

部署及設定 VMware Unified Access Gateway

Unified Access Gateway 3.3.1



vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為：

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

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

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

Copyright © 2018, 2019 VMware, Inc. 版權所有。 [版權和商標資訊](#)。

內容

部署及設定 VMware Unified Access Gateway 5

1 準備部署 VMware Unified Access Gateway 6

- Unified Access Gateway 作為安全閘道 6
- 使用 Unified Access Gateway 而非虛擬私人網路 7
- Unified Access Gateway 系統和網路需求 7
- DMZ 型 Unified Access Gateway 應用裝置的防火牆規則 9
- Unified Access Gateway 負載平衡拓撲 15
- Unified Access Gateway 搭配多個網路介面卡的 DMZ 設計 17
- 不停機升級 20
- 在不含網路通訊協定設定檔 (NPP) 的情況下部署 Unified Access Gateway 21
- 加入或退出客戶經驗改進計劃 22

2 部署 Unified Access Gateway 應用裝置 23

- 使用 OVF 範本精靈部署 Unified Access Gateway 23
- 使用 OVF 範本精靈來部署 Unified Access Gateway 24
- 從管理組態頁面設定 Unified Access Gateway 29
- 設定 Unified Access Gateway 系統設定 30
- 變更網路設定 31
- 設定使用者帳戶設定 32
- 更新 SSL 伺服器簽署的憑證 35

3 使用 PowerShell 部署 Unified Access Gateway 37

- 使用 PowerShell 部署 Unified Access Gateway 的系統需求 37
- 使用 PowerShell 來部署 Unified Access Gateway 應用裝置 38

4 Unified Access Gateway 的部署使用案例 42

- 使用 Horizon 與 Horizon Cloud with On-Premises Infrastructure 進行部署 42
- 對 Horizon 基礎結構支援 IPv4 和 IPv6 雙重模式 47
- 進階 Edge Service 設定 47
- 設定 Horizon 設定 49
- Blast TCP 和 UDP 外部 URL 組態選項 52
- Horizon 的端點符合性檢查 53
- 部署為 Reverse Proxy 54
- 使用 VMware Identity Manager 設定 Reverse Proxy 56
- 單一登入存取內部部署舊版 Web 應用程式的部署 60
- 身分識別橋接部署案例 61
- 設定身分識別橋接設定 63

- Unified Access Gateway 的 VMware AirWatch 元件 76
 - 在 Unified Access Gateway 上部署 VMware Tunnel 76
 - 關於 TLS 連接埠共用 79
 - Unified Access Gateway 上的 Content Gateway 79
 - 其他部署使用案例 80

- 5 使用 TLS/SSL 憑證設定 Unified Access Gateway 82**
 - 設定 Unified Access Gateway 應用裝置的 TLS/SSL 憑證 82
 - 選取正確的憑證類型 82
 - 將憑證檔案轉換為單行 PEM 格式 83
 - 變更 TLS 或 SSL 通訊所用的安全性通訊協定和加密套件 85

- 6 設定 DMZ 中的驗證 87**
 - 在 Unified Access Gateway 應用裝置上設定憑證或智慧卡驗證 87
 - 在 Unified Access Gateway 上設定憑證驗證 88
 - 取得憑證授權機構憑證 89
 - 在 Unified Access Gateway 中設定 RSA SecurID 驗證 90
 - 設定 Unified Access Gateway 的 RADIUS 91
 - 設定 RADIUS 驗證 91
 - 在 Unified Access Gateway 中設定 RSA 調適性驗證 93
 - 在 Unified Access Gateway 中設定 RSA 調適性驗證 94
 - 產生 Unified Access Gateway SAML 中繼資料 95
 - 建立其他服務提供者使用的 SAML 驗證器 96
 - 將服務提供者 SAML 中繼資料複製到 Unified Access Gateway 96

- 7 疑難排解 Unified Access Gateway 部署 97**
 - 監視所部署服務的健全狀況 97
 - 疑難排解部署錯誤 98
 - 疑難排解錯誤：身分識別橋接 100
 - 疑難排解錯誤：Cert-to-Kerberos 102
 - 疑難排解端點符合性 103
 - 疑難排解管理員 UI 中的憑證驗證 104
 - 疑難排解防火牆和連線問題 104
 - 疑難排解根使用者登入問題 106
 - 關於 Grub2 密碼 107
 - 從 Unified Access Gateway 應用裝置收集記錄 108
 - 匯出 Unified Access Gateway 設定 110
 - 疑難排解錯誤：Content Gateway 110

部署及設定 VMware Unified Access Gateway

《部署及設定 *Unified Access Gateway*》提供設計 VMware Horizon[®]、VMware Identity Manager™ 和 VMware AirWatch[®] 部署的相關資訊，這些部署使用 VMware Unified Access Gateway™ 來提供對組織應用程式的安全外部存取。這些應用程式可以是 Windows 應用程式、軟體即服務 (SaaS) 應用程式和桌面平台。本指南也提供部署 Unified Access Gateway 虛擬應用裝置以及在部署後變更組態設定的相關指示。

主要對象

此資訊適用於想要部署和使用 Unified Access Gateway 應用裝置的任何人。本資訊是專為具有經驗且熟悉虛擬機器技術和資料中心作業的 Linux 和 Windows 系統管理員所撰寫。

準備部署 VMware Unified Access Gateway

1

針對想從公司防火牆外部存取遠端桌面平台和應用程式的使用者，Unified Access Gateway 可做為安全閘道使用。

備註 VMware Unified Access Gateway[®] 先前稱為 VMware Access Point。

本章節討論下列主題：

- [Unified Access Gateway](#) 作為安全閘道
- 使用 [Unified Access Gateway](#) 而非虛擬私人網路
- [Unified Access Gateway](#) 系統和網路需求
- DMZ 型 [Unified Access Gateway](#) 應用裝置的防火牆規則
- [Unified Access Gateway](#) 負載平衡拓撲
- [Unified Access Gateway](#) 搭配多個網路介面卡的 DMZ 設計
- 不停機升級
- 在不含網路通訊協定設定檔 (NPP) 的情況下部署 [Unified Access Gateway](#)
- 加入或退出客戶經驗改進計劃

Unified Access Gateway 作為安全閘道

Unified Access Gateway 為應用裝置，通常安裝在非軍事區 (DMZ) 中。Unified Access Gateway 可用來確保只有進入公司資料中心的流量是代表經過嚴格驗證的遠端使用者流量。

Unified Access Gateway 會將驗證要求導向至適當的伺服器，並捨棄所有未經驗證的要求。使用者只能存取其有權存取的資源。

Unified Access Gateway 還能確保經過驗證之使用者的流量只能導向該使用者真正有權使用的桌面平台和應用程式資源。這個層級的保護涉及具體檢測桌面平台通訊協定、協調可能迅速變動的原則和網路位址，以便精確地控制存取權限。

Unified Access Gateway 可作為您的公司信任網路內連線的 Proxy 主機。這種設計可為虛擬桌面平台、應用程式主機以及伺服器阻擋面向公眾的網際網路，因此提供了額外一層的安全保護。

Unified Access Gateway 專為 DMZ 所設計。以下是實作的強化設定。

- 最新 Linux 核心和軟體修補程式
- 適用於網際網路和內部網路流量的多重 NIC 支援
- 已停用 SSH
- 已停用 FTP、Telnet、Rlogin 或 Rsh 服務
- 已停用不需要的服務

使用 Unified Access Gateway 而非虛擬私人網路

Unified Access Gateway 與通用 VPN 解決方案很類似，因為它們都可確保僅在代表經過嚴格驗證的使用者時，才會將流量轉送至內部網路。

Unified Access Gateway 優於通用 VPN 的方面包括下列項目。

- **Access Control Manager。** Unified Access Gateway 會自動套用存取規則。Unified Access Gateway 會辨識使用者的權利和在內部連線所需的定址。VPN 也有相同的功效，因為大多數的 VPN 允許管理員分別針對每位使用者或使用者群組設定網路連線規則。剛開始，使用 VPN 可以順利運作，但需要投入大量的管理工作來維護必要規則。
- **使用者介面。** Unified Access Gateway 不會變更簡潔的 Horizon Client 使用者介面。利用 Unified Access Gateway，當 Horizon Client 啟動時，經驗證的使用者會在其 Horizon Connection Server 環境中，並對其桌面平台和應用程式擁有受控制的存取權。根據 VPN 的要求，您必須先設定 VPN 軟體並分別進行驗證，然後才能啟動 Horizon Client。
- **效能。** Unified Access Gateway 是專為將安全性和效能最大化而設計。有了 Unified Access Gateway，您不需要其他封裝就可以保護 PCoIP、HTML Access 及 WebSocket 通訊協定。VPN 會實作為 SSL VPN。此實作可滿足安全需求，而且在啟用傳輸層安全性 (Transport Layer Security, TLS) 的情況下，我們都會認為它們是安全的，不過使用 SSL/TLS 的基礎通訊協定只是以 TCP 為基礎。論及利用無連線 UDP 式傳輸的現代化視訊遠端通訊協定，當強制透過 TCP 型傳輸時，其效能優勢可能會大打折扣。這種說法不見得適用於所有 VPN 技術，因為能額外與 DTLS 或 IPsec (而非 SSL/TLS) 協同作業的技術也能與 Horizon Connection Server 桌面平台通訊協定搭配運作。

Unified Access Gateway 系統和網路需求

若要部署 Unified Access Gateway 應用裝置，請確定您的系統符合硬體和軟體需求。

支援的 VMware 產品版本

您必須對特定版本的 Unified Access Gateway 使用特定版本的 VMware 產品。請參閱產品版本說明以取得關於相容性的最新資訊，並參閱 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 上的 VMware 產品互通性對照表。

ESXi 伺服器的硬體需求

部署 Unified Access Gateway 應用裝置的 VMware vSphere 版本必須與 VMware 產品支援的版本以及您使用的版本相同。

備註 UAG 支援自 vSphere 5.5.x 起的所有 vSphere 版本。

如果您計劃要使用 vSphere Web client，請確認已安裝用戶端整合外掛程式。如需詳細資訊，請參閱 vSphere 說明文件。開始部署精靈之前，若未安裝此外掛程式，精靈會提示您安裝外掛程式。這需要您關閉瀏覽器並結束精靈。

備註 在 Unified Access Gateway 應用裝置上設定時鐘 (UTC)，讓應用裝置擁有正確的時間。例如，開啟 Unified Access Gateway 虛擬機器上的主控台視窗，然後使用箭頭按鈕選取正確的時區。另外，確認 ESXi 主機的時間是否與 NTP 伺服器同步，並確認在應用裝置虛擬機器上執行的 VMware Tools 會將虛擬機器的時間與 ESXi 主機的時間同步。

虛擬應用裝置需求

Unified Access Gateway 應用裝置的 OVF 套件會自動選取 Unified Access Gateway 需要的虛擬機器組態。雖然您可以變更這些設定，但 VMware 建議您不要將 CPU、記憶體或磁碟空間變更為比預設 OVF 設定還要小的值。

- CPU 最低需求為 2000 MHz
- 至少 4 GB 記憶體

確定您要用於應用裝置的資料存放區具備足夠的可用磁碟空間，並符合其他系統需求。

- 虛擬應用裝置下載大小為 1.4 GB
- 精簡佈建磁碟最低需求為 2.6 GB
- 完整佈建磁碟最低需求為 20 GB

需要下列資訊才能部署虛擬應用裝置。

- 靜態 IP 位址 (建議)
- DNS 伺服器的 IP 位址
- 根使用者的密碼
- 管理員使用者的密碼
- Unified Access Gateway 應用裝置所指向負載平衡器之伺服器執行個體的 URL

支援的瀏覽器版本

支援啟動管理員 UI 的瀏覽器為 Chrome、Firefox 和 Internet Explorer。請使用最新版本的瀏覽器。

使用 Windows Hyper-V Server 時的硬體需求

使用 Unified Access Gateway 進行 VMware AirWatch 每一應用程式通道部署時，您可以在 Microsoft Hyper-V 伺服器上安裝 Unified Access Gateway 應用裝置。

支援的 Microsoft 伺服器為 Windows Server 2012 R2 和 Windows Server 2016。

網路功能組態需求

您可以使用一個、兩個或三個網路介面，Unified Access Gateway 要求替每個網路介面設定不同的靜態 IP 位址。許多 DMZ 實作使用分開的網路來保護不同的流量類型。請根據 Unified Access Gateway 部署所在之 DMZ 的網路設計來對其設定。

- 一個網路介面適合用於 POC (概念證明) 或測試用途。使用一個 NIC 時，外部、內部和管理流量都在同一個子網路上。
- 使用兩個網路介面時，外部流量位於一個子網路上，內部和管理流量位於另一個子網路上。
- 使用三個網路介面是最安全的選項。使用第三個 NIC 時，外部、內部和管理流量都能擁有自己的子網路。

記錄保留需求

記錄檔依預設會設定成使用特定數量的空間，且該數量會小於彙總中的磁碟大小總計。

Unified Access Gateway 的記錄檔依預設會輪替。您必須使用 syslog 保存這些記錄項目。請參閱從 [Unified Access Gateway 應用裝置收集記錄](#)。

DMZ 型 Unified Access Gateway 應用裝置的防火牆規則

DMZ 型 Unified Access Gateway 應用裝置需要在前端和後端防火牆設定某些防火牆規則。在安裝期間，Unified Access Gateway 服務預設設為接聽特定網路連接埠。

DMZ 型 Unified Access Gateway 應用裝置部署通常包含兩個防火牆：

- 保護 DMZ 和內部網路需要面向外部網路的前端防火牆。您可以設定此防火牆允許外部網路流量到達 DMZ。
- 提供第二層安全性則需要位於 DMZ 與內部網路之間的后端防火牆。您可以設定此防火牆僅接受發自 DMZ 內服務的流量。

防火牆原則可嚴格控制來自 DMZ 服務的輸入通訊，進而大幅降低內部網路出現漏洞的風險。

下表列出 Unified Access Gateway 內不同服務的連接埠需求。

備註 所有 UDP 連接埠都需要允許轉送資料包和回覆資料包。

表格 1-1. Horizon 連線伺服器的連接埠需求

連接埠	通訊協定	來源	目標	說明
443	TCP	網際網路	Unified Access Gateway	針對 Web 流量，Horizon Client XML - API、Horizon Tunnel 和 Blast Extreme
443	UDP	網際網路	Unified Access Gateway	UDP 443 會在內部轉送至 Unified Access Gateway 上 UDP 通道伺服器服務的 UDP 9443。
8443	UDP	網際網路	Unified Access Gateway	Blast Extreme (選用)
8443	TCP	網際網路	Unified Access Gateway	Blast Extreme (選用)
4172	TCP 與 UDP	網際網路	Unified Access Gateway	PCoIP (選用)
443	TCP	Unified Access Gateway	Horizon Broker	Horizon Client XML-API、Blast extreme HTML Access、Horizon Air 主控台存取 (HACA)
22443	TCP 與 UDP	Unified Access Gateway	桌面平台和 RDS 主機	Blast Extreme
4172	TCP 與 UDP	Unified Access Gateway	桌面平台和 RDS 主機	PCoIP (選用)
32111	TCP	Unified Access Gateway	桌面平台和 RDS 主機	USB 重新導向的架構通道
9427	TCP	Unified Access Gateway	桌面平台和 RDS 主機	MMR 和 CDR

備註 若要允許外部用戶端裝置連線至 DMZ 內的 Unified Access Gateway 應用裝置，前端防火牆必須允許特定連接埠上的流量。依預設，外部用戶端裝置和外部 Web 用戶端 (HTML Access) 會透過 TCP 連接埠 443 連線至 DMZ 內的 Unified Access Gateway 應用裝置。如果您使用 Blast 通訊協定，則必須在防火牆上開啟連接埠 8443，但您也可以設定 Blast 使用連接埠 443。

表格 1-2. Web Reverse Proxy 的連接埠需求

連接埠	通訊協定	來源	目標	說明
443	TCP	網際網路	Unified Access Gateway	針對 Web 流量
任意	TCP	Unified Access Gateway	內部網路網站	任何已設定且由內部網路接聽中的自訂連接埠。例如 80、443 和 8080 等。
88	TCP	Unified Access Gateway	KDC 伺服器/AD 伺服器	如果設定了對 Kerberos 的 SAML/對 Kerberos 的憑證，則需要身分識別橋接以存取 AD。
88	UDP	Unified Access Gateway	KDC 伺服器/AD 伺服器	如果設定了對 Kerberos 的 SAML/對 Kerberos 的憑證，則需要身分識別橋接以存取 AD。

表格 1-3. 管理員 UI 的連接埠需求

連接埠	通訊協定	來源	目標	說明
9443	TCP	管理員 UI	Unified Access Gateway	管理介面

表格 1-4. Content Gateway 基本端點組態的連接埠需求

連接埠	通訊協定	來源	目標	說明
443* 或任何連接埠 > 1024	HTTPS	裝置 (從網際網路和 Wi-Fi)	Unified Access Gateway Content Gateway 端點	如果使用 443, 則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	HTTPS	VMware AirWatch 裝置服務	Unified Access Gateway Content Gateway 端點	
443* 或任何連接埠 > 1024	HTTPS	Workspace ONE UEM 主控台	Unified Access Gateway Content Gateway 端點	如果使用 443, 則 Content Gateway 會在連接埠 10443 上接聽。
存放庫正在接聽的任何連接埠。	HTTP 或 HTTPS	Unified Access Gateway Content Gateway 端點	Web 型內容存放庫, 例如 SharePoint/WebDAV/CMIS 等	任何已設定且由內部網路網站接聽中的自訂連接埠。
137–139 和 445	CIFS 或 SMB	Unified Access Gateway Content Gateway 端點	網路共用型存放庫 (Windows 檔案共用)	內部網路共用

表格 1-5. Content Gateway 轉送端點組態的連接埠需求

連接埠	通訊協定	來源	目標/目的地	說明
443* 或任何連接埠 > 1024	HTTP/HTTPS	Unified Access Gateway 轉送伺服器 (Content Gateway 轉送)	Unified Access Gateway Content Gateway 端點	如果使用 443, 則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	HTTPS	裝置 (從網際網路和 Wi-Fi)	Unified Access Gateway 轉送伺服器 (Content Gateway 轉送)	如果使用 443, 則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	TCP	AirWatch 裝置服務	Unified Access Gateway 轉送伺服器 (Content Gateway 轉送)	如果使用 443, 則 Content Gateway 會在連接埠 10443 上接聽。
443* 或任何連接埠 > 1024	HTTPS	Workspace ONE UEM 主控台		
存放庫正在接聽的任何連接埠。	HTTP 或 HTTPS	Unified Access Gateway Content Gateway 端點	Web 型內容存放庫, 例如 SharePoint/WebDAV/CMIS 等	任何已設定且由內部網路網站接聽中的自訂連接埠。

表格 1-5. Content Gateway 轉送端點組態的连接埠需求 (繼續)

連接埠	通訊協定	來源	目標/目的地	說明
443* 或任何連接埠 > 1024	HTTPS	Unified Access Gateway (Content Gateway 轉送)	Unified Access Gateway Content Gateway 端點	如果使用 443, 則 Content Gateway 會在連接埠 10443 上接聽。
137–139 和 445	CIFS 或 SMB	Unified Access Gateway Content Gateway 端點	網路共用型存放庫 (Windows 檔案共用)	內部網路共用

備註 由於 Content Gateway 服務在 Unified Access Gateway 中會以非根使用者的身分執行, Content Gateway 無法在系統連接埠上執行, 因此自訂連接埠應 > 1024。

表格 1-6. VMware Tunnel 的连接埠需求

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
2020*	HTTP S	裝置 (從網際網路和 Wi-Fi)	VMware Tunnel 代理伺服器	安裝完成後請執行下列命令: netstat -tlpn grep [Port]	
8443*	TCP	裝置 (從網際網路和 Wi-Fi)	VMware Tunnel 每一應用程式通道	安裝完成後請執行下列命令: netstat -tlpn grep [Port]	1

表格 1-7. VMware Tunnel 基本端點組態

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
SaaS : 443 : 2001 *	HTTP S	VMware Tunnel	AirWatch Cloud Messaging 伺服器	curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping 預期的回應為 HTTP 200 確定。	2
SaaS : 443 內部部署 : 80 或 443	HTTP 或 HTTP S	VMware Tunnel	Workspace ONE UEM REST API 端點 <ul style="list-style-type: none"> SaaS: https://asXXX.awdm.com 或 https://asXXX.airwatchportals.com 內部部署: 通常是您的 DS 或主控台伺服器 	curl -Ivv https://<API URL>/api/mdm/ping 預期的回應是 HTTP 401 未經授權。	5
80、443、任何 TCP	HTTP 、 HTTP S 或 TCP	VMware Tunnel	內部資源	確認 VMware Tunnel 可透過必要的連接埠存取內部資源。	4

表格 1-7. VMware Tunnel 基本端點組態 (繼續)

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
514 *	UDP	VMware Tunnel	Syslog 伺服器		
內部部署: 2020	HTTP S	Workspace ONE UEM 主控台	VMware Tunnel 代理伺服器	內部部署使用者可以使用 telnet 命令測試連線: telnet <Tunnel Proxy URL> <port>	6

表格 1-8. VMware Tunnel 階層式組態

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
SaaS : 443 內部部署: 2001 *	TLS v1.2	VMware Tunnel 前端	AirWatch Cloud Messaging 伺服器	對 https://<AWCM URL>:<port>/awcm/status 使用 wget, 並確定您收到 HTTP 200 回應以進行驗證。	2
8443	TLS v1.2	VMware Tunnel 前端	VMware Tunnel 後端	使用 Telnet 從 VMware Tunnel 前端連線至連接埠上的 VMware Tunnel 後端伺服器	3
SaaS : 443 內部部署: 2001	TLS v1.2	VMware Tunnel 後端	AirWatch Cloud Messaging 伺服器	對 https://<AWCM URL>:<port>/awcm/status 使用 wget, 並確定您收到 HTTP 200 回應以進行驗證。	2
80 或 443	TCP	VMware Tunnel 後端	內部網站/Web 應用程式		4
80、443、 任何 TCP	TCP	VMware Tunnel 後端	內部資源		4
80 或 443	HTTP S	VMware Tunnel 前端 和後端	Workspace ONE UEM REST API 端點 <ul style="list-style-type: none"> ■ SaaS: https://asXXX.awdm.com 或 https://asXXX.airwatchportals.com ■ 內部部署: 通常是您的 DS 或主控台伺服器 	curl -Ivv https://<API URL>/api/mdm/ping 預期的回應是 HTTP 401 未經授權。	5

表格 1-9. VMware Tunnel 轉送端點組態

連接埠	通訊協定	來源	目標/目的地	驗證	附註 (請參閱頁面底部的「附註」一節)
SaaS : 443 內部部署 : 2001	HTTP 或 HTTP S	VMware Tunnel 轉送	AirWatch Cloud Messaging 伺服器	curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping 預期的回應為 HTTP 200 確定。	2
80 或 443	HTTP 或 HTTP S	VMware Tunnel 端點和轉送	Workspace ONE UEM REST API 端點 <ul style="list-style-type: none"> ■ SaaS: https://asXXX.awdm.com 或 https://asXXX.airwatchportals.com ■ 內部部署: 通常是您的 DS 或主控台伺服器 	curl -Ivv https://<API URL>/api/mdm/ping 預期的回應是 HTTP 401 未經授權。 僅在初始部署期間, VMware Tunnel 端點才需要存取 REST API 端點。	5
2010 *	HTTP S	VMware Tunnel 轉送	VMware Tunnel 端點	使用 Telnet 從 VMware Tunnel 轉送連線至連接埠上的 VMware Tunnel 端點伺服器	3
80、443、任何 TCP	HTTP S 或 TCP	VMware Tunnel 端點	內部資源	確認 VMware Tunnel 可透過必要的連接埠存取內部資源。	4
514 *	UDP	VMware Tunnel	Syslog 伺服器		
內部部署 : 2020	HTTP S	Workspace ONE UEM	VMware Tunnel 代理伺服器	內部部署使用者可以使用 telnet 命令測試連線: telnet <Tunnel Proxy URL> <port>	6

備註 下列幾點對於 VMware Tunnel 需求有效。

* - 此連接埠可在必要時根據您的環境限制進行變更。

- 1 如果使用連接埠 443，則每一應用程式通道會在連接埠 8443 上接聽。

備註 在相同的應用裝置上啟用 VMware Tunnel 和 Content Gateway 服務，並啟用 TLS 連接埠共用時，每項服務的 DNS 名稱都必須是唯一的。未啟用 TLS 時，這兩項服務只能使用一個 DNS 名稱，因為連接埠將會區分傳入流量。(針對 Content Gateway，如果使用 443，則 Content Gateway 會在連接埠 10443 上接聽。)

- 2 供 VMware Tunnel 查詢 Workspace ONE UEM 主控台以進行符合性和追蹤用途。
 - 3 僅供 VMware Tunnel 轉送拓撲將裝置要求轉送至內部 VMware Tunnel 端點。
 - 4 供使用 VMware Tunnel 的應用程式存取內部資源。
 - 5 VMware Tunnel 必須與 API 通訊以進行初始化。確定 REST API 與 VMware Tunnel 伺服器之間有連線存在。導覽至 **群組和設定 > 所有設定 > 系統 > 進階 > 站台 URL**，以設定 REST API 伺服器 URL。此頁面不適用於 SaaS 客戶。SaaS 客戶的 REST API URL 通常是您的主控台或裝置服務伺服器 URL。
 - 6 若要從 Workspace ONE UEM 主控台對 VMware Tunnel Proxy 成功執行「測試連線」，則必須符合此需求。此需求為選用，可以省略而不會遺失裝置的功能。針對 SaaS 客戶，Workspace ONE UEM 主控台可能已因為連接埠 2020 上的輸入網際網路需求，會在連接埠 2020 上具有 VMware Tunnel Proxy 的輸入連線。
-

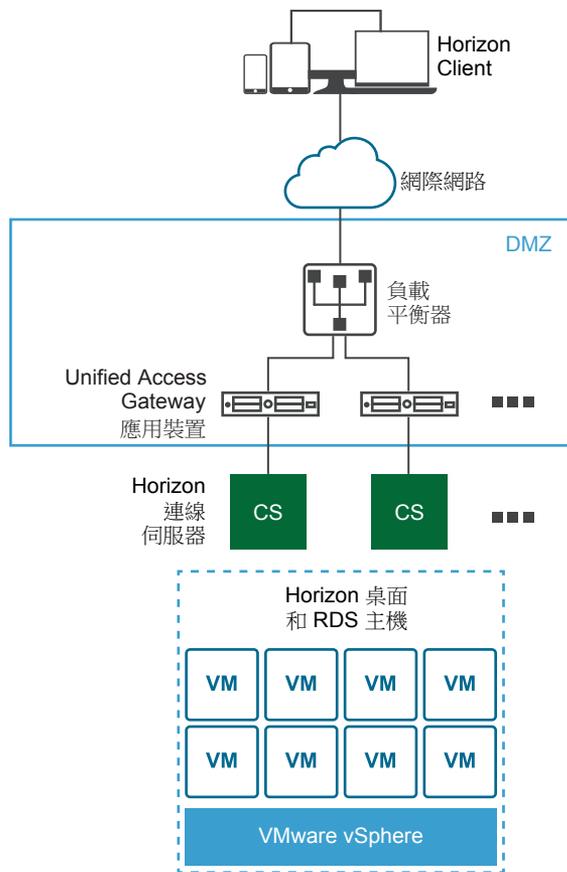
Unified Access Gateway 負載平衡拓撲

DMZ 中的 Unified Access Gateway 應用裝置可以設定為指向某個伺服器或位於一組伺服器前方的負載平衡器。Unified Access Gateway 應用裝置可與設定為使用 HTTPS 的標準第三方負載平衡解決方案搭配運作。

若 Unified Access Gateway 應用裝置指向伺服器前方的負載平衡器，在選擇伺服器執行個體時就不會固定不變。例如，負載平衡器可能會根據可用性以及負載平衡器所知道的每個伺服器執行個體上目前的工作階段數目來做出選擇。公司防火牆內部的伺服器執行個體通常具備負載平衡器，以便支援內部存取。在使用 Unified Access Gateway 時，您可以將 Unified Access Gateway 應用裝置指向這個通常已在使用中的相同負載平衡器。

您也可以讓一或多個 Unified Access Gateway 應用裝置指向某一個伺服器執行個體。在這兩種方法中，都請在 DMZ 中的兩部 (含) 以上 Unified Access Gateway 應用裝置前方使用負載平衡器。

圖 1-1 負載平衡器後方多個 Unified Access Gateway 應用裝置



Horizon 通訊協定

當 Horizon Client 使用者連接至 Horizon 環境時，系統會使用數個不同的通訊協定。第一個連線一律會是透過 HTTPS 的主要 XML-API 通訊協定。在成功驗證之後，系統也會建立一或多個次要通訊協定。

■ 主要 Horizon 通訊協定

使用者在 Horizon Client 輸入主機名稱，而這會啟動主要 Horizon 通訊協定。這是用於驗證授權和工作階段管理的控制通訊協定。此通訊協定透過 HTTPS 使用 XML 結構化訊息。此通訊協定有時稱為 Horizon XML-API 控制通訊協定。在上圖「負載平衡器後方多個 Unified Access Gateway 應用裝置」所示的負載平衡環境中，負載平衡器會將此連線路由傳送至其中一個 Unified Access Gateway 應用裝置。負載平衡器一般會先根據可用性選取應用裝置，然後根據目前工作階段的最小數量，從可用應用裝置路由傳送流量。此組態會在可用的一組 Unified Access Gateway 應用裝置之間，從不同的用戶端平均散佈流量。

■ 次要 Horizon 通訊協定

在 Horizon Client 對其中一個 Unified Access Gateway 應用裝置建立安全通訊之後，使用者隨即進行驗證。如果此驗證嘗試成功，則會從 Horizon Client 建立一或多個次要連線。這些次要連線可以包括下列項目：

- 用於封裝 TCP 通訊協定的 HTTPS 通道，例如 RDP、MMR/CDR 和用戶端架構通道。(TCP 443)

- Blast Extreme 顯示通訊協定 (TCP 443、TCP 8443、UDP 443 和 UDP 8443)
- PCoIP 顯示通訊協定 (TCP 4172 和 UDP 4172)

這些次要 Horizon 通訊協定必須路由傳送至主要 Horizon 通訊協定路由傳送到的相同

Unified Access Gateway 應用裝置。然後 Unified Access Gateway 即可根據經過驗證的使用者工作階段來授權次要通訊協定。Unified Access Gateway 的一項重要安全性功能是，僅在流量代表經過驗證的使用者時，Unified Access Gateway 才會將流量轉送至公司資料中心。如果錯誤地將次要通訊協定路由傳送至不同的 Unified Access Gateway 應用裝置，而非主要通訊協定應用裝置，則使用者不會獲得授權，且會放置在 DMZ 中。連線失敗。如果未正確設定負載平衡器，則錯誤地路由傳送次要通訊協定屬於常見問題。

