

Windows 版 VMware Horizon Client 安裝和設定 指南

VMware Horizon Client for Windows 2012

您可以在 VMware 網站上找到最新的技術文件，網址如下：

<https://docs.vmware.com/tw/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2013-2021 VMware, Inc. 保留所有權利。 [版權與商標資訊](#)。

目錄

Windows 版 VMware Horizon Client 安裝和設定指南 7

- 1 Windows 用戶端的系統需求與設定 8**
 - Windows 用戶端系統的系統需求 8
 - Horizon Client 功能的系統需求 10
 - 智慧卡驗證需求 10
 - 用戶端裝置憑證驗證需求 12
 - OPSWAT 整合需求 12
 - 即時音訊視訊系統需求 13
 - 掃描器重新導向的系統需求 13
 - 序列埠重新導向的系統需求 14
 - 使用 URL 內容重新導向的需求 15
 - HTML5 多媒體重新導向的系統需求 16
 - 瀏覽器重新導向的系統需求 17
 - 多媒體重新導向 (MMR) 的系統需求 17
 - 地理位置重新導向的系統需求 18
 - 工作階段協作功能的需求 19
 - 搭配使用商務用 Skype 與 Horizon Client 的需求 19
 - 支援的桌面平台作業系統 20
 - 準備 Horizon Client 適用的連線伺服器 20
 - 清除用來登入伺服器的最後一個使用者名稱 22
 - 設定 VMware Blast 選項 22
 - 使用 Internet Explorer Proxy 設定 24
 - 設定 Horizon Client 資料共用 24
 - 由 VMware 收集的 Horizon Client 資料 25
- 2 安裝 Windows 版 Horizon Client 27**
 - 在 Windows 用戶端作業系統中啟用 FIPS 模式 27
 - 啟用自動網際網路通訊協定選取 28
 - 安裝 Windows 版 Horizon Client 28
 - 從命令列安裝 Horizon Client 30
 - Horizon Client 的安裝命令 30
 - Horizon Client 的安裝內容 31
 - 從命令列安裝 Horizon Client 34
 - 確認 URL 內容重新導向安裝 35
 - 線上更新 Horizon Client 36

- 3 為使用者設定 Horizon Client 38**
 - 一般組態設定 38
 - 使用 URI 設定 Horizon Client 39
 - 用於建立 vmware-view URI 的語法 39
 - vmware-view URI 範例 43
 - 在 Horizon Client 中設定憑證檢查模式 46
 - 設定使用者的憑證檢查模式 47
 - 設定進階 TLS 選項 48
 - 自訂 Horizon Client 功能表 48
 - 自訂 Horizon Client 錯誤訊息 48
 - 設定游標事件處理 49
 - 使用群組原則設定來設定 Horizon Client 49
 - 用戶端 GPO 的指令碼定義設定 50
 - 用戶端 GPO 的安全性設定 51
 - 用戶端 GPO 的 RDP 設定 56
 - 用戶端 GPO 的一般設定 58
 - 用戶端 GPO 的 USB 設定 64
 - 用戶端 GPO 的 VMware Browser 重新導向設定 67
 - 用戶端 GPO 的 VMware Integrated Printing 設定 68
 - PCoIP 用戶端工作階段變數 ADMX 範本設定 68
 - 從命令列執行 Horizon Client 72
 - Horizon Client 命令使用 72
 - Horizon Client 組態檔 76
 - 使用 Windows 登錄設定 Horizon Client 77

- 4 管理遠端桌面平台和已發佈的應用程式連線 79**
 - 連線至遠端桌面平台或已發佈的應用程式 79
 - 使用未驗證存取連線至已發佈的應用程式 81
 - 共用位置資訊 83
 - 隱藏 VMware Horizon Client 視窗 84
 - 重新連線至遠端桌面平台或已發佈的應用程式 84
 - 在 Windows 用戶端桌面平台或開始功能表中建立捷徑 84
 - 使用伺服器所建立的捷徑 85
 - 設定開始功能表捷徑更新 85
 - 設定遠端桌面平台的自動連線功能 86
 - 登出或中斷連線 86
 - 從伺服器中斷連線 87

- 5 在遠端桌面平台或已發佈的應用程式中作業 88**
 - Windows 用戶端的功能支援 89

- 調整遠端桌面平台視窗的大小 90
- 監視器和螢幕解析度 90
 - 支援的多台監視器組態 90
 - 選取特定監視器來顯示遠端桌面平台 91
 - 在多台監視器設定中的單一監視器上顯示遠端桌面平台 92
 - 選取特定監視器來顯示已發佈的應用程式 93
 - 使用顯示調整 93
 - 使用 DPI 同步 94
 - 變更遠端桌面平台的顯示模式 96
 - 自訂遠端桌面平台的顯示解析度和顯示調整值 97
- 使用 USB 裝置 97
 - USB 重新導向限制 99
- 使用網路攝影機和麥克風 100
 - 將網路攝影機與即時音訊視訊功能搭配使用的時機 100
 - 在 Windows 用戶端系統上選取偏好的網路攝影機或麥克風 101
 - 搭配即時音訊視訊功能使用多個裝置 102
- 選取遠端桌面平台的慣用喇叭 102
- 共用遠端桌面平台工作階段 103
 - 邀請使用者加入遠端桌面平台工作階段 103
 - 管理共用遠端桌面平台工作階段 105
 - 加入遠端桌面平台工作階段 105
- 共用本機資料夾和磁碟機 106
- 在已發佈的應用程式中開啟本機檔案 109
- 複製與貼上 109
 - 複製與貼上文字和影像 110
 - 複製和貼上檔案及資料夾 111
 - 記錄複製和貼上活動 111
 - 設定用戶端剪貼簿記憶體大小 112
- 拖放 112
 - 拖曳文字和影像 112
 - 拖曳檔案和資料夾 113
 - 使用拖放功能的提示 113
- 已發佈應用程式的使用提示 114
 - 中斷連線之後重新連線至已發佈的應用程式 114
 - 從不同用戶端裝置使用已發佈應用程式的多重工作階段 115
 - 將本機 IME 與已發佈的應用程式搭配使用 116
- 從遠端桌面平台或已發佈的應用程式列印 117
 - 設定 VMware Integrated Printing 功能的列印喜好設定 117
 - 從遠端桌面平台列印至本機 USB 印表機 118
- 使用 URL 內容重新導向功能 118
- 改善遠端桌面平台中的滑鼠效能 119

[使用掃描器 120](#)

[重新導向序列埠 121](#)

[鍵盤快速鍵 122](#)

[鍵盤輸入方式語言同步 124](#)

[設定鎖定鍵同步 125](#)

6 疑難排解 Horizon Client 126

[重新啟動遠端桌面平台 126](#)

[重設遠端桌面平台或已發佈的應用程式 127](#)

[修復 Windows 版 Horizon Client 127](#)

[解除安裝 Windows 版 Horizon Client 128](#)

[鍵盤輸入的問題 129](#)

[Horizon Client 無預警結束時需要採取的動作 129](#)

[使用 Workspace ONE 模式連線至伺服器 130](#)

Windows 版 VMware Horizon Client 安裝和設定指南

本指南說明如何在 Microsoft Windows 用戶端系統上安裝、設定和使用 VMware Horizon[®] Client[™] 軟體。

本資訊適用於需要設定內含 Microsoft Windows 用戶端系統 (像是桌上型電腦與筆記型電腦) 之 Horizon 部署的管理員。這項資訊是針對具有經驗且熟悉虛擬機器技術和資料中心作業的系統管理員而撰寫的。

如果您是使用者，請參閱《Windows 版 VMware Horizon Client 使用者指南》文件或檢視 Windows 版 Horizon Client 線上說明。

Windows 用戶端的系統需求與設定

1

執行 Horizon Client 元件的系統必須滿足特定硬體和軟體需求。

連線至伺服器時，Windows 系統上的 Horizon Client 會使用 Microsoft Internet Explorer 網際網路設定，包括 Proxy 設定。請確定您的 Internet Explorer 設定正確無誤，且您可以透過 Internet Explorer 存取伺服器 URL。

本章節討論下列主題：

- [Windows 用戶端系統的系統需求](#)
- [Horizon Client 功能的系統需求](#)
- [搭配使用商務用 Skype 與 Horizon Client 的需求](#)
- [支援的桌面平台作業系統](#)
- [準備 Horizon Client 適用的連線伺服器](#)
- [清除用來登入伺服器的最後一個使用者名稱](#)
- [設定 VMware Blast 選項](#)
- [使用 Internet Explorer Proxy 設定](#)
- [設定 Horizon Client 資料共用](#)

Windows 用戶端系統的系統需求

您可以在使用支援的 Microsoft Windows 作業系統的 PC 和筆記型電腦上安裝 Windows 版 Horizon Client。

您安裝了 Horizon Client 的 PC 或筆記型電腦及其使用的週邊設備，必須符合某些系統需求。

型號

所有的 x86 或 x86-64 Windows 裝置

記憶體

最少 1 GB RAM

作業系統

Horizon Client 支援下列作業系統。

OS	版本	Service Pack 或服務選項	支援的版本
Windows 10	32 位元或 64 位元	版本 2009 SAC 版本 2004 SAC 版本 1909 SAC Enterprise 2019 LTSC Enterprise 2016 LTSC	家用版、專業版、工作站專業版、企業版、物聯網 (IoT) 企業版，以及教育版
Windows Server 2012 R2	64 位元	最新更新	Standard 和 Datacenter
Windows Server 2016	64 位元	最新更新	Standard 和 Datacenter
Windows Server 2019	64 位元	最新更新	Standard 和 Datacenter

Windows Server 2012 R2、Windows Server 2016 和 Windows Server 2019 支援在巢狀模式中執行 Horizon Client 的用途。如需在巢狀模式中所支援功能的相關資訊，請參閱 [VMware 知識庫 \(KB\) 文章 67248](#)。

重要 有時，會有在此文件發佈後才受支援的新 Windows 作業系統。如需最新的作業系統支援資訊，請參閱 [VMware 知識庫 \(KB\) 文章 58096](#)。

連線伺服器和 Horizon Agent

Horizon 7 (7.5 版) 及更新版本的最新維護版本。

如果用戶端系統從公司防火牆外部連線，請使用 Unified Access Gateway 應用裝置，如此，用戶端系統就不需要使用 VPN 連線。如果您的公司擁有內部無線網路，可用來路由存取裝置可使用的遠端桌面平台，則您不需要設定 Unified Access Gateway 或 VPN 連線。

顯示通訊協定

- PCoIP
- VMware Blast
- RDP

網路通訊協定

- IPv4
- IPv6

在自訂 Horizon Client 安裝期間，您可以啟用網際網路通訊協定的自動選取。如需詳細資訊，請參閱 [啟用自動網際網路通訊協定選取](#)。如需在 IPv6 環境中使用 Horizon 的相關資訊，請參閱《Horizon 安裝》文件。

PCoIP 和 VMware Blast 的硬體需求

- 支援 SSE2 擴展指令集的 x86 處理器，處理器速度為 800 MHz 或更快。

- 高於系統需求可用的 RAM，以支援各式監視器設定。請使用下列公式作為一般準則。

```
20MB + (24 * (# monitors) * (monitor width) * (monitor height))
```

一般而言，您可以使用下列計算方式。

```
1 monitor: 1600 x 1200: 64MB  
2 monitors: 1600 x 1200: 128MB  
3 monitors: 1600 x 1200: 256MB
```

RDP 的硬體需求

- 支援 SSE2 擴展指令集的 x86 處理器，處理器速度為 800 MHz 或更快。
- 128 MB RAM。

RDP 的軟體需求

- 若是 Windows 10，使用 RDP 10.0。
- 代理程式安裝程式會設定輸入 RDP 連線的本機防火牆規則，以符合主機作業系統目前的 RDP 連接埠，其通常是 3389。如果您變更 RDP 連接埠號碼，您必須變更相關聯的防火牆規則。

您可從 Microsoft 下載中心下載遠端桌面平台用戶端版本。

視訊和圖形需求

- 支援 Direct3D 11 Video 的圖形卡。
- 最新的視訊和圖形卡驅動程式。

.NET Framework 需求

Horizon Client 安裝程式需要 .NET Framework 4.5 版或更新版本。安裝程式會在安裝之前檢查是否已安裝 .NET Framework 4.5 版或更新版本。如果用戶端機器不符合此先決條件，則安裝程式會自動下載最新版的 .NET Framework。

Horizon Client 功能的系統需求

Horizon Client 功能具有特定硬體和軟體需求。

智慧卡驗證需求

使用智慧卡進行使用者驗證的用戶端裝置必須符合特定需求。

用戶端硬體和軟體需求

每個使用智慧卡進行使用者驗證的用戶端裝置，皆必須具備下列硬體和軟體。

- Horizon Client
- 相容的智慧卡讀卡機

Horizon Client 支援使用 PKCS#11 或 Microsoft CryptoAPI 提供者的智慧卡及智慧卡讀卡機。您可以選擇性地安裝 ActivIdentity ActivClient 軟體套件，其提供與智慧卡互動的工具。

■ 產品特定的應用程式驅動程式

使用智慧卡驗證的使用者必須具有智慧卡或 USB 智慧卡 Token，而每張智慧卡必須內含使用者憑證。

對於憑證發行範本中指定的密碼編譯服務提供者 (CSP)，請使用支援 RSA 搭配 SHA-256 演算法的 Microsoft 基礎智慧卡密碼編譯提供者或第三方智慧卡 CSP。

智慧卡註冊需求

若要在智慧卡上安裝憑證，管理員必須將電腦設定成註冊站。此電腦必須具有為使用者核發智慧卡憑證的權限，且必須是您為其核發憑證之網域的成員。

當您註冊智慧卡時，您可以選取所產生之憑證的金鑰大小。若要將智慧卡用於本機桌面平台，您必須在註冊智慧卡時選取 1024 位元或 2048 位元的金鑰大小。不支援具有 512 位元金鑰的憑證。

Microsoft TechNet 網站上可取得關於 Windows 系統規劃和實作智慧卡驗證的詳細資訊。

遠端桌面平台和已發佈的應用程式軟體需求

Horizon 管理員必須在虛擬桌面平台或 RDS 主機上安裝產品特定的應用程式驅動程式。

在 Horizon Client 中啟用使用者名稱提示文字方塊

在某些環境中，智慧卡使用者可使用單一智慧卡憑證向多個使用者帳戶進行驗證。使用者在使用智慧卡進行登入時，必須在**使用者名稱提示**文字方塊中輸入其使用者名稱。

若要讓**使用者名稱提示**文字方塊顯示在 Horizon Client 登入對話方塊中，您必須在連線伺服器中啟用智慧卡使用者名稱提示功能。如需啟用智慧卡使用者名稱提示功能的相關資訊，請參閱《Horizon 管理》文件。

如果您的環境使用 Unified Access Gateway 應用裝置進行外部安全存取，您必須將 Unified Access Gateway 應用裝置設定為支援智慧卡使用者名稱提示功能。智慧卡使用者名稱提示功能僅支援 Unified Access Gateway 2.7.2 及更新版本。如需在 Unified Access Gateway 中啟用智慧卡使用者名稱提示功能的相關資訊，請參閱《部署及設定 VMware Unified Access Gateway》文件。

即使在智慧卡使用者名稱提示功能啟用時，Horizon Client 仍繼續支援單一帳戶智慧卡憑證。

其他智慧卡驗證需求

除了符合 Horizon Client 系統的智慧卡需求之外，其他 Horizon 元件必須符合特定的組態需求，才能支援智慧卡。

連線伺服器和安全伺服器主機

管理員必須將所有受信任使用者憑證的所有適用憑證授權機構 (CA) 憑證鏈結新增至連線伺服器主機上 (或如果使用安全伺服器，則為安全伺服器主機上) 的伺服器信任存放區檔案。這些憑證鏈結包含根憑證，且若使用者的智慧卡憑證是由中繼憑證授權機構所核發，也必須包含中繼憑證。

如需設定連線伺服器以支援使用智慧卡的相關資訊，請參閱《Horizon 管理》文件。

Unified Access Gateway 應用裝置

如需在 Unified Access Gateway 應用裝置上設定智慧卡驗證的相關資訊，請參閱《部署及設定 VMware Unified Access Gateway》文件。

Active Directory

如需管理員可能需要在 Active Directory 中執行以實作智慧卡驗證的工作相關資訊，請參閱《Horizon 管理》文件。

用戶端裝置憑證驗證需求

使用用戶端裝置憑證驗證功能時，您可以為用戶端裝置設定憑證驗證。Unified Access Gateway 會驗證用戶端裝置。Microsoft 憑證服務與 Active Directory 可管理用戶端裝置的憑證建立和散發。裝置驗證成功後，使用者仍必須執行使用者驗證。

這項功能具有下列的需求。

- Unified Access Gateway 2.6 或更新版本
- Horizon 7 (7.5 版) 或更新版本
- 用戶端裝置上已安裝 Unified Access Gateway 會接受的憑證

如需如何設定 Unified Access Gateway 的相關資訊，請參閱 Unified Access Gateway 說明文件。

對於憑證發行範本中所指定的密碼編譯服務提供者 (CSP)，請使用 Microsoft 增強型 RSA 和 AES 密碼編譯提供者。此 CSP 可支援 SHA-256 憑證和 TLS v1.2。請使用 SHA-256。SHA-1 的強度太弱，不適合用於驗證。

若要讓 Windows 使用憑證來驗證用戶端裝置，該用戶端裝置上的使用者必須有權讀取憑證的私密金鑰。私密金鑰不需要為可匯出。憑證的金鑰使用方式必須包含數位簽章和金鑰編密 (a0)。

您可以將憑證安裝在用戶端裝置上的「目前使用者」或「本機電腦」憑證存放區。在 Windows 10 上，如果您將憑證安裝在「本機電腦」憑證存放區中，而且使用者不屬於「系統」或「本機管理員」使用者群組，則必須執行下列步驟來對使用者提供憑證私密金鑰讀取權限。如果您將憑證安裝在「目前使用者」憑證存放區，則不需要執行這些步驟。

- 1 開啟用戶端裝置上的「本機電腦」憑證存放區。
- 2 用滑鼠右鍵按一下裝置憑證，然後選取**所有工作 > 管理私密金鑰**。
- 3 新增使用者、對使用者指派讀取權限，然後按一下**確定**。

OPSWAT 整合需求

在某些公司中，管理員可能會將 Unified Access Gateway 與第三方 OPSWAT MetaAccess 應用程式整合。此整合通常用於公司自攜裝置 (BYOD) 環境中未受管理的裝置上，讓組織能夠定義 Horizon Client 裝置的裝置接受原則。

例如，管理員可能會定義一種裝置接受原則，要求用戶端裝置受到密碼保護或具有最低的作業系統版本。遵循裝置接受原則的用戶端裝置可透過 Unified Access Gateway 存取遠端桌面平台和已發佈的應用程式。Unified Access Gateway 會拒絕不符合裝置接受原則之用戶端裝置對遠端資源的存取。

如需詳細資訊，請參閱《部署及設定 VMware Unified Access Gateway》文件。

即時音訊視訊系統需求

即時音訊視訊功能可與標準網路攝影機、USB 音訊和類比音訊裝置搭配使用。此功能也可與標準會議應用程式搭配使用。若要支援即時音訊視訊，您的 Horizon 部署必須符合特定軟體和硬體需求。

虛擬桌面平台

若要在虛擬桌面平台中使用多個網路攝影機或麥克風，必須安裝 Horizon Agent 7.10 或更新版本。

將 Microsoft Teams 與即時音訊視訊搭配使用時，虛擬桌面平台至少要有 4 個 vCPU 和 4 GB 的 RAM。

Horizon Client 電腦或用戶端存取裝置

- 執行 Windows 版 Horizon Client 的所有作業系統上支援即時音訊視訊。如需相關資訊，請參閱 [Windows 用戶端系統的系統需求](#)。
- 必須安裝網路攝影機和音訊裝置驅動程式，且在用戶端電腦上網路攝影機和音訊裝置必須可使用。您不需在安裝代理程式的機器上安裝裝置驅動程式。

顯示通訊協定

- PCoIP
- VMware Blast

掃描器重新導向的系統需求

使用者可以使用連線到其本機用戶端系統的掃描器，將資訊掃描到其遠端桌面平台和應用程式上。若要使用此功能，遠端桌面平台和用戶端電腦必須符合特定系統需求。

遠端桌面平台

遠端桌面平台必須已安裝 Horizon Agent，並且在父系虛擬機器、範本虛擬機器或 RDS 主機上選取了 [掃描器重新導向] 安裝選項。在 Windows 桌面平台和 Windows Server 客體作業系統上，Horizon Agent [掃描器重新導向設定] 選項依預設為取消選取。

如需虛擬桌面平台和 RDS 主機支援哪些客體作業系統的相關資訊，以及在遠端桌面平台和已發佈的應用程式中設定掃描器重新導向的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中的〈設定掃描器重新導向〉。

Horizon Client 電腦或用戶端存取裝置

Windows 10 上支援掃描器重新導向。必須安裝掃描器裝置驅動程式，且在用戶端電腦上掃描器裝置必須可使用。無需在安裝代理程式的遠端桌面平台作業系統上安裝掃描器裝置驅動程式。

掃描裝置標準

TWAIN 或 WIA

顯示通訊協定

- PCoIP

- VMware Blast

RDP 桌面平台工作階段不支援掃描器重新導向。

序列埠重新導向的系統需求

透過序列埠重新導向功能，使用者可以將本機連接的序列 (COM) 埠 (例如內建 RS232 連接埠或 USB 轉序列介面卡) 重新導向至其遠端桌面平台和已發佈的應用程式。若要支援序列埠重新導向，您的 VMware Horizon 部署必須符合特定軟體和硬體需求。

虛擬桌面平台

必須安裝 Horizon Agent，並選取 [序列埠重新導向] 安裝選項。此安裝選項預設為取消選取狀態。

虛擬桌面平台支援下列作業系統。

- 32 位元或 64 位元的 Windows 7
- 32 位元或 64 位元的 Windows 8.x
- 32 位元或 64 位元的 Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

備註 Horizon Agent 2006 及更新版本不支援 Windows 7、Windows 8.x、Windows Server 2008 R2 和 Windows Server 2012 R2。

在虛擬桌面平台中不需要安裝序列埠裝置驅動程式。

已發佈的桌面平台和已發佈的應用程式

RDS 主機必須選取序列埠重新導向安裝選項，並安裝 Horizon Agent 7.6 或更新版本。此安裝選項預設為取消選取狀態。

已發佈的桌面平台和已發佈的應用程式支援下列作業系統。

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

備註 Horizon Agent 2006 及更新版本不支援 Windows Server 2008 R2 和 Windows Server 2012 R2。

在 RDS 主機中不需要安裝序列埠裝置驅動程式。

序列埠重新導向適用於完整桌面平台，RDS 主機上已發佈的應用程式不支援序列埠重新導向。

Horizon Client 電腦或用戶端存取裝置

Windows 10 用戶端系統上支援序列埠重新導向。必須安裝任何必要的序列埠裝置驅動程式，且序列埠必須可供使用。

顯示通訊協定

- PCoIP
- VMware Blast

RDP 桌面平台工作階段不支援序列埠重新導向。

如需設定序列埠重新導向的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中的〈設定序列埠重新導向〉。

使用 URL 內容重新導向的需求

透過 URL 內容重新導向功能，URL 內容將可從用戶端機器重新導向至遠端桌面平台或已發佈的應用程式 (用戶端至代理程式重新導向)，或從遠端桌面平台或已發佈的應用程式重新導向至用戶端機器 (代理程式至用戶端重新導向)。

例如，使用者可以按一下用戶端上的原生 Microsoft Word 應用程式中的連結，此時連結會在遠端 Internet Explorer 應用程式中開啟；或者，使用者可以按一下遠端 Internet Explorer 應用程式中的連結，讓連結在用戶端機器上的原生瀏覽器中開啟。您可以設定任意數量的通訊協定以進行重新導向，包括 HTTP、mailto 和 callto。

備註 使用 Chrome 瀏覽器的 URL 內容重新導向不支援 callto 通訊協定。

網頁瀏覽器

您可以在下列瀏覽器中輸入或按一下 URL，並讓該 URL 重新導向。

- Internet Explorer 9、10 和 11
- 64 位元或 32 位元 Chrome 60.0.3112.101，官方組建或更新版本
- Microsoft Edge 80.0.361.48 及更新版本 (官方組建)，64 位元或 32 位元 (Horizon Agent 2006 及更新版本)

URL 內容重新導向不適用於從 Windows 10 通用應用程式內部點按的連結，包含 Microsoft Edge 瀏覽器。

用戶端系統

您必須在安裝 Horizon Client 時啟用 URL 內容重新導向。您必須從命令列安裝 Horizon Client，才能啟用 URL 內容重新導向。如需相關資訊，請參閱[從命令列安裝 Horizon Client](#)。

若要透過 Chrome 或 Edge 瀏覽器使用 URL 內容重新導向，Horizon 管理員必須安裝並啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

第一次從 Chrome 瀏覽器重新導向 URL 時，系統會提示您在 Horizon Client 中開啟 URL。您必須按一下**開啟 URL: VMware Horizon Client 通訊協定**，才能執行 URL 內容重新導向。如果您選取**記住我對 URL: VMware Horizon Client 通訊協定連結的選擇**核取方塊，則不會再出現此提示。

遠端桌面平台或已發佈的應用程式

安裝 Horizon Agent 時，Horizon 管理員必須啟用 URL 內容重新導向。如需相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》和《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

若要透過 Chrome 瀏覽器使用 URL 內容重新導向，Horizon 管理員必須在 Windows 代理程式機器上安裝並啟用 VMware Horizon URL 內容重新導向 Helper 擴充功能。如需相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

Horizon 管理員還必須進行相關設定，以指定 Horizon Client 如何將 URL 內容從用戶端重新導向至遠端桌面平台或已發佈的應用程式，或指定 Horizon Agent 如何將 URL 內容從遠端桌面平台或已發佈的應用程式重新導向至用戶端。如需完整資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中的〈設定 URL 內容重新導向〉主題。

HTML5 多媒體重新導向的系統需求

Horizon Agent 和 Horizon Client 以及安裝代理程式與用戶端軟體的遠端桌面平台和用戶端系統都必須符合特定需求，才能支援 HTML5 多媒體重新導向功能。

使用 HTML5 多媒體重新導向時，如果使用者在遠端桌面平台中使用 Google Chrome 或 Microsoft Edge 瀏覽器，HTML5 多媒體內容將會傳送至用戶端系統。用戶端系統會播放多媒體內容，這可降低 ESXi 主機上的負載，且使用者會有更理想的音訊和視訊體驗。

遠端桌面平台

- 對於已選取 HTML5 多媒體重新導向自訂安裝選項的已發佈的桌面平台，必須在虛擬桌面平台或 RDS 主機上安裝 Horizon Agent。從 Horizon Agent 7.10 開始，HTML5 多媒體重新導向自訂安裝選項已移除，且依預設會安裝 HTML5 多媒體重新導向。如需詳細資訊，請參閱《在 Horizon 中設定虛擬桌面平台》和《在 Horizon 中設定已發佈的桌面平台和應用程式》文件中關於安裝 Horizon Agent 的主題。
- 必須在 Active Directory 伺服器上設定 HTML5 多媒體重新導向群組原則設定。請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於設定 HTML5 多媒體重新導向的主題。
- 必須安裝 Chrome 或 Edge 瀏覽器。
- 必須在 Chrome 或 Edge 瀏覽器中安裝 VMware Horizon HTML5 多媒體重新導向延伸。請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於設定 HTML5 多媒體重新導向的主題。

用戶端系統

- 安裝 Horizon Client 時，必須選取 [HTML5 多媒體重新導向和瀏覽器重新導向的支援] 自訂安裝選項。預設為選取此選項。

適用於遠端工作階段的顯示通訊協定

- PCoIP

- VMware Blast

TCP 連接埠

HTML5 多媒體重新導向會使用連接埠 9427。

限制

HTML5 多媒體重新導向功能有下列限制。

- 不支援 Horizon Client 相對滑鼠功能。
- 您無法使用靜音網站 (Chrome 瀏覽器) 或靜音索引標籤 (Edge 瀏覽器) 將重新導向的視訊內容靜音。

瀏覽器重新導向的系統需求

安裝代理程式與用戶端軟體的遠端桌面平台和用戶端系統都必須符合特定需求，才能支援瀏覽器重新導向功能。

使用瀏覽器重新導向時，如果使用者在遠端桌面平台中使用 Chrome 瀏覽器開啟網站，網頁將會呈現在用戶端系統上，而非代理程式系統上，且會透過遠端瀏覽器的檢視區來顯示。檢視區是瀏覽器視窗中包含網頁內容的部分。

遠端桌面平台

- 必須在虛擬桌面平台或在已發佈桌面平台的 RDS 主機上安裝 Horizon Agent 7.10 或更新版本。請參閱《在 Horizon 中設定虛擬桌面平台》和《在 Horizon 中設定已發佈的桌面平台和應用程式》文件中關於安裝 Horizon Agent 的主題。
- 必須在 Active Directory 伺服器上設定 VMware Browser 重新導向群組原則設定。請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於設定瀏覽器重新導向的主題。
- 必須安裝 Chrome 瀏覽器。
- 必須在 Chrome 瀏覽器中安裝 VMware Horizon 瀏覽器重新導向延伸。請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於設定瀏覽器重新導向的主題。

適用於遠端工作階段的顯示通訊協定

- PCoIP
- VMware Blast

多媒體重新導向 (MMR) 的系統需求

使用多媒體重新導向 (MMR) 時，系統會在用戶端系統上解碼多媒體串流。用戶端系統會播放媒體內容以減輕 ESXi 主機上的負載。

遠端桌面平台

如需作業系統需求和其他軟體需求以及組態設定的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於 Windows Media 多媒體重新導向的主題。

Horizon Client 電腦或用戶端存取裝置

Windows 10

支援的媒體格式

Windows Media Player 支援的媒體格式，例如：M4V；MOV；MP4；WMP；MPEG-4 Part 2；WMV 7、8 和 9；WMA；AVI；ACE；MP3；WAV。

使用 MMS 與 RTSP 時不支援 MP3。

備註 DRM 受保護的內容不會透過 Windows Media MMR 重新導向。

地理位置重新導向的系統需求

Horizon Agent 和 Horizon Client 以及安裝代理程式與用戶端軟體的虛擬桌面平台或 RDS 主機和用戶端機器都必須符合特定需求，才能支援地理位置重新導向功能。

透過地理位置重新導向功能，您可以將地理位置資訊從用戶端系統傳送至遠端桌面平台或已發佈的應用程式。

虛擬桌面平台或 RDS 主機

- 必須在設定 > 隱私權 > 位置中開啟 Windows 位置服務設定。
- 地理位置重新導向功能支援下列遠端桌面平台應用程式。

應用程式	平台
Google Chrome (最新版本)	所有虛擬桌面平台或 RDS 主機
Internet Explorer 11	所有虛擬桌面平台或 RDS 主機
Edge、Maps、Weather 以及其他 Win32 和 UWP 應用程式	Windows 10

必須在每個支援的瀏覽器中個別啟用位置權限設定 (如果有的話)。

- 必須在選取地理位置重新導向自訂安裝選項的情況下，安裝 Horizon Agent 7.6 或更新版本。此選項依預設為未選取狀態。請參閱《在 Horizon 中設定虛擬桌面平台》和《在 Horizon 中設定已發佈的桌面平台和應用程式》文件中關於安裝 Horizon Agent 的主題。
- 必須在 Active Directory 伺服器上設定 VMware 地理位置重新導向群組原則設定。請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於設定地理位置重新導向的主題。
- 針對 Internet Explorer 11，必須為 RDS 主機啟用 VMware Horizon 地理位置 IE 外掛程式。您不需要為 Windows 10 虛擬桌面平台啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。具有 VMware 地理位置重新導向驅動程式的 Windows 10 虛擬桌面平台可支援 Internet Explorer。請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於設定地理位置重新導向的主題。

- 針對 Chrome，必須啟用 VMware Horizon 地理位置重新導向 Chrome 外掛程式。請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於設定地理位置重新導向的主題。

用戶端系統

- 若要共用用戶端系統的位置資訊，您必須在 Horizon Client 中設定**地理位置**設定。如需相關資訊，請參閱[共用位置資訊](#)。
- 針對 Windows 10 用戶端系統，必須在**設定 > 隱私權 > 位置**中將 Windows **位置服務**設定為**開啟**，Horizon 才能存取您的所在位置。

適用於遠端工作階段的顯示通訊協定

- PCoIP
- VMware Blast

工作階段協作功能的需求

透過工作階段協作功能，使用者可以邀請其他使用者加入現有的遠端桌面平台工作階段。若要支援工作階段協作功能，您的 Horizon 部署必須符合特定需求。

工作階段協作者

若要加入協作工作階段，使用者必須已在用戶端系統上安裝 Windows、Mac 或 Linux 版 Horizon Client，或必須使用 HTML Access。

Windows 遠端桌面

必須在桌面平台集區或伺服器陣列層級上啟用工作階段協作功能。如需為桌面平台集區啟用工作階段協作功能的相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件。如需為伺服器陣列啟用工作階段協作功能的相關資訊，請參閱《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

您可以使用 Horizon Agent 群組原則設定來設定工作階段協作功能。如需相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

Linux 遠端桌面平台

如需 Linux 遠端桌面平台需求，請參閱《在 Horizon 中設定 Linux 桌面平台》文件。

連線伺服器

若要使用工作階段協作功能，連線伺服器執行個體就必須使用 Enterprise 授權。

顯示通訊協定

VMware Blast

工作階段協作功能不支援已發佈的應用程式工作階段。

搭配使用商務用 Skype 與 Horizon Client 的需求

使用者可以在虛擬桌面平台內執行商務用 Skype，而不會對虛擬基礎結構造成負面影響以及使網路超載。在 Skype 音訊和視訊通話期間，所有媒體處理都會在用戶端機器上執行，而非使用虛擬桌面平台。

若要使用此功能，您必須在安裝 Windows 版 Horizon Client 時，在用戶端機器上安裝「商務用 Skype 的虛擬化套件」功能。如需相關資訊，請參閱第 2 章 [安裝 Windows 版 Horizon Client](#)。

Horizon 管理員也必須在 Horizon Agent 安裝時，在虛擬桌面平台上安裝「商務用 Skype 的 VMware 虛擬化套件」功能。如需安裝 Horizon Agent 的相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件。

如需完整需求，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中的〈設定商務用 Skype〉。

支援的桌面平台作業系統

Horizon 管理員會建立具有客體作業系統的虛擬機器，並在客體作業系統中安裝代理程式軟體。使用者可從用戶端裝置登入至這些虛擬機器。

如需支援的 Windows 客體作業系統清單，請參閱《Horizon 安裝》文件。

也支援某些 Linux 客體作業系統。如需系統需求、設定 Linux 虛擬機器以及支援功能清單的相關資訊，請參閱《在 Horizon 中設定 Linux 桌面平台》文件。

準備 Horizon Client 適用的連線伺服器

Horizon 管理員必須設定特定的連線伺服器設定，使用者才能連線至伺服器並存取遠端桌面平台或已發佈的應用程式。

Unified Access Gateway 和安全伺服器

如果您的 VMware Horizon 部署包含 Unified Access Gateway 應用裝置，請設定連線伺服器，使其與 Unified Access Gateway 搭配運作。請參閱《部署及設定 VMware Unified Access Gateway》文件。Unified Access Gateway 應用裝置會執行相同角色作為安全伺服器。

如果您的 VMware Horizon 部署包含安全伺服器，請確認您使用連線伺服器 7.5 和安全伺服器 7.5 或更新版本的最新維護版本。如需詳細資訊，請參閱您 Horizon 版本適用的安裝文件。

備註 VMware Horizon 2006 及更新版本中不支援安全伺服器。

安全通道連線

如果您想要對用戶端裝置使用安全通道連線，而安全連線是以連線伺服器執行個體或安全伺服器的 DNS 主機名稱所設定，請確認用戶端裝置可解析此 DNS 名稱。

桌面平台和應用程式集區

設定桌面平台和應用程式集區時，請使用下列檢查清單。

- 確認是否已建立桌面平台或應用程式集區，以及您計畫使用的使用者帳戶有權存取集區。如需詳細資訊，請參閱《在 Horizon 中設定虛擬桌面平台》和《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

- 如果使用者擁有高解析度顯示器，並在以全螢幕模式檢視遠端桌面平台時，使用**高解析度模式**用戶端設定，請確認您為每個 Windows 遠端桌面平台都配置了足夠的 vRAM。vRAM 的數量取決於顯示解析度，以及為使用者設定的監視器數目。

使用者驗證

設定使用者驗證時，請使用下列檢查清單。

- 若要在 Horizon Client 中為使用者提供已發佈應用程式的未驗證存取，您必須在連線伺服器執行個體中啟用此功能。如需詳細資訊，請參閱《Horizon 管理》文件中關於未驗證存取的主題。
- 若要搭配 Horizon Client 使用雙因素驗證 (例如 RSA SecurID 或 RADIUS 驗證)，您必須為連線伺服器執行個體啟用雙因素驗證功能。從 Horizon 7 (7.11 版) 開始，您可以自訂 RADIUS 驗證登入頁面上的標籤。從 Horizon 7 (7.12 版) 開始，您可以將雙因素驗證設定為在遠端工作階段逾時之後發生。如需詳細資訊，請參閱《Horizon 管理》文件中關於雙因素驗證的主題。
- 針對使用者在 Horizon Client 的**選項**功能表中選取**以目前使用者身分登入**時所傳遞的使用者身分識別和認證資訊，若要允許連線伺服器執行個體接受這些資訊，請為連線伺服器執行個體啟用**接受以目前使用者身分登入**設定。此設定可在 Horizon 7 (7.8 版) 及更新版本中使用。如需詳細資訊，請參閱《Horizon 管理》文件。

您可以使用 Horizon Client 群組原則設定來設定「以目前使用者身分登入」功能，包括指定可接受「以目前使用者身分登入」驗證資訊的連線伺服器執行個體清單。如需這些用戶端設定的相關資訊，請參閱**用戶端 GPO 的安全性設定**。

- 若要在 Horizon Client 中隱藏伺服器 URL，請啟用**在用戶端使用者介面中隱藏伺服器資訊**全域設定。如需詳細資訊，請參閱《Horizon 管理》文件。
- 若要在 Horizon Client 中隱藏**網域**下拉式功能表，請啟用**在用戶端使用者介面中隱藏網域清單**全域設定。從 Horizon 7 (7.8 版) 開始，此設定依預設為啟用。如需詳細資訊，請參閱《Horizon 管理》文件。
- 若要將網域清單傳送至 Horizon Client，請啟用 Horizon Console 中的**傳送網域清單**全域設定。此設定可在 Horizon 7 (7.8 版) 及更新版本中使用，且依預設為停用。舊版的 Horizon 7 會傳送網域清單。如需詳細資訊，請參閱《Horizon 管理》文件。

下表顯示**傳送網域清單**和**在用戶端使用者介面中隱藏網域清單**全域設定如何決定使用者可用來登入伺服器的方式。

傳送網域清單設定	在用戶端使用者介面中隱藏網域清單設定	使用者登入方式
已停用 (預設值)	已啟用	<p>網域下拉式功能表已隱藏。使用者必須在使用者名稱文字方塊中輸入下列其中一個值。</p> <ul style="list-style-type: none"> ■ 使用者名稱 (不允許使用多個網域) ■ <i>domain\username</i> ■ <i>username@domain.com</i>
已停用 (預設值)	已停用	<p>如果在用戶端上設定了預設網域，則網域下拉式功能表中會出現該預設網域。如果用戶端無法識別預設網域，則網域下拉式功能表中會出現 *DefaultDomain*。使用者必須在使用者名稱文字方塊中輸入下列其中一個值。</p> <ul style="list-style-type: none"> ■ 使用者名稱 (不允許使用多個網域) ■ <i>domain\username</i> ■ <i>username@domain.com</i>
已啟用	已啟用	<p>網域下拉式功能表已隱藏。使用者必須在使用者名稱文字方塊中輸入下列其中一個值。</p> <ul style="list-style-type: none"> ■ 使用者名稱 (不允許使用多個網域) ■ <i>domain\username</i> ■ <i>username@domain.com</i>
已啟用	已停用	<p>使用者可以在使用者名稱文字方塊中輸入使用者名稱，然後從網域下拉式功能表中選取網域。或者，使用者也可以在使用者名稱文字方塊中輸入下列其中一個值。</p> <ul style="list-style-type: none"> ■ <i>domain\username</i> ■ <i>username@domain.com</i>

