosk basic operation. This account should:
    - Not be a local administrator.
    - Have a strong complex password.

Gallagher recommend a minimum password length of 8 characters and it should include at least three of the following four-character types, lowercase letters, uppercase letters, numbers, and symbols.

6 Prepare and deploy Visitor Management Kiosk

Manually deploy the Visitor Management Kiosk build from your Command Centre server.

1. On the Command Centre Server navigate to the “VMKioskSetup” installation folder. VMKioskSetup default location:
2. For 32-bit systems: C:\Program Files (x86)\Gallagher\Command Centre\VMKioskSetup\
3. For 64-bit systems: C:\Program Files\Gallagher\Command Centre\VMKioskSetup\
4. From the inside the VMKioskSetup folder locate the “VMKiosk” folder and copy this to a temporary location such as the desktop. You can rename the copied “VMKiosk” folder if desired.
5. Inside the “VMKiosk” folder locate the file “VMKiosk.exe.config”
6. Open the file using notepad or a basic text editor.
7. Locate the following section:

```
“<appSettings>

<add key="ServerUri" value="opc.tcp://localhost:4840/UA/CommandCentre/"/>

<add key="WorkflowScreenFactoryLabel" value="Visitor Management Example" />

<!-- in seconds -->
```

8. Modify the following line, replacing localhost with your Command Centre Server name:

```
“address=" value="opc.tcp://CommandCentreServerName:4840/UA/CommandCentre/"/>”
```

9. Save the modified file and exit your editor.
10. Move the VMKiosk folder to your target workstation, e.g. C:\VMKiosk.

Copyright © Gallagher Group Limited

7 Disable Boot Options

1. While logged in as your local administrator account, right click on the start button and select Command Prompt (Admin) to open a command prompt window with elevated administrative privileges.
2. Enter the following at the prompt to disable the F8 safe boot option on start-up:

```
bcdedit.exe -set {globalsettings} advancedoptions false
```

3. Enter the following at the prompt to disable start-up user interface.

```
bcdedit.exe -set {globalsettings} bootuxdisabled on
```

8 Enable Windows Embedded Shell Launcher

1. What Microsoft operating system are you using?
   If **Window 10**, go to Step 2.
   If **Windows 11**, go to Step 4.
2. To enable Windows Embedded Shell Launcher, right click on the **Start** button and select Command Prompt (Admin) to open a command prompt window with elevated administrative privileges.
3. Enter the following:

```
Dism /online /Enable-Feature /all /FeatureName:Client-EmbeddedShellLauncher
```

4. To enable Windows Embedded Shell Launcher, open Powershell with elevated administrative privileges.
5. Enter the following:

```
Enable-WindowsOptionalFeature -online -FeatureName Client-EmbeddedShellLauncher -all
```

   Note: This may take some time to run.

9 Set custom shell

1. Create and run a PowerShell script to configure the shell environment.
2. Open Notepad and copy and paste the following text into a new note, replacing:
   - KioskUserAccount with the windows account name you created in section 5 point number 6.
   - C:\VMKiosk\VMKiosk.exe with the correct path to your kiosk as determined in section 6 point number 10.

