



Cisco WebEx Meetings Server 管理指南 2.0 版

第一次發佈日期: 2014 年 02 月 06 日

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



目錄

Cisco WebEx Meetings Server 安裝指南 1

將 VMware vSphere 與系統搭配使用 3

使用 VMware vSphere 3

將 ESXi 主機設定為使用 NTP 伺服器 4

使用 VMware vCenter 來建立備份 4

使用 VMware vCenter 來擷取快照 5

將現有 VMDK 檔案附加至新虛擬機器 6

系統的網路檢查清單 9

適用於具有公開存取和非水平分割 DNS 之系統的網路檢查清單 9

適用於具有公開存取和水平分割 DNS 之系統的網路檢查清單 10

適用於沒有公開存取之系統的網路檢查清單 10

使用自動部署安裝系統 11

系統部署的一般概念 12

安裝檢查清單 13

自動部署所需資訊 13

透過 VMware vSphere 用戶端部署 OVA 檔案 16

OVA 部署失敗後複查您的網路配置 28

選取用於設定的語言 28

確認部署 29

確認您的系統的大小 29

選擇要安裝的系統 29

選擇系統部署的類型 30

提供 VMware vCenter 認證 30

選擇用於您的「媒體」虛擬機器的 vCenter 設定 31

輸入「媒體」虛擬機器的網路資訊 31

新增公開存取 32

選擇用於您的網際網路反向 Proxy 的 vCenter 設定 32

輸入網際網路反向 Proxy 的網路資訊	33
輸入公用 VIP 位址	33
輸入專用 VIP 位址	34
WebEx 網站和 WebEx 管理 URL	34
輸入 WebEx 網站和管理 URL	36
確認您的網路已正確設定	36
部署您的虛擬機器	36
檢查您的系統	37
使用手動部署安裝系統	39
系統部署的一般概念	39
安裝檢查清單	40
手動部署所需資訊	41
透過 VMware vSphere 用戶端部署 OVA 檔案	42
OVA 部署失敗後複查您的網路配置	54
選取用於設定的語言	54
確認部署	55
確認您的系統的大小	55
選擇要安裝的系統	55
選擇系統部署的類型	56
新增公開存取	56
輸入公用 VIP 位址	57
輸入專用 VIP 位址	57
WebEx 網站和 WebEx 管理 URL	58
輸入 WebEx 網站和管理 URL	59
確認您的網路已正確設定	59
部署您的虛擬機器	60
檢查您的系統	61
設定郵件伺服器、時區及地區設定	63
設定系統的郵件伺服器	63
設定系統的時區和地區設定	64
確認郵件伺服器、時區和地區設定	64
設定系統的第一個管理員帳戶	64
測試系統	65

在安裝後變更系統	67
新增 HA、更新、升級或擴充系統	67
準備系統更改程序	68
新增高可用性系統	69
使用自動部署新增 HA 系統	69
使用手動部署新增 HA 系統	71
確認您的主系統和您的 HA 系統版本相同	73
新增高可用性系統	74
測試系統	75
將系統擴充為較大的系統大小	77
準備系統擴充	77
準備系統更改程序	78
使用自動部署來擴充系統	79
使用手動部署來擴充系統	83
測試系統	86
更新系統	87
更新系統	87
連接 CD/DVD 光碟機中的 ISO 映像檔	88
繼續更新程序	89
完成更新	90
升級系統	91
準備升級	91
自動升級系統	92
手動升級系統	94
測試系統	96
授權重新主控與升級	96
存取 GLO 請求表單	96
在軟體升級或系統擴充之後重新主控授權	97
儲存授權請求	97
註冊要重新主控的授權	97
軟體升級後升級授權	98
Cisco WebEx Meetings Server 設定指南	101
使用儀表板	103

關於儀表板	103
檢視和編輯警報	105
檢視資源歷史記錄	107
使用「進行中的會議」圖表解決會議問題	107
檢視會議趨勢	108
檢視會議清單	109
排定維護時段	110
變更排定的維護時段	111
關於維護模式	112
開啓或關閉維護模式	114
管理使用者	117
關於管理使用者	117
關於逗號和 Tab 分隔的檔案	118
CSV 檔案欄位值	119
新增使用者	124
編輯使用者	124
啓動使用者	125
停用使用者	125
使用匯入停用使用者	126
匯入使用者	126
匯出使用者	127
使用匯出檔案將使用者匯入至新系統	127
設定追蹤碼	128
編輯追蹤碼	129
設定目錄整合	129
同步化使用者群組	133
使用 CUCM 配置 AXL Web 服務及目錄同步	134
使用 CUCM 來配置 LDAP 整合與驗證	135
傳送電子郵件給使用者	135
設定系統	137
設定系統內容	137
變更您的虛擬機器設定	137
配置高可用性系統	138

新增高可用性系統	138
移除高可用性系統	140
元件故障時的系統行為	140
變更虛擬 IP 位址	141
設定公開存取	142
新增對系統的公開存取	142
移除公開存取	143
擴充系統大小	144
設定一般設定	145
變更網站設定	145
變更管理設定	146
設定伺服器	146
設定郵件伺服器	146
設定 SMTP 伺服器	147
設定儲存伺服器	148
使用災害復原功能	149
設定 SNMP 設定	151
設定社群字串	152
新增社群字串	152
編輯社群字串	153
設定 USM 使用者	154
新增 USM 使用者	154
編輯 USM 使用者	155
設定通知目標	156
編輯通知目標	157
設定通知目標	157
管理授權	158
關於授權	158
透過使用 License Manager 來履行授權	164
使用 eFulfilment 來履行授權	165
透過聯絡 TAC 來履行授權	166
配置設定	167
設定您的公司資訊	168

配置您的品牌設定	169
移除公司標誌	170
設定您的會議設定	170
關於會議安全性	171
關於設定音訊設定	172
首次配置您的音訊設定	172
配置您的音訊設定	175
設定您的視訊設定	177
設定您的行動裝置設定	177
設定服務品質 (QoS)	178
關於 QoS 標記	178
設定密碼	179
配置您的一般密碼設定	180
設定您的使用者密碼設定	180
設定您的會議密碼	181
配置您的電子郵件設定	183
關於電子郵件範本	183
設定您的下載設定	206
關於下載	207
管理憑證	207
產生 SSL 憑證	208
產生憑證簽署請求 (CSR)	209
匯入 SSL 憑證	210
匯出 SSL 憑證	211
匯出適用於行動裝置的 SSL 憑證	211
下載您的 CSR 和私密金鑰	212
產生自我簽署憑證	213
還原 SSL 憑證	214
匯入 SSO IdP 憑證	215
匯入安全通信會議憑證	215
設定使用者階段作業安全性	217
配置同盟單一登入 (SSO) 設定	217
停用 SSO	220

設定您的雲端功能	220
設定虛擬機器安全性	221
更新加密金鑰	221
關於 FIPS	221
啟用與 FIPS 相容的加密	222
停用與 FIPS 相容的加密	223
管理報告	225
下載每月報告	225
關於每月報告	225
產生自訂詳細資訊報告	227
關於自訂詳細資訊報告	227
使用支援功能	231
自訂您的日誌	231
設定遠端支援帳戶	232
停用遠端支援帳戶	233
使用會議測試	234
使用系統資源測試	234



第 部分

Cisco WebEx Meetings Server 安裝指南

- [將 VMware vSphere 與系統搭配使用, 第 3 頁](#)
- [系統的網路檢查清單, 第 9 頁](#)
- [使用自動部署安裝系統, 第 11 頁](#)
- [使用手動部署安裝系統, 第 39 頁](#)
- [設定郵件伺服器、時區及地區設定, 第 63 頁](#)
- [在安裝後變更系統, 第 67 頁](#)
- [新增高可用性系統, 第 69 頁](#)
- [將系統擴充為較大的系統大小, 第 77 頁](#)
- [更新系統, 第 87 頁](#)
- [升級系統, 第 91 頁](#)



第 1 章

將 VMware vSphere 與系統搭配使用

- 使用 VMware vSphere, 第 3 頁
- 將 ESXi 主機設定為使用 NTP 伺服器, 第 4 頁
- 使用 VMware vCenter 來建立備份, 第 4 頁
- 使用 VMware vCenter 來擷取快照, 第 5 頁
- 將現有 VMDK 檔案附加至新虛擬機器, 第 6 頁

使用 VMware vSphere

系統的虛擬機器是使用 VMware vSphere 部署的。根據下列限制，Cisco WebEx Meetings Server 必須安裝在 VMware 虛擬機器上。

- 使用 VMware vSphere 5.0、5.0 更新 1 或 5.1。
不支援 vSphere 的較早發行版。
- 使用 VMware ESXi 5.0、5.0 更新 1 或 5.1。
使用較早 ESXi 版本會導致混淆未明確列出問題之 **不支援硬體** 的相關錯誤訊息。
- 請確保已設定 ESXi 主機的 DNS 伺服器，可以解析該 ESXi 主機中部署的虛擬機器的主機名稱。
- 您必須使用 VMware vCenter，來管理在其中部署 Cisco WebEx Meetings Server 系統的 ESXi 主機。
- 關閉虛擬機器時，請一律為每個虛擬機器選取 **Power > Shut Down Guest**。（請勿使用 **Power Off** 選項。）



附註

如需受支援 VMware 配置的相關詳細資料，請參閱 *Cisco WebEx Meetings Server* 系統需求。

將 ESXi 主機設定為使用 NTP 伺服器

系統使用 ESXi 主機來設定時間。將 ESXi 主機設定為使用網路時間通訊協定 (NTP) 以進行時鐘同步。



附註 這是高階程序。如需詳細指示，請參閱 VMware ESXi 文件。



重要須知 務必從 ESXi 主機設定 NTP 設定。

程序

- 步驟 1 使用 vSphere 用戶端，選取庫存面板中的 ESXi 主機。
- 步驟 2 選取 **Configuration** 標籤，然後選取「Software」區段中的 **Time Configuration**。
- 步驟 3 選取面板右上方的 **Properties**。
- 步驟 4 選取 **NTP Client Enabled**。
- 步驟 5 選取 **Options** 以設定 NTP 伺服器設定。
Cisco 建議您選取 **Start and stop with host**，以減少 ESXi 主機時間不正確的可能性。

使用 VMware vCenter 來建立備份

備份是運用 VMware 技術及 SAN 型資料傳送的傳統檔案系統。VMware® Data Recovery 可以建立虛擬機器的備份，而不會中斷它們的使用或者它們提供的資料和服務。Data Recovery 使用虛擬機器設備及用戶端外掛程式來管理和還原備份。備份設備是以開放式虛擬化格式 (OVF) 提供。Data Recovery 外掛程式需要 VMware vSphere Client。

Data Recovery 會管理現有備份，並移除較舊的備份。它也支援刪除重複作業來移除多餘資料。執行任何系統更改程序之前，我們建議您使用 VMware Data Recovery（隨附於 VMware vSphere 5.0 版）或 vSphere Data Protection（隨附於 vSphere 5.1 版）來建立每部虛擬機器的備份。（除了 vSphere Essentials Kit，VMware Data Recovery/vSphere Data Protection 還包含在 VMware vSphere 中。如需相關資訊，請參閱 http://www.vmware.com/pdf/vdr_11_admin.pdf。）

此外，也可以使用儲存伺服器來建立備份。如需相關資訊，請參閱[設定儲存伺服器](#)。

與備份不同，虛擬機器快照是系統在特定時間點的圖片。基於效能原因，建議您使用備份並將虛擬機器備份保留在與包含虛擬機器的實體磁碟機不同的儲存體位置。如需快照和已知效能問題的相關資訊，請參閱[使用 VMware vCenter 來擷取快照](#)。

程序

- 步驟 1** 將系統置於維護模式。如需完整的詳細資料，請參閱[關於維護模式, 第 112 頁](#)。請確保沒有活動中的會議，且確保您所選的時間對使用者的影響最低。
- 步驟 2** 遵循 VMware vSphere 文件中的指示，並使用 VMware Data Recovery（自 vSphere 5.1 版起稱為 VMware vSphere Data Protection）建立系統和各虛擬機器的備份。
如需此備份的完整詳細資訊，請參閱《*VMware Data Recovery* 管理指南》或《*vSphere Data Protection* 管理指南》。
- 附註** Cisco 建議您在完成系統更改程序、測試過系統，並對結果滿意之後刪除備份。

使用 VMware vCenter 來擷取快照

虛擬機器快照可用來在執行系統更改程序之後，快速復原虛擬機器。快照是系統在特定時間點的圖片，和備份不同（請參閱[使用 VMware vCenter 來建立備份](#)）。建議您除了取得快照之外，應該另行備份系統。



附註

如果原始虛擬機器磁碟檔遺失，則無法使用快照來復原虛擬機器。

快照是儲存在包含您虛擬機器的實體磁碟機上。如果您不及時刪除這些快照，您的最終使用者可能會因影響虛擬機器效能的已知問題，而遭遇音訊和視訊品質降低。因此，基於效能原因，我們建議您使用備份或將虛擬機器備份保留在與包含虛擬機器的實體磁碟機不同的儲存體位置。此外，快照可用於更新，但對於系統升級，我們建議您刪除所有快照並備份原始系統。（如需取得有關 VMware 快照的此已知問題的更多資訊，請移至 VMware 網站並閱讀白皮書《*Best Practices for Running VMware vSphere on Network Attached Storage*》。如需相關資訊，您也可以在 VMware 知識庫中搜尋快照影響效能。）

執行大多數系統更改程序之前，Cisco 建議您備份系統（特別是在執行升級時）或對每個虛擬機器製作快照（特別是在執行更新時）。可以使用 VMware Data Recovery（自 vSphere 5.1 版起稱為 VMware vSphere Data Protection）備份系統或擷取每部虛擬機器的快照。（除了 vSphere Essentials Kit，VMware Data Recovery/vSphere Data Protection 還包含在 VMware vSphere 中。）

出於效能原因，請確保將虛擬機器快照保留在與包含虛擬機器的實體磁碟機不同的儲存體位置。請務必讀取特定程序的準備部分。Cisco 列出了每個程序的特定注意事項。



記住

如果您的系統是由多個虛擬機器組成，請選取 **Power > Shut Down Guest**，然後擷取系統中每部虛擬機器的快照。給每部虛擬機器的快照標示相同的字首，例如 8 月 20 日，這樣您就可以知道這些快照是在同一時間取得的。



附註

Cisco 建議您保留快照的時間不超過 24 小時。如果您想要長時間保留它們，請改為建立備份。如需 VMware Data Recovery（自 vSphere 5.1 版起稱為 VMware vSphere Data Protection）的相關資訊，請參閱[使用 VMware vCenter 來建立備份](#)，第 4 頁。

程序

- 步驟 1 將系統置於維護模式。如需完整的詳細資訊，請參閱[關於維護模式](#)，第 112 頁。請確保沒有活動中的會議，且確保您所選的時間對使用者的影響最低。
- 步驟 2 在 VMware vCenter 上，為每個虛擬機器選取 **Power > Shut Down Guest**。
- 步驟 3 為每個虛擬機器選取 **Snapshot > Take Snapshot**。
- 步驟 4 輸入快照的名稱，然後選取確定。

下一步動作

- 完成程序並測試您的系統，以確認該程序執行成功。
- 如果您需要還原為快照，請確定每部虛擬機器的快照都是在相同時間擷取的。開啓具有不相符快照的系統電源可能會導致資料庫毀損。

將現有 VMDK 檔案附加至新虛擬機器

本節說明如何使用 VMware vCenter 將 VMDK 檔案從現有「管理」虛擬機器附加至新的「管理」虛擬機器。

雖然移動虛擬磁碟 VMDK 檔案有多種原因，但本節僅重點說明有關將資料從一個「管理」虛擬機器移至另一個「管理」虛擬機器的程序。在擴充或升級系統時，您將使用此程序。（我們重複使用儲存在管理虛擬機器的 Hard disk 4 上的系統資料。）



注意

建立 Hard disk 4 VMDK 檔案的副本，然後將它直接複製到升級或擴充系統中管理虛擬機器的虛擬機器資料夾中。如果您僅連接 Hard disk 4，則資料仍然儲存在舊管理虛擬機器的虛擬機器資料夾中。如果您意外刪除 vCenter 庫存中的現有「管理」虛擬機器，則您目前的系統會無法存取 Hard disk 4。



附註

如果您使用的是直接連接儲存 (DAS)，則必須將虛擬機器 VMDK 檔案移轉至新「管理」虛擬機器可以存取它的 LUN。



附註

我們將系統更改程序之前的「管理」虛擬機器稱為「現有的」管理虛擬機器。將擴充或升級之後的「管理」虛擬機器稱為「新的」管理虛擬機器。

程序

- 步驟 1 導覽 VMware vCenter 中的庫存，並尋找適合您系統的現有「管理」虛擬機器。
- 步驟 2 在虛擬機器名稱上按一下滑鼠右鍵，並選取 **Edit Settings...**。
顯示 **Virtual Machine Properties** 視窗。
- 步驟 3 選取 **Hardware** 標籤，然後選取 **Hard disk 4**。
- 步驟 4 為供將來參考，請將 **Disk File** 位置複製並貼上至其他文件。
這會指定 VMware vCenter 中該 VMDK 檔案的位置。
字串類似於 [EMC-LUN10-RAID5] webex-sysA-admin/webex-sysA-admin_3-000001.vmdk。
如果之前已升級了系統，則檔案名稱不會遵循現有虛擬機器的命名慣例。
- 步驟 5 請注意並記下 Hard disk 4 的儲存體位置，及虛擬機器資料夾的名稱。
資料夾名稱字串類似於 [EMC-LUN8-RAID5] webex-sysB-admin。
- 步驟 6 關閉 **Edit Settings...** 視窗，而不做任何變更。
- 步驟 7 將 vCenter 檢視切換為資料存放區和資料存放區叢集檢視。選取 **Inventory > View > Datastores and Datastore Clusters**。
- 步驟 8 選取現有「管理」虛擬機器所在的儲存體位置 (透過步驟 5)，並選取 **Browse this datastore**。
- 步驟 9 選取新部署的「管理」虛擬機器所在的儲存體位置 (針對擴充或升級的系統)，並選取 **Browse this datastore**。
- 步驟 10 將兩個資料存放區的瀏覽器視窗 (針對現有的與新的「管理」虛擬機器) 並排排列，使您能夠同時查看這兩個「管理」虛擬機器的資料夾。
- 步驟 11 開啓這兩個虛擬機器的資料夾，並將 VMDK 檔案從現有「管理」虛擬機器資料夾複製到新「管理」虛擬機器資料夾。
 - a) 在現有「管理」虛擬機器資料夾中，找到與 Hard disk 4 相關聯的 VMDK 檔案。請參閱步驟 4 中記下的檔案位置，以確認準確性。
 - b) 在檔案上按一下滑鼠右鍵，並選取 **複製**。
 - c) 在新「管理」虛擬機器資料夾內按一下滑鼠右鍵，並選取 **貼上**。
當貼上作業完成時，關閉這兩個資料存放區視窗。
 - d) 選取 **View > Inventory > Hosts and Clusters**，將 vCenter 檢視返回主機和叢集清單。
- 步驟 12 導覽 VMware vCenter 中的庫存，並尋找適合您系統的新 (擴充或升級) 管理虛擬機器。
- 步驟 13 在新部署虛擬機器的名稱上按一下滑鼠右鍵，並選取 **Edit Settings...**。
顯示 **Virtual Machine Properties** 視窗。
- 步驟 14 選取 **Hardware** 標籤，然後選取 **Hard disk 4**。
- 步驟 15 選取 **Remove**。
此動作不會立即移除虛擬機器。而是會排定移除現有虛擬機器。
- 步驟 16 選取 **Add**。