清除用來登入伺服器的最後一個使用者名稱

當使用者登入啟用了在用戶端使用者介面中隱藏網域清單全域設定的連線伺服器執行個體時，Horizon Client 中的網域下拉式功能表會是隱藏的，使用者必須在 Horizon Client 的**使用者名稱**文字方塊中提供網域資訊。例如，使用者必須以 *domain\username* 或 *username@domain* 的格式輸入其使用者名稱。

在 Windows 用戶端系統上，系統會使用一個登錄機碼來決定是否儲存最後一個使用者名稱，並在使用者下次登入至伺服器時將該名稱顯示於**使用者名稱**文字方塊中。若不要讓最後一個使用者名稱顯示於**使用者名稱**文字方塊中及公開網域資訊，您必須在 Windows 用戶端系統上，將 HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername 登錄機碼的值設為 1。

如需在 Horizon Client 中隱藏安全資訊 (包括網域下拉式功能表和伺服器 URL 資訊) 的相關資訊，請參閱《Horizon 管理》文件中關於全域設定的主題。

設定 VMware Blast 選項

您可以針對使用 VMware Blast 顯示通訊協定的遠端桌面平台和已發佈應用程式工作階段，設定 VMware Blast 選項。

您可以允許 H.264 解碼和高效率視訊編碼 (HEVC)。H.264 是視訊壓縮的產業標準，而視訊壓縮是將數位視訊轉換為在儲存或傳輸時佔用較少容量的格式的程序。在允許 H.264 解碼後，您也可以允許更高的色彩逼真度。

支援的最高解析度以及是否支援 HEVC，取決於用戶端上圖形處理器 (GPU) 的能力。支援 JPEG/PNG 4K 解析度的 GPU，可能不支援 H.264 的 4K 解析度。若不支援 H.264 的解析度，則 Horizon Client 會改用 JPEG/PNG。

如果您的環境使用 Proxy 伺服器，您可以指定是否允許 VMware Blast 連線使用作業系統 Proxy 伺服器。

對於 SSL Proxy 伺服器，您還必須為透過 SSL Proxy 伺服器進行的次要連線設定憑證檢查。如需詳細資訊，請參閱在 [Horizon Client 中設定憑證檢查模式](#)。

您可以在連線至伺服器之前或之後設定 VMware Blast 選項。

必要條件

若要使用高效率視訊編碼 (HEVC)，您必須安裝 Horizon Agent 7.7 或更新版本。若要使用 YUV 4:4:4 提升色彩準確度，您必須安裝 Horizon Agent 7.11 或更新版本。此外，用戶端系統必須具有支援 HEVC 解碼的 GPU。

用戶端的允許 **Blast 連線使用作業系統 Proxy 設定** 群組原則設定可決定 VMware Blast 連線是否可透過 Proxy 伺服器進行連線，以及使用者是否可在 Horizon Client 使用者介面中變更 VMware Blast Proxy 伺服器設定。如需詳細資訊，請參閱 [用戶端 GPO 的一般設定](#)。

根據安裝的 Horizon Agent 版本，Horizon 管理員可使用代理程式端群組原則設定來啟用或停用 VMware Blast 功能，包括 H.264 和 HEVC 高色彩準確度。如需相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中的「VMware Blast 原則設定」。

程序

- 1 啟動 Horizon Client。
- 2 按一下功能表列右上角的**選項**按鈕，然後選取**設定 VMware Blast**。

如果您已登入伺服器，則可以按一下桌面平台和應用程式選取視窗右上角的**設定** (齒輪) 圖示，然後選取 **VMware Blast**。

- 3 若要在 Horizon Client 中允許 H.264 解碼，請選取**允許 H.264 解碼**核取方塊。

選取此選項時 (預設設定)，若代理程式支援 H.264 軟體或硬體編碼，則 Horizon Client 會使用 H.264 解碼。如果代理程式不支援 H.264 軟體或硬體編碼，則 Horizon Client 會使用 JPG/PNG 解碼 (搭配 Horizon Agent 7.x) 或 Blast 轉碼器解碼 (搭配 Horizon Agent 2006 及更新版本)。取消選取此選項時，Horizon Client 會使用 JPG/PNG 解碼 (搭配 Horizon Agent 7.x) 或 Blast 轉碼器解碼 (搭配 Horizon Agent 2006 及更新版本)。

- 4 若要在 Horizon Client 允許 H.264 解碼時允許更高的色彩逼真度，請選取**允許高色彩準確度 (會縮短電池壽命並降低效能)**核取方塊。

選取此選項時，Horizon Client 會使用高色彩精確度，但僅限於代理程式支援高色彩精確度時。選取此選項可能會降低電池壽命與效能。此功能依預設為停用。

- 5 若要允許 HEVC，請選取**允許高效率視訊解碼 (HEVC)** 核取方塊。

選取此選項時，如果用戶端電腦配備支援 HEVC 解碼的 GPU，則效能和影像畫質都會得到提升。此功能依預設為停用。

如果選取了此選項，用戶端機器卻沒有支援 HEVC 解碼的 GPU，則 Horizon Client 會改為使用 H.264 解碼。

- 6 若要允許透過 Proxy 伺服器進行 VMware Blast 連線，請選取**允許 Blast 連線使用作業系統 Proxy 設定**核取方塊。
- 7 按一下**確定**儲存變更。

結果

當下一次使用者連線至遠端桌面平台或已發佈的應用程式，並選取 VMware Blast 顯示通訊協定時，變更就會生效。您的變更不會影響現有的 VMware Blast 工作階段。

使用 Internet Explorer Proxy 設定

Horizon Client 會使用 Internet Explorer 中設定的 Proxy 設定。

略過 Proxy 設定

Horizon Client 會使用 Internet Explorer Proxy 略過設定來略過連線伺服器主機、安全伺服器或 Unified Access Gateway 應用裝置的 HTTPS 連線。

如果在連線伺服器主機、安全伺服器或 Unified Access Gateway 應用裝置上啟用了安全通道，則必須使用 Horizon Client 組態 ADM 或 ADMX 範本檔中的通道 Proxy 略過位址清單群組原則設定來指定要略過通道連線的位址清單。Proxy 伺服器不會用於這些位址。請使用分號 (;) 分隔多個項目。此群組原則設定會建立下列登錄機碼：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

您無法將此群組原則設定用於直接連線。如果套用群組原則設定的效用不如預期，請嘗試略過本機位址的 Proxy。如需詳細資訊，請參閱 <https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/>。

Proxy 容錯移轉

Horizon Client 支援在 Internet Explorer 的**網際網路選項 > 連線 > LAN 設定**中，透過**自動設定**下方的**使用自動組態指令碼**設定進行 Proxy 容錯移轉。若要使用此設定，您必須建立可傳回多個 Proxy 伺服器的自動組態指令碼。

設定 Horizon Client 資料共用

如果 Horizon 管理員已選擇參與 VMware 客戶經驗改進計劃 (CEIP)，則 VMware 會透過連線伺服器從用戶端系統收集並接收匿名資料。您可以設定是否要與連線伺服器共用此用戶端資料。

如需設定 Horizon 以加入 CEIP 的相關資訊，請參閱《Horizon 管理》文件。

在 Horizon Client 中，資料共用依預設為啟用。您必須設定資料共用設定，之後才能連線至伺服器。此設定會套用至所有伺服器。連線至伺服器後，您無法變更 Horizon Client 資料共用設定。

您可以使用**允許資料共用**群組原則設定來啟用或停用資料共用，以及防止使用者變更 Horizon Client 中的設定。如需詳細資訊，請參閱[用戶端 GPO 的一般設定](#)。

程序

- 1 按一下功能表列右上角的**選項**按鈕，然後選取**允許資料共用**。
- 2 將資料共用模式設定為**開啟**或**關閉**，然後按一下**確定**。

由 VMware 收集的 Horizon Client 資料

如果 Horizon 管理員已選擇參與客戶經驗改進計劃，且已在用戶端系統上啟用資料共用，則 VMware 會收集用戶端系統的相關資料。

VMware 會收集用戶端系統的相關資料，以排定硬體和軟體相容性的優先處理順序。如果 Horizon 管理員選擇參與客戶經驗改進計劃，則 VMware 會收集與您的部署有關的匿名資料，以更能回應客戶的需求。VMware 不會收集可識別您組織的資料。Horizon Client 資訊會連同連線伺服器、桌面平台集區及遠端桌面平台的資料先一併傳送至連線伺服器執行個體，然後再傳送至 VMware。

資訊在傳送至連線伺服器執行個體時會進行加密。用戶端系統上的資訊會未經加密即記錄在使用者特定的目錄中。這些記錄檔並不包含個人識別資訊。

Horizon 管理員可在安裝連線伺服器時選擇是否要參與 VMware 客戶經驗改進計劃，或可於安裝後在 Horizon Console 中設定選項。

表 1-1. 從 Horizon Client 收集的資訊，供客戶體驗改善計畫使用

說明	此欄位會採用匿名形式嗎?
製作 Horizon Client 應用程式的公司	否
產品名稱	否
用戶端產品版本	否
用戶端二進位架構	否
用戶端版本編號	否
主機作業系統	否
主機作業系統核心	否
主機作業系統架構	否
主機系統型號	否
主機系統 CPU	否
主機系統處理器的核心數量	否
主機系統的記憶體 (MB)	否
連線的 USB 裝置數目	否
並行 USB 裝置連線上限	否
USB 裝置廠商識別碼	否

表 1-1. 從 Horizon Client 收集的資訊，供客戶體驗改善計畫使用 (續)

說明	此欄位會採用匿名形式嗎?
USB 裝置產品識別碼	否
USB 裝置系列	否
USB 裝置使用計數	否

安裝 Windows 版 Horizon Client

2

您可以從 VMware 網站或由連線伺服器提供的網頁存取頁面，取得 Windows Horizon Client 安裝程式。安裝 Horizon Client 後，可為使用者設定各種啟動選項。

本章節討論下列主題：

- 在 Windows 用戶端作業系統中啟用 FIPS 模式
- 啟用自動網際網路通訊協定選取
- 安裝 Windows 版 Horizon Client
- 從命令列安裝 Horizon Client
- 確認 URL 內容重新導向安裝
- 線上更新 Horizon Client

在 Windows 用戶端作業系統中啟用 FIPS 模式

如果您計劃安裝 Horizon Client 搭配聯邦資訊處理標準 (FIPS) 相容密碼編譯，則在執行 Horizon Client 安裝程式前，您必須先在用戶端作業系統中啟用 FIPS 模式。

在用戶端作業系統中啟用 FIPS 模式時，應用程式只會使用與 FIPS-140 相容並符合 FIPS 核准作業模式的密碼編譯演算法。您可以在 [本機安全性原則] 或 [群組原則] 中啟用特定的安全性設定，或是透過編輯 Windows 登錄機碼來啟用 FIPS 模式。

如需關於 FIPS 相容性的詳細資訊，請參閱《Horizon 安裝》文件。

設定 FIPS 組態屬性

若要在用戶端作業系統中啟用 FIPS 模式，您可以使用用戶端電腦的 Windows 群組原則設定或 Windows 登錄設定。

- 若要使用群組原則設定，請開啟群組原則編輯器，導覽至電腦設定\Windows 設定\安全性設定\本機原則\安全性選項，並啟用**系統加密編譯: 使用 FIPS 相容演算法於加密, 雜湊, 以及簽章**設定。
- 若要使用 Windows 登錄，請前往 HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled，並將 **Enabled** 設為 1。

如需 FIPS 模式的詳細資訊，請前往 <https://support.microsoft.com/en-us/kb/811833>。

重要 如果並未在執行 Horizon Client 安裝程式之前啟用 FIPS 模式，在自訂安裝期間即不會顯示使用 FIPS 相容密碼編譯的安裝程式選項。在一般安裝期間不會啟用 FIPS 相容密碼編譯。如果安裝 Horizon Client 時未搭配 FIPS 相容密碼編譯選項，而稍後決定要使用此選項，則您必須解除安裝用戶端、在用戶端作業系統中啟用 FIPS 模式，然後再次執行 Horizon Client 安裝程式。

啟用自動網際網路通訊協定選取

當您執行 Horizon Client 的自訂安裝時，可以啟用網際網路通訊協定的自動選取。使用自動選取時，Horizon Client 會檢查目前的網路，並透過 IPv4 或 IPv6 自動連線。

啟用自動選取時，Unified Access Gateway (3.3 版) 及更新版本支援搭配 VMware Blast 顯示通訊協定使用下列功能。

- 以目前使用者身分登入
- 音訊輸出
- 客戶經驗改進計劃資料收集
- 虛擬列印
- VMware Integrated Printing (需要 Horizon 7 (7.7 版) 或更新版本)
- HTML5 多媒體重新導向
- VMware 視訊
- USB 重新導向
- 即時音訊視訊 (RTAV)

安裝 Windows 版 Horizon Client

您可以執行 Windows 安裝程式檔案來安裝所有的 Horizon Client 元件。

此程序描述如何利用互動式安裝精靈來安裝 Horizon Client。若要從命令列安裝 Horizon Client，請參閱 [從命令列安裝 Horizon Client](#)。若要安裝 URL 內容重新導向功能，您必須從命令列執行安裝程式。

備註 您可以在遠端桌面平台虛擬機器中安裝 Horizon Client。如果公司的使用者透過 Windows 精簡型用戶端裝置存取已發佈的應用程式，則公司可以使用此安裝策略。

必要條件

- 確認用戶端系統使用支援的作業系統。請參閱 [Windows 用戶端系統的系統需求](#)。
- 確認您有包含 Horizon Client 安裝程式的下載頁 URL。此 URL 可能是在 <http://www.vmware.com/go/viewclients> 的 VMware 下載頁，或是連線伺服器執行個體的 URL。
- 確認您能以管理員身分登入用戶端系統。
- 確認網域控制站有最新的修補程式、有足夠的可用磁碟空間和可相互連接。

- 如果您想要以 FIPS 相容密碼編譯安裝 Horizon Client，請在用戶端作業系統中啟用 FIPS 模式。請參閱在 [Windows 用戶端作業系統中啟用 FIPS 模式](#)。
- 如果您打算選取 IPv6 通訊協定或自動網際網路通訊協定選取，請參閱《Horizon 安裝》文件以取得 IPv6 環境中功能無法使用的相關資訊。
- 如果您打算啟用自動網際網路通訊協定選取，請參閱[啟用自動網際網路通訊協定選取](#)以取得所支援功能的相關資訊。
- 如果您想要安裝 **USB 重新導向**元件，請執行下列工作：
 - 決定用戶端裝置的使用者是否可從遠端桌面平台存取本機連線的 USB 裝置。如果不允許存取，則請勿安裝 **USB 重新導向**元件，或是安裝該元件但使用群組原則設定將其停用。如果您使用群組原則來停用 USB 重新導向，但日後決定要為用戶端啟用 USB 重新導向時，您將不需要重新安裝 Horizon Client。如需詳細資訊，請參閱 [用戶端 GPO 的指令碼定義設定](#)。
 - 確認用戶端電腦上的 Windows 自動更新功能並未關閉。
- 決定是否使用此功能讓使用者以目前登入的使用者身分，登入 Horizon Client 及其遠端桌面平台。使用者登入用戶端系統時輸入的認證資訊會傳遞至連線伺服器執行個體，並最終傳遞至遠端桌面平台。一些用戶端作業系統並不支援此功能。
- 如果您不想要讓使用者必須提供連線伺服器執行個體的完整網域名稱 (FQDN)，請決定 FQDN，以便您在安裝期間加以提供。

程序

- 1 以管理員身分登入用戶端系統。
- 2 導覽至位於 <http://www.vmware.com/go/viewclients> 的 VMware 下載頁面。
- 3 下載安裝程式檔案，例如，VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe。
YYMM 是行銷版本號碼，y.y.y 是內部版本號碼，而 xxxxxx 是組建編號。
- 4 按兩下安裝程式檔案以開始安裝。

5 選取安裝類型並遵循提示。

選項	動作
一般安裝	<p>按一下同意並安裝。安裝程式會將用戶端設定為使用 IPv4 網際網路通訊協定，並安裝下列功能：</p> <ul style="list-style-type: none"> ■ USB 重新導向 ■ 以目前使用者的身分登入，包括顯示以目前使用者身分登入功能表選項。 ■ 商務用 Skype 的虛擬化套件 ■ HTML5 多媒體重新導向和瀏覽器重新導向的支援 ■ Microsoft Teams 的媒體最佳化
自訂安裝	<p>按一下自訂安裝，然後選取要安裝的功能。</p> <p>您必須選取此選項，以指定下列功能：</p> <ul style="list-style-type: none"> ■ 指定非預設安裝位置。 ■ 使用 IPv6 網際網路通訊協定。 ■ 啟用網際網路通訊協定的自動選取功能。Horizon Client 會檢查目前的網路，並透過 IPv4 或 IPv6 自動連線。 ■ 設定預設連線伺服器執行個體。 ■ 將預設登入行為設定為以目前使用者身分登入。 ■ 啟用 FIPS 相容密碼編譯。必須在用戶端作業系統上啟用 FIPS 模式，安裝程式中才會有 FIPS 相容密碼編譯自訂安裝選項可供使用。 ■ 在 64 位元機器上安裝 32 位元 Core Remote Experience 元件。 <p>備註 如果 64 位元用戶端機器上沒有產品的 64 位元外掛程式，則會安裝 32 位元 Core Remote Experience 元件。32 位元 Core Remote Experience 元件不支援 Microsoft Teams 的媒體最佳化功能。</p>

結果

某些功能必須在重新啟動用戶端系統後才會生效。

安裝程式會安裝 Windows 服務，包括 VMware Horizon Client (`horizon_client_service`) 和 VMware USB Arbitration Service (`VMUSBArbService`)。

後續步驟

啟動 Horizon Client，並確認您可以登入正確的遠端桌面平台或已發佈的應用程式。請參閱[連線至遠端桌面平台或已發佈的應用程式](#)。

從命令列安裝 Horizon Client

您可以在命令列中輸入安裝程式檔案名稱、安裝命令和安裝內容，藉以安裝 Horizon Client。

從命令列安裝 Horizon Client 時，您可以執行無訊息安裝。透過無訊息安裝，您可以在大型企業中有效率地部署 Horizon Client。

Horizon Client 的安裝命令

從命令列安裝 Horizon Client 時，您可以指定特定安裝命令。

下表說明 Horizon Client 安裝命令。

表 2-1. Horizon Client 安裝命令

命令	說明
<code>/?</code> 或 <code>/help</code>	列出 Horizon Client 安裝命令和內容。
<code>/silent</code>	以無訊息方式安裝 Horizon Client。您無須回應精靈提示。
<code>/install</code>	以互動方式安裝 Horizon Client。您必須回應精靈提示。
<code>/uninstall</code>	解除安裝 Horizon Client。
<code>/repair</code>	修復 Horizon Client。
<code>/norestart</code>	在安裝程序期間隱藏所有的重新啟動動作和重新啟動提示。
<code>/x /extract</code>	將安裝程式套件解壓縮至 %TEMP% 目錄。
<code>/l</code> 或 <code>/log</code>	指定用來安裝記錄檔的資料夾和命名模式。 例如，如果您指定下列命令，則 Horizon Client 安裝程式將會在名為 C:\Temp 的資料夾中建立具有前置詞 Test 的記錄檔。 <code>/log "C:\Temp\Test"</code>

Horizon Client 的安裝內容

從命令列安裝 Horizon Client 時，您可以指定特定安裝內容。

下表說明 Horizon Client 安裝內容。

表 2-2. Horizon Client 安裝內容

內容	說明	預設值
INSTALLDIR	Horizon Client 安裝所在的路徑和資料夾。例如： <code>INSTALLDIR=""D:\abc\my folder""</code> 括住路徑的雙引號組合，可讓安裝程式將空格轉譯為路徑的有效部分。	%ProgramFiles%\VMware \VMware Horizon View Client
VDM_IP_PROTOCOL_USAGE	Horizon Client 元件用於通訊的 IP (網際網路通訊協定) 版本。有效值如下： <ul style="list-style-type: none"> ■ IPv4 ■ IPv6 ■ Dual 如果您指定 Dual，Horizon Client 將會檢查目前的網路，並透過 IPv4 或 IPv6 自動連線。	IPv4

表 2-2. Horizon Client 安裝內容 (續)

內容	說明	預設值
VDM_FIPS_ENABLED	<p>決定是否要以 FIPS 相容密碼編譯來安裝 Horizon Client。</p> <p>值為 1 時，會安裝 Horizon Client 和 FIPS 相容密碼編譯。值為 0 時，則會安裝 Horizon Client，而不安裝 FIPS 相容密碼編譯。</p> <p>備註 在將此內容設為 1 之前，您必須先在 Windows 用戶端作業系統中啟用 FIPS 模式。請參閱在 Windows 用戶端作業系統中啟用 FIPS 模式。</p>	0
VDM_SERVER	<p>Horizon Client 使用者依預設連線的連線伺服器執行個體的完整網域名稱 (FQDN)。例如： VDM_Server=cs1.companydomain.com</p> <p>如果設定此屬性，Horizon Client 使用者即無須提供此 FQDN。</p>	無
LOGINASCURRENTUSER_DISPLAY	<p>決定以目前使用者身分登入是否會出現在 Horizon Client 功能表列的選項功能表中。有效值為 1 (啟用) 或 0 (停用)。</p>	1
LOGINASCURRENTUSER_DEFAULT	<p>決定依預設是否會在 Horizon Client 功能表列的選項功能表中選取以目前使用者身分登入。有效值為 1 (啟用) 和 0 (停用)。</p> <p>以目前使用者身分登入是預設登入行為時，使用者登入用戶端系統時所提供的身份識別和認證資訊都會傳遞至連線伺服器執行個體，且最終會傳遞至遠端桌面平台。如果以目前使用者身分登入不是預設登入行為，則使用者必須多次提供身份識別和認證資訊，才能存取遠端桌面平台或應用程式。</p>	0
ADDLOCAL	<p>指定要安裝的功能。有效值如下：</p> <ul style="list-style-type: none"> ■ ALL - 安裝所有可用功能，URL 內容重新導向除外。 ■ TSSO - 安裝「以目前使用者身分登入」功能。 ■ USB - 安裝 USB 重新導向功能。 <p>若要指定個別功能，請輸入以逗號分隔的功能名稱清單。不要在名稱間使用空格。</p> <p>例如，若要安裝附有 USB 重新導向功能、但沒有「以目前使用者身分登入」功能的 Horizon Client，請輸入下列命令：</p> <pre>VMware-Horizon-Client-y.y.y-xxxxxx.exe ADDLOCAL=USB</pre>	無

表 2-2. Horizon Client 安裝內容 (續)

內容	說明	預設值
INSTALL_32BITRMKS	<p>在 64 位元用戶端機器上，指定是否要安裝 32 位元 Core Remote Experience 元件。值為 1 時，會安裝 32 位元 Core Remote Experience 元件。值為 0 時，將會安裝 64 位元 Core Remote Experience 元件。</p> <p>如果 64 位元用戶端機器上沒有產品的 64 位元外掛程式，則會安裝 32 位元 Core Remote Experience 元件。</p> <p>此內容在 32 位元用戶端機器上無效。</p>	0
INSTALL_SFB	<p>決定是否安裝「商務用 Skype 的 VMware 虛擬化套件」功能。值為 1 時，系統會安裝功能。值為 0 時，則不會安裝此功能。</p>	1
INSTALL_HTML5MMR	<p>確定是否已安裝「HTML5 多媒體重新導向和瀏覽器重新導向的支援」功能。值為 1 時，系統會安裝功能。值為 0 時，則不會安裝此功能。</p>	1
REMOVE	<p>指定不要安裝的功能。有效值如下：</p> <ul style="list-style-type: none"> ■ ThinPrint - 不安裝虛擬列印功能。 ■ Scanner - 不安裝掃描器重新導向功能。 ■ FolderRedirection - 不安裝資料夾重新導向功能。 ■ SerialPort - 不安裝序列埠重新導向功能。 <p>若要指定多個功能，請輸入以逗號分隔的功能名稱清單。不要在名稱間使用空格。</p> <p>例如，下列命令不會安裝虛擬列印和掃描器重新導向功能：</p> <pre>VMware-Horizon-Client-y.y.y-xxxxxx.exe REMOVE=ThinPrint,Scanner</pre>	無
DESKTOP_SHORTCUT	<p>決定是否為 Horizon Client 建立桌面平台捷徑。值為 0 時，系統不會建立桌面平台捷徑。值為 1 時，系統會建立桌面平台捷徑。</p>	1
STARTMENU_SHORTCUT	<p>決定是否為 Horizon Client 建立 [開始] 功能表捷徑。值為 0 時，系統不會建立 [開始] 功能表捷徑。值為 1 時，系統會建立 [開始] 功能表捷徑。</p>	1
URL_FILTERING_ENABLED	<p>決定是否安裝 URL 內容重新導向功能。值為 1 時，系統會安裝功能。值為 0 時，則不會安裝此功能。</p> <p>在互動式安裝中將此內容設為 1 時，自訂安裝對話方塊中的 [其他] 功能下會出現 URL 內容重新導向 核取方塊，並且依預設為已選取。除非您將此內容設為 1，否則不會出現此核取方塊。</p> <p>備註 ADDLOCAL=ALL 內容未包含 URL 內容重新導向功能。</p>	0

表 2-2. Horizon Client 安裝內容 (續)

內容	說明	預設值
AUTO_UPDATE_ENABLED	決定是否啟用線上更新功能。值為 1 時，系統會啟用功能。值為 0 時，系統會停用功能。 如需詳細資訊，請參閱 線上更新 Horizon Client 。	1
INSTALL_TEAMS_REDIRECTION	決定是否啟用 Microsoft Teams 的媒體最佳化功能。值為 1 時，系統會啟用功能。值為 0 時，系統會停用功能。 如需關於此功能的詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。 備註 此功能不支援 32 位元 Core Remote Experience 元件。	1

從命令列安裝 Horizon Client

您可以輸入安裝程式檔案名稱並指定安裝命令和內容，而從命令列安裝 Horizon Client。您可以從命令列以無訊息方式安裝 Horizon Client。

必要條件

- 確認用戶端系統使用支援的作業系統。請參閱 [Windows 用戶端系統的系統需求](#)。
- 確認您能以管理員身分登入用戶端系統。
- 確認網域控制站有最新的修補程式、有足夠的可用磁碟空間和可相互連接。
- 如果您想要以 FIPS 相容密碼編譯安裝 Horizon Client，請在用戶端作業系統中啟用 FIPS 模式。請參閱 [在 Windows 用戶端作業系統中啟用 FIPS 模式](#)。
- 決定是否使用此功能讓使用者以目前登入的使用者身分，登入 Horizon Client 及其遠端桌面平台。使用者登入用戶端系統時輸入的認證資訊會傳遞至連線伺服器執行個體，並最終傳遞至遠端桌面平台。一些用戶端作業系統並不支援此功能。
- 熟悉 Horizon Client 安裝命令。請參閱 [Horizon Client 的安裝命令](#)。
- 熟悉 Horizon Client 安裝內容。請參閱 [Horizon Client 的安裝內容](#)。
- 決定是否要允許使用者從遠端桌面平台存取本機連線的 USB 裝置。如果不允許，請將 ADDLOCAL 安裝內容設定至功能清單，並忽略 USB 功能。如需詳細資訊，請參閱 [Horizon Client 的安裝內容](#)。
- 如果您不想要讓使用者必須提供連線伺服器執行個體的完整網域名稱 (FQDN)，請決定 FQDN，以便您在安裝期間加以提供。

程序

- 1 以管理員身分登入用戶端系統。
- 2 導覽至位於 <http://www.vmware.com/go/viewclients> 的 VMware 下載頁面。

3 下載 Horizon Client 安裝程式檔案，例如，VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe。
YYMM 是行銷版本號碼，y.y.y 是內部版本號碼，而 xxxxxx 是組建編號。

4 在 Windows 用戶端電腦上開啟命令提示字元。

5 在同一行中輸入安裝程式檔案名稱、安裝命令和安裝內容。

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe [commands] [properties]
```

結果

安裝程式會根據您所指定的安裝命令和內容來安裝 Horizon Client。如果您指定 `/silent` 安裝命令，則不會出現精靈提示。

安裝程式會安裝 Windows 服務，包括 VMware Horizon Client (`horizon_client_service`) 和 VMware USB Arbitration Service (`VMUSBArbService`)。

範例：範例安裝命令

下列命令會以互動方式安裝 Horizon Client，並啟用 URL 內容重新導向功能。

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe URL_FILTERING_ENABLED=1
```

下列命令會以無訊息方式安裝 Horizon Client，並在安裝程序期間隱藏所有的重新啟動動作和重新啟動提示。

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe /silent /norestart
```

後續步驟

如果您在安裝 Horizon Client 時啟用了 URL 內容重新導向功能，請確認該功能是否已安裝。請參閱[確認 URL 內容重新導向安裝](#)。

啟動 Horizon Client，並確認您可以登入正確的遠端桌面平台或已發佈的應用程式。請參閱[連線至遠端桌面平台或已發佈的應用程式](#)。

確認 URL 內容重新導向安裝

如果您在安裝 Horizon Client 時啟用了 URL 內容重新導向功能，請確認該功能是否已安裝。

必要條件

在安裝 Horizon Client 時指定 `URL_FILTERING_ENABLED=1` 安裝內容。請參閱[從命令列安裝 Horizon Client](#)。

程序

- 1 登入用戶端機器。
- 2 確認 `vmware-url-protocol-launch-helper.exe` 和 `vmware-url-filtering-plugin.dll` 檔案皆已安裝在 `%PROGRAMFILES%\VMware\VMware Horizon View Client\` 目錄中。
- 3 確認已在 Internet Explorer 中安裝並啟用 VMware Horizon View URL Filtering Plugin 附加元件。

線上更新 Horizon Client

您可以線上更新 Horizon Client。

依預設，紅點會出現在**選項**功能表上 (在您連線至伺服器之前)，以及**說明**按鈕 (在您連線至伺服器之後)，表示有新的 Horizon Client 版本可供使用。

在更新程序期間，依預設，您可以選取或取消選取**檢查更新並顯示徽章通知**核取方塊，以指定 Horizon Client 是否要自動檢查更新，並顯示新版本通知。

您可以透過設定下列群組原則設定，以控制線上更新功能的行為。

- **啟用 Horizon Client 線上更新**，這會啟用或停用線上更新功能。
- **Horizon Client 線上更新的 URL**，這會指定 Horizon Client 可從中擷取更新的替代 URL。
- **自動檢查更新**，這會控制**檢查更新並顯示徽章通知**核取方塊。
- **更新訊息快顯視窗**，這會控制**當有更新時，顯示快顯訊息**核取方塊。只有在已選取**檢查更新並顯示徽章通知**核取方塊時，**當有更新時，顯示快顯訊息**才會生效。
- **允許使用者略過 Horizon Client 更新**，這會控制**略過**按鈕。

如需關於這些群組原則設定的完整資訊，請參閱[用戶端 GPO 的一般設定](#)。

當您透過命令列安裝 Horizon Client 時，您也可以將 AUTO_UPDATE_ENABLED 內容設為 0 來停用線上更新功能。如需詳細資訊，請參閱[Horizon Client 的安裝內容](#)。

必要條件

- 在更新 Horizon Client 之前儲存您的工作。更新可能會起始系統重新開機。
- 確認您能以管理員身分登入用戶端系統。

程序

- 1 以管理員身分登入用戶端系統。
- 2 啟動 Horizon Client，然後按一下**軟體更新**。

選項	動作
連線到伺服器之前	按一下 選項 > 軟體更新 。
連線到伺服器之後	按一下 說明 > 軟體更新 。

- 3 若要檢查是否有可用的更新，請按一下**檢查更新**。

Horizon Client 會指出是否有可用的更新。

- 4 若要在新版本可供使用時開始更新程序，請按一下**下載並安裝**。

或者，您可以按一下**略過** (如果可用)，或按一下**稍後再提醒我**以在其他時間安裝更新。如果您按一下**略過**，則在下一個 Horizon Client 版本可供使用之前，將不會看到另一個更新通知。您仍可以按一下**軟體更新**，以手動檢查更新。

- 5 若要在下載 Horizon Client 後安裝更新，請按一下**確定**。
Horizon Client [互動式安裝精靈](#)隨即開啟。

為使用者設定 Horizon Client

3

為使用者設定 Horizon Client 時，可能涉及設定用來啟動 Horizon Client 的 URI、設定憑證檢查模式、設定進階 TLS 選項、自訂 Horizon Client 功能表，以及使用群組原則來設定自訂設定。

本章節討論下列主題：

- [一般組態設定](#)
- [使用 URI 設定 Horizon Client](#)
- [在 Horizon Client 中設定憑證檢查模式](#)
- [設定使用者的憑證檢查模式](#)
- [設定進階 TLS 選項](#)
- [自訂 Horizon Client 功能表](#)
- [自訂 Horizon Client 錯誤訊息](#)
- [設定游標事件處理](#)
- [使用群組原則設定來設定 Horizon Client](#)
- [從命令列執行 Horizon Client](#)
- [使用 Windows 登錄設定 Horizon Client](#)

一般組態設定

Horizon Client 提供數種組態機制，可簡化使用者的登入和遠端桌面平台選取體驗，並強制執行安全性原則。

下表僅顯示您可以一或多種方法設定的一些組態設定。

表 3-1. 一般組態設定

設定	用於設定的機制
伺服器位址	URI、群組原則、命令列、Windows 登錄
Active Directory 使用者名稱	URI、群組原則、命令列、Windows 登錄
網域名稱	URI、群組原則、命令列、Windows 登錄
遠端桌面平台顯示名稱	URI、群組原則、命令列

表 3-1. 一般組態設定 (續)

設定	用於設定的機制
視窗大小	URI、群組原則、命令列
顯示通訊協定	URI、命令列
設定憑證檢查	群組原則、Windows 登錄
設定 TLS 通訊協定和密碼編譯演算法	群組原則、Windows 登錄

使用 URI 設定 Horizon Client

您可以使用統一資源識別碼 (URI) 來建立網頁或電子郵件連結，讓使用者可以按一下來啟動 Horizon Client、連線至伺服器，或開啟遠端桌面平台或已發佈的應用程式。

您藉由建構 URI 的方式來建立這些連結以提供下列一些或全部資訊，因此您的使用者便無須提供：

- 伺服器位址
- 伺服器的連接埠號碼
- Active Directory 使用者名稱
- RADIUS 或 RSA SecurID 使用者名稱 (若與 Active Directory 使用者名稱不同時)
- 網域名稱
- 遠端桌面平台或已發佈的應用程式顯示名稱
- 視窗大小
- 動作包括重設、登出和啟動工作階段
- 顯示通訊協定
- 重新導向 USB 裝置的選項

若要建構 URI，請使用含有 Horizon Client 特定路徑和查詢部分的 `vmware-view` URI 配置。

若要使用 URI 來啟動 Horizon Client，必須已在用戶端電腦上安裝 Horizon Client。

用於建立 `vmware-view` URI 的語法

URI 語法包括 `vmware-view` URI 配置、指定遠端桌面平台或已發佈應用程式的路徑部分，以及指定遠端桌面平台或已發佈的應用程式動作或組態選項的查詢 (選用)。

URI 規格

使用下列語法建立 URI 以啟動 Horizon Client。

```
vmware-view://[authority-part]/[path-part][?query-part]
```

唯一所需的元素是 URI 配置，`vmware-view`。由於部分用戶端作業系統的某些版本會對配置名稱區分大小寫，請輸入 `vmware-view`。

重要 在所有元件中，必須先依據 UTF-8 [STD63] 編碼非 ASCII 字元，然後對應的 UTF-8 序列的每八位元並需進行百分比編碼，以顯示為 URI 字元。

如需有關 ASCII 字元的編碼資訊，請參閱 URL 編碼參考，網址為 <http://www.utf8-chartable.de/>。

authority-part

伺服器位址，以及選擇性的使用者名稱和/或非預設的連接埠號碼。伺服器名稱中不支援使用底線 (`_`)。伺服器名稱必須符合 DNS 語法。

若要指定使用者名稱，請使用下列語法。

```
user1@server-address
```

您無法指定包含網域的 UPN 位址。若要指定網域，您可以使用 URI 裡的 `domainName` 查詢部分。

若要指定連接埠號碼，請使用下列語法。

```
server-address:port-number
```

path-part

遠端桌面平台或已發佈應用程式的顯示名稱。建立桌面平台集區或應用程式集區時，系統會在 Horizon Console 中指定顯示名稱。如果顯示名稱包含空格，請使用 `%20` 編碼機制代表空格。

或者，您可以指定桌面平台或應用程式識別碼，這是包含桌面平台或應用程式集區識別碼的路徑字串。若要尋找桌面平台或應用程式識別碼，請在連線伺服器主機上開啟 ADSI Edit 並導覽至

`DC=vdi,dc=vmware,dc=int`，然後選取 `OU=Applications` 節點。此時會列出所有的桌面平台和應用程式集區。`distinguishedName` 屬性會指定識別碼值。您必須先對識別碼值進行編碼，再將其指定於 URI 中，例如 `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`。

如果您指定桌面平台或應用程式識別碼，即使桌面平台或應用程式識別碼在 ADSI Edit 中包含大寫字母，仍必須僅使用小寫字母。

備註 多個遠端桌面平台或已發佈的應用程式可以有相同的顯示名稱，但桌面平台和應用程式識別碼必須是唯一的。若要指定特定的遠端桌面平台或已發佈的應用程式，請使用桌面平台或應用程式識別碼而非顯示名稱。

query-part

要使用的組態選項，或是要執行的遠端桌面平台或已發佈的應用程式動作。查詢不區分大小寫。若要使用多項查詢，請在查詢之間使用 `&` 符號。如果查詢發生衝突，Horizon Client 會使用清單中的最後一個查詢。請使用下列語法。