Copyright © Gallagher Group Limited

See example below.

```
# Setup computer environment
$COMPUTER = "localhost"
$NAMESPACE = "root\standardcimv2\embedded"
# Create a handle to the class instance in order to call the static methods.
$ShellLauncherClass = [wmiclass]"\\$COMPUTER\${NAMESPACE}:WESL_UserSetting"
# This well-known security identifier (SID) corresponds to the BUILTIN\Administrators group.
$Admins_SID = "S-1-5-32-544"
# Create a function to retrieve the SID for a user account on a machine.
function Get-UsernameSID($AccountName) {
   $NTUserObject = New-Object System.Security.Principal.NTAccount($AccountName)
   $NTUserSID = $NTUserObject.Translate([System.Security.Principal.SecurityIdentifier])
            return $NTUserSID.Value }
# Get the SID for a user account named "KioskUserAccount". - this is the Windows user account that will be running VM Kiosk
$VMKiosk_SID = Get-UsernameSID("KioskUserAccount")
# Define actions to take when the shell program exits.
$restart_shell = 0
$restart_device = 1
$shutdown_device = 2
# Set the Kiosk as the shell for "KioskUserAccount", and restart the machine if the Kiosk is closed and identify the application to run in the shell.
$ShellLauncherClass.SetCustomShell($VMKiosk_SID, "c:\VMKiosk\VMKiosk.exe", ($null), ($null), $restart_shell)
# Set Explorer as the shell for administrators.
$ShellLauncherClass.SetCustomShell($Admins_SID, "explorer.exe")
# View the custom shells defined.
"`nCurrent settings for custom shells:"
Get-WmiObject -namespace $NAMESPACE -computer $COMPUTER -class WESL_UserSetting | Select Sid, Shell, DefaultAction
# Enable Shell Launcher
$ShellLauncherClass.SetEnabled($TRUE)
$IsShellLauncherEnabled = $ShellLauncherClass.IsEnabled()
"`nEnabled is set to " + $IsShellLauncherEnabled.Enabled
# Disable DCOM
Write-Host "disable DCom"
$littlepause = Read-Host "hit the any key to continue"
Set-ItemProperty -Path HKLM:\Software\Microsoft\ole -Name EnableDcom -Value “N”
#set network connection profile to private
Get-NetConnectionProfile | Set-NetConnectionProfile -NetworkCategory private
# Disable Command Shell from opening IE or the explorer window
Set-ItemProperty -Path HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer -name NoRun -Value 1 -Type DWord
```


Copyright © Gallagher Group Limited

3. Save the file as “KioskScript.ps1” to a folder on your installation drive; e.g. “C:\script”.
   Note: To run PowerShell scripts (files that end with .ps1), you must first set the execution policy to Remote Signed. This allows you to execute the “KioskScript.ps1” file.
4. Launch PowerShell by right clicking on the start button and selecting Command Prompt (Admin) to open a command prompt window with elevated administrative privileges.

Type the following at the prompt:

```
C:\Windows\system32>powershell
```

5. Navigate to the directory where you saved the PowerShell script (C:/script is the location where you saved the PowerShell script at step 3):

```
PS C:\Windows\system32> cd C:\script
```

6. Run the following command at the PowerShell prompt:

```
C:\script> Set-ExecutionPolicy RemoteSigned
```

7. Execute the script by typing the following at the prompt and pressing enter (C:/script is the location where you saved the PowerShell script at step 3):

```
PS C:\script> .\KioskScript.ps1
```

10 Configure Windows Automatic Logon (optional)

This step is an optional method; it enables the automatic logon of a specified windows user account.

1. To configure Windows auto logon, right click on the start button, select Run and type “regedit” to open the Windows Registry editor.
2. Locate the key:

```
HKEY_LOCAL_MACHINE*\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
```

3. Create the following registry values if not already present.

Type	Name	Value
DWORD	AutoAdminLogon	1
STRING	DefaultUserName	Windows User Account Name
STRING	DefaultPassword	Windows User Account Password

Gallagher recommend a minimum password length of 8 characters and should include at least three of the following four-character types, lowercase letters, uppercase letters, numbers, and symbols.

Copyright © Gallagher Group Limited

11 Configure Command Centre Automatic Logon (optional)

This step is an optional method; it enables the automatic logon of a specified Gallagher Command Centre operator account.
Note: The Gallagher registry keys, (i.e. **Gallagher** and **Command Centre**), will not be present after deploying the VM Kiosk's click once on a new Windows install.
The registry keys (**Gallagher** and **Command Centre**) will need to be manually created.