會顯示 **Add Hardware** 精靈。

步驟 17 選取 **Hard Disk**，然後選取 **Next**。

步驟 18 選取 **Use an existing virtual disk**，然後選取 **Next**。

步驟 19 選取瀏覽，並導覽至新擴充或升級的「管理」虛擬機器所在的資料存放區。導覽至新「管理」虛擬機器的資料夾。連按兩下此資料夾，然後選取在步驟 11 中作為複製來源的虛擬磁碟。選取確定。

步驟 20 在 **Virtual Device Node** 下拉清單中選取 **SCSI (0:3)**，然後選取 **Next**。

步驟 21 複查您的變更，如果正確無誤，則選取 **Finish**。否則，選取 **Back** 並修復任何錯誤。精靈完成後，您將在 **Hardware** 標籤中看到一個標記用於添加的新磁碟。

步驟 22 透過選取確定確認新增和移除操作。

步驟 23 在 VMware vCenter **Recent Tasks** 窗格中檢視此虛擬機器重新設定作業，確保沒有錯誤。



第 2 章

系統的網路檢查清單

- 適用於具有公開存取和非水平分割 DNS 之系統的網路檢查清單, 第 9 頁
- 適用於具有公開存取和水平分割 DNS 之系統的網路檢查清單, 第 10 頁
- 適用於沒有公開存取之系統的網路檢查清單, 第 10 頁

適用於具有公開存取和非水平分割 DNS 之系統的網路檢查清單

在部署系統期間，會顯示具有網路檢查清單鏈結的頁面。這些檢查清單提供了成功部署所需的 DNS 伺服器、防火牆及其他網路變更的摘要。在開始部署之前，請務必進行這些必要變更，就像我們在部署過程即將結束時進行網路連線檢查一樣。



附註

非水平分割 DNS 是公司最常用的 DNS 設定。如需取得有關非水平分割 DNS 的更多資訊，請參閱《Cisco WebEx Meetings Server 規劃指南》。



附註

如果您要部署大型系統，則必須選擇手動部署。

選取《Cisco WebEx Meetings Server 規劃指南》中正確的檢查清單。

- 自動部署：請參閱「適用於使用自動部署、公開存取及非水平分割 DNS 進行安裝或擴充的網路檢查清單」
- 手動部署：請參閱「適用於使用手動部署、公開存取及非水平分割 DNS 進行安裝或擴充的網路檢查清單」

適用於具有公開存取和水平分割 DNS 之系統的網路檢查清單

在部署系統期間，會顯示具有網路檢查清單鏈結的頁面。這些檢查清單提供了成功部署所需的DNS伺服器、防火牆及其他網路變更的摘要。在開始部署之前，請務必進行這些必要變更，就像我們在部署過程即將結束時進行網路連線檢查一樣。



附註

如果您要部署大型系統，則必須選擇手動部署。

選取《Cisco WebEx Meetings Server 規劃指南》中正確的檢查清單。

- 自動部署：請參閱「適用於使用自動部署、公開存取和水平分割 DNS 進行安裝和擴充的網路檢查清單」
- 手動部署：請參閱「適用於使用手動部署、公開存取和水平分割 DNS 進行安裝和擴充的網路檢查清單」

適用於沒有公開存取之系統的網路檢查清單

在部署系統期間，會顯示具有網路檢查清單鏈結的頁面。這些檢查清單提供了成功部署所需的DNS伺服器、防火牆及其他網路變更的摘要。在開始部署之前，請務必進行這些必要變更，就像我們在部署過程即將結束時進行網路連線檢查一樣。



附註

如果您要部署大型系統，則必須選擇手動部署。

選取《Cisco WebEx Meetings Server 規劃指南》中正確的檢查清單。

- 自動部署：請參閱「適用於使用自動部署且不提供公開存取進行安裝或擴充的網路檢查清單」
- 手動部署：請參閱「適用於使用手動部署、無公開存取進行安裝和擴充的網路檢查清單」



第 3 章

使用自動部署安裝系統

- [系統部署的一般概念, 第 12 頁](#)
- [安裝檢查清單, 第 13 頁](#)
- [自動部署所需資訊, 第 13 頁](#)
- [透過 VMware vSphere 用戶端部署 OVA 檔案, 第 16 頁](#)
- [選取用於設定的語言, 第 28 頁](#)
- [確認部署, 第 29 頁](#)
- [確認您的系統的大小, 第 29 頁](#)
- [選擇要安裝的系統, 第 29 頁](#)
- [選擇系統部署的類型, 第 30 頁](#)
- [提供 VMware vCenter 認證, 第 30 頁](#)
- [選擇用於您的「媒體」虛擬機器的 vCenter 設定, 第 31 頁](#)
- [輸入「媒體」虛擬機器的網路資訊, 第 31 頁](#)
- [新增公開存取, 第 32 頁](#)
- [選擇用於您的網際網路反向 Proxy 的 vCenter 設定, 第 32 頁](#)
- [輸入網際網路反向 Proxy 的網路資訊, 第 33 頁](#)
- [輸入公用 VIP 位址, 第 33 頁](#)
- [輸入專用 VIP 位址, 第 34 頁](#)
- [WebEx 網站和 WebEx 管理 URL, 第 34 頁](#)
- [輸入 WebEx 網站和管理 URL, 第 36 頁](#)
- [確認您的網路已正確設定, 第 36 頁](#)
- [部署您的虛擬機器, 第 36 頁](#)
- [檢查您的系統, 第 37 頁](#)

系統部署的一般概念

系統大小

•50 個並行使用者的系統

通常支援擁有 500 至 1000 個員工的公司

主要系統（沒有 HA）包含一個「管理」虛擬機器及一個選用的「網際網路反向 Proxy」（用於公開存取）

•250 個並行使用者的系統

通常支援擁有 2500 至 5000 個員工的公司

主要系統（沒有 HA）包含一個「管理」虛擬機器、一個「媒體」虛擬機器及一個選用的「網際網路反向 Proxy」（用於公開存取）

•800 個並行使用者的系統

通常支援擁有 8000 至 16,000 個員工的公司

主要系統（沒有 HA）包含一個「管理」虛擬機器、一個「媒體」虛擬機器及一個選用的「網際網路反向 Proxy」（用於公開存取）

•2000 個並行使用者的系統

通常支援擁有 20,000 至 40,000 個員工的公司

主要系統（沒有 HA）包含一個「管理」虛擬機器、三個「媒體」虛擬機器、兩個「Web」機器及一個選用的「網際網路反向 Proxy」（用於公開存取）

部署期間的使用規定

欄位名稱	描述
WebEx 網站 URL	使用者用於主持和出席會議的安全 http URL。
WebEx 管理 URL	管理員用於設定、監控及管理系統的安全 http URL。
公用 VIP	WebEx 網站 URL 的 IP 位址
專用 VIP	<ul style="list-style-type: none"> •管理網站 URL 的 IP 位址 •WebEx 網站 URL 的 IP 位址 (如果您使用水平分割 DNS，則僅適用於內部使用者)。

安裝檢查清單



限制

您必須使用 VMware vCenter，來管理在其中部署 Cisco WebEx Meetings Server 系統的 ESXi 主機。

網路變更

請參閱您的部署適用的網路檢查清單。有兩個考量：

- 公開存取：您的防火牆外部的使用者是否可以透過網際網路或行動裝置主持和存取會議。Cisco 建議使用公開存取，因為這樣能為您的行動辦公提供更好的使用者體驗。
- 您公司中 DNS 設定的類型：水平分割 DNS 或非水平分割 DNS（最常見的 DNS 設定）。如需取得有關這些 DNS 設定類型的更多資訊，請參閱《Cisco WebEx Meetings Server 規劃指南》。
- 從管理員桌面開啓連接埠 10200 至管理虛擬機器。
在部署期間 Web 瀏覽器使用連接埠 10200。

請為您的部署選取正確的檢查清單：

- [適用於具有公開存取和非水平分割 DNS 之系統的網路檢查清單, 第 9 頁](#)
- [適用於沒有公開存取之系統的網路檢查清單, 第 10 頁](#)
- [適用於具有公開存取和水平分割 DNS 之系統的網路檢查清單, 第 10 頁](#)

必填資訊



附註

如果您是執行自動部署（支援並行使用者人數為 50、250 及 800）系統或手動部署（支援所有系統大小），則所需資訊會有所不同。除非您要部署需要手動部署的 2000 位使用者系統，否則 Cisco 建議您選取自動部署。請參閱下面適當的鏈結。

請選擇以下其中一項，以取得部署類型所需資訊的檢查清單：

- [自動部署所需資訊, 第 13 頁](#)
- [手動部署所需資訊, 第 41 頁](#)

自動部署所需資訊

以下是您的系統所需的資訊 (依序列出)。



附註

請務必先將虛擬機器 FQDN、IP 位址、WebEx 和管理網站 URL 及 VIP 位址新增至您的 DNS 伺服器，然後再開始系統部署。我們會在部署期間使用此資訊來為您查找 IP 位址。

為了避免任何 DNS 問題，您可能要測試這些 URL 和 IP 位址，然後再開始 OVA 部署。否則，系統部署將會失敗，直到您更正這些錯誤為止。

欄位名稱	描述	系統的值
vCenter URL	您系統中虛擬機器的 vCenter 伺服器的安全 http 位址。	
vCenter 使用者名稱	要為系統部署虛擬機器的使用者名稱此使用者必須具有管理員特權：部署、設定、開啓或關閉，以及刪除虛擬機器。	
vCenter 密碼	vCenter 使用者的密碼。	
（僅限並行使用者人數為 250 和 800 的系統） ESXi 主機	媒體虛擬機器的 ESXi 主機。 附註 此 ESXi 主機必須與上述 vCenter URL 在相同的 vCenter 上。	
（僅限並行使用者人數為 250 和 800 的系統） 資料存放區	媒體虛擬機器的資料存放區。	
（僅限並行使用者人數為 250 和 800 的系統） 虛擬機器連接埠群組	媒體虛擬機器的連接埠群組。 附註 Cisco 建議您選擇為管理虛擬機器選取的相同連接埠群組。	
（僅限並行使用者人數為 250 和 800 的系統） 媒體虛擬機器的 FQDN	媒體虛擬機器的完整網域名稱（全部小寫字元）。	
（僅限並行使用者人數為 250 和 800 的系統） 媒體虛擬機器的 IPv4 位址	媒體虛擬機器的 IPv4 位址。我們將為此媒體虛擬機器自動查找相應的 IPv4 位址。	

欄位名稱	描述	系統的值
(僅限公開存取) ESXi 主機	<p>網際網路反向 Proxy 虛擬機器的 ESXi 主機。</p> <p>附註 Cisco 建議您選取與為管理及其他內部虛擬機器所選 ESXi 主機不同的 ESXi 主機。</p> <p>若要允許網際網路反向 Proxy 的流量，請確定 ESXi 主機已設定連接埠群組，該群組可以路由其 IP 位址由網際網路反向 Proxy 使用的 VLAN。</p>	
(僅限公開存取) 資料存放區	網際網路反向 Proxy 虛擬機器的資料存放區。	
(僅限公開存取) 虛擬機器連接埠群組	<p>網際網路反向 Proxy 虛擬機器的連接埠群組。</p> <p>附註 出於安全性考慮，Cisco 建議您選取與為管理虛擬機器所選連接埠群組不同的連接埠群組。</p>	
(僅限公開存取) 網際網路反向 Proxy 的 FQDN	「網際網路反向 Proxy」虛擬機器的完整網域名稱（全部小寫字元）。	
(僅限公開存取) 網際網路反向 Proxy IPv4 位址	網際網路反向 Proxy 虛擬機器的 IPv4 位址。我們將為此網際網路反向 Proxy 虛擬機器自動查找相應的 IPv4 位址。	
(僅限公開存取) IPv4 閘道	網際網路反向 Proxy 虛擬機器的 IPv4 閘道。	
(僅限公開存取) IPv4 子網路遮罩	網際網路反向 Proxy 虛擬機器的子網路遮罩。	
(僅限公開存取) 主要 DNS 伺服器 IPv4 位址	網際網路反向 Proxy 虛擬機器的 DNS 伺服器。	
(僅限公開存取) 次要 DNS 伺服器 IPv4 位址	(可選) 網際網路反向 Proxy 虛擬機器的其他 DNS 伺服器。	
公用 VIP	WebEx 網站 URL (網站使用者存取該 URL 來主持和出席會議) 的 IP 位址	

欄位名稱	描述	系統的值
專用 VIP	<ul style="list-style-type: none"> •管理網站 URL (管理員用來設定、監控及管理系統) 的 IP 位址 •WebEx 網站 URL 的 IP 位址 (如果您使用水平分割 DNS，則僅適用於內部使用者)。 	
WebEx 網站 URL	使用者用於主持和出席會議的安全 http URL (全部小寫字元)。	
WebEx 管理 URL	管理員用於設定、監控及管理系統的安全 http URL (全部小寫字元)。	

下一步動作

使用此資訊，在瀏覽器視窗中輸入部署 URL 來開始系統部署。(部署 URL 將顯示在管理虛擬機器的主控台視窗中。)



附註

如果在完成設定之前將系統重新開機，則會產生新的密碼，您必須將部署 URL 與新密碼一起使用。

透過 VMware vSphere 用戶端部署 OVA 檔案

在部署系統之前，您必須使用 VMware vSphere 用戶端為系統部署管理虛擬機器。



附註

提供了以下程序作為一般指導。在 OVA 部署期間看到的真實畫面，可能因 vCenter、儲存體和網路配置而與此程序稍有不同。請參閱 VMware vSphere 文件，以取得有關 OVA 精靈的完整資訊。

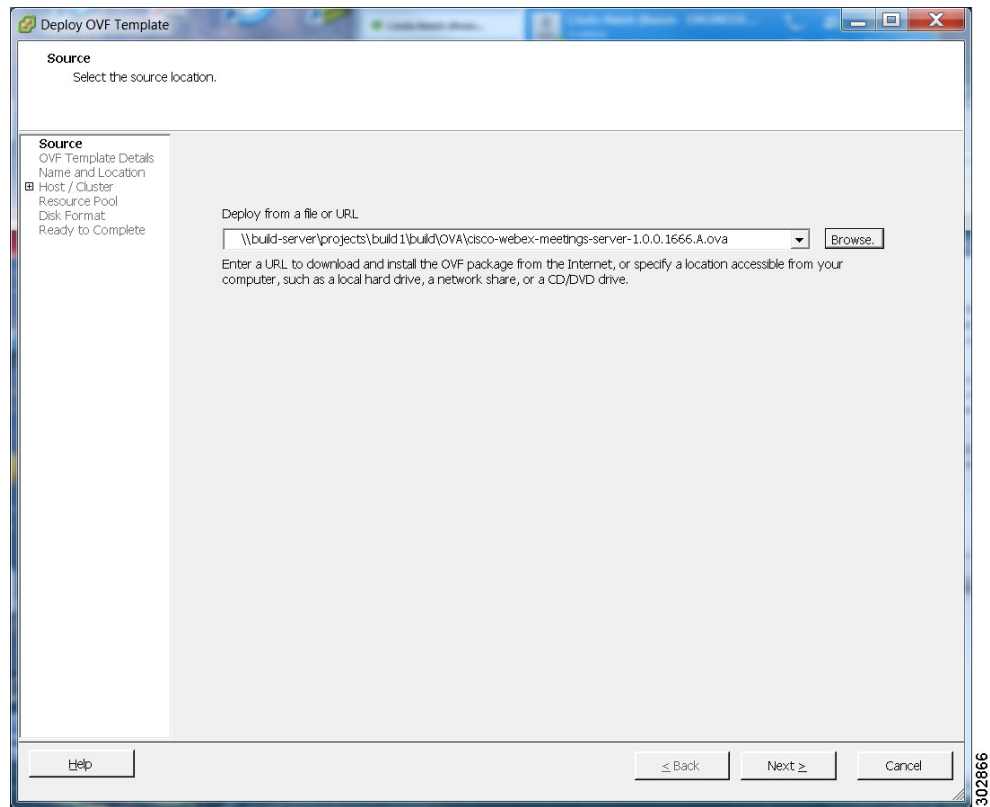
開始之前

請取得用於您系統的 Cisco WebEx Meetings Server OVA 檔案，並將此檔案置於可從 VMware vSphere 存取的位置。

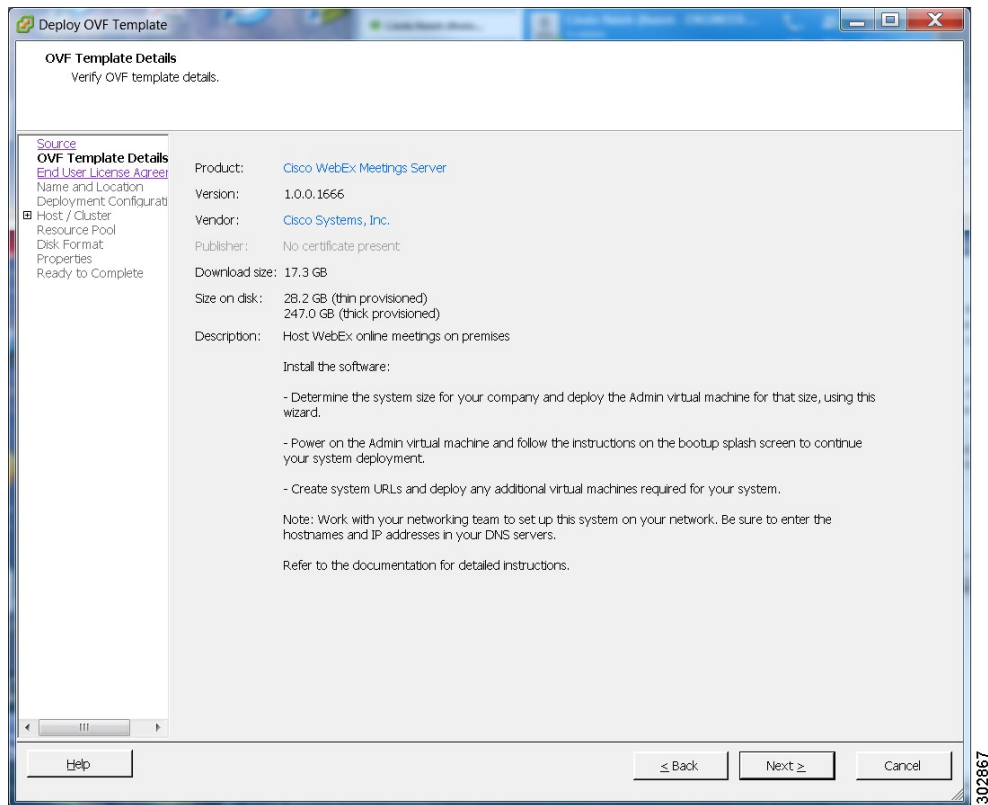
您必須使用 VMware vCenter，來管理在其中部署 Cisco WebEx Meetings Server 系統的 ESXi 主機。使用 vSphere 用戶端，登入 vCenter，及為管理虛擬機器部署 OVA 檔案。