```
query1=value1[&query2=value2...]
```


支援的查詢

此類型的 Horizon Client 支援下列查詢。如果您要為多種類型的用戶端 (例如, 桌面平台用戶端和行動用戶端) 建立 URI, 請參閱各類用戶端系統的安裝和設定指南, 以取得支援的查詢清單。

動作

表 3-2. 能與 action 查詢搭配使用的值

值	說明
browse	顯示指定的伺服器上主控的可用遠端桌面平台和已發佈的應用程式清單。使用此動作時, 您不需要指定遠端桌面平台或已發佈的應用程式。
start-session	開啟指定的遠端桌面平台或已發佈的應用程式。如果未提供任何動作查詢, 且提供了遠端桌面平台或已發佈的應用程式名稱, <code>start-session</code> 即為預設的動作。
reset	關閉並重新啟動指定的遠端桌面平台或已發佈的應用程式。尚未儲存的資料會遺失。重設遠端桌面平台等同於按下實體 PC 上的 [重設] 按鈕。
restart	關閉並重新啟動指定的遠端桌面平台。重新啟動遠端桌面平台等同於 Windows 作業系統重新啟動命令。作業系統通常會在重新啟動之前提示使用者儲存任何未儲存的資料。
logoff	將使用者從遠端桌面平台的客體作業系統登出。如果您指定已發佈的應用程式, 則該動作將被忽略, 或使用者會看到警告訊息「URI 動作無效」。

args

指定在已發佈的應用程式啟動時所要新增的命令列引數。使用語法 `args=value`, 其中 `value` 為字串。針對下列字元使用百分比編碼:

- 冒號 (:) 請使用 `%3A`
- 反斜線 (\) 請使用 `%5C`
- 空格 () 請使用 `%20`
- 雙引號 (") 請使用 `%22`

例如, 若要為 Notepad++ 應用程式指定檔案名稱 "My new file.txt", 請使用 `%22My%20new%20file.txt%22`。

appProtocol

就已發佈的應用程式而言, 有效值為 `PCoIP` 和 `BLAST`。例如, 若要指定 PCoIP, 請使用語法 `appProtocol=PCoIP`。

connectUSBOnInsert

當您插入 USB 裝置時, 會將該裝置連線至前景遠端桌面平台或已發佈的應用程式。如果您為遠端桌面平台指定 `unattended` 查詢, 則會隱含地設定此查詢。若要使用此查詢, 您必須將 `action` 查詢設定成 `start-session` 或者不要有 `action` 查詢。有效值為 `true` 和 `false`。語法範例為 `connectUSBOnInsert=true`。

connectUSBOnStartup

將目前連線至用戶端系統的所有 USB 裝置重新導向至遠端桌面平台或已發佈的應用程式。如果您為遠端桌面平台指定 **unattended** 查詢，則會隱含地設定此查詢。若要使用此查詢，您必須將 **action** 查詢設定成 **start-session** 或者不要有 **action** 查詢。有效值為 **true** 和 **false**。語法範例為 **connectUSBOnStartup=true**。

desktopLayout

設定遠端桌面平台視窗的大小。若要使用此查詢，您必須將 **action** 查詢設定為 **start-session** 或不要有 **action** 查詢。

表 3-3. desktopLayout 查詢的有效值

值	說明
fullscreen	一台監視器上全螢幕顯示。此值為預設值。
multimonitor	所有監視器上全螢幕顯示。
windowLarge	大視窗。
windowSmall	小視窗。
WxH	自訂解析度，以畫素單位指定寬度乘高度。語法範例為 desktopLayout=1280x800 。

desktopProtocol

針對遠端桌面平台，有效值為 **RDP**、**PCoIP** 和 **BLAST**。例如，若要指定 PCoIP，請使用語法 **desktopProtocol=PCoIP**。

domainName

指定與連線至遠端桌面平台或已發佈應用程式的使用者相關聯的 NETBIOS 網域名稱。例如，您可以使用 **mycompany** 而非 **mycompany.com**。

filePath

指定您要以已發佈的應用程式開啟的檔案在本機系統上的路徑。您必須指定完整路徑，包括磁碟機代號在內。針對下列字元使用百分比編碼：

- 冒號 (:) 請使用 **%3A**
- 反斜線 (\) 請使用 **%5C**
- 空格 () 請使用 **%20**

例如，若要代表檔案路徑 **C:\test file.txt**，請使用 **C%3A%5Ctest%20file.txt**。

launchMinimized

以最小化模式啟動 Horizon Client。Horizon Client 會維持最小化狀態，直到指定的遠端桌面平台或已發佈的應用程式啟動為止。語法為 **launchMinimized=true**。您無法透過自動查詢來使用此查詢。

tokenUserName

指定 RSA 或 RADIUS 使用者名稱。唯有 RSA 或 RADIUS 使用者名稱和 Active Directory 使用者名稱不同時，才使用此查詢。如果您未指定此查詢，但需要進行 RSA 或 RADIUS 驗證，則 Horizon Client 會使用 Windows 使用者名稱。語法是 **tokenUserName=*name***。

unattended

在 Kiosk 模式中建立伺服器與遠端桌面平台的連線。如果您使用此查詢，則從用戶端裝置的 MAC 位址產生帳戶名稱時，請勿指定使用者資訊。如果您已在 ADAM 中建立自訂帳戶名稱 (如開頭為「custom-」的名稱)，則必須指定帳戶資訊。

useExisting

如果此選項設定為 **true**，則只能執行一個 Horizon Client 執行個體。如果使用者嘗試連線至第二個伺服器，他們必須先登出第一個伺服器，而造成遠端桌面平台和已發佈的應用程式工作階段中斷連線。如果此選項設定為 **false**，則可執行多個 Horizon Client 執行個體，使用者也可同時連線至多個伺服器。預設值是 **true**。語法範例為 **useExisting=false**。

unauthenticatedAccessEnabled

如果此選項設為 **true**，則依預設會啟用 [未驗證存取] 功能。使用「未驗證存取」匿名登入選項會顯示在使用者介面中，並且已選取。如果此選項設為 **false**，則會停用 [未驗證存取] 功能。使用「未驗證存取」匿名登入設定會隱藏並停用。此選項設為 "" 時，將會停用 [未驗證存取] 功能，並且在使用者介面中隱藏並停用使用「未驗證存取」匿名登入設定。語法範例為 **unauthenticatedAccessEnabled=true**。

unauthenticatedAccessAccount

如果「未驗證存取」功能已啟用，將會設定要使用的帳戶。如果 [未驗證存取] 功能停用，則會忽略此查詢。使用 **anonymous1** 使用者帳戶的語法範例為 **unauthenticatedAccessAccount=anonymous1**。

vmware-view URI 範例

您可以使用 **vmware-view** URI 配置建立超文字連結或按鈕，並在電子郵件中或網頁上加入這些連結。例如，使用者可以按一下 URI 連結，以使用您指定的啟動選項來啟動遠端桌面平台。

URI 語法範例

在每個 URI 範例後均會說明使用者在按下 URI 連結後會看見的情形。

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client 會啟動並連線至 **view.mycompany.com** 伺服器。[登入] 對話方塊會提示使用者輸入使用者名稱、網域名稱和密碼。成功登入之後，用戶端會連線至顯示名稱為主要桌面平台的遠端桌面平台，且使用者會登入客體作業系統。

備註 在此範例中，系統會使用預設的顯示通訊協定和視窗大小。預設顯示通訊協定為 PCoIP，而預設視窗大小為全螢幕。

2 `vmware-view://view.mycompany.com/cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`

Horizon Client 會啟動並連線至 `view.mycompany.com` 伺服器。[登入] 對話方塊會提示使用者輸入使用者名稱、網域名稱和密碼。成功登入後，用戶端會連線至遠端桌面平台，且其桌面平台識別碼為 `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (編碼值 `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`)。

3 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

除了針對連線伺服器執行個體採用非預設的連接埠 7555 之外，此 URI 與先前的範例具有同樣的效果。(預設連接埠為 443。)因為提供了遠端桌面平台識別碼，儘管 URI 中並未包含 `start-session` 動作，遠端桌面平台仍會開啟。

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCoIP`

Horizon Client 會啟動並連線至 `view.mycompany.com` 伺服器。在 [登入] 對話方塊中，**使用者名稱** 文字方塊填入了 `fred`。該使用者必須提供網域名稱及密碼。成功登入之後，用戶端會連線至顯示名稱為 `Finance Desktop` 的遠端桌面平台，且使用者會登入客體作業系統。該連線採用 `PCoIP` 顯示通訊協定。

5 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client 會啟動並連線至 `view.mycompany.com` 伺服器。在 [登入] 對話方塊中，使用者必須提供使用者名稱、網域名稱和密碼。成功登入之後，用戶端會連線至顯示名稱為計算器的已發佈應用程式。該連線採用 `VMware Blast` 顯示通訊協定。

6 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client 會啟動並連線至 `view.mycompany.com` 伺服器。在 [登入] 對話方塊中，**使用者名稱** 文字方塊中填入了 `fred`，且**網域**文字方塊填入了 `mycompany`。該使用者僅必須提供密碼。成功登入之後，用戶端會連線至顯示名稱為財務桌面平台的遠端桌面平台，且使用者會登入客體作業系統。

7 `vmware-view://view.mycompany.com/`

Horizon Client 會啟動，並且會向使用者顯示連線至 `view.mycompany.com` 伺服器的登入提示。

8 `vmware-view://view.mycompany.com/Primary%20Desktop?action=reset`

Horizon Client 會啟動並連線至 `view.mycompany.com` 伺服器。[登入] 對話方塊會提示使用者輸入使用者名稱、網域名稱和密碼。成功登入之後，Horizon Client 會顯示對話方塊，提示使用者確認主要桌面平台的重設作業。

備註 只有在 Horizon 管理員已為遠端桌面平台啟用重設功能時，才可使用此動作。

9 `vmware-view://view.mycompany.com/Primary%20Desktop?action=restart`

Horizon Client 會啟動並連線至 `view.mycompany.com` 伺服器。[登入] 對話方塊會提示使用者輸入使用者名稱、網域名稱和密碼。成功登入之後，Horizon Client 會顯示對話方塊，提示使用者確認 Primary Desktop 的重新啟動作業。

備註 只有在 Horizon 管理員已為遠端桌面平台啟用重新啟動功能時，才可使用此動作。

10 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSBOnStartup=true`

此 URI 和第一個範例具有同樣的效果，並會將連線到用戶端系統的所有 USB 裝置重新導向至遠端桌面平台。

11 `vmware-view://`

如果 Horizon Client 未執行，則會開始執行。如果 Horizon Client 已在執行中，則會移至前景。

12 `vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22`

在伺服器 10.10.10.10 上啟動 My Notepad++，並將引數 My new file.txt 傳遞至已發佈應用程式的啟動命令中。空格和雙引號會使用百分比逸出。由於檔案名稱包含空格，因此會以雙引號括住。

您也可以使用下列語法，在 Windows 命令列提示字元中輸入此命令：

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

在此範例中，雙引號會使用字元 \ 的方式逸出。

13 `vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt`

在伺服器 10.10.10.10 上啟動 Notepad++ 12，並將引數 a.txt b.txt 傳遞至已發佈應用程式的啟動命令中。由於引數未以引號括住，因此會以空格分隔多個檔案名稱，且兩個檔案會在 Notepad++ 中個別開啟。

備註 已發佈應用程式在使用命令列引數的方式上可能有所不同。例如，如果您將引數 a.txt b.txt 傳遞至 WordPad，WordPad 將只會開啟一個 a.txt 檔案。

14 `vmware-view://view.mycompany.com/Notepad?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1`

Horizon Client 會使用 **anonymous1** 使用者帳戶啟動並連線至 `view.mycompany.com` 伺服器。「記事本」應用程式會在未提示使用者提供登入認證的情況下啟動。

HTML 程式碼範例

您可以使用 URI 建立超文字連結和按鈕，並加入至電子郵件或網頁中。以下範例顯示如何使用第一個 URI 範例中的 URI，對標示為 **測試連結** 的超文字連結和標示為 **測試按鈕** 的按鈕進行編碼。

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</a><br>
```

```
<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>
</body>
</html>
```

在 Horizon Client 中設定憑證檢查模式

Horizon Client 與伺服器之間連線時會發生伺服器憑證檢查。憑證是一種數位身分識別格式，類似於護照或駕駛人的駕照。

伺服器憑證檢查包括下列檢查：

- 憑證已被撤銷了嗎？
- 憑證是否用於驗證寄件者身分並將伺服器通訊加密以外的目的？也就是說，它是正確的憑證類型嗎？
- 憑證是否已到期，或是尚未生效？也就是說，根據電腦的時鐘，憑證有效嗎？
- 憑證上的一般名稱是否符合傳送該憑證的伺服器主機名稱？如果負載平衡器將 Horizon Client 重新導向至一台其憑證與在 Horizon Client 中輸入的主機名稱不符的伺服器，則會發生不符的情形。另一個會發生不符的原因是您在用戶端輸入 IP 位址，而非主機名稱。
- 憑證是由未知或未受信任的憑證授權機構 (CA) 簽署的嗎？自我簽署憑證是一種未受信任的憑證授權機構。若要通過此檢查，必須將憑證之信任鏈放在裝置之本機憑證存放區的根目錄。

如需將自我簽署根憑證散佈到網域中的所有 Windows 用戶端系統的資訊，請參閱《Horizon 安裝》文件中的〈將根憑證新增至信任的根憑證授權機構〉。

若要設定憑證檢查模式，請啟動 Horizon Client，並在 Horizon Client 功能表列的**選項**功能表中選取**設定 SSL**。您可以選取下列其中一個選項。

- **永不連線至未受信任的伺服器**。此設定表示如果任一憑證檢查失敗，則無法連線至伺服器。錯誤訊息列出失敗的檢查。
- **在連線至未受信任的伺服器前提出警告**。此設定表示如果憑證檢查失敗，您可以按一下**繼續**以忽略警告，因為伺服器使用自我簽署的憑證。針對自我簽署憑證，憑證名稱不需要符合您在 Horizon Client 中輸入的伺服器名稱。如果憑證已到期，您也可以收到警告。
- **不要驗證伺服器身分識別憑證**。此設定表示不會發生憑證檢查。

如果管理員稍後從受信任的憑證授權機構安裝安全憑證，且在您連線時所有憑證檢查均通過，則系統會為該伺服器記住這個受信任的連線。以後，如果那台伺服器再度提出自我簽署憑證的話，則該連線會失敗。在特別的伺服器提出可完全驗證的憑證之後，每次都必須這樣做。

重要 如果您先前曾使用群組原則來設定公司的用戶端系統，以使用特定的密碼 (例如，藉由設定 [SSL 加密套件順序] 群組原則設定)，則您現在必須使用 Horizon Client 群組原則安全性設定。請參閱[用戶端 GPO 的安全性設定](#)。或者，您可以在用戶端系統上使用 SSLCipherList 登錄設定。請參閱[使用 Windows 登錄設定 Horizon Client](#)。

您可以在 Horizon Client 中設定預設憑證檢查模式，並防止使用者加以變更。如需詳細資訊，請參閱[設定使用者的憑證檢查模式](#)。

使用 SSL Proxy 伺服器

如果您使用 SSL Proxy 伺服器來檢查從用戶端環境傳送到網際網路的流量，請啟用[允許透過 SSL Proxy 的連線](#)設定。此設定會允許針對透過 SSL Proxy 伺服器的次要連線進行憑證檢查，並同時套用至 Blast 安全閘道和安全通道連線。如果您使用 SSL Proxy 伺服器並啟用憑證檢查，卻未啟用[允許透過 SSL Proxy 的連線](#)設定，則連線會因為指紋不相符而失敗。如果您啟用[不要驗證伺服器身分識別憑證](#)選項，則無法使用[允許透過 SSL Proxy 的連線](#)設定。當[不要驗證伺服器身分識別憑證](#)選項啟用時，Horizon Client 就不會驗證憑證或指紋，並且一律會允許 SSL Proxy。

您可以使用設定 **Horizon Client 的 SSL Proxy 憑證檢查行為** 群組原則設定，來設定是否允許針對透過 SSL Proxy 伺服器的次要連線進行憑證檢查。如需詳細資訊，請參閱[用戶端 GPO 的安全性設定](#)。

若要允許透過 Proxy 伺服器進行 VMware Blast 連線，請參閱[設定 VMware Blast 選項](#)。

設定使用者的憑證檢查模式

您可以設定使用者的憑證檢查模式。例如，您可以設定一律執行完整驗證。當伺服器與 Horizon Client 之間產生 TLS 連線時，就會執行憑證檢查。

您可以為使用者設定下列其中一項憑證驗證策略。

- 使用者可以在 Horizon Client 中選取憑證檢查模式。
- (無驗證) 不執行憑證檢查。
- (警告) 如果伺服器出示自我簽署憑證，則會對使用者發出警告。使用者可決定是否允許此類型的連線。
- (完整安全性) 執行完整驗證，凡是無法通過完整驗證的連線均會遭到拒絕。

如果您使用 SSL Proxy 伺服器來檢查從用戶端環境傳送到網際網路的流量，則可以針對透過 SSL Proxy 伺服器的次要連線設定其憑證檢查。此功能同時適用於 Blast 安全閘道和安全通道連線。您也可以允許對 VMware Blast 連線使用 Proxy 伺服器。

如需可執行之憑證檢查類型的相關資訊，請參閱在 [Horizon Client 中設定憑證檢查模式](#)。

您可以使用 Horizon Client 群組原則設定，來設定憑證檢查模式、允許使用 SSL Proxy、限制在建立加密 TLS 連線之前對某些密碼編譯演算法和通訊協定的使用，以及為 VMware Blast 連線啟用 Proxy 使用。如需詳細資訊，請參閱[用戶端 GPO 的安全性設定](#)和[用戶端 GPO 的一般設定](#)。

如果您不想將憑證檢查模式設定為群組原則，您可以將 CertCheckMode 值名稱新增至用戶端電腦上的下列任一登錄機碼中，以啟用憑證檢查：

- 針對 32 位元 Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security
- 針對 64 位元 Windows: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security

在登錄機碼中使用下列各值：

- 0 會實作 Do not verify server identity certificates。
- 1 會實作 Warn before connecting to untrusted servers。
- 2 會實作 Never connect to untrusted servers。

如果您在登錄機碼中同時設定了群組原則設定及 CertCheckMode 設定，則群組原則設定的優先順序會高於登錄機碼值。

設定進階 TLS 選項

您可以選取用來對 Horizon Client 和伺服器之間，以及 Horizon Client 和遠端桌面平台中的代理程式之間的通訊進行加密的安全性通訊協定和密碼編譯演算法。

這些安全性選項也可用來加密 USB 通道。

使用預設設定時，加密套件會使用 128 位元或 256 位元 AES、移除匿名 DH 演算法，然後依加密演算法金鑰長度的順序為目前加密清單排序。

依預設會啟用 TLS v1.1 和 TLS v1.2。不支援 SSL v2.0、SSL v3.0 和 TLS v1.0。

如果您為 Horizon Client 設定安全性通訊協定，但未在用戶端連線的伺服器上啟用該通訊協定，則會發生 TLS 錯誤，且連線將會失敗。

重要 您在 Horizon Client 中啟用的通訊協定也必須有至少一個在遠端桌面平台上啟用，否則 USB 裝置無法重新導向至遠端桌面平台。

在用戶端系統上，您可以使用群組原則設定或 Windows 登錄設定，來變更預設加密和通訊協定。如需使用群組原則設定的相關資訊，請參閱[用戶端 GPO 的安全性設定](#)中的設定 **SSL 通訊協定和密碼編譯演算法** 設定。如需在 Windows 登錄中使用 SSLCipherList 設定的相關資訊，請參閱[使用 Windows 登錄設定 Horizon Client](#)。

自訂 Horizon Client 功能表

您可以使用 Horizon Client 群組原則來隱藏 Horizon Client 使用者介面中特定功能表的某些項目。

如需有關使用 Horizon Client 群組原則的一般資訊，請參閱[使用群組原則設定來設定 Horizon Client](#)。

如需使用可控制 Horizon Client 功能表的群組原則詳細資訊，請參閱[用戶端 GPO 的一般設定](#)中隱藏應用程式快顯功能表中的項目、隱藏桌面平台快顯功能表中的項目、隱藏桌面平台工具列中的項目、隱藏系統匣功能表中的項目以及隱藏用戶端工具列功能表中的項目群組原則設定的說明。

自訂 Horizon Client 錯誤訊息

您可以使用 Horizon Client [自訂錯誤畫面註腳](#)群組原則設定，將自訂說明文字新增至 Horizon Client 使用者介面中所顯示的所有錯誤訊息底部。例如，說明文字可能會告知使用者如何連絡貴公司的服務台。

您必須在本機用戶端系統上建立純文字 (.txt) 檔案，才能包含說明文字。此文字檔案最多可包含 2048 個字元 (包括控制字元在內)。同時支援 ANSI 和 Unicode 兩種編碼。在設定自訂錯誤畫面註腳群組原則設定時，請指定此文字檔案的完整路徑。

如需有關使用 Horizon Client 群組原則的一般資訊，請參閱[使用群組原則設定來設定 Horizon Client](#)。

如需有關使用自訂錯誤畫面註腳群組原則設定的詳細資訊，請參閱[用戶端 GPO 的一般設定](#)。

設定游標事件處理

您可以在 Windows 用戶端系統上的 C:\ProgramData\VMware\VMware Horizon View\config.ini 檔案中進行設定，以最佳化游標事件處理。

備註 若要使用游標事件處理，則必須在遠端桌面平台上安裝 Horizon Agent 2006 或更新版本。

設定	說明
RemoteDisplay.allowCursorWarping	啟用或停用游標翹曲功能。 如果啟用此功能，且滑鼠處於絕對模式，則遠端代理程式將偵測到突然的游標移動，並透過移動本機游標將其反映至用戶端。停用此功能時，用戶端會忽略遠端代理程式中突然的游標移動。 有效值為 TRUE 或 FALSE。預設值為 TRUE。
RemoteDisplay.allowCursorEventsOnLowLatencyChannel	決定是否將低延遲通道用於游標更新。有效值為 TRUE 或 FALSE。預設值為 TRUE。

您可以設定設定滑鼠聯合的延遲上限群組原則設定，以設定聯合滑鼠移動時允許的延遲上限。如需詳細資訊，請參閱[用戶端 GPO 的一般設定](#)。

您也可以代理程式機器上設定游標事件處理。例如，您可以使用代理程式端游標翹曲群組原則設定來設定游標翹曲，且您可以修改代理程式機器上的 Windows 登錄設定，以啟用或停用聯合滑鼠移動事件和低延遲通道。用戶端和代理程式上的設定必須相符才能啟用此功能。如需代理程式端設定的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

使用群組原則設定來設定 Horizon Client

Horizon Client 包含可用來設定 Horizon Client 功能和行為的群組原則 ADMX 範本檔。您可以將 ADMX 範本檔中的原則設定新增至 Active Directory 中新的或現有的 GPO，藉以最佳化及保護遠端桌面平台和已發佈的應用程式連線。

此範本檔包含「電腦組態」與「使用者組態」群組原則。

- [電腦組態] 原則設定適用於 Horizon Client 的原則，不論在主機上執行用戶端的是誰。
- 「使用者組態」原則設定的 Horizon Client 原則會套用至所有執行 Horizon Client 的使用者以及 RDP 連線設定。「使用者組態」原則會覆寫對等的「電腦組態」原則。

Horizon Client 會在遠端桌面平台和已發佈的應用程式啟動時以及使用者登入時套用原則。

Horizon Client 組態 ADMX 範本檔 (vdm_client.admx) 和所有提供群組原則設定的 ADMX 檔案皆可從 VMware-Horizon-Extras-Bundle-YMMM-x.x.x-yyyyyyy.zip 中取得，其中 YMMM 為行銷版本號碼，x.x.x 為內部版本號碼，yyyyyyy 為組建編號。您可以從 VMware 下載網站下載此 ZIP 檔案，網址為：<https://my.vmware.com/web/vmware/downloads>。您必須將此檔案複製到 Active Directory 伺服器，並使用群組原則管理編輯器新增系統管理範本。如需指示，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

用戶端 GPO 的指令碼定義設定

您可以為許多從命令列執行 Horizon Client 時可設定的相同設定進行群組原則設定，包括遠端桌面平台視窗大小、登入使用者名稱和登入網域名稱。

下表說明 VMware Horizon Client 組態 ADMX 範本檔中的指令碼定義設定。此範本檔提供每個指令碼定義設定的「電腦組態」和「使用者組態」版本。「使用者組態」設定會覆寫對等的「電腦組態」設定。這些設定會出現在群組原則管理編輯器的 **VMware Horizon Client 組態 > 指令碼定義** 資料夾中。

表 3-4. VMware Horizon Client 組態範本：指令碼定義

設定	說明
Automatically connect if only one launch item is entitled	如果使用者僅有權使用一個遠端桌面平台，請將使用者連線至該遠端桌面平台。此設定可讓使用者無需從只包含一個遠端桌面平台的清單中選取遠端桌面平台。
Connect all USB devices to the desktop or remote application on launch	決定在遠端桌面平台或已發佈的應用程式啟動時，用戶端系統上所有可用的 USB 裝置是否會連線至遠端桌面平台或已發佈的應用程式。
Connect USB devices to the desktop or remote application when they are plugged in	決定在 USB 裝置插入用戶端系統時，這些裝置是否會連線至遠端桌面平台或已發佈的應用程式。
DesktopLayout	指定使用者在登入遠端桌面平台時看到的 Horizon Client 視窗配置。配置選項如下： <ul style="list-style-type: none"> ■ Full Screen ■ Multimonitor ■ Window - Large ■ Window - Small 此設定只有在同時設定 DesktopName to select setting 時才可用。
DesktopName to select	指定 Horizon Client 在登入期間使用的預設桌面平台。
Disable 3rd-party Terminal Services plugins	決定 Horizon Client 是否檢查安裝為一般 RDP 外掛程式的協力廠商終端機服務外掛程式。如果您並未設定此設定，Horizon Client 預設為檢查協力廠商外掛程式。此設定不會影響 Horizon 專用的外掛程式，例如 USB 重新導向。
Locked Guest Size	如果顯示用於一台監視器上，請指定遠端桌面平台的螢幕解析度。如果您將遠端桌面平台顯示設定為 所有監視器 ，則此設定不會正常運作。 啟用此設定後，系統會停用遠端桌面平台自動調整功能，且會在 Horizon Client 使用者介面中隱藏 允許顯示調整值 選項。
Logon DomainName	指定 Horizon Client 登入時使用的 NetBIOS 網域。
Logon Password	指定 Horizon Client 登入時使用的密碼。Active Directory 會以純文字格式儲存密碼。為提高安全性，請勿指定此設定。使用者能以互動式方法輸入密碼。
Logon UserName	指定 Horizon Client 登入時使用的密碼。Active Directory 會以純文字格式儲存密碼。

表 3-4. VMware Horizon Client 組態範本：指令碼定義 (續)

設定	說明
Server URL	指定 Horizon Client 登入時使用的 URL，例如 <code>https://view1.example.com</code> 。
Suppress error messages (when fully scripted only)	決定是否在登入期間隱藏 Horizon Client 錯誤訊息。 此設定僅適用於完全以指令碼撰寫登入程序時，例如，當所有必要的登入資訊都是透過群組原則預先填入時。 如果因為登入資訊不正確造成登入失敗，使用者並不會收到通知，且 Horizon Client 程序將會終止。
Disconnected application session resumption behavior	決定當使用者重新連線至伺服器時，執行中已發佈應用程式的行為執行方式。選擇如下所示： <ul style="list-style-type: none"> ■ 要求重新連線以開啟應用程式 ■ 自動重新連線以開啟應用程式 ■ 不詢問且不自動重新連線 此設定啟用時，使用者將無法在 Horizon Client 中設定已發佈應用程式的重新連線行為。 此設定停用時，使用者將可在 Horizon Client 中設定已發佈應用程式的重新連線行為。此設定依預設為停用。
Enable Unauthenticated Access to the server	決定使用者在使用 Horizon Client 時是否必須輸入認證才能存取其已發佈的應用程式。 當此設定啟用時，Horizon Client 中的 使用「未驗證存取」匿名登入 設定會顯示為停用狀態，並且已選取。如果「未驗證存取」無法使用，則用戶端可能會回復為使用其他驗證方法。 當此設定停用時，使用者一律必須輸入認證才能登入並存取其已發佈的應用程式。Horizon Client 中的 使用「未驗證存取」匿名登入 設定會隱藏並取消選取。 依預設，使用者可以在 Horizon Client 中啟用「未驗證存取」。使用「未驗證存取」匿名登入設定會顯示為啟用狀態，並且取消選取。
Account to use for Unauthenticated Access	指定在 Enable Unauthenticated Access to the server 群組原則設定啟用時，或使用者在 Horizon Client 中選取 使用「未驗證存取」匿名登入 以啟用「未驗證存取」時，讓 Horizon Client 用來匿名登入伺服器的「未驗證存取」使用者帳戶。 如果「未驗證存取」未用於特定的伺服器連線，則會忽略此設定。依預設，使用者可以選取帳戶。
Use existing client instance when connect to same server	決定是否將連線新增至使用者已連線至相同伺服器的現有 Horizon Client 執行個體。 未設定時，此設定依預設為停用。

用戶端 GPO 的安全性設定

安全性設定包括憑證、登入認證和單一登入功能的群組原則。

下表說明 Horizon Client 組態 ADMX 範本檔中的安全性設定。此表格說明設定是同時包含「電腦組態」和「使用者組態」設定，還是僅包含「電腦組態」設定。對於兩種設定的安全性設定而言，「使用者組態」設定會覆寫同等的「電腦組態」設定。這些設定會出現在群組原則管理編輯器的 **VMware Horizon Client 組態 > 安全性設定** 資料夾中。

表 3-5. Horizon Client 組態範本：安全性設定

設定	電腦	使用者	說明
Allow command line credentials	X		<p>決定是否可以透過 Horizon Client 命令列選項提供使用者認證。如果已停用此設定，則使用者從命令列執行 Horizon Client 時就無法使用 smartCardPIN 和 password 選項。</p> <p>此設定依預設為啟用。</p> <p>對等的 Windows 登錄值為 AllowCmdLineCredentials。</p>
Configures the SSL Proxy certificate checking behavior of the Horizon Client	X		<p>針對 Blast 安全閘道和安全通道連線，決定是否允許針對透過 SSL Proxy 伺服器的次要連線進行憑證檢查。</p> <p>未設定此設定時 (預設值)，使用者可以在 Horizon Client 中手動變更 SSL Proxy 設定。請參閱在 Horizon Client 中設定憑證檢查模式。</p> <p>依預設，Horizon Client 會針對 Blast 安全閘道和安全通道連線封鎖 SSL Proxy 連線。</p>
Servers Trusted For Delegation	X		<p>指定有哪些連線伺服器執行個體會接受使用者在 Horizon Client 功能表列的 選項 功能表中選取以 目前使用者身分登入 時所傳遞的使用者身分識別和認證資訊。如果未指定任何連線伺服器執行個體，則所有連線伺服器執行個體都會接受這項資訊，除非您在 Horizon Console 中為連線伺服器執行個體停用 允許以目前使用者身分登入 驗證設定。</p> <p>若要新增連線伺服器執行個體，請使用下列其中一種格式：</p> <ul style="list-style-type: none"> ■ domain\system\$ ■ system\$@domain.com ■ 連線伺服器服務的服務主體名稱 (SPN)。 <p>對等的 Windows 登錄值為 BrokersTrustedForDelegation。</p>

表 3-5. Horizon Client 組態範本：安全性設定 (續)

設定	電腦	使用者	說明
Certificate verification mode	X		<p>設定 Horizon Client 執行的憑證檢查層級。您可以選取下列其中一種模式：</p> <ul style="list-style-type: none"> ■ No Security。不會執行憑證檢查。 ■ Warn But Allow。如果憑證檢查因伺服器使用自我簽署憑證而失敗，使用者將會看到警告，但可加以忽略。針對自我簽署憑證，憑證名稱不需要符合使用者在 Horizon Client 中輸入的伺服器名稱。 <p>如果發生任何其他憑證錯誤情況，則 Horizon Client 會顯示錯誤，並防止使用者連線至伺服器。</p> <p>Warn But Allow 是預設值。</p> <ul style="list-style-type: none"> ■ Full Security。如果發生任何類型的憑證錯誤，使用者就無法連線至伺服器。Horizon Client 會對使用者顯示憑證錯誤。 <p>設定此設定時，使用者可以檢視 Horizon Client 中選取的憑證驗證模式，但是無法進行設定。[憑證檢查模式] 對話方塊會通知使用者管理員已鎖定此設定。</p> <p>當此設定停用時，Horizon Client 使用者可以選取憑證檢查模式。此設定依預設為停用。</p> <p>若要允許伺服器執行 Horizon Client 提供的憑證選取，用戶端必須建立對連線伺服器或安全伺服器主機的 HTTPS 連線。如果您將 TLS 卸載至與連線伺服器或安全伺服器主機建立 HTTP 連線的中繼裝置，則不支援憑證檢查。</p> <p>如果您不想將此設定設為群組原則，您也可以將 CertCheckMode 值名稱新增至用戶端電腦上的下列其中一個登錄機碼，以啟用憑證驗證：</p> <ul style="list-style-type: none"> ■ 針對 32 位元 Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security ■ 針對 64 位元 Windows: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security <p>在登錄機碼中使用下列各值：</p> <ul style="list-style-type: none"> ■ 0 會實作 No Security。 ■ 1 會實作 Warn But Allow。 ■ 2 會實作 Full Security。 <p>如果您在 Windows 登錄機碼中同時設定了群組原則設定及 CertCheckMode 設定，則群組原則設定的優先順序會高於登錄機碼值。</p> <p>備註 在未來的 Horizon Client 版本中，可能不再支援使用 Windows 登錄來設定此設定，而必須使用群組原則設定。</p>

表 3-5. Horizon Client 組態範本：安全性設定 (續)

設定	電腦	使用者	說明
Default value of the 'Log in as current user' checkbox	X	X	<p>指定 Horizon Client 功能表列的選項功能表中以目前使用者身分登入的預設值。</p> <p>此設定會覆寫 Horizon Client 安裝期間指定的預設值。</p> <p>如果使用者從命令列執行 Horizon Client 並指定 <code>LogInAsCurrentUser</code> 選項，則該值會覆寫此設定。</p> <p>在選項功能表中選取以目前使用者身分登入時，使用者登入用戶端系統時所提供的身分識別和認證資訊都會傳遞至連線伺服器執行個體，且最終會傳遞至遠端桌面平台或已發佈的應用程式。如果取消選取以目前使用者身分登入，則使用者必須多次提供身分識別和認證資訊，才能存取遠端桌面平台或已發佈的應用程式。</p> <p>此設定依預設為停用。</p> <p>對等的 Windows 登錄值為 <code>LogInAsCurrentUser</code>。</p>
Display option to Log in as current user	X	X	<p>決定以目前使用者身分登入是否會顯示在 Horizon Client 功能表列的選項功能表中。</p> <p>以目前使用者身分登入顯示時，使用者將可加以選取或取消選取，並覆寫其預設值。以目前使用者身分登入隱藏時，使用者將無法從 Horizon Client 的選項功能表覆寫其預設值。</p> <p>您可以使用原則設定 <code>Default value of the 'Log in as current user' checkbox</code>，指定以目前使用者身分登入的預設值。</p> <p>此設定依預設為啟用。</p> <p>對等的 Windows 登錄值為 <code>LogInAsCurrentUser_Display</code>。</p>
Enable jump list integration	X		<p>決定跳躍清單是否會出現在 Windows 7 及更新版本系統工作列上的 Horizon Client 圖示中。跳躍清單可讓使用者連線至最近的伺服器、遠端桌面平台和已發佈的應用程式。</p> <p>如果 Horizon Client 為共用狀態，您可能不希望使用者看到最近的桌面平台和已發佈的應用程式名稱。您可以停用此設定以停用跳躍清單。</p> <p>此設定依預設為啟用。</p> <p>對等的 Windows 登錄值為 <code>EnableJumplist</code>。</p>
Enable SSL encrypted framework channel	X	X	<p>決定是否為 View 5.0 及更早版本的遠端桌面平台啟用 TLS。在 View 5.0 之前，透過連接埠 TCP 32111 傳送至遠端桌面平台的資料不會加密。</p> <ul style="list-style-type: none"> ■ 啟用：啟用 TLS，但如果遠端桌面平台沒有 TLS 支援，則允許回復為之前的未加密連線。例如，View 5.0 和更早版本的桌面平台並沒有 TLS 支援。啟用是預設設定。 ■ 停用：停用 TLS。如果通道不存在，且之後可能由 WAN 加速器產品進行最佳化，則此設定可能有用。 ■ 強制執行：啟用 TLS，並拒絕連線至沒有 TLS 支援的遠端桌面平台。 <p>對等的 Windows 登錄值為 <code>EnableTicketSSLAuth</code>。</p>

表 3-5. Horizon Client 組態範本：安全性設定 (續)

設定	電腦	使用者	說明
Configures SSL protocols and cryptographic algorithms	X	X	<p>設定加密清單，以限制在建立加密 TLS 連線之前對某些密碼編譯演算法和通訊協定的使用。加密清單由一個或多個以冒號分隔的加密字串組成。加密字串須區分大小寫。</p> <p>預設值為 TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES</p> <p>此加密字串表示會啟用 TLS v1.1 和 TLS v1.2，並停用 SSL v.2.0、SSL v3.0 和 TLS v1.0。SSL v2.0、SSL v3.0 和 TLS v1.0 已不再是核准的通訊協定，且會永久停用。</p> <p>加密套件會使用具有 128 位元或 256 位元 AES 的 ECDHE、ECDH 和 RSA。GCM 是慣用模式。</p> <p>如需詳細資訊，請參閱 http://www.openssl.org/docs/apps/ciphers.html。</p> <p>對等的 Windows 登錄值為 SSLCipherList。</p>
Enable Single Sign-On for smart card authentication	X		<p>決定是否啟用智慧卡驗證的單一登入。啟用單一登入時，Horizon Client 會先將加密的智慧卡 PIN 儲存在暫存記憶體中，再提交至連線伺服器。停用單一登入時，Horizon Client 不會顯示自訂 PIN 碼對話方塊。</p> <p>對等的 Windows 登錄值為 EnableSmartCardSSO。</p>
Ignore certificate revocation problems	X	X	<p>決定是否忽略與已撤銷的伺服器憑證相關聯的錯誤。當伺服器傳送的憑證已撤銷，或用戶端無法確認憑證的撤銷狀態時，即會發生這些錯誤。</p> <p>此設定依預設為停用。</p> <p>備註 啟用此設定時，用戶端可能只會在伺服器憑證驗證期間使用快取的 URL。快取的 URL 資訊類型可以是 CRL 發佈點 (CDP) 和授權機構資訊存取 (OCSP 和 CA 簽發者存取方法)。</p>
Unlock remote sessions when the client machine is unlocked	X	X	<p>決定是否啟用「遞迴解除鎖定」功能。遞迴解除鎖定功能可在用戶端機器解除鎖定之後才解除鎖定所有遠端工作階段。在使用者利用「以目前使用者身分登入」功能登入伺服器後才會套用此功能。</p> <p>此設定依預設為啟用。</p>

下列設定會出現在群組原則管理編輯器的 **VMware Horizon Client 組態 > 安全性設定 > NTLM 設定資料** 夾中。

表 3-6. Horizon Client 組態範本：安全性設定、NTLM 驗證設定

設定	電腦	使用者	說明
Allow NTLM Authentication	X		<p>啟用此設定時，以目前使用者身分登入功能會允許 NTLM 驗證。停用此設定時，則不會將 NTLM 驗證用於任何伺服器。</p> <p>啟用此設定時，您可以從允許從 Kerberos 後援至 NTLM 下拉式功能表中選取是或否。</p> <ul style="list-style-type: none"> 如果您選取是，當用戶端無法擷取伺服器的 Kerberos 票證時，即可能使用 NTLM 驗證。 如果您選取否，則僅允許對一律使用 NTLM 伺服器群組原則設定中列出的伺服器執行 NTLM 驗證。 <p>未進行此設定時，則允許對一律使用 NTLM 伺服器群組原則設定中列出的伺服器進行 NTLM 驗證。</p> <p>若要使用 NTLM 驗證，伺服器 SSL 憑證必須是有效的，且 Windows 原則不得限制使用 NTLM。</p> <p>如需如何在連線伺服器執行個體中設定從 Kerberos 後援至 NTLM 的相關資訊，請參閱《VMware Horizon Console 管理》文件中的〈使用隨 Windows 型 Horizon Client 提供的以目前使用者身分登入功能〉。</p>
Always use NTLM for servers	X		<p>啟用此設定時，以目前使用者身分登入功能將一律對列出的伺服器使用 NTLM 驗證。若要建立伺服器清單，請按一下顯示，然後在值資料行中輸入伺服器名稱。伺服器的命名格式為完整網域名稱 (FQDN)。</p>

用戶端 GPO 的 RDP 設定

使用 Microsoft RDP 顯示通訊協定時，您可以為如音訊、印表機、連接埠和其他裝置的重新導向等選項設定群組原則設定。

下表說明 Horizon Client 組態 ADMX 範本檔中的遠端桌面通訊協定 (RDP) 設定。所有 RDP 設定都是「使用者組態」設定。這些設定會出現在群組原則管理編輯器的 **VMware Horizon Client 組態 > RDP 設定** 資料夾中。