1. To configure Gallagher Visitor Management Kiosk Auto Logon; while still in the Windows Registry editor create the following key.
    - 32-bit Windows installations:

```
HKEY_LOCAL_MACHINE*\SOFTWARE\Gallagher\Command Centre
```

    - 64-bit Windows installations:

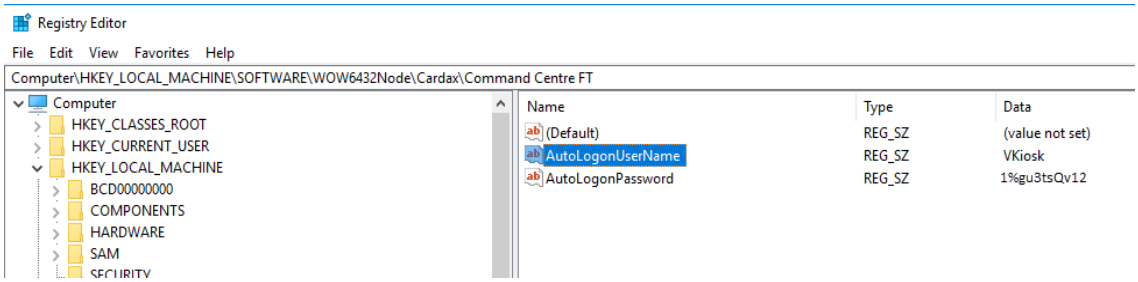
```
HKEY_LOCAL_MACHINE*\SOFTWARE\WOW6432Node\Gallagher\Command Centre
```

2. Create the following registry values if not already present.

Type	Name	Value
STRING	AutoLogonUserName	Command Centre Operator Logon
STRING	AutoLogonPassword	Command Centre Operator Password

Note: The order when adding the strings to the registry. The AutoLogonUserName must be created first and the AutoLogonPassword.

Example:



Gallagher recommend a minimum password length of 8 characters and should include at least three of the following four-character types, lowercase letters, uppercase letters, numbers, and symbols.

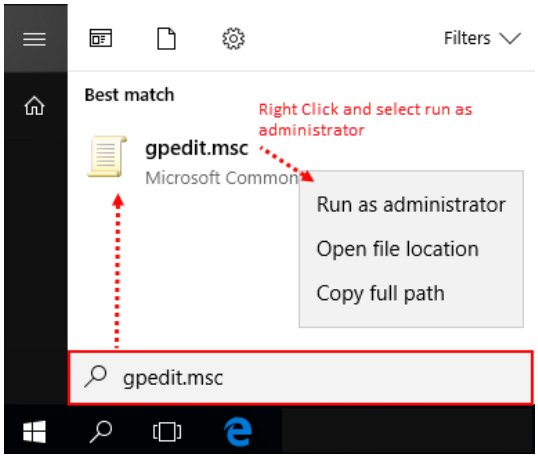
12 Preventing installation of all devices (optional)

As an administrator you can prevent standard users from installing any device, but allow administrators to install or update devices. This can be achieved by configuring the computer policies.

Copyright © Gallagher Group Limited

1. Open the Editor by a run command. Press Windows Key and R key simultaneously to turn on Run dialog, enter gpedit.msc. Right click on gpedit.msc and select “Run as administrator.