內容閘道和通道代理伺服器的負載平衡考量事項

當您使用負載平衡器搭配內容閘道和通道代理伺服器時，請留意下列考量事項：

- 設定負載平衡器來「傳送原始 HTTP 標頭」以避免裝置發生連線問題。內容閘道和通道代理伺服器會使用要求 HTTP 標頭中的資訊來驗證裝置。
- 每一應用程式通道元件會要求每個用戶端在連線建立後進行驗證。連線之後，系統將會為用戶端建立一個工作階段並儲存在記憶體中。如此一來，每一項用戶端資料都會使用相同的工作階段，讓資料可以使用相同的金鑰進行加密和解密。設計負載平衡解決方案時，必須在啟用 IP/工作階段型持續性的情況下設定負載平衡器。替代的解決方案可能是在用戶端上使用 DNS 循環配置資源，這表示用戶端針對每個連線可以選取不同的伺服器。

Unified Access Gateway 搭配多個網路介面卡的 DMZ 設計

Unified Access Gateway 的其中一個組態設定為要使用的虛擬網路介面卡 (NIC) 數量。部署 Unified Access Gateway 時，您會為網路選取部署組態。

您可以指定一、二或三個 NIC 設定，其指定方式為 onenic、twonic 或 threenic。

減少每個虛擬 LAN 上已開啟連接埠的數量，並區隔不同類型的網路流量以大幅改善安全性。主要優勢在於區隔與隔離不同類型的網路流量以作為深度防禦 DMZ 安全性設計策略的一部分。這可透過在 DMZ 內實作不同的實體交換器並在 DMZ 內具有多個虛擬 LAN，或隸屬於完整 VMware NSX 所管理 DMZ 的一部分來實現。

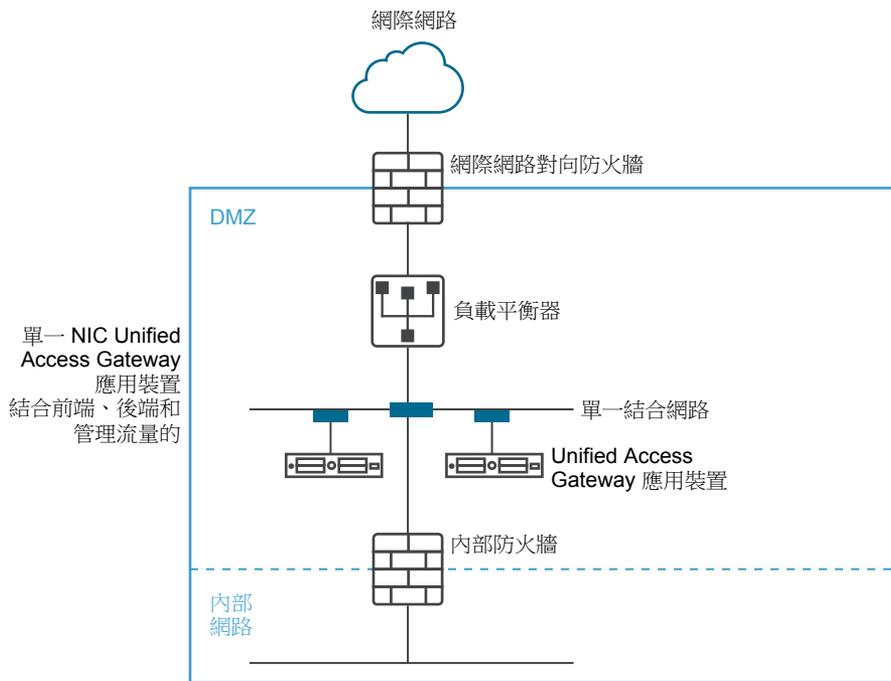
一般的單一 NIC DMZ 部署

最簡單的 Unified Access Gateway 部署是使用單一 NIC，其中的所有網路流量會結合在單一網路上。來自網際網路對向防火牆的流量會導向至其中一個可用的 Unified Access Gateway 應用裝置。然後

Unified Access Gateway 會經由內部防火牆將授權流量轉送至內部網路上的資源。

Unified Access Gateway 會捨棄未經授權的流量。

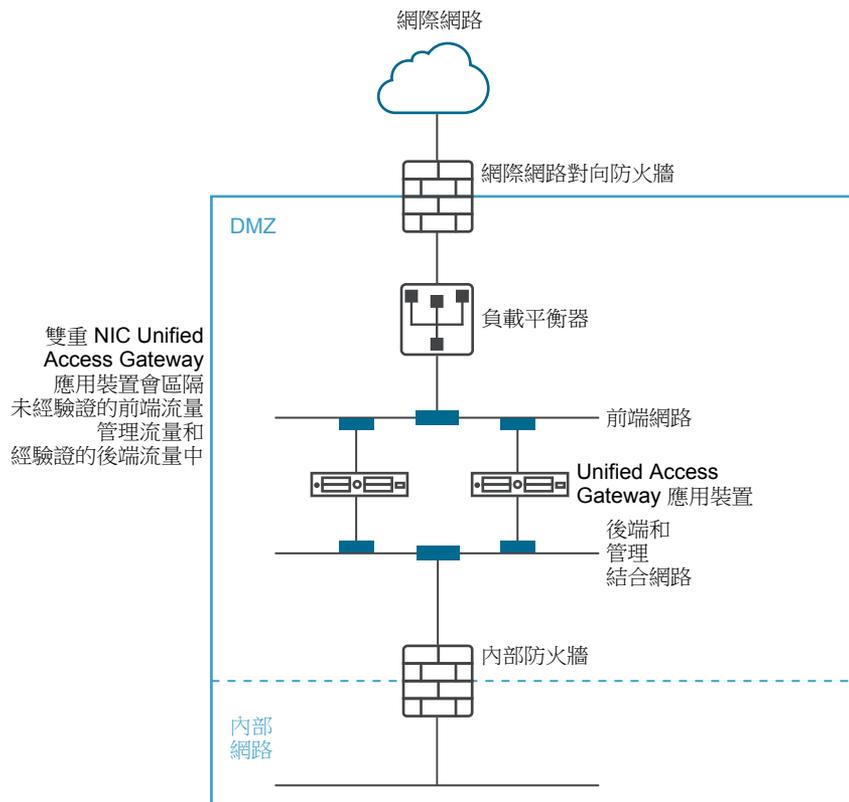
圖 1-2 Unified Access Gateway 單一 NIC 選項



從後端和管理流量區隔未經驗證的使用者流量

對於單一 NIC 部署的改善即為指定兩個 NIC。第一個仍會用於網際網路對向未經驗證的存取，但後端驗證流量和管理流量則會區隔至不同的網路上。

圖 1-3 Unified Access Gateway 兩個 NIC 選項



在兩個 NIC 部署中，Unified Access Gateway 必須授權流量透過內部防火牆進入內部網路。未經授權的流量不會在此後端網路上。管理流量 (例如 Unified Access Gateway 的 REST API) 只會在此第二個網路上

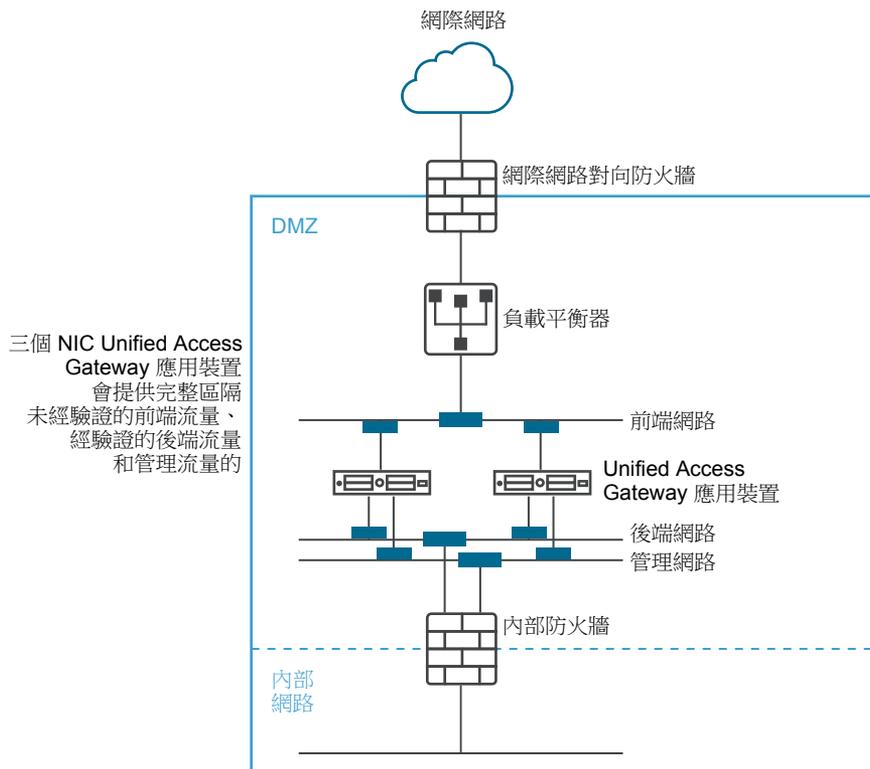
如果在未經驗證的前端網路上的裝置 (例如負載平衡器) 遭到破解，則在這兩個 NIC 部署中便無法重新設定裝置略過 Unified Access Gateway。它會結合第 4 層防火牆規則與第 7 層 Unified Access Gateway 安全性。相同地，如果網際網路對向防火牆設定錯誤而允許通過 TCP 連接埠 9443，則這仍不會將 Unified Access Gateway 管理 REST API 向網際網路使用者公開。深度防禦原則會使用多層級防護，例如知道單一組態錯誤或系統攻擊不一定會產生整體的弱點

在兩個 NIC 部署中，您可以在 DMZ 內的後端網路上放置額外的基礎結構系統 (如 DNS 伺服器、RSA SecurID 驗證管理員伺服器)，以便讓這些伺服器無法顯示在網際網路對向網路上。在 DMZ 內放置基礎結構系統可防禦來自遭破解前端系統之網際網路對向 LAN 的第 2 層攻擊，並可有效減少整體攻擊面。

多數 Unified Access Gateway 網路流量為 Blast 和 PCoIP 的顯示通訊協定。利用單一 NIC，往返於網際網路的顯示通訊協定流量會與往返於後端系統的流量結合。使用兩個以上的 NIC 時，流量會遍及前端和後端 NIC 與網路。這可減少單一 NIC 的潛在瓶頸，並產生效能優勢。

Unified Access Gateway 也支援進一步的區隔，即允許將管理流量區隔至特定的管理 LAN。如此一來，通往連接埠 9443 的 HTTPS 管理流量僅能夠從管理 LAN 進行傳輸。

圖 1-4 Unified Access Gateway 三個 NIC 選項



不停機升級

不停機升級可讓您在使用者不停機的情況下升級 Unified Access Gateway。

當靜止模式值設定為 [是]，當負載平衡器檢查應用裝置的健全狀況時，Unified Access Gateway 應用裝置會顯示為無法使用。進入負載平衡器的要求會傳送至負載平衡器後方的下一個 Unified Access Gateway 應用裝置。

先決條件

- 在負載平衡器後方設定兩個或多個 Unified Access Gateway 應用裝置。
- [健全狀況檢查 URL] 設定已設定了 URL，其負載平衡器會進行連線以便檢查 Unified Access Gateway 應用裝置的健全狀況。
- 在負載平衡器中檢查應用裝置的健全狀況。輸入 REST API 命令 GET <https://mycoUnifiedAccessGateway.com:443/favicon.ico>。

如果 [靜止模式] 設定為 [否]，則回應為 HTTP/1.1 200 OK，如果 [靜止模式] 設定為 [是]，則為 HTTP/1.1 503。

備註

- 請勿使用 GET `https://mycoUnifiedAccessGateway.com:443/favicon.ico` 以外的任何其他 URL。這樣會導致不正確的狀態回應與資源流失。
 - 不支援將 `favicon.ico` 用於 Content Gateway 和 VMware Tunnel 服務。
-

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在 [進階設定] 區段中，按一下**系統組態**齒輪圖示。
- 3 在**靜止模式**列中，啟用**是以暫停 Unified Access Gateway 應用裝置**。
當應用裝置停止時，在工作階段關閉之後，應用裝置維護的現有工作階段會持續 10 小時。
- 4 按一下**儲存**。
進入負載平衡器的新要求會傳送至下一個 Unified Access Gateway 應用裝置。

下一個

- 對於 vSphere 部署：
 - a 透過匯出檔案來備份 JSON 檔案。
 - b 刪除處於靜止模式的舊 Unified Access Gateway 應用裝置。
 - c 部署新版的 Unified Access Gateway 應用裝置。
 - d 匯入您稍早匯出的 JSON 檔案。
- 對於 PowerShell 部署：
 - a 刪除處於靜止模式的 Unified Access Gateway 應用裝置。
 - b 使用第一次部署期間所使用的相同 INI 檔案重新部署 Unified Access Gateway。請參閱[使用 PowerShell 來部署 Unified Access Gateway 應用裝置](#)。

備註 如果您在重新啟用負載平衡器後看到通道伺服器憑證錯誤訊息，則套用先前在 Unified Access Gateway 應用裝置上使用的相同 SSL 伺服器憑證和私密金鑰 PEM 檔案。這是必要作業，因為私密金鑰基於安全因素無法匯出，因此 JSON 或 INI 檔案不可包含與 SSL 伺服器憑證相關聯的私密金鑰。使用 PowerShell 部署時會自動完成此作業，且您不需重新套用憑證。

在不含網路通訊協定設定檔 (NPP) 的情況下部署 Unified Access Gateway

Unified Access Gateway 的最新版本不接受來自網路通訊協定設定檔的網路遮罩或首碼和預設閘道設定。

部署您的 Unified Access Gateway 執行個體時，您必須提供此網路資訊。

如果是靜態部署，設定您的 Unified Access Gateway 執行個體時，請指定 IPv4 或 IPv6 位址、個別 NIC 的網路遮罩或首碼，以及 IPv4/IPv6 預設閘道。如果您未提供此資訊，則預設會對 IP 位址配置使用 DHCPV4+DHCPV6。

設定網路內容時，請注意下列事項：

- 如果您針對 NIC 的 IPMode 選取 STATICV4，則必須為該 NIC 指定 IPv4 位址和網路遮罩。
- 如果您為 NIC 的 IPMode 選取 STATICV6，則須為該 NIC 指定 IPv6 位址網路遮罩。
- 如果您針對 NIC 的 IPMode 同時選取 STATICV4 和 STATICV6，則必須為該 NIC 指定 IPv4 和 IPv6 位址和網路遮罩。
- 如果您未提供位址和網路遮罩資訊，則會由 DHCP 伺服器配置這些值。
- IPv4 和 IPv6 預設閘道內容為選用，但如果 Unified Access Gateway 需要與不在 Unified Access Gateway 中任何 NIC 之本機區段上的 IP 位址進行通訊，則必須進行指定。

如需關於設定網路內容的詳細資訊，請參閱[使用 OVF 範本精靈來部署 Unified Access Gateway](#)。

加入或退出客戶經驗改進計劃

VMware 客戶經驗改進計劃 (CEIP) 會提供資訊給 VMware，以便改善其產品和服務、修正問題，以及給予您如何部署和使用 VMware 產品的最佳建議。

本產品參與 VMware 的客戶經驗改進計劃 (「CEIP」)。關於透過 CEIP 所收集的資料以及 VMware 將其用於何種用途的詳細資料，請見 <https://www.vmware.com/tw/solutions/trustvmware/ceip.html> 上信任與保證中心的說明。

您可以隨時透過管理員 UI 加入或退出本產品的 CEIP。

程序

- 1 在**進階設定 > 系統組態**中，選取 [是] 或 [否]。

如果您選取 [是]，則 [客戶經驗改進計劃] 對話方塊會顯示已勾選的核取方塊，表示您即將加入此計劃。

- 2 檢閱對話方塊上的資訊，然後按一下**關閉**。
- 3 在 [系統組態] 頁面上按一下**儲存**以儲存您的變更。

部署 Unified Access Gateway 應用裝置

2

Unified Access Gateway 會封裝為 OVF，並且部署至 vSphere ESX 或 ESXi 主機作為預先設定的虛擬應用裝置。

您可以使用兩種主要方法在 vSphere ESX 或 ESXi 主機上安裝 Unified Access Gateway 應用裝置。支援 Microsoft Server 2012 和 2016 Hyper-V 角色。

- vSphere Client 或 vSphere Web Client 可用來部署 Unified Access Gateway OVF 範本。系統將提示您進行基本設定，包括 NIC 部署組態、IP 位址和管理介面密碼。部署 OVF 之後，登入 Unified Access Gateway 管理員使用者介面以設定 Unified Access Gateway 系統設定、設定多個使用案例中的安全 Edge Service，以及設定 DMZ 中的驗證。請參閱[使用 OVF 範本精靈來部署 Unified Access Gateway](#)。
- PowerShell 指令碼可以用來部署 Unified Access Gateway 和設定多個使用案例中的安全 Edge Service。您會下載 ZIP 檔案、為環境設定 PowerShell 指令碼，以及執行指令碼以部署 Unified Access Gateway。請參閱[使用 PowerShell 來部署 Unified Access Gateway 應用裝置](#)。

備註 針對每一應用程式通道和 Proxy 使用案例，您可以將 Unified Access Gateway 部署在 ESXi 或 Microsoft Hyper-V 環境中。

備註 在以上這兩個部署方法中，如果並未提供管理員 UI 密碼，則您稍後將無法新增管理員 UI 使用者來啟用對管理員 UI 或 API 的存取。如果您想要這麼做，則必須使用有效的密碼重新部署 Unified Access Gateway 執行個體。

本章節討論下列主題：

- [使用 OVF 範本精靈部署 Unified Access Gateway](#)
- [從管理組態頁面設定 Unified Access Gateway](#)
- [更新 SSL 伺服器簽署的憑證](#)

使用 OVF 範本精靈部署 Unified Access Gateway

若要部署 Unified Access Gateway，您必須使用 vSphere Client 或 vSphere Web Client 部署 OVF 範本，接著開啟應用裝置的電源，然後進行設定。

部署 OVF 時，您會設定需要的網路介面 (NIC) 數量、IP 位址及設定管理員根密碼。

部署 Unified Access Gateway 之後，移至管理使用者介面 (UI) 以設定 Unified Access Gateway 環境。在管理員 UI 中，設定桌面平台和應用程式資源，以及要在 DMZ 中使用的驗證方法。若要登入至管理員 UI 頁面，請移至 <https://<mycoUnifiedGatewayAppliance>.com:9443/admin/index.html>。

使用 OVF 範本精靈來部署 Unified Access Gateway

您可以透過登入 vCenter Server 並使用 [部署 OVF 範本] 精靈來部署 Unified Access Gateway 應用裝置。

有兩個版本的 Unified Access Gateway OVA 可供使用，即標準 OVA 和 FIPS 版本的 OVA。

OVA 的 FIPS 版本支援下列 Edge Service：

- Horizon (僅限傳遞驗證)
- VMware 每一應用程式通道

重要事項 FIPS 140-2 版本會使用 FIPS 認證的密碼集和雜湊執行，並啟用支援 FIPS 認證資料庫的限制服務。在 FIPS 模式中部署 Unified Access Gateway 時，應用裝置無法變更為標準 OVA 部署模式。

Unified Access Gateway 大小調整選項

若要簡化將 Unified Access Gateway 應用裝置部署為 Workspace ONE 安全開道的程序，可以將大小調整選項新增至應用裝置中的部署組態。部署組態可供您選擇「標準」或「大型」虛擬機器。

- **標準：**如果 Horizon 部署支援最多 2000 個 Horizon 連線，則建議使用此組態，以配合連線伺服器容量。針對並行連線最多 10,000 個的 Workspace ONE UEM 部署 (行動使用案例)，也建議使用此組態。
- **大型：**針對 Unified Access Gateway 需要支援超過 10,000 個並行連線的 Workspace ONE UEM 部署，建議使用此組態。此大小可讓 Content Gateway、每一應用程式通道和 Proxy 以及 Reverse Proxy 使用相同的 Unified Access Gateway 應用裝置。

先決條件

- 檢閱精靈中可用的部署選項。請參閱 [Unified Access Gateway 系統和網路需求](#)。
- 決定要為 Unified Access Gateway 應用裝置設定的網路介面和靜態 IP 位址數量。請參閱 [網路功能組態需求](#)。
- 從 VMware 網站 (<https://my.vmware.com/web/vmware/downloads>) 下載 Unified Access Gateway 應用裝置的 .ova 安裝程式檔案，或決定要使用的 URL (範例：http://example.com/vapps/euc-access-point-Y.Y.0-xxxxxxx_OVF10.ova)，其中 Y.Y 是版本號碼，而 xxxxxxx 是組建編號。
- 若為 Hyper-V 部署，且如果您要升級使用靜態 IP 的 Unified Access Gateway，請先刪除較舊的應用裝置，然後再部署 Unified Access Gateway 的較新執行個體。
- 若要在使用者不停機的情況下將較舊的應用裝置升級為 Unified Access Gateway 的新執行個體，請參閱 [不停機升級](#) 一節。

程序

- 1 使用原生 vSphere Client 或 vSphere Web Client 登入 vCenter Server 執行個體。
針對 IPv4 網路，請使用原生 vSphere Client 或 vSphere Web Client。對於 IPv6 網路，請使用 vSphere Web Client。
- 2 選取功能表命令來啟動**部署 OVF 範本**精靈。

選項	功能表命令
vSphere Client	選取 檔案 > 部署 OVF 範本 。
vSphere Web Client	選取屬於虛擬機器的有效父系物件的任何詳細目錄物件，例如資料中心、資料夾、叢集、資源集區或主機，並從 動作 功能表中選取 部署 OVF 範本 。

- 3 在 [選取來源] 頁面上，瀏覽至您下載的 .ova 檔案或輸入 URL，然後按**下一步**。
檢閱產品詳細資料、版本和大小需求。
- 4 按照提示進行，並參考下列準則以完成精靈。ESXi 和 Hyper-V 部署皆有兩個選項可指派 Unified Access Gateway 的 IP 指派。如果您打算升級，請先針對 Hyper-V 刪除具有相同 IP 位址的舊機器，然後再部署具有新位址的新機器。針對 ESXi，您可以關閉舊機器，並使用靜態指派以相同的 IP 位址部署新的機器。

選項	說明
名稱和位置	輸入 Unified Access Gateway 虛擬應用裝置的名稱。該名稱在詳細目錄資料夾內必須是唯一的。名稱區分大小寫。 選取虛擬應用裝置的位置。
部署組態	對於 IPv4 或 IPV6 網路，您可以使用一、二或三個網路介面 (NIC)。許多 DMZ 實作使用分開的網路來保護不同的流量類型。請根據 Unified Access Gateway 部署所在之 DMZ 的網路設計來對其設定。連同 NIC 數目，您也可以為 Unified Access Gateway 選擇 標準 或 大型 部署選項。 備註 標準 和 大型 部署的虛擬機器選項： <ul style="list-style-type: none"> ■ 標準 - 2 核心和 4 GB RAM ■ 大型 - 4 核心和 16 GB RAM
主機/叢集	選取要在其中執行虛擬應用裝置的主機或叢集。
磁碟格式	對於評估和測試環境，選取 [精簡佈建] 格式。對於生產環境，選取其中一個 [完整佈建] 格式。[完整佈建積極式歸零] 是一種完整虛擬磁碟格式，支援容錯之類的叢集功能，但需要的建立時間比其他虛擬磁碟類型還要久。

選項	說明
設定網路/網路對應	<p>如果您使用 vSphere Web Client, [設定網路] 頁面可讓您將每個 NIC 對應至網路, 並指定通訊協定設定。</p> <p>將 OVF 範本中使用的網路對應到詳細目錄中的網路。</p> <p>a 選取表格中的第一列 網際網路, 然後按一下向下箭頭來選取目的地網路。如果您選取 IPv6 作為 IP 通訊協定, 則必須選取具有 IPv6 功能的網路。</p> <p>在您選取該列之後, 您可以在視窗下半部輸入 DNS 伺服器、閘道和網路遮罩的 IP 位址。</p> <p>b 如果您使用多個 NIC, 請選取下一列 ManagementNetwork, 接著選取目的地網路, 然後您可以為該網路輸入 DNS 伺服器、閘道和網路遮罩的 IP 位址。</p> <p>如果您僅使用一個 NIC, 則所有列都會對應到相同網路。</p> <p>c 如果您有第三個 NIC, 則也請選取第三列並完成設定。</p> <p>如果您僅使用兩個 NIC, 對於這個第三列 BackendNetwork, 請選取您用於 ManagementNetwork 的相同網路。</p> <p>備註 忽略 IP 通訊協定下拉式功能表 (如果有顯示), 且不要在此處進行任何選取。IP 通訊協定 (IPv4/IPv6/兩者) 的實際的選取取決於在自訂網路內容時, 對 NIC 1 (eth0)、NIC 2 (eth1) 和 NIC 3 (eth2) 之 IPMode 所指定的 IP 模式。</p>

選項	說明
自訂網路內容	<p>在 [內容] 頁面上的文字方塊是 Unified Access Gateway 專屬的，對於其他類型的虛擬應用裝置來說可能並非必要。精靈頁面中的文字會說明每個設定。如果文字在精靈右側被截斷，請從視窗右下角拖曳以調整其大小。針對 STATICV4 的每個 NIC，您必須輸入 NIC 的 IPv4 位址。針對 STATICV6，您必須輸入 NIC 的 IPv6 位址。如果將文字方塊保留空白，則 IP 位址預設會配置為 DHCPV4+DHCPV6。</p> <p>重要事項 Unified Access Gateway 的最新版本不接受來自網路通訊協定設定檔 (NPP) 的網路遮罩或首碼值和預設閘道設定。若要使用靜態 IP 配置來設定 Unified Access Gateway，您必須在網路內容下設定網路遮罩/首碼。這些值無法從 NPP 填入。</p>
	<ul style="list-style-type: none"> ■ NIC 1 的 IPMode (eth0): STATICV4/STATICV6/DHCPV4/DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/DHCPV4+DHCPV6/DHCPV4+AUTOV6。 ■ NIC 2 的 IPMode (eth1): STATICV4/STATICV6/DHCPV4/DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/DHCPV4+DHCPV6/DHCPV4+AUTOV6。 ■ NIC 3 的 IPMode (eth2): STATICV4/STATICV6/DHCPV4/DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/DHCPV4+DHCPV6/DHCPV4+AUTOV6。 ■ 使用 {tcp udp}/listening-port-number/destination-ip-address:destination-port-number 格式的轉送規則逗號分隔清單。例如針對 IPv4 時為 tcp/5262/10.110.92.129:9443, tcp/5263/10.20.30.50:7443。 ■ NIC 1 (eth0) IPv4 位址。如果您已針對 NIC 模式輸入 STATICV4，請輸入 NIC 的 IPv4 位址。 <ul style="list-style-type: none"> ■ 使用 ipv4-network-address/bits ipv4-gateway-address 格式之 NIC 1 (eth0) 的 IPv4 自訂路由逗號分隔清單。例如，20.2.0.0/16 10.2.0.1, 20.9.0.0/16 10.2.0.2, 10.2.0.1/32
	<p>備註 如果未指定 ipv4-gateway-address，所新增個別路由的閘道為 0.0.0.0</p>
	<ul style="list-style-type: none"> ■ NIC 1 (eth0) IPv6 位址。如果您已針對 NIC 模式輸入 STATICV6，請輸入 NIC 的 IPv6 位址。 ■ NIC 1 (eth0) IPv4 網路遮罩。輸入 NIC 的 IPv4 網路遮罩。 ■ NIC 1 (eth0) IPv6 首碼。輸入 NIC 的 IPv6 首碼。 ■ DNS 伺服器位址。針對 Unified Access Gateway 應用裝置的網域名稱伺服器輸入以空格分隔的 IPv4 或 IPv6 位址。IPv4 項目的範例為 192.0.2.1, 192.0.2.2。IPv6 項目的範例為 fc00:10:112:54::1 ■ IPv4 預設閘道。如果 Unified Access Gateway 需要與不在 Unified Access Gateway 中任何 NIC 之本機區段上的 IP 位址進行通訊，請輸入 IPv4 預設閘道。 ■ IPv6 預設閘道。如果 Unified Access Gateway 需要與不在 Unified Access Gateway 中任何 NIC 之本機區段上的 IP 位址進行通訊，請輸入 IPv6 預設閘道。 ■ NIC 2 (eth1) IPv4 位址。如果您已針對 NIC 模式輸入 STATICV4，請輸入 NIC 的 IPv4 位址。

選項	說明
	<ul style="list-style-type: none"> 使用 <code>ipv4-network-address/bits ipv4-gateway-address</code> 格式之 NIC 2 (eth1) 的 IPv4 自訂路由逗號分隔清單。例如, 20.2.0.0/16 10.2.0.1, 20.9.0.0/16 10.2.0.2, 10.2.0.1/32 <p>備註 如果未指定 <code>ipv4-gateway-address</code>, 所新增個別路由的閘道為 0.0.0.0</p> <ul style="list-style-type: none"> NIC 2 (eth1) IPv6 位址。如果您已針對 NIC 模式輸入 STATICV6, 請輸入 NIC 的 IPv6 位址。 NIC 2 (eth1) IPv4 網路遮罩。輸入此 NIC 的 IPv4 網路遮罩。 NIC 2 (eth1) IPv6 首碼。輸入此 NIC 的 IPv6 首碼。 NIC 3 (eth2) IPv4 位址。如果您已針對 NIC 模式輸入 STATICV4, 請輸入 NIC 的 IPv4 位址。 使用 <code>ipv4-network-address/bits ipv4-gateway-address</code> 格式之 NIC 3 (eth2) 的 IPv4 自訂路由逗號分隔清單。例如, 20.2.0.0/16 10.2.0.1, 20.9.0.0/16 10.2.0.2, 10.2.0.1/32 <p>備註 如果未指定 <code>ipv4-gateway-address</code>, 所新增個別路由的閘道為 0.0.0.0</p> <ul style="list-style-type: none"> NIC 3 (eth2) IPv6 位址。如果您已針對 NIC 模式輸入 STATICV6, 請輸入 NIC 的 IPv6 位址。 NIC 3 (eth2) IPv4 網路遮罩。輸入此 NIC 的 IPv4 網路遮罩。 NIC 3 (eth2) IPv6 首碼。輸入此 NIC 的 IPv6 首碼。 虛擬機器根使用者密碼。輸入供根使用者用來登入虛擬機器主控台的密碼。 管理員 UI 密碼。輸入管理員使用者的密碼, 以便從管理員 UI 設定 Unified Access Gateway 以及存取 REST API。 <p>其他設定皆為選用或已輸入預設設定。</p>
加入 CEIP	選取加入 VMware 客戶經驗改進計劃以加入 CEIP, 或取消選取此選項以離開 CEIP。

5 在 [即將完成] 頁面上, 選取**部署後開啟電源**, 然後按一下**完成**。

vCenter Server 狀態區域會出現 [部署 OVF 範本] 工作, 以供您監控部署。您也可以在此在虛擬機器上開啟主控台, 檢視在系統開機期間顯示的主控台訊息。檔案 `/var/log/boot.msg` 中也會記錄這些訊息。