程序

- 步驟 1** 登入您的 VMware vSphere 用戶端。
務必以包含管理員特權的使用者身份登入：部署、設定、開啓或關閉，以及刪除虛擬機器。

步驟 2 選取 File > Deploy OVF Template...**步驟 3 選取瀏覽，以導覽至 OVA 檔案的位置。選取 Next。**

您可以選取 **Cisco WebEx Meetings Server** 鏈結，以移至具有此系統相關詳細資訊的網頁。



步驟 4 閱讀「最終使用者授權協議」並選取**接受**，然後選取 **Next**。

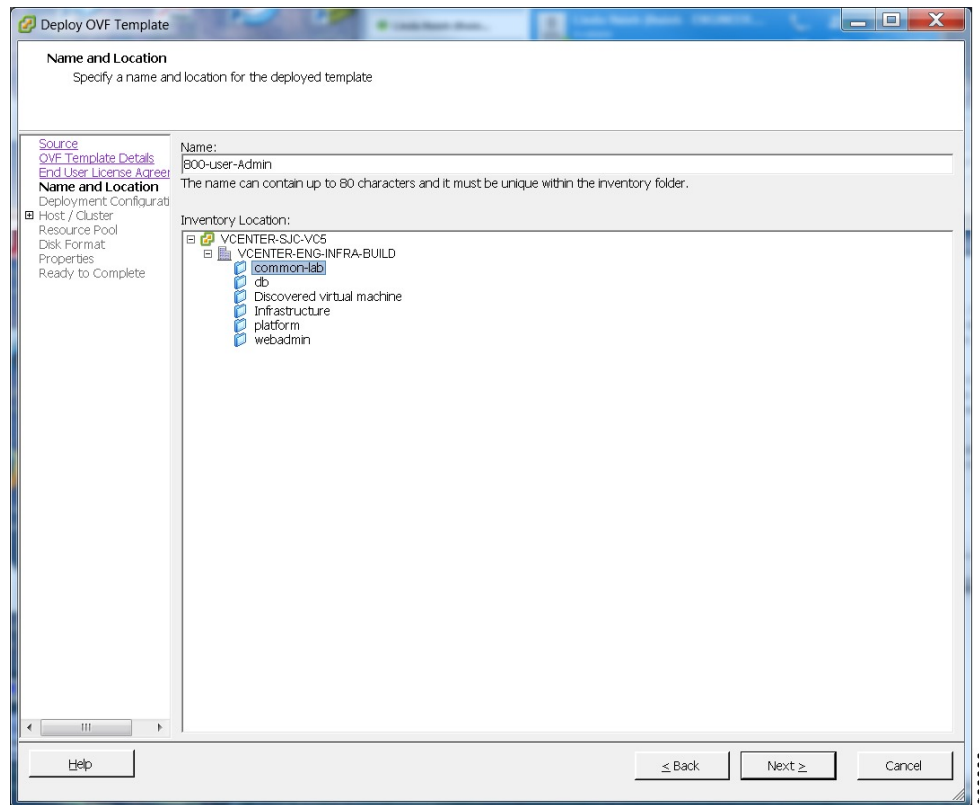
步驟 5 導覽至 vCenter 庫存中要放置管理虛擬機器的位置並選取此位置。

步驟 6 輸入適合您系統大小的虛擬機器名稱，然後選取**Next**。如需為您公司選取正確大小的相關資訊，請參閱[系統大小](#)。

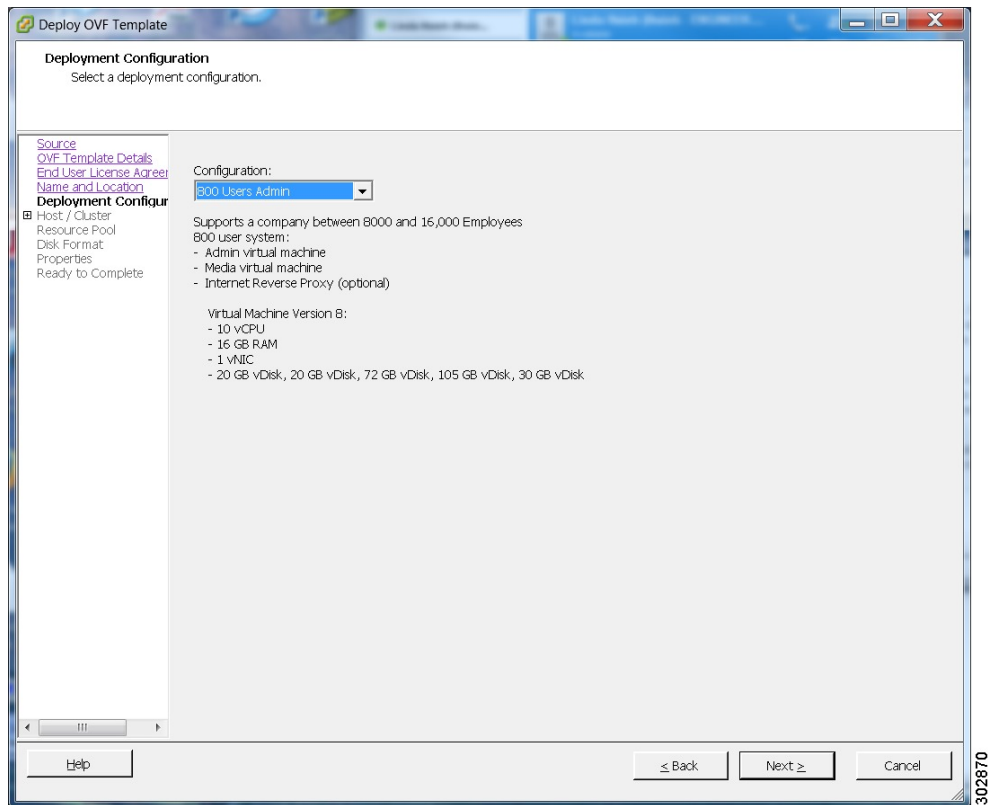
附註 您必須先部署管理虛擬機器，然後才部署任何其他虛擬機器。如果選取自動部署（建議），則我們將為您部署其他虛擬機器。如果您選擇手動部署（2000 個並行使用者的系統必須使用此選項），則在部署管理虛擬機器後，必須使用這個相同的精靈來部署其他虛擬機器。

Cisco 建議您在虛擬機器名稱中包含類型；例如，管理虛擬機器名稱中的「管理」，以能夠輕易在 vCenter 庫存中識別。

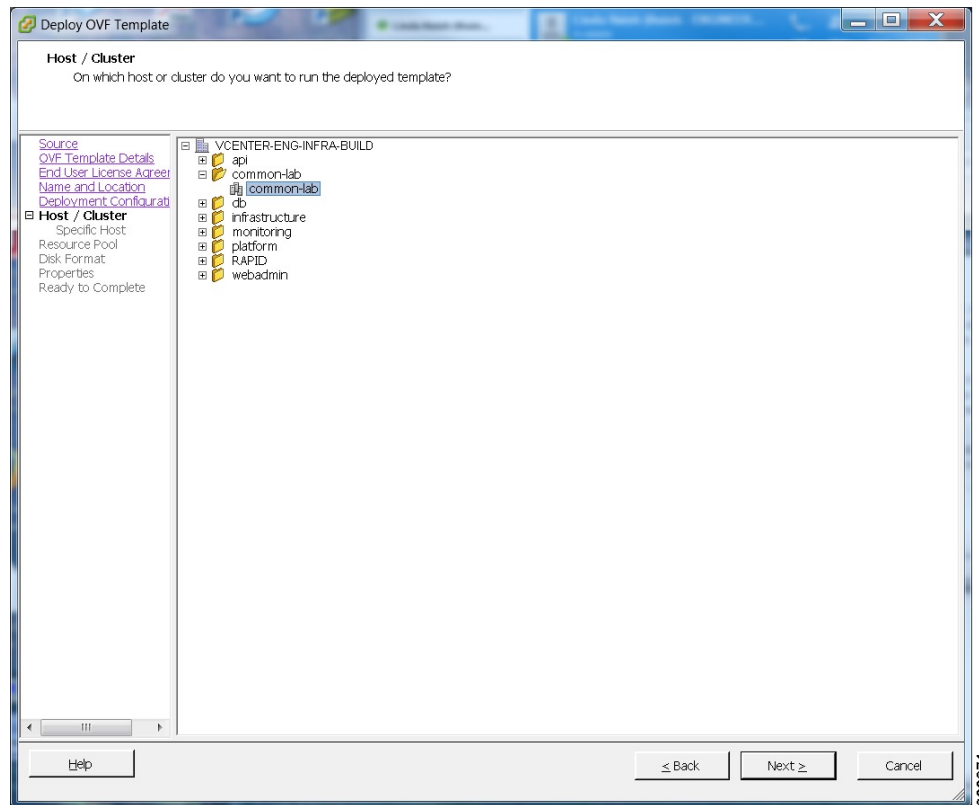
附註 您系統的所有內部虛擬機器，都必須位在與管理虛擬機器相同的子網路中。（視所選系統大小而定，可能需要一個或多個媒體和 Web 內部虛擬機器。）



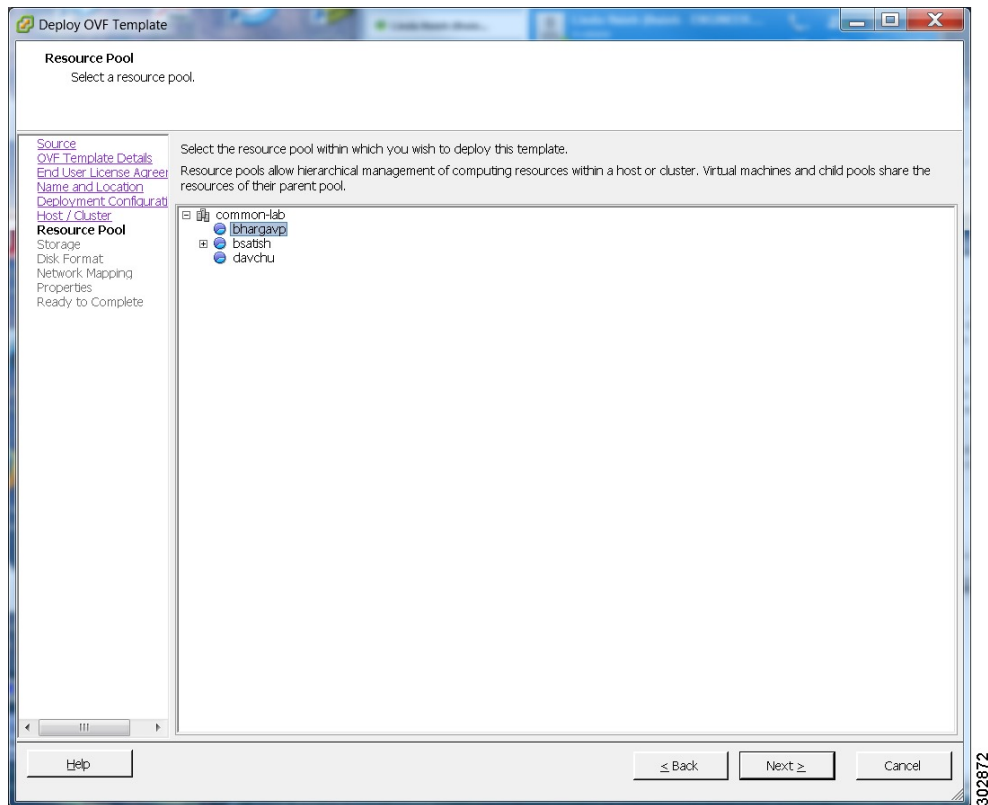
- 步驟 7** 從下拉清單中，選取適用於您系統大小的虛擬機器，然後選取 **Next**。
務必先部署管理虛擬機器，然後再於您的系統中部署任何其他虛擬機器。



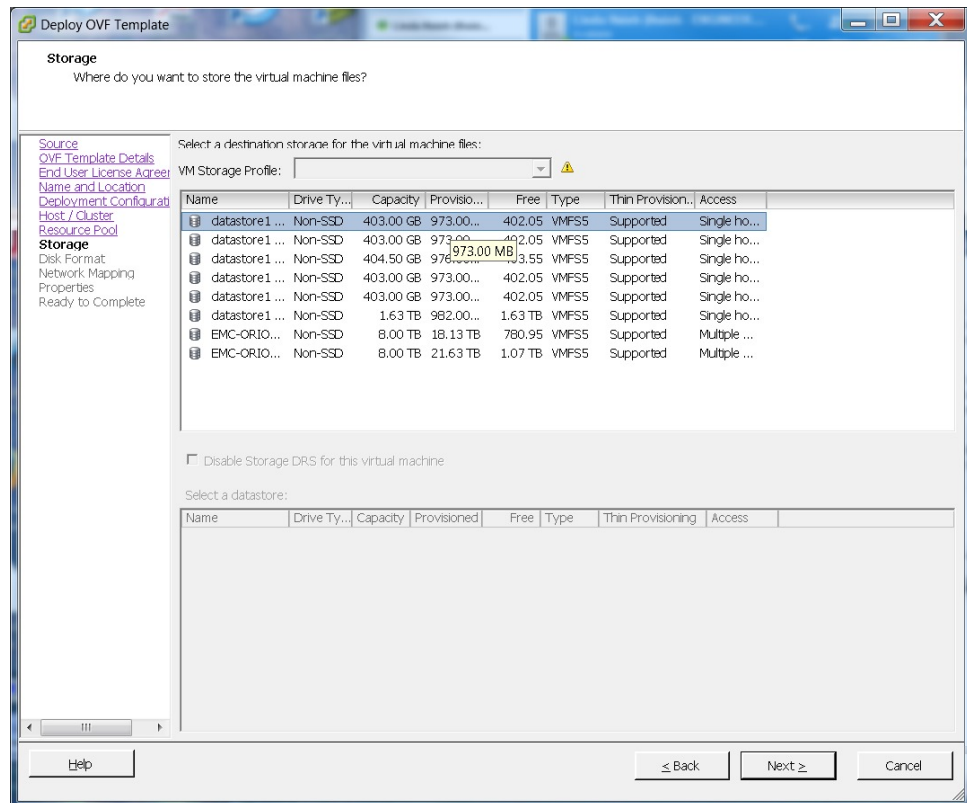
步驟 8 導覽 vCenter 庫存，然後選取要部署系統之虛擬機器所在的 ESXi 主機或叢集。選取 **Next**。



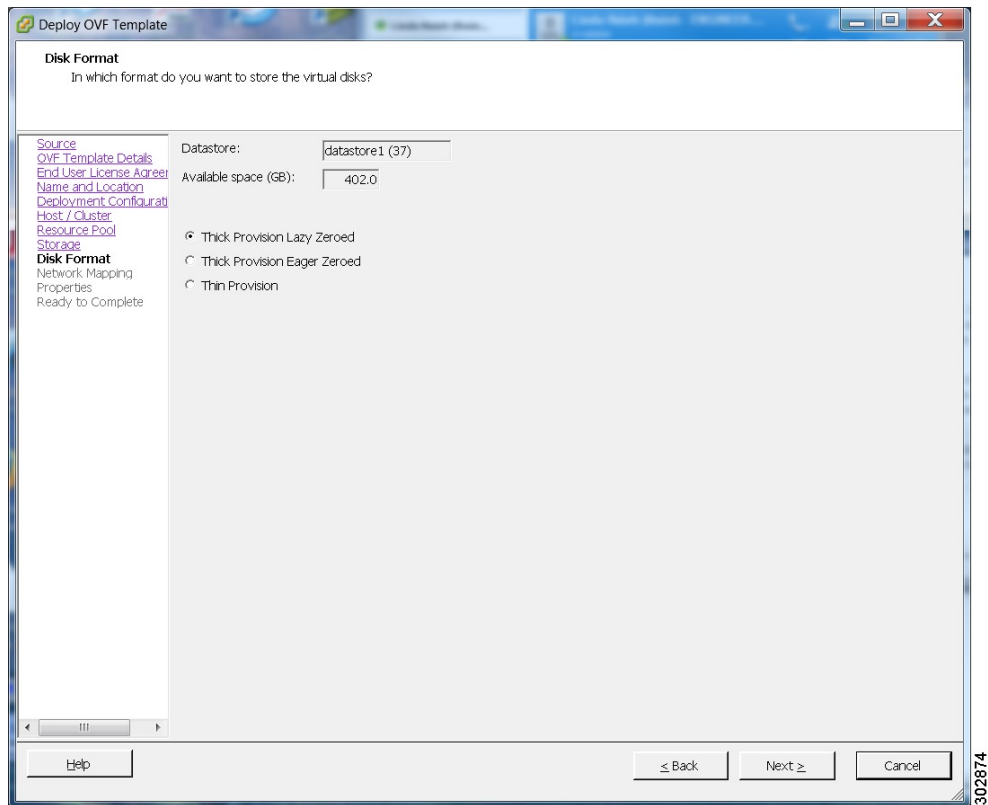
- 步驟 9** 如果叢集包含資源集區，請選取要部署 OVA 範本的資源集區，然後選取 **Next**。資源集區會共用 CPU 和記憶體資源，以與 VMware 功能（例如 DRS 或 vMotion）搭配使用。資源集區必須專屬於單一 ESXi 主機。不建議將 VMware 資源集區與 Cisco WebEx Meetings Server 搭配使用。



- 步驟 10** 選取您的虛擬機器的資料存放區，以及您的虛擬機器的佈建類型。您必須選取 **Thick Provisioning**，並建立系統所需的最大虛擬磁碟空間。使用 Thin Provisioning，VMware 會依需要分配檔案系統空間，這可能會導致效能較差。消極零已足夠，積極零可接受，但積極零將需要更長時間才能完成。