表 3-7. Horizon Client 組態管理範本：RDP 設定

設定	說明
Audio redirection	<p>決定是否重新導向遠端桌面平台上播放的音訊資訊。選取下列其中一項設定：</p> <ul style="list-style-type: none"> 停用音訊： 停用音訊。 在虛擬機器中播放 (為 VoIP USB 支援所需)： 在遠端桌面平台內播放音訊。此設定需要共用的 USB 音訊裝置，才能在用戶端上提供聲音。 重新導向至用戶端： 音訊重新導向至用戶端。此設定是預設模式。 <p>此設定僅適用於 RDP 音訊。透過 MMR 重新導向的音訊會在用戶端上播放。</p>
Enable audio capture redirection	<p>決定是否將預設音訊輸入裝置從用戶端重新導向至遠端工作階段。啟用此設定時，用戶端上的錄音裝置會出現在遠端桌面平台上，而且可以錄製音訊輸入。</p> <p>預設設定會遭到停用。</p>

表 3-7. Horizon Client 組態管理範本：RDP 設定 (續)

設定	說明
以 Bitmap cache file size in unit 為單位的, for number bpp bitmaps	<p>指定點陣圖快取的大小 (以 KB 或 MB 為單位), 用於特定的每個畫素位元 (bpp) 點陣圖色彩設定。</p> <p>針對下列單位和 bpp 組合, 提供此設定的不同版本:</p> <ul style="list-style-type: none"> ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
In-memory bitmap cache size in KB for 8bpp bitmaps	<p>指定用於每個像素 8 位元顏色設定的 RAM 點陣圖快取大小 (以 KB 為單位)。如果 ScaleBitmapCachesByBPP 為 true (預設值), 則此快取大小會與每一像素的位元組數相乘, 用以決定實際的 RAM 快取大小。</p> <p>此設定啟用時, 請輸入以 KB 為單位的大小。</p>
Bitmap caching/cache persistence active	決定是否使用持續性點陣圖快取 (作用中)。持續性點陣圖快取可改善效能, 但需要額外的磁碟空間。
Color depth	<p>指定遠端桌面平台的色彩深度。選取下列其中一項可用設定:</p> <ul style="list-style-type: none"> ■ 8 位元 ■ 15 位元 ■ 16 位元 ■ 24 位元 ■ 32 位元
Cursor shadow	決定遠端桌面平台上的指標下方是否出現陰影。
Desktop background	決定用戶端連線到遠端桌面平台時是否出現桌面平台背景。
Desktop composition	<p>決定是否在遠端桌面平台上啟用桌面平台轉譯緩衝處理。</p> <p>啟用桌面平台轉譯緩衝處理時, 個別視窗將不再如舊版 Microsoft Windows 中一般, 直接繪製到螢幕或主要顯示裝置上。繪圖會重新導向至視訊記憶體中的螢幕外介面, 接著再轉譯到桌面平台影像中, 並呈現於顯示器上。</p>
Enable compression	決定是否壓縮 RDP 資料。此設定依預設為啟用。
Enable RDP Auto-Reconnect	決定 RDP 用戶端元件是否在 RDP 通訊協定連線失敗後, 嘗試重新連線到遠端桌面平台。如果已在 Horizon Console 中啟用 使用安全通道連線至桌面平台 選項, 則此設定沒有任何作用。此設定依預設為停用。
Font smoothing	決定是否將消除鋸齒套用於遠端桌面平台上的字型。
Menu and window animation	決定是否在用戶端連線到遠端桌面平台時啟用功能表和視窗的動畫。
Redirect clipboard	決定是否在用戶端連線到遠端桌面平台時重新導向本機剪貼簿資訊。
Redirect drives	<p>決定是否在用戶端連線到遠端桌面平台時重新導向本機磁碟機。預設會重新導向本機磁碟機。</p> <p>啟用此設定或維持此設定不變, 即可將遠端桌面平台上重新導向的磁碟機上的資料複製到用戶端電腦上的磁碟機。如果允許從遠端桌面平台將資料傳遞至使用者的用戶端電腦會在您的部署中暴露出潛在的安全性風險, 請停用此設定。另一種方式是啟用 Microsoft Windows 群組原則設定 Do not allow drive redirection, 藉以停用遠端桌面平台虛擬機器中的資料夾重新導向。</p> <p>Redirect drives 設定僅適用於 RDP。</p>
Redirect printers	決定是否在用戶端連線到遠端桌面平台時重新導向本機印表機。
Redirect serial ports	決定是否在用戶端連線到遠端桌面平台時重新導向本機 COM 連接埠。

表 3-7. Horizon Client 組態管理範本：RDP 設定 (續)

設定	說明
Redirect smart cards	決定是否在用戶端連線到遠端桌面平台時重新導向本機智慧卡。 備註 此設定會同時套用至 RDP 和 PCoIP 連線。
Redirect supported plug-and-play devices	決定是否在用戶端連線到遠端桌面平台時重新導向本機隨插即用和銷售點裝置。此行為與代理程式之 USB 重新導向元件所管理的重新導向不同。
Shadow bitmaps	決定點陣圖是否加上陰影。此設定在全螢幕模式下沒有作用。
Show contents of window while dragging	決定使用者將資料夾拖曳至新位置時是否顯示資料夾內容。
Themes	決定用戶端連線到遠端桌面平台時是否顯示主題。
Windows key combination redirection	決定套用 Windows 組合鍵的位置。 此設定可讓您將組合鍵傳送至遠端虛擬機器，或在本機上套用組合鍵。 依預設組合鍵會套用到本機。
Enable Credential Security Service Provider	指定遠端桌面平台連線是否使用網路層級驗證 (NLA)。如果客體作業系統需要 NLA 以進行遠端桌面平台連線，您必須啟用此設定，否則 Horizon Client 可能無法連線至遠端桌面平台。除了啟用此設定之外，您還必須驗證是否符合下列條件： <ul style="list-style-type: none"> ■ 用戶端和客體作業系統都支援 NLA。 ■ 已啟用連線伺服器執行個體的直接用戶端連線。NLA 不支援通道連線。

用戶端 GPO 的一般設定

一般設定包括 Proxy 選項、時區轉送、多媒體加速和其他顯示設定。

一般設定

下表說明 Horizon Client 組態 ADMX 範本檔中的一般設定。一般設定同時包含「電腦組態」和「使用者組態」設定。「使用者組態」設定會覆寫對等的「電腦組態」設定。這些設定會出現在群組原則管理編輯器的 **VMware Horizon Client 組態** 資料夾中。

表 3-8. Horizon Client 組態範本：一般設定

設定	電腦	使用者	說明
Allow Blast connections to use operating system proxy settings	X		設定對 VMware Blast 連線使用 Proxy 伺服器。 啟用此設定時，VMware Blast 可透過 Proxy 伺服器進行連線。 停用此設定時，VMware Blast 則無法使用 Proxy 伺服器。 未進行此設定 (預設值) 時，使用者可以在 Horizon Client 使用者介面中設定 VMware Blast 連線是否可使用 Proxy 伺服器。請參閱 設定 VMware Blast 選項 。
Allow data sharing	X		啟用此設定時，Horizon Client 使用者介面中的資料共用模式設定會設為「開啟」，且使用者無法變更此設定。 停用此設定時，Horizon Client 使用者介面中的資料共用模式設定會設為「關閉」，且使用者無法變更此設定。 未設定此設定時 (預設值)，使用者可以變更 Horizon Client 使用者介面中的資料共用模式設定。

表 3-8. Horizon Client 組態範本：一般設定 (續)

設定	電腦	使用者	說明
Allow display scaling	X	X	<p>啟用此設定時，系統會針對所有遠端桌面平台和已發佈應用程式啟用顯示調整值功能。</p> <p>停用此設定時，系統會針對所有遠端桌面平台和已發佈的應用程式停用顯示調整值功能。</p> <p>如果未設定此設定 (預設設定)，則使用者可以啟用或停用 Horizon Client 使用者介面中的顯示調整值功能。</p> <p>您也可以透過啟用鎖定客體大小群組原則設定來隱藏 Horizon Client 使用者介面中的顯示調整值喜好設定。如需詳細資訊，請參閱 用戶端 GPO 的指令碼定義設定。</p>
Allow user to skip Horizon Client update	X		<p>指定使用者是否可以在 Horizon Client 更新視窗中按一下略過按鈕。如果使用者按一下略過，則在下一個 Horizon Client 版本可供使用之前，將不會看到另一個更新通知。</p>
Always hide the remote floating language (IME) bar for Hosted Apps	X	X	<p>強制關閉應用程式工作階段的浮動語言列。當此設定啟用時，無論本機 IME 功能是否啟用，已發佈應用程式工作階段中一律不會顯示浮動語言列。當此設定停用時，僅在停用本機 IME 功能時才會顯示浮動語言列。此設定依預設為停用。</p>
Always on top		X	<p>決定 Horizon Client 視窗是否始終是最頂端的視窗。啟用此設定可防止 Windows 工作列遮住全螢幕 Horizon Client 視窗。此設定依預設為停用。</p>
Automatic input focus in a virtual desktop window	X	X	<p>啟用此設定時，如果使用者將遠端桌面平台帶到前端，則 Horizon Client 會自動將輸入傳送至遠端桌面平台。換句話說，焦點不會在視窗的框架中，並且使用者不需再於遠端桌面平台的視窗中按一下來移動焦點。</p>
Automatically check for updates	X		<p>指定是否自動檢查 Horizon Client 的軟體更新。此設定會控制 Horizon Client 更新視窗上的檢查更新並顯示徽章通知核取方塊。此設定依預設為啟用。</p>
Automatically install shortcuts when configured on the Horizon server		X	<p>在連線伺服器執行個體上設定已發佈的應用程式和遠端桌面平台捷徑時，此設定會指定當使用者連線至伺服器時捷徑的安裝方式，以及是否安裝在用戶端機器上。</p> <p>此設定啟用時，系統會在用戶端機器上安裝捷徑。系統不會提示使用者安裝捷徑。</p> <p>此設定停用時，則一律不在用戶端機器上安裝捷徑。系統不會提示使用者安裝捷徑。</p> <p>依預設系統會提示使用者安裝捷徑。</p>
Automatically synchronize the keypad, scroll and caps lock keys	X		<p>此設定啟用時，Num Lock、Scroll Lock 和 Caps Lock 鍵的切換狀態會從用戶端裝置同步至遠端桌面平台。在 Horizon Client 中，系統會選取自動同步數字鍵台、捲軸和 Caps Lock 鍵設定核取方塊，且設定會無法使用。</p> <p>此設定停用時，鎖定鍵切換狀態會從遠端桌面平台同步至用戶端裝置。在 Horizon Client 中，系統會取消選取自動同步數字鍵台、捲軸和 Caps Lock 鍵設定核取方塊，且設定會無法使用。</p> <p>此設定啟用或停用時，使用者將無法在 Horizon Client 中修改自動同步數字鍵台、捲軸和 Caps Lock 鍵設定。</p> <p>若未進行此設定，則使用者可以透過在 Horizon Client 中設定自動同步數字鍵台、捲軸和 Caps Lock 鍵設定，來啟用或停用遠端桌面平台的鎖定鍵同步。請參閱設定鎖定鍵同步。</p> <p>此設定依預設不會設定。</p>

表 3-8. Horizon Client 組態範本：一般設定 (續)

設定	電腦	使用者	說明
Block multiple Horizon Client instances per Windows session	X		防止使用者在 Windows 工作階段期間啟動多個 Horizon Client 執行個體。 此設定啟用時，Horizon Client 會以單一執行個體模式執行，且使用者無法在 Windows 工作階段中啟動多個 Horizon Client 執行個體。 此設定停用時，使用者可以在 Windows 工作階段中啟動多個 Horizon Client 執行個體。此設定依預設為停用。
Configure maximum latency for mouse coalescing	X		設定聯合滑鼠移動事件時所允許的延遲上限 (以毫秒為單位)。有效值為 0 到 50。值為 0 時，系統會停用功能。 聯合滑鼠移動事件可以降低用戶端至代理程式的頻寬使用，但可能會輕微增加滑鼠移動的延遲。 此設定依預設為停用。
Custom error screen footer	X		可讓您在所有 Horizon Client 錯誤訊息的底部新增自訂說明文字。您必須在本機用戶端系統上以純文字 (.txt) 檔案提供說明文字。此文字檔案最多可包含 2048 個字元 (包括控制字元在內)。同時支援 ANSI 和 Unicode 兩種編碼。 此設定啟用時，您可以在顯示的文字方塊中指定含有自訂說明文字的檔案完整路徑，例如 C:\myDocs\errorFooter.txt。 此設定依預設為停用。
Default value of the "Hide the selector after launching an item" check box	X	X	設定是否要依預設選取 啟動項目後隱藏選取器 核取方塊。此設定依預設為停用。
Disable desktop disconnect messages	X	X	指定是否停用遠端桌面平台中斷連線時正常顯示的訊息。這些訊息預設為顯示。
Disable sharing files and folders		X	指定是否可在 Horizon Client 中使用用戶端磁碟機重新導向功能。 此設定啟用時，Horizon Client 中的所有用戶端磁碟機重新導向功能都會停用，包括使用已發佈的應用程式開啟本機檔案的功能。此外，下列是 Horizon Client 使用者介面中隱藏的元素： <ul style="list-style-type: none"> ■ [設定] 對話方塊中的 [共用] 面板。 ■ 遠端桌面平台 選項 功能表中的 共用資料夾 項目。 ■ 系統匣中 Horizon Client 的 共用 項目。 ■ 當您連線至伺服器後，第一次連線至遠端桌面平台或應用程式時所顯示的 [共用] 對話方塊。 此設定停用時，用戶端磁碟機重新導向功能可完全正常運作。此設定依預設為停用。
Disable time zone forwarding	X		決定是否停用遠端桌面平台與已連線用戶端之間的時間區同步處理。
Disable toast notifications	X	X	決定是否停用來自 Horizon Client 的快顯通知。 如果您不希望使用者在螢幕角落看到快顯通知，請啟用此設定。 備註 如果啟用此設定，使用者就不會在「工作階段逾時」功能作用中時看見五分鐘的警告。

表 3-8. Horizon Client 組態範本：一般設定 (續)

設定	電腦	使用者	說明
Disallow passing through client information in a nested session	X		指定是否要防止 Horizon Client 在巢狀工作階段中傳遞用戶端資訊。啟用此設定時，Horizon Client 若是在遠端工作階段內執行，將會傳送實際的實體用戶端資訊，而不是虛擬機器裝置資訊。此設定會套用於下列用戶端資訊：裝置名稱和網域、用戶端類型、IP 位址以及 MAC 位址。依預設會停用此設定，這表示允許在巢狀工作階段中傳遞用戶端資訊。
Display modifier function key	X	X	指定使用者可以按下的切換輔助按鍵和功能鍵組合，以便在 PCoIP 或 VMware Blast 遠端桌面工作階段中擷取並插入輸入時，變更用戶端機器上的顯示組態。 未設定此設定時 (預設設定)，使用者必須使用滑鼠來取消擷取遠端桌面平台，然後按下 Windows 標誌鍵 + P 來選取簡報顯示模式。 此設定不適用於已發佈的應用程式工作階段。
Disable opening local files in hosted applications		X	指定 Horizon Client 是否要登錄主控應用程式支援的副檔名所適用的本機處理常式。 此設定啟用時，Horizon Client 將不會登錄任何副檔名處理常式，且不允許使用者覆寫此設定。 此設定停用時，Horizon Client 一律會登錄副檔名處理常式。依預設，系統會登錄副檔名處理常式，但使用者可在 Horizon Client 使用者介面中停用此功能；方法是在 [設定] 對話方塊的 [共用] 面板上，使用 開啟從本機檔案系統以遠端應用程式開啟本機檔案 的功能設定。如需詳細資訊，請參閱 共用本機資料夾和磁碟機 。 此設定依預設為停用。
Don't check monitor alignment on spanning		X	根據預設，如果畫面合併時未形成精確的矩形，用戶端桌面平台就不會跨越多部監視器。啟用此設定會覆寫預設值。此設定依預設為停用。
Enable multi-media acceleration		X	決定是否在用戶端上啟用多媒體重新導向 (MMR)。 如果 Horizon Client 視訊顯示硬體沒有重疊支援，則 MMR 無法正確運作。
Enable relative mouse	X	X	使用 PCoIP 顯示通訊協定時啟用相對滑鼠。相對滑鼠模式會改進某些圖形應用程式和遊戲的滑鼠行為。如果遠端桌面平台不支援相對滑鼠，則不會使用此設定。此設定依預設為停用。
Enable the shade		X	決定是否顯示 Horizon Client 視窗頂端的「網底」功能表列。此設定依預設為啟用。 備註 「網底」功能表列在 Kiosk 模式下預設為停用狀態。
Enable Horizon Client online update	X		啟用線上更新功能。此設定依預設為啟用。 備註 當您透過命令列安裝 Horizon Client 時，您也可以將 AUTO_UPDATE_ENABLED 內容設為 0 來停用線上更新功能。如需詳細資訊，請參閱 Horizon Client 的安裝內容 。

表 3-8. Horizon Client 組態範本：一般設定 (續)

設定	電腦	使用者	說明
Hide items in application context menu	X	X	<p>針對您在桌面平台和應用程式選取器視窗中，於已發佈的應用程式上按一下滑鼠右鍵時出現的快顯功能表，使用此設定即可隱藏其中的項目。</p> <p>此設定啟用時，您可以設定下列選項：</p> <ul style="list-style-type: none"> ■ 隱藏設定 -- 選取是，可隱藏快顯功能表中的設定項目。 ■ 隱藏建立桌面平台的捷徑 -- 選取是，可隱藏快顯功能表中的建立桌面平台的捷徑項目。 ■ 隱藏新增至 [開始] 功能表 -- 選取是，可隱藏快顯功能表中的新增至 [開始] 功能表項目。 ■ 隱藏標記為我的最愛 -- 選取是，可隱藏快顯功能表中的標記為我的最愛項目。 <p>此設定依預設為停用。</p>
Hide items in desktop context menu	X	X	<p>針對您在桌面平台和應用程式選取器視窗中，於遠端桌面平台上按一下滑鼠右鍵時出現的快顯功能表，使用此設定即可隱藏其中的項目。</p> <p>此設定啟用時，您可以設定下列選項：</p> <ul style="list-style-type: none"> ■ 隱藏重設桌面平台 -- 選取是，可隱藏快顯功能表中的重設桌面平台項目。 ■ 隱藏重新啟動桌面平台 -- 選取是，可隱藏快顯功能表中的重新啟動桌面平台項目。 ■ 隱藏顯示 -- 選取是，可隱藏快顯功能表中的顯示項目。 ■ 隱藏設定 -- 選取是，可隱藏快顯功能表中的設定項目。 ■ 隱藏建立桌面平台的捷徑 -- 選取是，可隱藏快顯功能表中的建立桌面平台的捷徑項目。 ■ 隱藏新增至 [開始] 功能表 -- 選取是，可隱藏快顯功能表中的新增至 [開始] 功能表項目。 ■ 隱藏標記為我的最愛 -- 選取是，可隱藏快顯功能表中的標記為我的最愛項目。 <p>此設定依預設為停用。</p>
Hide items in desktop toolbar	X	X	<p>使用此設定即可隱藏遠端桌面平台視窗中功能表列上的項目。</p> <p>此設定啟用時，您可以設定下列選項。</p> <ul style="list-style-type: none"> ■ 隱藏說明 -- 選取是，可隱藏選項功能表中的說明項目。 ■ 隱藏支援資訊 -- 選取是，可隱藏選項功能表中的支援資訊項目。 ■ 隱藏已啟用的相對滑鼠 -- 選取是，可隱藏選項功能表中的啟用相對滑鼠項目。 ■ 隱藏共用資料夾 -- 選取是，可隱藏選項功能表中的共用資料夾項目。 ■ 隱藏允許顯示調整值 -- 選取是，可隱藏選項功能表中的允許顯示調整值項目。 ■ 隱藏重設桌面平台 -- 選取是，可隱藏選項功能表中的重設桌面平台項目。 ■ 隱藏重新啟動桌面平台 -- 選取是，可隱藏選項功能表中的重新啟動桌面平台項目。 ■ 隱藏連線 USB 裝置 -- 選取是，可隱藏功能表列中的連線 USB 裝置功能表。 <p>此設定依預設為停用。</p>

表 3-8. Horizon Client 組態範本：一般設定 (續)

設定	電腦	使用者	說明
Hide items in system tray menu	X	X	<p>針對您在本機用戶端系統上，於系統匣中的 Horizon Client 圖示上按一下滑鼠右鍵時出現的快顯功能表，使用此設定即可隱藏其中的項目。</p> <p>此設定啟用時，您可以設定下列選項。</p> <ul style="list-style-type: none"> ■ 隱藏共用 -- 選取是，可隱藏 Horizon Client 的共用項目。 ■ 隱藏設定 -- 選取是，可隱藏 Horizon Client 的設定項目。 <p>此設定依預設為停用。</p>
Hide items in the client toolbar menu	X	X	<p>使用此設定即可隱藏桌面平台和應用程式選取器視窗頂端工具列中的項目。</p> <p>此設定啟用時，您可以設定下列選項。</p> <ul style="list-style-type: none"> ■ 隱藏我的最愛切換 -- 選取是，可隱藏顯示我的最愛 (星形) 圖示。 ■ 隱藏設定齒輪 -- 選取是，可隱藏設定 (齒輪) 圖示。 <p>此設定依預設為停用。</p>
Hotkey combination to grab input focus	X	X	<p>設定快速鍵組合，來為上次使用的 PCoIP 或 VMware Blast 遠端桌面工作階段擷取輸入焦點。快速鍵包括一或兩個輔助按鍵以及一個字母鍵。</p> <p>停用或未設定此設定時，使用者可藉由在遠端桌面平台的視窗內部按一下來擷取焦點。此設定依預設不會設定。</p>
Hotkey combination to release input focus	X	X	<p>設定快速鍵組合，以從 PCoIP 或 VMware Blast 遠端桌面工作階段釋放輸入焦點。快速鍵包括一到兩個輔助按鍵以及一個功能鍵。</p> <p>停用或未設定此設定時，使用者可以透過按下 Ctrl+Alt 或在遠端桌面平台的視窗外部按一下來釋放焦點。此設定依預設不會設定。</p>
Pin the shade		X	<p>決定是否啟用 Horizon Client 視窗頂端的釘住網底功能，且不會自動隱藏功能表列。如果停用網底，則此設定沒有作用。此設定依預設為啟用。</p>
Save resolution and DPI to server	X		<p>決定 Horizon Client 是否會在伺服器上儲存自訂顯示解析度和顯示調整值設定。如需自訂遠端桌面平台的顯示解析度和顯示調整值設定的相關資訊，請參閱自訂遠端桌面平台的顯示解析度和顯示調整值。</p> <p>啟用此設定時，如果已為遠端桌面平台自訂顯示解析度或顯示調整值，則每次使用者開啟遠端桌面平台時，無論使用者用來登入至遠端桌面平台的用戶端裝置為何，系統皆會自動套用自訂設定。</p> <p>此設定依預設為停用。</p>
Tunnel proxy bypass address list	X		<p>指定通道位址的清單。Proxy 伺服器不會用於這些位址。請使用分號 (;) 分隔多個項目。</p>
Update message pop-up	X		<p>指定在有新版本的 Horizon Client 可供使用時，是否自動向使用者顯示更新快顯訊息。此設定會控制 Horizon Client 更新視窗上的當有更新時，顯示快顯訊息核取方塊。此設定依預設為停用。</p>
URL for Horizon Client online help	X		<p>指定 Horizon Client 可從中擷取說明頁面的替代 URL。此設定主要用於無法擷取遠端主控說明系統的環境，因為這類環境沒有網際網路存取。</p>
URL for Horizon Client online update	X		<p>指定 Horizon Client 可從中擷取更新的替代 URL。此設定適用於定義其自有私人/個人更新中心的環境中。若未啟用此設定，將會使用 VMware 官方更新伺服器。</p>

用戶端 GPO 的 USB 設定

您可以為 Horizon Agent 和 Horizon Client 定義 USB 原則設定。在連線時，Horizon Client 會從 Horizon Agent 下載 USB 原則設定，並將這些設定與 Horizon Client USB 原則設定搭配使用，以決定可使用哪些裝置從主機重新導向。

用於分割複合 USB 裝置的原則設定

下表說明 Horizon Client 組態 ADMX 範本檔中用來分割複合 USB 裝置的每個原則設定。此設定適用於電腦層級。GPO 中屬於電腦層級的設定會優先於 HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB 上的登錄。這些設定會出現在群組原則管理編輯器的 **VMware Horizon Client 組態 > View USB 組態** 資料夾中。

如需關於使用原則來控制 USB 重新導向的詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

表 3-9. Horizon Client 組態範本：USB 分割設定

設定	說明
Allow Auto Device Splitting	允許複合 USB 裝置的自動分割。 該預設值未定義，其相當於 false 。
Exclude Vid/Pid Device From Split	排除依照廠商和產品識別碼指定的複合 USB 裝置，不進行分割。設定的格式為 <code>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]..</code> 您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 例如: vid-0781_pid-55** 該預設值未定義。
Split Vid/Pid Device	將依照廠商和產品識別碼指定的複合 USB 裝置元件視為個別裝置。設定格式為 <code>vid-xxxx_pid-yyy(exintf:zz[;exintf:ww])</code> 您可以使用 exintf 關鍵字，藉由指定他們的介面號碼來將元件自重新導向清單中排除。您必須以十六進位指定識別碼，及以十進位指定介面號碼，包括任何前置的 0。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。 例如: vid-0781_pid-554c(exintf:01;exintf:02) 備註 Horizon 不會自動包含您未明確排除的元件。您必須指定篩選原則，例如 Include Vid/Pid Device ，以納入那些元件。 該預設值未定義。

用於篩選 USB 裝置的原則設定

下表說明 Horizon Client 組態 ADMX 範本檔中用來篩選 USB 裝置的原則設定。此設定適用於電腦層級。GPO 中屬於電腦層級的設定會優先於 HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB 上的登錄。

如需關於為 USB 重新導向設定篩選原則設定的詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

表 3-10. Horizon Client 組態範本：USB 篩選設定

設定	說明
Allow Audio Input Devices	<p>允許將音訊輸入裝置重新導向。</p> <p>該預設值未定義，其相當於 true。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Allow Audio Output Devices	<p>允許將音訊輸出裝置重新導向。</p> <p>該預設值未定義，其相當於 false。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Allow HID-Bootable	<p>允許將鍵盤或滑鼠以外在啟動時可使用的輸入裝置 (亦稱為 HID 可開機裝置) 重新導向。</p> <p>該預設值未定義，其相當於 true。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Allow Device Descriptor Failsafe Behavior	<p>即使在 Horizon Client 無法取得 config/device 描述元時，仍允許重新導向裝置。</p> <p>若要在無法取得組態/描述元的情形允許裝置，請將其納入 Include 篩選器當中，例如 IncludeVidPid 或 IncludePath。</p> <p>該預設值未定義，其相當於 false。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 > 無法由代理程式設定的設定 資料夾中。</p>
Allow Other Input Devices	<p>允許重新導向隱藏式可開機裝置或具備整合式指標裝置之鍵盤以外的輸入裝置。</p> <p>該預設值未定義，其相當於 true。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Allow Keyboard and Mouse Devices	<p>允許將整合指向裝置 (例如滑鼠、軌跡球或觸控板) 的鍵盤重新導向。</p> <p>該預設值未定義，其相當於 false。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Allow Smart Cards	<p>允許將智慧卡裝置重新導向。</p> <p>該預設值未定義，其相當於 false。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Allow Video Devices	<p>允許將視訊裝置重新導向。</p> <p>該預設值未定義，其相當於 true。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Disable Remote Configuration	<p>當執行 USB 裝置篩選時，請將代理程式設定的使用設為停用。</p> <p>該預設值未定義，其相當於 false。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 > 無法由代理程式設定的設定 資料夾中。</p>

表 3-10. Horizon Client 組態範本：USB 篩選設定 (續)

設定	說明
Exclude All Devices	<p>排除所有 USB 裝置，避免重新導向。如果設定為 true，您可以使用其他原則設定，以允許將特定裝置或裝置系列重新導向。如果設定為 false，您可以使用其他原則設定，以避免將特定裝置或裝置系列重新導向。</p> <p>如果在代理程式上將 Exclude All Devices 的值設為 true，且此設定已傳遞至 Horizon Client，則代理程式設定會覆寫 Horizon Client 設定。</p> <p>該預設值未定義，其相當於 false。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Exclude Automatically Connection Device Family	<p>排除裝置系列以避免自動轉送。使用下列語法：</p> <pre>family-name[;...]</pre> <p>例如：</p> <pre>storage;hid</pre>
Exclude Automatically Connection Vid/Pid Device	<p>排除具有特定廠商和產品識別碼的裝置，以避免自動轉送。使用下列語法：</p> <pre>vid-xxxx_pid-xxx *[*;...]</pre> <p>例如：</p> <pre>vid-0781_pid-554c;vid-0781_pid-9999</pre>
Exclude Device Family	<p>排除裝置系列，避免重新導向。設定的格式為 <i>family_name_1[;family_name_2]...</i></p> <p>例如：bluetooth;smart-card</p> <p>如果您已啟用自動裝置分割功能，則 Horizon 會檢查複合 USB 裝置各個介面的裝置系列，以決定要排除的介面。如果您已經停用自動裝置分割功能，Horizon 便會檢驗整個複合 USB 裝置的裝置系列。</p> <p>該預設值未定義。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Exclude Vid/Pid Device	<p>排除具有特定廠商和產品識別碼的裝置，以避免重新導向。設定的格式為 <i>vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</i></p> <p>您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。</p> <p>例如：vid-0781_pid-***;vid-0561_pid-554c</p> <p>該預設值未定義。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Exclude Path	<p>排除位於特定集線器或連接埠路徑上的裝置，避免重新導向。設定的格式為 <i>bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2]...</i></p> <p>您必須以十六進位指定匯流排和連接埠號碼。您不能在路徑中使用萬用字元。</p> <p>例如：bus-1/2/3_port-02;bus-1/1/4_port-ff</p> <p>該預設值未定義。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 > 無法由代理程式設定的設定 資料夾中。</p>

表 3-10. Horizon Client 組態範本：USB 篩選設定 (續)

設定	說明
Include Device Family	<p>納入可重新導向的裝置系列。設定的格式為 <i>family_name_1</i>;<i>family_name_2</i>...</p> <p>例如: storage</p> <p>該預設值未定義。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>
Include Path	<p>納入位於特定集線器或連接埠路徑上並可重新導向的裝置。設定的格式為 <i>bus-x1</i>[/<i>y1</i>].../<i>port-z1</i>;<i>bus-x2</i>[/<i>y2</i>].../<i>port-z2</i>]...</p> <p>您必須以十六進位指定匯流排和連接埠號碼。您不能在路徑中使用萬用字元。</p> <p>例如: bus-1/2_port-02;bus-1/7/1/4_port-0f</p> <p>該預設值未定義。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 > 無法由代理程式設定的設定 資料夾中。</p>
Include Vid/Pid Device	<p>指定具有指定廠商和產品識別碼且可重新導向的 USB 裝置。設定的格式為 <i>vid-xxx1_pid-yyy2</i>;<i>vid-xxx2_pid-yyy2</i>]...</p> <p>您必須以十六進位指定識別碼。您可以在識別碼中使用萬用字元 (*) 以取代個別數字。</p> <p>例如: vid-0561_pid-554c</p> <p>該預設值未定義。</p> <p>此設定會出現在群組原則管理編輯器的 VMware Horizon Client 組態 > View USB 組態 資料夾中。</p>

巢狀工作階段的考量事項

在巢狀模式或雙躍點案例中，使用者會從實體用戶端系統連線至遠端桌面平台、在遠端桌面平台 (巢狀工作階段) 內啟動 Horizon Client，以及連線至另一個遠端桌面平台。若要讓裝置在巢狀工作階段中如預期般運作，您必須在實體用戶端電腦上和巢狀工作階段中以相同的方式設定 USB 原則設定。

用戶端 GPO 的 VMware Browser 重新導向設定

您可以為瀏覽器重新導向功能設定群組原則設定。

下表說明 Horizon Client 組態 ADMX 範本檔中的瀏覽器重新導向設定。所有瀏覽器重新導向設定皆為電腦組態設定。這些設定會出現在群組原則管理編輯器的 **VMware Horizon Client 組態 > VMware Browser 重新導向** 資料夾中。

如需代理程式端瀏覽器重新導向設定的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

表 3-11. Horizon Client 組態範本：VMware Browser 重新導向設定

設定	說明
Enable WebRTC camera and microphone access for browser redirection	此設定啟用時，使用 WebRTC 的重新導向頁面將可存取用戶端系統的相機和麥克風。 此設定依預設為啟用。
Ignore certificate errors for browser redirection	此設定啟用時，會忽略重新導向的頁面中發生的憑證錯誤，並繼續瀏覽。 此設定依預設為停用。
Enable cache for browser redirection	此設定啟用時，瀏覽歷程記錄 (包括 Cookie) 會儲存在用戶端系統上。 備註 停用此設定不會清除快取。如果先停用然後重新啟用此設定，那麼將重複使用快取。 此設定依預設為啟用。

用戶端 GPO 的 VMware Integrated Printing 設定

您可以為 VMware Integrated Printing 功能設定群組原則設定。

下表說明 Horizon Client 組態 ADMX 範本檔中的 VMware Integrated Printing 設定。該表格說明設定是同時包含「電腦組態」和「使用者組態」設定，還是僅包含「電腦組態」設定。對於兩種設定的設定而言，「使用者組態」設定會覆寫同等的「電腦組態」設定。這些設定會出現在群組原則管理編輯器的 **VMware Horizon Client 組態 > VMware Integrated Printing** 資料夾中。

如需設定 VMware Integrated Printing 設定的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

表 3-12. Horizon Client 組態範本：VMware Integration Printing 設定

設定	電腦	使用者	說明
Do not redirect client printer(s)	X	X	決定是否重新導向用戶端印表機。 此設定啟用時，將不會重新導向用戶端印表機。停用或未進行此設定時，則會重新導向所有用戶端印表機。 此設定依預設不會設定。
Allow to redirect L1 local printers to inner session	X	X	決定是否將 L1 本機印表機重新導向至內部工作階段。 VMware 支援在遠端桌面平台內執行 Horizon Client。此組態通常稱為巢狀模式，涉及三個階層與兩個躍點，如下所示： <ul style="list-style-type: none"> ■ L0 (端點) - 安裝 Horizon Client 所在的實體機器。 ■ L1 (第一個躍點遠端桌面平台) - 安裝 Horizon Client 和 Horizon Agent 所在的遠端桌面平台。 ■ L2 (第二個躍點已發佈的桌面平台或已發佈的應用程式) - 第二個躍點用戶端連線的已發佈的桌面平台或已發佈的應用程式。 啟用此設定時，L1 本機印表機即會重新導向至內部工作階段。未設定或停用此設定時，L1 本機印表機不會重新導向至內部工作階段。 此設定依預設不會設定。

PCoIP 用戶端工作階段變數 ADMX 範本設定

PCoIP 用戶端工作階段變數 ADMX 範本檔 (pcoip.client.admx) 中包含與 PCoIP 顯示通訊協定相關的原則設定。您可以設定管理員可以覆寫的電腦預設值，或者，您可以設定管理員無法覆寫的使用者設定。

可覆寫的設定會出現在群組原則管理編輯器的 **PCoIP 用戶端工作階段變數 > 可覆寫的管理員預設值** 資料夾中。無法覆寫的設定會出現在群組原則管理編輯器的 **PCoIP 用戶端工作階段變數 > 未覆寫的設定** 資料夾中。

ADMX 檔案可從 VMware-Horizon-Extras-Bundle-YMMM-x.x.x-yyyyyy.zip 中取得，而您可以從 VMware 下載網站下載該 zip 檔案，網址為 <https://my.vmware.com/web/vmware/downloads>。在 [桌面平台及終端使用者運算] 下，選取 VMware Horizon 下載，其中有包含 ZIP 檔案的 GPO 服務包。

表 3-13. PCoIP 用戶端工作階段變數

設定	說明
Configure PCoIP client image cache size policy	<p>控制 PCoIP 用戶端映像快取的大小。用戶端會使用映像快取，儲存之前傳輸的顯示部分。映像快取可減少重複傳輸的資料量。</p> <p>當此設定停用時，PCoIP 會使用預設的用戶端影像快取大小 (250 MB)。</p> <p>當您啟用此設定時，可以在最小 50 MB 到最大 300 MB 之間設定用戶端映像快取大小。預設值為 250 MB。</p> <p>此設定依預設為停用。</p>
Configure PCoIP event log cleanup by size in MB	<p>啟用依 PCoIP 事件記錄的大小 (MB) 進行清理的組態。此設定經設定後，將會依大小 (MB) 控制記錄檔清理。例如，如果 <i>m</i> 設為非零值，則會以無訊息方式刪除大於 <i>m</i> MB 的記錄檔。設為 0 表示不會依據大小清理檔案。當此設定停用時，預設的依大小 (MB) 事件記錄清理設定為 100。此設定依預設為停用。</p>
Configure PCoIP event log cleanup by time in days	<p>啟用依 PCoIP 事件記錄的時間 (天數) 進行清理的組態。此設定經設定後，將會依時間 (天數) 控制記錄檔清理。例如，如果 <i>n</i> 設為非零值，則會以無訊息方式刪除存留超過 <i>n</i> 天的記錄檔。設為 0 表示不會依據時間清理檔案。當此原則停用時，預設的依時間 (天數) 事件記錄清理設定為 7。此設定依預設為停用。</p> <p>記錄檔清理會在工作階段啟動時執行一次。在下一個工作階段開始之前不會套用對此設定所做的任何變更。</p>
Configure PCoIP event log verbosity	<p>設定 PCoIP 事件記錄詳細資訊。值的範圍為 0 (最不詳細) 至 3 (最詳細)。</p> <p>當此設定啟用時，您可以設定從 0 到 3 的詳細資訊等級。當此設定停用時，預設的事件記錄詳細資訊等級為 2。此設定依預設為停用。</p> <p>在作用中的 PCoIP 工作階段期間修改此設定時，新設定會立即生效。</p>
Configure PCoIP session encryption algorithms	<p>控制 PCoIP 端點在工作階段交涉期間公告的加密演算法。</p> <p>選取其中一個核取方塊即會停用相關聯的加密演算法。您必須至少啟用一種演算法。</p> <p>此設定會同時套用於代理程式和用戶端。端點會交涉所使用的實際工作階段加密演算法。如果啟用 FIPS140-2 核准模式，則在 AES-128-GCM 加密和 AES-256-GCM 加密皆停用時，將會覆寫停用 AES-128-GCM 加密值。</p> <p>Configure SSL Connections 設定停用時，Salsa20-256round12 和 AES-128-GCM 演算法都可用於此端點的交涉。此設定依預設為停用。</p> <p>按喜好順序，支援的加密演算法為 SALSA20/12-256、AES-GCM-128 和 AES-GCM-256。依預設，所有支援的加密演算法均可供此端點用於交涉。</p>

表 3-13. PCoIP 用戶端工作階段變數 (續)