6 部署完成後, 確認使用者可以透過開啟瀏覽器並輸入下列 URL 來連線至應用裝置:

```
https://FQDN-of-UAG-appliance
```

在此 URL 中, `FQDN-of-UAG-appliance` 是 Unified Access Gateway 應用裝置的 DNS 可解析完整網域名稱。

如果部署成功, 您會看到 Unified Access Gateway 所指向之伺服器所提供的網頁。如果部署不成功, 您可以刪除應用裝置虛擬機器, 然後重新部署應用裝置。最常見的錯誤是未正確輸入憑證指紋。

Unified Access Gateway 應用裝置會自動部署並啟動。

下一個

- 登入 Unified Access Gateway 管理員使用者介面 (UI) 並設定桌面平台和應用程式資源，允許透過 Unified Access Gateway 以及要在 DMZ 中使用的驗證方法，進行網際網路的遠端存取。管理主控台 URL 的格式為 `https://<mycoUnified Access Gatewayappliance.com>:9443/admin/index.html`。

重要事項 您必須使用管理員 UI 來完成部署後 Unified Access Gateway 組態。如果並未提供管理員 UI 密碼，則您稍後將無法新增管理員 UI 使用者來啟用對管理員 UI 或 API 的存取。如果想要新增管理員 UI 使用者，則必須使用有效的管理員 UI 密碼來重新部署您的 Unified Access Gateway 執行個體。

備註 如果您無法存取管理員 UI 登入畫面，請檢查以確認虛擬機器是否在 OVA 的安裝期間顯示 IP 位址。如果未設定 IP 位址，請使用 UI 中提及的 VAMI 命令來重新設定 NIC。以 `"cd /opt/vmware/share/vami"` 形式執行命令，然後執行命令 `"./vami_config_net"`。

- 如果您使用 vSphere 或 PowerShell 進行部署，請執行健全狀況檢查並確保新部署的執行個體傳回 200 OK 回應。

從管理組態頁面設定 Unified Access Gateway

部署 OVF 且 Unified Access Gateway 應用裝置開啟電源之後，請登入 Unified Access Gateway 管理員使用者介面以進行設定。

備註 當您第一次啟動 Unified Access Gateway 管理主控台時，系統會提示您變更在部署應用裝置時所設定的密碼。

[一般設定] 頁面和 [進階設定] 頁面包含下列項目。

- Unified Access Gateway 系統組態和 TLS 伺服器憑證
- Horizon、Reverse Proxy、VMware Tunnel 及內容閘道 (也稱為 CG) 的 Edge Service 設定
- RSA SecurID、RADIUS、X.509 憑證，以及 RSA 調適性驗證的驗證設定
- SAML 身分識別提供者和服務提供者設定
- 網路設定
- 端點符合性檢查提供者設定
- 身分識別橋接設定組態
- 帳戶設定

下列選項可從 [支援設定] 頁面存取。

- 下載 Unified Access Gateway 記錄檔。
- 匯出 Unified Access Gateway 設定以擷取組態設定。
- 設定記錄層級設定。
- 匯入 Unified Access Gateway 設定以建立和更新整個 Unified Access Gateway 組態。

設定 Unified Access Gateway 系統設定

您可以設定用來從管理員組態頁面加密用戶端與 Unified Access Gateway 應用裝置之間通訊的安全性通訊協定和密碼編譯演算法。

先決條件

- 檢閱 Unified Access Gateway 部署內容。需要下列設定資訊：
 - Unified Access Gateway 應用裝置的靜態 IP 位址
 - DNS 伺服器的 IP 位址
 - 管理主控台的密碼
 - Unified Access Gateway 應用裝置所指向的伺服器執行個體或負載平衡器的 URL
 - 儲存事件記錄檔的 Syslog 伺服器 URL

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在 [進階設定] 區段中，按一下**系統組態**齒輪圖示。
- 3 編輯下列 Unified Access Gateway 應用裝置組態值。

選項	預設值和說明
UAG 名稱	唯一的 UAG 應用裝置名稱。
地區設定	<p>指定在產生錯誤訊息時使用的語言設定。</p> <ul style="list-style-type: none"> ■ en_US 表示美式英文。這是預設值。 ■ ja_JP 表示日文 ■ fr_FR 表示法文 ■ de_DE 表示德文 ■ zh_CN 表示簡體中文 ■ zh_TW 表示繁體中文 ■ ko_KR 表示韓文 ■ es 表示西班牙文 ■ pt_BR 表示葡萄牙文 (巴西) ■ en_BR 表示英式英文
加密套件	<p>在多數情況下，不需要變更預設的設定。這是可用來加密用戶端與 Unified Access Gateway 應用裝置之間通訊的密碼編譯演算法。加密設定可用於啟用各種安全性通訊協定。</p>
接受加密順序	預設值為 [否]。選取 是 可啟用 TLS 加密清單順序控制。
TLS 1.0 已啟用	預設值為 [否]。選取 是 可啟用 TLS 1.0 安全性通訊協定。
TLS 1.1 已啟用	預設值為 [是]。TLS 1.1 安全性通訊協定已啟用。
TLS 1.2 已啟用	預設值為 [是]。TLS 1.2 安全性通訊協定已啟用。

選項	預設值和說明
Syslog URL	輸入用來記錄 Unified Access Gateway 事件的 Syslog 伺服器 URL。這個值可以是 URL、主機名稱或 IP 位址。如果您未設定 Syslog 伺服器 URL，則不會記錄任何事件。 最多可提供兩個 URL。以逗號分隔的 URL。範例： syslog://server1.example.com:514, syslog://server2.example.com:514
Syslog 稽核 URL	輸入用來記錄 Unified Access Gateway 稽核事件的 Syslog 伺服器 URL。這個值可以是 URL、主機名稱或 IP 位址。如果您未設定 Syslog 伺服器 URL，則不會記錄任何稽核事件。 最多可提供兩個 URL。以逗號分隔的 URL。範例： syslog://server1.example.com:514, syslog://server2.example.com:514
健全狀況檢查 URL	輸入負載平衡器連線到的 URL，並檢查 Unified Access Gateway 的健全狀況。
要快取的 Cookie	Unified Access Gateway 快取的 Cookie 集。預設值為 [無]。
IP 模式	選取靜態 IP 模式，可為 STATICV4 或 STATICV6。
工作階段逾時	預設值為 3600000 毫秒。
靜止模式	啟用是 可暫停 Unified Access Gateway 應用裝置，達成一致的狀態來執行維護工作
監控間隔	預設值為 60 。
密碼使用期限	目前管理員密碼的有效天數。預設值為 90 天。若要密碼永不到期，請指定為零 (0)。
要求逾時	指定要求逾時，以秒為單位。預設值為 3000 。
本文接收逾時	指定本文接收逾時，以秒為單位。預設值為 5000 。
用戶端連線閒置逾時	指定關閉連線之前，用戶端連線可以維持閒置的時間 (以秒為單位)。預設值為 360 秒 (6 分鐘)。零值表示無閒置逾時。
驗證逾時	指定驗證逾時，以秒為單位。預設值為 300000 。
加入 CEIP	啟用時，會將客戶經驗改進計劃 (「CEIP」) 資訊傳送給 VMware。如需詳細資料，請參閱 加入或退出客戶經驗改進計劃 。

4 按一下儲存。

下一個

針對 Unified Access Gateway 部署時所搭配的元件設定 Edge Service 設定。設定 Edge 設定之後，請設定驗證設定。

變更網路設定

您可以從管理員 UI 為已設定的網路修改網路設定，例如 IP 位址、子網路遮罩、預設閘道和 IP 配置模式。

修改網路設定時，請留意下列限制：

- IPv4 是唯一受支援的 IP 模式，IPv6 不受支援。
- 當管理網路 IP 的 IP 位址動態變更時，對新的 IP 位址將不支援瀏覽器重新導向。
- 變更實際網路對向網路介面的 IP 位址、子網路遮罩或預設閘道時，所有目前的工作階段皆會遺失。

先決條件

- 確定您具有管理員權限。
- 如果您要將 IP 變更為靜態 IP 位址、子網路遮罩或預設閘道，則必須事先得知位址、子網路遮罩和預設閘道。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在**進階設定**下，按一下**網路設定**旁邊的齒輪圖示。
此時會顯示已設定的網路及其設定的清單。
- 3 在 [網路設定] 視窗中，按一下要變更設定之網路旁邊的齒輪圖示，然後輸入下列資訊：

IPv4 組態

標籤	說明
IPv4 配置模式	選取要以靜態還是動態方式配置 IP。
IPv4 位址	網路的 IP 位址。如果您選取 [動態 IP] 配置，則不需要指定 IP 位址。
IPv4 網路遮罩	網路的 IPv4 網路遮罩。如果您選取 [動態 IP] 配置，則不需要指定 IPv4 網路遮罩。
IPv4 預設閘道	Unified Access Gateway 的 IPv4 預設閘道位址。如果您選取 [動態 IP] 配置，則不需要指定預設閘道 IP 位址。
IPv4 靜態路由	網路的 IPv4 自訂路由。它無法修改。

IPv6 組態無法修改。

標籤	說明
IPv6 配置模式	指定 IP 的配置方式為靜態、動態或自動。
IPv6 位址	網路的 IP 位址。
IPv6 首碼	網路的 IPv6 首碼。
IPv6 預設閘道	Unified Access Gateway 的 IPv6 預設閘道位址。

- 4 按一下**儲存**。

如果成功變更設定，將會顯示一則成功訊息。如果無法更新網路設定，則會顯示錯誤訊息。

設定使用者帳戶設定

作為擁有 Unified Access Gateway 系統完整存取權的超級使用者管理員，您可以從管理員組態頁面新增和刪除使用者、變更密碼，以及修改使用者的角色。

包括低權限管理員的詳細資料等帳戶設定無法從應用裝置設定加以匯出或匯入。若要在 Unified Access Gateway 的新執行個體上設定新的低權限帳戶，請透過管理員 UI 來手動設定。

新增低權限管理員

您現在可以設定和新增可執行數目有限工作 (例如唯讀作業和系統監控等) 的低權限管理員。

備註 目前，您僅能將一個低權限管理員新增至 Unified Access Gateway 的執行個體。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在 [進階設定] 下，選取 [帳戶設定] 齒輪圖示。
- 3 在 [帳戶設定] 視窗中，按一下**新增**。
角色會自動設定為 `ROLE_MONITORING`。
- 4 在 [帳戶設定] 視窗中，輸入下列資訊：
 - a 使用者的唯一使用者名稱。
 - b (選擇性) 新增使用者後，如果您想要立即啟用使用者，請選取**已啟用**方塊。
 - c 輸入使用者的密碼。密碼長度至少必須有 8 個字元，至少包含一個大寫字母和一個小寫字母、一個數字和一個特殊字元，其中包括 `!@#$%*()`。
 - d 確認密碼。
- 5 按一下**儲存**。

您新增的管理員會在帳戶設定下列出。

下一個

低權限管理員可登入系統以變更密碼或執行監控工作。

修改使用者帳戶設定

作為超級使用者管理員，您可以變更使用者的密碼，以及啟用或停用使用者。

您也可以變更自己的密碼，但無法停用自己的帳戶。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在 [進階設定] 區段中，按一下 [帳戶設定]。
使用者清單隨即顯示。
- 3 按一下您想要修改其帳戶之使用者旁的齒輪圖示。

4 編輯下列值。

- a 根據您想要啟用或停用使用者來選取或取消選取**啟用**方塊。
- b 若要重設使用者密碼，請輸入新密碼並確認密碼。如果您以管理員身分登入，則也必須輸入舊密碼。

密碼長度至少必須有 8 個字元，至少包含一個大寫字母和一個小寫字母、一個數字和一個特殊字元，其中包括 ! @ # \$ % * () 。

5 按一下**儲存**。

使用 Unified Access Gateway 主控台重設管理員密碼

如果忘記部署期間設定的管理員使用者密碼，使用者可以使用根使用者認證登入 Unified Access Gateway 主控台，並重設管理員 UI 密碼。

先決條件

您必須擁有以根使用者或具有根權限之使用者身分登入虛擬機器的密碼。使用者必須是 *族* 群組的一部分。

程序

- 1 以根使用者身分登入 Unified Access Gateway 主控台的作業系統。

- 2 輸入下列命令以重設管理員的密碼。

```
adminpwd
```

```
New password for user "admin": *****
```

```
Retype new password: *****
```

在此範例中，密碼的長度至少為 8 個字元，至少包含一個大寫字母和一個小寫字母、一個數字和一個特殊字元，其中包括 ! @ # \$ % * () 。

此時將顯示下列訊息。

```
adminpwd: password for "admin" updated successfully
```

- 3 輸入下列命令，以重設具有較低權限之管理員的密碼。

```
adminpwd [-u <username>]
```

```
New password for user "jdoe": *****
```

```
Retype new password: *****
```

在此範例中，密碼的長度至少為 8 個字元，至少包含一個大寫字母和一個小寫字母、一個數字和一個特殊字元，其中包括 ! @ # \$ % * () 。

此時將顯示下列訊息。

```
adminpwd: password for "jdoe" updated successfully
```

已成功重設管理員使用者密碼。

下一個

使用者現在可以使用剛才設定的管理員密碼登入 Unified Access Gateway 介面。使用 `adminpwd` CLI 命令重設密碼後首次登入時，系統會要求使用者變更密碼。

備註 變更密碼後，使用者必須在第一次嘗試時登入。

刪除使用者

身為超級使用者管理員，您可以刪除非根使用者。

您無法刪除根管理員。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在 [進階設定] 下，選取 [帳戶設定] 齒輪圖示。
使用者清單隨即顯示。
- 3 按一下要刪除之使用者旁邊的「x」按鈕。

警告 會立即刪除使用者。此動作無法復原。

系統會刪除使用者帳戶，並顯示一則訊息。

更新 SSL 伺服器簽署的憑證

您可以在簽署的憑證到期時加以取代，或將預設憑證替代為 CA 簽署的憑證。

若是生產環境，VMware 強烈建議您盡快更換預設憑證。在部署 Unified Access Gateway 應用裝置時所產生的預設 TLS/SSL 伺服器憑證並未經信任的憑證授權機構簽署。

在上傳憑證時，請留意下列考量事項：

- 您可以將管理員和使用者的預設憑證取代為 CA 簽署的 PEM 憑證。
- 當您使用管理員介面上傳 CA 簽署的憑證時，管理員介面上的 SSL 連接器會更新並重新啟動，以確保上傳的憑證能夠生效。如果連接器無法使用上傳的 CA 簽署憑證來重新啟動，則會產生自我簽署憑證並將其套用於管理員介面，並通知使用者先前嘗試上傳憑證並未成功。

先決條件

- 新簽署的憑證和私密金鑰會儲存到您可以存取的電腦。
- 將憑證轉換為 PEM 格式檔案，再將 `.pem` 檔案轉換為單行格式。請參閱[將憑證檔案轉換為單行 PEM 格式](#)。

程序

- 1 在管理主控台中，按一下**選取**。
- 2 在 [進階設定] 區段中，按一下 [SSL 伺服器憑證設定] 齒輪圖示。

- 3 選取**管理員介面**或**網際網路介面**，將憑證套用至其中一個介面。您也可以選取兩個介面，而同時對兩者套用憑證。
- 4 選取 **PEM** 或 **PFX** 的憑證類型。
- 5 如果憑證類型為 **PEM**：
 - a 在 [私密金鑰] 列，按一下**選取**並瀏覽至私密金鑰檔案。
 - b 按一下**開啟**以上傳檔案。
 - c 在 [憑證鏈結] 列，按一下**選取**並瀏覽至憑證鏈結檔案。
 - d 按一下**開啟**以上傳檔案。
- 6 如果憑證類型為 **PFX**：
 - a 在 [上傳 PFX] 列，按一下**選取**並瀏覽至 **pfx** 檔案。
 - b 按一下**開啟**以上傳檔案。
 - c 輸入 PFX 憑證的密碼。
 - d 輸入 PFX 憑證的別名。

有多個憑證存在時，您可以使用別名加以區分。
- 7 按一下**儲存**。

憑證更新成功時，會顯示確認訊息。

下一個

- 如果您使用 **CA** 簽署的憑證來更新憑證，但簽署憑證的 **CA** 並不知名，請設定用戶端，使其信任根憑證和中繼憑證。
- 如果您已為**管理員介面**上傳 **CA** 簽署的憑證，請關閉瀏覽器，然後在新的瀏覽器視窗中重新開啟管理員 UI。
- 如果管理員介面上已有 **CA** 簽署的憑證生效，但您上傳了自我簽署憑證，則管理員 UI 可能不會如預期般運作。請清除瀏覽器快取，然後在新視窗中開啟管理員 UI。

使用 PowerShell 部署 Unified Access Gateway

3

您可以使用 PowerShell 指令碼來部署 Unified Access Gateway。提供的 PowerShell 指令碼可作為範例指令碼，您可加以改寫來符合您環境的特定需求。

使用 PowerShell 指令碼時，為了部署 Unified Access Gateway，指令碼會呼叫 OVF Tool 命令，並確認設定以自動建構正確的命令列語法。這個方法也能讓您在部署期間套用 TLS/SSL 伺服器憑證組態等進階設定。

本章節討論下列主題：

- [使用 PowerShell 部署 Unified Access Gateway 的系統需求](#)
- [使用 PowerShell 來部署 Unified Access Gateway 應用裝置](#)

使用 PowerShell 部署 Unified Access Gateway 的系統需求

若要使用 PowerShell 指令碼部署 Unified Access Gateway，您必須使用特定版本的 VMware 產品。

- 具有 vCenter Server 的 VMware vSphere ESXi 主機。
- PowerShell 指令碼會在 Windows 8.1 或更新版本機器或 Windows Server 2008 R2 或更新版本上執行。

此機器也可以是在 Windows 上執行的 vCenter Server 或單獨的 Windows 機器。

- 執行指令碼的 Windows 機器必須安裝 VMware OVF Tool 命令。

您必須從 <https://www.vmware.com/support/developer/ovf/> 安裝 OVF Tool 4.0.1 或更新版本。

您必須選取要使用的 vSphere 資料存放區和網路。

使用 PowerShell 來部署 Unified Access Gateway 應用裝置

PowerShell 指令碼能為您的環境備妥所有組態設定。當您執行 PowerShell 指令碼來部署 Unified Access Gateway 時，解決方案會在首次系統開機時做好生產準備。

重要事項 您可以利用 PowerShell 部署在 INI 檔案中提供所有設定，而 Unified Access Gateway 執行個體在開機後便會處於生產就緒狀態。如果您在部署後不想變更任何設定，則不需提供管理員 UI 密碼。

不過，如果並未在部署期間提供管理員 UI 密碼，則管理員 UI 和 API 皆無法使用。

備註 如果並未在部署時提供管理員 UI 密碼，則您稍後將無法新增使用者來啟用對管理員 UI 或 API 的存取。如果想要新增管理員 UI 使用者，則必須使用有效的密碼來重新部署您的 Unified Access Gateway 執行個體。

先決條件

- 若為 Hyper-V 部署，且如果您要升級使用靜態 IP 的 Unified Access Gateway，請先刪除較舊的應用裝置，然後再部署 Unified Access Gateway 的較新執行個體。
- 請確認系統需求適當且可供使用。

以下是在環境中部署 Unified Access Gateway 的範例指令碼。

圖 3-1 範例 PowerShell 指令碼

```

PS C:\uagdeploy-330-v45> .\uagdeploy.ps1 -iniFile uagt-basic.ini
Unified Access Gateway (UAG) virtual appliance deployment script
Enter a root password for Vivek_LB9: *****
Re-enter the root password: *****
Enter an optional admin password for the REST API management access for Vivek_LB9: *****
Re-enter the admin password: *****
Join the VMware Customer Experience Improvement Program?
This setting is supported in UAG versions 3.1 and newer.
VMware's Customer Experience Improvement Program (CEIP) provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products.
As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual.
Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.
If you prefer not to participate in VMware's CEIP for UAG 3.1 and newer, you should enter no.
You may join or leave VMware's CEIP for this product at any time. In the UAG Admin UI in System Configuration, there is a setting 'Join CEIP' which can be set to yes or no and has immediate effect.
To join the VMware Customer Experience Improvement Program with Unified Access Gateway version 3.1 and newer, either enter yes or just hit return as the default for this setting is yes.
Join CEIP for Vivek_LB9? (default is yes for UAG 3.1 and newer):
Deployment will use a self-signed SSL/TLS server certificate (SSLcert)
Deployment will use a self-signed SSL/TLS server certificate (SSLcertAdmin)
Deployment will use the specified Certificate Auth PEM file
Opening OVA source: C:\Users\Administrator\Downloads\ueuc-unified-access-gateway-3.3.1.0-9451727_OVF10.ova
The manifest validates
Source is signed and the certificate validates
Opening VM target: w:\administrator%40vsphere.local\10.110.88.3\443\BLRM-IDM-DC/host/BLRM-IDM-CLUSTER/Resources/
Powering off VM: Vivek_LB9
Deleting VM: Vivek_LB9
Deploying to VM: w:\administrator%40vsphere.local\10.110.88.3\443\BLRM-IDM-DC/host/BLRM-IDM-CLUSTER/Resources/
Transfer Completed
Powering on VM: Vivek_LB9
Task Completed
Received IP address: 10.110.93.219
Completed successfully
Note that the IP addresses will be set to the specified IP addresses for each NIC
UAG virtual appliance Vivek_LB9 deployed successfully
PS C:\uagdeploy-330-v45>
  
```

程序

- 1 從 My VMware 將 Unified Access Gateway OVA 下載至您的 Windows 機器。
- 2 將 `uagdeploy-XXX.zip` 檔案下載到 Windows 機器上的資料夾。

您可以前往 <https://communities.vmware.com/docs/DOC-30835> 取得 ZIP 檔案。

- 3 開啟 PowerShell 指令碼，並將目錄修改為指令碼的所在位置。

4 為 Unified Access Gateway 虛擬應用裝置建立 INI 組態檔案。

例如：部署新的 Unified Access Gateway 應用裝置 *AP1*。組態檔案的名稱為 *ap1.ini*。該檔案含有 AP1 的所有組態設定。您可以使用 *apdeploy.ZIP* 檔案中的範例 INI 檔案來建立 INI 檔案，接著再適度修改設定。

備註

- 您可以將獨一無二的 INI 檔案用於環境中的多個 Unified Access Gateway 部署。您必須適度變更 INI 檔案中的 IP 位址和名稱參數，才能部署多個應用裝置。
- 不支援將 *healthCheckUrl* 設定的 *favicon.ico* 值用於 Content Gateway 和 VMware Tunnel。

要修改的 INI 檔案範例。

```
[General]
netManagementNetwork=
netInternet=
netBackendNetwork=
name=
dns=10.112.64.1
ip0=10.108.120.119
diskMode=
source=
defaultGateway=10.108.120.125
target=
ds=
authenticationTimeout=300000
fipsEnabled=false
uagName=trustedcert
locale=en_US
ipModeforNIC3=DHCPV4_DHCPV6
tls12Enabled=true
ipMode=DHCPV4_DHCPV6
requestTimeoutMsec=10000
ipModeforNIC2=DHCPV4_DHCPV6
tls11Enabled=true
clientConnectionIdleTimeout=180
tls10Enabled=false
adminCertRolledBack=false
honorCipherOrder=false
cookiesToBeCached=none
healthCheckUrl=/favicon.ico
quiesceMode=false
isCiphersSetByUser=false
tlsPortSharingEnabled=true
ceipEnabled=true
bodyReceiveTimeoutMsec=15000
monitorInterval=60
cipherSuites=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_
AES_128_CBC_SHA
adminPasswordExpirationDays=90
httpConnectionTimeout=120
isTLS11SetByUser=false
```

```

sessionTimeout=36000000
ssl30Enabled=false

[WebReverseProxy1]
proxyDestinationUrl=https://10.108.120.21
trustedCert1=
instanceId=view
healthCheckUrl=/favicon.ico
userNameHeader=AccessPoint-User-ID
proxyPattern=/(.*)
landingPagePath=/
hostEntry1=10.108.120.21 HZNView.uagqe.auto.com

[Horizon]
proxyDestinationUrl=https://enterViewConnectionServerUrl
trustedCert1=
gatewayLocation=external
disableHtmlAccess=false
healthCheckUrl=/favicon.ico
proxyDestinationIPSupport=IPV4
smartCardHintPrompt=false
queryBrokerInterval=300
proxyPattern=(/view-client(.*)|portal(.*)|appblast(.*))
matchWindowsUserName=false
windowsSSOEnabled=false

[SSLCert]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

[SSLCertAdmin]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

```

- 5 若要確定指令碼執行成功，請輸入 PowerShell `set-executionpolicy` 命令。

```
set-executionpolicy -scope currentuser unrestricted
```

如果指令碼執行目前受到限制，您才必須執行這個命令一次。

- a (選擇性) 如果出現與指令碼相關的警告，請執行下列命令以解除封鎖警告：`unlock-file -path .\uagdeploy.ps1`

- 6 執行命令以開始部署。如果您未指定 `.INI` 檔案，指令碼的預設值為 `ap.ini`。

```
.\uagdeploy.ps1 -iniFile uag1.ini
```

7 當出現提示時，請輸入認證並完成指令碼。

備註 如果系統提示您新增目標機器的指紋，請輸入 **yes**。

Unified Access Gateway 應用裝置部署即告完成，並可供生產之用。

如需 PowerShell 指令碼的詳細資訊，請參閱 <https://communities.vmware.com/docs/DOC-30835>。

下一個

如果您想要升級 Unified Access Gateway 同時保留現有的設定，請編輯 `.ini` 檔案將來源參考變更為新版本，然後重新執行 `.ini` 檔案：`uagdeploy.ps1 uag1.ini`。此程序可能需要長達 3 分鐘。

```
[General]
name=UAG1
source=C:\temp\uec-unified-access-gateway-3.2.1-7766089_OVF10.ova
```

如果您想要在服務不中斷的情況下升級，請參閱[不停機升級](#)。

Unified Access Gateway 的部署使用案例

4

本章中說明的部署案例可協助您找出並組織環境中的 Unified Access Gateway 部署。

您可以使用 Unified Access Gateway、Horizon、Horizon Cloud with On-Premises Infrastructure 和 VMware AirWatch 來部署 VMware Identity Manager。

本章節討論下列主題：

- 使用 Horizon 與 Horizon Cloud with On-Premises Infrastructure 進行部署
- Horizon 的端點符合性檢查
- 部署為 Reverse Proxy
- 單一登入存取內部部署舊版 Web 應用程式的部署
- Unified Access Gateway 的 VMware AirWatch 元件
- 其他部署使用案例

使用 Horizon 與 Horizon Cloud with On-Premises Infrastructure 進行部署

您可以使用 Unified Access Gateway 和 Horizon Cloud with On-Premises Infrastructure 雲端基礎結構來部署 Horizon Air。

部署案例

Unified Access Gateway 能提供安全的遠端存取能力，供您存取客戶資料中心內的內部部署虛擬桌面平台和應用程式。它能與 Horizon 或 Horizon Air 的內部部署搭配運作，以進行統合管理。

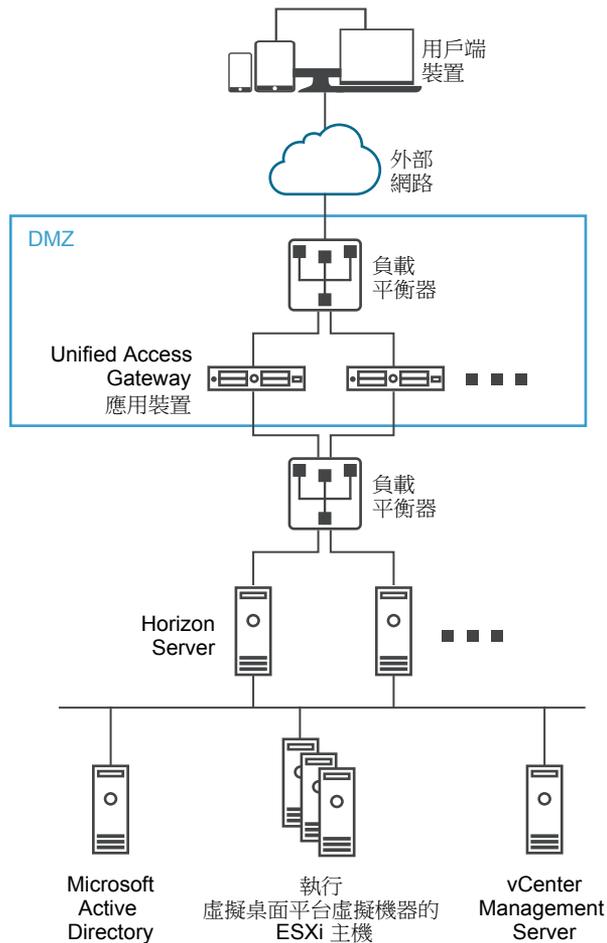
Unified Access Gateway 讓企業得以有效保證使用者的身分識別，而且能精準控制使用者對於有權使用之桌面平台和應用程式的存取權限。

Unified Access Gateway 虛擬應用裝置通常部署在網路的非軍事區 (DMZ)。在 DMZ 中部署能確保所有進入資料中心並前往桌面平台和應用程式資源的流量是代表經過嚴格驗證之使用者的流量。

Unified Access Gateway 虛擬應用裝置還能確保經過驗證之使用者的流量只能導向該使用者有權使用的桌面平台和應用程式資源。這個層級的保護涉及具體檢測桌面平台通訊協定、協調可能迅速變動的原則和網路位址，以便精確地控制存取權限。

下圖顯示包含前端和後端防火牆的組態範例。

圖 4-1 DMZ 拓撲中的 Unified Access Gateway



您必須確認已滿足需求才能以 Horizon 順暢地部署 Unified Access Gateway。

- Unified Access Gateway 應用裝置指向 Horizon Server 前方的負載平衡器，伺服器執行個體的選擇不會固定不變。
- 依預設，連接埠 8443 必須可供 Blast TCP/UDP 使用。不過，也可以將連接埠 443 設定為可供 Blast TCP/UDP 使用。

備註 如果您將 Unified Access Gateway 設定為使用 IPv4 和 IPv6 兩種模式，則必須將 Blast TCP/UDP 設定為連接埠 443。您可以啟用 Unified Access Gateway 以作為橋接，供 IPv6 Horizon 用戶端連線至 IPv4 後端的連線伺服器或代理程式環境。請參閱對 [Horizon 基礎結構支援 IPv4 和 IPv6 雙重模式](#)。

- 使用 Unified Access Gateway 部署 Horizon 時，必須啟用 Blast 安全閘道和 PCoIP 安全閘道。這可確保顯示通訊協定可以自動透過 Unified Access Gateway 成為 Proxy。*BlastExternalURL* 和 *pcoipExternalURL* 設定會指定 Horizon Client 使用的連線位址，以便透過 Unified Access Gateway 上的適當閘道路由傳送這些顯示通訊協定連線。由於這些閘道能代表經過驗證的使用者確保顯示通訊協定流量受到控制，因此能改善安全性。未經過驗證的顯示通訊協定流量會遭到 Unified Access Gateway 忽略。