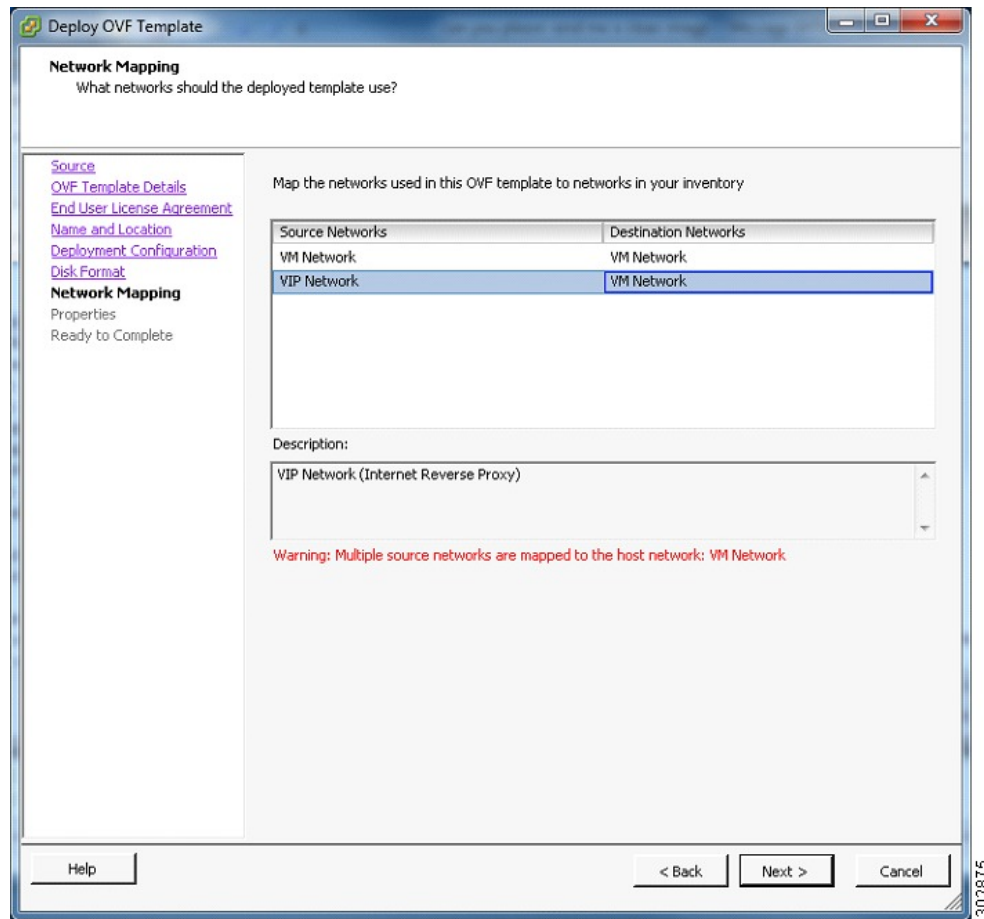


302873



步驟 11 設定網路對應。對於每種來源網路，從 **Destination Networks** 欄的下拉清單中選取目標網路。選取 **Next**。

附註 「VM Network」和「VIP Network」都必須對應至「Destination Networks」欄中的相同值。您可以忽略有關多個來源網路對應至相同主機網路的警告訊息。



步驟 12 為虛擬機器輸入以下資訊，然後選取 **Next**：

- 虛擬機器的主機名稱（請勿在這裡加入網域）
- 虛擬機器的網域
- 虛擬機器的 IPv4 位址 (Eth0)
- 虛擬機器的子網路遮罩
- 閘道 IP 位址
- 包含此虛擬機器的主機名稱和 IP 位址的項目的主要 DNS 伺服器
- 包含此虛擬機器的主機名稱和 IP 位址的項目的次要 DNS 伺服器
- 在安裝過程中開啓此虛擬機器的電源後顯示的語言

附註 若要避免 DNS 問題，則可以測試 URL 和 IP 位址，然後再開始 OVA 部署。如果發生錯誤，則部署將失敗。

Deploy OVF Template

Customize the software solution for this deployment.

Source
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Host / Cluster](#)
[Resource Pool](#)
[Storage](#)
[Disk Format](#)
[Network Mapping](#)
Properties
 Ready to Complete

Networking Properties

Hostname for the virtual machine
 2-64 alphanumeric characters | Required | Hostname only, not including the domain
 docs-sj-vm24

DNS local domain name
 Domain name | Required | Domain name for the virtual machine (for example, "your_company".com)
 cisco.com

IPv4 address
 IPv4 format | Required | Physical IP address (Eth0) for the virtual machine
 192.0.2.122

IPv4 Subnet mask
 IPv4 format | Required | Netmask for the virtual machine
 255.255.255.0

IPv4 Gateway
 IPv4 format | Required | Gateway for the virtual machine
 192.0.2.1

Primary DNS Server IPv4 Address
 IPv4 format | Required | Internal DNS server that contains entries for the hostname and IP address of this virtual machine
 198.51.100.100

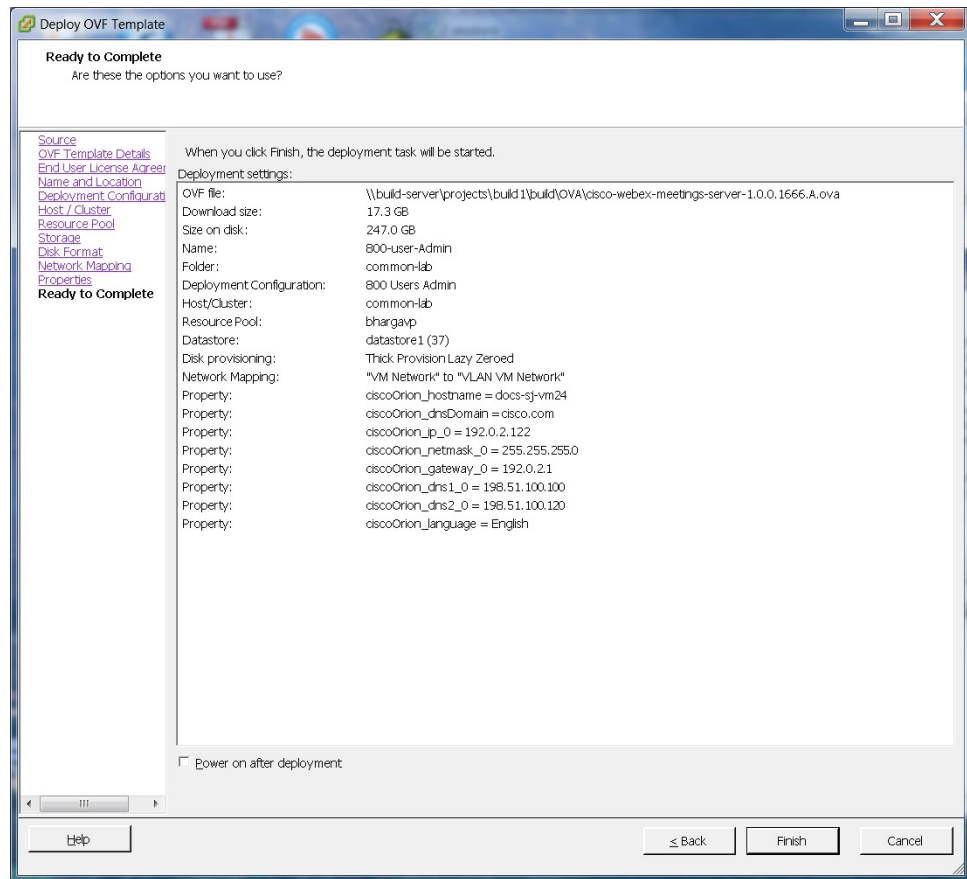
Secondary DNS Server IPv4 Address
 IPv4 format | Optional | Internal DNS server that contains entries for the hostname and IP address of this virtual machine
 198.51.100.120

System language
 String of alphanumeric characters | Required | Language displayed during the installation process, following power on of the Admin virtual machine
 English

Help ≤ Back Next ≥ Cancel

步驟 13 確認您已輸入的資訊。如果存在任何錯誤，請選取 **Back**，然後變更值。

步驟 14 勾選 **Power on after deployment**，然後選取 **Finish**。



步驟 15 如果您要部署管理虛擬機器，請移至 vCenter，並開啓虛擬機器的主控制台視窗。開啓電源後，我們將檢查您在 OVA 部署期間輸入的網路資訊。

- 如果我們可以確認連線，則會顯示一個綠色勾選標記。
- 如果存在問題，則會顯示一個紅色 X 標記。修正錯誤，並重新嘗試 OVA 部署。

步驟 16 確認所有資訊後，請記下主控制台視窗中所顯示區分大小寫的 URL。軟體管理員將在 Web 瀏覽器中鍵入此 URL，然後繼續系統部署。

附註 如果系統在設定完成之前已重新開機，則會產生新密碼，您必須將 URL 與新密碼搭配使用。

下一步動作

如果您是執行手動部署，則 Cisco 建議您在此時為系統部署剩餘的虛擬機器。這可避免與開啓虛擬機器電源相關的任何問題，例如逾時。

如果部署成功，請在瀏覽器視窗中繼續系統部署。

如果部署失敗，請參閱 [OVA 部署失敗後複查您的網路配置](#)。

OVA 部署失敗後複查您的網路配置

確認針對虛擬機器的網路輸入項目。



重要須知

除部署失敗後之外，請勿對系統中的任何虛擬機器使用 **Edit Settings...**。系統啟動並執行後，您必須使用 WebEx 管理網站對虛擬機器設定進行進一步編輯。如果您使用 vSphere 用戶端，系統不會接受這些變更。



附註

如需詳細步驟，請參閱您的 VMware vSphere 文件。

程序

- 步驟 1 在 vSphere 用戶端，在虛擬機器上選取 **Power > Shut Down Guest**。
- 步驟 2 在庫存中尋找虛擬機器，然後在 **Edit settings...** 上按一下滑鼠右鍵。
- 步驟 3 選取 **Options** 標籤。
- 步驟 4 選取 **Properties** 並確認已正確輸入所有網路資訊。如果需要任何變更，請使用正確的設定重新部署 OVA。
網路問題的一個可能原因是未正確設定 ESXi 主機的 VLAN 路由。由於虛擬機器在該 VLAN 上，因此虛擬機器不會有網路連線。透過 ESXi 主機駐留的網路，您應可以 ping 將用於系統中虛擬機器的 VLAN 的預設閘道 IP 位址。

選取用於設定的語言

確定用於設定系統的偏好語言。



附註

在系統部署完成之前，請勿關閉此瀏覽器視窗。如果您提前關閉瀏覽器，則可能必須重新啟動部署。

開始之前

請確定您已從 VMware vCenter 部署管理虛擬機器。請參閱[透過 VMware vSphere 用戶端部署 OVA 檔案, 第 16 頁](#)

程序

步驟 1 從下拉功能表中選取語言。

步驟 2 選取下一步。

確認部署

程序

步驟 1 確認是要部署新系統還是延長現有系統。

步驟 2 選取下一步。

確認您的系統的大小

在您使用 OVA 檔案部署管理虛擬機器時，已選取系統的大小。

• 確認您在 OVA 部署期間選取的系統大小是正確的。

如果您選取的系統大小是正確的，請選取下一步。

如果您選取的系統大小不正確，則選取我要變更系統大小。

- a) 使用 VMware vSphere 用戶端，為系統大小不正確的「管理」虛擬機器選取 **Power > Shut Down Guest**。
- b) 在虛擬機器上按一下滑鼠右鍵，然後選取 **Delete from Disk**。
- c) 重新部署 OVA 檔案，並選取系統大小正確的「管理」虛擬機器。

選擇要安裝的系統

程序

步驟 1 確定安裝的類型。

• 如果您是第一次安裝此系統，則選擇**安裝主要系統**。

• 如果您已安裝主要系統，且想要備援高可用性系統，則選擇**建立高可用性 (HA) 備援系統**。

附註 您不應在安裝主要系統之前安裝 HA 系統，因為除非已安裝主要系統，否則您無法使用 HA 系統。

步驟 2 選取下一步。

選擇系統部署的類型

確定要部署系統所需的任何其他虛擬機器的方式。如果您已選取 2000 個使用者的系統，則必須選取手動部署。

程序

步驟 1 選取希望自己部署虛擬機器，還是希望我們為您部署虛擬機器。

- **自動：** 這是最快的安裝方式。我們將部署您系統所需的所有虛擬機器。除非您要部署需要手動部署的 2000 個使用者系統，否則 Cisco 建議您選取自動。

附註 透過使用 Cisco WebEx 管理，您仍可以在完成部署後對系統進行變更。

- **手動：** 您必須使用 VMware vCenter 手動部署每個虛擬機器。回答一些有關您系統的問題後，我們將提供您系統所需的虛擬機器清單。

有關自動或手動部署的決策取決於以下情況：

- 如果您有時間限制，則自動部署比手動部署更快。
- 如果您偏好逐步指導，則選取自動部署。
- 如果您熟悉 VMware vCenter 但不想提供您的 vCenter 認證，請選取手動部署。

步驟 2 選取下一步。

提供 VMware vCenter 認證

如果您選取自動部署，則 Cisco WebEx Meetings Server 會要求您提供 vCenter 認證以便為您部署虛擬機器。

開始之前

系統的所有 ESXi 主機都必須屬於相同的 VMware vCenter。

程序

- 步驟 1 為將在其中部署系統的 vCenter 輸入安全的 https URL。
- 步驟 2 輸入我們將用於部署虛擬機器的使用者名稱。vCenter 使用者必須包含允許該管理者部署、配置、開啓電源和關閉電源及刪除虛擬機器的管理員特權。
- 步驟 3 輸入此使用者名稱的密碼。
- 步驟 4 選取下一步。

選擇用於您的「媒體」虛擬機器的 vCenter 設定

250 個使用者和 800 個使用者系統部署需要媒體虛擬機器。

程序

- 步驟 1 從下拉清單中，選擇用於媒體虛擬機器的 ESXi 主機。
- 步驟 2 選擇媒體虛擬機器的資料存放區。
- 步驟 3 選擇媒體虛擬機器的虛擬機器連接埠群組。
Cisco 建議您選擇為管理虛擬機器選取的相同連接埠群組。
- 步驟 4 選取下一步。

輸入「媒體」虛擬機器的網路資訊

透過輸入媒體虛擬機器的完整網域名稱，Cisco WebEx Meetings Server 會嘗試填寫網路資訊。



附註

媒體虛擬機器必須與管理虛擬機器位在相同的子網路上。不要編輯媒體虛擬機器的網域、IPv4 網道、子網路遮罩或 DNS 伺服器。

程序

- 步驟 1 輸入「媒體」虛擬機器的 FQDN。
您應該已經輸入 DNS 伺服器中媒體虛擬機器的主機名稱和 IP 位址。Cisco WebEx Meetings Server 會尋找並填寫 IPv4 位址。
- 步驟 2 選取下一步。

新增公開存取

如果您新增公開存取，使用者可以透過網際網路或行動裝置主持或出席會議。如需為您的公司進行此設定的其他資訊，請參閱《Cisco WebEx Meetings Server 規劃指南》。



附註 您永遠都可以在稍後透過 WebEx 管理網站變更此選項。

程序

步驟 1 選擇外部使用者是否可以主持或出席會議。

- 如果您要新增公開存取，請確認建立網際網路反向 Proxy 虛擬機器勾選方塊已勾選。
- 如果您只想要內部使用者（有公司的防火牆保護）主持或出席會議，則取消勾選建立網際網路反向 Proxy 虛擬機器勾選方塊。

步驟 2 選取下一步。

下一步動作

- 具有公開存取：[選擇用於您的網際網路反向 Proxy 的 vCenter 設定, 第 32 頁](#)
- 沒有公開存取：[輸入專用 VIP 位址, 第 34 頁](#)

選擇用於您的網際網路反向 Proxy 的 vCenter 設定

公開存取需要網際網路反向 Proxy 虛擬機器。輸入您在安裝檢查清單中記下的值。

雖然這不是強制的，但基於安全考量，Cisco 建議您將網際網路反向 Proxy 與管理虛擬機器置於不同的子網路。這樣做可確保網際網路反向 Proxy 與內部（「管理」與「媒體」，如果適用）虛擬機器之間的網路層次隔離。



附註 請確定 VMware vCenter 所需的防火牆連接埠已開啓，以便 vCenter 可以部署網際網路反向 Proxy 虛擬機器。如需必要的防火牆連接埠的相關資訊，請參閱《Cisco WebEx Meetings Server 規劃指南》。

程序

- 步驟 1 從下拉清單中，選擇用於網際網路反向 Proxy 虛擬機器的 ESXi 主機。
- 步驟 2 選擇網際網路反向 Proxy 的資料存放區。
- 步驟 3 選擇網際網路反向 Proxy 的虛擬機器連接埠群組。
- 步驟 4 選取下一步。

輸入網際網路反向 Proxy 的網路資訊

網際網路反向 Proxy 可讓使用者從網際網路或行動裝置主持或出席會議。

開始之前

- 基於安全考量，Cisco 建議您應將網際網路反向 Proxy 置於與管理虛擬機器不同的子網路中。
- 在您的 DNS 伺服器中輸入網際網路反向 Proxy 的主機名稱和 IP 位址，以從外部網路啟用查詢。



附註

如果您具有從內部網路啟用查詢的 DNS 伺服器，則亦請在這些 DNS 伺服器中輸入網際網路反向 Proxy 的主機名稱和 IP 位址。此舉可在內部虛擬機器（「管理」與「媒體」，如果適用）和網際網路反向 Proxy 之間實現安全連線。

- 為網際網路反向 Proxy 輸入以下內容，然後選取下一步：

完整網域名稱 (FQDN)

您應該已經輸入 DNS 伺服器中網際網路反向 Proxy 虛擬機器的主機名稱和 IP 位址。我們將為您尋找並填寫 **IPv4 位址** 欄位。

IPv4 閘道

IPv4 子網路遮罩

主要 DNS 伺服器 IPv4 位址

（選用）次要 DNS 伺服器 IPv4 位址

輸入公用 VIP 位址

- 此公用 VIP 位址必須可以在網際網路和內部網路上看見（僅限水平分割 DNS）。
- 此公用 VIP 位址必須與網際網路反向 Proxy 位於同一個子網路。
- 如果您沒有水平分割 DNS，則所有使用者都會使用公用 VIP 位址來主持和出席會議。