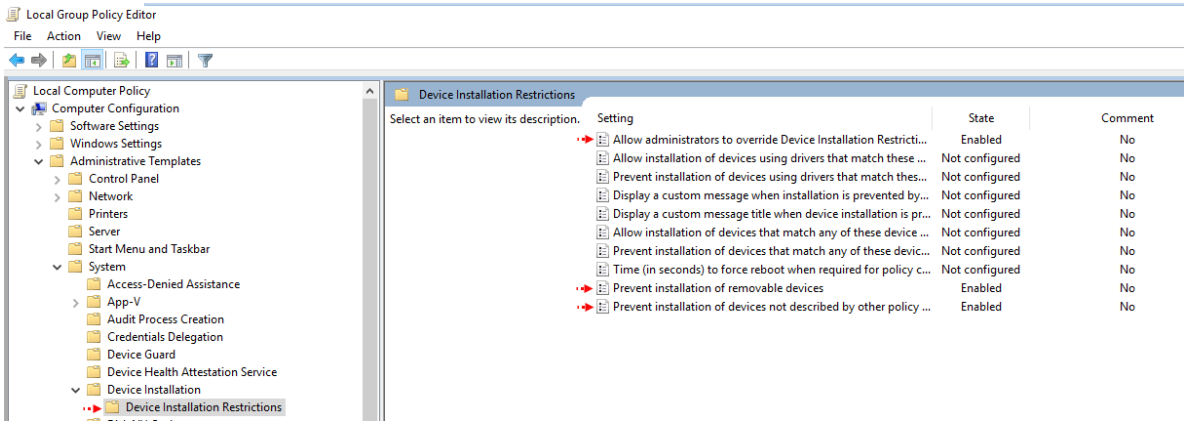
Example:



2. In the Local Group Policy Editor navigation pane, navigate to the following “Computer Configuration” location.

Administrative Templates > System > Device Installation > Device Installation Restrictions

Example:



3. Right-click “Allow administrators to override device installation policy”.
   - Open “Properties” and in the Setting tab, click “Enabled” to turn the policy setting on and then select apply.
4. Right-click “Prevent installation of devices not described by other policy settings”.
   - Open “Properties” and in the Setting tab, click “Enabled” to turn the policy on and then select apply.
5. Right-click “Prevent installation of removable devices”.
   - Open “Properties” and in the Setting tab, click “Enabled” to turn the policy on and then select apply.

Copyright © Gallagher Group Limited

Appendix A - Physical Security Considerations

1. When designing a cabinet or stand for the Kiosk system, the following should be considered.
2. No cables should be exposed/visible; Ethernet and power cables connecting to wall sockets should be shielded via the use of capping or secured cable runs.
3. External ports such as USB and PS2 serial should be not be exposed or accessible.
4. Vandal protection should be implemented for any external devices such as printers and barcode scanners.

Note: A Power buttons be placed in a discreet but accessible location on the outside of the Kiosk as per electric standards.

Copyright © Gallagher Group Limited

Appendix B - Shell Removal

The following script will remove the custom shell configuration. To do so:

1. Create and run a PowerShell script to configure the shell environment.
2. Open Notepad and copy and paste the following text into a new note, replacing KioskUserAccount with the windows account name you created in section 5 point number 6.

```
# Setup computer environment
$COMPUTER = "localhost"
$NAMESPACE = "root\standardcimv2\embedded"
# Create a handle to the class instance in order to call the static methods.
$ShellLauncherClass = [wmiclass]"\\$COMPUTER\${NAMESPACE}:WESL_UserSetting"
# This well-known security identifier (SID) corresponds to the BUILTIN\Administrators group.
$Admins_SID = "S-1-5-32-544"
# Create a function to retrieve the SID for a user account on a machine.
function Get-UsernameSID($AccountName) {
   $NTUserObject = New-Object System.Security.Principal.NTAccount($AccountName)
   $NTUserSID = $NTUserObject.Translate([System.Security.Principal.SecurityIdentifier])
            return $NTUserSID.Value }
# Get the SID for a user account named "KioskUserAccount".
$VMKiosk_SID = Get-UsernameSID("KioskUserAccount")
$ShellLauncherClass.RemoveCustomShell($Admins_SID)
$ShellLauncherClass.RemoveCustomShell($VMKiosk_SID)
# Disable Shell Launcher
$ShellLauncherClass.SetEnabled($FALSE)
$IsShellLauncherEnabled = $ShellLauncherClass.IsEnabled()
"`nEnabled is set to " + $IsShellLauncherEnabled.Enabled
```


Copyright © Gallagher Group Limited