- 在 Horizon 連線伺服器執行個體上停用安全閘道 (Blast 安全閘道和 PCoIP 安全閘道)，並在 Unified Access Gateway 應用裝置上啟用這些閘道。

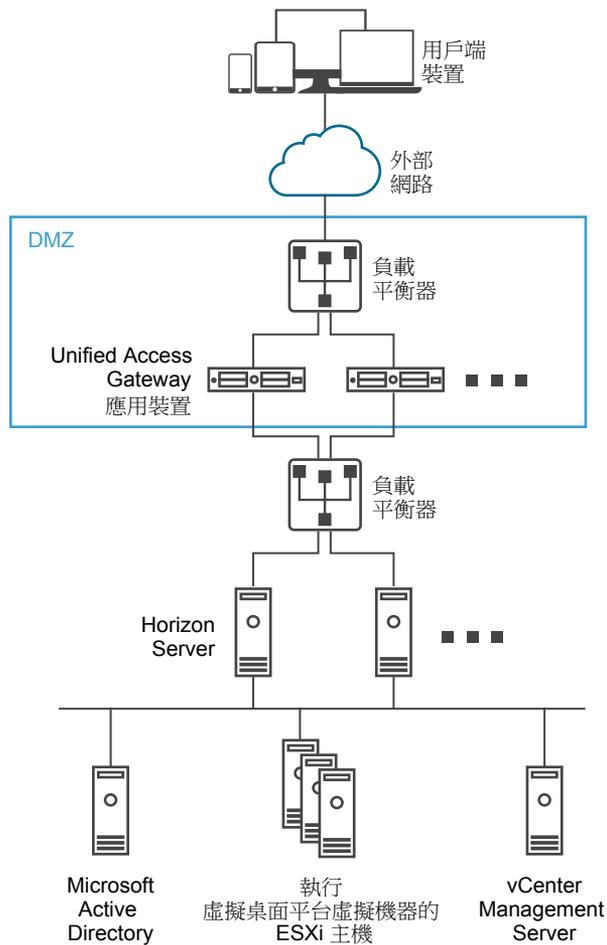
建議使用者使用 Unified Access Gateway 應用裝置 (而非 Horizon 安全伺服器) 來部署 Horizon 7。

備註 當 Proxy 模式中有重疊時，Horizon Connection Server 無法搭配已啟用的 Web Reverse Proxy 正常運作。因此，如果在相同的 Unified Access Gateway 執行個體上使用 Proxy 模式同時設定並啟用了 Horizon 和 Web Reverse Proxy 執行個體，請從 Horizon 設定中移除 Proxy 模式「/」，並保留 Web Reverse Proxy 中的模式以防止重疊。保留 Web Reverse Proxy 執行個體中的「/」Proxy 模式可確保使用者在按一下 Unified Access Gateway 的 URL 時會顯示正確的 Web Reverse Proxy 頁面。如果僅設定了 Horizon 設定，則不需要進行前述變更。

Horizon 安全伺服器和 Unified Access Gateway 應用裝置之間的差異如下所示。

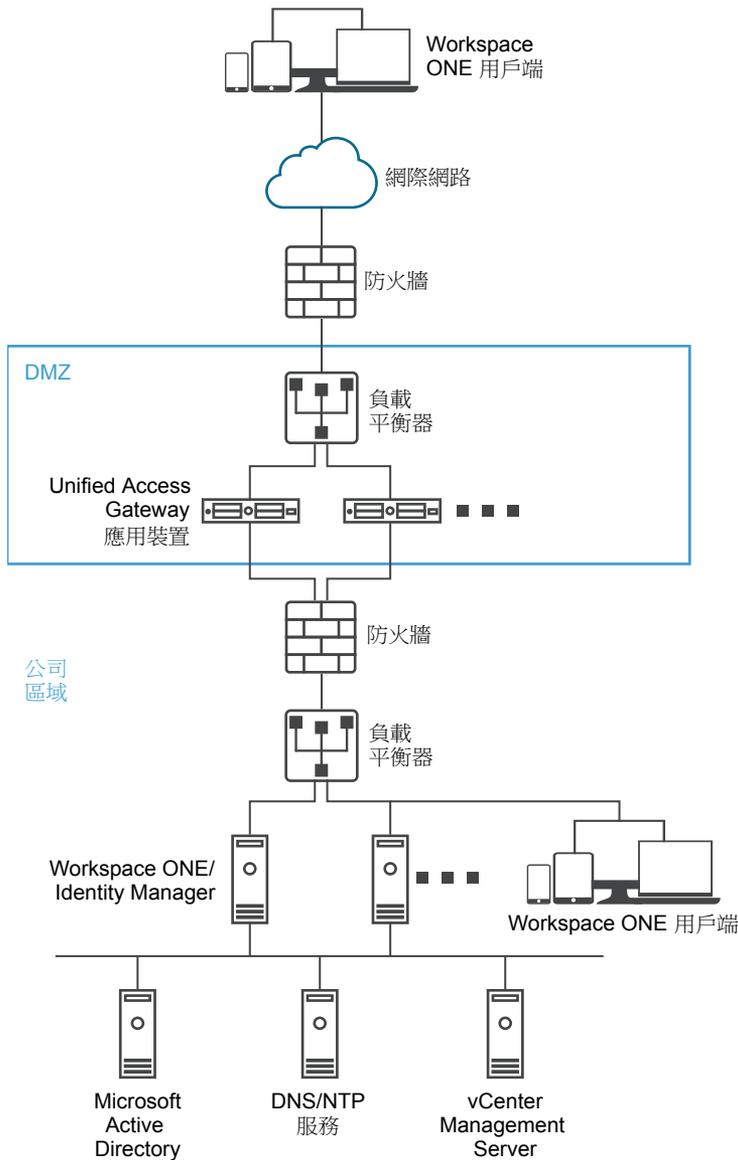
- 安全部署。Unified Access Gateway 可實作為強化、鎖定且預先設定的 Linux 虛擬機器。
- 可擴充。您可以將 Unified Access Gateway 連接到個別的 Horizon 連線伺服器，或透過多部 Horizon 連線伺服器前方的負載平衡器予以連接，藉此改善高可用性。它可作為 Horizon Client 與後端 Horizon 連線伺服器之間的層。由於部署快速，因此它能迅速垂直擴充或垂直縮減，以滿足快速變遷的企業需求。

圖 4-2 指向負載平衡器的 Unified Access Gateway 應用裝置



或者，您也可以讓一或多部 Unified Access Gateway 應用裝置指向個別伺服器執行個體。在這兩種方法中，都請在 DMZ 中的兩部 (含) 以上 Unified Access Gateway 應用裝置前方使用負載平衡器。

圖 4-3 指向 Horizon Server 執行個體的 Unified Access Gateway 應用裝置



驗證

使用者驗證與 Horizon 安全伺服器類似。Unified Access Gateway 支援的使用者驗證方法包括：

- Active Directory 使用者名稱和密碼。
- Kiosk 模式。如需 Kiosk 模式的詳細資料，請參閱 Horizon 說明文件。
- RSA SecurID 雙因素驗證，由 RSA 針對 SecurID 正式認證。
- 透過各種第三方雙因素安全性廠商解決方案的 RADIUS。
- 智慧卡、CAC 或 PIV X.509 使用者憑證。
- SAML。

搭配 Horizon Connection Server 時，以上驗證方法都能獲得支援。Unified Access Gateway 不需要直接與 Active Directory 通訊。這種模式的通訊能作為透過 Horizon Connection Server 的 Proxy，因此能直接存取 Active Directory。在根據驗證原則驗證使用者工作階段後，Unified Access Gateway 就能將權利資訊的要求以及桌面平台和應用程式的啟動要求轉送給 Horizon Connection Server。Unified Access Gateway 還能管理其桌面平台和應用程式通訊協定處理常式，讓它們只轉送授權的通訊協定流量。

Unified Access Gateway 本身會處理智慧卡驗證。內容包括讓 Unified Access Gateway 與線上憑證狀態通訊協定 (Online Certificate Status Protocol, OCSP) 伺服器通訊，以便檢查 X.509 憑證撤銷等選項。

對 Horizon 基礎結構支援 IPv4 和 IPv6 雙重模式

您可以使用 Unified Access Gateway 以作為橋接，供 IPv6 Horizon 用戶端連線至 IPv4 後端的連線伺服器或代理程式環境。

您可以在 twonic 模式中部署 Unified Access Gateway，使前端 NIC 處於混合 IPv4/IPv6 模式，而 Horizon 後端或管理 NIC 處於 IPv4 模式。Horizon 後端環境可能包含連線伺服器、代理程式桌面平台或其他伺服器端基礎結構。

備註 當您在 IPv4/IPv6 模式中設定 Unified Access Gateway 時，請確保 TCP/UDP 的 Blast 外部 URL 設為 443。請參閱[使用 Horizon 與 Horizon Cloud with On-Premises Infrastructure 進行部署與設定 Horizon 設定](#)。

備註 不支援將 Horizon IPv6 至 IPv4 橋接功能用於 PCoIP 或 Blast UDP。

支援下列 Horizon 用戶端和伺服器 IP 模式。

表格 4-1. 支援的 Horizon 設定 (IP 模式)

Horizon Client 模式	Horizon Server 模式	支援
IPv4	IPv4	是
IPv6	IPv4	是
IPv6	IPv6	是
IPv4	IPv6	否

安裝 Horizon 用戶端時，如果您選取**自動選取**或**雙重**，則連線會根據目前的網路透過 IPv4 或 IPv6 進行。

進階 Edge Service 設定

Unified Access Gateway 會使用不同的變數區分 Edge Service、設定的 Web Proxy 以及 Proxy 目的地 URL。

Proxy 模式和未受保護的模式

Unified Access Gateway 會使用 Proxy 模式將傳入 HTTP 要求轉送至正確的 Edge Service，例如 Horizon 或所設定的其中一個 Web Reverse Proxy 執行個體，例如 VMware Identity Manager。因此，它可以用作一個篩選器，以決定處理傳入流量時是否需要 Reverse Proxy。

如果選取了 **Reverse Proxy**，則 **Proxy** 會使用指定的未受保護模式，以決定是否允許傳入流量在不經驗證的情況下進入後端。

使用者必須指定 **Proxy** 模式，而指定未受保護的模式為選用。具有本身的登入機制，且想要讓登入頁面路徑、**Javascript** 或映像資源等特定 **URL** 在不經驗證的情況下傳遞後端的 **Web Reverse Proxy** (例如 **VMware Identity Manager**) 會使用未受保護的模式。

備註 未受保護的模式是 **Proxy** 模式的子集，因此兩者之間針對 **Reverse Proxy** 可能會有部分重複路徑。

每個 **Edge Service** 可以有不同的模式。例如，可以將 **Horizon** 的 **Proxy Pattern** 設定為 (`/|/view-client(.*)|/portal(.*)|/appblast(.*)`)，以及將 **VMware Identity Manager** 的模式設定為 (`/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*)`)。

備註 當 **Proxy** 模式中有重疊時，**Horizon Connection Server** 無法搭配已啟用的 **Web Reverse Proxy** 正常運作。因此，如果在相同的 **Unified Access Gateway** 執行個體上使用 **Proxy** 模式同時設定並啟用了 **Horizon** 和 **Web Reverse Proxy** 執行個體 (例如 **VMware Identity Manager**)，請從 **Horizon** 設定中移除 **Proxy** 模式「/」，並保留 **VMware Identity Manager** 中的模式以防止重疊。

保留 **Web Reverse Proxy** 執行個體 (**VMware Identity Manager**) 中的「/」**Proxy** 模式可確保使用者在按一下 **Unified Access Gateway** 的 **URL** 時會顯示 **VMware Identity Manager** 頁面。

如果僅設定了 **Horizon** 設定，則不需要進行前述變更。

Proxy 主機模式

如果設定了多個 **Web Reverse Proxy** 執行個體，且 **Proxy** 模式中有重疊，則 **Unified Access Gateway** 會使用 **Proxy Host Pattern** 來加以區分。將 **Proxy Host Pattern** 設定為 **Reverse Proxy** 的 **FQDN**。

例如，可以將 **SharePoint** 的主機模式設定為 *sharepoint.myco.com*，以及將 **JIRA** 的模式設定為 *jira.myco.com*。

主機項目

僅在 **Unified Access Gateway** 無法連線後端伺服器或應用程式時才設定此文字方塊。當您將後端應用程式的 **IP** 位址和主機名稱新增至「主機項目」時，系統會將該資訊新增至 **Unified Access Gateway** 的 `/etc/hosts` 檔案。此欄位為所有 **Edge Service** 設定的通用欄位。

Proxy 目的地 URL

這是 **Unified Access Gateway** 為 **Proxy** 之 **Edge Service** 設定的後端伺服器應用程式 **URL**。例如：

- 針對 **Horizon Connection Server**，連線伺服器 **URL** 為 **Proxy** 目的地 **URL**。
- 針對 **Web Reverse Proxy**，所設定 **Web Reverse Proxy** 的應用程式 **URL** 為 **Proxy** 目的地 **URL**。

單一 Reverse Proxy 組態

當 **Unified Access Gateway** 接收到具有 **URI** 的單一傳入要求時，系統會使用 **Proxy** 模式來決定是要轉送要求或將其捨棄。

多個 Reverse Proxy 組態

- 1 將 Unified Access Gateway 設定為 Reverse Proxy，並且具有 URI 路徑的傳入要求到達時，Unified Access Gateway 會使用 Proxy 模式來比對正確的 Web Reverse Proxy 執行個體。如果有相符項目，則會使用相符的模式。如果有多個相符項目，則會在步驟 2 中重複進行篩選和比對程序。如果沒有相符項目，則會捨棄要求，並將 HTTP 404 傳送回用戶端。
- 2 Proxy 主機模式用來篩選已在步驟 1 中篩選的清單。HOST 標頭則用來篩選要求，以及尋找 Reverse Proxy 執行個體。如果有相符項目，則會使用相符的模式。如果有多個相符項目，則會在步驟 3 中重複進行篩選和比對程序。
- 3 請注意下列事項：
 - 系統會使用步驟 2 中已篩選清單的第一個相符項目。此相符項目可能不會永遠是正確的 Web Reverse Proxy 執行個體。因此，如果 Unified Access Gateway 中有多個 Reverse Proxy 設定，請確保 Web Reverse Proxy 執行個體的 Proxy 模式和 Proxy 主機模式的組合是唯一的。
 - 所有已設定 Reverse Proxy 的主機名稱應解析為與 Unified Access Gateway 執行個體之外部位址相同的 IP 位址。

如需設定 Reverse Proxy 的詳細資訊和相關指示，請參閱[使用 VMware Identity Manager 設定 Reverse Proxy](#)。

範例：兩個已設定的 Reverse Proxy，具有衝突 Proxy 模式、不同主機模式

假設第一個 Reverse Proxy 的 Proxy 模式為 `/(.*)` 且主機模式為 `host1.domain.com`，而第二個 Reverse Proxy 的模式為 `(/app2(.*)|/app3(.*)|/)` 且主機模式為 `host2.domain.com`。

- 如果提出將路徑設定為 `https://host1.domain.com/app1/index.html` 的要求，則要求會轉送至第一個 Reverse Proxy。
- 如果提出將路徑設定為 `https://host2.domain.com/app2/index.html` 的要求，則要求會轉送至第二個 Reverse Proxy。

範例：兩個 Reverse Proxy，具有互斥 Proxy 模式

假設第一個 Reverse Proxy 的 Proxy 模式為 `/app1(.*)`，而第二個 Reverse Proxy 的 Proxy 模式為 `(/app2(.*)|/app3(.*)|/)`。

- 如果提出將路徑設定為 `https://<uag domain name>/app1/index.html` 的要求，則要求會轉送至第一個 Reverse Proxy。
- 如果提出將路徑設定為 `https://<uag domain name>/app3/index.html` 或 `https://<uag domain name>/` 的要求，則要求會轉送至第二個 Reverse Proxy。

設定 Horizon 設定

您可以使用 Unified Access Gateway 和 Horizon Cloud with On-Premises Infrastructure 雲端基礎結構來部署 Horizon Air。對於 Horizon 部署，Unified Access Gateway 應用裝置會取代 Horizon 安全伺服器。

先決條件

如果您想要同時擁有 Horizon 和 Web Reverse Proxy 執行個體 (例如, 在相同的 Unified Access Gateway 執行個體上設定並啟用的 VMware Identity Manager), 請參閱[進階 Edge Service 設定](#)。

程序

- 1 在管理員 UI 的**手動設定**區段中, 按一下**選取**。
- 2 在**一般設定 > Edge Service 設定**中, 按一下**顯示**。
- 3 按一下 **Horizon 設定**齒輪圖示。
- 4 在 [Horizon 設定] 頁面中, 將 [否] 變更為**是**以啟用 Horizon。
- 5 為 Horizon 設定下列 Edge Service 設定資源:

選項	說明
識別碼	依預設會設定為 Horizon。Unified Access Gateway 可與使用 Horizon XML 通訊協定的伺服器進行通訊, 例如 Horizon 連線伺服器、Horizon Air 和 Horizon Cloud with On-Premises Infrastructure。
連線伺服器 URL	輸入 Horizon server 或負載平衡器的位址。輸入格式為 <code>https://00.00.00.00</code> 。
連線伺服器 URL 指紋	輸入 Horizon server 指紋的清單。 如果未提供指紋的清單, 請確保伺服器憑證是由信任的 CA 核發。輸入十六進位的指紋數字。例如, sha1= C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3。
啟用 PCoIP	將 [否] 變更為 是 可指定是否啟用 PCoIP 安全閘道。
PCoIP 外部 URL	Horizon 用戶端用來對此 Unified Access Gateway 應用裝置建立 Horizon PCoIP 工作階段的 URL。它必須包含 IPv4 位址, 且不是主機名稱。例如, <code>10.1.2.3:4172</code> 。預設值為 Unified Access Gateway IP 位址和連接埠 4172。
啟用 Blast	若要使用 Blast 安全閘道, 請將 [否] 變更為 是 。
連線伺服器 IP 模式	從下拉式功能表中選取 IPv4、IPv6 或 IPv4+IPv6。預設值為 IPv4。

6 若要設定驗證方法規則和其他進階設定，請按一下較多。

選項	說明
驗證方法	<p>選取要使用的驗證方法。</p> <p>預設會使用使用者名稱和密碼的傳遞驗證。您在 Unified Access Gateway 中設定的驗證方法會在下拉式功能表中列出。目前支援 RSA SecurID 和 RADIUS 驗證方法。</p> <p>若要設定包括在第一個驗證嘗試失敗時套用第二個驗證方法的驗證。</p> <ol style="list-style-type: none"> 從第一個下拉式功能表選取一個驗證方法。 按一下 + 並選取 AND 或 OR。 從第三個下拉式功能表選取第二個驗證方法。 <p>若要要求使用者透過兩個驗證方法進行驗證，請在下拉式功能表中將 OR 變更為 AND。</p> <p>備註</p> <ul style="list-style-type: none"> 使用 PowerShell 部署時，針對 RSA SecurID 驗證，請將此選項設定為使用 securid-auth AND sp-auth 來顯示密碼畫面。 使用 vSphere 部署時，針對 RSA SecurID 驗證，請將此選項設定為使用 securid-auth 來顯示密碼畫面。 將以下文字行加入 INI 檔案的 Horizon 區段。 <pre>authMethods=securid-auth && sp-auth matchWindowsUserName=true</pre> <p>在 INI 檔案的底部新增區段。</p> <pre>[SecurIDAuth] serverConfigFile=C:\temp\sdconf.rec externalHostName=192.168.0.90 internalHostName=192.168.0.90</pre> <p>兩個 IP 位址皆應設定為 Unified Access Gateway 的 IP 位址。sdconf.rec 檔案是從 RSA 驗證管理員取得的，該檔案的設定必須完整。請確認您使用的是 Access Point 2.5 或更新版本 (或 Unified Access Gateway 3.0 或更新版本)，而且可以從 Unified Access Gateway 並透過網路存取 RSA 驗證管理員伺服器。重新執行 uagdeploy PowerShell 命令，以重新部署針對 RSA SecurID 設定的 Unified Access Gateway。</p>
健全狀況檢查 URI 路徑	Unified Access Gateway 為了進行健全狀況狀態監控而連線之連線伺服器的 URI 路徑。
Blast 外部 URL	<p>Horizon 用戶端用來對此 Unified Access Gateway 應用裝置建立 Horizon Blast 或 BEAT 工作階段的 URL。例如，https://uag1.myco.com 或 https://uag1.myco.com:443。</p> <p>如果未指定 TCP 連接埠號碼，則預設 TCP 連接埠為 8443。如果未指定 UDP 連接埠號碼，則預設 UDP 連接埠也是 8443。</p>
啟用通道	如果使用了 Horizon 安全通道，請將 [否] 變更為是。用戶端會使用此外部 URL 透過 Horizon 安全閘道進行通道連線。此通道用於 RDP、USB 和多媒體重新導向 (MMR) 流量。
通道外部 URL	<p>Horizon 用戶端用來對此 Unified Access Gateway 應用裝置建立 Horizon 通道工作階段的 URL。例如，https://uag1.myco.com 或 https://uag1.myco.com:443。</p> <p>如果未指定 TCP 連接埠號碼，則預設 TCP 連接埠為 443。</p>

選項	說明
端點符合性檢查提供者	選取端點符合性檢查提供者。預設值為 OPSWAT。
Proxy 模式	輸入將相關 URI 與 Horizon Server URL (proxyDestinationUrl) 比對的規則運算式。其預設值為 (/ /view-client(.*) /portal(.*) /appblast(.*))。
SAML SP	輸入 Horizon XMLAPI 代理之 SAML 服務提供者的名稱。此名稱必須符合所設定服務提供者中繼資料的名稱，或為特殊值 DEMO。
符合 Windows 使用者名稱	將 [否] 變更為是 以符合 RSA SecurID 與 Windows 使用者名稱。如果設為 [是]，則 securID-auth 會設定為 true，並且會強制 securID 與 Windows 使用者名稱相符。
閘道位置	從中起始連線要求的位置。安全伺服器 和 Unified Access Gateway 會設定閘道位置。位置可以是外部或內部的。
受信任的憑證	將受信任的憑證新增到此 Edge Service。按一下「+」來選取 PEM 格式的憑證，然後新增至信任存放區。按一下「-」可從信任存放區移除憑證。依預設，別名名稱是 PEM 憑證的檔案名稱。編輯別名文字方塊以提供不同的名稱。
回應安全性標頭	<p>按一下「+」可新增標頭。輸入安全性標頭的名稱。輸入值。按一下「-」可移除標頭。編輯現有的安全性標頭，以更新標頭的名稱和值。</p> <p>重要事項 在您按一下儲存後，才會儲存標頭名稱和值。依預設會顯示部分標準安全性標頭。僅在已設定後端伺服器的回應中沒有對應的標頭存在時，才會將已設定標頭新增至用戶端的 Unified Access Gateway 回應。</p> <p>備註 請謹慎修改安全性回應標頭。修改這些參數可能會影響到 Unified Access Gateway 的安全運作。</p>
主機項目	<p>輸入要在 /etc/hosts 檔案中新增加的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias。按一下「+」符號可新增多個主機項目。</p> <p>重要事項 只有在按一下儲存後，才會儲存主機項目。</p>
停用 HTML Access	如果設定為 [是]，則會停用 Horizon 的 Web 存取。如需詳細資料，請參閱 Horizon 的端點符合性檢查 。

7 按一下**儲存**。

Blast TCP 和 UDP 外部 URL 組態選項

Blast 安全閘道包含 Blast Extreme Adaptive Transport (BEAT) 網路功能，它會根據網路情況 (例如不同的速度和封包遺失) 進行動態調整。在 Unified Access Gateway 中，您可以設定 BEAT 通訊協定所使用的連接埠。

Blast 會使用標準連接埠 TCP 8443 和 UDP 8443。UDP 443 也可以用來透過 UDP 通道伺服器存取桌面平台。連接埠組態是透過 Blast 外部 URL 內容而設定。

表格 4-2. BEAT 連接埠選項

Blast 外部 URL	用戶端使用的 TCP 連接埠	用戶端使用的 UDP 連接埠	說明
https://ap1.myco.com	8443	8443	此為預設表單，且需要在防火牆開啟 TCP 8443 以及選用的 UDP 8443，才能允許從網際網路到 Unified Access Gateway 的連線
https://ap1.myco.com:443	443	8443	需要開啟 TCP 443 或 UDP 8443 時，請使用此表單。
https://ap1.myco.com:xxxx	xxxx	8443	
https://ap1.myco.com:xxx x/?UDPPort=yyyy	xxxx	yyyy	

若要設定預設值以外的連接埠，部署時必須為相關的通訊協定新增內部 IP 轉送規則。轉送規則可以在部署時的 OVF 範本中指定，或透過利用 PowerShell 命令輸入的 INI 檔案指定。

Horizon 的端點符合性檢查

除了 Unified Access Gateway 所提供的使用者驗證服務以外，端點符合性檢查上的 Unified Access Gateway 功能還可以為存取 Horizon 桌面平台提供額外一層的安全保護。

您可以使用端點符合性檢查功能來確保符合各種原則，例如端點上的防毒原則或加密原則。

端點符合性原則定義於雲端或內部部署中執行的服務上。

如果已啟用端點符合性檢查，則 Unified Access Gateway 僅允許符合規範的 VDI 桌面平台啟動，並封鎖所有不符合規範的端點使其無法啟動。

先決條件

- 1 註冊 OPSWAT 帳戶並在 OPSWAT 站台上登錄您的應用程式。請參閱 <https://go.opswat.com/communityRegistration>。
- 2 請記下用戶端金鑰和用戶端秘密金鑰。您需要這些金鑰才能在 Unified Access Gateway 中設定 OPSWAT。
- 3 登入 OPSWAT 站台並設定您端點的符合性原則。請參閱相關的 OPSWAT 說明文件。
- 4 在 OPSWAT 首頁上，按一下 **連線 Metadefender Endpoint Management** 並將代理程式軟體下載並安裝至用戶端裝置。

程序

- 1 登入管理員 UI 並移至 **進階設定 > 端點符合性檢查提供者設定**。
- 2 按一下 **新增**，新增用戶端金鑰和用戶端密碼金鑰詳細資料。
已填入 **端點符合性檢查提供者** 和 **主機名稱** 欄位。請勿變更這些值。
- 3 從管理員 UI 中，導覽至 Horizon 設定，找到 **端點符合性檢查提供者** 欄位，並從下拉式功能表中選取 OPSWAT。
- 4 按一下 **儲存**。

5 使用端點符合性檢查提供者用戶端連線至遠端桌面平台。

會列出已設定的 Horizon View 桌面平台，且當您啟動桌面平台時，系統會驗證用戶端裝置是否合規。

部署為 Reverse Proxy

Unified Access Gateway 可用作 Web Reverse Proxy，並且可以在 DMZ 中作為單純的 Reverse Proxy 或驗證 Reverse Proxy。

部署案例

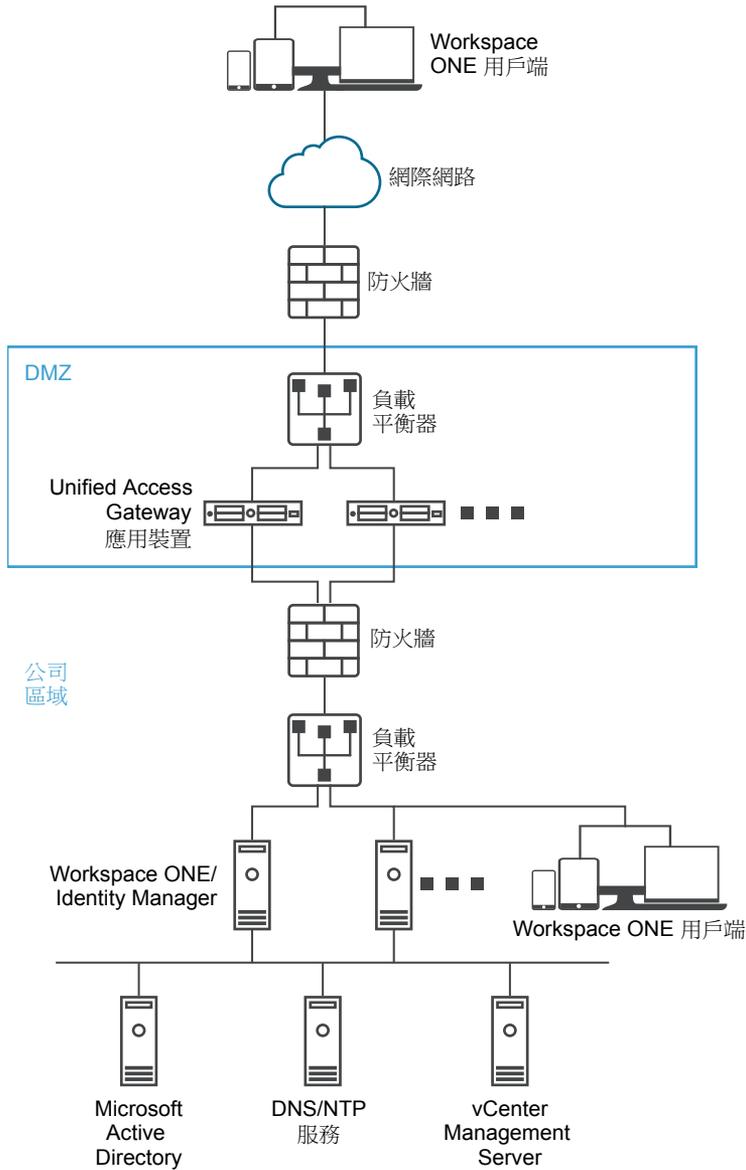
Unified Access Gateway 可讓您從遠端安全地存取內部部署的 VMware Identity Manager。

Unified Access Gateway 應用裝置通常部署在網路的非軍事區 (DMZ)。利用 VMware Identity Manager，Unified Access Gateway 應用裝置可作為使用者的瀏覽器與資料中心的 VMware Identity Manager 服務之間的 Web Reverse Proxy。Unified Access Gateway 也允許從遠端存取 Workspace ONE 目錄來啟動 Horizon 應用程式。

備註 Unified Access Gateway 的單一執行個體可以同時處理最多 15000 個 TCP 連線。如果預期的負載超過 15000 個，則必須在負載平衡器後方設定 Unified Access Gateway 的多個執行個體。

如需設定 Reverse Proxy 時所用設定的相關資訊，請參閱進階 [Edge Service](#) 設定。

圖 4-4 指向 VMware Identity Manager 的 Unified Access Gateway 應用裝置



瞭解 Reverse Proxy

Unified Access Gateway 提供遠端使用者對應用程式入口網站的存取，以進行單一登入並存取其資源。應用程式入口網站是一種 Unified Access Gateway 作為 Reverse Proxy 的 SharePoint、JIRA 或 VIDM 之類的後端應用程式。