設定	說明
Configure PCoIP virtual channels	<p>指定可以及無法透過 PCoIP 工作階段操作的虛擬通道。此設定也會決定是否停用 PCoIP 主機上的剪貼簿處理。</p> <p>PCoIP 工作階段中使用的虛擬通道必須出現在虛擬通道授權清單中。出現在未授權虛擬通道清單中的虛擬通道無法在 PCoIP 工作階段中使用。</p> <p>您最多可以指定 15 個在 PCoIP 工作階段中使用的虛擬通道。</p> <p>請使用分隔號 () 字元分隔多個通道名稱。例如，允許 mksvchan 和 vdp_rdpvcbridge 虛擬通道的虛擬通道授權字串為 mksvchan vdp_rdpvcbridge。</p> <p>如果通道名稱包含分隔號或反斜線 (\) 字元，請在前面插入反斜線字元。例如，通道名稱 awkward \channel 輸入為 awk\ ward\channel。</p> <p>授權的虛擬通道清單為空白時，表示不允許所有虛擬通道。未授權的虛擬通道清單為空白時，表示允許所有虛擬通道。</p> <p>虛擬通道設定會同時套用至代理程式和用戶端。代理程式和用戶端上的虛擬通道都必須啟用，才能使用虛擬通道。</p> <p>虛擬通道設定會另外提供一個核取方塊，讓您停用 PCoIP 主機上的遠端剪貼簿處理。此值僅適用於代理程式。</p> <p>依預設，會啟用所有虛擬通道，包括剪貼簿處理。</p>
Configure SSL cipher list	<p>設定 TLS/SSL 加密清單，以限制在建立加密 TLS/SSL 連線之前對於加密套件的使用。清單由一或多個以冒號分隔的加密套件字串組成。所有加密套件字串皆不區分大小寫。</p> <p>預設值為 ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH。</p> <p>如果進行此設定，則會忽略 Configure SSL connections to satisfy Security Tools 設定中的強制執行用於 SSL 連線交涉的 AES-256 或更強的加密核取方塊。</p> <p>此設定必須同時套用到 PCoIP 伺服器 and PCoIP 用戶端。</p>
Configure SSL connections to satisfy Security Tools	<p>指定建立 TLS 工作階段交涉連線的方式。為符合安全工具 (例如連接埠掃描器) 的需求，請啟用此設定，並執行下列動作：</p> <ol style="list-style-type: none"> 將簽署了任何要用於 PCoIP 之伺服器憑證的憑證授權機構所包含的憑證，儲存在「受信任的根憑證」憑證存放區中。 設定代理程式，使其僅從憑證存放區載入憑證。如果使用的是本機電腦的個人存放區，請將 CA 憑證存放區名稱保持不變為值 ROOT，除非您在步驟 1 使用了不同的存放區位置。 <p>此設定停用時，AES-128 加密套件將無法使用，且端點將會使用機器帳戶的 MY 存放區中的「憑證授權機構」憑證和 ROOT 存放區中的「憑證授權機構」憑證。此設定依預設為停用。</p>
Configure SSL protocols	<p>設定 OpenSSL 通訊協定，以限制在建立加密 TLS 連線之前對特定通訊協定的使用。通訊協定清單由一個或多個以冒號分隔的 OpenSSL 通訊協定字串組成。所有加密字串皆不區分大小寫。</p> <p>預設值為 TLS1.1:TLS1.2，這表示已啟用 TLS v1.1 和 TLS v1.2，並停用 SSL v2.0、SSLv3.0 和 TLS v1.0。</p> <p>如果同時在用戶端和代理程式上設定此設定，則會遵循 OpenSSL 通訊協定交涉規則。</p>
Configure the Client PCoIP UDP port	<p>指定軟體 PCoIP 用戶端使用的 UDP 用戶端連接埠。UDP 連接埠值會指定要使用的基礎 UDP 連接埠。如果基礎連接埠無法使用，則會由 UDP 連接埠範圍值決定要額外嘗試多少個連接埠。</p> <p>此範圍從基礎連接埠跨越至基礎連接埠和連接埠範圍的總和。例如，如果基礎連接埠為 50002 且連接埠範圍為 64，則範圍會從 50002 跨越至 50066。</p> <p>此設定僅適用於用戶端。</p> <p>根據預設，基礎連接埠為 50002 且連接埠範圍為 64。</p>

表 3-13. PCoIP 用戶端工作階段變數 (續)

設定	說明
Configure the maximum PCoIP session bandwidth	<p>指定 PCoIP 工作階段中的最大頻寬 (單位 KB/秒)。頻寬包括所有映像處理、音訊、虛擬通道、USB 和控制 PCoIP 流量。</p> <p>請將此值設定為端點所連線之連結的整體容量，並考量預期的並行 PCoIP 工作階段數目。例如，單一使用者的 VDI 組態 (即單一 PCoIP 工作階段) 是透過 4Mbit/s 網際網路連線來連線時，請將此值設為 4Mbit，或設定一個比此值低 10% 的值，留一些空間供其他網路流量使用。當您預期會有多個並行 PCoIP 工作階段共用一個包含多個 VDI 使用者或單一 RDS 組態的連結時，可能需要相應地調整此設定。但是，降低此值會限制每個作用中工作階段的最大頻寬。</p> <p>設定此值可防止代理程式嘗試以高於連結容量的速率傳輸，這樣可能造成大量封包遺失並產生較差的使用者體驗。此值為對稱的。它會強制用戶端和代理程式使用用戶端和代理程式端上所設定的兩個值中的較低者。例如，將最大頻寬設定為 4Mbit/s 會強制代理程式以較低速率傳輸，即使該設定是在用戶端上設定的也一樣。</p> <p>在端點上停用此設定時，端點將不會實施任何頻寬限制。當此設定啟用時，設定會用作端點的最大頻寬限制 (單位為 kbps)。</p> <p>預設值為 900000 kbps。</p> <p>此設定會套用於代理程式和用戶端。如果兩個端點擁有不同的設定，則會使用較小的值。</p>
Configure the PCoIP session bandwidth floor	<p>指定 PCoIP 工作階段所保留頻寬的下限 (單位為每秒 kb)。</p> <p>此設定會設定端點的預期最小頻寬傳輸速率。當您使用此設定保留端點的頻寬時，使用者就不必等待可用的頻寬，如此就能改善工作階段的回應能力。</p> <p>請確認不要過度訂閱所有端點的總保留頻寬。確定組態中所有連線的頻寬下限總和未超過網路能力。預設值為 0，表示未保留最小頻寬。當此設定停用時，系統不會保留最小頻寬。此設定依預設為停用。</p> <p>此設定會套用於代理程式和用戶端，但是只會影響設定此設定所在的端點。</p> <p>在作用中的 PCoIP 工作階段期間修改此設定時，變更會立即生效。</p>
Configure the PCoIP session MTU	<p>針對 PCoIP 工作階段的 UDP 封包，指定傳輸單元最大值 (MTU) 大小。</p> <p>MTU 大小包括 IP 和 UDP 封包標頭。TCP 會使用標準 MTU 探索機制設定 MTU，而此設定不會對其造成影響。</p> <p>MTU 大小的最大值為 1500 個位元組。MTU 大小的最小值為 500 個位元組。預設值為 1300 個位元組。</p> <p>通常您不需要變更 MTU 大小。如果您使用非一般的網路設定而造成 PCoIP 封包分段，請變更此值。</p> <p>此設定會套用於代理程式和用戶端。如果兩個端點擁有不同的 MTU 大小設定，則會使用最小的值。</p> <p>如果停用或未設定此設定，用戶端會使用預設值與代理程式交涉。</p>

表 3-13. PCoIP 用戶端工作階段變數 (續)

設定	說明
Configure the PCoIP transport header	<p>設定 PCoIP 傳輸標頭以及設定傳輸工作階段優先順序。</p> <p>PCoIP 傳輸標頭為 32 位元標頭，會新增至所有 PCoIP UDP 封包 (但只有在傳輸標頭已啟用且雙方皆支援時)。PCoIP 傳輸標頭會允許網路裝置在處理網路壅塞時決定較佳的優先順序/QoS。傳輸標頭預設為啟用。</p> <p>傳輸工作階段優先順序會決定 PCoIP 傳輸標頭報告的 PCoIP 工作階段優先順序。網路裝置會根據指定的傳輸工作階段優先順序，決定較佳的優先順序/QoS。</p> <p>啟用 Configure the PCoIP transport header 設定時，可使用下列傳輸工作階段優先順序：</p> <ul style="list-style-type: none"> ■ 高 ■ 中 (預設值) ■ 低 ■ 未定義 <p>PCoIP 代理程式和用戶端交涉傳輸工作階段優先順序值。如果 PCoIP 代理程式指定了傳輸工作階段優先順序值，則工作階段會使用代理程式所指定的工作階段優先順序。如果只有用戶端指定了傳輸工作階段優先順序，則工作階段會使用用戶端所指定的工作階段優先順序。如果代理程式和用戶端都沒有指定傳輸工作階段優先順序，或是指定了未定義優先順序，則工作階段會使用預設值，即中優先順序。</p>
Enable/disable audio in the PCoIP session	<p>決定是否在 PCoIP 工作階段中啟用音訊。兩個端點都必須啟用音訊。啟用此設定時，會允許 PCoIP 音訊。停用此設定時，會停用 PCoIP 音訊。依預設會啟用音訊。</p>

從命令列執行 Horizon Client

您可以透過命令列或指令碼執行 Horizon Client。如果您要實作以 Kiosk 為基礎的應用程式，而且其允許使用者存取遠端桌面平台應用程式，則可以從命令列執行 Horizon Client。

若要從命令列執行 Horizon Client，您可以使用 `vmware-view.exe` 命令。`vmware-view.exe` 命令包含您可以指定以變更 Horizon Client 行為的選項。

Horizon Client 命令使用

`vmware-view` 命令的語法會控制 Horizon Client 的作業。

在 Windows 命令提示字元中使用 `vmware-view` 命令的下列格式。

```
vmware-view [command_line_option [argument]] ...
```

`vmware-view` 命令可執行檔案的預設路徑視用戶端系統而定。您可以將此路徑新增至用戶端系統上的 `PATH` 環境變數。

- 32 位元系統: C:\Program Files\VMware\VMware Horizon View Client\
- 64 位元系統: C:\Program Files (x86)\VMware\VMware Horizon View Client\

下表顯示您能夠與 `vmware-view` 命令搭配使用的命令列選項。

表 3-14. Horizon Client 命令列選項

選項	說明
/?	顯示命令選項的清單。
-appName <i>application_name</i>	指定已發佈的應用程式顯示於桌面平台和應用程式選取視窗中的名稱。此名稱是在集區建立精靈中為應用程式集區指定的顯示名稱。
-appProtocol <i>protocol</i>	指定要使用的已發佈應用程式顯示通訊協定 (如果有的話)。有效的通訊協定如下： <ul style="list-style-type: none"> ■ VMware Blast ■ PCoIP
-appSessionReconnectionBehavior <i>argument</i>	指定已發佈應用程式的重新連線行為設定。有效引數如下： <p>always 實作自動重新連線以開啟應用程式設定。</p> <p>never 實作不要求重新連線，且不自動重新連線設定。</p> <p>ask 實作要求重新連線以開啟應用程式設定。</p> <p>使用此選項時，Horizon Client 會停用已發佈應用程式的重新連線設定。</p>
-args <i>argument</i>	指定在已發佈的應用程式啟動時要新增的命令列引數。例如： <pre>vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""</pre>
-connectUSBOnStartup	設定為 true 時，會將連線至主機的所有 USB 裝置重新導向至遠端桌面平台或已發佈的應用程式。如果您為遠端桌面平台指定 -unattended 選項，則會隱含地設定此選項。預設值為 false 。
-connectUSBOnInsert	當設定為 true 且您插入 USB 裝置時，系統會將該裝置連線至前景遠端桌面平台或已發佈的應用程式。如果您為遠端桌面平台指定 -unattended 選項，則會隱含地設定此選項。預設值為 false 。
-desktopLayout <i>window_size</i>	指定顯示遠端桌面平台視窗的方式。有效的視窗大小值如下： <p>fullscreen 全螢幕顯示。</p> <p>multimonitor 多台監視器顯示。</p> <p>windowLarge 大視窗。</p> <p>windowSmall 小視窗。</p> <p>length X width 自訂大小，例如 800 X 600。</p>
-desktopName <i>desktop_name</i>	指定遠端桌面平台顯示於桌面平台和應用程式選取視窗中的名稱。此名稱即為在集區建立精靈中為集區指定的顯示名稱。 <p>重要 請不要在 Kiosk 模式下為用戶端指定此選項。當遠端桌面平台以 Kiosk 模式執行時，此選項無效。在 Kiosk 模式下，系統會與授權的遠端桌面平台清單中的第一個遠端桌面平台建立連線。</p>
-desktopProtocol <i>protocol</i>	指定所要使用、將在桌面平台和應用程式選取視窗中顯示的顯示通訊協定。有效的顯示通訊協定如下： <ul style="list-style-type: none"> ■ Blast ■ PCoIP ■ RDP

表 3-14. Horizon Client 命令列選項 (續)

選項	說明
<code>-domainName domain_name</code>	指定使用者登入 Horizon Client 所使用的 NETBIOS 網域。例如，使用 <code>mycompany</code> 而非 <code>mycompany.com</code> 。
<code>-file file_path</code>	指定含有額外命令選項和引數的組態檔案路徑。請參閱 Horizon Client 組態檔 。
<code>-h</code>	顯示說明選項。
<code>-hideClientAfterLaunchSession</code>	設定為 <code>true</code> 時，在啟動遠端工作階段之後，將會隱藏桌面平台和應用程式選取器視窗，以及顯示 VMware Horizon Client 功能表。設定為 <code>false</code> 時，在啟動遠端工作階段之後，將會顯示桌面平台和應用程式選取器視窗，以及顯示 VMware Horizon Client 功能表。預設值為 <code>true</code> 。
<code>-installShortcutsThenQuit</code>	<p>使用此選項可安裝伺服器上所設定的桌面平台和應用程式捷徑。當您搭配使用此選項與足夠的伺服器驗證資訊時，Horizon Client 會以無訊息方式連線至伺服器、安裝捷徑，然後結束。如果伺服器驗證失敗，則 Horizon Client 會以無訊息方式結束。</p> <p>若要在用戶端系統上自動安裝捷徑，請建立會在用戶端系統啟動時執行的指令碼。例如：</p> <pre>vmware-view.exe -serverURL serverurl -userName user -domainName domain -password password -installShortcutsThenQuit vmware-view.exe -serverURL serverurl -loginAsCurrentUser true - installShortcutsThenQuit</pre> <p>如需伺服器所建立捷徑的相關資訊，請參閱 使用伺服器所建立的捷徑。</p>
<code>-languageId Locale_ID</code>	在 Horizon Client 中為不同的語言提供當地語系化支援。如果具有資源程式庫，請指定要使用的地區設定識別碼 (LCID)。若是美國英文，請輸入值 <code>0x409</code> 。
<code>-launchMinimized</code>	<p>以最小化模式啟動 Horizon Client。</p> <p>如果您提供 <code>-appName</code> 或 <code>-desktopName</code> 選項，則 Horizon Client 會維持最小化狀態，直到指定的遠端桌面平台或已發佈的應用程式啟動為止。</p> <p>您無法將此選項與 <code>-unattended</code> 或 <code>-nonInteractive</code> 選項搭配使用。</p>
<code>-listMonitors</code>	<p>列出索引值並顯示所連接監視器的配置資訊。例如：</p> <pre>1: (0, 0, 1920, 1200) 2: (1920, 0, 3840, 1200) 3: (-900, -410, 0, 1190)</pre> <p>您可以在 <code>-monitors</code> 選項中使用這些索引值。</p>
<code>-loginAsCurrentUser</code>	設定為 <code>true</code> 時，系統會利用使用者登入用戶端系統時所提供的認證資訊來登入伺服器，且最終會登入至遠端桌面平台。預設值為 <code>false</code> 。
<code>-monitors "n[,n,n,n]"</code>	<p>指定要在多台監視器設定中使用的監視器，其中 <code>n</code> 為監視器的索引值。您可以使用 <code>-listMonitors</code> 選項來決定所連接監視器的索引值。您可以使用逗號分隔來指定最多四個索引值。例如：</p> <pre>-monitors "1,2"</pre> <p>除非 <code>-desktopLayout</code> 設為 <code>multimonitor</code>，否則此選項沒有作用。</p>
<code>-nonInteractive</code>	<p>從指令碼啟動 Horizon Client 時，會隱藏錯誤訊息方塊。如果您指定 <code>-unattended</code> 選項，則會隱含設定此選項。</p> <p>備註 如果您在非互動模式中登入伺服器，則不會提示您安裝開始功能表捷徑 (如果有的話)，且依預設會安裝捷徑。</p>

表 3-14. Horizon Client 命令列選項 (續)

選項	說明
-noVMwareAddins	防止載入 VMware 特定虛擬通道，例如虛擬列印。
-password <i>password</i>	指定使用者登入 Horizon Client 所使用的密碼。密碼由命令主控台或其他指令碼工具在純文字中處理。如果您自動產生密碼，則不需要為處於 Kiosk 模式的用戶端指定此選項。為提高安全性，請勿指定此選項。使用者能以互動式方法輸入密碼。
-printEnvironmentInfo	顯示用戶端裝置的 IP 位址、MAC 位址及機器名稱。
-serverURL <i>connection_server</i>	指定伺服器的 URL、IP 位址或 FQDN。
-shutdown	關閉所有遠端桌面平台和已發佈的應用程式，以及相關的使用者介面元件。
-singleAutoConnect	如果使用者僅有權使用一個遠端桌面平台或已發佈的應用程式，在使用者通過伺服器驗證後，將會連線至該遠端桌面平台或已發佈的應用程式。此設定可讓使用者不需要從只包含一個項目的清單中選取遠端桌面平台或已發佈的應用程式。
-smartCardPIN <i>PIN</i>	指定使用者在插入智慧卡進行登入時所使用的 PIN 碼。
-usernameHint <i>user_name</i>	指定要作為使用者名稱提示的帳戶名稱。
-standalone	<p>啟動可連線至相同或不同伺服器的第二個 Horizon Client 執行個體。此選項支援回溯相容性。-standalone 是用戶端的預設行為，因此不需要指定。</p> <p>對相同或不同伺服器建立多個遠端桌面平台連線時，支援使用安全通道。</p> <p>備註 第二個遠端桌面平台連線可能無法存取本機硬體，例如 USB 裝置、智慧卡、印表機和多台監視器。</p>
-supportText <i>file_name</i>	指定文字檔案的完整路徑。檔案的內容會顯示在 [支援資訊] 對話方塊中。
-unattended	<p>在非互動模式中啟動 Horizon Client (這種作法適合於 Kiosk 模式下的用戶端)。您也必須指定下列資訊：</p> <ul style="list-style-type: none"> ■ 用戶端的帳戶名稱 (如果您未從用戶端裝置的 MAC 位址產生帳戶名稱)。此名稱的開頭必須是字串「custom-」，或是您已在 ADAM 中設定的替代前置詞。 ■ 用戶端的密碼 (如果您為用戶端設立帳戶時沒有自動產生密碼)。 <p>-unattended 選項會隱含設定</p> <p>-nonInteractive、-connectUSBOnStartup、-connectUSBOnInsert 和</p> <p>-desktopLayout multimonitor 選項。</p>
-unauthenticatedAccessAccount	<p>指定在 [未驗證存取] 啟用時用來匿名登入伺服器的「未驗證存取」使用者帳戶。如果 [未驗證存取] 未啟用，則會忽略此選項。</p> <p>例如：</p> <pre>vmware-view.exe -serverURL view.mycompany.com -unauthenticatedAccessEnabled true -unauthenticatedAccessAccount anonymous1</pre>
-unauthenticatedAccessEnabled	<p>設定為 true 時會啟用「未驗證存取」。如果「未驗證存取」無法使用，用戶端可以回復為使用其他驗證方法。Horizon Client 中的使用「未驗證存取」匿名登入設定會顯示為停用狀態，並且已選取。</p> <p>設定為 false 時，您必須輸入認證才能登入和存取應用程式。Horizon Client 中的使用「未驗證存取」匿名登入設定會隱藏並取消選取。</p> <p>若未指定此選項，您可以在 Horizon Client 中啟用 [未驗證存取]。使用「未驗證存取」匿名登入設定會顯示為啟用狀態，並且取消選取。</p>

表 3-14. Horizon Client 命令列選項 (續)

選項	說明
<code>-useExisting</code>	<p>可讓您從單一 Horizon Client 工作階段啟動多個遠端桌面平台和已發佈的應用程式。當您指定此選項時，Horizon Client 會確認是否有具有相同使用者名稱、網域和伺服器 URL 的工作階段存在，如果有，則會重複使用該工作階段，而不會建立工作階段。</p> <p>例如，在下列命令中，<code>user-1</code> 會啟動「小算盤」應用程式，且建立新的工作階段。</p> <pre>vmware-view.exe -userName user-1 -password secret -domainName domain -appName Calculator -serverURL view.mycompany.com -useExisting</pre> <p>而在下一個命令中，<code>user1</code> 會以相同使用者名稱、網域和伺服器 URL 啟動「小畫家」應用程式，且使用相同的工作階段。</p> <pre>vmware-view.exe -userName user-1 -password secret -domainName domain -appName Paint -serverURL view.mycompany.com -useExisting</pre>
<code>-userName user_name</code>	<p>指定使用者登入 Horizon Client 所使用的帳戶名稱。如果您用戶端裝置的 MAC 位址產生帳戶名稱，則不需要為處於 Kiosk 模式的用戶端指定此選項。</p>

除了 `-file`、`-languageId`、`-printEnvironmentInfo`、`-smartCardPIN` 和 `-unattended`，您可依照 Active Directory 群組原則來指定所有選項。

備註 群組原則設定的優先順序會高於您從命令列指定的設定。

Horizon Client 組態檔

您可從組態檔中讀取 Horizon Client 的命令列選項。

您可以將組態檔案的路徑指定為 `vmware-view` 命令之 `-file file_path` 選項的引數。檔案必須是 Unicode (UTF-16) 或 ASCII 文字檔案。

範例：非互動應用程式的組態檔案範例

以下範例顯示了非互動應用程式的組態檔案內容。

```
-serverURL https://view.yourcompany.com
-username autouser
-password auto123
-domainName companydomain
-desktopName autodesktop
-nonInteractive
```

範例：Kiosk 模式用戶端的組態檔案範例

以下範例顯示一個處於 Kiosk 模式中、且帳戶名稱以用戶端 MAC 位址為基礎的用戶端。該用戶端具有自動產生的密碼。

```
-serverURL 145.124.24.100
-unattended
```

使用 Windows 登錄設定 Horizon Client

您可以在 Windows 登錄中定義 Horizon Client 的預設設定，而不是在命令列上指定這些設定。群組原則設定的優先順序會高於 Windows 登錄設定，而 Windows 登錄設定的優先順序又高於命令列。

備註 未來的 Horizon Client 版本可能不再支援 Windows 登錄設定，而必須使用群組原則設定。

下表列出用來登入 Horizon Client 的登錄設定。這些設定都位在登錄的 HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\ 下。此位置會隨著使用者而有所不同。下表說明的 HKEY_LOCAL_MACHINE 設定為電腦通用設定，適用於有權登入 Windows 網域環境中電腦的所有本機使用者和所有網域使用者。

表 3-15. 認證的 Horizon Client 登錄設定

登錄設定	說明
密碼	預設密碼。
UserName	預設使用者名稱。

下表列出未包含登入認證的 Horizon Client 登錄設定。這些設定的位置取決於如下所述的系統類型：

- 對於 32 位元 Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\
- 對於 64 位元 Windows: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\

表 3-16. Horizon Client 登錄設定

登錄設定	說明
DomainName	預設 NETBIOS 網域名稱。例如，您可以使用 <code>mycompany</code> 而非 <code>mycompany.com</code> 。
EnableShade	決定是否啟用 Horizon Client 視窗頂端的功能表列（網底）。依預設會啟用此功能表列，但處於 Kiosk 模式的用戶端除外。如果值為 <code>false</code> ，會停用功能表列。 備註 此設定僅適用於您已將顯示配置設定為 所有監視器 或 全螢幕 的情況。
ServerURL	預設連線伺服器執行個體的 URL、IP 位址或 FQDN。
EnableSoftKeypad	如果設定為 <code>true</code> ，且 Horizon Client 視窗具有焦點，則實體鍵盤、螢幕鍵盤、滑鼠和手寫板事件會傳送至遠端桌面平台或已發佈的應用程式，即使滑鼠或螢幕鍵盤位於 Horizon Client 視窗以外也一樣。預設值為 <code>false</code> 。

下表顯示您可以新增的安全性設定。這些設定的位置取決於如下所述的系統類型：

- 針對 32 位元 Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security
- 針對 64 位元 Windows: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security

表 3-17. 安全性設定

登錄設定	說明及有效值
CertCheckMode	<p>憑證檢查模式。有效值如下：</p> <ul style="list-style-type: none"> ■ 0 會實作 Do not verify server identity certificates。 ■ 1 會實作 Warn before connecting to untrusted servers。 ■ 2 會實作 Never connect to untrusted servers。
SSLCipherList	<p>設定加密清單，以限制在建立加密 TLS 連線之前對某些密碼編譯演算法和通訊協定的使用。加密清單由一個或多個以冒號分隔的加密字串組成。所有加密字串均區分大小寫。</p> <p>預設值為 TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES。</p> <p>此預設值表示會啟用 TLS v1.1 和 TLS v1.2，並停用 SSL v2.0、SSL v3.0 和 TLS v1.0。SSL v2.0、SSL v3.0 和 TLS v1.0 已不再是核准的通訊協定，且會永久停用。</p> <p>加密套件會使用 128 位元或 256 位元 AES，移除匿名 DH 演算法，並依加密演算法金鑰長度的順序為目前的加密清單排序。</p> <p>如需關於組態的參考資訊，請參閱 http://www.openssl.org/docs/apps/ciphers.html。</p>

管理遠端桌面平台和已發佈的應用程式連線

4

使用者可以使用 Horizon Client 連線至伺服器、登入或登出遠端桌面平台，以及使用已發佈的應用程式。使用者也可以重新啟動和重設遠端桌面平台以及重設已發佈的應用程式，以進行疑難排解。

根據您設定原則的方式，使用者將可在其遠端桌面平台和已發佈的應用程式上執行多種作業。

本章節討論下列主題：

- [連線至遠端桌面平台或已發佈的應用程式](#)
- [使用未驗證存取連線至已發佈的應用程式](#)
- [共用位置資訊](#)
- [隱藏 VMware Horizon Client 視窗](#)
- [重新連線至遠端桌面平台或已發佈的應用程式](#)
- [在 Windows 用戶端桌面平台或開始功能表中建立捷徑](#)
- [使用伺服器所建立的捷徑](#)
- [設定遠端桌面平台的自動連線功能](#)
- [登出或中斷連線](#)
- [從伺服器中斷連線](#)

連線至遠端桌面平台或已發佈的應用程式

若要連線至遠端桌面平台或已發佈的應用程式，您必須提供伺服器的名稱以及使用者帳戶的認證。

在您讓使用者存取其遠端桌面平台和已發佈的應用程式之前，請測試您是否可以從用戶端裝置連線至遠端桌面平台或已發佈的應用程式。您可能需要為您的使用者帳戶指定伺服器並提供認證。

必要條件

- 取得登入認證，例如使用者名稱和密碼、RSA SecurID 使用者名稱和密碼、RADIUS 驗證認證，或智慧卡個人識別碼 (PIN)。
- 取得登入用的 NETBIOS 網域名稱。例如，您可以使用 `mycompany` 而非 `mycompany.com`。
- 執行 [準備 Horizon Client 適用的連線伺服器](#) 所述的管理工作。

- 如果您不在公司網路內，因而需要以 VPN 連線存取遠端桌面平台和已發佈的應用程式，請確認用戶端裝置已設定為使用 VPN 連線，並開啟該連線。
- 確認您是否擁有可讓您存取遠端桌面平台或已發佈應用程式之伺服器的完整網域名稱 (FQDN)。伺服器名稱中不支援使用底線 (_)。如果連接埠不是 443，您也需要連接埠號碼。
- 如果您計劃使用 RDP 顯示通訊協定來連線至遠端桌面平台，請確認已啟用 AllowDirectRDP 代理程式群組原則設定。如需相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。
- 針對伺服器所出示的憑證設定憑證檢查模式。若要決定要使用哪一個模式，請參閱 [在 Horizon Client 中設定憑證檢查模式](#)。

程序

- 1 如果需要 VPN 連線，請開啟 VPN。
- 2 啟動 Horizon Client。
- 3 (選擇性) 若要以目前已登入的 Windows 網域使用者身分登入，請按一下功能表列右上角的**選項**按鈕，並選取**以目前使用者身分登入**。

只有在用戶端系統上已安裝**以目前使用者身分登入**功能時，才能使用此設定。

- 4 連線至伺服器。

選項	動作
連線至新伺服器	按兩下 + 新增伺服器 按鈕，或按一下功能表列上的 新增伺服器 ，接著輸入伺服器的名稱，然後按一下 連線 。
連線至現有伺服器	按兩下伺服器圖示，或是在伺服器圖示上按一下滑鼠右鍵，然後選取 連線 。

Horizon Client 與伺服器之間的連線一律使用 TLS。TLS 連線的預設連接埠為 443。如果未將伺服器設定為使用預設連接埠，請使用格式：**伺服器名稱:連接埠**，例如 **view.company.com:1443**。

您可能會看到一則要求您先行確認的訊息，之後才會顯示登入對話方塊。

- 5 如果系統提示您輸入 RSA SecurID 認證或 RADIUS 驗證認證，請輸入認證，並按一下 **繼續**。
- 6 請輸入有權使用至少一個遠端桌面平台或已發佈應用程式的使用者認證，並選取網域，然後按一下 **登入**。

如果您將使用者名稱輸入為 **username@domain**，則 Horizon Client 會將其視為使用者主體名稱 (UPN)，且**網域**下拉式功能表將會停用。

如果**網域**下拉式功能表是隱藏的，則必須以 **username@domain** 或 **domain\username** 的形式輸入使用者名稱。

- 7 如果 Horizon Client 提示您將已發佈的應用程式或遠端桌面平台安裝到 Windows **開始**功能表，請按一下**是**或**否**。

當您第一次連線至已針對已發佈應用程式或遠端桌面平台設定捷徑的伺服器時，可能出現此提示。如果您按一下**是**，則在您有權使用的情況下，系統會為這些已發佈應用程式或遠端桌面平台將**開始**功能表捷徑安裝在用戶端系統上。如果您按一下**否**，則不會安裝**開始**功能表捷徑。

Horizon 管理員可以設定在 **Horizon Server 設定時自動安裝捷徑** 群組原則設定，以提示使用者安裝捷徑 (預設值)、自動安裝捷徑，或永不安裝捷徑。

- 8 (選擇性) 若要設定遠端桌面平台的顯示設定，請在遠端桌面平台圖示上按一下滑鼠右鍵，然後選取設定。

選項	動作
選取顯示通訊協定	如果 Horizon 管理員允許，請使用 連線方式 下拉式功能表來選取顯示通訊協定。
選取顯示配置	使用 顯示 下拉式功能表來選取視窗大小或使用多個監視器。

- 9 若要連線至遠端桌面平台或已發佈的應用程式，請在桌面平台和應用程式選取視窗中按兩下遠端桌面平台或已發佈應用程式的圖示。

如果您連線至已發佈的桌面平台，且已發佈的桌面平台已設定為使用不同的顯示通訊協定，您將無法立即連線。Horizon Client 會提示您使用已設定的通訊協定，或是登出讓 Horizon Client 可以使用不同的顯示通訊協定進行連線。

結果

在您連線後，遠端桌面平台或已發佈的應用程式隨即開啟。

如果您有權使用伺服器上的多個遠端桌面平台或已發佈的應用程式，則桌面平台和應用程式選取器視窗會保持開啟，讓您能夠連線至多個遠端桌面平台和已發佈的應用程式。

如果已啟用用戶端磁碟機重新導向功能，則會顯示 [共用] 對話方塊，然後您可以允許或拒絕存取本機檔案系統上的檔案。如需詳細資訊，請參閱[共用本機資料夾和磁碟機](#)。

第一次連線至伺服器時，Horizon Client 會將伺服器的捷徑儲存在 Horizon Client 主視窗上。當您下次需要連線至伺服器時，可以按兩下此伺服器捷徑。

如果驗證伺服器失敗，或用戶端無法連線至遠端桌面平台或已發佈的應用程式，請執行下列工作：

- 確認伺服器的憑證是否運作正常。若否，則在 Horizon Console 中，您可能也會看見遠端桌面平台上的代理程式無法連線。這些症狀指出憑證問題造成了額外的連線問題。
- 確認設定於連線伺服器執行個體中的標記允許從這位使用者進行連線。請參閱《Horizon 管理》文件。
- 確認此使用者有權存取此遠端桌面平台或已發佈的應用程式。請參閱《在 Horizon 中設定虛擬桌面平台》或《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。
- 如果您使用 RDP 顯示通訊協定來連線至遠端桌面平台，請確認該遠端桌面平台作業系統允許遠端桌面平台連線。

後續步驟

進行啟動設定。如果您不要求使用者提供伺服器的主機名稱，或您想要設定其他啟動設定，請使用命令列選項來建立遠端桌面平台捷徑。請參閱[從命令列執行 Horizon Client](#)。

使用未驗證存取連線至已發佈的應用程式

如果您有「未驗證存取」使用者帳戶，則可匿名登入伺服器並連線至已發佈的應用程式。

在您讓使用者使用「未驗證存取」功能來存取已發佈的應用程式之前，請測試您是否可從用戶端裝置連線至已發佈的應用程式。您可能需要為您的使用者帳戶指定伺服器並提供認證。

依預設，使用者會從**選項**功能表中選取**使用「未驗證存取」匿名登入**設定，並選取用來匿名登入的使用者帳戶。Horizon 管理員可設定群組原則設定以預先選取**使用「未驗證存取」匿名登入**設定，並讓使用者以特定的「未驗證存取」使用者帳戶登入。

必要條件

- 執行 [準備 Horizon Client 適用的連線伺服器](#) 所述的管理工作。
- 在連線伺服器執行個體上設定「未驗證存取」使用者。如需相關資訊，請參閱《Horizon 管理》文件中的〈提供適用於已發佈應用程式的未驗證存取〉。
- 如果位在公司網路外部，請確認您的用戶端裝置已設定為使用 VPN 連線，並開啟該連線。
- 請確認您是否具有可讓您對已發佈的應用程式進行存取之伺服器的完整網域名稱 (FQDN)。伺服器名稱中不支援使用底線 (_)。如果連接埠不是 443，您也需要連接埠號碼。
- 在 Horizon Client 中針對伺服器所出示的憑證設定憑證檢查模式。若要決定要使用哪一個模式，請參閱 [在 Horizon Client 中設定憑證檢查模式](#)。
- (選用) 設定**要用於「未驗證存取」的帳戶**和**使用「未驗證存取」匿名登入**群組原則設定，以變更預設的「未驗證存取」行為。如需相關資訊，請參閱 [用戶端 GPO 的指令碼定義設定](#)。

程序

- 1 如果需要 VPN 連線，請開啟 VPN。
- 2 啟動 Horizon Client。
- 3 按一下功能表列中的**選項**按鈕，然後選取**使用「未驗證存取」匿名登入**。

根據用戶端系統的設定方式，此設定可能會預先選取。

- 4 連線至可讓您進行未驗證存取的伺服器。

選項	動作
連線至新伺服器	按兩下 + 新增伺服器 按鈕，或按一下功能表列中的 + 新增伺服器 按鈕，輸入伺服器的名稱，然後按一下 連線 。
連線至現有伺服器	按兩下 Horizon Client 主視窗上的伺服器圖示。

Horizon Client 與伺服器之間的連線一律使用 TLS。TLS 連線的預設連接埠為 443。如果未將伺服器設定為使用預設連接埠，請使用本範例所顯示的格式：**view.company.com:1443**。

您可能會看到一則要求您先行確認的訊息，之後才會顯示 [登入] 對話方塊。

- 5 當 [登入] 對話方塊顯示時，視需要從**使用者帳戶**下拉式功能表中選取帳戶。

若僅有一個使用者帳戶可供使用，則系統會停用下拉式功能表，並預先選取使用者帳戶。

- 6 (選擇性) 若一律使用此帳戶核取方塊可供使用，則在選取後將會在您下次連線至伺服器時略過 [登入] 對話方塊。

若要在下次連線至伺服器之前取消選取此設定，請在 Horizon Client 主視窗的伺服器圖示上按一下滑鼠右鍵，並選取忘記已儲存的「未驗證存取」帳戶。

- 7 按一下**登入**以登入伺服器。

應用程式選取器視窗隨即出現。

- 8 若要啟動已發佈的應用程式，請按兩下已發佈的應用程式圖示。

共用位置資訊

針對遠端桌面平台或已發佈的應用程式啟用地理位置重新導向功能時，您可以將用戶端系統的位置資訊與遠端桌面平台或已發佈的應用程式共用。

若要共用用戶端系統的位置資訊，您必須在 Horizon Client 中進行設定。

必要條件

Horizon 管理員必須為遠端桌面平台或已發佈的應用程式設定地理位置重新導向功能。

此工作涉及在安裝 Horizon Agent 時啟用地理位置重新導向功能。此外，它也包括設定群組原則以設定地理位置重新導向功能，以及啟用 VMware Horizon 地理位置重新導向 IE 外掛程式。如需完整需求，請參閱[地理位置重新導向的系統需求](#)。

程序

- 1 連線至伺服器。
- 2 開啟**設定**對話方塊，並選取左窗格中的**地理位置**。
 - 在桌面平台和應用程式選取器視窗的右上角，按一下**設定** (齒輪) 圖示。
 - 在遠端桌面平台和應用程式選取器視窗中，以滑鼠右鍵按一下遠端桌面平台或已發佈的應用程式，然後選取**設定**。
- 3 設定地理位置設定。

選項	動作
與遠端桌面平台和已發佈的應用程式共用用戶端系統的位置資訊	選取 共用您的位置 核取方塊。
當您連線至遠端桌面平台或已發佈的應用程式時，不要顯示 [地理位置] 對話方塊	選取 連線至桌面平台或應用程式時不要顯示對話方塊 核取方塊。[地理位置] 對話方塊會詢問您是否要與遠端桌面平台或已發佈的應用程式共用位置資訊。 如果取消選取此核取方塊，則當您第一次連線至遠端桌面平台或已發佈的應用程式時，即會出現 [地理位置] 對話方塊。例如，如果您登入伺服器並連線至遠端桌面平台，您就會看到 [地理位置] 對話方塊。如果您後來連線至其他遠端桌面平台或已發佈的應用程式，您就不會再次看到該對話方塊。若要再看到該對話方塊，您必須中斷與伺服器的連線，並再次登入。

- 4 若要儲存變更，請按一下**套用**。

5 若要關閉對話方塊，請按一下**確定**。

隱藏 VMware Horizon Client 視窗

您可以在開啟遠端桌面平台或已發佈的應用程式之後隱藏 VMware Horizon Client 視窗。

您可以使用群組原則設定來設定在遠端桌面平台或已發佈的應用程式開啟後是否一律隱藏視窗。如需詳細資訊，請參閱[用戶端 GPO 的一般設定](#)。

程序

- ◆ 若要在開啟遠端桌面平台或已發佈的應用程式之後隱藏 VMware Horizon Client 視窗，請按一下 VMware Horizon Client 視窗角落的**關閉**按鈕。
- ◆ 若要進行一項設定，以在遠端桌面平台或已發佈的應用程式開啟後一律隱藏 VMware Horizon Client 視窗，請在連線至伺服器之前按一下功能表列中的**選項**按鈕，然後選取**啟動項目後隱藏選取器**。
- ◆ 若要在隱藏 VMware Horizon Client 視窗後顯示此視窗，請以滑鼠右鍵按一下系統匣中的 VMware Horizon Client 圖示並選取 **VMware Horizon Client**；或者，如果您已登入遠端桌面平台，請按一下功能表列中的**選項**按鈕並選取**切換至其他桌面平台**。