- 如果您具有水平分割 DNS，且已新增公開存取，則外部使用者會使用公用 VIP 位址來主持和出席會議。

如需取得有關非水平分割、水平分割 DNS 及公開存取的更多資訊，請參閱《Cisco WebEx Meetings Server 規劃指南》。



附註

如果您要建立高可用性 (HA) 系統，則不需要重新輸入此資訊，因為我們將使用您為主要系統輸入的資訊。

- 輸入公用 VIP IPv4 位址，然後選取下一步。

輸入專用 VIP 位址

管理員透過對應至專用 VIP 位址的管理網站 URL，來設定、監控及維護系統。



附註

如果您有水平分割 DNS，則內部使用者也可使用專用 VIP 位址來主持和出席會議。



附註

如果您要新增高可用性 (HA) 系統，則不需要重新輸入此資訊，因為我們將使用您為主要系統輸入的資訊。

開始之前

專用虛擬 IP (VIP) 位址必須與內部（「管理」與「媒體」，如果適用）虛擬機器位在相同的子網路上。

- 輸入 IPv4 專用 VIP 位址，然後選取下一步。

WebEx 網站和 WebEx 管理 URL

WebEx 網站 URL

最終使用者存取 WebEx 網站 URL 以主持或出席會議。此 URL 解析為專用 VIP 位址或公用 VIP 位址，視您是否使用水平分割 DNS 而定。

- 當您不使用「水平分割」DNS 時，針對所有使用者解析為公用 VIP 位址。
- 當您使用水平分割 DNS 時，針對所有外部使用者解析為公用 VIP 位址。
- 當您使用水平分割 DNS 時，針對內部使用者解析為專用 VIP 位址。

WebEx 管理 URL

管理員存取 WebEx 管理 URL 以設定、管理和監控系統。此 URL 解析為專用 VIP 位址。

WebEx 網站和 WebEx 管理 URL 的名稱

您可以為這些 URL 選擇全部由小寫字元組成的幾乎任何名稱。但是，您不能在網站 URL 中使用以下內容作為主機名稱：

- 與組成系統的任何虛擬機器的主機名稱相同的名稱
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version
- WBXService
- WebEx

輸入 WebEx 網站和管理 URL

- 您不能在管理或 WebEx 網站 URL 的主機名稱部分重複使用您系統中虛擬機器的主機名稱。
- WebEx 網站 URL 必須與 WebEx 管理 URL 不同。



附註

如果您要新增高可用性 (HA) 系統，則不需要重新輸入此資訊，因為我們將使用您為主要系統輸入的資訊。

- 輸入以下安全的 (https) URL，然後選取下一步。

主持和出席會議的使用者的 WebEx 網站 URL

管理您系統的系統管理員的 WebEx 管理 URL

確認您的網路已正確設定

此螢幕提供您的系統所需網路變更的線上說明鏈結。線上說明提供有關 DNS 伺服器變更及防火牆設定的詳細資訊。



附註

您必須對 DNS 伺服器和防火牆進行必要的變更，因為我們將在下一步驟測試網路連線。

- 如果您尚未執行此操作，請完成網路配置，然後選取下一步。
選取下一步後：

- 自動部署：我們將開始部署您系統所需的虛擬機器。
- 手動部署：在下一個螢幕上，您將輸入虛擬機器的主機名稱並部署它們（如果您尚未部署的話）。如果您已部署這些虛擬機器，請開啓其電源並驗證所有虛擬機器電源是否都已成功開啓。

部署您的虛擬機器

根據您稍早前輸入的資訊，我們將部署您系統所需的虛擬機器。



附註

部署需要數分鐘才能完成。在成功部署所有虛擬機器並開啓其電源之前，請勿離開此頁面，否則部署會失敗，並會顯示指示問題的錯誤訊息。

- 完成以下其中一項操作

如果沒有任何錯誤，則在狀態顯示所有綠色勾選標記時，選取下一步。

如果您看到錯誤，請修正錯誤，然後選取下一步。



附註

您可能想要選取**下載日誌檔案**，以取得此部署的日誌檔案。這可讓您具有部署的記錄，您可以使用此記錄來疑難排解失敗的部署。



附註

在重做部署前，請務必關閉所有有錯的虛擬機器，並將其刪除。否則，在重新進行系統部署時，您可能會看到有關現有虛擬機器的錯誤訊息。

檢查您的系統

根據您稍早前輸入的資訊，我們將檢查您的系統設定。我們將確認虛擬機器具有所需的最低設定，及驗證 WebEx 網站和 WebEx 管理 URL。



附註

系統檢查需要數分鐘才能完成。在所有檢查都已成功完成之前，請勿離開此頁面，否則系統檢查會失敗，並會顯示指示問題的錯誤訊息。



附註

如果您在檢查完成之前重新載入頁面，會將您送回此系統部署的第一個頁面。但是，如果檢查已完成，則會將您帶至基本設定的第一個頁面（您可以在此設定郵件伺服器和管理員）。



附註

在部署過程中使用的管理網站 URL 是管理虛擬機器的主機名稱。但是，在基本配置期間會使用管理網站 URL 來取代主機名稱。結果，當您第一次登入管理網站時，系統可能提示您接受憑證異常。

•完成以下其中一項操作：

如果沒有任何錯誤，則請在狀態全部顯示綠色勾選標記時，選取下一步。繼續執行[設定系統的郵件伺服器](#)，第 63 頁。

如果網路連線存在問題，則檢查是否已正確輸入 WebEx 網站和管理 URL 與 IP 位址。檢查這些網站是否在正確的子網路中，且已正確輸入在 DNS 伺服器中。

如果您的系統會議符合最低系統容量發生問題，則您有兩種選擇。

我們建議您從 VMware vCenter 關閉所有虛擬機器，並手動刪除它們。然後，在資源符合或超過最低需求的系統上重新嘗試系統部署。

您可以選擇繼續進行目前的安裝。如果繼續，則必須確認放棄請求 Cisco 技術支援的權利。透過勾選錯誤訊息勾選方塊進行確認，然後選取下一步。

如果您的一個或多個虛擬機器存在其他問題，則透過 VMware vCenter 關閉這些有錯的虛擬機器的電源，並手動刪除它們。然後，在修正問題後重新嘗試系統部署。



附註

在重做部署前，請務必關閉所有有錯的虛擬機器，並將其刪除。否則，在重新進行系統部署時，您可能會看到有關現有虛擬機器的錯誤訊息。

在極少數情況下，您可能會看到**未測試**。

這並非表示您的虛擬機器有任何問題。它僅僅表示我們未完成系統檢查（例如，由於網路連線暫時中斷）。完成部署後，您便可以登入管理網站並檢查這些資源。

- 選取繼續以移至基本設定的第一頁（您可以在這裡設定郵件伺服器及管理員）。如果其他管理員負責基本設定，請記下此 URL 並將其傳送給軟體管理員。



第 4 章

使用手動部署安裝系統

- [系統部署的一般概念, 第 39 頁](#)
- [安裝檢查清單, 第 40 頁](#)
- [手動部署所需資訊, 第 41 頁](#)
- [透過 VMware vSphere 用戶端部署 OVA 檔案, 第 42 頁](#)
- [選取用於設定的語言, 第 54 頁](#)
- [確認部署, 第 55 頁](#)
- [確認您的系統的大小, 第 55 頁](#)
- [選擇要安裝的系統, 第 55 頁](#)
- [選擇系統部署的類型, 第 56 頁](#)
- [新增公開存取, 第 56 頁](#)
- [輸入公用 VIP 位址, 第 57 頁](#)
- [輸入專用 VIP 位址, 第 57 頁](#)
- [WebEx 網站和 WebEx 管理 URL, 第 58 頁](#)
- [輸入 WebEx 網站和管理 URL, 第 59 頁](#)
- [確認您的網路已正確設定, 第 59 頁](#)
- [部署您的虛擬機器, 第 60 頁](#)
- [檢查您的系統, 第 61 頁](#)

系統部署的一般概念

系統大小

- 50 個並行使用者的系統

通常支援擁有 500 至 1000 個員工的公司

主要系統（沒有 HA）包含一個「管理」虛擬機器及一個選用的「網際網路反向 Proxy」（用於公開存取）

•250 個並行使用者的系統

通常支援擁有 2500 至 5000 個員工的公司

主要系統（沒有 HA）包含一個「管理」虛擬機器、一個「媒體」虛擬機器及一個選用的「網際網路反向 Proxy」（用於公開存取）

•800 個並行使用者的系統

通常支援擁有 8000 至 16,000 個員工的公司

主要系統（沒有 HA）包含一個「管理」虛擬機器、一個「媒體」虛擬機器及一個選用的「網際網路反向 Proxy」（用於公開存取）

•2000 個並行使用者的系統

通常支援擁有 20,000 至 40,000 個員工的公司

主要系統（沒有 HA）包含一個「管理」虛擬機器、三個「媒體」虛擬機器、兩個「Web」機器及一個選用的「網際網路反向 Proxy」（用於公開存取）

部署期間的使用規定

欄位名稱	描述
WebEx 網站 URL	使用者用於主持和出席會議的安全 http URL。
WebEx 管理 URL	管理員用於設定、監控及管理系統的安全 http URL。
公用 VIP	WebEx 網站 URL 的 IP 位址
專用 VIP	<ul style="list-style-type: none"> •管理網站 URL 的 IP 位址 •WebEx 網站 URL 的 IP 位址 (如果您使用水平分割 DNS，則僅適用於內部使用者)。

安裝檢查清單



限制

您必須使用 VMware vCenter，來管理在其中部署 Cisco WebEx Meetings Server 系統的 ESXi 主機。

網路變更

請參閱您的部署適用的網路檢查清單。有兩個考量：

- 公開存取：您的防火牆外部的使用者是否可以透過網際網路或行動裝置主持和存取會議。
Cisco 建議使用公開存取，因為這樣能為您的行動辦公提供更好的使用者體驗。
- 您公司中 DNS 設定的類型：水平分割 DNS 或非水平分割 DNS（最常見的 DNS 設定）。
如需取得有關這些 DNS 設定類型的更多資訊，請參閱《Cisco WebEx Meetings Server 規劃指南》。
- 從管理員桌面開啓連接埠 10200 至管理虛擬機器。
在部署期間 Web 瀏覽器使用連接埠 10200。

請為您的部署選取正確的檢查清單：

- [適用於具有公開存取和非水平分割 DNS 之系統的網路檢查清單, 第 9 頁](#)
- [適用於沒有公開存取之系統的網路檢查清單, 第 10 頁](#)
- [適用於具有公開存取和水平分割 DNS 之系統的網路檢查清單, 第 10 頁](#)

必填資訊



附註

如果您是執行自動部署（支援並行使用者人數為 50、250 及 800）系統或手動部署（支援所有系統大小），則所需資訊會有所不同。除非您要部署需要手動部署的 2000 位使用者系統，否則 Cisco 建議您選取自動部署。請參閱下面適當的鏈結。

請選擇以下其中一項，以取得部署類型所需資訊的檢查清單：

- [自動部署所需資訊, 第 13 頁](#)
- [手動部署所需資訊, 第 41 頁](#)

手動部署所需資訊

在手動部署中，您可以使用 OVA 精靈從 vSphere 用戶端建立適用於您系統的所有虛擬機器。然後，您可以使用手動部署安裝系統。

如果您要部署 2000 個使用者的系統，則必須選擇手動部署。



附註

請務必先將虛擬機器 FQDN、IP 位址、WebEx 和管理網站 URL 及 VIP 位址新增至您的 DNS 伺服器，然後再開始系統部署。我們將在部署結束時使用本資訊來檢查網路連線。

為了避免任何 DNS 問題，您可能要測試這些 URL 和 IP 位址，然後再開始 OVA 部署。否則，系統部署將會失敗，直到您更正這些錯誤為止。

以下是您的系統所需的資訊 (依序列出)。

欄位名稱	描述	系統的值
公用 VIP	WebEx 網站 URL（網站使用者存取該 URL 來主持和出席會議）的 IP 位址	
專用 VIP	<ul style="list-style-type: none"> •管理網站 URL (管理員用來設定、監控及管理系統) 的 IP 位址 •WebEx 網站 URL 的 IP 位址 (如果您使用水平分割 DNS，則僅適用於內部使用者)。 	
WebEx 網站 URL	使用者用於主持和出席會議的安全 http URL（全部小寫字元）。	
WebEx 管理 URL	管理員用於設定、監控及管理系統的安全 http URL（全部小寫字元）。	
內部虛擬機器的 FQDN	根據您所選取的系統大小，媒體和網路虛擬機器的完整網域名稱（全部小寫字元）。	
（僅限公開存取） 網際網路反向 Proxy 虛擬機器的 FQDN	如果您計劃新增公開存取，則需要輸入「網際網路反向 Proxy」虛擬機器的完整網域名稱（全部小寫字元）。	

下一步動作

使用此資訊，在瀏覽器視窗中輸入部署 URL 來開始系統部署。（部署 URL 將寫入管理虛擬機器的主控台視窗中。）



附註

如果在完成設定之前將系統重新開機，則會產生新的密碼，您必須將部署 URL 與新密碼一起使用。

透過 VMware vSphere 用戶端部署 OVA 檔案

在部署系統之前，您必須使用 VMware vSphere 用戶端為系統部署管理虛擬機器。



附註

提供了以下程序作為一般指導。在 OVA 部署期間看到的真實畫面，可能因 vCenter、儲存體和網路配置而與此程序稍有不同。請參閱 VMware vSphere 文件，以取得有關 OVA 精靈的完整資訊。

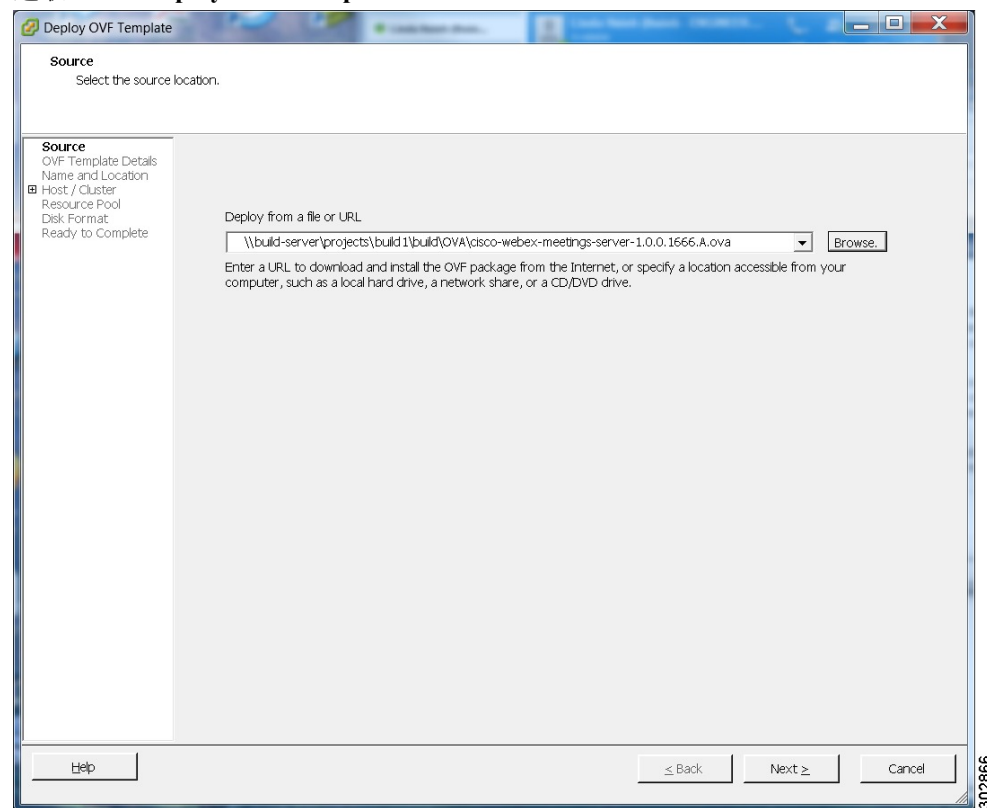
開始之前

請取得用於您系統的 Cisco WebEx Meetings Server OVA 檔案，並將此檔案置於可從 VMware vSphere 存取的位置。

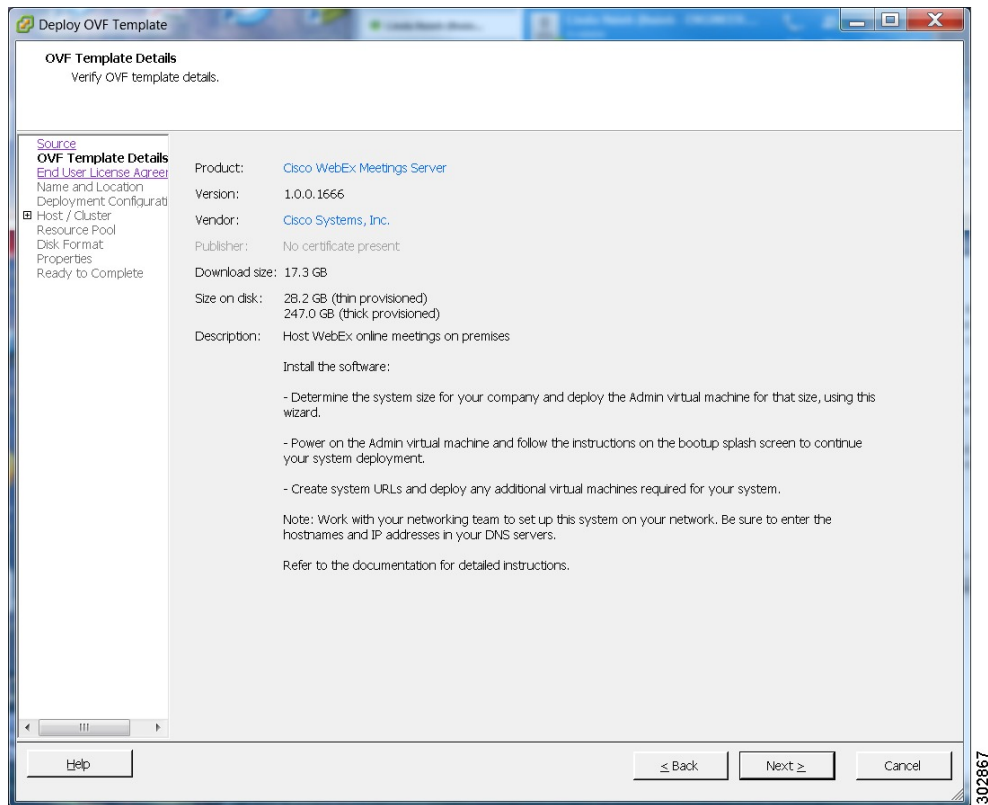
您必須使用 VMware vCenter，來管理在其中部署 Cisco WebEx Meetings Server 系統的 ESXi 主機。使用 vSphere 用戶端，登入 vCenter，及為管理虛擬機器部署 OVA 檔案。

程序

- 步驟 1** 登入您的 VMware vSphere 用戶端。
務必以包含管理員特權的使用者身份登入：部署、設定、開啓或關閉，以及刪除虛擬機器。
- 步驟 2** 選取 **File > Deploy OVF Template...**