備註 當 Proxy 模式中有重疊時，Horizon Connection Server 無法搭配已啟用的 Web Reverse Proxy 正常運作。因此，如果在相同的 Unified Access Gateway 執行個體上使用 Proxy 模式同時設定並啟用了 Horizon 和 Web Reverse Proxy 執行個體，請從 Horizon 設定中移除 Proxy 模式「/」，並保留 Web Reverse Proxy 中的模式以防止重疊。保留 Web Reverse Proxy 執行個體中的「/」Proxy 模式可確保使用者在按一下 Unified Access Gateway 的 URL 時會顯示正確的 Web Reverse Proxy 頁面。如果僅設定了 Horizon 設定，則不需要進行前述變更。

啟用和設定 Reverse Proxy 時，請注意下列幾點：

- 您必須在 Edge Service 管理員上啟用 Reverse Proxy 的驗證。目前支援 RSA SecurID 和 RADIUS 驗證方法。
- 在 Web Reverse Proxy 上啟用驗證之前，您必須先產生身分識別提供者中繼資料 (IDP 中繼資料)。
- Unified Access Gateway 能在搭配或未搭配瀏覽器型用戶端驗證的情況下提供 VMware Identity Manager 和 Web 應用程式的遠端存取權，進而啟動 Horizon 桌面平台。
- 您可以設定多個 Reverse Proxy 執行個體，且可刪除每個已設定的執行個體。

圖 4-5 已設定多個 Reverse Proxy



使用 VMware Identity Manager 設定 Reverse Proxy

您可以設定 Web Reverse Proxy 服務以搭配使用 Unified Access Gateway 和 VMware Identity Manager。

先決條件

請注意，使用 VMware Identity Manager 部署具有下列需求：

- 分割 DNS。主機名稱在外部應該會解析為 Unified Access Gateway 的 IP 位址。在內部的 Unified Access Gateway 上，相同的主機名稱應該會透過內部 DNS 對應或 Unified Access Gateway 上的主機名稱項目以解析為實際的 Web 伺服器。

備註 如果您僅使用 Web Reverse Proxy 部署，則不需要設定身分識別橋接。

- VMware Identity Manager 服務必須以完整網域名稱 (FQDN) 作為主機名稱。
- Unified Access Gateway 必須使用內部 DNS。這表示 Proxy 目的地 URL 必須使用 FQDN。
- 如果 Unified Access Gateway 執行個體中有多個 Reverse Proxy 設定，則 Web Reverse Proxy 執行個體的 Proxy 模式和 Proxy 主機模式的組合必須是唯一的。
- 所有已設定 Reverse Proxy 的主機名稱應解析為 Unified Access Gateway 執行個體之 IP 位址相同的 IP 位址。
- 如需進階 Edge Service 設定的相關資訊，請參閱進階 [Edge Service 設定](#)。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在**一般設定 > Edge Service 設定**中，按一下**顯示**。
- 3 按一下 **Reverse Proxy 設定** 齒輪圖示。
- 4 在 [Reverse Proxy 設定] 頁面中，按一下**新增**。
- 5 在 [啟用 Reverse Proxy 設定] 區段，將**否**變更為**是**以啟用 Reverse Proxy。
- 6 設定下列 Edge Service 設定。

選項	說明
識別碼	Edge Service 識別碼會設定為 Web Reverse Proxy。
執行個體 ID	用來從所有其他 Web Reverse Proxy 執行個體中識別和區分某個 Web Reverse Proxy 執行個體的唯一名稱。
Proxy 目的地 URL	輸入 Web 應用程式的位址，這通常是後端 URL。例如，對於 VMware Identity Manager，在用戶端電腦上新增 IP 位址、VMware Identity Manager 主機名稱和外部 DNS。在管理員 UI 中，新增 IP 位址、VMware Identity Manager 主機名稱和內部 DNS。

選項	說明
Proxy 目的地 URL 指紋	<p>針對 proxyDestination URL，輸入可接受 SSL 伺服器憑證指紋的清單。如果您指定 *，則系統會接受任何憑證。指紋的格式為 <code>[alg]=xx:xx</code>，其中 <code>alg</code> 可以是預設值 <code>sha1</code> 或 <code>md5</code>。xx 為十六進位數字。「:」分隔符號可以是空格，或不使用。系統會忽略指紋中的大小寫。例如：</p> <pre>sha1=B6 77 DC 9C 19 94 2E F1 78 F0 AD 4B EC 85 D1 7A F8 8B DC 34 sha256=ad:5c:f1:48:47:94:7e:80:82:73:13:6c:83:52:be:78:ed:ff:50:23:56:a8:42:8a:d9:30:fc:3a:33:d6:c6:db</pre> <p>如果未設定指紋，則必須由受信任的 CA 核發伺服器憑證。</p>
Proxy 模式	<p>輸入轉送至目的地 URL 的相符 URI 路徑。例如，您可以輸入 <code>(/ /SAAS(.*) /hc(.*) /web(.*) /catalog-portal(.*)</code>。</p> <p>備註 當您設定多個 Reverse Proxy 時，請在 Proxy 主機模式中提供主機名稱。</p>

7 若要設定其他進階設定，請按一下較多。

選項	說明
驗證方法	<p>預設會使用使用者名稱和密碼的傳遞驗證。您在 Unified Access Gateway 中設定的驗證方法會在下拉式功能表中列出。支援 RSA SecurID、RADIUS，以及裝置憑證驗證方法。</p>
健全狀況檢查 URI 路徑	<p>Unified Access Gateway 會連線至此 URI 路徑，以檢查您 Web 應用程式的健全狀況。</p>
SAML SP	<p>當您將 Unified Access Gateway 設定為 VMware Identity Manager 的已驗證 Reverse Proxy 時需要使用此選項。輸入 View XML API 代理之 SAML 服務提供者的名稱。此名稱必須符合使用 Unified Access Gateway 設定之服務提供者的名稱，或為特殊值 DEMO。如果使用 Unified Access Gateway 設定多個服務提供者，則其名稱必須是唯一的。</p>
外部 URL	<p>預設值為 Unified Access Gateway 主機 URL，連接埠 443。您可以輸入其他外部 URL。輸入為 <code>https://<host:port></code>。</p>

選項	說明
未受保護的模式	輸入已知的 VMware Identity Manager 重新導向模式。例如： <code>(/ /catalog-portal(.*) / /SAAS/ /SAAS/ /SAAS/API/1.0/GET/image(.*) /SAAS/horizon/css(.*) /SAAS/horizon/angular(.*) /SAAS/horizon/js(.*) /SAAS/horizon/js-lib(.*) /SAAS/auth/login(.*) /SAAS/jersey/manager/api/branding /SAAS/horizon/images/(.*) /SAAS/jersey/manager/api/images/(.*) /hc/(.*)/authenticate/(.*) /hc/static/(.*) /SAAS/auth/saml/response /SAAS/auth/authenticatedUserDispatcher /web(.*) /SAAS/apps/ /SAAS/horizon/portal/(.*) /SAAS/horizon/fonts(.*) /SAAS/API/1.0/POST/sso(.*) /SAAS/API/1.0/REST/system/info(.*) /SAAS/API/1.0/REST/auth/cert(.*) /SAAS/API/1.0/REST/oauth2/activate(.*) /SAAS/API/1.0/GET/user/devices/register(.*) /SAAS/API/1.0/oauth2/token(.*) /SAAS/API/1.0/REST/oauth2/session(.*) /SAAS/API/1.0/REST/user/resources(.*) /hc/t/(.*)/(.*)/authenticate(.*) /SAAS/API/1.0/REST/auth/logout(.*) /SAAS/auth/saml/response(.*) /SAAS/(.*)/(.*)auth/login(.*) /SAAS/API/1.0/GET/apps/launch(.*) /SAAS/API/1.0/REST/user/applications(.*) /SAAS/auth/federation/sso(.*) /SAAS/auth/oauth2/authorize(.*) /hc/prepareSaml/failure(.*) /SAAS/auth/oauthtoken(.*) /SAAS/API/1.0/GET/metadata/idp.xml /SAAS/auth/saml/artifact/resolve(.*) /hc/(.*)/authAdapter(.*) /hc/authenticate/(.*) /SAAS/auth/logout /SAAS/common.js /SAAS/auth/launchInput(.*) /SAAS/launchUsersApplication.do(.*) /hc/API/1.0/REST/thinapp/download(.*) /hc/t/(.*)/(.*)/logout(.*) /SAAS/auth/wsfed/services(.*) /SAAS/auth/wsfed/active/logon(.*)</code>)
驗證 Cookie	輸入驗證 Cookie 名稱。例如： HZN
登入重新導向 URL	如果使用者從入口網站登出，請輸入重新導向 URL 以重新登入。例如： /SAAS/auth/login?dest=%s
Proxy 主機模式	外部主機名稱，用來檢查傳入主機以查看它是否符合該特定執行個體的模式。設定 Web Reverse Proxy 執行個體時，主機模式為選用。
受信任的憑證	將受信任的憑證新增到此 Edge Service。按一下「+」來選取 PEM 格式的憑證，然後新增至信任存放區。按一下「-」可從信任存放區移除憑證。依預設，別名名稱是 PEM 憑證的檔案名稱。編輯別名文字方塊以提供不同的名稱。

選項	說明
回應安全性標頭	<p>按一下「+」可新增標頭。輸入安全性標頭的名稱。輸入值。按一下「-」可移除標頭。編輯現有的安全性標頭，以更新標頭的名稱和值。</p> <p>重要事項 在您按一下儲存後，才會儲存標頭名稱和值。依預設會顯示部分標準安全性標頭。僅在已設定後端伺服器的回應中沒有對應的標頭存在時，才會將已設定標頭新增至用戶端的 Unified Access Gateway 回應。</p> <p>備註 請謹慎修改安全性回應標頭。修改這些參數可能會影響到 Unified Access Gateway 的安全運作。</p>
主機項目	<p>輸入要在 <code>/etc/hosts</code> 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如， 10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias。按一下「+」符號可新增多個主機項目。</p> <p>重要事項 只有在按一下儲存後，才會儲存主機項目。</p> <p>備註 僅在使用 VMware Identity Manager 時才適用 UnSecure Pattern、Auth Cookie 和 Login Redirect URL 選項。此處提供的值也適用於 Access Point 2.8 和 Unified Access Gateway 2.9。</p> <p>備註 「驗證 Cookie」和「未受保護的模式」內容對驗證 Reverse Proxy 而言無效。您必須使用 Auth Methods 內容來定義驗證方法。</p>

8 按一下**儲存**。

下一個

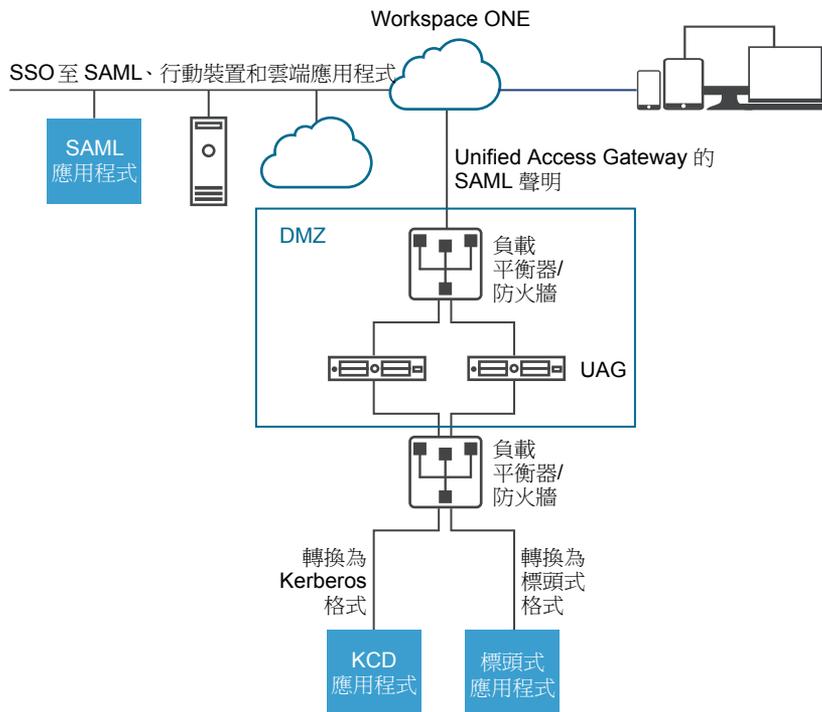
若要啟用身分識別橋接，請參閱[設定身分識別橋接設定](#)。

單一登入存取內部部署舊版 Web 應用程式的部署

可以設定 **Unified Access Gateway** 身分識別橋接功能，以便為使用 Kerberos 限制委派 (KCD) 或標頭式驗證的舊版 Web 應用程式提供單一登入 (SSO)。

身分識別橋接模式中的 **Unified Access Gateway** 會作為將使用者驗證傳遞至所設定舊版應用程式的服務提供者。VMware Identity Manager 則作為身分識別提供者，並提供進入 SAML 應用程式的 SSO。當使用者存取需要 KCD 或標頭式驗證的舊版應用程式時，Identity Manager 會驗證使用者。具有使用者資訊的 SAML 聲明會傳送至 **Unified Access Gateway**。**Unified Access Gateway** 會使用此驗證以允許使用者存取應用程式。

圖 4-6 Unified Access Gateway 身分識別橋接模式



身分識別橋接部署案例

可以設定 Unified Access Gateway 身分識別橋接模式以在雲端或內部部署環境中與 VMware Workspace[®] ONE[®] 搭配使用。

在雲端中使用 Unified Access Gateway 身分識別橋接搭配 Workspace ONE 用戶端

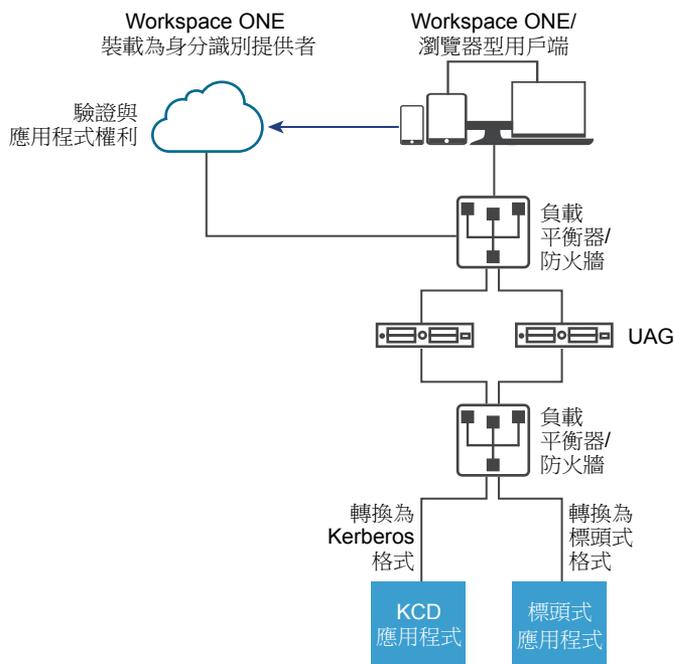
可以設定身分識別橋接模式，以在雲端中與 Workspace ONE 搭配使用來驗證使用者。當使用者要求存取舊版 Web 應用程式時，身分識別提供者會套用適當的驗證和授權原則。

如果使用者通過驗證，則身分識別提供者會建立 SAML Token，並將它傳送給使用者。使用者會將 SAML Token 傳遞至 DMZ 中的 Unified Access Gateway。Unified Access Gateway 會驗證 SAML Token，並從 Token 擷取使用者主體名稱。

如果要求是針對 Kerberos 驗證，則會使用 Kerberos 限制委派來與 Active Directory 伺服器交涉。Unified Access Gateway 會模擬使用者來擷取 Kerberos Token 以使用應用程式進行驗證。

如果要求是針對標頭式驗證，則會將使用者標頭名稱傳送至網頁伺服器以要求使用應用程式進行驗證。應用程式會將回應傳送回 Unified Access Gateway。回應會傳回給使用者。

圖 4-7 雲端中的 Unified Access Gateway 身分識別橋接搭配 Workspace ONE



在內部部署使用身分識別橋接搭配 Workspace ONE 用戶端

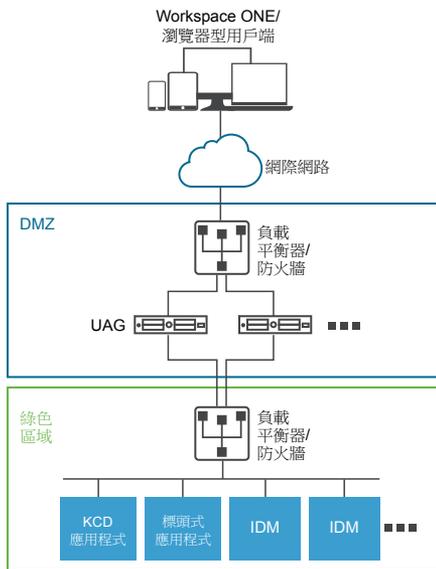
將身分識別橋接模式設定為在內部部署環境中使用 Workspace ONE 驗證使用者時，使用者會輸入用來透過 Unified Access Gateway Proxy 存取內部部署舊版 Web 應用程式的 URL。Unified Access Gateway 會將要求重新導向至身分識別提供者以進行驗證。身分識別提供者會對要求套用驗證和授權原則。如果使用者通過驗證，則身分識別提供者會建立 SAML Token，並將 Token 傳送給使用者。

使用者會將 SAML Token 傳遞至 Unified Access Gateway。Unified Access Gateway 會驗證 SAML Token，並從 Token 擷取使用者主體名稱。

如果要求是針對 Kerberos 驗證，則會使用 Kerberos 限制委派來與 Active Directory 伺服器交涉。Unified Access Gateway 會模擬使用者來擷取 Kerberos Token 以使用應用程式進行驗證。

如果要求是針對標頭式驗證，則會將使用者標頭名稱傳送至網頁伺服器以要求使用應用程式進行驗證。應用程式會將回應傳送回 Unified Access Gateway。回應會傳回給使用者。

圖 4-8 Unified Access Gateway 身分識別橋接內部部署



搭配使用身分識別橋接與對 Kerberos 的憑證

您可以設定身分識別橋接，以便為使用憑證驗證的內部部署舊版非 SAML 應用程式提供單一登入 (SSO)。請參閱[針對身分識別橋接設定 Web Reverse Proxy \(對 Kerberos 的憑證\)](#)。

設定身分識別橋接設定

在後端應用程式中設定了 Kerberos 時，若要在 Unified Access Gateway 中設定身分識別橋接，您需要上傳身分識別提供者中繼資料和 Keytab 檔案，並設定 KCD 領域設定。

備註 此版本的身分識別橋接可用單一網域設定支援跨網域。這表示使用者和 SPN 帳戶可以位於不同的網域。

當身分識別橋接啟用了標頭式驗證時，則不需要 Keytab 設定和 KCD 領域設定。

設定身分識別橋接設定使用 Kerberos 驗證之前，請確定下列項目可供使用。

- 已設定身分識別提供者，且已儲存身分識別提供者的 SAML 中繼資料。SAML 中繼資料檔案會上傳至 Unified Access Gateway (僅適用於 SAML 案例)。
- 針對 Kerberos 驗證，一部已啟用 Kerberos 的伺服器，且包含用於識別所使用金鑰發佈中心的領域名稱。
- 針對 Kerberos 驗證，將 Kerberos Keytab 檔案上傳至 Unified Access Gateway。Keytab 檔案包括 Active Directory 服務帳戶的認證，該帳戶已設定來代表網域中的任何使用者針對指定的後端服務來取得 Kerberos 票證。
- 確保已開啟下列連接埠：
 - 用於傳入 HTTP 要求的連接埠 443

- 用於與 Active Directory 進行 Kerberos 通訊的 TCP/UDP 連接埠 88
- Unified Access Gateway 使用 TCP 來與後端應用程式通訊。後端接聽所在的適當連接埠，例如 TCP 連接埠 8080。

備註

- 不支援為相同 Unified Access Gateway 執行個體上兩個不同 Reverse Proxy 執行個體同時進行身分識別橋接的 SAML 和對 Kerberos 的憑證設定。
- 不支援在相同應用裝置上未啟用身分識別橋接，且具有憑證授權機構但無憑證式驗證的 Web Reverse Proxy 執行個體。

使用 SAML 的標頭式驗證

從 IDP 到 SP (如果使用身分識別橋接，則為 Unified Access Gateway) 的 SAML 回應包含具有 SAML 屬性的 SAML 判斷提示。SAML 屬性可在 IDP 中設定為指向不同的參數，例如使用者名稱和電子郵件等。

在使用 SAML 的標頭式驗證中，SAML 屬性的值可作為 HTTP 標頭傳送至後端代理目的地。定義於 Unified Access Gateway 中的 SAML 屬性名稱與 IDP 中的名稱相同。例如，如果身分識別提供者將此屬性定義為 Name: userName Value: idmadmin，則 Unified Access Gateway 中的 SAML 屬性名稱必須定義為 "userName"。

系統會忽略與 IDP 中所定義屬性不相符的 SAML 屬性。Unified Access Gateway 支援多個 SAML 屬性和多重值的 SAML 屬性。以下將針對各個案例，提供身分識別提供者預期會傳回的 SAML 判斷提示範例節錄。例如，

1. 預期 IDP 針對多個 SAML 屬性傳回的 SAML 回應

```
<saml:AttributeStatement>
  <saml:Attribute Name="userName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xsd:string">idmadmin</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="userEmail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">63ecfabf-a577-46c3-b4fa-
  caf7ae49a6a3</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

在上述範例中，判斷提示包含兩個屬性，即 "userName" 和 "userEmail"。如果僅為 "userName" 設定了標頭式驗證，且標頭名稱為 "HTTP_USER_NAME"，則傳送的標頭為 "HTTP_USER_NAME: idmadmin"。由於未在 Unified Access Gateway 上設定用於標頭式驗證的 "userEmail"，因此不會將其作為標頭傳送。

2. 預期 IDP 針對多重值 SAML 屬性傳回的 SAML 回應

```
<saml:AttributeStatement>
  <saml:Attribute Name="group" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All
```