重新連線至遠端桌面平台或已發佈的應用程式

基於安全考量，Horizon 管理員可以設定在非使用狀態一段期間後，將您登出伺服器並鎖定已發佈應用程式的逾時。

依預設，如果您已開啟 Horizon Client，並且連線至特定伺服器超過 10 小時，則必須再次登入。此逾時適用於遠端桌面平台和已發佈的應用程式連線。

您會在已發佈的應用程式自動鎖定的 30 秒前收到警告提示。如果您未回應，已發佈的應用程式即會鎖定。依預設，逾時會在 15 分鐘非使用狀態後發生，但 Horizon 管理員可變更此逾時期間。

例如，如果您開啟了一或多個已發佈的應用程式，然後您離開電腦，則當您一小時後回來時，已發佈的應用程式視窗可能已不再處於開啟狀態。而您會看到一個對話方塊，提示您按一下**確定**，讓已發佈的應用程式視窗再次顯示。

若要在 Horizon Console 中設定這些逾時設定，請選取**設定 > 全域設定**，按一下**一般設定**索引標籤，然後按一下**編輯**。

在 Windows 用戶端桌面平台或開始功能表中建立捷徑

您可以為遠端桌面平台或已發佈的應用程式建立捷徑。捷徑會出現在用戶端系統的桌面平台上，就像本機安裝的應用程式的捷徑一樣。您也可以建立 Windows [開始] 功能表捷徑。

程序

- 1 啟動 Horizon Client 並登入伺服器。
- 2 在桌面平台和應用程式選取器視窗中，以滑鼠右鍵按一下遠端桌面平台或已發佈的應用程式，然後從快顯功能表中選取**建立桌面平台的捷徑**或**新增至 [開始] 功能表**。

結果

根據您所選取的命令，Horizon Client 會在桌面平台上或用戶端系統上 Windows [開始] 功能表中建立捷徑。

後續步驟

您可以重新命名、刪除捷徑，或對此捷徑執行可對本機安裝的應用程式捷徑執行的任何動作。如果您在尚未登入伺服器的情況下使用捷徑，在遠端桌面平台或已發佈的應用程式開啟之前，Horizon Client 會提示您登入。

使用伺服器所建立的捷徑

Horizon 管理員可以為特定遠端桌面平台和已發佈應用程式設定 [開始] 功能表或桌面平台捷徑。

如果您有權使用具有捷徑的遠端桌面平台或已發佈的應用程式，當您連線至伺服器時，Horizon Client 就會在用戶端系統的 [開始] 功能表中或/或桌面平台上放置捷徑。

在 Windows 10 系統上，Horizon Client 會將捷徑放置在應用程式清單中。如果 Horizon 管理員為捷徑建立類別資料夾，則該類別資料夾會顯示在 VMware 應用程式資料夾下，或在應用程式清單中顯示為類別。

您可以使用群組原則設定來設定 Horizon Client 會自動安裝捷徑、在安裝捷徑之前提示使用者，或是一律不安裝捷徑。如需詳細資訊，請參閱[用戶端 GPO 的一般設定](#)中的**在 Horizon Server 設定時自動安裝捷徑群組原則設定**。

您可以搭配使用 `vmware-view` 命令和 `-installShortcutsThenQuit` 選項，來建立會在用戶端系統自動啟動並安裝捷徑時執行的指令碼。如需詳細資訊，請參閱[Horizon Client 命令使用](#)。

如果您在尚未登入伺服器的情況下按一下伺服器建立的捷徑，在遠端桌面平台或已發佈的應用程式開啟之前，Horizon Client 會提示您登入。

如果 Horizon 管理員修改了伺服器上的遠端桌面平台和已發佈的應用程式捷徑，依預設，下次您連線至該伺服器時，用戶端系統上的捷徑即會更新。您可以變更 Horizon Client 中的預設捷徑更新行為。如需詳細資訊，請參閱[設定開始功能表捷徑更新](#)。

若要從用戶端系統中移除伺服器建立的捷徑，您可以從 Horizon Client 伺服器選取視窗中刪除伺服器，或解除安裝 Horizon Client。

備註 在處於 Kiosk 模式的用戶端上，系統不會提示使用者安裝伺服器建立的捷徑，且不會建立伺服器建立的捷徑。

設定開始功能表捷徑更新

您可以設定在連線至伺服器時，是否要將對伺服器上的遠端桌面平台和已發佈應用程式捷徑所做的變更，套用至用戶端系統。

必要條件

除非您先前已從伺服器安裝捷徑，否則您無法變更捷徑更新設定。

程序

- 1 啟動 Horizon Client 並連線至伺服器。
- 2 開啟 [設定] 對話方塊，然後選取**捷徑**。
 - 在桌面平台和應用程式選取器視窗的右上角，按一下**設定 (齒輪)** 圖示。
 - 以滑鼠右鍵按一下遠端桌面平台或已發佈的應用程式圖示，並選取**設定**。
- 3 選取或取消選取**自動更新應用程式和桌面平台捷徑的清單**核取方塊，然後按一下**確定**。

設定遠端桌面平台的自動連線功能

您可以將伺服器設定為在連線至伺服器時自動開啟特定遠端桌面平台。您無法將伺服器設定為自動開啟已發佈的應用程式。

必要條件

取得用來連線到伺服器的認證，例如使用者名稱和密碼、RSA SecurID 使用者名稱和密碼、RADIUS 驗證使用者名稱和密碼，或智慧卡個人識別碼 (PIN)。

程序

- 1 啟動 Horizon Client 並登入伺服器。
- 2 在桌面平台和應用程式選取器視窗中，以滑鼠右鍵按一下遠端桌面平台，然後選取**自動連線至此桌面平台**。
- 3 若要儲存變更，請按一下**套用**。
- 4 若要結束對話方塊，請按一下**確定**。
- 5 中斷與伺服器的連線。
- 6 重新連線至伺服器。
Horizon Client 會自動啟動遠端桌面平台。
- 7 (選擇性) 如果您需要停用遠端桌面平台的自動連線功能，請在遠端桌面平台的功能表列中按一下**選項**下拉式功能表，然後取消選取**自動連線至此桌面平台**選項。

登出或中斷連線

如果您沒有登出就從遠端桌面平台中斷連線，則遠端桌面平台中的應用程式可能仍會保持開啟狀態。您也可以從伺服器中斷連線，並將已發佈的應用程式保持執行狀態。

即使您在沒有開啟遠端桌面平台，您也可以從遠端桌面平台登出。此功能的結果如同傳送 **Ctrl+Alt+Del** 至遠端桌面平台，然後按一下**登出**一樣。

備註 遠端桌面平台不支援 Windows 按鍵組合 **Ctrl+Alt+Del**。相反地，按一下功能表列中的**傳送 Ctrl+Alt+Delete** 按鈕。或者，您可以按下 **Ctrl+Alt+Insert**。

程序

- ◆ 沒有登出就從遠端桌面平台中斷連線。

選項	動作
從遠端桌面平台視窗	執行下列其中一個動作： <ul style="list-style-type: none"> ■ 按一下遠端桌面平台視窗角落中的關閉按鈕。 ■ 從遠端桌面平台視窗的功能表列，選取選項 > 中斷連線。
從桌面平台和應用程式式選取器視窗	在桌面平台和應用程式式選取器視窗的左上角，按一下 中斷此伺服器的連線 圖示，然後按一下警告對話方塊中的 確定 。 如果您有權使用伺服器上的多個遠端桌面平台或已發佈的應用程式，則桌面平台和應用程式式選取器視窗即會開啟。

備註 Horizon 管理員可將遠端桌面平台設定為在中斷連線時登出。在此情況下，遠端桌面平台上任何開啟的應用程式都會關閉。

- ◆ 從遠端桌面平台登出和中斷連線。

選項	動作
從遠端桌面平台內	使用 Windows 開始 功能表登出。
從功能表列	選取 選項 > 中斷連線並登出 。 如果您使用此程序，在遠端桌面平台開啟的檔案將在沒有事先儲存的情況下關閉。

- ◆ 中斷與已發佈應用程式的連線。

選項	動作
從已發佈的應用程式而非伺服器中斷連線	以平常的方式結束已發佈的應用程式，例如，按一下應用程式視窗角落中的 關閉 按鈕。
從已發佈的應用程式和伺服器中斷連線	在應用程式選取器視窗的左上角，按一下 中斷此伺服器的連線 圖示，然後按一下警告對話方塊中的 確定 。
關閉應用程式選取器視窗，但將已發佈的應用程式保持執行狀態	按一下 關閉 按鈕。應用程式選取器視窗即會關閉。

- ◆ 沒有開啟遠端桌面平台時登出。

如果您使用此程序，在遠端桌面平台開啟的檔案將在沒有事先儲存的情況下關閉。

- 啟動 Horizon Client，連線至讓您存取遠端桌面平台的伺服器，並提供驗證認證。
- 在遠端桌面平台圖示上按一下滑鼠右鍵，然後選取**登出**。

從伺服器中斷連線

使用完遠端桌面平台或已發佈的應用程式後，您可以從伺服器中斷連線。

若要從伺服器中斷連線，請按一下 Horizon Client 視窗左上角的**中斷此伺服器的連線**圖示或按下 Alt+D。

在遠端桌面平台或已發佈的應用程式中作業

5

Windows 版 Horizon Client 提供熟悉且個人化的桌面平台和應用程式環境。使用者可以存取 USB 和連線至其本機 Windows 電腦的其他裝置、將文件傳送至其本機電腦能偵測到的任何印表機、使用智慧卡進行驗證，以及使用多台監視器。

本章節討論下列主題：

- Windows 用戶端的功能支援
- 調整遠端桌面平台視窗的大小
- 監視器和螢幕解析度
- 使用 USB 裝置
- 使用網路攝影機和麥克風
- 選取遠端桌面平台的慣用喇叭
- 共用遠端桌面平台工作階段
- 共用本機資料夾和磁碟機
- 在已發佈的應用程式中開啟本機檔案
- 複製與貼上
- 拖放
- 已發佈應用程式的使用提示
- 從遠端桌面平台或已發佈的應用程式列印
- 使用 URL 內容重新導向功能
- 改善遠端桌面平台中的滑鼠效能
- 使用掃描器
- 重新導向序列埠
- 鍵盤快速鍵
- 鍵盤輸入方式語言同步
- 設定鎖定鍵同步

Windows 用戶端的功能支援

某些客體作業系統和遠端桌面平台功能需要特定的 Horizon Agent 版本。規劃要提供給使用者的功能時，請使用此資訊。

支援的 Windows 虛擬桌面平台

Windows 虛擬桌面平台是單一工作階段虛擬機器。

此版本的 Horizon Client 可與已安裝 Horizon Agent 7.5 或更新版本的 Windows 虛擬桌面平台搭配使用。支援的客體作業系統包括 Windows 7、Windows 8.x、Windows 10、Windows Server 2012 R2、Windows Server 2016 和 Windows Server 2019，但具有下列限制：

- Windows Server 2019 虛擬桌面平台需要 Horizon Agent 7.7 或更新版本。
- Horizon Agent 2006 及更新版本不支援 Windows 7 和 Windows 8.x 虛擬桌面平台。

支援 RDS 主機上已發佈的桌面平台

RDS 主機是已安裝 Windows 遠端桌面服務和 Horizon Agent 的伺服器電腦。多個使用者可以同時在一部 RDS 主機上擁有已發佈的桌面平台工作階段。RDS 主機可以是實體機器，也可以是虛擬機器。

此版本的 Horizon Client 可與已安裝 Horizon Agent 7.5 或更新版本的 RDS 主機搭配使用。支援的客體作業系統包括 Windows Server 2012、Windows Server 2012 R2、Windows Server 2016 和 Windows Server 2019，但具有下列限制：

- Windows Server 2019 RDS 主機需要 Horizon Agent 7.7 或更新版本。
- Horizon Agent 2006 及更新版本不支援 Windows Server 2012 RDS 主機。

特定遠端桌面平台功能的需求

多數遠端桌面平台功能可與 Horizon Agent 7.5 搭配使用，但某些功能需要更新版本的 Horizon Agent。

功能	需求
拖曳文字和影像	Horizon Agent 7.9 或更新版本
拖曳檔案和資料夾	Horizon Agent 7.7 或更新版本
地理位置重新導向	Horizon Agent 7.6 或更新版本
瀏覽器重新導向	Horizon Agent 7.10 或更新版本
VMware Integrated Printing 和依據位置列印	Horizon Agent 7.7 或更新版本

此版本的 Windows 版 Horizon Client 不支援 Horizon Agent 7.x 版中支援的下列遠端桌面平台功能：

- 虛擬列印 (也稱為 ThinPrint)
- Flash URL 重新導向
- Flash 重新導向

支援的 Linux 桌面平台

如需所支援 Linux 客體作業系統的清單以及所支援功能的相關資訊，請參閱《在 Horizon 中設定 Linux 桌面平台》文件。

調整遠端桌面平台視窗的大小

當您拖曳遠端桌面平台視窗的角落以調整其大小時，工具提示會在視窗的右下角顯示螢幕解析度。

如果您使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定，當您變更遠端桌面平台視窗的大小時，工具提示會改為顯示不同的螢幕解析度。如果您需要將遠端桌面平台視窗的大小調整為特定解析度，則此資訊相當實用。

如果 Horizon 管理員已鎖定客體大小，或您使用的是 RDP 顯示通訊協定，則無法變更遠端桌面平台視窗的解析度。在這些情況下，解析度工具提示會顯示初始解析度。

如果您有多台監視器，則可以選取用來顯示遠端桌面平台視窗的監視器。如需詳細資訊，請參閱 [選取特定監視器來顯示遠端桌面平台](#)。您也可以設定要在單一監視器上開啟的遠端桌面平台視窗。如需詳細資訊，請參閱 [在多台監視器設定中的單一監視器上顯示遠端桌面平台](#)。

監視器和螢幕解析度

您可以將遠端桌面平台或已發佈的應用程式延伸至多台監視器。若您擁有高解析度監視器，您可以使用高解析度來檢視遠端桌面平台或已發佈的應用程式。

支援的多台監視器組態

Horizon Client 支援下列多台監視器組態。

- 從 Horizon 7 (7.8 版) 開始，支援六台解析度為 2560 X 1600 的監視器，搭配執行 Windows 10 (1703 版) 及更新版本的虛擬桌面平台。更新的 Windows 顯示規格需要 Windows 10 (1803 版) 或更新版本，才能在 Horizon 7 (7.9 版) 及更新版本上支援六台監視器。
- 使用即時複製桌面平台集區時，監視器數量上限為四個 (4K 解析度)。
- 使用兩台或更多台監視器時，這些監視器不必處於相同模式。例如，如果您使用的筆記型電腦與外部監視器連接，則這台外部監視器可為直向模式或橫向模式。
- 使用硬體版本 13 或更早版本時，監視器可以並排擺放、兩層各兩台的堆疊，或是當您僅使用兩台監視器、且總高度低於 4096 像素時，便可以垂直堆疊。
- 若要使用選擇性的多台監視器功能，您必須使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定。如需詳細資訊，請參閱 [選取特定監視器來顯示遠端桌面平台](#) 和 [選取特定監視器來顯示已發佈的應用程式](#)。
- 若要使用 vSGA 3D 轉譯功能，您必須使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定。您最多可以使用兩台監視器，解析度可高達 1920 X 1200。若是 4K (3840 X 2160) 解析度，則僅支援一台監視器。
- 對於 vGPU 或其他 GPU 傳遞模式，廠商硬體和驅動程式會決定監視器數目和最大解析度。如需詳細資訊，請參閱《NVIDIA GRID 虛擬 GPU 使用者指南》，或前往廠商網站。

- 如果您使用五台或更多台監視器，並連線至使用 VMware Blast 的遠端工作階段，則當您在不登出原始工作階段的情況下，從不同裝置使用相同的使用者認證連線至使用 PCoIP 的工作階段時，與新工作階段的初始連線會失敗。
- 使用 VMware Blast 顯示通訊協定時，支援 8K (7680 x 4320) 的遠端桌面平台螢幕解析度。支援兩個 8K 顯示器。桌面平台虛擬機器的硬體版本必須為 14 (ESXi 6.7 或更新版本)。您必須在虛擬機器中配置足夠的系統資源，才能支援 8K 顯示。如需適用於 GRID 型桌面平台和適用於 NVIDIA vGPU 設定檔之所支援監視器組態的相關資訊，請參閱 NVIDIA 網站上的《虛擬 GPU 軟體使用者指南》。只有 Windows 用戶端支援此功能。
- 可透過 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定，支援 4K (3840 x 2160) 的遠端桌面平台畫面解析度。支援的 4K 顯示器數目取決於桌面平台虛擬機器的硬體版本以及 Windows 版本。

硬體版本	Windows 版本	支援的 4K 顯示器數目
10 (ESXi 5.5.x 相容)	7、8、8.x、10	1
11 (ESXi 6.0 相容)	7 (停用 3D 轉譯功能和 Windows Aero)	3
11	7 (啟用 3D 轉譯功能)	1
11	8、8.x、10	1
13 或 14	7、8、8.x、10 (啟用 3D 轉譯功能)	1
13 或 14	7、8、8.x、10	4

為了達到最佳效能，虛擬機器應具備至少 2 GB RAM 和 2 個 vCPU。此功能可能需要良好的網路條件，例如 1000Mbps 頻寬與低網路延遲，以及低封包遺失率。

備註 遠端桌面平台螢幕解析度設定為 3840 x 2160 (4K) 時，螢幕上的項目可能會顯得比較小，您也無法使用遠端桌面平台中的 [螢幕解析度] 對話方塊讓文字和其他項目變大。在此案例中，您可以將用戶端機器的 DPI 設定為適當設定，並啟用 DPI 同步功能，將用戶端機器的 DPI 設定重新導向至遠端桌面平台。

- 如果使用 Microsoft RDP 7，則可用來顯示遠端桌面平台的監視器數量上限為 16。
- 如果使用 Microsoft RDP 顯示通訊協定，則遠端桌面平台必須安裝 Microsoft 遠端桌面連線 (RDC) 6.0 或更新版本。

選取特定監視器來顯示遠端桌面平台

如果您有兩台以上監視器，則可以選取用來顯示遠端桌面平台視窗的監視器。例如，如果您有兩台監視器，您可以指定讓遠端桌面平台視窗僅在其中一台監視器上顯示。

從 Horizon 7 (7.8 版) 開始，您最多可以選取六台相鄰的監視器，且各自具有執行 Windows 10 (1703 版) 及更新版本的虛擬桌面平台。從 Horizon 7 (7.9 版) 開始，您最多可以選取六台相鄰的監視器，且各自具有執行 Windows 10 (1803 版) 及更新版本的虛擬桌面平台。監視器可以並排或垂直堆疊。例如，您可以設定為兩列，每列各有三台監視器。使用其他 Windows 版本或更早的 VMware Horizon 版本時，則最多可以使用四台相鄰的監視器。

必要條件

您必須擁有兩台或更多的監視器。

程序

1 啟動 Horizon Client 並連線至伺服器。

2 開啟遠端桌面平台的 [設定] 對話方塊。

- 在桌面平台和應用程式選取視窗的右上角，按一下**設定** (齒輪) 圖示，然後選取左窗格中的遠端桌面平台。
- 在桌面平台和應用程式選取視窗中，以滑鼠右鍵按一下遠端桌面平台，然後選取**設定**。

3 從**連線方式**下拉式功能表中，選取 **PCoIP** 或 **VMware Blast**。

當 Horizon 管理員已啟用**連線方式**下拉式功能表時，此功能表才會出現。

4 從**顯示**下拉式功能表中，選取**所有監視器**。

目前連線至用戶端系統之監視器的縮圖，會出現在 [顯示] 設定下。顯示拓撲會符合用戶端系統上的顯示設定。

5 若要選取或取消選取要用來顯示遠端桌面平台視窗的監視器，請按一下縮圖。

當您選取監視器時，其縮圖會變色。如果您違反顯示選取規則，系統會顯示一則警告訊息。

6 若要儲存變更，請按一下**套用**。

7 若要關閉對話方塊，請按一下**確定**。

8 連線至遠端桌面平台。

當您連線至遠端桌面平台時，系統即會立即套用您的變更。在您結束 Horizon Client 之後，Horizon Client 會將顯示設定儲存在遠端桌面平台的喜好設定檔案中。

在多台監視器設定中的單一監視器上顯示遠端桌面平台

如果您有兩台以上的監視器，但想要讓遠端桌面平台視窗僅顯示在一台監視器上，您可以將遠端桌面平台視窗設定為在單一監視器上開啟。

必要條件

您必須擁有兩台或更多的監視器。

程序

1 啟動 Horizon Client 並連線至伺服器。

2 開啟遠端桌面平台的 [設定] 對話方塊。

- 在桌面平台和應用程式選取視窗的右上角，按一下**設定** (齒輪) 圖示，然後選取左窗格中的遠端桌面平台。
- 在桌面平台和應用程式選取視窗中，以滑鼠右鍵按一下遠端桌面平台，然後選取**設定**。

- 3 從**連線方式**下拉式功能表中，選取 **PCoIP** 或 **VMware Blast**。

當 Horizon 管理員已啟用**連線方式**下拉式功能表時，此功能表才會出現。

- 4 從**顯示**下拉式功能表中，選取**全螢幕**、**視窗 - 大**、**視窗 - 小**或**自訂**。

視窗 - 大會將視窗大小設定為 1904 x 978 像素。**視窗 - 小**會將視窗大小設定為 640 x 480 像素。如果您選取**自訂**，則可以選取特定視窗大小。

- 5 若要儲存變更，請按一下**套用**。

- 6 若要關閉對話方塊，請按一下**確定**。

結果

依預設，遠端桌面平台視窗會在主要監視器上開啟。您可以將遠端桌面平台視窗拖曳至非主要監視器，當您下次開啟遠端桌面平台時，遠端桌面平台視窗就會顯示在相同的監視器上。視窗開啟時會置中顯示於監視器內，且會使用您針對顯示模式選取的視窗大小，而非您透過拖曳視窗來調整大小時所建立的大小。

選取特定監視器來顯示已發佈的應用程式

如果您有兩台以上監視器，您可以選取要在哪些監視器上顯示已發佈的應用程式視窗。例如，如果您有兩台監視器，您可以指定讓已發佈的應用程式視窗僅在其中一台監視器上顯示。

您最多可以選取四台相鄰的監視器。監視器可以並排、兩兩堆疊或垂直堆疊。最多可以垂直堆疊兩台監視器。

必要條件

您必須擁有兩台或更多的監視器。

程序

- 1 啟動 Horizon Client 並連線至伺服器。
- 2 開啟已發佈應用程式的 [設定] 對話方塊。
 - 按一下桌面平台和應用程式選取視窗右上角的**設定** (齒輪) 圖示，然後選取**應用程式**。
 - 在桌面平台和應用程式選取視窗中，以滑鼠右鍵按一下已發佈的應用程式，然後選取**設定**。
- 3 在 [顯示] 設定下方，選取或取消選取要顯示已發佈的應用程式視窗的監視器。

當您選取監視器時，其縮圖會變色。如果您違反顯示選取規則，系統會顯示一則警告訊息。
- 4 若要儲存變更，請按一下**套用**。
- 5 若要關閉對話方塊，請按一下**確定**。

使用顯示調整

使用者若視力不佳或擁有高解析度螢幕 (例如 4K 監視器)，通常可藉由將用戶端系統上的 DPI (每英寸點數) 設定為大於 100% 來啟用調整。DPI 設定可控制文字、應用程式和圖示的大小。較低的 DPI 設定可讓尺寸變得較小，較高的設定則可讓尺寸變得較大。利用顯示調整值功能，遠端桌面平台和已發佈的應用程式可支援用戶端系統的調整設定，並顯示正常而非極小的大小。

Horizon Client 會將從遠端桌面平台或已發佈的應用程式接收的 DPI 設定與用戶端系統的 DPI 設定進行比較。如果 DPI 設定不相符，且已啟用顯示調整值功能，則 Horizon Client 會計算調整係數。例如，如果遠端桌面平台的 DPI 設定為 100%，且用戶端系統的 DPI 設定為 200%，則 Horizon Client 會將遠端桌面平台的 DPI 設定依照 2 ($200 / 100 = 2$) 的係數進行縮放。

Horizon Client 會為每個遠端桌面平台個別儲存顯示調整值設定。針對已發佈的應用程式，顯示調整設定會套用至目前已登入使用者可使用的所有已發佈應用程式。

在多台監視器設定中，使用顯示調整並不會影響 Horizon Client 支援的監視器數目和最大解析度。允許顯示調整值且該功能生效時，將會根據用戶端系統的 DPI 設定來進行調整。

您可以透過啟用 Horizon Client **鎖定客體大小** 群組原則設定來隱藏顯示調整設定。

您可以透過設定 **允許顯示調整值** 群組原則設定，以針對所有遠端桌面平台和已發佈的應用程式啟用或停用顯示調整值功能。如需相關資訊，請參閱 [用戶端 GPO 的一般設定](#)。**允許顯示調整值** 依預設會啟用，且在使用者介面中勾選此選項。

此程序說明如何在連線至遠端桌面平台或已發佈的應用程式之前啟用顯示調整值功能。在連線至遠端桌面平台之後，您可以從 Horizon Client 功能表列中選取 **選項 > 允許顯示調整值**，以啟用顯示調整功能。

程序

- 1 啟動 Horizon Client 並連線至伺服器。
- 2 在桌面平台和應用程式選取器視窗中，以滑鼠右鍵按一下遠端桌面平台或已發佈的應用程式，然後選取 **設定**。
- 3 選取 **允許顯示調整值** 核取方塊。
如果系統管理員已預先設定顯示調整值，則核取方塊會變暗。如果系統管理員已隱藏顯示調整值設定，則不會顯示核取方塊。
- 4 若要儲存變更，請按一下 **套用**。
- 5 若要關閉對話方塊，請按一下 **確定**。

使用 DPI 同步

DPI 同步功能可確保遠端桌面平台或已發佈的應用程式工作階段中的 DPI 設定符合用戶端系統的 DPI 設定。

如同顯示調整值功能，DPI 同步功能可改善高 DPI 顯示器上文字和圖示的可讀性。與增加字型 and 影像大小且可能使其模糊的顯示調整值功能不同，DPI 同步功能會增加字型和影像的大小並使其維持清晰。因此，為了獲得最佳使用者體驗，一般會偏好使用 DPI 同步功能。

如果 DPI 同步功能和顯示調整值功能同時啟用，在任何指定時間只有一項功能會生效。

DPI 同步 代理程式群組原則設定會決定是否啟用 DPI 同步功能。此功能依預設為啟用。

與遠端桌面平台的 DPI 同步行為

預設 DPI 同步行為取決於代理程式機器中安裝的 Horizon Agent 版本。

從 Horizon Agent 2012 開始，用戶端的每台監視器 DPI 設定會同步至代理程式，且依預設變更會在遠端工作階段期間立即生效。此功能由**每個監視器的 DPI 同步**代理程式群組原則設定所控制。虛擬桌面平台和實體桌面平台依預設支援每個監視器的 DPI 同步功能。不支援已發佈的桌面平台。

在舊版 Horizon Agent 中，Horizon Client 僅支援同步至系統 DPI 設定。DPI 同步會在初始連線期間發生，而在重新連線時，顯示調整值會於必要時運作。當 DPI 同步正常運作，且用戶端系統的 DPI 設定符合遠端桌面平台的 DPI 設定時，即使您在使用者介面中選取**允許顯示調整值**選項，顯示調整值也無法生效。Windows 不會允許使用者變更目前使用者工作階段的系統層級 DPI 設定，因此僅在您登入並啟動遠端工作階段時，DPI 同步才會發生。如果使用者在遠端工作階段期間變更 DPI 設定，則他們必須登出後並再次登入，讓遠端桌面平台的 DPI 設定符合用戶端系統的新 DPI 設定。

代理程式 DPI 設定位於 Windows 登錄的 `Computer\HKEY_CURRENT_USER\Control Panel\Desktop:logPixels` 中。

備註 系統 DPI 設定可能與主監視器的 DPI 設定不同。例如，如果您關閉主監視器，且系統切換到的外部顯示器具有與主要監視器不同的 DPI 設定，則系統 DPI 設定仍會與先前所關閉主要監視器的 DPI 設定相同。

此版本的 Horizon Client 不支援隨 Horizon Agent 7.8 至 2006 版一併提供的**每個連線的 DPI 同步**代理程式群組原則設定。

如需有關 DPI 同步群組原則設定的詳細資訊，請參閱 Horizon Agent 版本的《在 Horizon 中設定遠端桌面平台功能》文件。

虛擬桌面平台支援的客體作業系統

針對虛擬桌面平台，下列客體作業系統支援 DPI 同步功能：

- 32 位元或 64 位元的 Windows 7
- 32 位元或 64 位元的 Windows 8.x
- 32 位元或 64 位元的 Windows 10
- 設定為桌面平台的 Windows Server 2008 R2
- 設定為桌面平台的 Windows Server 2012 R2
- 設定為桌面平台的 Windows Server 2016
- 設定為桌面平台的 Windows Server 2019

備註 對於已設定為桌面平台的 Windows Server 機器，不支援每個監視器的 DPI 同步功能。

已發佈的桌面平台和已發佈的應用程式支援的 RDS 主機

針對已發佈的桌面平台和已發佈的應用程式，下列 RDS 主機支援 DPI 同步功能：

- Windows Server 2012 R2
- Windows Server 2016

■ Windows Server 2019

備註 對於 RDS 主機，不支援每個監視器的 DPI 同步功能。此限制不適用於在具有虛擬機器主控應用程式功能的桌面平台集區上執行的已發佈應用程式。

變更遠端桌面平台的顯示模式

您可以在連線至遠端桌面平台之前或之後變更顯示模式，例如，從**所有監視器**模式變更為**全螢幕**模式。已發佈的應用程式不支援此功能。

程序

- 1 啟動 Horizon Client 並連線至伺服器。
- 2 開啟遠端桌面平台的 [設定] 對話方塊。
 - 在桌面平台和應用程式選取視窗的右上角，按一下**設定** (齒輪) 圖示，然後選取左窗格中的遠端桌面平台。
 - 在桌面平台和應用程式選取視窗中，以滑鼠右鍵按一下遠端桌面平台，然後選取**設定**。
- 3 從**顯示**下拉式功能表中，選取顯示模式。

選項	說明
所有監視器	在多台監視器上顯示遠端桌面平台視窗。依預設，遠端桌面平台視窗會顯示在所有監視器上。
全螢幕	使遠端桌面平台視窗填滿螢幕。
視窗 - 大	將遠端桌面平台視窗大小設定為 1904 x 978 像素。
視窗 - 小	將遠端桌面平台視窗大小設定為 640 x 480 像素。
自訂	顯示一個滑桿，讓您用來設定自訂的遠端桌面平台視窗大小。

- 4 若要儲存變更，請按一下**套用**。
- 5 若要關閉對話方塊，請按一下**確定**。

如果您已連線至遠端桌面平台，您的變更將會立即套用。如果您未連線至遠端桌面平台，則會在連線時套用您的變更。在您結束 Horizon Client 之後，Horizon Client 會將顯示設定儲存在遠端桌面平台的喜好設定檔案中。

結果

如果您使用**所有監視器**模式，並按一下**最小化**按鈕，當您再將視窗最大化時，視窗將回復為**所有監視器**模式。同樣地，如果您使用**全螢幕**模式，並將視窗最小化，當您將視窗最大化時，視窗將在一台監視器上回復為**全螢幕**模式。

備註 如果 Horizon Client 使用所有監視器，而且您將已發佈的應用程式視窗最大化，則視窗只會展開至包含該應用程式之監視器的全螢幕。

自訂遠端桌面平台的顯示解析度和顯示調整值

您可以使用 Horizon Client 來自訂遠端桌面平台的顯示解析度和顯示調整值。顯示解析度會決定文字和影像的清晰度。在較高的解析度下 (例如 1600 x 1200 像素)，項目看起來更鮮明。顯示調整值以百分比表示，可增加或縮減文字、圖示和導覽元素的大小。

依預設，自訂顯示解析度和顯示調整值設定僅會儲存在本機用戶端系統上。管理員可以使用**將解析度和 DPI 儲存到伺服器**群組原則設定，將這些設定儲存到伺服器，如此會一律套用這些設定，不論您用來登入遠端桌面平台的用戶端裝置為何。如需詳細資訊，請參閱[用戶端 GPO 的一般設定](#)。

這項功能有下列限制和考量。

- 在多台監視器模式下，不支援自訂遠端桌面平台的顯示解析度和調整值。
- 如果您選取高於或低於用戶端解析度的自訂解析度，則 Horizon Client 會將遠端桌面平台視窗的大小調整為符合用戶端視窗。
- 如果您在遠端桌面工作階段期間自訂顯示解析度，您的變更將立即生效。如果您在遠端桌面工作階段期間自訂顯示調整值，則必須先登出再重新登入，您的變更才會生效。
- Horizon Client **鎖定客體大小**群組原則設定優先於顯示解析度自訂。如需詳細資訊，請參閱 [用戶端 GPO 的指令碼定義設定](#)。

程序

- 1 啟動 Horizon Client 並連線至伺服器。
- 2 在桌面平台和應用程式選取器視窗中，以滑鼠右鍵按一下遠端桌面平台，然後選取**設定**。
- 3 在**連線方式**功能表中，選取 **VMware Blast** 或 **PCoIP**。
- 4 從**顯示**下拉式功能表中，選取**全螢幕**、**視窗 - 大**、**視窗 - 小**或**自訂**。
- 5 若要自訂顯示解析度，請從**解析度**下拉式功能表中選取解析度。
如果您選取**自動** (預設設定)，則 Horizon Client 會讓遠端桌面平台符合用戶端視窗大小。如果遠端桌面平台不支援您選取的顯示解析度，則會使用預設設定。
- 6 若要自訂顯示調整值，請從**調整**下拉式功能表中選取縮放大小。
如果您選取**自動** (預設設定)，則 Horizon Client 會將用戶端系統的顯示調整值同步至遠端桌面平台。
- 7 若要儲存變更，請按一下**確定**。

使用 USB 裝置

使用 USB 重新導向功能時，您可以在遠端桌面平台或已發佈的應用程式中使用本機附加的 USB 裝置，例如隨身碟。

使用 USB 重新導向功能時，連結至本機用戶端系統的大多數 USB 裝置可以透過 Horizon Client 中的功能表使用。您可以使用這些功能表來連線與中斷連線裝置。

如需 USB 裝置需求和 USB 重新導向限制的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

您可以手動或自動地將 USB 裝置連線至遠端桌面平台或發佈的應用程式。

此程序說明如何使用 Horizon Client 將 USB 裝置設定為自動連線至遠端桌面平台或已發佈的應用程式。您也可以使用 Horizon Client 命令列介面或藉由設定群組原則來設定自動連線。

如需關於指令介面的相關資訊，請參閱[從命令列執行 Horizon Client](#)。如需設定群組原則的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

必要條件

- 若要使用 USB 裝置搭配遠端桌面平台或發佈的應用程式，Horizon 管理員必須啟用 USB 重新導向功能。

此工作包括安裝 Horizon Agent 的 USB 重新導向元件，並且可以包括設定有關 USB 重新導向的原則。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件和[用戶端 GPO 的 USB 設定](#)。

- 必須在 Horizon Client 中安裝 USB 重新導向元件。如果安裝時未包括此元件，請解除安裝 Horizon Client 並再次執行安裝程式以納入 USB 重新導向元件。

如需安裝指示，請參閱《Windows 版 VMware Horizon Client 安裝和設定指南》文件。

- 請熟悉 [USB 重新導向限制](#)。

程序

- ◆ 手動將 USB 裝置連線至遠端桌面平台。
 - a 將 USB 裝置連線至本機用戶端系統。
 - b 從遠端桌面平台中的 VMware Horizon Client 功能表列，按一下**連線 USB 裝置**。
 - c 選取 USB 裝置。

該裝置被手動地從本機系統重新導向至遠端桌面平台。

- ◆ 將 USB 裝置連線至發佈的應用程式。
 - a 將 USB 裝置連線至本機用戶端系統。
 - b 啟動 Horizon Client 並連線至發佈的應用程式。
 - c 按一下桌面平台和應用程式選取器視窗右上角的**設定** (齒輪) 圖示，然後按一下 **USB 裝置**。
 - d 在右窗格中選取 USB 裝置，按一下**連線**，接著選取發佈的應用程式，然後按一下**確定**。

Horizon Client 會將 USB 裝置連線到您選取的已發佈應用程式。USB 裝置也可供與您所選取應用程式位於相同伺服器陣列中的其他應用程式使用。

- e (選擇性) 若要設定 Horizon Client 以自動在應用程式啟動時將 USB 裝置連線至已發佈的應用程式，請選取**啟動時自動連線**核取方塊。
- f (選擇性) 若要設定 Horizon Client 以自動在您將裝置插入本機系統時將 USB 裝置連線至已發佈的應用程式，請選取**插入時自動連線**核取方塊。

發佈的應用程式必須啟動且位於前景，此行為才會生效。

- g 若要關閉 [設定] 對話方塊，請按一下**確定**。
- h 當您使用完發佈的應用程式時，請再次開啟 [設定] 對話方塊，接著選取 **USB 裝置**，然後選取**中斷連線**。

您必須釋放 USB 裝置才能從本機系統進行存取。

- ◆ 設定 Horizon Client 以便在您將 USB 裝置插入本機系統時，自動將這些裝置連線至遠端桌面平台。
如果您計劃連結使用 MTP 驅動程式的裝置 (例如使用 Android 系統的 Samsung 智慧型手機和平板電腦)，您就必須使用自動連線功能。
 - a 在您插入 USB 裝置之前，請先啟動 Horizon Client 並連線至遠端桌面平台。
 - b 從遠端桌面平台的 VMware Horizon Client 功能表列，選取**連線 USB 裝置 > 插入時自動連線**。
 - c 插入 USB 裝置。

您在啟動 Horizon Client 後連線到本機系統的 USB 裝置，將重新導向到遠端桌面平台。

- ◆ 將 Horizon Client 設定為在 Horizon Client 啟動時自動將 USB 裝置連線到遠端桌面平台。
 - a 從遠端桌面平台的 VMware Horizon Client 功能表列，選取**連線 USB 裝置 > 啟動時自動連線**。
 - b 插入 USB 裝置並重新啟動 Horizon Client。

您在啟動 Horizon Client 時連線到本機用戶端系統的 USB 裝置，將重新導向到遠端桌面平台。

結果

USB 裝置顯示在遠端桌面平台或發佈的應用程式中。USB 裝置最多可能需要 20 秒才會顯示在遠端桌面平台或已發佈的應用程式中。您首次將裝置連線至遠端桌面平台時，系統可能會提示您安裝驅動程式。

如果幾分鐘後 USB 裝置並未顯示在遠端桌面平台或發佈的應用程式中，請中斷連線並將裝置重新連線到用戶端電腦。

後續步驟

如果您有 USB 重新導向的問題，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中關於對 USB 重新導向問題進行疑難排解的主題。

USB 重新導向限制

USB 重新導向功能具有某些限制。

- 從 Horizon Client 的功能表存取 USB 裝置，並在遠端桌面平台或已發佈的應用程式中使用此裝置時，您無法在本機裝置存取此 USB 裝置。
- 未在功能表中出現、但可以在遠端桌面平台或已發佈的應用程式中使用的 USB 裝置包含人性化介面裝置，例如鍵盤和指標裝置。遠端桌面平台或已發佈的應用程式和本機裝置會同時使用這些裝置。與這些 USB 裝置的互動有時會因為網路延遲而變慢。
- 大型的 USB 磁碟機需要幾分鐘的時間才會出現在遠端桌面平台或已發佈的應用程式中。
- 一些 USB 裝置需要特定的驅動程式。如果未事先安裝必要的驅動程式，當您將 USB 裝置連接到遠端桌面平台或已發佈的應用程式時，系統可能會提示您安裝驅動程式。