- 步驟 3** 選取瀏覽，以導覽至 OVA 檔案的位置。選取 **Next**。
您可以選取 **Cisco WebEx Meetings Server** 鏈結，以移至具有此系統相關詳細資訊的網頁。



步驟 4 閱讀「最終使用者授權協議」並選取**接受**，然後選取 **Next**。

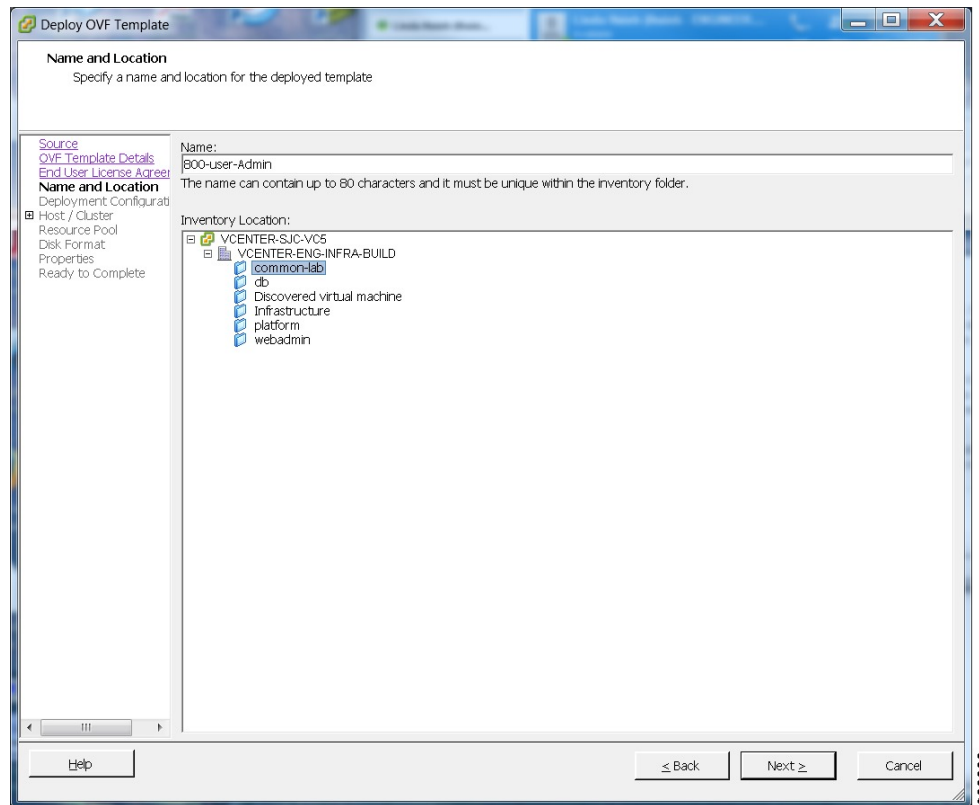
步驟 5 導覽至 vCenter 庫存中要放置管理虛擬機器的位置並選取此位置。

步驟 6 輸入適合您系統大小的虛擬機器名稱，然後選取**Next**。如需為您公司選取正確大小的相關資訊，請參閱[系統大小](#)。

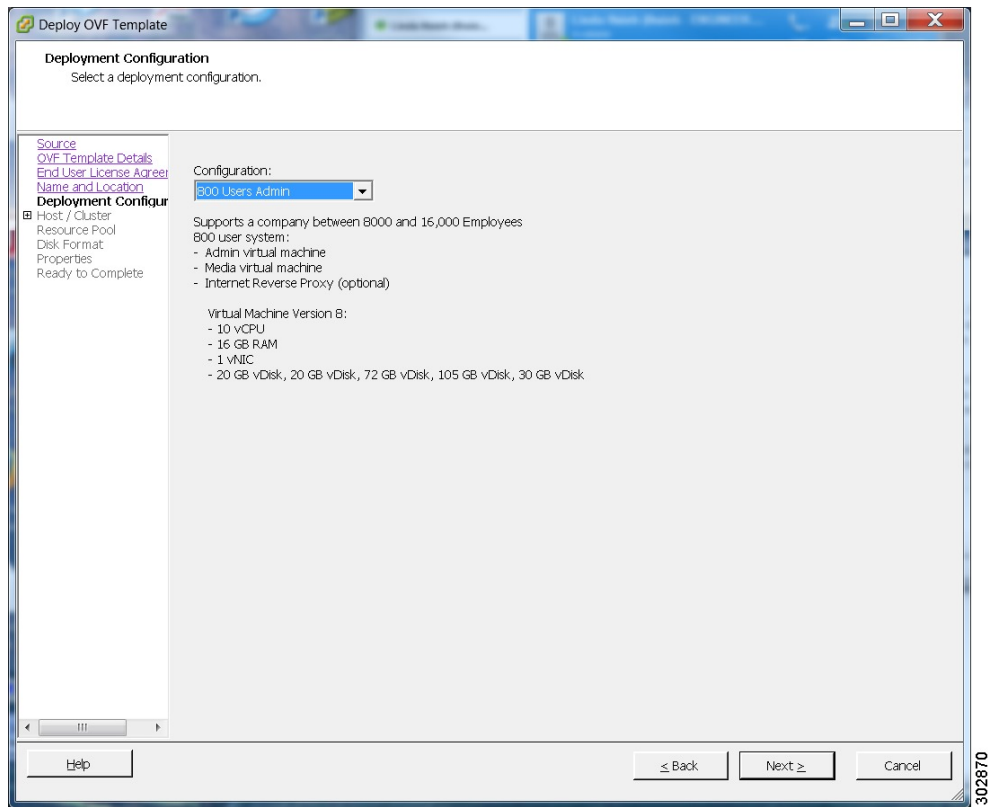
附註 您必須先部署管理虛擬機器，然後才部署任何其他虛擬機器。如果選取自動部署（建議），則我們將為您部署其他虛擬機器。如果您選擇手動部署（2000 個並行使用者的系統必須使用此選項），則在部署管理虛擬機器後，必須使用這個相同的精靈來部署其他虛擬機器。

Cisco 建議您在虛擬機器名稱中包含類型；例如，管理虛擬機器名稱中的「管理」，以能夠輕易在 vCenter 庫存中識別。

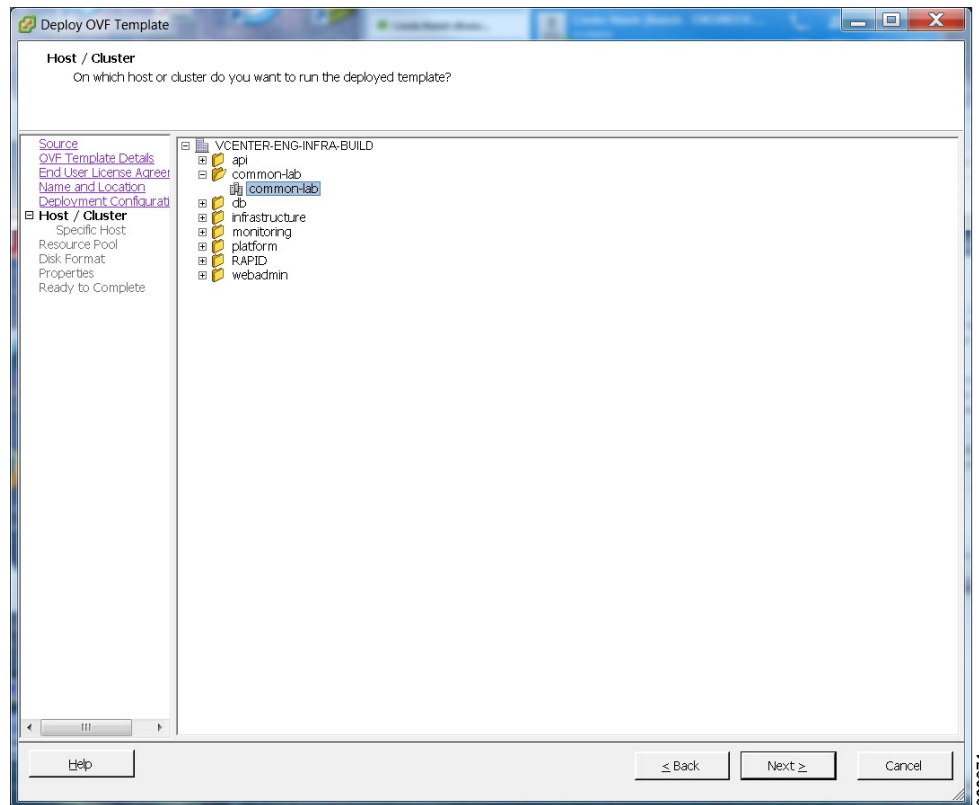
附註 您系統的所有內部虛擬機器，都必須位在與管理虛擬機器相同的子網路中。（視所選系統大小而定，可能需要一個或多個媒體和 Web 內部虛擬機器。）



- 步驟 7** 從下拉清單中，選取適用於您系統大小的虛擬機器，然後選取 **Next**。
務必先部署管理虛擬機器，然後再於您的系統中部署任何其他虛擬機器。

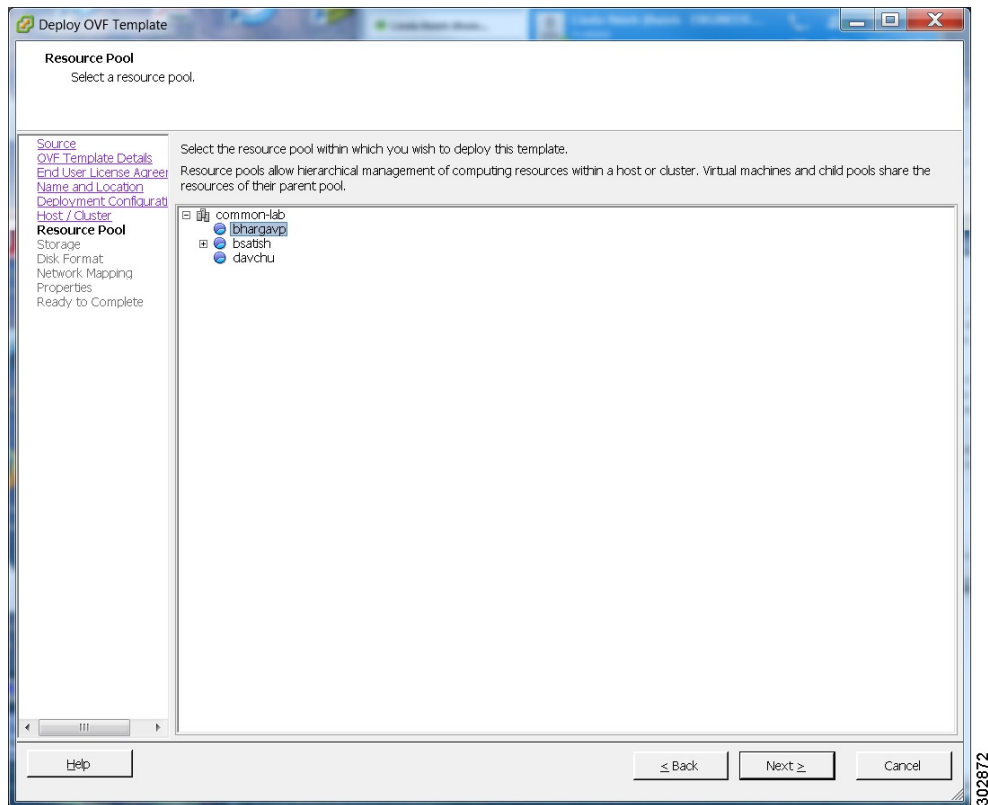


步驟 8 導覽 vCenter 庫存，然後選取要部署系統之虛擬機器所在的 ESXi 主機或叢集。選取 **Next**。

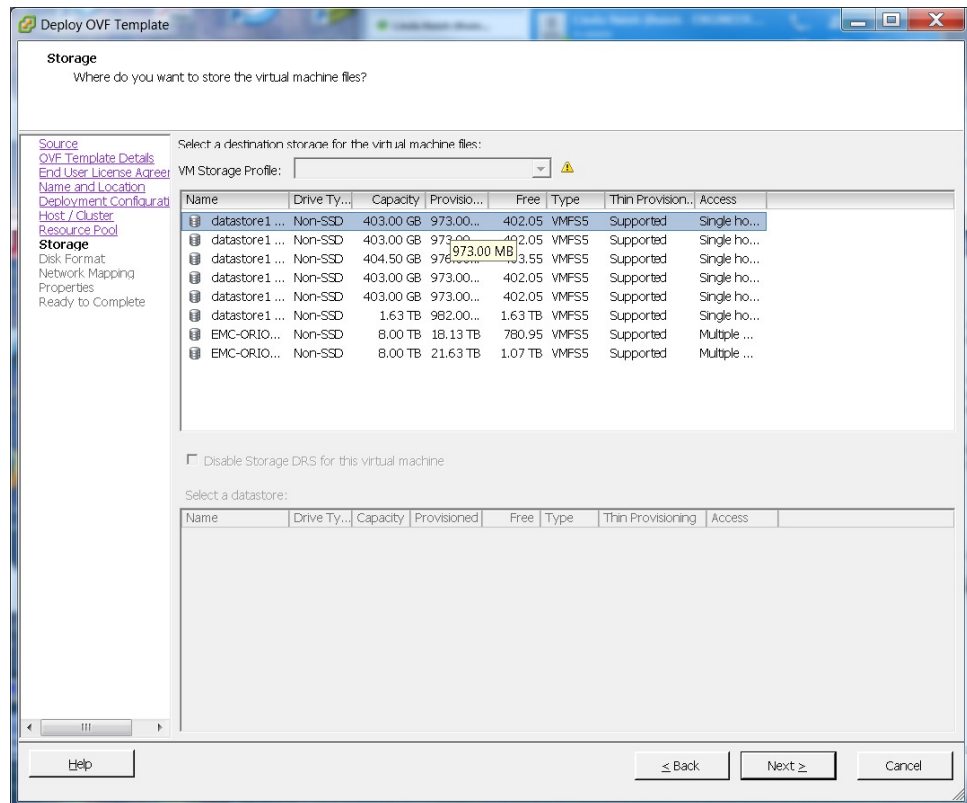


302871

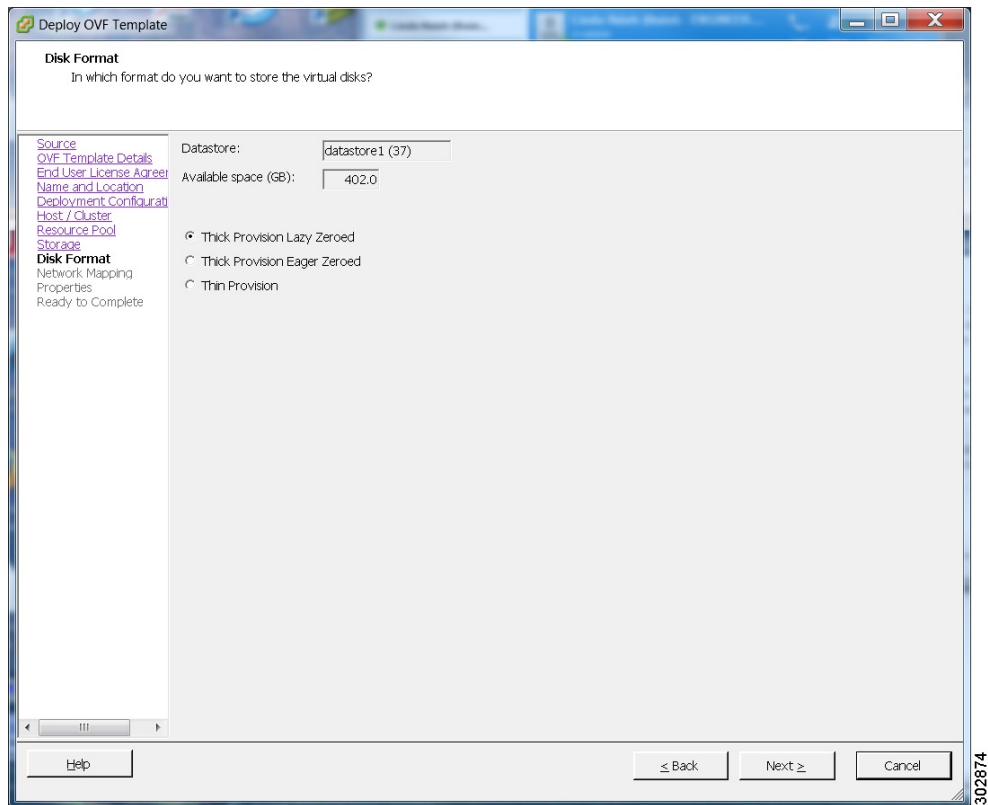
- 步驟 9** 如果叢集包含資源集區，請選取要部署 OVA 範本的資源集區，然後選取 **Next**。資源集區會共用 CPU 和記憶體資源，以與 VMware 功能（例如 DRS 或 vMotion）搭配使用。資源集區必須專屬於單一 ESXi 主機。不建議將 VMware 資源集區與 Cisco WebEx Meetings Server 搭配使用。



- 步驟 10** 選取您的虛擬機器的資料存放區，以及您的虛擬機器的佈建類型。您必須選取 **Thick Provisioning**，並建立系統所需的最大虛擬磁碟空間。使用 Thin Provisioning，VMware 會依需要分配檔案系統空間，這可能會導致效能較差。消極零已足夠，積極零可接受，但積極零將需要更長時間才能完成。

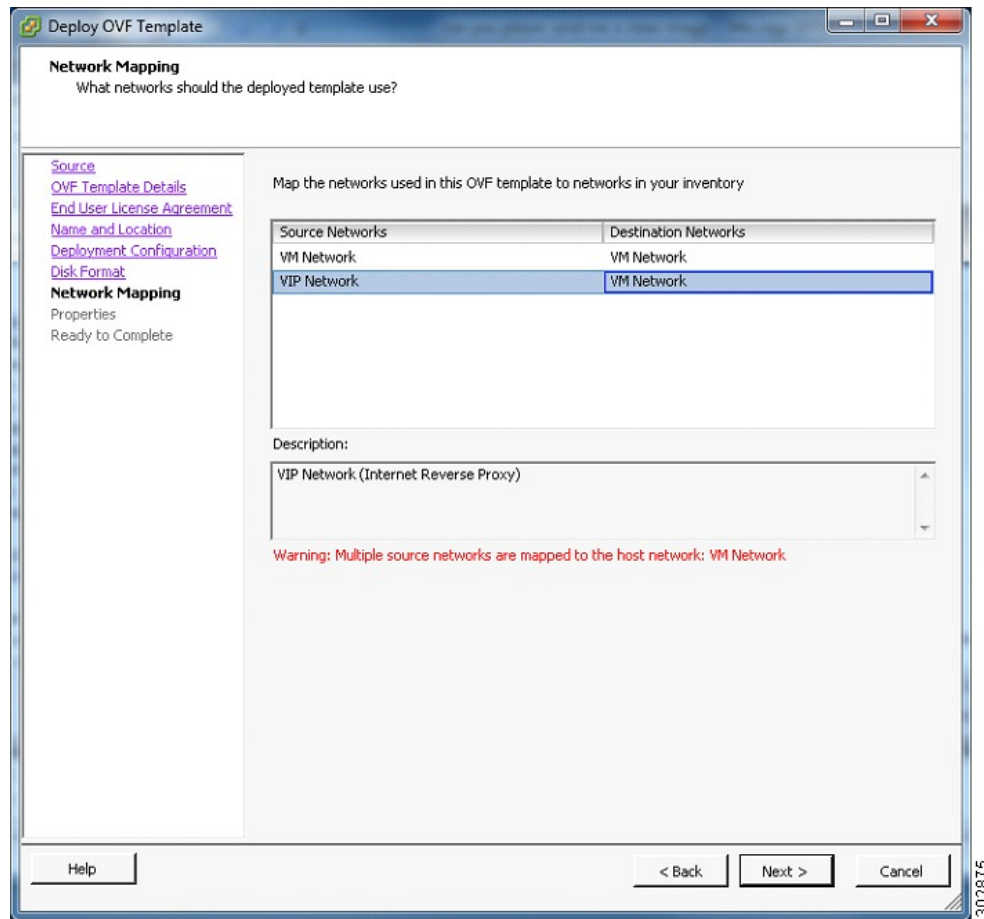


302873



步驟 11 設定網路對應。對於每種來源網路，從 **Destination Networks** 欄的下拉清單中選取目標網路。選取 **Next**。

附註 「VM Network」和「VIP Network」都必須對應至「Destination Networks」欄中的相同值。您可以忽略有關多個來源網路對應至相同主機網路的警告訊息。



步驟 12 為虛擬機器輸入以下資訊，然後選取 **Next**：

- 虛擬機器的主機名稱（請勿在這裡加入網域）
- 虛擬機器的網域
- 虛擬機器的 IPv4 位址 (Eth0)
- 虛擬機器的子網路遮罩
- 閘道 IP 位址
- 包含此虛擬機器的主機名稱和 IP 位址的項目的主要 DNS 伺服器
- 包含此虛擬機器的主機名稱和 IP 位址的項目的次要 DNS 伺服器
- 在安裝過程中開啓此虛擬機器的電源後顯示的語言

附註 若要避免 DNS 問題，則可以測試 URL 和 IP 位址，然後再開始 OVA 部署。如果發生錯誤，則部署將失敗。

Deploy OVF Template

Customize the software solution for this deployment.