```

Employees</saml:AttributeValue>
  <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All
Contractors</saml:AttributeValue>
  <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All
Executives</saml:AttributeValue>
  <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>

```

在上述範例中，屬性 "group" 包含四個值，即 "All Employees"、"All Contractors"、"All Executives" 和 "All"。如果僅為 "group" 設定了標頭式驗證，且標頭名稱為 "HTTP_GROUP"，則傳送的標頭為 "HTTP_GROUP: All Employees, All Contractors, All Executives, All"，並以所有屬性值的逗號分隔清單作為標頭值。

設定領域設定

設定網域領域名稱、領域的金鑰發佈中心和 KDC 逾時。

領域是負責維護驗證資料的管理實體的名稱。為 Kerberos 驗證領域選取描述性的名稱非常重要。設定領域，也稱為網域名稱，以及 Unified Access Gateway 中對應的 KDC 服務。當 UPN 要求進入特定領域時，Unified Access Gateway 會在內部解析 KDC 以使用 Kerberos 提供的票證。

慣例是以大寫字母輸入相同的領域名稱與網域名稱。例如，領域名稱為 EXAMPLE.NET。Kerberos 用戶端會使用領域名稱來產生 DNS 名稱。

從 Unified Access Gateway 3.0 版開始，您可以刪除先前定義的領域。

重要事項 如果是跨網域設定，請新增所有領域的詳細資料，包括主要網域及次要網域或子網域和相關聯的 KDC 資訊。請確定領域之間有信任關係。

先決條件

一部已啟用 Kerberos 的伺服器，且包含用於識別所使用金鑰發佈中心的領域名稱。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下 **選取**。
- 2 在 **進階設定 > 身分識別橋接設定** 區段中，選取 **領域設定** 齒輪圖示。
- 3 按一下 **新增**。
- 4 填妥表單。

標籤	說明
領域的名稱	使用網域名稱輸入領域。以大寫字母輸入領域。領域必須符合 Active Directory 中設定的網域名稱。
金鑰發佈中心	輸入領域的 KDC 伺服器。如果要新增一部以上伺服器，請以逗號區隔清單。
KDC 逾時 (以秒為單位)	輸入要等候 KDC 回應的時間。預設為 3 秒。

5 按一下**儲存**。

下一個

設定 Keytab 設定。

上傳 Keytab 設定

Keytab 是一個檔案，其中包含 Kerberos 主體和加密金鑰的配對。系統會針對需要單一登入的應用程式建立一個 Keytab 檔案。Unified Access Gateway 身分識別橋接會使用 Keytab 檔案來使用 Kerberos 向遠端系統進行驗證，而無需輸入密碼。

當使用者從身分識別提供者經過驗證進入 Unified Access Gateway 時，Unified Access Gateway 會從 Kerberos 網域控制站要求 Kerberos 票證以驗證使用者。

Unified Access Gateway 會使用 Keytab 檔案來模擬使用者，以向內部 Active Directory 網域進行驗證。

Unified Access Gateway 必須在 Active Directory 網域上具有網域使用者服務帳戶。

Unified Access Gateway 不會直接加入網域。

備註 如果管理員為某個服務帳戶重新產生 Keytab 檔案，則必須再次將 Keytab 檔案上傳至 Unified Access Gateway。

先決條件

存取 Kerberos Keytab 檔案以上傳至 Unified Access Gateway。Keytab 檔案為二進位檔案。若可能，請使用 SCP 或其他安全方法在電腦之間傳輸 Keytab。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在**進階設定 > 身分識別橋接設定**區段中，選取**上傳 Keytab 設定**齒輪圖示。
- 3 (選用) 在**主體名稱**文字方塊中輸入 Kerberos 主體名稱。

每個主體一律使用完整領域名稱。領域應該使用大寫字母。

請確定此處輸入的主體名為在 Keytab 檔案中找到的第一個主體。如果相同的主體名稱未在上傳的 Keytab 檔案中，則上傳 Keytab 檔案會失敗。

- 4 在**選取 Keytab 檔案**欄位中，按一下**選取**，並瀏覽至您儲存的 Keytab 檔案。按一下**開啟**。

如果您未輸入主體名稱，則會使用在 Keytab 中找到的第一個主體。您可以將多個 Keytab 合併成一個檔案。

- 5 按一下**儲存**。

下一個

為 Unified Access Gateway 身分識別橋接設定 Web Reverse Proxy。

針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的 SAML)

若要針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的 SAML)，您必須已將身分識別提供者中繼資料檔案儲存至 Unified Access Gateway。

然後，您可以在管理主控台上啟用身分識別橋接，並設定服務的外部主機名稱。

上傳身分識別提供者中繼資料

若要設定身分識別橋接功能，您必須將身分識別提供者的 SAML 憑證中繼資料 XML 檔案上傳至 Unified Access Gateway。

先決條件

SAML 中繼資料 XML 檔案必須儲存至您可以存取的電腦。

如果您使用 VMware Identity Manager 作為身分識別提供者，請從 VMware Identity Manager 管理主控台的目錄 > 設定 SAML 中繼資料 > 身分識別提供者 (IdP) 中繼資料連結下載並儲存 SAML 中繼資料檔案。

程序

- 1 在管理主控台的手動設定下方，按一下**選取**。
- 2 在**進階設定 > 身分識別橋接設定**區段中，選取**上傳身分識別提供者中繼資料**齒輪圖示。
- 3 在**實體 ID** 文字方塊中輸入身分識別提供者的實體 ID。
如果未在 [實體 ID] 文字方塊中輸入值，則系統會剖析中繼資料檔案中的身分識別提供者名稱，並用作身分識別提供者的實體 ID。
- 4 在 **IDP 中繼資料** 區段中，按一下**選取**，並瀏覽至您儲存的中繼資料檔案。按一下**開啟**。
- 5 按一下**儲存**。

下一個

針對 KDC 驗證，設定領域設定和 Keytab 設定。

針對標頭式驗證，當您設定身分識別橋接功能時，請以包含使用者 ID 之 HTTP 標頭的名稱來填入 [使用者標頭名稱] 選項。

針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的 SAML)

啟用身分識別橋接，設定服務的外部主機名稱，並下載 Unified Access Gateway 服務提供者中繼資料檔案。

此中繼資料檔案會上傳至 VMware Identity Manager 服務中的 Web 應用程式組態頁面。

先決條件

您必須已在 Unified Access Gateway 管理主控台上設定下列身分識別橋接設定。您可以在**進階設定**區段下找到這些設定。

- 身分識別提供者中繼資料已上傳至 Unified Access Gateway。
- 已設定 Kerberos 主體名稱，並已將 Keytab 檔案上傳至 Unified Access Gateway。

- 領域名稱和金鑰發佈中心資訊。

請確保 TCP/UDP 連接埠 88 已開啟，因為 Unified Access Gateway 使用此連接埠來與 Active Directory 進行 Kerberos 通訊。

程序

- 1 在管理員 UI 的手動設定區段中，按一下**選取**。
- 2 在**一般設定 > Edge Service 設定**行中，按一下**顯示**。
- 3 按一下 **Reverse Proxy 設定**齒輪圖示。
- 4 在 **Reverse Proxy 設定**頁面中按一下**新增**，以建立 Proxy 設定。
- 5 將**啟用 Reverse Proxy 設定**設為 [是]，並設定下列 Edge Service 設定。

選項	說明
識別碼	Edge Service 識別碼會設定為 Web Reverse Proxy。
執行個體 ID	Web Reverse Proxy 執行個體的唯一名稱。
Proxy 目的地 URL	指定 Web 應用程式的內部 URI。Unified Access Gateway 必須可以解析和存取此 URL。
Proxy 目的地 URL 指紋	輸入 URI 以符合此 Proxy 設定。指紋的格式為 [alg]=xx:xx，其中 alg 可以是 sha1 (預設值) 或 md5。「xx」為十六進位數字。例如，sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3。 如果未設定指紋，則必須由受信任的 CA 核發伺服器憑證。
Proxy 模式	輸入轉送至目的地 URL 的相符 URI 路徑。例如，您可以輸入 (/ /SAAS(.*) /hc(.*) /web(.*) /catalog-portal(.*)。 注意：當您設定多個 Reverse Proxy 時，請在 Proxy 主機模式中提供主機名稱

- 6 若要設定其他進階設定，請按一下**較多**。

選項	說明
驗證方法	預設會使用使用者名稱和密碼的傳遞驗證。您在 Unified Access Gateway 中設定的驗證方法會在下拉式功能表中列出。支援 RSA SecurID、RADIUS，以及裝置憑證驗證方法。
健全狀況檢查 URI 路徑	Unified Access Gateway 會連線至此 URI 路徑，以檢查您 Web 應用程式的健全狀況。
SAML SP	當您將 Unified Access Gateway 設定為 VMware Identity Manager 的已驗證 Reverse Proxy 時需要使用此選項。輸入 View XML API 代理之 SAML 服務提供者的名稱。此名稱必須符合使用 Unified Access Gateway 設定之服務提供者的名稱，或為特殊值 DEMO。如果使用 Unified Access Gateway 設定多個服務提供者，則其名稱必須是唯一的。
外部 URL	預設值為 Unified Access Gateway 主機 URL，連接埠 443。您可以輸入其他外部 URL。輸入為 https://<host:port>。

選項	說明
未受保護的模式	輸入已知的 VMware Identity Manager 重新導向模式。例如： <code>(/ /catalog-portal(.*) / /SAAS/ /SAAS/SAAS/API/1.0/GET/image(.*) /SAAS/horizon/css(.*) /SAAS/horizon/angular(.*) /SAAS/horizon/js(.*) /SAAS/horizon/js-lib(.*) /SAAS/auth/login(.*) /SAAS/jersey/manager/api/branding /SAAS/horizon/images/(.*) /SAAS/jersey/manager/api/images/(.*) /hc/(.*)/authenticate/(.*) /hc/static/(.*) /SAAS/auth/saml/response /SAAS/auth/authenticatedUserDispatcher /web(.*) /SAAS/apps/ /SAAS/horizon/portal/(.*) /SAAS/horizon/fonts(.*) /SAAS/API/1.0/POST/sso(.*) /SAAS/API/1.0/REST/system/info(.*) /SAAS/API/1.0/REST/auth/cert(.*) /SAAS/API/1.0/REST/oauth2/activate(.*) /SAAS/API/1.0/GET/user/devices/register(.*) /SAAS/API/1.0/oauth2/token(.*) /SAAS/API/1.0/REST/oauth2/session(.*) /SAAS/API/1.0/REST/user/resources(.*) /hc/t/(.*)/(.*)/authenticate(.*) /SAAS/API/1.0/REST/auth/logout(.*) /SAAS/auth/saml/response(.*) /SAAS/(.*)/(.*)auth/login(.*) /SAAS/API/1.0/GET/apps/launch(.*) /SAAS/API/1.0/REST/user/applications(.*) /SAAS/auth/federation/sso(.*) /SAAS/auth/oauth2/authorize(.*) /hc/prepareSaml/failure(.*) /SAAS/auth/oauth2token(.*) /SAAS/API/1.0/GET/metadata/idp.xml /SAAS/auth/saml/artifact/resolve(.*) /hc/(.*)/authAdapter(.*) /hc/authenticate/(.*) /SAAS/auth/logout /SAAS/common.js /SAAS/auth/launchInput(.*) /SAAS/launchUsersApplication.do(.*) /hc/API/1.0/REST/thinapp/download(.*) /hc/t/(.*)/(.*)/logout(.*) /SAAS/auth/wsfed/services(.*) /SAAS/auth/wsfed/active/login(.*)</code>)
驗證 Cookie	輸入驗證 Cookie 名稱。例如： HZN
登入重新導向 URL	如果使用者從入口網站登出，請輸入重新導向 URL 以重新登入。例如： <code>/SAAS/auth/login?dest=%s</code>
Proxy 主機模式	外部主機名稱，用來檢查傳入主機以查看它是否符合該特定執行個體的模式。設定 Web Reverse Proxy 執行個體時，主機模式為選用。
受信任的憑證	將受信任的憑證新增到此 Edge Service。按一下「+」來選取 PEM 格式的憑證，然後新增至信任存放區。按一下「-」可從信任存放區移除憑證。依預設，別名名稱是 PEM 憑證的檔案名稱。編輯別名文字方塊以提供不同的名稱。
回應安全性標頭	<p>按一下「+」可新增標頭。輸入安全性標頭的名稱。輸入值。按一下「-」可移除標頭。編輯現有的安全性標頭，以更新標頭的名稱和值。</p> <p>重要事項 在您按一下儲存後，才會儲存標頭名稱和值。依預設會顯示部分標準安全性標頭。僅在已設定後端伺服器的回應中沒有對應的標頭存在時，才會將已設定標頭新增至用戶端的 Unified Access Gateway 回應。</p> <p>備註 請謹慎修改安全性回應標頭。修改這些參數可能會影響到 Unified Access Gateway 的安全運作。</p>
主機項目	<p>輸入要在 /etc/hosts 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如，10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias。按一下「+」符號可新增多個主機項目。</p> <p>重要事項 只有在按一下儲存後，才會儲存主機項目。</p>

7 在 [啟用身分識別橋接] 區段中，將否變更為是。

8 設定下列身分識別橋接設定。

選項	說明
驗證類型	選取 SAML。
SAML 屬性	傳遞作為要求標頭的 SAML 屬性清單。僅在 啟用身分識別橋接 設定為 是 ，且 驗證類型 設定為 SAML 時，才會顯示此選項。按一下「+」可將 SAML 屬性新增為標頭的一部分。
身分識別提供者	從下拉式功能表選取身分識別提供者。
Keytab	在下拉式功能表中，選取針對此 Reverse Proxy 設定的 Keytab。
目標服務主體名稱	輸入 Kerberos 服務主體名稱。每個主體一律使用完整領域名稱。例如， myco_hostname@MYCOMPANY 。以大寫字母輸入領域名稱。如果您不新增名稱至文字方塊，則服務主體名稱會衍生自 Proxy 目的地 URL 的主機名稱。
服務登陸頁面	輸入在驗證聲明後將使用者重新導向至身分識別提供者的頁面。預設設定為 /。
使用者標頭名稱	針對標頭式驗證，輸入包含衍生自聲明之使用者 ID 的 HTTP 標頭名稱。

9 在 [下載 SP 中繼資料] 區段中，按一下**下載**。

儲存服務提供者中繼資料檔案。

10 按一下**儲存**。

下一個

將 Unified Access Gateway 服務提供者中繼資料檔案新增至 VMware Identity Manager 服務中的 Web 應用程式組態頁面。

將中繼資料檔案新增至 VMware Identity Manager 服務

必須將您下載的 Unified Access Gateway 服務提供者中繼資料檔案上傳至 VMware Identity Manager 服務中的 Web 應用程式組態頁面。

使用的 SSL 憑證必須與多個負載平衡 Unified Access Gateway 伺服器中所使用的憑證相同。

先決條件

您必須已將 Unified Access Gateway 服務提供者中繼資料檔案儲存至電腦。

程序

- 1 登入 VMware Identity Manager 管理主控台。
- 2 在 [目錄] 索引標籤中，按一下**新增應用程式**，並選取**建立新的應用程式**。
- 3 在 [應用程式詳細資料] 頁面的 [名稱] 文字方塊中輸入使用者易記名稱。
- 4 選取 **SAML 2.0 POST** 驗證設定檔。
您也可以新增此應用程式的說明及圖示，向 Workspace ONE 入口網站中的使用者顯示。
- 5 按**下一步**，並在 [應用程式組態] 頁面中，向下捲動至**透過下列項目設定**區段。
- 6 選取 [中繼資料 XML] 選項按鈕並將 Unified Access Gateway 服務提供者中繼資料文字貼入 [中繼資料 XML] 文字方塊內。

- 7 (選用) 在 [屬性對應] 區段中，將下列屬性名稱對應至使用者設定檔值。FORMAT 欄位值為「基本」。必須以小寫輸入屬性名稱。

名稱	設定的值
upn	userPrincipalName
userid	Active Directory 使用者 ID

- 8 按一下**儲存**。

下一個

授權使用者和群組使用此應用程式。

備註 Unified Access Gateway 僅支援單一網域使用者。如果身分識別提供者設定了多個網域，則僅能將應用程式授權給單一網域中的使用者。

針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的憑證)

在您設定 Unified Access Gateway 橋接功能，以便為使用憑證驗證的內部部署舊版非 SAML 應用程式提供單一登入 (SSO) 之前，請先設定 Workspace ONE UEM 主控台以擷取和使用 CA 憑證。

啟用 AirWatch 主控台以擷取和使用 CA 憑證

您可以在 CA 伺服器中新增使用者範本，並在 AirWatch 主控台中進行設定，讓 AirWatch 能夠擷取並使用 CA 憑證。

1 新增使用者範本

首先，在 CA 伺服器中新增使用者範本，讓 AirWatch 能夠擷取憑證。

2 在主控台中新增憑證授權單位

在 VMware AirWatch 主控台中新增憑證授權單位 (CA)。

3 新增憑證授權單位要求範本

請在 AirWatch 主控台中新增憑證授權單位之後新增 CA 要求範本。

4 更新安全性原則以使用擷取的 CA 憑證

在 AirWatch 主控台中更新安全性原則以使用擷取的 CA 憑證。

新增使用者範本

首先，在 CA 伺服器中新增使用者範本，讓 AirWatch 能夠擷取憑證。

程序

- 1 登入設定 CA 的伺服器。
- 2 按一下**開始**，然後輸入 `mmc.exe`。
- 3 在 **MMC** 視窗中，移至**檔案 > 新增/移除嵌入式管理單元**。
- 4 在**新增或移除嵌入式管理單元**視窗中，選取**憑證範本**，然後按一下**新增**。

- 5 按一下**確定**。
- 6 在**憑證範本**視窗中向下捲動，並選取**使用者 > 複製範本**，
- 7 在**新範本的內容**視窗中，選取**一般**索引標籤，然後提供**範本顯示名稱**的名稱。
範本名稱會自動填入此名稱，不含空格。
- 8 選取**主體名稱**索引標籤，然後選取在要求中提供。
- 9 按一下**套用**，然後再按一下**確定**。
- 10 在 **MMC** 視窗中，移至**檔案 > 新增/移除嵌入式管理單元**。
- 11 在**新增或移除嵌入式管理單元**視窗中，選取**憑證授權單位**，然後按一下**新增**。
- 12 在 **MMC** 視窗中，選取**憑證授權單位 > 憑證範本**。
- 13 以滑鼠右鍵按一下**憑證授權單位**，然後選取**新增 > 要發出的憑證範本**。
- 14 選取您在步驟 6 中建立的範本。

下一個

確認您新增的範本顯示於清單中。

登入 AirWatch 主控台並新增 CA。

在主控台中新增憑證授權單位

在 VMware AirWatch 主控台中新增憑證授權單位 (CA)。

先決條件

- 您必須已在 CA 伺服器中新增使用者範本。
- 您必須具有 CA 簽發者的名稱。登入 Active Directory (AD) 伺服器，並從命令提示字元執行 `certutil` 命令以取得 CA 簽發者名稱。
- 指定 CA 的**使用者名稱**以作為**服務帳戶**類型。

程序

- 1 登入 AirWatch 主控台，並選取適當的組織群組。
- 2 移至**所有設定**，然後從下拉式功能表中按一下**企業整合 > 憑證授權單位**。
- 3 按一下**憑證授權單位**索引標籤，然後按一下**新增**。
- 4 輸入憑證授權單位的下列資訊：

選項	說明
名稱	CA 的有效名稱
授權單位類型	Microsoft ADCS
通訊協定	ADCS
伺服器主機名稱	AD 伺服器的主機名稱
授權單位名稱	CA 簽發者名稱

選項	說明
驗證	服務帳戶
使用者名稱	具有格式為 <i>domain\username</i> 之服務帳戶的使用者名稱。
密碼	使用者名稱的密碼
其他選項	無

5 按一下儲存。

新增憑證授權單位要求範本

請在 AirWatch 主控台中新增憑證授權單位之後新增 CA 要求範本。

先決條件

- 1 您必須已在 CA 伺服器中新增使用者範本。
- 2 您必須已在 AirWatch 主控台中新增 CA。

程序

- 1 登入 AirWatch 主控台，移至**所有設定**，然後從下拉式清單中按一下**企業整合 > 憑證授權單位**。
- 2 按一下**要求範本**索引標籤，然後按一下**新增**。
- 3 輸入範本的下列資訊：

選項	說明
名稱	憑證範本的有效名稱
說明 (選擇性)	範本的說明
憑證授權單位	先前新增的憑證授權單位
發行範本	在 CA 伺服器中建立之使用者範本的名稱
主旨名稱	若要新增主體名稱，請將游標停留在值欄位上 (預設值「CN=」後面)，接著按一下「+」按鈕，然後選取適當的電子郵件地址
私密金鑰長度	2048
私密金鑰類型	選取簽署
SAN 類型	按一下 新增 ，然後選擇 使用者主體名稱
自動憑證更新 (選用)	
啟用憑證撤銷 (選用)	
發佈私密金鑰 (選用)	

4 按一下儲存。

更新安全性原則以使用擷取的 CA 憑證

在 AirWatch 主控台中更新安全性原則以使用擷取的 CA 憑證。

先決條件

程序

- 1 登入 AirWatch 主控台，移至**所有設定**，然後從下拉式清單中按一下**應用程式 > 安全性和原則 > 安全性原則**。
- 2 針對目前的設定選取**覆寫**。
- 3 啟用**整合式驗證**。
 - a 選取**使用憑證**。
 - b 將**認證來源**設為**已定義的憑證授權單位**。
 - c 指定先前設定的**憑證授權單位**和**憑證範本**。
- 4 將**允許的站台**設為 *****。
- 5 按一下**儲存**。

針對身分識別橋接設定 Web Reverse Proxy (對 Kerberos 的憑證)

設定 Unified Access Gateway 橋接功能，以便為使用憑證驗證的內部部署舊版非 SAML 應用程式提供單一登入 (SSO)。

先決條件

開始進行組態程序之前，請確定您可以使用下列檔案和憑證：

- 後端應用程式 (例如 Sharepoint 或 JIRA) 的 Keytab 檔案
- 根 CA 憑證或含有使用者中繼憑證的整個憑證鏈結。
- 您必須已在 Workspace ONE UEM 主控台中新增並上傳憑證。請參閱[啟用 AirWatch 主控台以擷取和使用 CA 憑證](#)。

請參閱相關產品說明文件，以產生非 SAML 應用程式的根憑證和使用者憑證以及 Keytab 檔案。

請確保 TCP/UDP 連接埠 88 已開啟，因為 Unified Access Gateway 使用此連接埠來與 Active Directory 進行 Kerberos 通訊。

程序

- 1 從**驗證設定 > X509 憑證**移至：
 - a 在**根憑證**和**中繼 CA 憑證**中，按一下**選取**並上傳整個憑證鏈結。
 - b 在**啟用憑證撤銷**中，將設定切換為**是**。
 - c 選取**啟用 OCSP 撤銷**的核取方塊。

- d 在 **OCSP URL** 文字方塊中，輸入 OCSP 回應者 URL。

Unified Access Gateway 會將 OCSP 要求傳送至指定的 URL，並接收包含指出憑證是否已撤銷之相關資訊的回應。

- e 僅在需要將 OCSP 要求傳送至用戶端憑證中的 OCSP URL 時，才應選取**使用來自憑證的 OCSP URL** 核取方塊。如果未啟用此設定，則預設為 OCSP URL 文字方塊中的值。

X.509 憑證

- 2 在**進階設定 > 身分識別橋接設定 > OSCP 設定**中，按一下**新增**。
 - a 按一下**選取**並上傳 OCSP 簽署憑證。
- 3 選取**領域設定**齒輪圖示並依照**設定領域設定**中所述設定領域設定。
- 4 從**一般設定 > Edge Service 設定**，選取 **Reverse Proxy 設定**齒輪圖示。
- 5 將**啟用身分識別橋接設定**設為**是**，接著設定下列身分識別橋接設定，然後按一下**儲存**。

選項	說明
驗證類型	從下拉式功能表中選取 CERTIFICATE。
Keytab	在下拉式功能表中，選取針對此 Reverse Proxy 設定的 Keytab。
目標服務主體名稱	輸入 Kerberos 服務主體名稱。每個主體一律使用完整領域名稱。例如， myco_hostname@MYCOMPANY 。以大寫字母輸入領域名稱。如果您不新增名稱至文字方塊，則服務主體名稱會衍生自 Proxy 目的地 URL 的主機名稱。
使用者標頭名稱	針對標頭式驗證，輸入包含衍生自判斷提示之使用者 ID 的 HTTP 標頭名稱，或使用預設值 AccessPoint-User-ID 。

下一個

當您使用 VMware Browser 存取目標網站時，目標網站將會作為 Reverse Proxy。

Unified Access Gateway 會驗證提供的憑證。如果憑證有效，則瀏覽器會顯示後端應用程式的使用者介面頁面。

如需特定的錯誤訊息和疑難排解資訊，請參閱[疑難排解錯誤：身分識別橋接](#)。

Unified Access Gateway 的 VMware AirWatch 元件

您可以使用 Unified Access Gateway 應用裝置來部署 VMware Tunnel。Unified Access Gateway 支援 ESXi 或 Microsoft Hyper-V 環境上的部署。VMware Tunnel 可讓個別應用程式透過安全而有效的方法存取公司資源。Content Gateway (CG) 是 VMware AirWatch 內容管理解決方案的元件，可讓您安全地在行動裝置上存取內部部署存放庫內容。

VMware Tunnel 和 Content Gateway 的 DNS 需求

在相同的應用裝置上啟用 VMware Tunnel 和 Content Gateway 服務，並啟用 TLS 連接埠共用時，每項服務的 DNS 名稱都必須是唯一的。未啟用 TLS 時，這兩項服務只能使用一個 DNS 名稱，因為連接埠將會區分傳入流量。

在 Unified Access Gateway 上部署 VMware Tunnel

使用 Unified Access Gateway 應用裝置部署 VMware Tunnel，可讓個別應用程式透過安全而有效的方法存取公司資源。Unified Access Gateway 支援 ESXi 或 Microsoft Hyper-V 環境上的部署。

VMware Tunnel 由兩個獨立元件所組成：通道代理伺服器 and 每一應用程式通道。您可以使用單層或多層網路架構模型來部署 VMware Tunnel。

通道代理伺服器和每一應用程式通道部署模型皆可用於 Unified Access Gateway 應用裝置上的多層網路。此部署包含一個部署於 DMZ 中的前端 Unified Access Gateway 伺服器，以及一個部署於內部網路中的後端伺服器。

通道代理伺服器元件可透過從 VMware AirWatch 部署的 VMware Browser 或任何具有 VMware AirWatch SDK 功能的應用程式，保護使用者裝置與網站之間的網路流量。行動應用程式能利用通道代理伺服器來建立安全的 HTTPS 連線，進而保護機密資料。裝置會使用透過 SDK 核發的憑證對通道代理伺服器進行驗證，如 Workspace ONE UEM 主控台中所設定。一般而言，當未受管理的裝置需要安全地存取內部資源時，即應使用此元件。

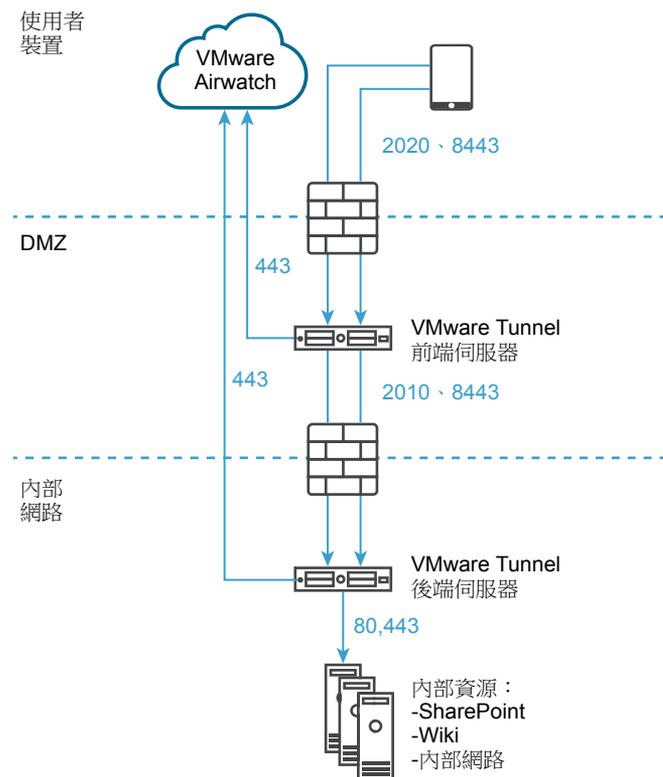
對於完整註冊的裝置，每一應用程式通道元件可讓裝置不需要 VMware AirWatch SDK 即可連線至內部資源。此元件會使用 iOS、Android、Windows 10 和 macOS 作業系統的原生每一應用程式 VPN 功能。

如需關於這些平台和 VMware Tunnel 元件功能的詳細資訊，請參閱 [WorkSpace ONE UEM 說明文件頁面](#) 中的最新《VMware Tunnel》說明文件。

為您的 VMware AirWatch 環境部署 VMware Tunnel 涉及下列作業：

- 1 設定初始硬體。
- 2 在 Workspace ONE UEM 主控台中設定 VMware Tunnel 主機名稱和連接埠資訊。請參閱 [DMZ 型 Unified Access Gateway 應用裝置的防火牆規則](#)。
- 3 下載並部署 Unified Access Gateway OVF 範本。
- 4 手動設定 VMware Tunnel。

圖 4-9 VMware Tunnel 多層部署：代理伺服器和每一應用程式通道



AirWatch v9.1 及更高版本支援階層式模式作為 VMware Tunnel 的多層部署模型。使用「階層式模式」時，每個從網際網路連至前端通道伺服器的通道元件皆必須有專用的輸入連接埠。前端和後端伺服器皆必須能夠與 AirWatch API 和 AWCM 伺服器進行通訊。VMware Tunnel 階層式模式支援每一應用程式通道元件的多層架構。

如需 Content Gateway 和通道代理伺服器的負載平衡考量事項，請參閱 [Unified Access Gateway 負載平衡拓撲](#)。

前往 [VMware AirWatch 說明文件](#) 頁面，以取得 VMware AirWatch 指南和版本說明的完整清單。

設定的 VMware AirWatch 的 VMware Tunnel 設定

通道代理伺服器部署能透過 VMware Browser 行動應用程式保護使用者裝置和網站之間的網路流量。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下 **選取**。
- 2 導覽至 **一般設定 > Edge Service 設定**，然後按一下 **顯示**。
- 3 按一下 **VMware Tunnel 設定** 齒輪圖示。
- 4 將 [否] 變更為 **是** 以啟用通道代理伺服器。
- 5 設定下列 Edge Service 設定資源。

選項	說明
API 伺服器 URL	輸入 VMware AirWatch API 伺服器 URL。例如，您可以輸入 <code>https://example.com:<連接埠></code> 。
API 伺服器使用者名稱	輸入用來登入 API 伺服器的使用者名稱。
API 伺服器密碼	輸入用來登入 API 伺服器的密碼。
組織群組 ID	輸入使用者的組織。
通道伺服器主機名稱	輸入在 Workspace ONE UEM 主控台中設定的 VMware Tunnel 外部主機名稱。

- 6 若要設定其他進階設定，請按一下 **較多**。

選項	說明
連出代理伺服器主機	輸入安裝連出代理伺服器所在的主機名稱。 備註 這不是通道代理伺服器。
連出代理伺服器連接埠	輸入連出代理伺服器的連接埠號碼。
連出代理伺服器使用者名稱	輸入用來登入連出代理伺服器的使用者名稱。
連出代理伺服器密碼	輸入用來登入連出代理伺服器的密碼。
NTLM 驗證	將 [否] 變更為 是 以指定連出代理伺服器要求需要 NTLM 驗證。
用於 VMware Tunnel 代理伺服器	將 [否] 變更為 是 以使用此 Proxy 作為 VMware Tunnel 的連出代理伺服器。如果未啟用，則 Unified Access Gateway 會對初始 API 呼叫使用此 Proxy，以便從 Workspace ONE UEM 主控台取得組態。
主機項目	輸入要在 /etc/hosts 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如， <code>10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias</code> 。按一下「+」符號可新增多個主機項目。 重要事項 只有在按一下 儲存 後，才會儲存主機項目。
受信任的憑證	選取要新增到信任存放區的受信任憑證檔案 (PEM 格式)。依預設，別名名稱是 PEM 憑證的檔案名稱。編輯別名文字方塊以提供不同的名稱。

7 按一下儲存。

使用 PowerShell 為 VMware AirWatch 部署 VMware Tunnel

您可以使用 PowerShell 為 VMware AirWatch 部署 VMware Tunnel。

如需使用 PowerShell 部署 VMware Tunnel 的相關資訊，請觀看此視訊：



VMware AirWatch Tunnel PowerShell 部署

(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_airwatch_tunnel_powershell)

關於 TLS 連接埠共用

每當多個 Edge Service 設定為使用 TCP 連接埠 443 時，依預設會在 Unified Access Gateway 上啟用 TLS 連接埠共用。支援的 Edge Service 為 VMware Tunnel (每一應用程式 VPN)、Content Gateway 和 Web Reverse Proxy。

備註 如果您要共用 TCP 連接埠 443，請確保每個設定的 Edge Service 具有指向 Unified Access Gateway 的唯一外部主機名稱。

Unified Access Gateway 上的 Content Gateway

Content Gateway (CG) 是 VMware AirWatch 內容管理解決方案的元件，可讓您安全地在行動裝置上存取內部部署存放庫內容。

先決條件

您必須使用 Workspace ONE UEM 主控台設定 Content Gateway 節點，才能設定 Unified Access Gateway 上的 Content Gateway。設定節點之後，請記下自動產生的 *Content Gateway* 組態 GUID。如需詳細資訊，請參閱《VMware Workspace ONE UEM》說明文件中的設定 Content Gateway 節點一節。

備註 縮寫 CG 也可用來表示 Content Gateway。

您也可以參閱下列說明文件，以瞭解 Content Gateway 架構和安全性概觀：

- 1 [Content Gateway 的基本 \(僅限端點\) 部署模型](#)
- 2 [Content Gateway 的轉送部署模型](#)

程序

- 1 導覽至一般設定 > Edge Service 設定 > Content Gateway 設定，然後按一下齒輪圖示。
- 2 選取是以啟用 Content Gateway 設定。

3 進行下列設定，然後按一下**儲存**。

選項	說明
識別碼	表示此服務已啟用。
API 伺服器 URL	VMware AirWatch API 伺服器 URL [http[s]://]hostname[:port] 目的地 URL 必須包含通訊協定、主機名稱或 IP 位址，以及連接埠號碼。例如： <code>https://load-balancer.example.com:8443</code> Unified Access Gateway 會從 API 伺服器提取 Content Gateway 的組態。
API 伺服器使用者名稱	用來登入 API 伺服器的使用者名稱。
API 伺服器密碼	用來登入 API 伺服器的密碼。
Content Gateway 主機名稱	用來設定 Edge 設定的主機名稱。
Content Gateway 組態 GUID	VMware AirWatch Content Gateway 組態識別碼。此識別碼會在使用 Workspace ONE UEM 主控台設定 Content Gateway 時自動產生。組態 GUID 會在 UEM 主控台的 Content Gateway 頁面上，顯示於 設定 > 內容 > Content Gateway 下方。
連出代理伺服器主機	安裝連出代理伺服器所在的主機。Unified Access Gateway 會透過連出代理伺服器 (若已設定) 建立 API 伺服器的連線。
連出代理伺服器連接埠	連出代理伺服器的連接埠。
連出代理伺服器使用者名稱	登入連出代理伺服器的使用者名稱。
連出代理伺服器密碼	登入連出代理伺服器的密碼。
NTLM 驗證	指定連出代理伺服器是否需要 NTLM 驗證。
受信任的憑證	將受信任的憑證新增到此 Edge Service。按一下「+」來選取 PEM 格式的憑證，然後新增至信任存放區。按一下「-」可從信任存放區移除憑證。依預設，別名名稱是 PEM 憑證的檔案名稱。編輯別名文字方塊以提供不同的名稱。
主機項目	輸入要在 <code>/etc/hosts</code> 檔案中新增的詳細資料。每個項目依序應包括一個 IP、一個主機名稱和一個選用的主機名稱別名 (以空格區隔)。例如， 10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias 。按一下「+」可新增多個主機項目。 重要事項 只有在按一下 儲存 後，才會儲存主機項目。

備註 在 Unified Access Gateway 上，連接埠 80 上的 Content Gateway 不允許 HTTP 流量，因為 TCP 連接埠 80 由 Edge Service Manager 所使用。

其他部署使用案例

您可以在相同的應用裝置上 (例如 Horizon 與 Web Reverse Proxy，以及 Unified Access Gateway 與 VMware Tunnel、Content Gateway 和 Web Reverse Proxy) 部署 Unified Access Gateway 與多個 Edge Service。

部署 Unified Access Gateway 與多個服務的考量

一併部署 Edge Service 之前，請注意下列重要考量。

- 了解並符合網路需求 - 請參閱 [DMZ 型 Unified Access Gateway 應用裝置的防火牆規則](#)。
- 遵循調整大小的準則 - 請參閱 [使用 OVF 範本精靈來部署 Unified Access Gateway](#) 主題中調整大小選項的小節。
- 當 Proxy 模式中有重疊時，Horizon Connection Server 無法搭配已啟用的 Web Reverse Proxy 正常運作。因此，如果在相同的 Unified Access Gateway 執行個體上使用 Proxy 模式同時設定並啟用了 Horizon 和 Web Reverse Proxy 執行個體，請從 Horizon 設定中移除 Proxy 模式「/」，並保留 Web Reverse Proxy 中的模式以防止重疊。保留 Web Reverse Proxy 執行個體中的「/」Proxy 模式可確保使用者在按一下 Unified Access Gateway 的 URL 時會顯示正確的 Web Reverse Proxy 頁面。如果僅設定了 Horizon 設定，則不需要進行前述變更。
- 部署 Unified Access Gateway 與 VMware Tunnel、Content Gateway 以及 Web Reverse Proxy 的結合服務時，如果對所有服務使用相同的連接埠 443，則每個服務應具有唯一的外部主機名稱。請參閱 [關於 TLS 連接埠共用](#)。
- 您可以使用管理員 UI 來獨立設定不同的 Edge Service，且可以根據需要匯入任何先前的設定。使用 PowerShell 部署時，INI 檔案會使部署生產就緒。
- 如果在相同 Unified Access Gateway 應用裝置上啟用 Horizon Blast 和 VMware Tunnel，則必須將 VMware Tunnel 設定為使用與 443 或 8443 不同的其他連接埠號碼。如果您想要對 VMware Tunnel 使用連接埠 443 或 8443，則必須在個別的 Unified Access Gateway 應用裝置上部署 Horizon Blast 服務。

使用 TLS/SSL 憑證設定 Unified Access Gateway

5

您必須設定 Unified Access Gateway 應用裝置的 TLS/SSL 憑證。

備註 設定 Unified Access Gateway 應用裝置的 TLS/SSL 憑證僅適用於 Horizon、Horizon Air 及 Web Reverse Proxy。

設定 Unified Access Gateway 應用裝置的 TLS/SSL 憑證

用戶端在連線至 Unified Access Gateway 應用裝置時必須使用 TLS/SSL。面向用戶端的 Unified Access Gateway 應用裝置和終止 TLS/SSL 連線的中繼伺服器需要 TLS/SSL 伺服器憑證。

TLS/SSL 伺服器憑證是由憑證授權機構 (CA) 簽署。CA 是一個受信任的實體，可保證憑證的身分及其建立者。當憑證是由信任的 CA 簽署時，使用者不會再收到要求他們確認憑證的訊息，而精簡型用戶端裝置可以連線，無需要求額外組態。

當您部署 Unified Access Gateway 應用裝置時就會產生預設的 TLS/SSL 伺服器憑證。針對生產環境，VMware 建議您盡快取代預設憑證。預設憑證並非由信任的 CA 所簽署。預設憑證只能用於非生產環境。

選取正確的憑證類型

您可將多種 TLS/SSL 憑證類型用於 Unified Access Gateway。為您的部署選取正確的憑證類型十分重要。憑證類型不同，其成本也不同，端視其可使用在的伺服器數目而定。

無論您選取何種憑證類型，請務必遵循 VMware 的安全建議：針對憑證使用完整網域名稱 (FQDN)。請勿使用簡單伺服器名稱或 IP 位址，即使針對內部網域內的通訊。

單一伺服器名稱憑證

您可針對特定伺服器，產生具有主體名稱的憑證。例如：`dept.example.com`。

如果只有一個 Unified Access Gateway 應用裝置需要憑證，這種憑證類型就很有用。

當您提交憑證簽署要求至 CA 時，需提供要與憑證相關聯的伺服器名稱。請確定 Unified Access Gateway 應用裝置可以解析您提供的伺服器名稱，使其符合憑證關聯的名稱。

主體別名

主體別名 (SAN) 是在核發憑證時可以新增至憑證的屬性。使用此屬性新增主體名稱 (URL) 至憑證，讓憑證可以驗證多個伺服器。

例如，假設針對位於負載平衡器後面的 Unified Access Gateway 應用裝置核發了三個憑證：
`ap1.example.com`、`ap2.example.com` 和 `ap3.example.com`。透過在此範例中新增代表負載平衡器主機名稱的主體別名，例如 `horizon.example.com`，憑證就能生效，因為它符合用戶端指定的主機名稱。

提交憑證簽署要求至 CA 時，請提供外部介面負載平衡器虛擬 IP 位址 (VIP) 作為一般名稱和 SAN 名稱。請確定 Unified Access Gateway 應用裝置可以解析您提供的伺服器名稱，使其符合憑證關聯的名稱。

憑證會用於連接埠 443。

萬用字元憑證

產生萬用字元憑證以用於多個服務。例如：`*.example.com`。

如果有多個伺服器需要憑證，萬用字元就很有用。如果除了 Unified Access Gateway 應用裝置以外，您環境中還有其他應用程式需要 TLS/SSL 憑證，您也能為這些伺服器使用萬用字元憑證。不過，如果使用與其他服務共用的萬用字元憑證，則 VMware Horizon 產品的安全性也會取決於上述其他服務的安全性。

備註 萬用字元憑證只能用於單一網域層級。例如，具有主體名稱 `*.example.com` 的萬用字元憑證可以用於子網域 `dept.example.com`，但不能用於 `dept.it.example.com`。

您匯入至 Unified Access Gateway 應用裝置的憑證必須是用戶端機器信任的，也必須能夠適用於 Unified Access Gateway 的所有執行個體以及所有負載平衡器，無論是使用萬用字元還是主體別名 (SAN) 憑證。

將憑證檔案轉換為單行 PEM 格式

若要使用 Unified Access Gateway REST API 進行憑證設定或要使用 PowerShell 指令碼，您必須將憑證轉換為 PEM 格式檔案以取得憑證鏈結和私密金鑰，接著必須將 `.pem` 檔案轉換為包含內嵌換行字元的單行格式。

設定 Unified Access Gateway 時，可能有三種憑證類型需要加以轉換。

- 請一律為 Unified Access Gateway 應用裝置安裝並設定 TLS/SSL 伺服器憑證。
- 如果計劃使用智慧卡驗證，您必須針對將要放在智慧卡上的憑證，安裝並設定信任的 CA 簽發者憑證。
- 如果計劃使用智慧卡驗證，VMware 建議您為 Unified Access Gateway 應用裝置上所安裝的 SAML 伺服器憑證，安裝並設定簽署 CA 的根憑證。

對於這三種憑證類型，執行相同程序以將憑證轉換為包含憑證鏈結的 PEM 格式檔案。對於 TLS/SSL 伺服器憑證和根憑證，另請將每個檔案轉換為包含私密金鑰的 PEM 檔案。接著必須將每個 `.pem` 檔案轉換為可將 JSON 字串傳遞至 Unified Access Gateway REST API 的單行格式。

先決條件

- 確認您擁有憑證檔案。檔案可能是 PKCS#12 (`.p12` 或 `.pfx`) 格式，也可能是 Java JKS 或 JCEKS 格式。
- 自行熟悉您將用來轉換憑證的 `openssl` 命令列工具。請參閱 <https://www.openssl.org/docs/apps/openssl.html>。

現在，您可以使用這些 `.pem` 檔案並搭配 <https://communities.vmware.com/docs/DOC-30835> 上的部落格文章〈Using PowerShell to Deploy VMware Unified Access Gateway〉(使用 PowerShell 部署 VMware Unified Access Gateway) 內附的 PowerShell 指令碼，來設定 Unified Access Gateway 的憑證。或者，您也可以建立並使用 JSON 要求來設定憑證。

下一個

您可以使用 CA 簽署的憑證更新預設的自我簽署憑證。請參閱[更新 SSL 伺服器簽署的憑證](#)。若是智慧卡憑證，請參閱在 [Unified Access Gateway 應用裝置上設定憑證或智慧卡驗證](#)。

變更 TLS 或 SSL 通訊所用的安全性通訊協定和加密套件

雖然在幾乎所有情況下都無須變更預設設定，您仍可設定用來加密用戶端和 Unified Access Gateway 應用裝置之間通訊的安全性通訊協定和密碼編譯演算法。

預設設定包括使用 128 位元或 256 位元 AES 加密的加密套件 (除了匿名 DH 演算法)，然後按強度對其排序。依預設會啟用 TLS v1.1 和 TLS v1.2。TLS v1.0 和 SSL v3.0 會停用。

先決條件

- 自行熟悉 Unified Access Gateway REST API。此 API 的規格位於安裝 Unified Access Gateway 的虛擬機器上，可從下列 URL 取得：<https://access-point-appliance.example.com:9443/rest/swagger.yaml>。
- 自行熟悉用於設定加密套件和通訊協定的特定內容：`cipherSuites`、`ssl30Enabled`、`tls10Enabled`、`tls11Enabled` 和 `tls12Enabled`。

程序

- 1 建立 JSON 要求，用以指定要使用的通訊協定和加密套件。

下列範例具有預設設定。