- 如果您計劃要連結的 USB 裝置使用 MTP 驅動程式 (例如, 使用 Android 系統的 Samsung 智慧型手機和平板電腦), 請設定 Horizon Client, 使其自動將 USB 裝置連線至遠端桌面平台或已發佈的應用程式。否則, 如果您試圖使用功能表項目來手動重新導向 USB 裝置的話, 除非您拔除裝置插頭, 然後再重插回去, 否則該裝置不會被重新導向。
- 請勿使用**連線 USB 裝置**功能表來連線至掃描器。若要使用掃描器裝置, 請使用掃描器重新導向功能。請參閱[使用掃描器](#)。
- USB 音訊裝置的重新導向取決於網路的狀態, 而且並不可靠。即使處於閒置狀態, 一些裝置仍需要高資料流量。音訊輸入和輸出裝置可順利搭配即時音訊視訊功能運作。您不需要針對那些裝置使用 USB 重新導向。
- 除非您以管理員使用者身分連線, 否則您無法在已發佈的桌面平台中格式化重新導向的 USB 磁碟機。
- 已發佈的應用程式會在啟動時自動連線, 並在插入的功能不適用於全域應用程式權利時自動連線。

備註 請勿將 USB 裝置 (例如 USB 乙太網路裝置) 和觸控式螢幕裝置, 重新導向至遠端桌面平台或已發佈的應用程式。如果您重新導向 USB 乙太網路裝置, 您的用戶端系統會失去網路連線。如果您重新導向觸控式螢幕裝置, 遠端桌面平台或已發佈的應用程式會接收到觸控輸入, 但不會接收到鍵盤輸入。如果您將遠端桌面平台或已發佈的應用程式設為自動連線 USB 裝置, 您可以設定原則以排除特定的裝置。

使用網路攝影機和麥克風

透過即時音訊視訊功能, 您將可在遠端桌面平台或已發佈的應用程式中使用本機用戶端系統的網路攝影機或麥克風。即時音訊視訊功能與標準會議應用程式和瀏覽器型視訊應用程式相容。它支援標準網路攝影機、音訊 USB 裝置以及類比音訊輸入。

如需在代理程式機器上設定即時音訊視訊功能的相關資訊 (包括設定畫面播放速率和影像解析度), 請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

將網路攝影機與即時音訊視訊功能搭配使用的時機

如果 Horizon 管理員已設定即時音訊視訊功能, 您即可在遠端桌面平台或已發佈的應用程式中使用內建於或連線至用戶端電腦的網路攝影機。您可在會議應用程式, 如 Skype、Webex 或 Google Hangouts 使用網路攝影機。

在遠端桌面平台設定應用程式 (如 Skype、Webex 或 Google Hangouts) 期間, 您可以從應用程式的功能表選取輸入和輸出裝置。

對於已安裝 Horizon Agent 7.9 或更早版本的虛擬桌面平台, 以及已發佈的桌面平台和已發佈的應用程式, 即時音訊視訊只能重新導向一個網路攝影機, 且網路攝影機在應用程式中會命名為 VMware 虛擬網路攝影機。對於已安裝 Horizon Agent 7.10 或更新版本的虛擬桌面平台, 即時音訊視訊可以重新導向多個網路攝影機, 且重新導向的網路攝影機名稱會是附加了 (VDI) 的實際裝置名稱, 例如 C670i FHD 網路攝影機 (VDI)。

對於許多應用程式, 您都不需要選取輸入裝置。

當用戶端電腦使用網路攝影機時，遠端工作階段無法同時使用該攝影機。此外，當遠端工作階段使用網路攝影機時，用戶端電腦即無法同時使用該攝影機。

重要 如果您使用 USB 網路攝影機，請勿從 Horizon Client 中的**連線 USB 裝置**功能表加以連線。如果這麼做，則會透過 USB 重新導向路由該裝置，且其效能將無法用於視訊聊天。

如果有多個網路攝影機連線至用戶端電腦，您必須設定偏好的網路攝影機，以用於已發佈的桌面平台和已發佈的應用程式之遠端工作階段，以及用於不支援多個網路攝影機的虛擬桌面平台。

如需詳細資訊，請參閱在 [Windows 用戶端系統上選取偏好的網路攝影機或麥克風](#)。

在 Windows 用戶端系統上選取偏好的網路攝影機或麥克風

在使用即時音訊視訊功能時，如果有多個網路攝影機或麥克風連線至用戶端系統，則您可以透過在 Horizon Client 中設定即時音訊視訊設定，來指定偏好的網路攝影機或麥克風。

使用即時音訊視訊功能時，視訊裝置、音訊輸入裝置和音訊輸出裝置可在不需使用 USB 重新導向的情況下正常運作，且會大幅降低所需的網路頻寬量。同時支援類比音訊輸入裝置。

如果可用，則會在遠端桌面平台或已發佈的應用程式中使用偏好的網路攝影機或麥克風。如果偏好的網路攝影機或麥克風無法使用，則會使用另一個網路攝影機或麥克風。

備註 如果您使用 USB 網路攝影機或麥克風，請勿從 Horizon Client 中的**連線 USB 裝置**功能表進行連線。如果這麼做，則會透過 USB 重新導向路由該裝置，且該裝置無法使用即時音訊視訊功能。

對於已安裝 Horizon Agent 7.10 或更新版本的虛擬桌面平台，即時音訊視訊功能支援多個網路攝影機和麥克風裝置。

必要條件

- 確認已在用戶端系統上安裝 USB 網路攝影機、USB 麥克風或其他類型的麥克風，並且可運作。
- 確認您為遠端桌面平台或已發佈的應用程式使用了 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定。
- 連線至伺服器。

程序

- 1 開啟**設定**對話方塊，並選取左窗格中的**即時音訊視訊**。
 - 在桌面平台和應用程式選取器視窗的右上角，按一下**設定** (齒輪) 圖示。
 - 在遠端桌面平台和應用程式選取器視窗中，以滑鼠右鍵按一下遠端桌面平台或已發佈的應用程式，然後選取**設定**。
- 2 若要設定偏好的網路攝影機，請從**偏好的網路攝影機**下拉式功能表中選取網路攝影機。
- 3 若要設定偏好的麥克風，請從**偏好的麥克風**下拉式功能表中選取特定的麥克風，或選取**全部**。

如果遠端桌面平台支援多個具有即時音訊視訊功能的裝置，而您選取特定的麥克風，則只有選取的麥克風和網路攝影機裝置會重新導向至遠端桌面平台。如果您選取**全部**，則所有可用的麥克風和網路攝影機裝置都會重新導向至遠端桌面平台。

4 若要儲存變更，請按一下**確定**或**套用**。

搭配即時音訊視訊功能使用多個裝置

如果有多個網路攝影機或麥克風連線至用戶端電腦，且遠端桌面平台支援使用即時音訊視訊功能來進行多個裝置重新導向，則您可以在遠端桌面平台中使用所有連線至用戶端電腦的網路攝影機和麥克風。

只有已安裝 Horizon Agent 7.10 或更新版本的虛擬桌面平台才支援此功能。已發佈的桌面平台或已發佈的應用程式不支援此功能。如需完整的系統需求，請參閱[即時音訊視訊系統需求](#)。

以下是搭配即時音訊視訊功能來使用多個網路攝影機或麥克風的提示。

- 當您連線至遠端桌面平台時，即時音訊視訊功能會將目前連線至用戶端電腦的所有網路攝影機和麥克風重新導向。遠端桌面平台會決定哪個網路攝影機和麥克風是預設裝置。您不需要在 Horizon Client 中設定偏好的網路攝影機或麥克風。
- 如果您想要在商務用 Skype 等應用程式中依預設使用相同的麥克風，您必須設定預設麥克風。否則，所有麥克風都會重新導向，且您必須在每次使用應用程式時選取麥克風。如需詳細資訊，請參閱在[Windows 用戶端系統上選取偏好的網路攝影機或麥克風](#)。
- 如果您將網路攝影機或麥克風與用戶端電腦中斷連線，且該裝置並未用於遠端桌面平台中的應用程式，則即時音訊視訊功能會立即在遠端桌面平台中刪除該裝置。如果該裝置正由遠端桌面平台中的應用程式使用中，則即時音訊視訊功能會在應用程式釋放該裝置後將其刪除。
- 重新導向裝置的顯示名稱為實際的裝置名稱，但會附加 (VDI)，例如 C670i FHD 網路攝影機 (VDI)。
- 您可以在遠端桌面平台中同時使用多個重新導向的裝置。

選取遠端桌面平台的慣用喇叭

如果用戶端系統連接了多個喇叭，您可以指定遠端桌面平台中慣用的喇叭。

這項功能具有下列的限制。

- 僅虛擬桌面平台支援此功能。已發佈的桌面平台和已發佈的應用程式不支援此功能。
- 如果在遠端工作階段期間從用戶端系統新增或移除喇叭，則這些變更不會在遠端桌面平台中生效。

必要條件

- 確認已在用戶端系統上安裝多個喇叭且可運作。
- 確認您正在使用 VMware Blast 顯示通訊協定連線至遠端桌面平台。此功能無法與任何其他顯示通訊協定搭配使用。
- 確認已在遠端桌面平台中安裝 Horizon Agent 2012 或更新版本。對於舊版 Horizon Agent，音訊會在連接至用戶端系統的預設音訊裝置上播放。
- 連線至伺服器。

程序

- 1 開啟**設定**對話方塊，並選取左窗格中的**即時音訊視訊**。
 - 在桌面平台和應用程式選取器視窗的右上角，按一下**設定** (齒輪) 圖示。

- 在桌面平台和應用程式選取器視窗中，以滑鼠右鍵按一下遠端桌面平台，然後選取**設定**。

2 從慣用的喇叭下拉式功能表中，選取一個喇叭。

備註 此功能與即時音訊視訊功能無關，即使顯示在**即時音訊視訊**頁面上也是如此。

如果您選取特定的喇叭，則只會將選取的喇叭重新導向至遠端桌面平台。如果您選取**全部**，則會將所有可用的喇叭重新導向至遠端桌面平台。如果您選取**預設**，音訊會在連接至用戶端系統的預設音訊裝置上播放。

3 若要儲存變更，請按一下**確定**或**套用**。

共用遠端桌面平台工作階段

透過工作階段協作功能，您可以邀請其他使用者加入現有的遠端桌面平台工作階段。以這種方式共用的遠端桌面平台工作階段稱為協作工作階段。與其他使用者共用工作階段的使用者稱為工作階段擁有者，而加入共用工作階段的使用者則稱為工作階段協作者。

Horizon 管理員必須啟用工作階段協作功能。

對於 Windows 桌面平台，這項工作包括在桌面平台集區或伺服器陣列層級上啟用工作階段協作功能。此外也包括使用群組原則設定工作階段協作功能，例如可用的邀請方法。如需完整需求，請參閱[工作階段協作功能的需求](#)。

如需為 Windows 桌面平台啟用工作階段協作功能的相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》文件。如需為伺服器陣列啟用工作階段協作功能的相關資訊，請參閱《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。如需使用群組原則設定來設定工作階段協作功能的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

如需為 Linux 桌面平台啟用工作階段協作功能的相關資訊，請參閱《在 Horizon 中設定 Linux 桌面平台》文件。

邀請使用者加入遠端桌面平台工作階段

透過工作階段協作功能，您可以透過電子郵件、即時訊息 (僅限 Windows 遠端桌面平台) 或將連結複製到剪貼簿並將連結轉送至使用者，來邀請使用者加入遠端桌面平台工作階段。

您僅能邀請屬於伺服器允許驗證之網域的使用者。依預設，您最多可以邀請五個使用者。Horizon 管理員可變更您可以邀請的使用者數目上限。

工作階段協作功能具有下列限制。

- 如果您有多部監視器，則工作階段協作者將只會看見主要監視器。
- 當您建立要共用的遠端桌面平台工作階段時，必須選取 VMware Blast 顯示通訊協定。工作階段協作功能不支援 PCoIP 或 RDP 工作階段。
- 不支援 H.264 硬體編碼。如果工作階段擁有者使用硬體編碼，則當協作者加入工作階段時，兩者皆會回復為使用軟體編碼。
- 不支援匿名協作。工作階段協作者必須可透過 Horizon 支援的驗證機制進行識別。

- 工作階段協作者必須已安裝 Windows、Mac 或 Linux 版 Horizon Client，或必須使用 HTML Access。
- 如果工作階段使用協作者具有不受支援的 Horizon Client 版本，則使用者按一下協作連結時將會顯示錯誤訊息。
- 您無法使用工作階段協作功能來共用已發佈的應用程式工作階段。

必要條件

- 必須啟用並設定工作階段協作功能。
- 若要使用電子郵件邀請方法，則必須安裝電子郵件應用程式。
- 若要使用 Windows 遠端桌面平台的 IM 邀請方法，必須安裝和設定商務用 Skype。

程序

- 1 連線至已啟用工作階段協作功能的遠端桌面平台。

您必須使用 VMware Blast 顯示通訊協定。

- 2 在遠端桌面平台的系統匣中，按一下 **VMware Horizon 協作** 圖示，例如 。

此協作圖示的外觀會隨作業系統版本而有所不同。

- 3 在 [VMware Horizon 協作] 對話方塊開啟時，輸入使用者名稱 (例如 **testuser** 或 **domain\testuser**)，或輸入想要加入遠端桌面平台工作階段之使用者的電子郵件地址。

第一次輸入特定使用者的使用者名稱或電子郵件地址時，您必須按一下**查閱「user」**、輸入逗號 (,)，或按 **Enter** 鍵以驗證使用者。針對 Windows 遠端桌面平台，工作階段協作功能會在您下次輸入使用者的使用者名稱或電子郵件地址時記住使用者。

- 4 選取邀請方法。

並非所有邀請方法都適用。

選項	動作
電子郵件	將協作邀請複製到剪貼簿，並在預設電子郵件應用程式中開啟新的電子郵件訊息。必須安裝電子郵件應用程式才能使用此邀請方法。
即時訊息 (IM)	(僅適用於 Windows 遠端桌面平台) 將協作邀請複製到剪貼簿，並在商務用 Skype 中開啟新的視窗。按 Ctrl+V 將連結貼到商務用 Skype 視窗中。必須安裝並設定商務用 Skype 才能使用此邀請方法。
複製連結	將協作邀請複製到剪貼簿。您必須手動開啟另一個應用程式 (例如「記事本」)，然後按 Ctrl+V 貼上邀請。

結果

在您傳送邀請後，VMware Horizon 協作圖示也會出現在桌面平台上，而工作階段協作使用者介面會變為儀表板，其中顯示目前協作工作階段的狀態，且可讓您執行特定動作。

當工作階段協作者接受邀請以加入 Windows 遠端桌面工作階段時，工作階段協作功能會通知您，且系統匣中的 VMware Horizon 協作圖示上會出現紅點。當工作階段協作者接受邀請加入 Linux 遠端桌面工作階段時，主要工作階段桌面平台中會顯示通知。

後續步驟

在 [VMware Horizon 協作] 對話方塊中管理遠端桌面平台工作階段。請參閱[管理共用遠端桌面平台工作階段](#)。

管理共用遠端桌面平台工作階段

在您傳送工作階段協作邀請後，工作階段協作者使用者介面會變成儀表板，其中顯示目前共用遠端桌面平台工作階段 (協作工作階段) 的狀態，且可讓您執行特定動作。

Horizon 管理員可以防止將控制權移交給工作階段協作者。針對 Windows 遠端桌面平台，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中的[允許將控制傳送至協作者](#)群組原則設定。針對 Linux 遠端桌面平台，請參閱《在 Horizon 中設定 Linux 桌面平台》文件中的 `collaboration.enableControlPassing` 參數。

必要條件

啟動協作工作階段。請參閱[邀請使用者加入遠端桌面平台工作階段](#)。

程序

- 1 在遠端桌面平台中，按一下系統匣中的 **VMware Horizon 協作** 圖示。
所有工作階段協作者的名稱都會出現在 [名稱] 欄中，其狀態則出現在 [狀態] 欄中。
- 2 使用 VMware Horizon 工作階段協作儀表板以管理協作工作階段。

選項	動作
撤銷邀請或移除協作者	在 [狀態] 欄中，按一下 移除 。
將控制權移交給工作階段協作者	工作階段協作者加入工作階段後，請將 [控制] 欄中的開關切換為 開啟 。 若要取回工作階段的控制權，請按兩下或按任意鍵。工作階段協作者也可藉由將 [控制] 欄中的開關切換為 關閉 ，或按一下 交回控制權 按鈕來交回控制權。
新增協作者	按一下 新增協作者 。
結束協作工作階段	按一下 結束協作 。所有作用中協作者的連線都會中斷。 在 Windows 遠端桌面平台中，您也可以按一下 VMware Horizon 工作階段協作 圖示旁的 停止 按鈕，結束協作工作階段。在 Linux 遠端桌面平台無法使用 停止 按鈕。

加入遠端桌面平台工作階段

透過工作階段協作功能，您可以按一下協作邀請中的連結來加入遠端桌面平台工作階段。此連結可能位於電子郵件或即時訊息中，或是在工作階段擁有者轉送給您的文件中。或者，您可以登入伺服器，然後在遠端桌面平台和應用程式選取器視窗中按兩下工作階段的圖示。

下列程序說明如何經由協作邀請加入遠端桌面平台工作階段。

備註 在 Cloud Pod 架構環境中，您無法藉由登入伺服器來加入協作工作階段，除非您登入工作階段擁有者的網蔕。

當您使用工作階段協作功能加入遠端桌面平台工作階段時，您無法在遠端桌面平台工作階段中使用下列功能。

- USB 重新導向
- 即時音訊視訊 (RTAV)
- 多媒體重新導向
- 用戶端磁碟機重新導向
- 智慧卡重新導向
- VMware Integrated Printing
- Microsoft Lync 重新導向
- 檔案重新導向和保留在 Dock 中功能
- 剪貼簿重新導向

您也無法在遠端桌面平台工作階段中變更遠端桌面平台的解析度。

必要條件

若要使用工作階段協作功能來加入遠端桌面工作階段，您必須已在用戶端系統上安裝 Windows、Mac 或 Linux 版 Horizon Client，或必須使用 HTML Access。

程序

- 1 按一下協作邀請中的連結。

Horizon Client 會在用戶端系統上開啟。

- 2 輸入您的認證以登入 Horizon Client。

在您驗證成功之後，隨即開始協作工作階段，且您會看見工作階段擁有者的遠端桌面平台。如果工作階段擁有者將滑鼠和鍵盤控制權移轉給您，您即可使用遠端桌面平台。

- 3 若要將滑鼠和鍵盤控制權交還給工作階段擁有者，請按一下系統匣中的 **VMware Horizon 協作** 圖示，並將 [控制] 欄中的開關切換為 **關閉**，或按一下 **交回控制權** 按鈕。

- 4 若要退出協作工作階段，請按一下 **選項 > 中斷連線**。

共用本機資料夾和磁碟機

使用用戶端磁碟機重新導向功能，您可以將本機用戶端系統上的資料夾和磁碟機與遠端桌面平台和已發佈的應用程式共用。

共用磁碟機可包含對應的磁碟機和 USB 儲存裝置。對應的磁碟機可具有 UNC (通用命名慣例) 路徑。

共用資料夾名稱的最大長度為 117 個字元。

用戶端磁碟機重新導向功能不支援共用 Microsoft OneDrive、Google 雲端硬碟和企業檔案儲存區。

在 Windows 遠端桌面平台中，共用的資料夾和磁碟機會出現在**本機**資料夾或**電腦**資料夾中，視 Windows 作業系統版本而定。在記事本等已發佈的應用程式中，您可以瀏覽至共用的資料夾或磁碟機，並開啟其中的檔案。

用戶端磁碟機重新導向設定會套用至所有遠端桌面平台和已發佈的應用程式。

必要條件

若要與遠端桌面平台或已發佈的應用程式共用資料夾和磁碟，則必須在 Horizon Agent 中安裝用戶端磁碟機重新導向功能。依預設會安裝用戶端磁碟機重新導向功能。

您可以藉由啟用群組原則設定，在 Horizon Client 中隱藏用戶端磁碟機重新導向功能。如需詳細資訊，請參閱[用戶端 GPO 的一般設定](#)中的**停用共用檔案和資料夾**。

透過 Horizon Agent 7.8 及更新版本，您可以藉由設定**顯示含有磁碟機代號的重新導向裝置**群組原則設定，為用戶端磁碟機重新導向功能所重新導向的磁碟機設定磁碟機代號行為。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

透過 Horizon Agent 7.9 及更新版本，您可以使用**納入 Vid/Pid 裝置**和**排除 Vid/Pid 裝置**群組原則設定，在重新導向中納入或排除具有指定廠商和產品識別碼之裝置上的資料夾。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

使用 Horizon Agent 7.10 及更新版本時，您可以使用**設定磁碟機代號對應模式**和**定義磁碟機代號對應表**群組原則設定，來設定磁碟機代號的對應方式。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

如果已在連線伺服器執行個體上啟用安全通道，將用戶端系統上的瀏覽器設定為使用 Proxy 伺服器會導致用戶端磁碟機重新導向效能不佳。為了獲得最佳用戶端磁碟機重新導向效能，請將瀏覽器設定為不使用 Proxy 伺服器或自動偵測 LAN 設定。

程序

- 1 開啟 [設定] 對話方塊，並顯示 [共用] 面板。

選項	說明
從桌面平台和應用程式選取器視窗	在遠端桌面平台或已發佈的應用程式圖示上按一下滑鼠右鍵，選取 設定 ，然後選取出現在視窗左窗格中的 共用 。
從您連線至遠端桌面平台或已發佈的應用程式時會出現的 [共用] 對話方塊中	在對話方塊中按一下 設定 > 共用 連結。
從遠端桌面平台內	從功能表列中選取 選項 > 共用資料夾 。

2 進行用戶端磁碟機重新導向設定。

選項	動作
與遠端桌面平台和已發佈的應用程式共用特定資料夾或磁碟機	<p>按一下新增按鈕，瀏覽至要共用的資料夾或磁碟並加以選取，然後按一下確定。</p> <p>備註 如果 USB 裝置已利用 USB 重新導向功能連線到遠端桌面平台或已發佈的應用程式，則您無法共用 USB 裝置上的資料夾。</p> <p>另外，請勿開啟 USB 重新導向功能，這會在啟動時或插入裝置時自動連接 USB 裝置。如果您這麼做，則下次您啟動 Horizon Client 或插入 USB 裝置時，裝置將使用 USB 重新導向功能而非用戶端磁碟機重新導向功能來連接。</p> <p>如果已設定磁碟機代號對應，則不會重新導向在共用清單中設定的資料夾。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中的〈使用群組原則來設定磁碟機代號行為〉。</p>
停止共用特定資料夾或磁碟	在 [資料夾] 清單中選取資料夾或磁碟，然後按一下 移除 按鈕。
允許遠端桌面平台和已發佈的應用程式存取本機使用者目錄中的檔案	選取 共用您的本機檔案 <i>使用者-名稱</i> 核取方塊。
與遠端桌面平台及已發佈的應用程式共用 USB 儲存裝置	<p>選取允許存取卸除式儲存裝置核取方塊。用戶端磁碟機重新導向功能會自動共用用戶端系統中插入的所有 USB 儲存裝置，以及所有 FireWire 和 Thunderbolt 連線的外部磁碟。選取要共用的特定裝置並非必要。</p> <p>備註 系統不會共用已透過 USB 重新導向功能連線到遠端桌面平台或已發佈應用程式的 USB 儲存裝置。如果您使用加密的 USB 隨身碟，則在插入 USB 裝置之前必須先啟動 Horizon Client，以便 Horizon Client 可以偵測到該裝置。</p> <p>如果已取消選取此核取方塊，您就可以使用 USB 重新導向功能，將 USB 儲存裝置連線至遠端桌面平台和已發佈的應用程式。</p>
當您連線至遠端桌面平台或已發佈的應用程式時，不要顯示 [共用] 對話方塊	<p>選取連線至桌面平台或應用程式時不要顯示對話方塊核取方塊。</p> <p>如果取消選取此核取方塊，則當您第一次連線至遠端桌面平台或已發佈的應用程式時，即會出現 [共用] 對話方塊。例如，如果您登入伺服器並連線至遠端桌面平台，您就會看到 [共用] 對話方塊。如果您後來連線至其他遠端桌面平台或已發佈的應用程式，您就不會看到該對話方塊。若要再看到該對話方塊，您必須中斷與伺服器的連線，並再次登入。</p>

後續步驟

確認您可以從遠端桌面平台或已發佈的應用程式內部看到共用的資料夾。

- 在 Windows 遠端桌面平台中，開啟 [檔案總管]，然後在**本機**資料夾中查詢，或開啟 Windows 檔案總管並在**電腦**資料夾中查詢，視 Windows 作業系統版本而定。
- 在發佈的應用程式中，選取**檔案 > 開啟**或**檔案 > 另存新檔**，然後導覽至資料夾或磁碟機。

您選取要共用的資料夾和磁碟機可能會使用下列一個 (或多個) 命名慣例。

命名慣例	範例
<i>folder-name on desktop-name</i>	jsmith on JSMITH-W03
<i>folder-name (drive-number:)</i>	jsmith (Z:)
<i>folder-name on desktoptop-name (drive-number:)</i>	jsmith on JSMITH-W03 (Z:)

對於某些 Horizon Agent 版本，重新導向的資料夾可以具有兩個入口，例如 Windows 10 中的**裝置和磁碟機及網路位置**下方，而這兩個入口會同時顯示。如果所有磁碟區標籤 (從 A: 到 Z:) 都已在使用中，則重新導向的資料夾只會有一個入口。

在已發佈的應用程式中開啟本機檔案

您可以開啟從本機檔案系統直接在已發佈的應用程式中開啟本機檔案的功能。

透過此功能，當您在本機檔案上按一下滑鼠右鍵時，用戶端系統上的**開啟方式**功能表會列出可用的已發佈應用程式。

您也可以設定在按兩下檔案時，自動在已發佈的應用程式中開啟檔案。利用此功能，本機檔案系統中具有特定副檔名的所有檔案都會向您登入的伺服器進行登錄。例如，如果 Microsoft Word 是伺服器上的已發佈應用程式，您可以在本機檔案系統上的 .docx 檔案上按一下滑鼠右鍵，然後以 Microsoft Word 已發佈的應用程式開啟該檔案。

必要條件

若要在已發佈的應用程式中開啟本機檔案，Horizon 管理員必須在 Horizon Agent 中安裝用戶端磁碟機重新導向功能。依預設會安裝用戶端磁碟機重新導向功能。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

您可以藉由啟用群組原則設定，在 Horizon Client 中隱藏用戶端磁碟機重新導向功能。如需詳細資訊，請參閱[用戶端 GPO 的一般設定](#)中的**停用共用檔案和資料夾**。

程序

- 1 連線至伺服器。
- 2 開啟 [設定] 對話方塊，並顯示 [共用] 面板。

選項	說明
從桌面平台和應用程式選取器視窗	在遠端桌面平台或已發佈的應用程式圖示上按一下滑鼠右鍵，選取 設定 ，然後選取出現在視窗左窗格中的 共用 。
從您連線至遠端桌面平台或已發佈的應用程式時會出現的 [共用] 對話方塊中	在對話方塊中按一下 設定 > 共用 連結。
從遠端桌面平台內	從功能表列中選取 選項 > 共用資料夾 。

- 3 選取在**主控應用程式中開啟本機檔案**核取方塊。

將此選項啟用時，您可以在本機檔案系統中的檔案上按一下滑鼠右鍵，並選取在已發佈的應用程式中開啟檔案。您也可以變更檔案的內容，讓所有具備該副檔名的檔案依預設以已發佈的應用程式開啟 (例如當您按兩下檔案時)。例如，您可以在檔案上按一下滑鼠右鍵，選取**內容**，並按一下**變更**，選取要用來開啟該檔案類型的已發佈應用程式。

複製與貼上

依預設，您可以從用戶端系統複製並貼到遠端桌面平台或已發佈的應用程式。

如果您使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定，則 Horizon 管理員可將此功能設定為僅允許從用戶端系統複製並貼到遠端桌面平台或已發佈的應用程式、僅允許從遠端桌面平台或已發佈的應用程式複製並貼到用戶端系統、二者皆可或二者皆不可。

Horizon 管理員會藉由設定代理程式群組原則來設定複製和貼上的能力。根據 Horizon Server 和代理程式版本，Horizon 管理員可能也可以使用群組原則來限制複製並貼上作業期間的剪貼簿格式，或使用智慧型原則來控制遠端桌面平台中的複製並貼上行為。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

複製與貼上文字和影像

依預設，您可以從用戶端系統複製並貼到遠端桌面平台或已發佈的應用程式。您也可以從遠端桌面平台或已發佈的應用程式複製並貼上到用戶端系統，或是在兩個遠端桌面平台或已發佈的應用程式之間複製並貼上 (如果 Horizon 管理員啟用這些功能)。

支援的資料格式如下。

- CF_BITMAP
- CF_DIB
- CF_HDROP (檔案類型)
- CF_UNICODETEXT
- Biff12
- Art::GVML ClipFormat
- HTML 格式
- RTF (Rich Text Format)

例如，若要在用戶端系統上複製文字，請選取文字，然後按下 **Ctrl+C**。若要將文字貼上到遠端桌面平台，請在遠端桌面平台中按下 **Ctrl+V**。

這項功能具有下列的限制。

- 如果您複製格式化文字，一些資料為文字，而另一些資料為格式資訊。如果複製大量格式化文字或文字和影像，當您嘗試貼上文字和影像時，您可能會看到一些或全部的純文字，但沒有任何格式或影像。之所以發生此問題，是因為這三種類型的資料有時是單獨存放的。例如，依據文件的類型，影像可能會存放為影像或 RTF 資料。
- 如果文字和 RTF 資料的總使用量少於剪貼簿的大小上限，則會貼上格式化文字。RTF 資料通常無法截斷，因此如果文字和格式化的總使用量超過剪貼簿的大小上限，則會捨棄 RTF 資料，而僅貼上純文字。
- 如果您無法貼上單次操作所選的所有格式化文字和影像，您在每次操作時可能需要複製和貼上較少量的資料。

複製和貼上檔案及資料夾

依預設，您可以從用戶端系統將檔案和資料夾複製並貼到遠端桌面平台或已發佈的應用程式。如果 Horizon 管理員啟用這些功能，則您也可以從遠端桌面平台或已發佈的應用程式將檔案和資料夾複製並貼到用戶端系統。

例如，若要在用戶端系統上複製檔案，請選取檔案，然後按下 **Ctrl+C**。若要將檔案貼上到遠端桌面平台，請在遠端桌面平台中按下 **Ctrl+V**。

此功能需要在代理程式機器上安裝 Horizon Agent 2012 或更新版本。

若要使用此功能，則必須在代理程式機器上安裝用戶端磁碟機重新導向功能。如需詳細資訊，請參閱《在 Horizon 中設定虛擬桌面平台》或《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

您可以停用此功能，方法是在代理程式機器的**設定剪貼簿重新導向格式**群組原則設定中，啟用**從傳入的剪貼簿資料中篩選檔案和資料夾**和**從傳出的剪貼簿資料中篩選檔案和資料夾**設定。如需控制此功能的代理程式群組原則設定的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

這項功能具有下列的限制。

- 當您嘗試複製並貼上多個檔案時，對某些特殊資料夾可能沒有作用 (例如桌面資料夾或最近存取的檔案清單資料夾)，原因在於該資料夾可能會顯示不在相同父資料夾中的檔案和資料夾。此功能僅能複製並貼上位於相同父資料夾中的檔案和資料夾。
- 對於某些應用程式 (例如 WordPad 和 PowerPoint)，此功能可能無法正常運作。

記錄複製和貼上活動

當您啟用剪貼簿稽核功能時，Horizon Agent 會在代理程式機器上的事件記錄中記錄關於複製和貼上活動的資訊。剪貼簿稽核功能依預設為停用。

此功能僅適用於複製和貼上文字及影像。不適用於複製和貼上檔案及資料夾。

若要啟用剪貼簿稽核功能，您必須設定**設定剪貼簿稽核**群組原則設定。

如果 Horizon Agent 7.6 安裝在代理程式機器上，則事件記錄中僅會記錄從代理程式機器複製到用戶端電腦的剪貼簿資料相關資訊。如果 Horizon Agent 7.7 或更新版本安裝在代理程式機器上，則您可以將剪貼簿稽核功能設定為僅記錄從用戶端電腦複製到代理程式機器的資料相關資訊、僅記錄從代理程式機器複製到用戶端電腦的資料相關資訊，或同時記錄雙向複製的資料相關資訊。

您可以選擇設定**當用戶端不支援稽核時，是否封鎖對用戶端的剪貼簿重新導向**群組原則設定，以指定是否對不支援剪貼簿稽核功能的用戶端封鎖剪貼簿重新導向。

如需用於剪貼簿重新導向的群組原則設定的詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

記錄複製和貼上活動相關資訊的事件記錄稱為 VMware Horizon RX Audit。若要在代理程式機器上檢視事件記錄，請使用 Windows 事件檢視器。若要從集中位置檢視事件記錄，請設定 VMware Log Insight 或 Windows Event Collector。如需 Log Insight 的相關資訊，請移至 <https://docs.vmware.com/tw/vRealize-Log-Insight/index.html>。如需 Windows Event Collector 的相關資訊，請參閱 Microsoft 說明文件。

設定用戶端剪貼簿記憶體大小

您可以為伺服器 and 用戶端設定剪貼簿記憶體大小。

此功能僅適用於複製和貼上文字及影像。不適用於複製和貼上檔案及資料夾。

建立 PCoIP 或 VMware Blast 工作階段時，伺服器會將其剪貼簿記憶體大小傳送至用戶端。有效的剪貼簿記憶體大小是比伺服器 and 用戶端剪貼簿記憶體大小更小的值。

若要設定用戶端剪貼簿記憶體大小，請修改 Windows 登錄值 HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize。值類型為 REG_DWORD。指定值的單位為 KB。如果指定 0 或未指定值，預設的用戶端剪貼簿記憶體大小將是 8192 KB (8 MB)。

取決於您的網路，如果剪貼簿記憶體大小太大，可能會影響效能。VMware 建議您不要將剪貼簿記憶體大小設定為超過 16 MB 的值。

複製和貼上作業的剪貼簿記憶體大小上限為 65,535 KB。由於此限制包括中繼資料和格式設定資料，因此實際資料大小必須小於 65,535 KB。若要傳輸大量資料，請使用用戶端磁碟機重新導向功能。

拖放

視 Horizon Agent 版本和其設定方式而定，拖放功能運作方式有所不同。

透過 Horizon Agent 7.9 及更新版本，您可以拖放用戶端系統和遠端桌面平台和已發佈應用程式之間的檔案、資料夾、文字、RTF 文字和影像。對於 Horizon Agent 7.7 及 7.8，您在用戶端系統和遠端桌面平台與已發佈的應用程式之間只能拖放檔案和資料夾。較早的 Horizon Agent 版本不支援拖放。

根據 Horizon Agent 版本，Horizon 管理員可使用特定的群組原則設定或智慧型原則來設定拖放行為。如需關於設定拖放功能的完整資訊，請參閱您 VMware Horizon 版本的《在 Horizon 中設定遠端桌面平台功能》文件。

拖曳文字和影像

使用 Horizon Agent 7.9 及更新版本時，您可以從用戶端系統將文字、影像和其他資料格式拖曳至已在遠端桌面平台中開啟的應用程式或已發佈的應用程式。例如，您可以將文字從用戶端系統上的瀏覽器拖曳到遠端桌面平台中的 WordPad 應用程式。取決於對拖放功能的設定，您也可以將文字、影像和其他資料格式從已在遠端桌面平台中開啟的應用程式或已發佈的應用程式拖曳到用戶端系統。

支援的資料格式如下。

- HTML 格式
- RTF 文字格式 (RTF)
- CF_BITMAP
- CF_DIB
- CF_UNICODETEXT
- FileGroupDescriptorW
- FileGroupDescriptor

■ FileContents

Horizon 管理員可以設定群組原則設定來設定拖放行為。對於 Horizon Agent 7.9 和 Dynamic Environment Manager 9.8 及更新版本，Horizon 管理員也可使用智慧型原則來設定拖放行為，包括完全停用拖放功能。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

拖曳檔案和資料夾

透過 Horizon Agent 7.7 及更新版本，您可以在 Windows 用戶端系統和遠端桌面平台與已發佈的應用程式之間拖放檔案和資料夾。您可以同時拖放多個檔案和資料夾。進度列會顯示拖放作業的狀態。

如果在用戶端系統與遠端桌面平台之間拖曳檔案或資料夾，檔案或資料夾將會顯示在目標系統的檔案系統中。如果您將檔案拖放到開啟的應用程式 (例如記事本) 中，文字將顯示在該應用程式中。如果您將檔案拖放新的電子郵件訊息中，檔案將成為該電子郵件訊息的附件。

依預設，從用戶端系統拖放到遠端桌面平台和已發佈應用程式的功能為啟用，且從遠端桌面平台和已發佈的應用程式拖放到用戶端系統的功能為停用。Horizon 管理員可以設定群組原則設定來控制拖放方向。

拖放檔案、資料夾和檔案內容的操作需要在 Horizon Agent 中安裝用戶端磁碟機重新導向功能。依預設會安裝用戶端磁碟機重新導向功能。如需關於設定拖放功能 (包括功能需求) 的完整資訊，請參閱您 VMware Horizon 版本的《在 Horizon 中設定遠端桌面平台功能》文件。

使用拖放功能的提示

使用拖放功能時，請遵循下列提示。

備註 視 Horizon Agent 版本而定，某些提示可能不適用於您的環境。

- 您必須使用 VMware Blast 或 PCoIP 顯示通訊協定。
- 如果啟用了相對滑鼠功能 (**選項 > 啟用相對滑鼠**)，則只能從用戶端系統拖放到虛擬桌面平台。
- 拖放作業正在進行時，您必須等到該拖放作業完成後才能啟動新的拖放作業。
- 您無法在巢狀模式中使用拖放功能。
- 進行拖放時，您必須使用主要滑鼠按鈕 (依預設為左按鈕)。不支援使用次要滑鼠按鈕 (依預設為右按鈕)，也不支援按住 **Ctrl+Shift+Alt** 再按主要滑鼠按鈕。
- 您無法在遠端桌面平台之間進行拖放。
- 您無法在不同伺服器陣列中已發佈的應用程式之間進行拖放。
- 如果在用戶端系統與遠端桌面平台之間拖放檔案或資料夾，檔案或資料夾將會顯示在目標系統的檔案系統中。如果您將檔案拖放到開啟的應用程式 (例如記事本) 中，文字將顯示在該應用程式中。如果您將檔案拖放新的電子郵件訊息中，檔案將成為該電子郵件訊息的附件。
- 您可以同時拖放多個檔案和資料夾。進度列會顯示拖放作業的狀態。
- 依預設，從用戶端系統拖放到遠端桌面平台和已發佈應用程式的功能為啟用，且從遠端桌面平台和已發佈的應用程式拖放到用戶端系統的功能為停用。

- 如果您拖曳格式化的文字，一些資料為文字，而另一些資料為格式資訊。如果拖曳大量格式化的文字或文字和影像，當您嘗試拖放文字和影像時，您可能會看到一些或全部的純文字，但沒有任何格式或影像。之所以發生此問題，是因為這三種類型的資料有時是單獨存放的。例如，依據文件的類型，影像可能會存放為影像或 RTF 資料。
- 如果您同時拖曳純文字和 RTF 資料，而資料大小總計小於拖放大小臨界值，就會複製格式化的文字。因為 RTF 資料無法截斷，如果資料大小總計大於拖放大小臨界值，則會捨棄 RTF 資料並僅複製純文字 (或部分純文字)。
- 如果您無法拖曳單次操作的所有格式化的文字和影像，每次操作時您可能需要拖曳較少量的資料。
- 將檔案從用戶端系統拖放到已發佈的應用程式時，您無法透過按一下**另存新檔**將檔案複製回用戶端系統上的其他檔案。您可以透過按一下**儲存**，將檔案複製回用戶端系統上的相同檔案。
- 如果您將檔案從用戶端系統拖曳到遠端桌面平台中的應用程式，該檔案會複製到遠端桌面平台，且您只能編輯檔案的複本。
- 在 64 位元 Windows 機器中，如果您無法從 Horizon Client 拖曳到本機 64 位元應用程式，請嘗試使用 32 位元版本的本機應用程式。
- 如果目標本機應用程式無法接受拖曳的物件，請嘗試將物件拖曳到本機檔案系統，然後從本機檔案系統將其拖曳到目標本機應用程式。
- 存在用於 Fault Tolerance 的內建逾時機制。