Source
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Deployment Configuration](#)
[Host / Cluster](#)
[Resource Pool](#)
[Storage](#)
[Disk Format](#)
[Network Mapping](#)
Properties
 Ready to Complete

Networking Properties

Hostname for the virtual machine
 2-64 alphanumeric characters | Required | Hostname only, not including the domain

DNS local domain name
 Domain name | Required | Domain name for the virtual machine (for example, "your_company".com)

IPv4 address
 IPv4 format | Required | Physical IP address (Eth0) for the virtual machine

IPv4 Subnet mask
 IPv4 format | Required | Netmask for the virtual machine

IPv4 Gateway
 IPv4 format | Required | Gateway for the virtual machine

Primary DNS Server IPv4 Address
 IPv4 format | Required | Internal DNS server that contains entries for the hostname and IP address of this virtual machine

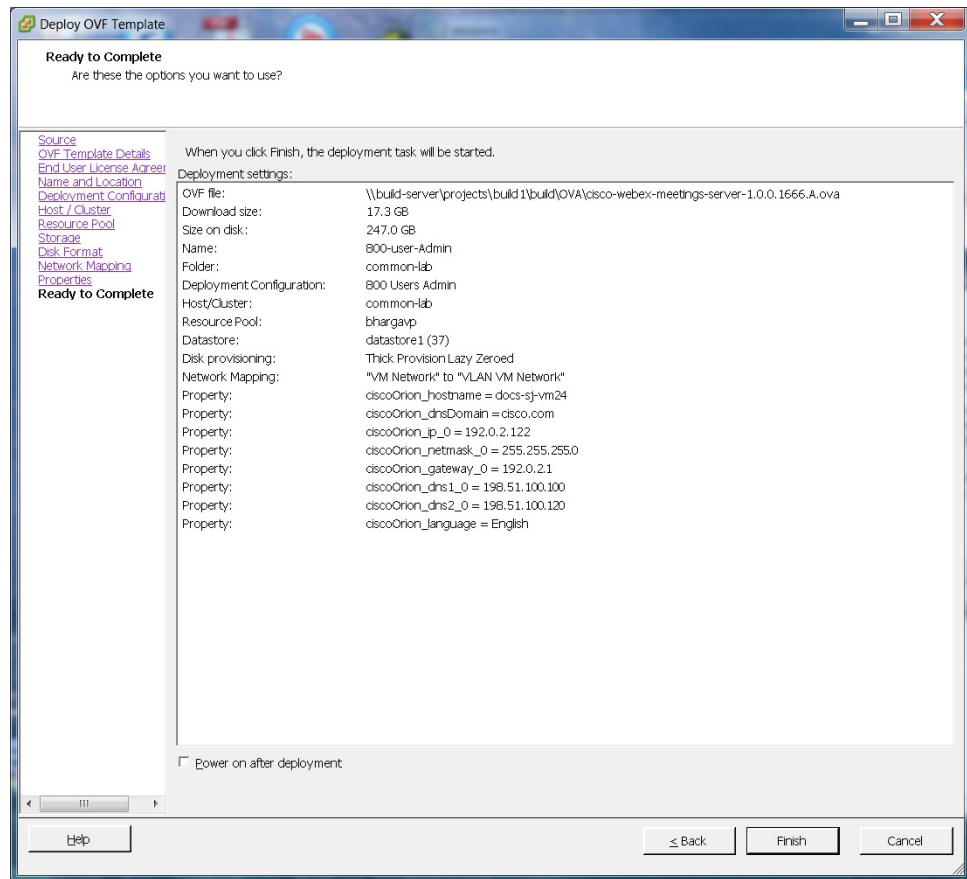
Secondary DNS Server IPv4 Address
 IPv4 format | Optional | Internal DNS server that contains entries for the hostname and IP address of this virtual machine

System language
 String of alphanumeric characters | Required | Language displayed during the installation process, following power on of the Admin virtual machine

Help ≤ Back Next ≥ Cancel

步驟 13 確認您已輸入的資訊。如果存在任何錯誤，請選取 **Back**，然後變更值。

步驟 14 勾選 **Power on after deployment**，然後選取 **Finish**。



步驟 15 如果您要部署管理虛擬機器，請移至 vCenter，並開啓虛擬機器的主控制台視窗。開啓電源後，我們將檢查您在 OVA 部署期間輸入的網路資訊。

- 如果我們可以確認連線，則會顯示一個綠色勾選標記。
- 如果存在問題，則會顯示一個紅色 X 標記。修正錯誤，並重新嘗試 OVA 部署。

步驟 16 確認所有資訊後，請記下主控制台視窗中所顯示區分大小寫的 URL。軟體管理員將在 Web 瀏覽器中鍵入此 URL，然後繼續系統部署。

附註 如果系統在設定完成之前已重新開機，則會產生新密碼，您必須將 URL 與新密碼搭配使用。

下一步動作

如果您是執行手動部署，則 Cisco 建議您在此時為系統部署剩餘的虛擬機器。這可避免與開啓虛擬機器電源相關的任何問題，例如逾時。

如果部署成功，請在瀏覽器視窗中繼續系統部署。

如果部署失敗，請參閱 [OVA 部署失敗後複查您的網路配置](#)。

OVA 部署失敗後複查您的網路配置

確認針對虛擬機器的網路輸入項目。



重要須知

除部署失敗後之外，請勿對系統中的任何虛擬機器使用 **Edit Settings...**。系統啟動並執行後，您必須使用 WebEx 管理網站對虛擬機器設定進行進一步編輯。如果您使用 vSphere 用戶端，系統不會接受這些變更。



附註

如需詳細步驟，請參閱您的 VMware vSphere 文件。

程序

- 步驟 1 在 vSphere 用戶端，在虛擬機器上選取 **Power > Shut Down Guest**。
- 步驟 2 在庫存中尋找虛擬機器，然後在 **Edit settings...** 上按一下滑鼠右鍵。
- 步驟 3 選取 **Options** 標籤。
- 步驟 4 選取 **Properties** 並確認已正確輸入所有網路資訊。如果需要任何變更，請使用正確的設定重新部署 OVA。
網路問題的一個可能原因是未正確設定 ESXi 主機的 VLAN 路由。由於虛擬機器在該 VLAN 上，因此虛擬機器不會有網路連線。透過 ESXi 主機駐留的網路，您應可以 ping 將用於系統中虛擬機器的 VLAN 的預設閘道 IP 位址。

選取用於設定的語言

確定用於設定系統的偏好語言。



附註

在系統部署完成之前，請勿關閉此瀏覽器視窗。如果您提前關閉瀏覽器，則可能必須重新啟動部署。

開始之前

請確定您已從 VMware vCenter 部署管理虛擬機器。請參閱[透過 VMware vSphere 用戶端部署 OVA 檔案, 第 16 頁](#)

程序

步驟 1 從下拉功能表中選取語言。

步驟 2 選取下一步。

確認部署

程序

步驟 1 確認是要部署新系統還是延長現有系統。

步驟 2 選取下一步。

確認您的系統的大小

在您使用 OVA 檔案部署管理虛擬機器時，已選取系統的大小。

• 確認您在 OVA 部署期間選取的系統大小是正確的。

如果您選取的系統大小是正確的，請選取下一步。

如果您選取的系統大小不正確，則選取我要變更系統大小。

- a) 使用 VMware vSphere 用戶端，為系統大小不正確的「管理」虛擬機器選取 **Power > Shut Down Guest**。
- b) 在虛擬機器上按一下滑鼠右鍵，然後選取 **Delete from Disk**。
- c) 重新部署 OVA 檔案，並選取系統大小正確的「管理」虛擬機器。

選擇要安裝的系統

程序

步驟 1 確定安裝的類型。

• 如果您是第一次安裝此系統，則選擇**安裝主要系統**。

• 如果您已安裝主要系統，且想要備援高可用性系統，則選擇**建立高可用性 (HA) 備援系統**。

附註 您不應在安裝主要系統之前安裝 HA 系統，因為除非已安裝主要系統，否則您無法使用 HA 系統。

步驟 2 選取下一步。

選擇系統部署的類型

確定要部署系統所需的任何其他虛擬機器的方式。如果您已選取 2000 個使用者的系統，則必須選取手動部署。

程序

步驟 1 選取希望自己部署虛擬機器，還是希望我們為您部署虛擬機器。

- **自動：** 這是最快的安裝方式。我們將部署您系統所需的所有虛擬機器。除非您要部署需要手動部署的 2000 個使用者系統，否則 Cisco 建議您選取自動。

附註 透過使用 Cisco WebEx 管理，您仍可以在完成部署後對系統進行變更。

- **手動：** 您必須使用 VMware vCenter 手動部署每個虛擬機器。回答一些有關您系統的問題後，我們將提供您系統所需的虛擬機器清單。

有關自動或手動部署的決策取決於以下情況：

- 如果您有時間限制，則自動部署比手動部署更快。
- 如果您偏好逐步指導，則選取自動部署。
- 如果您熟悉 VMware vCenter 但不想提供您的 vCenter 認證，請選取手動部署。

步驟 2 選取下一步。

新增公開存取

如果您新增公開存取，使用者可以透過網際網路或行動裝置主持或出席會議。如需為您的公司進行此設定的其他資訊，請參閱《Cisco WebEx Meetings Server 規劃指南》。



附註 您永遠都可以在稍後透過 WebEx 管理網站變更此選項。

程序

步驟 1 選擇外部使用者是否可以主持或出席會議。

- 如果您要新增公開存取，請確認**建立網際網路反向 Proxy 虛擬機器**勾選方塊已勾選。
- 如果您只想要內部使用者（有公司的防火牆保護）主持或出席會議，則取消勾選**建立網際網路反向 Proxy 虛擬機器**勾選方塊。

步驟 2 選取下一步。

下一步動作

- 具有公開存取：[選擇用於您的網際網路反向 Proxy 的 vCenter 設定, 第 32 頁](#)
- 沒有公開存取：[輸入專用 VIP 位址, 第 34 頁](#)

輸入公用 VIP 位址

- 此公用 VIP 位址必須可以在網際網路和內部網路上看見（僅限水平分割 DNS）。
- 此公用 VIP 位址必須與網際網路反向 Proxy 位於同一個子網路。
- 如果您沒有水平分割 DNS，則所有使用者都會使用公用 VIP 位址來主持和出席會議。
- 如果您具有水平分割 DNS，且已新增公開存取，則外部使用者會使用公用 VIP 位址來主持和出席會議。

如需取得有關非水平分割、水平分割 DNS 及公開存取的更多資訊，請參閱《*Cisco WebEx Meetings Server 規劃指南*》。



附註

如果您要建立高可用性 (HA) 系統，則不需要重新輸入此資訊，因為我們將使用您為主要系統輸入的資訊。

- 輸入公用 VIP IPv4 位址，然後選取下一步。

輸入專用 VIP 位址

管理員透過對應至專用 VIP 位址的管理網站 URL，來設定、監控及維護系統。



附註

如果您有水平分割 DNS，則內部使用者也可使用專用 VIP 位址來主持和出席會議。



附註

如果您要新增高可用性 (HA) 系統，則不需要重新輸入此資訊，因為我們將使用您為主要系統輸入的資訊。

開始之前

專用虛擬 IP (VIP) 位址必須與內部（「管理」與「媒體」，如果適用）虛擬機器位在相同的子網路上。

- 輸入 IPv4 專用 VIP 位址，然後選取下一步。

WebEx 網站和 WebEx 管理 URL

WebEx 網站 URL

最終使用者存取 WebEx 網站 URL 以主持或出席會議。此 URL 解析為專用 VIP 位址或公用 VIP 位址，視您是否使用水平分割 DNS 而定。

- 當您不使用「水平分割」DNS 時，針對所有使用者解析為公用 VIP 位址。
- 當您使用水平分割 DNS 時，針對所有外部使用者解析為公用 VIP 位址。
- 當您使用水平分割 DNS 時，針對內部使用者解析為專用 VIP 位址。

WebEx 管理 URL

管理員存取 WebEx 管理 URL 以設定、管理和監控系統。此 URL 解析為專用 VIP 位址。

WebEx 網站和 WebEx 管理 URL 的名稱

您可以為這些 URL 選擇全部由小寫字元組成的幾乎任何名稱。但是，您不能在網站 URL 中使用以下內容作為主機名稱：

- 與組成系統的任何虛擬機器的主機名稱相同的名稱
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- manager

- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version
- WBXService
- WebEx

輸入 WebEx 網站和管理 URL

- 您不能在管理或 WebEx 網站 URL 的主機名稱部分重複使用您系統中虛擬機器的主機名稱。
- WebEx 網站 URL 必須與 WebEx 管理 URL 不同。



附註

如果您要新增高可用性 (HA) 系統，則不需要重新輸入此資訊，因為我們將使用您為主要系統輸入的資訊。

- 輸入以下安全的 (https) URL，然後選取下一步。

主持和出席會議的使用者的 WebEx 網站 URL

管理您系統的系統管理員的 WebEx 管理 URL

確認您的網路已正確設定

此螢幕提供您的系統所需網路變更的線上說明鏈結。線上說明提供有關 DNS 伺服器變更及防火牆設定的詳細資訊。



附註

您必須對 DNS 伺服器 and 防火牆進行必要的變更，因為我們將在下一步驟測試網路連線。

•如果您尚未執行此操作，請完成網路配置，然後選取下一步。

選取下一步後：

•自動部署：我們將開始部署您系統所需的虛擬機器。

•手動部署：在下一個螢幕上，您將輸入虛擬機器的主機名稱並部署它們（如果您尚未部署的話）。如果您已部署這些虛擬機器，請開啓其電源並驗證所有虛擬機器電源是否都已成功開啓。

部署您的虛擬機器



附註

提供有關系統中虛擬機器的資訊後，我們將嘗試連線至為系統部署的每個虛擬機器。

在系統已連線至所有虛擬機器之前，請勿離開此頁面，否則連線會失敗，並會顯示指示問題的錯誤訊息。

程序

步驟 1 輸入您系統所需的任何其他虛擬機器的完整網域名稱 (FQDN)。(在透過 OVA 檔案進行部署時，您稍早前已輸入管理虛擬機器 FQDN。)

步驟 2 如果您尚未完成此動作，請使用 VMware vCenter 部署系統所需的所有其他虛擬機器。

步驟 3 開啓所有虛擬機器的電源，並驗證其電源是否成功開啓。然後選取偵測虛擬機器。我們正在嘗試連線至這些虛擬機器。這可能需要幾分鐘的時間。

步驟 4 請等到所有虛擬機器都顯示已連線狀態，然後完成以下其中一項操作

•如果沒有任何錯誤，則狀態會全部顯示綠色勾選標記。如果您感到滿意，請選取下一步。否則，您仍可以變更虛擬機器的 FQDN，然後再次選取偵測虛擬機器。

•如果您看到錯誤，請修正錯誤，然後選取下一步。

附註 您可能想要選取下載日誌檔案，以取得此部署的日誌檔案。這可讓您具有部署的記錄，您可以使用此記錄來疑難排解失敗的部署。

•如果您的一個或多個虛擬機器存在其他問題，則透過 VMware vCenter 關閉這些有錯的虛擬機器的電源，並手動刪除它們。修正問題後，透過 OVA 檔案重新部署虛擬機器，然後選取偵測虛擬機器。

附註 在重做部署前，請務必關閉所有有錯的虛擬機器，並將其刪除。否則，您可能看到關於現有的虛擬機器的錯誤訊息。

檢查您的系統

根據您稍早前輸入的資訊，我們將檢查您的系統設定。我們將確認虛擬機器具有所需的最低設定，及驗證 WebEx 網站和 WebEx 管理 URL。



附註

系統檢查需要數分鐘才能完成。在所有檢查都已成功完成之前，請勿離開此頁面，否則系統檢查會失敗，並會顯示指示問題的錯誤訊息。



附註

如果您在檢查完成之前重新載入頁面，會將您送回此系統部署的第一個頁面。但是，如果檢查已完成，則會將您帶至基本設定的第一個頁面（您可以在此設定郵件伺服器和管理員）。



附註

在部署過程中使用的管理網站 URL 是管理虛擬機器的主機名稱。但是，在基本配置期間會使用管理網站 URL 來取代主機名稱。結果，當您第一次登入管理網站時，系統可能提示您接受憑證異常。