```
{
  "cipherSuites":
  "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA",
  "ssl30Enabled": "false",
  "tls10Enabled": "false",
  "tls11Enabled": "true",
  "tls12Enabled": "true"
}
```

- 2 使用 REST 用戶端 (例如 `curl` 或 `postman`)，以使用 JSON 要求來叫用 Unified Access Gateway REST API 並設定通訊協定和加密套件。

在此範例中，access-point-appliance.example.com 是 Unified Access Gateway 應用裝置的完整網域名稱。

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-appliance.example.com:9443/rest/v1/config/system < ~/ciphers.json
```

`ciphers.json` 是您在上一個步驟中建立的 JSON 要求。

將會使用您指定的加密套件和通訊協定。

設定 DMZ 中的驗證

初始部署 Unified Access Gateway 時，Active Directory 密碼驗證會設定為預設值。使用者輸入其 Active Directory 使用者名稱和密碼之後，這些憑證會傳送到後端系統進行驗證。

您可以設定 Unified Access Gateway 服務以執行憑證/智慧卡驗證、RSA SecurID 驗證、RADIUS 驗證和 RSA 調適性驗證。

備註 使用 Active Directory 的密碼驗證是可搭配 AirWatch 部署使用的唯一驗證方法。

本章節討論下列主題：

- 在 Unified Access Gateway 應用裝置上設定憑證或智慧卡驗證
- 在 Unified Access Gateway 中設定 RSA SecurID 驗證
- 設定 Unified Access Gateway 的 RADIUS
- 在 Unified Access Gateway 中設定 RSA 調適性驗證
- 產生 Unified Access Gateway SAML 中繼資料

在 Unified Access Gateway 應用裝置上設定憑證或智慧卡驗證

您可以在 Unified Access Gateway 中設定 x509 憑證驗證，以允許用戶端在其桌面平台或行動裝置上使用憑證進行驗證，或是使用智慧卡配接器進行驗證。

憑證式驗證是根據使用者所擁有的驗證工具 (私密金鑰或智慧卡)，以及個人所知道的驗證內容 (私密金鑰的密碼或智慧卡 PIN)。智慧卡驗證提供雙因素驗證，一是驗證個人擁有的 (智慧卡)，一是驗證個人知道的 (PIN)。使用者可將智慧卡用於登入遠端 Horizon 桌面平台作業系統，以及用於啟用智慧卡功能的應用程式，例如採用憑證簽署電子郵件以證明寄件者身分的電子郵件應用程式。

利用此功能，系統會對 Unified Access Gateway 服務執行智慧卡憑證驗證。Unified Access Gateway 使用 SAML 聲明來向 Horizon server 傳遞有關使用者的 X.509 憑證與智慧卡 PIN 的資訊。

您可以設定憑證撤銷檢查，以防止使用者憑證已撤銷的使用者進行驗證。通常當使用者離開組織、遺失智慧卡，或調動部門時，就會撤銷憑證。支援使用「憑證撤銷清單」(CRL) 和「線上憑證狀態通訊協定」(OCSP) 的憑證撤銷檢查。CRL 是核發憑證的 CA 所發佈的撤銷憑證清單。OCSP 是用來取得憑證撤銷狀態的憑證驗證通訊協定。

您可以在憑證驗證配接器組態中同時設定 CRL 和 OCSP。當您同時設定兩種類型的憑證撤銷檢查，且若啟用了 **OCSP 失敗** 核取方塊時，則使用 CRL，將會先檢查 OCSP，如果 OCSP 失敗，撤銷檢查會退而使用 CRL。

備註 如果 CRL 失敗，撤銷檢查不會回復使用 OCSP。

備註 針對 VMware Identity Manager，驗證一律會透過 Unified Access Gateway 傳遞至 VMware Identity Manager 服務。只有當 Unified Access Gateway 搭配 Horizon 7 使用時，才能設定在 Unified Access Gateway 應用裝置上執行智慧卡驗證。

在 Unified Access Gateway 上設定憑證驗證

您可從 Unified Access Gateway 管理主控台啟用並設定憑證驗證。

先決條件

- 從簽署由您的使用者提供之憑證的 CA 取得根憑證和中繼憑證。請參閱 [取得憑證授權機構憑證](#)
- 確認已在服務提供者上新增 Unified Access Gateway SAML 中繼資料，且服務提供者 SAML 中繼資料已複製到 Unified Access Gateway 應用裝置。
- (選用) 適用於憑證驗證的有效憑證原則的物件識別碼 (OID) 清單。
- CRL 的檔案位置和 OCSP 伺服器的 URL，用於撤銷檢查。
- (選用) OCSP 回應簽署憑證檔案位置。
- 同意表單內容 (如果同意表單會在驗證前顯示)。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下 **選取**。
- 2 在 [一般設定] 的 [驗證設定] 區段中，按一下 **顯示**。
- 3 按一下 [X.509 憑證] 行的齒輪。
- 4 設定 X.509 憑證表單。

星號表示必填文字方塊。所有其他文字方塊均為選填。

選項	說明
啟用 X.509 憑證	將 [否] 變更為 是 可啟用憑證驗證。
*根憑證和中繼 CA 憑證	按一下 選取 以選取要上傳的憑證檔案。您可選取多個已編碼為 DER 或 PEM 的根 CA 和中繼 CA 憑證。
啟用憑證撤銷	將 [否] 變更為 是 可啟用憑證撤銷檢查。撤銷檢查會導致已撤銷使用者憑證的使用者無法驗證。
使用來自憑證的 CRL	選取此核取方塊，可使用由核發憑證的 CA 所發行的憑證撤銷清單 (CRL) 來驗證憑證的狀態 (已撤銷或未撤銷)。
CRL 位置	輸入要從中擷取 CRL 的伺服器檔案路徑或本機檔案路徑
啟用 OCSP 撤銷	選取此核取方塊，以使用線上憑證狀態通訊協定 (OCSP) 憑證驗證通訊協定瞭解憑證的撤銷狀態。

選項	說明
若 OCSP 失敗則使用 CRL	如果您同時設定 CRL 和 OCSP，您可以選取此方塊，以在 OCSP 檢查無法使用時回復為使用 CRL。
傳送 OCSP Nonce	如果您希望在回應中傳送 OCSP 要求的唯一識別碼，請選取此核取方塊。
OCSP URL	如果您已啟用 OCSP 撤銷，請輸入用於撤銷檢查的 OCSP 伺服器位址。
使用來自憑證的 OCSP URL	選取此方塊以使用 OCSP URL。
驗證之前啟用同意表單	選取此核取方塊以包含同意表單頁面，使其在使用者使用憑證驗證登入其 Workspace ONE 入口網站前顯示。

5 按一下儲存。

下一個

已設定 X.509 憑證驗證，且 Unified Access Gateway 應用裝置設定在負載平衡器後方時，請確定 Unified Access Gateway 已設定在負載平衡器使用 SSL 傳遞，並且未設定在負載平衡器終止 SSL。此組態可確保 SSL 信號交換會在 Unified Access Gateway 與用戶端之間進行，以便將憑證傳遞至 Unified Access Gateway。

取得憑證授權機構憑證

針對您使用者和管理員提供的智慧卡上的所有受信任使用者憑證，您必須取得所有適用的 CA (憑證授權機構) 憑證。這些憑證包含根憑證，而且，如果使用者的智慧卡憑證是由中繼憑證授權機構發給的，則可以包含中繼憑證。

如果您沒有使用者和管理員所提供智慧卡上簽署憑證的 CA 根憑證或中繼憑證，您可以從 CA 簽署的使用者憑證或包含該憑證的智慧卡匯出憑證。請參閱 [從 Windows 取得 CA 憑證](#)。

程序

- ◆ 從以下其中一個來源取得 CA 憑證。
 - 執行 Microsoft 憑證服務的 Microsoft IIS 伺服器。請參閱 Microsoft TechNet 網站以取得在您組織中安裝 Microsoft IIS、發行憑證，及散佈憑證的相關資訊。
 - 信任 CA 的公用根憑證。這在已具備智慧卡基礎結構與標準化智慧卡散佈及驗證方法的環境中，是最常見的根憑證來源。

下一個

將根憑證、中繼憑證或兩者新增至伺服器信任存放區檔案。

從 Windows 取得 CA 憑證

如果您具有 CA 簽署的使用者憑證或包含憑證的智慧卡，則當 Windows 信任根憑證時，可以從 Windows 匯出根憑證。若使用者憑證的發行者為中繼憑證授權單位，您可匯出該憑證。

程序

- 1 如果使用者憑證在智慧卡上，請將智慧卡插入讀卡機中，將使用者憑證新增至您的個人存放區。
如果使用者憑證未出現在您的個人存放區中，請使用讀卡機軟體將使用者憑證匯出至檔案。在此程序的步驟 4 中使用此檔案。
- 2 在 Internet Explorer 中，選取工具 > 網際網路選項。
- 3 在內容索引標籤上，按一下憑證。
- 4 在個人索引標籤上，選取您要使用的憑證，並按一下檢視。
如果使用者憑證未出現在清單中，請按一下匯入手動從檔案匯入憑證。匯入憑證後，您便可以從清單中選取憑證。
- 5 在憑證路徑索引標籤中，選取樹狀結構頂端的憑證，並按一下檢視憑證。
如果已將使用者憑證簽署成為信任階層的一部分，則正在簽署的憑證可由另一個更高層級的憑證簽署。選取父憑證 (實際簽署使用者憑證的憑證) 作為您的根憑證。在某些情況下，發行者可能是中繼 CA。
- 6 在詳細資料索引標籤上，按一下複製到檔案。
憑證匯出精靈隨即出現。
- 7 按下一步 > 下一步，並輸入您要匯出的檔案名稱與位置。
- 8 按下一步將檔案儲存在指定的位置作為根憑證。

下一個

將 CA 憑證新增至伺服器信任存放區檔案。

在 Unified Access Gateway 中設定 RSA SecurID 驗證

將 Unified Access Gateway 應用裝置設為 RSA SecurID 伺服器中的驗證代理程式之後，您必須將 RSA SecurID 組態資訊新增至 Unified Access Gateway 應用裝置。

先決條件

- 確認 RSA 驗證管理員 (RSA SecurID 伺服器) 已安裝且正確設定。
- 從 RSA SecurID 伺服器下載壓縮的 `sdconf.rec` 檔案，並解壓縮伺服器組態檔。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下選取。
- 2 在 [一般設定] 的 [驗證設定] 區段中，按一下顯示。
- 3 按一下 [RSA SecurID] 行的齒輪。
- 4 設定 RSA SecurID 頁面。
設定 SecurID 頁面時需要在 RSA SecurID 伺服器上使用的資訊和產生的檔案。

選項	動作
啟用 RSA SecurID	將 [否] 變更為是 可啟用 SecurID 驗證。
*名稱	名稱為 <code>securid-auth</code> 。
*反覆運算的數目	輸入允許的驗證嘗試次數。這是使用 RSA SecurID Token 時，登入嘗試失敗次數的上限。預設為五次嘗試。 備註 當您設定多個目錄且利用額外的目錄實作 RSA SecurID 驗證時，請將 允許的驗證嘗試次數 設定為與每個 RSA SecurID 組態相同的值。如果值不同，SecurID 驗證將會失敗。
*外部主機名稱	輸入 Unified Access Gateway 執行個體的 IP 位址。輸入的值必須與將 Unified Access Gateway 應用裝置做為驗證代理程式新增至 RSA SecurID 伺服器時所用的值相符。
*內部主機名稱	在 RSA SecurID 伺服器中輸入指派給 IP 位址提示的值。
*伺服器組態	按一下 變更 以上傳 RSA SecurID 伺服器組態檔案。首先，您必須從 RSA SecurID 伺服器下載壓縮檔，並解壓縮伺服器組態檔 (依預設名稱為 <code>sdconf.rec</code>)。
*名稱 ID 尾碼	以 <code>@somedomain.com</code> 的形式輸入名稱識別碼。它可用來將其他內容 (例如網域名稱) 傳送至 RADIUS 伺服器或 RSA SecurID 伺服器。例如，如果使用者以 <code>user1</code> 的身分登入，則會將 <code>user1@somedomain.com</code> 傳送至伺服器。

設定 Unified Access Gateway 的 RADIUS

您可以設定 Unified Access Gateway，以便要求使用者使用 RADIUS 驗證。您會在 Unified Access Gateway 應用裝置上設定 RADIUS 伺服器資訊。

RADIUS 支援提供範圍廣泛的替代式雙因素 Token 型驗證選項。因為雙因素驗證解決方案 (例如 RADIUS) 可與安裝在不同伺服器上的驗證管理員搭配使用，您必須設定 RADIUS 伺服器，並可供 Identity Manager 服務存取

當使用者登入，且 RADIUS 驗證啟用時，瀏覽器中會顯示一個特殊的登入對話方塊。使用者在登入對話方塊中輸入其 RADIUS 驗證使用者名稱和密碼。如果 RADIUS 伺服器發出存取挑戰，則 Unified Access Gateway 會顯示對話方塊並提示輸入第二個密碼。目前支援的 RADIUS 挑戰限制為提示文字輸入。

使用者在對話方塊中輸入認證後，RADIUS 伺服器便可將 SMS 簡訊或電子郵件，或使用其他額外機制的文字，連同代碼傳送到使用者手機。使用者可將此文字與代碼輸入到登入對話方塊以完成驗證。

如果 RADIUS 伺服器提供從 Active Directory 匯入使用者的功能，則使用者可能會先看到要求提供 Active Directory 認證的提示，然後才會看到要求提供 RADIUS 驗證使用者名稱與密碼的提示。

設定 RADIUS 驗證

在 Unified Access Gateway 應用裝置上，您必須啟用 RADIUS 驗證、輸入來自 RADIUS 伺服器的組態設定，並將驗證類型變更為 RADIUS 驗證。

先決條件

- 確認要做為驗證管理員伺服器的伺服器已安裝 RADIUS 軟體並加以設定。設定 RADIUS 伺服器，然後從 Unified Access Gateway 設定 RADIUS 要求。請參閱 RADIUS 廠商的設定指南，以取得設定 RADIUS 伺服器的相關資訊。

需要下列 RADIUS 伺服器資訊。

- RADIUS 伺服器的 IP 位址或 DNS 名稱。
- 驗證連接埠號碼。驗證連接埠通常為 1812。
- 驗證類型。驗證類型包括 PAP (密碼驗證通訊協定)、CHAP (Challenge Handshake 驗證通訊協定)、MSCHAP1、MSCHAP2 (Microsoft Challenge Handshake 驗證通訊協定，版本 1 和 2)。
- 用於在 RADIUS 通訊協定訊息中加密和解密的 RADIUS 共用密碼。
- RADIUS 驗證所需的特定逾時和重試值

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在 [一般設定] 的 [驗證設定] 區段中，按一下**顯示**。
- 3 按一下 [RADIUS] 行的齒輪。

選項	動作
啟用 RADIUS	將 [否] 變更為 是 以啟用 RADIUS 驗證。
名稱*	名稱為 radius-auth
驗證類型*	輸入 RADIUS 伺服器支援的驗證通訊協定。PAP、CHAP、MSCHAP1 或 MSCHAP2 中的一個。
共用密碼*	輸入 RADIUS 共用密碼。
允許的驗證嘗試次數 *	使用 RADIUS 登入時，輸入登入嘗試失敗的次數上限。預設為三次嘗試。
對 RADIUS 伺服器的嘗試次數*	輸入重試嘗試的總數。如果主要伺服器未回應，服務會等待設定的時間經過後再次進行重試。
伺服器逾時 (以秒為單位)*	輸入 RADIUS 伺服器逾時 (以秒為單位)，在此時間之後，如果 RADIUS 伺服器未回應，即會傳送重試。
RADIUS 伺服器主機名稱*	輸入 RADIUS 伺服器的主機名稱或 IP 位址。
驗證連接埠*	輸入 RADIUS 驗證連接埠號碼。連接埠通常為 1812。
領域首碼	(選用) 使用者帳戶位置稱為領域。 如果您指定領域首碼字串，則該名稱傳送至 RADIUS 伺服器時會放置在使用者名稱的開頭。例如，如果輸入的使用者名稱為 jdoe ，並指定領域首碼 DOMAIN-1\ ，則會將使用者名稱 DOMAIN-1jdoe 傳送至 RADIUS 伺服器。如果不設定這些欄位，則只會傳送所輸入的使用者名稱。
領域尾碼	(選用) 如果設定領域尾碼，則字串會放置在使用者名稱的結尾。例如，如果尾碼為 @myco.com ，則會傳送使用者名稱 jdoe@myco.com 至 RADIUS 伺服器。

選項	動作
名稱 ID 尾碼	以 <code>@somedomain.com</code> 的形式輸入名稱識別碼。它可用來將其他內容 (例如網域名稱) 傳送至 RADIUS 伺服器或 RSA SecurID 伺服器。例如, 如果使用者以 <code>user1</code> 的身分登入, 則會將 <code>user1@somedomain.com</code> 傳送至伺服器。
登入頁面複雜密碼提示	輸入要在使用者登入頁面的訊息中顯示的文字字串, 可引導使用者輸入正確的 RADIUS 密碼。例如, 如果將此欄位設定為 先 AD 密碼然後 SMS 密碼 , 登入頁面訊息會顯示 先輸入您的 AD 密碼然後輸入 SMS 密碼 。預設的文字字串為 RADIUS 密碼 。
啟用次要伺服器	將 [否] 變更為 是 可針對高可用性設定次要 RADIUS 伺服器。如步驟 3 所述, 設定次要伺服器資訊。

4 按一下 **儲存**。

在 Unified Access Gateway 中設定 RSA 調適性驗證

與針對 Active Directory 僅進行使用者名稱及密碼驗證相比, RSA 調適性驗證的實作能提供更強大的多重要素驗證。調適性驗證能根據風險程度和原則來監控及驗證使用者登入嘗試。

啟用調適性驗證時, 系統會使用在 RSA Policy Management 應用程式中設定之風險原則內的風險指標, 以及調適性驗證的 Unified Access Gateway 組態來判斷是否使用者名稱和密碼來驗證使用者, 抑或是需要其他資訊來驗證使用者。

驗證支援的 RSA 調適性驗證方法

Unified Access Gateway 中支援的 RSA 調適性驗證強式驗證方法, 即為透過電話、電子郵件或 SMS 簡訊和挑戰問題進行的額外驗證。您可以在服務上啟用可提供的 RSA 調適性驗證方法。RSA 調適性驗證原則會判斷該使用哪個次要驗證方法。

額外驗證是一種需要隨著使用者名稱和密碼傳送額外驗證的程序。當使用者在 RSA 調適性驗證伺服器中註冊時, 他們需要根據伺服器組態提供電子郵件地址、電話號碼或兩者。若需要額外驗證, RSA 調適性驗證伺服器會透過提供的通道傳送一次性密碼。除了使用者名稱和密碼之外, 使用者還需要輸入該密碼。

當使用者在 RSA 調適性驗證伺服器中註冊時, 挑戰問題會要求使用者回答一系列的問題。您可以設定要回答的註冊問題數目, 以及登入頁面上出現的挑戰問題數目。

向 RSA 調適性驗證伺服器註冊使用者

您必須先在 RSA 調適性驗證資料庫中佈建使用者, 才能使用調適性驗證來進行驗證。當使用者首次以他們的使用者名稱和密碼登入時, 系統會將他們新增至 RSA 調適性驗證資料庫。根據您在服務中設定 RSA 調適性驗證的方式, 當使用者登入時, 系統會要求他們提供電子郵件地址、電話號碼、文字訊息服務號碼 (SMS), 或是要求他們設定挑戰問題的回應。

備註 RSA 調適性驗證不允許在使用者名稱中使用國際字元。如果您想要允許在使用者名稱中使用多位元組字元, 請聯絡 RSA 支援以設定 RSA 調適性驗證和 RSA 驗證管理員。

在 Unified Access Gateway 中設定 RSA 調適性驗證

若要為服務設定 RSA 調適性驗證，您需要啟用 RSA 調適性驗證；選取要套用的調適性驗證方法，以及新增 Active Directory 連線資訊和憑證。

先決條件

- 以用於次要驗證的驗證方法正確設定了 RSA 調適性驗證。
- 有關 SOAP 端點位址和 SOAP 使用者名稱的詳細資料。
- 可供使用的 Active Directory 組態資訊和 Active Directory SSL 憑證。

程序

- 1 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 2 在 [一般設定] 的 [驗證設定] 區段中，按一下**顯示**。
- 3 按一下 [RSA 調適性驗證] 行的齒輪。
- 4 選取適合環境的設定。

備註 星號表示必填欄位。其他欄位為選填。

選項	說明
啟用 RSA AA 介面卡	將 [否] 變更為 是 以啟用 RSA 調適性驗證。
名稱*	名稱為 rsaaa-auth。
SOAP 端點*	輸入 RSA 調適性驗證介面卡和服務整合所需的 SOAP 端點位址。
SOAP 使用者名稱*	輸入用來簽署 SOAP 訊息的使用者名稱和密碼。
SOAP 密碼*	輸入 RSA 調適性驗證 SOAP API 密碼。
RSA 網域	輸入調適性驗證伺服器的網域位址。
啟用 OOB 電子郵件	選取 [是] 以啟用利用電子郵件訊息傳送一次性密碼給使用者的頻外驗證。
啟用 OOB SMS	選取 [是] 以啟用利用 SMS 簡訊傳送一次性密碼給使用者的頻外驗證。
啟用 SecurID	選取 [是] 以啟用 SecurID。系統會要求使用者輸入其 RSA Token 和密碼。
啟用密碼問題	如果您要使用註冊和挑戰問題來進行驗證，請選取 [是]。
註冊問題數目*	輸入使用者註冊驗證介面卡伺服器時需要設定的問題數目。
挑戰問題數目*	輸入使用者必須正確回答才能登入的挑戰問題數目。
允許的驗證嘗試次數*	輸入在認定驗證失敗之前，要向嘗試登入之使用者顯示挑戰問題的次數。
目錄類型*	Active Directory 是唯一支援的目錄。
使用 SSL	如果您的目錄連線使用 SSL，請選取 [是]。您可以在 [目錄憑證] 欄位中新增 Active Directory SSL 憑證。
伺服器主機*	輸入 Active Directory 主機名稱。
伺服器連接埠	輸入 Active Directory 連接埠號碼。
使用 DNS 服務位置	如果目錄連線使用 DNS 服務位置，請選取 [是]。
基本 DN	輸入要開始搜尋帳戶的 DN。例如，OU=myUnit,DC=myCorp,DC=com。

選項	說明
繫結 DN*	輸入可搜尋使用者的帳戶。例如， CN=binduser,OU=myUnit,DC=myCorp,DC=com
繫結密碼	輸入繫結 DN 帳戶的密碼。
搜尋屬性	輸入包含使用者名稱的帳戶屬性。
目錄憑證	若要建立安全的 SSL 連線，請將目錄伺服器憑證新增至文字方塊。若為多重伺服器案例，請新增憑證授權機構的根憑證。
使用 STARTTLS	將 [否] 變更為是可使用 STARTTLS。

5 按一下**儲存**。

產生 Unified Access Gateway SAML 中繼資料

您必須在 Unified Access Gateway 應用裝置上產生 SAML 中繼資料並與伺服器交換中繼資料，才能建立智慧卡驗證需要的共同信任。

安全性聲明標記語言 (SAML) 是一種以 XML 為基礎的標準，用於說明以及交換不同安全網域之間的驗證與授權資訊。在被稱為 SAML 聲明的 XML 文件中，SAML 在身分識別提供者與服務提供者之間傳遞使用者相關資訊。在此案例下，Unified Access Gateway 是身分識別提供者而伺服器是服務提供者。

先決條件

- 在 Unified Access Gateway 應用裝置上設定時鐘 (UTC)，讓應用裝置擁有正確的時間。例如，開啟 Unified Access Gateway 虛擬機器上的主控台視窗，然後使用箭頭按鈕選取正確的時區。另外，確認 ESXi 主機的時間是否與 NTP 伺服器同步。確認在應用裝置虛擬機器上執行的 VMware Tools 會將虛擬機器的時間與 ESXi 主機的時間同步。

重要事項 如果 Unified Access Gateway 應用裝置上的時鐘不符合伺服器主機上的時鐘，智慧卡驗證可能會無法運作。

- 取得可用來簽署 Unified Access Gateway 中繼資料的 SAML 簽署憑證。

備註 如果您的設定中有多部 Unified Access Gateway 應用裝置，VMware 建議您建立並使用特定的 SAML 簽署憑證。在此情況下，所有應用裝置都必須設定為使用相同的簽署憑證，以便伺服器可以接受來自任何一部 Unified Access Gateway 應用裝置的聲明。使用特定的 SAML 簽署憑證時，來自所有應用裝置的 SAML 中繼資料皆相同。

- 將 SAML 簽署憑證轉換為 PEM 格式檔案，再將 .pem 檔案轉換為單行格式 (如果您尚未這麼做)。請參閱 [將憑證檔案轉換為單行 PEM 格式](#)。

程序

- 在管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 在 [進階設定] 區段中，按一下 **SAML 身分識別提供者設定**齒輪圖示。
- 選取**提供憑證**核取方塊。
- 若要新增私密金鑰檔案，請按一下**選取**並瀏覽至憑證的私密金鑰檔案。

- 5 若要新增憑證鏈結檔案，請按一下**選取**並瀏覽至憑證鏈結檔案。
- 6 按一下**儲存**。
- 7 在 [主機名稱] 文字方塊中，輸入主機名稱並下載身分識別提供者設定。