已發佈應用程式的使用提示

已發佈應用程式的外觀與風格類似於本機用戶端系統上安裝的應用程式。使用已發佈的應用程式時，請遵循下列提示。

- 您可以透過已發佈的應用程式來最小化和最大化已發佈的應用程式。當已發佈的應用程式最小化時，它會出現在用戶端系統的工作列中。您也可以在工作列中按一下已發佈應用程式的圖示，將其最小化和最大化。
- 您可以透過已發佈的應用程式，或在工作列中以滑鼠右鍵按一下應用程式的圖示，以結束已發佈的應用程式。
- 您可以按下 **Alt+Tab** 在開啟的已發佈應用程式之間切換。
- 如果已發佈的應用程式建立了 Windows 系統匣項目，該項目也會出現在用戶端系統的系統匣中。依預設，系統匣圖示只是為了顯示通知。您可以比照自訂原生安裝之應用程式的相同方式來自訂此行為。

備註 如果您開啟 [控制台] 以自訂通知區域圖示，則已發佈應用程式的圖示名稱將列出為 [VMware Horizon Client - 應用程式名稱]。

中斷連線之後重新連線至已發佈的應用程式

您在 Horizon Client 中斷伺服器的連線後，執行中的已發佈應用程式仍可保持開啟。您可以設定在 Horizon Client 重新連線至伺服器時，執行中的已發佈應用程式將如何運作。

您可以透過命令列或藉由設定群組原則設定，在 Horizon Client 中停用已發佈應用程式的重新連線行為設定。群組原則設定優先於命令列設定。如需詳細資訊，請參閱 [Horizon Client 命令使用中的 -appSessionReconnectionBehavior 選項](#)，或 [用戶端 GPO 的指令碼定義設定中的 Disconnected application session resumption behavior 群組原則設定](#)。

程序

- 1 在 Horizon Client 桌面平台與應用程式選取器視窗中，於已發佈的應用程式上按一下滑鼠右鍵，然後選取**設定**。
- 2 在 [遠端應用程式] 窗格中，選取應用程式重新連線行為設定。

選項	說明
要求重新連線以開啟已發佈的應用程式	當您重新連線至伺服器時，Horizon Client 會通知您有一或多個已發佈的應用程式正在執行。您可以按一下 重新連線到應用程式 以重新開啟已發佈的應用程式視窗，或按一下 現在不要 而不重新開啟已發佈的應用程式視窗。
自動重新連線以開啟已發佈的應用程式	當您重新連線至伺服器時，執行中的已發佈應用程式的視窗會重新開啟。
不要求重新連線，且不自動重新連線	當您重新連線至伺服器時，Horizon Client 不會提示您重新開啟執行中的已發佈應用程式，且執行中的已發佈應用程式視窗不會重新開啟。

- 3 若要儲存變更，請按一下**確定**。

結果

下次 Horizon Client 連線至伺服器時，設定便會生效。

從不同用戶端裝置使用已發佈應用程式的多重工作階段

為已發佈的應用程式啟用多重工作階段模式時，當您從不同用戶端裝置登入伺服器，可以使用同一個已發佈應用程式的多重工作階段。

例如，如果您以多重工作階段模式在用戶端 A 上開啟已發佈的應用程式，然後在用戶端 B 上開啟同一個已發佈的應用程式，已發佈的應用程式會在用戶端 A 上保持開啟，且該已發佈的應用程式會在用戶端 B 上開啟新工作階段。相較之下，停用多重工作階段模式時(單一工作階段模式)，已發佈的應用程式在用戶端 A 上的工作階段會中斷連線，而在用戶端 B 上重新連線。

多重工作階段模式功能具有下列限制。

- 多重工作階段模式不適用於不支援多個執行個體的應用程式，例如商務用 Skype。
- 當您在多重工作階段模式下使用已發佈的應用程式時，如果應用程式工作階段中斷連線，則系統會自動將您登出，且任何未儲存的資料都將遺失。

必要條件

Horizon 管理員必須為應用程式集區的啟用多重工作階段模式。除非 Horizon 管理員允許，否則使用者無法修改已發佈應用程式的多重工作階段模式。請參閱《[在 Horizon 中設定已發佈的桌面平台和應用程式](#)》。此功能需要 Horizon 7 (7.7 版) 或更新版本。

程序

- 1 連線至伺服器。
- 2 開啟 [設定] 對話方塊，並選取左窗格中的**多重啟動**。
 - 在桌面平台和應用程式選取視窗的右上角，按一下**設定** (齒輪) 圖示。
 - 在桌面平台和應用程式選取視窗中，以滑鼠右鍵按一下遠端桌面平台或已發佈的應用程式，然後選取**設定**。

如果沒有可在多重工作階段模式中使用的已發佈應用程式，則**多重啟動**設定不會顯示。

- 3 選取您想要在多重工作階段模式中使用的已發佈應用程式，然後按一下**確定**。

對於已發佈的應用程式，如果 Horizon 管理員已強制執行多重工作階段模式，則您無法變更此設定。

將本機 IME 與已發佈的應用程式搭配使用

如果您使用非英文鍵盤和地區設定，可以使用本機用戶端系統中安裝的 IME (輸入法編輯器)，將非英文字元傳送至已發佈的應用程式。

您可以使用本機用戶端系統的通知區域 (系統匣) 中的快速鍵與圖示，切換至不同的 IME。您不需要在主控已發佈應用程式的伺服器上安裝 IME。

啟用此功能時，系統會使用本機 IME。如果在主控已發佈應用程式的伺服器上安裝並設定了某個 IME，該遠端 IME 將會被忽略。

此功能依預設為停用。啟用或停用此功能時，您必須從伺服器中斷連線並再次登入才能讓變更生效。

必要條件

- 請確認用戶端系統中安裝有一或多個 IME。
- 確認本機用戶端系統上的輸入語言與 IME 中使用的語言相符。

程序

- 1 在 Horizon Client 桌面平台與應用程式選取器視窗中，於已發佈的應用程式上按一下滑鼠右鍵，然後選取**設定**。
- 2 在 [遠端應用程式] 窗格中，選取**將本機 IME 延伸至主控應用程式**核取方塊，然後按一下**確定**。
- 3 重新啟動工作階段。

選項	動作
登出伺服器	從伺服器中斷連線、重新登入，並重新連線至已發佈的應用程式。您可以繼續使用中斷連線但未關閉的已發佈應用程式，以及任何遠端桌面平台。
重設應用程式	在已發佈的應用程式圖示上按一下滑鼠右鍵，選取 設定 ，然後按一下 重設 。使用此選項時，任何開啟的遠端桌面平台不會中斷連線，但所有已發佈的應用程式會關閉，且必須重新啟動。

此設定僅會在您重新啟動工作階段之後生效。此設定會套用至伺服器上所有已發佈的應用程式。

- 4 使用本機 IME 的方式與您在本機安裝之應用程式上的使用方式相同。

結果

IME 的語言指定與圖示會出現在本機用戶端系統的通知區域 (系統匣)。您可以使用快速鍵切換至不同的語言或 IME。執行特定動作的按鍵組合 (例如用於剪下文字的 CTRL+X 與移動至不同索引標籤的 Alt + 向右鍵) 可正常運作。

備註 在 Windows 7 與 8.x 系統上，您可以使用文字服務和輸入語言對話方塊 (可在 **控制台 > 地區及語言 > [鍵盤及語言] 索引標籤 > [變更鍵盤] 按鈕 > 文字服務和輸入語言 > [進階按鍵設定] 索引標籤** 中找到) 來指定 IME 的快速鍵。

從遠端桌面平台或已發佈的應用程式列印

透過 VMware Integrated Printing 功能，您可以從遠端桌面平台或已發佈的應用程式列印至網路印表機或本機連結的印表機。

如需安裝 VMware Integrated Printing 功能的相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》或《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

如需設定 VMware Integrated Printing 功能的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

如需支援 VMware Integrated Printing 功能之遠端桌面平台類型的相關資訊，請參閱 [Windows 用戶端的功能支援](#)。

設定 VMware Integrated Printing 功能的列印喜好設定

您可以在遠端桌面平台中設定 VMware Integrated Printing 功能的列印喜好設定。透過 VMware Integrated Printing 功能，您可以從遠端桌面平台使用本機或網路印表機，而不需在 Windows 遠端桌面平台中安裝其他印表機驅動程式。對於每部透過此功能而可使用的印表機，您可以設定資料壓縮、列印品質、雙面列印和顏色等設定的喜好設定。

在單一使用者虛擬機器桌面平台上，每個虛擬印表機依預設會顯示為 `<printer_name>(vdi)`。在已發佈的桌面平台或已發佈的應用程式中，每個虛擬印表機依預設會顯示為 `<printer_name>(v<session_ID>)`。

從 Horizon Agent 7.12 開始，您可以使用群組原則來修改重新導向的用戶端印表機的印表機命名慣例。如需資訊，請參閱適用於您 Horizon Agent 版本的《在 Horizon 中設定遠端桌面平台功能》文件。

必要條件

若要使用 VMware Integrated Printing，Horizon 管理員必須在遠端桌面平台中安裝 VMware Integrated Printing 功能。此工作涉及在 Horizon Agent 安裝程式中啟用 **VMware Integrated Printing** 選項。如需安裝 Horizon Agent 的相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》或《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。如需設定 VMware Integrated Printing 功能的相關資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

若要確定是否已在遠端桌面平台中安裝 VMware Integrated Printing 功能，請確認遠端桌面平台檔案系統中是否有 `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` 和 `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` 檔案存在。

此功能需要 Horizon Agent 7.7 或更新版本。

程序

- 1 在 Windows 遠端桌面平台中，移至**控制台 > 硬體和音效 > 裝置和印表機**。
- 2 在**裝置和印表機**視窗中，以滑鼠右鍵按一下虛擬印表機，然後從快顯功能表中選取**印表機內容**。
- 3 在**一般索引標籤**上，按一下**喜好設定**。
- 4 在 [列印喜好設定] 對話方塊中，選取不同的標籤，並指定要使用的設定。
- 5 若要儲存變更，請按一下**確定**。

從遠端桌面平台列印至本機 USB 印表機

USB 印表機是一種連結到本機用戶端系統之 USB 連接埠的印表機。您可以從遠端桌面平台將列印工作傳送至連結到本機用戶端系統的 USB 印表機。

您可以使用 USB 重新導向功能或 VMware Integrated Printing 功能，從遠端桌面平台列印至 USB 印表機。重新導向的 USB 印表機和虛擬印表機可一起運作而不會發生衝突。

使用 USB 重新導向功能

若要使用 USB 重新導向功能將 USB 印表機連結至遠端桌面平台中的虛擬 USB 連接埠，則必須在遠端桌面平台和用戶端系統上安裝所需的印表機驅動程式。

如果您使用 USB 重新導向功能來重新導向 USB 印表機，USB 印表機依邏輯將不再連結至本機用戶端系統上的實體 USB 連接埠，且它不會出現在本機用戶端系統上的本機印表機清單中。您可以從遠端桌面平台列印至 USB 印表機，但已無法再從本機用戶端系統列印至 USB 印表機。

在遠端桌面平台中，重新導向的 USB 印表機會顯示為 `<printer_name>`。

如需詳細資訊，請參閱[使用 USB 裝置](#)。

使用 VMware Integrated Printing 功能

當您使用 VMware Integrated Printing 功能將列印工作傳送至 USB 印表機時，您可以從遠端桌面平台和本機用戶端系統列印至 USB 印表機，且無須在遠端桌面平台中安裝印表機驅動程式。

若要使用 VMware Integrated Printing 功能，您必須在安裝 Horizon Agent 時啟用該功能。如需安裝資訊，請參閱《在 Horizon 中設定虛擬桌面平台》或《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

如需詳細資訊，請參閱[設定 VMware Integrated Printing 功能的列印喜好設定](#)。

使用 URL 內容重新導向功能

Horizon 管理員可將您在遠端桌面平台或已發佈的應用程式內點選的 URL 連結，設定為在本機用戶端系統的預設瀏覽器中開啟。URL 連結可以指向網頁、電話號碼、電子郵件地址或其他類型的連結。這項功能稱為 URL 內容重新導向。

Horizon 管理員也可以將您在本機用戶端系統上的瀏覽器或發佈的應用程式內點選的 URL 連結，設定為會在遠端桌面平台或已發佈的應用程式中開啟。如果 Horizon Client 尚未開啟，請按一下 URL 連結，它便會啟動並提示您登入。

Horizon 管理員可以基於安全性目的而設定 URL 內容重新導向功能。例如，若您在公司，且按一下會指向公司網路外部 URL 的連結，則該連結可能會在已發佈的應用程式中以更安全的方式開啟。管理員可以設定要由哪個已發佈的應用程式開啟連結。

透過 Chrome 使用 URL 內容重新導向

第一次從用戶端上的 Chrome 瀏覽器重新導向 URL 時，系統會提示您在 Horizon Client 中開啟 URL。如果您選取記住我對 **URL: VMware Horizon Client 通訊協定連結** 的選擇核取方塊 (建議)，然後按一下 **開啟 VMware Horizon Client 通訊協定**，則不會再出現此提示。

改善遠端桌面平台中的滑鼠效能

當您在遠端桌面平台中使用 3D 應用程式時，如果您使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定，則啟用相對滑鼠功能將能改善滑鼠的效能。

在大多數情況下，如果使用不需要 3D 呈現的應用程式，Horizon Client 將使用絕對座標傳輸滑鼠指標移動的相關資訊。如果使用絕對座標，用戶端會在本機呈現滑鼠的移動，而此舉會改善效能 (特別是位於企業網路之外的時候)。

執行的工作如果需要使用圖形密集的應用程式 (例如 AutoCAD)，或是玩 3D 視訊遊戲，您可以啟用相對滑鼠功能 (其使用相對座標而非絕對座標) 以改善滑鼠效能。

在啟用相對滑鼠功能時，如果您在 WAN 上而位於企業網路之外，效能可能會不好。

必要條件

Horizon 管理員必須為桌面平台集區開啟 3D 轉譯。如需集區設定和可用於 3D 轉譯的選項相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》或《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

程序

- 1 啟動 Horizon Client 並登入伺服器。
- 2 以滑鼠右鍵按一下遠端桌面平台，然後選取 **VMware Blast** 或 **PCoIP**。
- 3 連線至遠端桌面平台。
- 4 從 Horizon Client 功能表列中選取 **選項 > 啟用相對滑鼠**。

此為切換選項。若要停用相對滑鼠功能，請再次選取 **選項 > 啟用相對滑鼠**。

備註 如果在視窗模式，而非全螢幕模式中使用 Horizon Client，並啟用了相對滑鼠功能，則可能無法將滑鼠指標移到 Horizon Client 功能表選項或將指標移出 Horizon Client 視窗。若要解決這種情況，請按下 Ctrl+Alt。

使用掃描器

透過掃描器重新導向功能，您可以使用連線至本機用戶端系統的掃描器，將資訊掃描到遠端桌面平台和已發佈的應用程式中。此功能所需使用的頻寬較 USB 重新導向大幅減少，因此可重新導向掃描資料。

掃描器重新導向支援與 TWAIN 和 WIA (Windows Image Acquisition) 格式相容的標準掃描裝置。您必須將掃描器裝置驅動程式安裝在本機用戶端系統上。您不需要在遠端桌面平台上安裝掃描器裝置驅動程式。

Horizon 管理員已設定掃描器重新導向功能時，如果您使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定，則可以在遠端桌面平台或已發佈的應用程式中使用連線至本機用戶端系統的掃描器。


重要 請勿從 Horizon Client 中的**連線 USB 裝置**功能表來連線至掃描器。可能會導致無法使用。

將掃描資料重新導向至遠端桌面平台或已發佈的應用程式時，您無法在本機用戶端電腦上存取掃描器。相反地，在本機用戶端電腦上使用掃描器時，您無法在遠端桌面平台或已發佈的應用程式上存取掃描器。

Horizon 管理員可設定群組原則設定，以控制 [VMware Horizon 掃描器重新導向喜好設定] 對話方塊中可用的選項。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件。

備註 如果 Horizon 管理員將掃描器重新導向設定為使用特定掃描器，而該掃描器無法使用，則掃描器重新導向將無法運作。

掃描器重新導向功能的使用提示

- 若要變更掃描器重新導向設定，請按一下遠端桌面平台的系統匣或通知區域中出現的掃描器圖示 ()。在已發佈的應用程式中，系統匣圖示將重新導向至本機用戶端電腦。

備註 您不需要使用在按一下掃描器圖示時顯示的功能表。無需進一步進行組態設定，掃描器重新導向即可運作。如果功能表未列出任何掃描器，則表示連接到本機用戶端系統的掃描器不相容。如果掃描器圖示未顯示，則表示掃描器重新導向功能已停用或未安裝在遠端桌面平台上。掃描器圖示也不會在不支援此功能的本機用戶端系統上顯示。

- 如果即使掃描應用程式未顯示 [掃描] 對話方塊，您仍想要顯示 [TWAIN 掃描內容] 對話方塊，請在掃描器圖示功能表中按一下**喜好設定**選項，然後選取**強制執行 TWAIN 掃描內容對話方塊**核取方塊。
- 若要顯示實際的掃描器名稱而非 VMware 虛擬 *nnn* 掃描器，請按一下掃描器圖示功能表中的**喜好設定**選項，然後選取**使用廠商定義的 TWAIN 掃描器名稱**核取方塊。
- 若要選取選項以控制影像壓縮或決定如何選取預設掃描器，請在掃描器圖示功能表中按一下**喜好設定**選項，然後選取**壓縮或預設索引標籤**。
- 如果您打算根據 VMware 建議使用即時音訊視訊功能來重新導向網路攝影機，請在掃描器圖示功能表中按一下**喜好設定**選項，然後選取**隱藏網路攝影機類型的影像裝置**核取方塊。
- 多數 TWAIN 掃描器依預設為顯示掃描器設定對話方塊，但仍有一些掃描器不會顯示。對於未顯示設定選項的掃描器，您可以使用掃描器圖示功能表中的**喜好設定**選項，然後選取**強制執行 TWAIN 掃描內容對話方塊**選項。

- 若要在遠端桌面平台上顯示 [TWAIN 掃描器內容] 對話方塊，請在掃描器圖示功能表中按一下**喜好設定**選項，然後選取**代理程式 (VMware 掃描內容對話方塊)**核取方塊。若要在本機用戶端系統上顯示 [TWAIN 掃描器內容] 對話方塊，請選取**用戶端 (原生掃描內容對話方塊, 如果支援的話)**核取方塊。

備註 在代理程式端 [TWAIN 掃描器內容] 對話方塊中，某些不常見的選項可能不會包含在內。若要使用這些不常見的選項，請選取**用戶端 (原生掃描內容對話方塊, 如果支援的話)**核取方塊。

- 可能無法掃描過大的影像或以過高解析度進行掃描。在此情況下，您可能會看到掃描進度列指示器凍結，或掃描器應用程式可能會意外結束。如果您最小化遠端桌面平台，則本機用戶端系統上可能會顯示一則錯誤訊息，通知您設定的解析度過高。若要解決此問題，請降低解析度或將影像裁切為較小大小，然後再次掃描。

重新導向序列埠

藉由序列埠重新導向功能，您可以重新導向本機連接的序列 (COM) 埠，例如內建 RS232 連接埠和 USB 轉序列介面卡。印表機、條碼讀取器及其他序列裝置之類的裝置皆可連接至這些連接埠，並且在遠端桌面平台中使用。

如果 Horizon 管理員已設定序列埠重新導向功能，而且您使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定，則不需要進行其他組態，序列埠重新導向即可在遠端桌面平台中運作。例如，本機用戶端系統上的 COM1 會在遠端桌面平台上重新導向為 COM1。COM2 會重新導向為 COM2。已在使用中的 COM 連接埠會進行對應以避免衝突。例如，如果遠端桌面已有 COM1 和 COM2 存在，則依預設會將用戶端系統上的 COM1 對應至 COM3。

您必須在本機用戶端系統上安裝任何必要的裝置驅動程式，但無須在遠端桌面平台上安裝這些裝置驅動程式。例如，如果您使用的 USB 轉序列介面卡需要特定的裝置驅動程式，才能在本機用戶端系統上運作，則您必須安裝這些驅動程式，不過只有用戶端系統才需要安裝。

重要 如果您使用的裝置是插在 USB 轉序列介面卡上，請勿從 Horizon Client 中的**連線 USB 裝置**功能表連接該裝置。如果這麼做，則會透過 USB 重新導向路由該裝置，並避開序列埠重新導向功能。

序列埠重新導向功能的使用提示

- 按一下遠端桌面平台的系統匣或通知區域中出現的序列埠圖示 (🔌) 來連線、中斷連線或自訂對應的 COM 連接埠。

您按一下序列埠圖示時，**VMware Horizon 的序列 COM 重新導向**快顯功能表將出現。如果管理員已鎖定組態，快顯功能表中的項目會變暗。僅在 Horizon 管理員已設定序列埠重新導向功能且符合所有需求時，才會顯示此圖示。如需詳細資訊，請參閱[序列埠重新導向的系統需求](#)。

- 在快顯功能表中，連接埠項目會列示為 **連接埠 對應於 連接埠**，例如，**COM1 對應於 COM3**。第一個連接埠 (亦即此範例中的 COM1) 是本機用戶端系統上的實體連接埠或 USB 轉序列介面卡。第二個連接埠 (亦即此範例中的 COM3) 是遠端桌面平台中使用的連接埠。
- 若要選取**連接埠屬性**命令，請以滑鼠右鍵按一下 COM 連接埠。

在 [COM 屬性] 對話方塊中，您可以設定要在遠端桌面工作階段啟動時自動連線的連接埠，您也可以忽略部分數據機及其他裝置所需的 DSR (data-set-ready 訊號)。

您也可以變更遠端桌面平台所使用的連接埠號碼。例如，如果用戶端系統的 COM1 連接埠對應於遠端桌面平台的 COM3，但是您使用的應用程式需要 COM1，您可以將連接埠號碼變更為 COM1。如果遠端桌面平台中已有 COM1 存在，您可能會看見 **COM1 (重疊)**。您仍然可以使用這個重疊的連接埠。遠端桌面平台可以透過該連接埠接收來自伺服器 and 用戶端系統的序列資料。

- 請先連線至對應的 COM 連接埠，再嘗試啟動需要存取此連接埠的應用程式。例如，以滑鼠右鍵按一下 COM 連接埠，並選取**連線**來使用遠端桌面平台中的連接埠。當您啟動應用程式時，應用程式會開啟序列埠。

在遠端桌面平台開啟並使用重新導向的 COM 連接埠時，您無法存取本機電腦的連接埠。另一方面，在本機電腦使用 COM 連接埠時，您無法存取遠端桌面平台的連接埠。

- 在遠端桌面平台中，您可以使用 Windows 裝置管理員的**連接埠設定**索引標籤來設定特定 COM 連接埠的傳輸速率。請在用戶端系統的 Windows 裝置管理員中使用相同的設定。僅在應用程式未指定連接埠設定的情況下，才會使用此索引標籤中的設定。
- 您中斷 COM 連接埠的連線前，必須先在應用程式中關閉連接埠或關閉應用程式。您接著即可選取**中斷連線**命令來中斷連線，並且使實體 COM 連接埠可以在用戶端電腦上開放使用。
- 若您設定要自動連線的序列埠，並啟動開啟該序列埠的應用程式，然後中斷連線並重新連線至遠端桌面工作階段，自動連線功能將無法運作。您也無法使用序列埠的系統匣圖示功能表選項進行連線。在大多數情況下，應用程式無法再使用該序列埠。您必須停止應用程式、中斷與遠端桌面工作階段的連線，然後再重新連線以解決問題。

鍵盤快速鍵

您可以將鍵盤快速鍵用於功能表命令和常用動作。

常用鍵盤快速鍵

這些鍵盤快速鍵在 Horizon Client 中的運作方式與它們在所有應用程式中的運作方式相同。

表 5-1. 常用鍵盤快速鍵

動作	按鍵或按鍵組合
按一下對話方塊中反白顯示的按鈕	按 Enter。
開啟快顯功能表	按 Shift+F10。
按一下對話方塊中的 取消 按鈕	按 ESC。
在伺服器選取視窗或桌面平台和應用程式選取器視窗中的項目之間導覽	使用方向鍵朝箭頭方向移動。若要移至右側，請按 Tab。若要移至左側，請按 Shift+Tab。
從伺服器選取視窗或桌面平台和應用程式選取器視窗中刪除項目	按 Delete。
在 Windows 8.x 中，在 開始 視窗和遠端桌面平台視窗之間導覽	按 Windows 按鍵。

伺服器選擇視窗按鍵組合

您可以在 Horizon Client 的伺服器選擇視窗中使用這些按鍵組合。

表 5-2. 伺服器選擇按鍵組合

功能表命令或動作	按鍵組合
在瀏覽器視窗中開啟線上說明	Alt+O+H、Ctrl+H
新增伺服器命令	Alt+N
開啟支援資訊視窗	Alt+O+S
開啟關於 Horizon Client 視窗	Alt+O+V
設定 SSL 命令	Alt+O+O
啟動項目後隱藏選取器命令	Alt+O+I

桌面平台和應用程式選取器的鍵盤快速鍵

當您在 Horizon Client 中選取遠端桌面平台和已發佈的應用程式時，您可以使用這些鍵盤快速鍵。

表 5-3. 桌面平台和應用程式選取器的鍵盤快速鍵

功能表命令或動作	按鍵組合
在瀏覽器視窗中開啟線上說明	Alt+O+H、Ctrl+H
開啟選項功能表	Alt+O
開啟支援資訊視窗	Alt+O+S
開啟關於 Horizon Client 視窗	Alt+O+V
從遠端桌面平台登出	Shift+F10+O
中斷連線並從伺服器登出	Alt+D
在顯示我的最愛和顯示全部間切換	Alt+F
顯示我的最愛時，在輸入已發佈應用程式或遠端桌面平台名稱的前幾個字元後，前往下一個與搜尋相符的項目	F4
顯示我的最愛時，前往上一個與搜尋相符的項目	Shift+F4
標記為我的最愛或移除我的最愛指定	Shift+F10+F
開啟設定功能表	Alt+S 或 Shift+F10+S
啟動選取的項目	Enter 或 Shift+F10+L
將遠端桌面平台或已發佈應用程式的捷徑釘選到 [開始] 功能表 (適用於 Windows 7 及更早版本)，或是用戶端系統上的 [開始] 視窗 (適用於 Windows 8.x 及更新版本)	Shift+F10+A
開啟選取的遠端桌面平台的顯示設定快顯功能表	Shift+F10+D
使用 PCoIP 顯示通訊協定連線到所選遠端桌面平台	Shift+F10+P
使用 RDP 顯示通訊協定連線到所選遠端桌面平台	Shift+F10+M
為選取的項目建立遠端桌面平台捷徑	Shift+F10+C
將選取的項目新增至 [開始] 功能表或 [開始] 視窗	Shift+F10+A
重設選取的遠端桌面平台 (如果管理員允許您重設)	Shift+F10+R
重新整理遠端桌面平台和已發佈的應用程式清單	F5

桌面平台視窗快速鍵

若要使用這些快速鍵，在按這些按鍵之前，您必須按 **Ctrl+Alt** 或在 Horizon Client 功能表列上按一下，而非在遠端桌面平台內按一下。僅在您使用 VMware Blast 顯示通訊協定或 PCoIP 顯示通訊協定時，這些快速鍵才會正常運作。

表 5-4. 遠端桌面平台視窗快速鍵

功能表命令或動作	按鍵組合
釋放滑鼠指標，使其不再處於遠端桌面平台內	Ctrl+Alt
開啟選項功能表	Alt+O
開啟支援資訊視窗	Alt+O+M
開啟關於 Horizon Client 視窗	Alt+O+V
開啟共用資料夾設定對話方塊	Alt+O+F
切換啟用顯示調整值	Alt+O+N
切換至其他桌面平台命令	Alt+O+S
自動連線至此桌面平台命令	Alt+O+A
啟用相對滑鼠命令	Alt+O+E
傳送 Ctrl+Alt+Del 命令	Alt+O+C
中斷連線命令	Alt+O+D
中斷連線並登出命令	Alt+O+L
連線 USB 裝置命令	Alt+U

輸入焦點的鍵盤快速鍵

您可以使用用於擷取輸入焦點的快速鍵組合和用於釋放輸入焦點的快速鍵組合群組原則設定來設定輸入焦點的鍵盤快速鍵。您可以使用在虛擬桌面平台視窗中的自動輸入的焦點群組原則設定，以在使用者將遠端桌面平台帶到前端時，自動將輸入傳送至遠端桌面平台。對於無法使用點按滑鼠來擷取和釋放遠端桌面平台的使用者，這些功能會很有用。如需詳細資訊，請參閱[用戶端 GPO 的一般設定](#)

鍵盤輸入方式語言同步

當您連線至遠端桌面平台時，用戶端系統上的鍵盤輸入方式語言會在遠端桌面平台中同步化。

此功能在用戶端系統上支援下列鍵盤輸入方式語言。

- 日文
- 英文
- 中文
- 韓文
- 法文
- 德文

- 西班牙文

如果不支援鍵盤輸入方式語言，則不會發生同步。

鍵盤輸入方式語言同步化由代理程式端**鍵盤地區設定同步化**群組原則設定所控制。如需詳細資訊，請參閱《在 Horizon 中設定遠端桌面平台功能》文件中的「VMware Blast 群組原則設定」。

設定鎖定鍵同步

您可以設定 Horizon Client，以將 Num Lock、Scroll Lock 和 Caps Lock 鍵的切換狀態從用戶端系統同步至遠端桌面平台，方法是啟用 Horizon Client 中的設定。此設定依預設為停用。

您也可以使用 Horizon Client **自動同步數字鍵台、捲軸和 Caps Lock 鍵**群組原則設定，以設定鎖定鍵同步。此群組原則設定啟用或停用時，使用者無法變更 Horizon Client 使用者介面中的鎖定鍵同步設定。如需詳細資訊，請參閱**用戶端 GPO 的一般設定**。

如果**自動同步數字鍵台、捲軸和 Caps Lock 鍵**群組原則設定已停用或未設定，或未選取 Horizon Client 鎖定鍵同步設定 (預設設定)，則依預設會將鎖定鍵切換狀態從遠端桌面平台同步至用戶端系統。

程序

- 1 啟動 Horizon Client 並連線至伺服器。
- 2 開啟遠端桌面平台的 [設定] 對話方塊。
 - 在桌面平台和應用程式選取視窗的右上角，按一下**設定** (齒輪) 圖示，然後選取左窗格中的遠端桌面平台。
 - 在桌面平台和應用程式選取視窗中，以滑鼠右鍵按一下遠端桌面平台，然後選取**設定**。
- 3 若要啟用鎖定鍵同步功能，請選取**自動同步數字鍵台、捲軸和 Caps Lock 鍵**核取方塊，然後按一下**確定**。

疑難排解 Horizon Client

6

透過重新啟動或重設遠端桌面平台或已發佈的應用程式，或透過重新安裝 Horizon Client，即可解決 Horizon Client 的多數問題。

本章節討論下列主題：

- [重新啟動遠端桌面平台](#)
- [重設遠端桌面平台或已發佈的應用程式](#)
- [修復 Windows 版 Horizon Client](#)
- [解除安裝 Windows 版 Horizon Client](#)
- [鍵盤輸入的問題](#)
- [Horizon Client 無預警結束時需要採取的動作](#)
- [使用 Workspace ONE 模式連線至伺服器](#)

重新啟動遠端桌面平台

如果遠端桌面平台作業系統停止回應，您可能需要重新啟動遠端桌面平台。重新啟動遠端桌面平台類似於 Windows 作業系統重新啟動命令。遠端桌面平台作業系統通常會在重新啟動之前提示您儲存任何未儲存的資料。

只有在 Horizon 管理員已為遠端桌面平台啟用重新啟動功能時，您才可以重新啟動遠端桌面平台。

如需啟用桌面平台重新啟動功能的相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》或《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

程序

- ◆ 使用[重新啟動桌面平台](#)命令。

選項	動作
從遠端桌面平台內	從功能表列中選取 選項 > 重新啟動桌面平台 。
從桌面平台選取器視窗	在遠端桌面平台圖示上按一下滑鼠右鍵，然後選取 重新啟動桌面平台 。

Horizon Client 會提示您確認重新啟動動作。

結果

遠端桌面平台中的作業系統會重新啟動，且用戶端會中斷連線並登出遠端桌面平台。

後續步驟

請先等候適當的時間讓系統重新啟動，再試著重新連線至遠端桌面平台。

如果重新啟動遠端桌面平台並未解決問題，則可能需要重設遠端桌面平台。請參閱[重設遠端桌面平台或已發佈的應用程式](#)。

重設遠端桌面平台或已發佈的應用程式

如果桌面平台作業系統停止回應，且重新啟動遠端桌面平台無法解決問題，您可能必須重設遠端桌面平台。

重設遠端桌面平台等同於按下實體 PC 上的 [重設] 按鈕，以強迫 PC 重新啟動。遠端桌面平台上任何開啟的檔案都會在未儲存的情況下關閉。

重設已發佈的應用程式會結束所有開啟的應用程式。

只有在 Horizon 管理員已為遠端桌面平台啟用重設功能時，您才可以重設遠端桌面平台。

如需啟用桌面平台重設功能的相關資訊，請參閱《在 Horizon 中設定虛擬桌面平台》或《在 Horizon 中設定已發佈的桌面平台和應用程式》文件。

程序

- 1 若要重設遠端桌面平台，請使用**重設桌面平台**命令。

選項	動作
從遠端桌面平台內	從功能表列選取 選項 > 重設桌面平台 。
從桌面平台和應用程式選取器視窗	在遠端桌面平台圖示上按一下滑鼠右鍵，然後選取 重設桌面平台 。

- 2 若要重設已發佈的應用程式，請使用桌面平台和應用程式選取器視窗中的**重設**按鈕。
 - a 按一下功能表列中的**設定**按鈕 (齒輪圖示)。
 - b 選取左窗格中的**應用程式**，按一下右窗格中的**重設**按鈕，然後按一下**確定**。

結果

當您重設遠端桌面平台時，遠端桌面平台中的作業系統會重新啟動，且用戶端會中斷連線並從遠端桌面平台登出。當您重設已發佈的應用程式時，已發佈的應用程式會結束。

後續步驟

請先等候適當的時間讓系統重新啟動，再試著重新連線至遠端桌面平台或已發佈的應用程式。

修復 Windows 版 Horizon Client

有時，您可以藉由修復 Horizon Client 來解決 Horizon Client 的問題。

必要條件

- 確認您能以管理員身分登入用戶端系統。
- 確認您擁有 Horizon Client 安裝程式。如果您沒有安裝程式，則無法修復 Horizon Client。

程序

- ◆ 若要以互動方式修復 Horizon Client，請執行下列其中一個工作。

- 按兩下 Horizon Client 安裝程式，然後按一下**修復**。
- 從命令列執行 Horizon Client 安裝程式，然後輸入 `/repair` 命令。

例如，在命令提示字元中輸入下列命令：

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /repair
```

其中 `y.y.y` 是版本號碼，而 `xxxxxx` 是組建編號。

- ◆ 若要以無訊息方式修復 Horizon Client，請從命令列執行 Horizon Client 安裝程式，然後輸入 `/silent` 和 `/repair` 命令。

例如，在命令列中輸入下列命令：

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /repair
```

其中 `y.y.y` 是版本號碼，而 `xxxxxx` 是組建編號。

解除安裝 Windows 版 Horizon Client

如果修復 Horizon Client 仍無法解決問題，您可能需要先解除安裝 Horizon Client 再加以重新安裝。

若您有 Horizon Client 安裝程式，則此程序說明如何解除安裝 Horizon Client。

若您沒有 Horizon Client 安裝程式，則可以使用在 Windows 系統上解除安裝其他應用程式的相同方式來解除安裝 Horizon Client。例如，在 Windows 10 系統上，您可以使用 Windows 作業系統來解除安裝或變更程式功能 (**控制台 > 程式和功能 > 解除安裝或變更程式**)。

必要條件

確認您能以管理員身分登入用戶端系統。

程序

- ◆ 若要以互動方式解除安裝 Horizon Client，請執行下列其中一個工作。

- 按兩下 Horizon Client 安裝程式，然後按一下**移除**。
- 從命令列執行 Horizon Client 安裝程式，然後輸入 `/uninstall` 命令。

例如，在命令提示字元中輸入下列命令：

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /uninstall
```


其中 *y.y.y* 是版本號碼，而 *xxxxxx* 是組建編號。

- ◆ 若要以無訊息方式解除安裝 Horizon Client，請從命令列執行 Horizon Client 安裝程式，然後輸入 `/silent` 和 `/uninstall` 命令。

例如，在命令提示字元中輸入下列命令：

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /uninstall
```

其中 *y.y.y* 是版本號碼，而 *xxxxxx* 是組建編號。

後續步驟

重新安裝 Horizon Client。請參閱第 2 章 [安裝 Windows 版 Horizon Client](#)。

鍵盤輸入的問題

當您在遠端桌面平台或已發佈的應用程式中輸入時，按鍵輸入似乎都無法運作。

問題

當您連線至遠端桌面平台或已發佈的應用程式時，您在輸入時沒有顯示任何字元。其他症狀可能是單一按鍵持續自行重複運作。

原因

某些安全性軟體 (例如 Norton 360 Total Security) 包含可偵測按鍵輸入記錄軟體並封鎖按鍵輸入記錄的功能。此安全性功能的目的是在於保護系統免於間諜軟體的威脅，而這些軟體會竊取密碼和信用卡號碼。此安全性軟體可能會封鎖 Horizon Client，使其無法將按鍵輸入傳送至遠端桌面平台或已發佈的應用程式。

解決方案

- ◆ 因此請在用戶端系統上，關閉防毒軟體或安全性軟體的按鍵輸入記錄偵測功能。

Horizon Client 無預警結束時需要採取的動作

Horizon Client 未經關閉而自行結束。

問題

Horizon Client 無預警結束。根據伺服器組態，您可能會看見像是「未與 View 連線伺服器建立安全連線」之類的訊息。有時並不會顯示訊息。

原因

伺服器的連線中斷時便會發生此問題。

解決方案

- ◆ 重新啟動 Horizon Client。當伺服器再次執行時，您即可成功連線。如果持續發生連線問題，請連絡您的系統管理員或 VMware 支援。

使用 Workspace ONE 模式連線至伺服器

您不能直接透過 Horizon Client 連線到伺服器，否則您的遠端桌面平台和已發佈的應用程式權利不會顯示在 Horizon Client 中。

問題

- 直接透過 Horizon Client 連線至伺服器時，Horizon Client 會將您重新導向至 Workspace ONE 入口網站。
- 透過 URI 或捷徑開啟遠端桌面平台或已發佈的應用程式時，或透過檔案關聯開啟本機檔案時，要求會將您重新導向至 Workspace ONE 入口網站以進行驗證。
- 透過 Workspace ONE 開啟遠端桌面平台或已發佈的應用程式且 Horizon Client 啟動之後，您無法在 Horizon Client 中查看或開啟其他授權的遠端桌面平台或已發佈的應用程式。

原因

Horizon 管理員可以在連線伺服器執行個體上啟用 Workspace ONE 模式。在連線伺服器執行個體上啟用 Workspace ONE 模式時，此行為是正常的。

解決方案

使用 Workspace ONE 來連線至已啟用 Workspace ONE 的伺服器，並存取您的遠端桌面平台和已發佈的應用程式。