建立其他服務提供者使用的 SAML 驗證器

在 Unified Access Gateway 應用裝置上產生 SAML 中繼資料後，您可以將該資料複製到後端服務提供者。複製此資料給服務提供者是建立 SAML 驗證器程序的一部分，如此可讓 Unified Access Gateway 做為身分識別提供者。

對於 Horizon Air 伺服器，請參閱產品說明文件中的特定指示。

將服務提供者 SAML 中繼資料複製到 Unified Access Gateway

在建立並啟用 SAML 驗證器以便讓 Unified Access Gateway 可以做為身分識別提供者後，即可在該後端系統上產生 SAML 中繼資料，並使用中繼資料在 Unified Access Gateway 應用裝置上建立服務提供者。此資料交換可在身分識別提供者 (Unified Access Gateway) 和後端服務提供者 (例如 Horizon Connection Server) 之間建立信任。

先決條件

確認已在後端服務提供者伺服器上為 Unified Access Gateway 建立 SAML 驗證器。

程序

- 1 擷取服務提供者 SAML 中繼資料 (通常是 XML 檔案的形式)。

如需相關指示，請參閱服務提供者的說明文件。

不同的服務提供者有不同的程序。例如，您必須開啟瀏覽器並輸入 `https://connection-server.example.com/SAML/metadata/sp.xml` 之類的 URL

接著，您可以使用**另存新檔**命令，將網頁儲存為 XML 檔案。此檔案的內容開頭為下列文字：

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

- 2 在 Unified Access Gateway 管理員 UI 的 [手動設定] 區段中，按一下**選取**。
- 3 在 [進階設定] 區段中，按一下 **SAML 伺服器提供者設定** 齒輪圖示。
- 4 在 [服務提供者名稱] 文字方塊中，輸入服務提供者名稱。
- 5 在 [中繼資料 XML] 文字方塊中，貼上您在步驟 1 中建立的中繼資料檔案。
- 6 按一下**儲存**。

Unified Access Gateway 和服務提供者現在可以交換驗證與授權資訊了。

疑難排解 Unified Access Gateway 部署

7

您可以使用多種程序來診斷及修正於環境中部署 Unified Access Gateway 時遭遇的問題。

您可以使用疑難排解程序來調查此類問題的成因，並試圖自行修正問題，或者您也可以向 VMware 技術支援取得協助。

本章節討論下列主題：

- [監視所部署服務的健全狀況](#)
- [疑難排解部署錯誤](#)
- [疑難排解錯誤：身分識別橋接](#)
- [疑難排解錯誤：Cert-to-Kerberos](#)
- [疑難排解端點符合性](#)
- [疑難排解管理員 UI 中的憑證驗證](#)
- [疑難排解防火牆和連線問題](#)
- [疑難排解根使用者登入問題](#)
- [從 Unified Access Gateway 應用裝置收集記錄](#)
- [匯出 Unified Access Gateway 設定](#)
- [疑難排解錯誤：Content Gateway](#)

監視所部署服務的健全狀況

您可以從管理員 UI 的 [Edge 設定] 中快速查看您部署的服務已設定、啟動並成功執行。

圖 7-1 健全狀況檢查



服務前方會顯示一個圓形。色彩編碼如下所示。

- 黑色圓形 - 設定尚未設定。
- 紅色圓形 - 服務已關閉。
- 琥珀色圓形 - 服務部分執行中。
- 綠色圓形 - 服務正在執行中，且並未發生任何問題。

疑難排解部署錯誤

當您在環境中部署 Unified Access Gateway 時，可能會遭遇難題。您可以使用多種程序來診斷及修正部署時發生的問題。

執行從網際網路下載的指令碼時出現安全警告

請確認 PowerShell 指令碼是您要執行的指令碼，然後從 PowerShell 主控台執行以下命令：

```
unblock-file .\uagdeploy.ps1
```

找不到 ovftool 命令

請確認您已在 Windows 機器上安裝 OVF Tool 軟體，且該軟體安裝在指令碼預期的位置。

內容 netmask1 中的網路無效

這則訊息可能會指出 netmask0、netmask1 或 netmask2。請確認已在 netInternet、netManagementNetwork 及 netBackendNetwork 這三個網路各自的 INI 檔案中設定值。

關於作業系統識別碼不受支援的警告訊息

警告訊息顯示指定的作業系統識別碼 SUSE Linux Enterprise Server 12.0 64-bit (id:85) 在選定主機上不受支援。它與以下 OS 識別碼對應：Other Linux (64-bit)。

請忽略這則警告訊息。它會自動與支援的作業系統對應。

定位器無法參考物件錯誤

這則錯誤通知您 vSphere OVF Tool 使用的 `target=` 值不是 vCenter Server 環境所需的正確值。請使用 <https://communities.vmware.com/docs/DOC-30835> 列示的表格，以取得用來參考 vCenter 主機或叢集之目標格式的範例。最上層物件的指定方式如下：

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/
```

物件現可列出要在下一層使用的可能名稱。

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/Cluster1/
or
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esxhost1
```

在目標中使用的資料夾名稱、主機名稱及叢集名稱有區分大小寫。

錯誤訊息：無法從工作階段擷取用戶端憑證：sessionId

- 檢查是否已在瀏覽器中正確安裝使用者憑證。
- 檢查是否已在浏览器和 Unified Access Gateway 上啟用預設 TLS 通訊協定 1.1 版和 1.2 版。

無法使用在 Chrome 瀏覽器上啟動的 VMware vSphere Web Client 部署 Unified Access Gateway ova

您必須在 vSphere Web Client 上用來部署 ova 檔案的瀏覽器上安裝用戶端整合外掛程式。在 Chrome 瀏覽器上安裝外掛程式後，系統會顯示一則錯誤訊息，指出瀏覽器並未安裝，且將不允許您在來源位置中輸入 ova 檔案 URL。這是 Chrome 瀏覽器方面的問題，與 Unified Access Gateway ova 無關。建議您使用不同的瀏覽器來部署 Unified Access Gateway ova。

無法使用 VMware vSphere HTML4/5 Web Client 部署 Unified Access Gateway ova

您可能會遇到錯誤，例如為內容指定的值無效。此問題與 Unified Access Gateway ova 無關。建議您改用 vSphere FLEX 用戶端來部署 ova。

無法使用 VMware vSphere 6.7 HTML5 Web Client 部署 Unified Access Gateway ova

您可能會在 VMware vSphere 6.7 HTML5 Web Client 的部署內容頁面上發現遺漏的欄位。此問題與 Unified Access Gateway ova 無關。建議您改用 vSphere FLEX 用戶端來部署 ova。

無法從 VMware Identity Manager 透過 Chrome 啟動 XenApp

部署 Unified Access Gateway 作為來自 VMware Identity Manager 的 Web Reverse Proxy 之後，您可能無法從 Chrome 瀏覽器啟動 XenApp。

請遵循下列步驟來解決此問題。

- 1 若要從 VMware Identity Manager 服務停用功能旗標 `orgUseNonNPAPIForCitrixLaunch`，請使用下列 REST API。

```
PUT https://fqdn/SAAS/jersey/manager/api/tenants/settings?tenantId=tenantname
{ "items": [ { "name": "orgUseNonNPAPIForCitrixLaunch", "value": "false" } ] }
with the following two headers:
Content-Type application/vnd.vmware.horizon.manager.tenants.tenant.config.list+json
Authorization HZN value_of_HZN_cookie_for_admin_user
```

- 2 等待 24 小時使變更生效，或重新啟動 VMware Identity Manager 服務。
 - 若要在 Linux 上重新啟動服務，請登入虛擬應用裝置並執行下列命令：`service horizon-workspace restart`。
 - 若要在 Windows 上重新啟動服務，請執行下列指令碼：`install_dir\usr\local\horizon\scripts\horizonService.bat restart`。

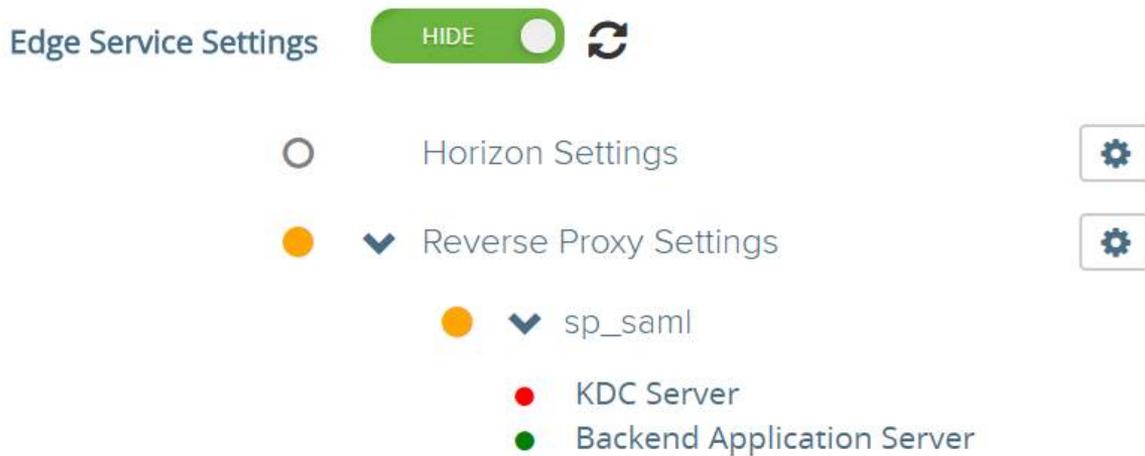
疑難排解錯誤：身分識別橋接

當您在環境中設定對 Kerberos 的憑證或對 Kerberos 的 SAML 時，可能會遭遇難題。您可以使用多種程序來診斷和修正這些問題。

監控 KDC 伺服器 and 後端應用程式伺服器的健全狀況。

您可以從管理員 UI 的 [Edge 設定] 中快速查看您部署的服務已設定、啟動並成功執行。

圖 7-2 健全狀況檢查 - Reverse Proxy 設定



服務前方會顯示一個圓形。色彩編碼如下所示。

- 紅色圓形：如果狀態為紅色，則可能表示下列其中一種情況。
 - Unified Access Gateway 與 Active Directory 之間的連線問題
 - Unified Access Gateway 與 Active Directory 之間的連接埠封鎖問題。
-
- 備註** 確認 Active Directory 機器中已開放 TCP 和 UDP 連接埠 88。
-
- 已上傳的 Keytab 檔案中主體名稱和密碼認證可能不正確。
 - 綠色圓形：如果狀態為綠色，則表示 Unified Access Gateway 可以使用 Keytab 檔案中提供的認證來登入 Active Directory。

建立 Kerberos 內容時發生錯誤：時鐘誤差太大

此錯誤訊息：

```
ERROR: "wsportal.WsPortalEdgeService[createKerberosLoginContext: 119][39071f3d-9363-4e22-a8d9-5e288ac800fe]: Error creating kerberos context.
Identity bridging may not work
javax.security.auth.login.LoginException: Clock skew too great"
```

顯示於 Unified Access Gateway 時間與 AD 伺服器時間顯著不同步時。請重設 AD 伺服器上的時間以符合 Unified Access Gateway 上的確切 UTC 時間。

建立 Kerberos 內容時發生錯誤：名稱或服務不明

此錯誤訊息：

```
wsportal.WsPortalEdgeService[createKerberosLoginContext: 133][]: Error creating kerberos context.
Identity bridging may not work
javax.security.auth.login.LoginException: Name or service not known
```

顯示於 Unified Access Gateway 無法連線至設定的領域，或使用 Keytab 檔案中所提供的使用者詳細資料無法連線至 KDC 時。請確認下列項目：

- Keytab 檔案使用正確的 SPN 使用者帳戶密碼產生並上傳至 Unified Access Gateway
- 已將後端應用程式 IP 位址和主機名稱正確新增至主機項目。

接收使用者：user@domain.com 的 Kerberos Token 時發生錯誤，錯誤：Kerberos 委派錯誤：方法名稱：gss_acquire_cred_impersonate_name：未指定的 GSS 失敗。次要代碼可能會提供更多資訊

"Kerberos Delegation Error: Method name: gss_acquire_cred_impersonate_name: Server not found in Kerberos database"

如果顯示此訊息，請檢查是否：

- 網域之間有信任關係。
- 目標 SPN 名稱已正確設定。

疑難排解錯誤：Cert-to-Kerberos

當您在環境中設定 Cert-to-Kerberos 時，可能會遭遇難題。您可以使用多種程序來診斷和修正這些問題。

錯誤訊息：內部錯誤。請連絡管理員

檢查 /opt/vmware/gateway/logs/authbroker.log 中的訊息

```
"OSCP validation of CN=clientCert, OU=EUC, O=<org name>, ST=<state name>, C=IN failed with "Could not send OSCP request to responder: Connection refused (Connection refused) , will attempt CRL validation"
```

這表示「X.509 憑證」中設定的 OSCP URL 無法連線或不正確。

OCSP 憑證無效時發生錯誤

```
"revocation.RevocationCheck: OSCP validation of CN=clientCert failed with "Could not verify signing certificate for OSCP responder:http://asdkad01/ocsp". will attempt CRL validation."
```

顯示於上傳了無效的 OCSP 憑證或是 OCSP 憑證已撤銷時。

OCSP 回應驗證失敗時發生錯誤

```
"WARN ocsf.BouncyCastleOCSPHandler: Failed to verify OCSP response:  
CN=asdkAD01.Asdk.ADrevocation.RevocationCheck: 08/23 14:25:49,975" [tomcat-http--26]  
WARN revocation.RevocationCheck: OCSP validation of CN=clientCert failed with "Could  
not verify signing certificate for OCSP responder: http://asdkad01/ocsp". will  
attempt CRL validation."
```

有時會在 OCSP 回應驗證失敗時顯示。

錯誤訊息：無法從工作階段擷取用戶端憑證：<sessionId>

如果顯示此訊息：

- 請檢查 X.509 憑證設定並判斷是否已設定
- 如果已設定 X.509 憑證設定：請檢查用戶端瀏覽器上安裝的用戶端憑證，以查看是否由 [X.509 憑證] 設定中 [根憑證和中繼 CA 憑證] 欄位上傳的相同 CA 所核發。

疑難排解端點符合性

當您在環境中部署端點符合性檢查提供者時，可能會遭遇難題。您可以使用多種程序來診斷及修正部署時發生的問題。

備註 `Esmanager.log` 會記錄用於符合性檢查之裝置的 MAC 位址相關資訊。如果裝置具有多個 NIC 或切換至不同網路，則在識別用於端點符合性檢查的 MAC 位址時相當實用。

Unified Access Gateway 會顯示「不正確的用戶端認證」

Unified Access Gateway 會呼叫 OPSWAT API 以驗證所提供的用戶端金鑰和用戶端密碼。如果認證不正確，則不會儲存設定，從而導致

不正確的用戶端認證

錯誤。

確認 [使用者名稱] 和 [密碼] 欄位中輸入正確的用戶端金鑰與用戶端密碼。

若要產生用戶端認證，請在此處登錄您的應用程式：<https://gears.opswat.com/o/app/register>。

Unified Access Gateway 會顯示「DNS 無法解析主機 `https://gears.opswat.com`」

使用 Ping 命令來探索您區域 `gears.opswat.com` 的 IP 位址。

然後，使用來自 Ping 命令的 IP 位址以建立 `https://gears.opswat.com` 的 `/etc/hosts` 項目。從管理員 UI 導覽至 Horizon 設定並為 View Edge Service 提供主機項目中的值。

Unified Access Gateway 會顯示「連線至主機 https://gears.opswat.com 時要求逾時」

如果 UAG 中的 gears.opswat.com 主機項目設定錯誤或 https://gears.opswat.com 不接受連線要求，則可能會發生此情況。

疑難排解管理員 UI 中的憑證驗證

如果您在驗證 PEM 格式的憑證時發生錯誤，請查閱此處的錯誤訊息以取得更多資訊。

以下是產生錯誤的可能案例清單。

錯誤	問題
PEM 格式無效。可能是由於 BEGIN 格式錯誤。請參閱記錄以取得詳細資料。	PrivateKey BEGIN 憑證無效。
PEM 格式無效。例外狀況訊息：找不到 ---END RSA PRIVATE KEY。請參閱記錄以取得詳細資料。	PrivateKey END 憑證無效。
PEM 格式無效。例外狀況訊息：建立 RSA 私密金鑰時發生問題：java.lang.IllegalArgumentException: 無法從 byte[]: corrupted stream 建構序列 - 找到超出界限的長度。請參閱記錄以取得詳細資料。	憑證中的 PrivateKey 已損毀。
無法從 PEM 字串剖析憑證。請參閱記錄以取得詳細資料。	PublicKey BEGIN 憑證無效。
遇到格式錯誤的 PEM 資料。請參閱記錄以取得詳細資料。	PublicKey END 憑證無效。
遇到格式錯誤的 PEM 資料。請參閱記錄以取得詳細資料。	憑證中的 PublicKey 已損毀。
沒有目標/結尾憑證可供建置鏈結。	沒有目標/結尾憑證。
無法建置憑證鏈結路徑，所有目標憑證皆無效。可能缺少中繼憑證/根憑證。	沒有可供建置的憑證鏈結。
不明確的錯誤：找到多個憑證鏈結，但不確定要傳回哪一個	有多個憑證鏈結。
無法建置憑證鏈結路徑 CertificateExpiredException: 憑證已於 20171206054737GMT+00:00 到期。請參閱記錄以取得詳細資料。	憑證已到期。

疑難排解防火牆和連線問題

您可以從 Unified Access Gateway 執行個體透過各種工具和命令 (例如 tcpdump 和 curl) 來監控、測試和疑難排解網路問題，例如防火牆和連線問題。

安裝並執行 tcpdump

tcpdump 是一項命令列工具，可用來分析 TCP 封包以進行疑難排解和測試。

如果您尚未在 Unified Access Gateway 執行個體上安裝 tcpdump，請從命令列執行下列命令以安裝 tcpdump：

```
/etc/vmware/gss-support/install.sh
```

下列範例顯示 `tcpdump` 的使用方式：

- 執行下列命令以監控通過特定連接埠的流量。

備註 如果您指定連接埠 **8443**，請確定外部防火牆並未封鎖 **UDP 8443**。

a `tcpdump -i eth0 -n -v udp port 8443`

b `tcpdump -i eth0 -n -v tcp port 8443`

c `tcpdump -i any -n -v port 22443`

- 執行下列命令以追蹤 **RADIUS** 伺服器往來於 **Unified Access Gateway** 的封包：

```
nslookup <radius-server-hostname>
tracert <radius-server-hostname>
tcpdump -i any -n -v port 1812
```

- 執行下列命令以追蹤 **RSA SecurID** 伺服器往來於 **Unified Access Gateway** 的封包：

```
nslookup <rsa-auth-server-hostname>
tracert <rsa-auth-server-hostname>
```

使用 curl 命令

您也可以使用 `curl` 命令擷取網路連線的相關資訊。

- 執行下列命令以測試後端連線伺服器或 **Web** 伺服器的連線：

```
curl -v -k https://<hostname-or-ip-address>:443/
```

您可以在 `esmanager.log` 檔案中檢視後端伺服器的連線問題：

```
07/14 07:29:03,882[nioEventLoopGroup-7-1]ERROR
view.ViewEdgeService[onFailure: 165][]: Failed to resolve hostname
address in proxyDestinationUrl:xref:mbxxx-cs.xyz.in
```

- 您無法使用 `tcpdump` 測試後端虛擬桌面平台 (例如 **PCoIP 4172** 和 **Blast 22443**) 的連線，因為在工作階段準備就緒之前，桌面平台不會接聽這些連接埠號碼。請檢視記錄以確認這些連接埠是否發生連線失敗。

- 針對 **Horizon** 架構通道 **TCP** 連線，請執行下列命令：

```
curl -v telnet://<virtualdesktop-ip-address>:32111
```

- 針對 **Horizon MMR/CDR** **TCP** 連線，請執行下列命令：

```
curl -v telnet://<virtualdesktop-ip-address>:9427
```

- 執行下列命令以測試從 **Unified Access Gateway** 到虛擬桌面平台的連接埠連線。執行此命令之前，請確保對虛擬桌面平台的工作階段處於作用中狀態。

```
curl -v telnet://<virtualdesktop-ip-address>:22443
```

PowerShell 命令

從 PowerShell 命令列執行下列命令以監控特定連接埠的連線：

- 1 `Test-NetConnection <uag-hostname-or-ip-address> -port 443`
- 2 `Test-NetConnection <uag-hostname-or-ip-address> -port 8443`
- 3 `Test-NetConnection <uag-hostname-or-ip-address> -port 4172`

疑難排解根使用者登入問題

如果您使用正確的使用者名稱和密碼，以根使用者身分登入 Unified Access Gateway 主控台，但卻收到「登入不正確」錯誤時，請檢查鍵盤對應問題，並重設根密碼。

發生登入錯誤的原因有以下幾種：

- 所使用的鍵盤並未根據 Unified Access Gateway 的鍵盤定義正確對應特定的密碼字元
- 密碼已過期。部署 OVA 檔案之後根密碼已過期 365 天。
- 在部署應用裝置時未正確設定密碼。這是舊版 Unified Access Gateway 的已知問題。
- 忘記密碼。

若要測試鍵盤的對應字元是否正確，請嘗試在「登入:」使用者名稱提示出現時輸入密碼。這可讓您檢視每個密碼字元，並找出解譯錯誤的字元。

若是其他原因，請重設應用裝置的根密碼。

備註 若要重設根密碼，您必須：

- 擁有 vCenter 的登入存取權
- 知道 vCenter 的登入密碼
- 擁有存取應用裝置主控台的權限

如果您為應用裝置設定了 Grub 2 開機載入器功能表密碼，則需要在此程序中輸入該密碼。

程序

- 1 從 vCenter 重新啟動應用裝置，並立即連線至主控台。
- 2 當 Photon OS 啟動顯示畫面顯示時，按下 `e` 來輸入 GNU GRUB 編輯功能表

- 3 在 GNU GRUB 中編輯功能表中，移至開頭為 `linux` 行的結尾，接著新增空格，然後輸入 `/$photon_linux root=$rootpartition rw init=/bin/bash`。新增這些值後，GNU GRUB 編輯功能表看起來應完全類似下列：

```
GNU GRUB version 2.02~rc2

setparams 'Photon'

linux /$photon_linux root=$rootpartition rw init=/bin/bash
if [ -f /$photon_initrd ]; then
  initrd /$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```

備註 針對 FIPS 應用裝置，`fips=1` 應如顯示般保留在行的結尾。

```
GNU GRUB version 2.02~rc2

setparams 'Photon'

linux /$photon_linux root=$rootpartition rw init=/bin/bash fips=1
if [ -f /$photon_initrd ]; then
  initrd /$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```

- 4 按 F10 鍵，然後在 `bash` 命令提示字元中輸入 `passwd` 來變更密碼。

```
passwd New password: Retype new password: passwd: password updated successfully
```

```
[ OK ] Started Cleaning Up and Shutting Down Daemons.
[ OK ] Started Cleanup udevd DB.
[ OK ] Reached target Switch Root.
Starting Switch Root...
root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# _
```

- 5 在命令提示字元中，取消掛接檔案系統 `umount/`
- 6 將應用裝置重新開機 `reboot -f`
- 在應用裝置重新開機後，使用新設定的密碼以根使用者身分登入。

關於 Grub2 密碼

您可以在根使用者登入中使用 Grub2 密碼。

從 Unified Access Gateway 3.1 開始，依預設系統會設定 Grub2 編輯密碼。

使用者名稱為 `root`，而密碼則與您在部署 Unified Access Gateway 時所設定的根密碼相同。此密碼一律不會重設，除非您登入機器並明確進行重設。

備註 透過任何命令登入機器並手動變更根密碼時將不會重設 Grub2 密碼。這兩個密碼為互斥。系統僅在部署期間才會為兩者設定相同的密碼 (使用 UAG 3.1 版及更新版本時)。

從 Unified Access Gateway 應用裝置收集記錄

從管理員 UI 的 [支援設定] 區段下載 `UAG-log-archive.zip` 檔案。該 ZIP 檔案包含來自 Unified Access Gateway 應用裝置的所有記錄。

設定記錄層級

您可以透過管理員 UI 來管理記錄層級設定。移至 [支援設定](#) 頁面，並選取 [記錄層級設定](#)。可以產生的記錄層級為「資訊」、「警告」、「錯誤」和「偵錯」。記錄層級依預設會設定為「資訊」。

記錄層級所收集資訊類型的說明如下所示。

表格 7-1. 記錄層級

層級	收集的資訊類型
資訊	「資訊」層級指出可突顯服務進度的資訊訊息。
錯誤	「錯誤」層級指出可能仍允許服務繼續執行的錯誤事件。
警告	「警告」層級指出可能有害但通常可復原或可忽略的情況。
偵錯	指定一般有助於偵錯問題的事件、檢視或操縱應用裝置的內部狀態，以及在您的環境中測試部署案例。

收集記錄

從管理員 UI 的 [支援設定] 區段下載記錄 ZIP 檔案。

這些記錄檔是從應用裝置的 `/opt/vmware/gateway/logs` 目錄收集而來。

下表包含 ZIP 檔案中所含各種檔案的說明。

表格 7-2. 包含有助於疑難排解之系統資訊的檔案

檔案名稱	說明	Linux 命令 (如果適用)
<code>rpm-version.log</code>	Unified Access Gateway 應用裝置的版本。	
<code>ipv4-forwardrules</code>	在應用裝置上設定的 IPv4 轉送規則。	
<code>df.log</code>	包含應用裝置上的磁碟空間使用量相關資訊。	<code>df -a -h --total</code>
<code>netstat.log</code>	包含開啟的連接埠和現有 TCP 連線的相關資訊。	<code>netstat -anop</code>
<code>netstat-s.log</code>	從應用裝置建立時開始的網路統計資料 (已傳送/已接收的位元組等)。	<code>netstat -s</code>
<code>netstat-r.log</code>	在應用裝置上建立的靜態路由。	<code>netstat -r</code>

表格 7-2. 包含有助於疑難排解之系統資訊的檔案 (繼續)

檔案名稱	說明	Linux 命令 (如果適用)
uag_config.json、 uag_config.ini	Unified Access Gateway 應用裝置的完整組態，以 json 和 ini 檔案的形式顯示所有設定。	
ps.log	包含下載記錄時正在執行的處理程序。	ps -elf --width 300
ifconfig.log	應用裝置的網路介面組態。	ifconfig -a
free.log	下載記錄時的 RAM 可用性。	free
top.log	下載記錄時依記憶體使用量排序的處理程序清單。	top -b -o %MEM -n 1
iptables.log	IPv4 的 IP 表格。	iptables-save
ip6tables.log	IPv6 的 IP 表格。	ip6tables-save
w.log	運作時間、機器目前的使用者及其處理程序的相關資訊。	w
systemctl.log	目前在應用裝置上執行的服務清單	systemctl
resolv.conf	用來將本機用戶端直接連線至所有已知的 DNS 伺服器	

表格 7-3. Unified Access Gateway 的記錄檔

檔案名稱	說明	Linux 命令 (如果適用)
supervisord.log	主管 (Edge Service Manager 的管理員、管理員和 AuthBroker) 記錄。	
esmanager-x.log、 esmanager-std- out.log	Edge Service Manager 記錄，顯示在應用裝置上執行的後端處理程序。	
audit.log	所有管理員使用者作業的稽核記錄。	
authbroker.log	包含處理 Radius 和 RSA SecurID 驗證之 AuthBroker 處理程序所產生記錄訊息。	
admin.log、admin- std-out.log	管理員 GUI 記錄。包含在連接埠 9443 上提供 Unified Access Gateway REST API 之處理程序的記錄訊息。	
bsg.log	包含 Blast 安全閘道的記錄訊息。	
SecurityGateway_xxx. log	包含 PCoIP 安全閘道的記錄訊息。	
utserver.log	包含 UDP 通道伺服器所產生的記錄訊息。	
activeSessions.csv	作用中 Horizon 或 WRP 工作階段的清單。	
haproxy.conf	包含用於 TLS 連接埠共用的 HA Proxy 組態參數。	
vami.log	包含在部署期間執行 vami 命令以設定網路介面所產生的記錄訊息。	
content- gateway.log、 content-gateway- wrapper.log、 0.content-gateway- YYYY-mm.dd.log.zip	包含來自 Content Gateway 的記錄訊息。	

表格 7-3. Unified Access Gateway 的記錄檔 (繼續)

檔案名稱	說明	Linux 命令 (如果適用)
admin-zookeeper.log	包含用來儲存 Unified Access Gateway 組態之資料層的相關記錄訊息。	
tunnel.log	包含作為 XML API 處理的一部分之通道處理程序的記錄訊息。您必須在 Horizon 設定中啟用通道才能檢視此記錄。	
admin-auditlog.log	包含使用者登入或變更密碼、登入和登出時成功及失敗嘗試時的日期、時間、使用者名稱、來源 IP 位址、管理員 UI 的 SysLog 稽核 URL，以及要求裝載變更的相關資訊。	
tunnel-snap.tar.gz	包含 VMware Tunnel 伺服器 Proxy 記錄檔的 Tarball。	
aw-appliance-agent.log	應用裝置代理程式 (用於啟動 AirWatch 服務) 記錄檔。	
config.yml	包含 Content Gateway 組態和記錄層級詳細資料。	
smb.conf	包含 SMB 用戶端組態。	
smb-connector.conf	包含 SMB 通訊協定和記錄層級詳細資料。	

結尾是「-std-out.log」的記錄檔包含寫入至各種處理程序之 stdout 的資訊，而這些記錄檔通常是空白檔案。

匯出 Unified Access Gateway 設定

從管理員 UI 匯出 JSON 和 INI 格式的 Unified Access Gateway 組態設定。

您可以匯出所有 Unified Access Gateway 組態設定，並將其儲存為 JSON 或 INI 格式。您可以透過 Powershell 指令碼，使用匯出的 INI 檔案來部署 Unified Access Gateway。

程序

- 1 導覽至 **支援設定 > 匯出 Unified Access Gateway 設定**。
- 2 按一下 **JSON** 或 **INI**，以想要的格式匯出 Unified Access Gateway 設定。若要同時以這兩種格式儲存設定，請按一下 **記錄封存** 按鈕。

依預設檔案會儲存在您的 [下載] 資料夾中。

疑難排解錯誤：Content Gateway

當您在環境中設定 Content Gateway 時，可能會遭遇難題。您可以使用此程序來診斷和修正問題。

使用在 NetApp 伺服器上主控之共用的使用者同步、下載和上傳問題。

若要手動變更組態檔，請遵循下列步驟：

- 1 登入 vSphere Client
- 2 開啟設定 Content Gateway 所在的 Unified Access Gateway 主控台。
- 3 導覽至 /opt/airwatch/content-gateway/conf

- 4 編輯 `config.yml` 檔案
- 5 將參數 `aw.fileshare.jcifs.active` 的旗標值修改為 `true`。預設值為 `false`。
- 6 使用命令重新啟動 Content Gateway 服務

```
$ service content-gateway restart
```