•完成以下其中一項操作：

如果沒有任何錯誤，則請在狀態全部顯示綠色勾選標記時，選取下一步。繼續執行[設定系統的郵件伺服器](#), 第 63 頁。

如果網路連線存在問題，則檢查是否已正確輸入 WebEx 網站和管理 URL 與 IP 位址。檢查這些網站是否在正確的子網路中，且已正確輸入在 DNS 伺服器中。

如果您的系統會議符合最低系統容量發生問題，則您有兩種選擇。

我們建議您從 VMware vCenter 關閉所有虛擬機器，並手動刪除它們。然後，在資源符合或超過最低需求的系統上重新嘗試系統部署。

您可以選擇繼續進行目前的安裝。如果繼續，則必須確認放棄請求 Cisco 技術支援的權利。透過勾選錯誤訊息勾選方塊進行確認，然後選取下一步。

如果您的一個或多個虛擬機器存在其他問題，則透過 VMware vCenter 關閉這些有錯的虛擬機器的電源，並手動刪除它們。然後，在修正問題後重新嘗試系統部署。



附註

在重做部署前，請務必關閉所有有錯的虛擬機器，並將其刪除。否則，在重新進行系統部署時，您可能會看到有關現有虛擬機器的錯誤訊息。

在極少數情況下，您可能會看到**未測試**。

這並非表示您的虛擬機器有任何問題。它僅僅表示我們未完成系統檢查（例如，由於網路連線暫時中斷）。完成部署後，您便可以登入管理網站並檢查這些資源。

- 選取繼續以移至基本設定的第一頁 (您可以在這裡設定郵件伺服器及管理員)。如果其他管理員負責基本設定，請記下此 URL 並將其傳送給軟體管理員。



第 5 章

設定郵件伺服器、時區及地區設定

- 設定系統的郵件伺服器, 第 63 頁
- 設定系統的時區和地區設定, 第 64 頁
- 確認郵件伺服器、時區和地區設定, 第 64 頁
- 設定系統的第一個管理員帳戶, 第 64 頁
- 測試系統, 第 65 頁

設定系統的郵件伺服器

透過設定此郵件伺服器，系統可以使用您的公司郵件伺服器，將電子郵件傳送給管理員（警示、警報、報告等）和使用者（會議邀請、密碼重設等）。

開始之前

您必須已成功部署完成系統所需的虛擬機器。

程序

步驟 1 輸入系統將用於傳送電子郵件的郵件伺服器的完整網域名稱 (FQDN)。

步驟 2 如果您希望 **TLS** 已啟用，則請勾選此勾選方塊。

步驟 3 如果您不想使用預設值，您可以編輯**連接埠**欄位。
依預設，SMTP 連接埠號碼為 25 或 465（安全的 SMTP 連接埠號碼）。

附註 「Web」節點和「管理」節點會將 SMTP 要求傳送至所配置的郵件伺服器。如果內部「Web」和「管理」虛擬機器與郵件伺服器之間有防火牆，則可能會封鎖 SMTP 流量。若要確保郵件伺服器配置和郵件通知正常運作，請確保連接埠 25 或 465（安全 SMTP 連接埠號）在郵件伺服器與「Web」和「管理」虛擬機器之間是開啓的。

步驟 4 如果您想要啓用郵件伺服器驗證，請勾選**伺服器驗證已啟用**勾選方塊。
如果您啓用伺服器驗證，則會顯示**使用者名稱**和**密碼**欄位。

步驟 5 如果已顯示，請輸入**使用者名稱**和**密碼**認證，供系統存取您的公司郵件伺服器。

來自系統的電子郵件是由 `admin@<WebEx-site-URL>` 傳送。請確定郵件伺服器能夠識別此使用者。

步驟 6 選取下一步。

設定系統的時區和地區設定

開始之前

如果您所執行的是 Windows 7，並且在 Internet Explorer 10 瀏覽器中開啓您的 Cisco WebEx 網站，則可能想要選取文件 Internet Explorer 10 標準，以確定應用程式中的所有按鈕都能正常運作。

- 選取工具 > 開發人員工具。

- 在「開發人員工具」頂端，選取文件模式：IE7 標準 > Internet Explorer 10 標準。

程序

步驟 1 從下拉清單選取系統的本地時區。

步驟 2 從下拉清單中選取系統的國家地區設定。

步驟 3 選取下一步。

確認郵件伺服器、時區和地區設定

您已在先前的螢幕上輸入這些設定。

- 複查您先前輸入的資訊。如果存在任何錯誤，則選取上一步。否則，選取下一步。

設定系統的第一個管理員帳戶

系統會在部署過程中，建立單一管理員帳戶。



注意

此管理員必須登入系統，建立密碼，及新增其他管理員和使用者。否則，其他使用者都不具有對系統的存取權。

開始之前

您必須已正確設定系統的郵件伺服器，才能將電子郵件傳送給管理員和使用者。

程序

-
- 步驟 1** 輸入管理員的姓名。
 - 步驟 2** 輸入管理員的完整電子郵件地址，然後透過再次輸入來確認。
 - 步驟 3** 選取下一步建立密碼。
 - 步驟 4** 輸入密碼，然後再次輸入以確認。
 - 步驟 5** 選取提交以登入 WebEx 管理網站。
 - 步驟 6** 您必須登入系統，並新增其他使用者。建立每個新使用者後，系統會傳送電子郵件給每個使用者，歡迎並要求使用者登入及建立密碼。
 初始登入後，每個管理員都可檢視系統的教程。管理員可以立即檢視教程，或決定稍後再進行檢視。
-

測試系統

本節中列示一些在系統上執行的建議測試。您可以使用本產品支援頁面上提供的兩個診斷工具，來完成這些測試並驗證您的系統：「會議測試」及「系統資源測試」。

測試升級的系統時，您可以保留原始系統直到您完成測試升級的系統為止（但您無法同時開啓兩個系統）。對升級的系統測試結果感到滿意後，您可以移除（永久）原始系統。移除或刪除現有系統時，請確定您的升級系統正在執行。這樣可以避免意外移除基本虛擬機器磁碟 (VMDK) 檔案，升級系統可能會存取該檔案。

- 新增、編輯、啓動及停用使用者。
- 排定和舉行場會議。
- 重新排定現有會議。
- 刪除一系列會議或未來的會議。
- 開啓會議附件。
- 播放會議錄製檔。



第 6 章

在安裝後變更系統

本章列出完成系統的初始部署後可以執行的不同系統更改程序。

- [新增 HA、更新、升級或擴充系統, 第 67 頁](#)
- [準備系統更改程序, 第 68 頁](#)

新增 HA、更新、升級或擴充系統

下列程序被視為「系統更改」程序，且需要管理員預先準備：

- 新增或移除高可用性 (HA) 系統
- 透過使用 ISO 更新檔案將系統更新至更高版本
- 透過使用升級版本的 OVA 檔案重新部署系統來升級系統
- 將系統大小由目前大小擴充至較大大小

在執行這些程序時，您需要將系統進入維護模式。因此，您可能想要將這些程序中的幾個排定在一起，例如，在同一維護時段擴充系統和更新系統。

請注意以下約束：

- 如果您已將 HA 新增至系統，並且想要擴充或升級系統，則需要在完成升級後再次重新部署 HA 系統。

系統擴充或升級需要部署新系統，將系統資料傳送至已擴充或升級的系統。部署新系統時，將要求您在部署主系統或 HA 系統之間進行選擇 - 您不能一次部署這兩個系統。因此，您必須先使用 OVA 檔案部署主系統，然後再使用部署主系統所使用的相同 OVA 檔案部署 HA 系統。

- 如果您計劃新增 HA 系統並加以更新（使用 ISO 更新檔案），則我們建議您先新增 HA 系統，然後再更新結合的系統（主系統和 HA 系統）。

更新程序會更新整個系統（無論是否含有 HA 系統）。如果您先更新系統，然後再新增 HA，您需要先部署 HA 系統，然後再更新 HA 系統（如此主系統和 HA 系統會使用相同版本）。如果您先新增 HA，則更新程序會同時更新結合的主系統和 HA 系統。

- 更新程序會更新整個系統（無論是否含有網際網路反向 Proxy）。

準備系統更改程序

本節說明如何準備主系統更改程序：透過建立系統備份、擴充系統、新增高可用性系統、啓用公開存取、更新或升級系統等。

儘管您可以選擇這樣做，但是擴充或升級系統無需備份。在擴充或升級期間，要部署新系統並將現有系統的資料傳送給新系統。如果擴充或升級有問題，則可以關閉新系統的電源並繼續使用現有系統。



注意

由於此程序需要以獨佔方式存取系統，因此使用者無法存取會議的系統。請務必將此程序排定在對使用者干擾最少的時間進行。

其他系統管理員不應在進行此程序期間存取系統。如果他們這樣做，系統不會儲存其變更，並且結果可能難以預料。他們必須等到此程序完成，然後再登入 Cisco WebEx 管理以執行其作業。



附註

在開始系統更改程序之前，請務必與其他系統管理員協調。



注意

如果您不需要建立虛擬機器的備份，則不需要完成此程序。但是，Cisco 建議的最佳作法是建立備份。備份可讓您在程序失敗時還原系統。

程序

步驟 1 登入 Cisco WebEx 管理網站。

步驟 2 選取開啟維護模式。

步驟 3 使用 VMware Data Recovery (自 vSphere 5.1 版起稱為 VMware vSphere Data Protection) 來建立每個虛擬機器的備份。

備份可協助您將虛擬機器恢復為系統更改程序之前的狀態。如需進一步資訊，請參閱 [使用 VMware vCenter 來建立備份, 第 4 頁](#)。如需此備份的完整詳細資訊，請參閱《*VMware Data Recovery 管理指南*》或《*vSphere Data Protection 管理指南*》。

附註 如果您準備進行擴充或升級，請移除現有系統上的所有 VMware 快照。這樣可以避免意外移除 Hard disk 4 的基本 VMDK 檔案，擴充或升級系統可能會存取該檔案。

步驟 4 重新登入 Cisco WebEx 管理網站，但不關閉維護模式。

步驟 5 繼續執行系統更改程序。



第 7 章

新增高可用性系統

- [使用自動部署新增 HA 系統, 第 69 頁](#)
- [使用手動部署新增 HA 系統, 第 71 頁](#)
- [確認您的主系統和您的 HA 系統版本相同, 第 73 頁](#)
- [新增高可用性系統, 第 74 頁](#)
- [測試系統, 第 75 頁](#)

使用自動部署新增 HA 系統

在開始之前

- 您必須已成功部署主系統。
- 主系統處於維護模式。
- 建立主系統和 HA 系統的備份。請參閱[使用 VMware vCenter 來建立備份, 第 4 頁](#)。

新增高可用性系統之前的考量

高可用性系統是新增至系統且成為系統一部分的冗餘系統。它在發生虛擬機器故障時提供高可用性。

高可用性 (HA) 系統具有以下約束

- HA 系統必須使用與主系統相同的發行版本。
如果您更新過主系統，則請務必對 HA 系統進行相同更新。
- 如果已授予您權利（使用相應的服務合約），則 Cisco 建議您使用基本版本（在任何修補程式之前）與主系統相同的 OVA 檔案來部署 HA 系統。
- HA 系統大小必須與主系統相同。
- 如果您已在主系統上新增公開存取，則必須也將其新增至 HA 系統。

- HA 系統的內部虛擬機器必須與主系統的內部虛擬機器位於同一個子網路。
- 如果您已新增公開存取，則 HA 系統的網際網路反向 Proxy 虛擬機器和主系統的網際網路反向 Proxy 虛擬機器必須位於同一個網路。
- 此過程會對您的系統新增虛擬機器，所以您的現行安全憑證將變成無效且需要更新，除非您使用自我簽署憑證。
- 如果您先前曾有 HA 系統且已將其移除，現在又要重新部署新的 HA 系統，則將無法重複使用前一個 HA 系統中的虛擬機器。必須使用新的虛擬機器重新部署新的 HA 系統。

使用自動部署新增高可用性系統的作業摘要

請按順序遵循這些作業。

作業	描述	如需取得詳細資訊，請參閱
1	使用 VMware vSphere 用戶端，為 HA 系統部署管理虛擬機器。	透過 VMware vSphere 用戶端部署 OVA 檔案, 第 16 頁
2	開啟 HA 系統的「管理」虛擬機器，並記下部署 URL。	
3	在 Web 瀏覽器中輸入該 URL，並繼續部署您的 HA 系統。	
4	為 HA 系統部署選取首選語言。	選取用於設定的語言, 第 28 頁
5	確認 HA 系統的系統大小。（此系統大小必須與主系統相符。）	確認您的系統的大小, 第 29 頁
6	選取建立高可用性 (HA) 冗餘系統。	選擇要安裝的系統, 第 29 頁
7	選取自動部署。（簡而言之，Cisco 建議進行與主系統相同的選取。）	選擇系統部署的類型, 第 30 頁
8	輸入您的 vCenter 認證，以便我們可以為您部署 HA 系統的虛擬機器。	提供 VMware vCenter 認證, 第 30 頁
9	為 HA 系統的媒體虛擬機器選取 ESXi 主機、資料存放區及虛擬機器連接埠群組 (若適用)。 附註 請選擇使用與主系統相同的虛擬機器連接埠群組。	選擇用於您的「媒體」虛擬機器的 vCenter 設定, 第 31 頁
10	輸入 HA 系統的「媒體」虛擬機器的完整網域名稱 (若適用)。（如果您已使用 HA 系統的项目更新您的 DNS 伺服器，則我們將為您查詢 IP 位址。）	輸入「媒體」虛擬機器的網路資訊, 第 31 頁
11	如果您已為主系統新增公開存取，則請確保已勾選建立網際網路反向 Proxy 虛擬機器勾選方塊。否則，請取消勾選此勾選方塊。 附註 如果您尚未啟用公開存取，請跳到作業 14。	新增公開存取, 第 32 頁

作業	描述	如需取得詳細資訊，請參閱
12	如果您已新增公開存取，則請為 HA 系統的網際網路反向 Proxy 虛擬機器選取 ESXi 主機、資料存放區及虛擬機器連接埠群組。 附註 請選擇使用與主系統相同的虛擬機器連接埠群組。	選擇用於您的網際網路反向 Proxy 的 vCenter 設定, 第 32 頁
13	輸入網際網路反向 Proxy 的主機名稱和網路資訊。	輸入網際網路反向 Proxy 的網路資訊, 第 33 頁
14	檢查是否已進行 HA 系統所需的所有網路、DNS 伺服器及防火牆設定變更。	確認您的網路已正確設定, 第 36 頁
15	成功部署 HA 系統的虛擬機器後，請選取下一步以繼續執行 HA 系統檢查。	部署您的虛擬機器, 第 36 頁
16	成功完成 HA 系統檢查後，請選取下一步。	檢查您的系統, 第 37 頁
17	請確認主系統和 HA 系統使用相同版本。如果不是，則請更新 HA 系統。	確認您的主系統和您的 HA 系統版本相同, 第 73 頁
18	在 Cisco WebEx 管理中將此高可用性系統新增至主系統。	新增高可用性系統, 第 74 頁

使用手動部署新增 HA 系統

在開始之前

- 您必須已成功部署主系統。
- 主系統處於維護模式。
- 建立主系統和 HA 系統的備份。請參閱[使用 VMware vCenter 來建立備份, 第 4 頁](#)。

新增高可用性系統之前的考量

高可用性系統是新增至系統且成為系統一部分的冗餘系統。它在發生虛擬機器故障時提供高可用性。

高可用性 (HA) 系統具有以下約束

- HA 系統必須使用與主系統相同的發行版本。
如果您更新過主系統，則請務必對 HA 系統進行相同更新。
- 如果已授予您權利（使用相應的服務合約），則 Cisco 建議您使用基本版本（在任何修補程式之前）與主系統相同的 OVA 檔案來部署 HA 系統。
- HA 系統大小必須與主系統相同。
- 如果您已在主系統上新增公開存取，則必須也將其新增至 HA 系統。

- HA 系統的內部虛擬機器必須與主系統的內部虛擬機器位於同一個子網路。
- 如果您已新增公開存取，則 HA 系統的網際網路反向 Proxy 虛擬機器和主系統的網際網路反向 Proxy 虛擬機器必須位於同一個網路。
- 此過程會對您的系統新增虛擬機器，所以您的現行安全憑證將變成無效且需要更新，除非您使用自我簽署憑證。
- 如果您先前曾有 HA 系統且已將其移除，現在又要重新部署新的 HA 系統，則將無法重複使用前一個 HA 系統中的虛擬機器。必須使用新的虛擬機器重新部署新的 HA 系統。

使用手動部署新增高可用性系統的作業摘要

請按順序遵循這些作業。

作業	描述	如需取得詳細資訊，請參閱
1	使用 VMware vSphere 用戶端，為 HA 系統部署管理虛擬機器。	透過 VMware vSphere 用戶端部署 OVA 檔案, 第 16 頁
2	開啟 HA 系統的「管理」虛擬機器，並記下部署 URL。	
3	在 Web 瀏覽器中輸入該 URL，並繼續部署您的 HA 系統。	
4	為 HA 系統部署選取首選語言。	選取用於設定的語言, 第 28 頁
5	確認 HA 系統的系統大小。（此系統大小必須與主系統相符。）	確認您的系統的大小, 第 29 頁
6	選取建立高可用性 (HA) 冗餘系統。	選擇要安裝的系統, 第 29 頁
7	選取手動部署。（簡而言之，Cisco 建議進行與主系統相同的選取。）	選擇系統部署的類型, 第 30 頁
8	如果您已為主系統新增公開存取，則請確保已勾選建立網際網路反向 Proxy 虛擬機器勾選方塊。否則，請取消勾選此勾選方塊。	新增公開存取, 第 32 頁
9	檢查是否已進行 HA 系統所需的所有網路、DNS 伺服器及防火牆設定變更。	確認您的網路已正確設定, 第 36 頁
10	成功部署 HA 系統的虛擬機器後，請選取下一步以繼續執行 HA 系統檢查。	部署您的虛擬機器, 第 60 頁
11	成功完成 HA 系統檢查後，請選取下一步。	檢查您的系統, 第 37 頁
12	請確認主系統和 HA 系統使用相同版本。如果不是，則請更新 HA 系統。	確認您的主系統和您的 HA 系統版本相同, 第 73 頁
13	在 Cisco WebEx 管理中將此高可用性系統新增至主系統。	新增高可用性系統, 第 74 頁

確認您的主系統和您的 HA 系統版本相同

高可用性 (HA) 系統的版本必須與主系統版本完全相同。瀏覽器頁面上列出了 HA 系統的版本。若要檢查主系統的版本，請在主系統上完成以下步驟：

程序

- 步驟 1 在獨立的瀏覽器視窗中，登入主系統上的「WebEx 管理」網站。
- 步驟 2 在儀表板標籤上，檢查系統窗格中的主系統版本號。
- 步驟 3 如果主系統的版本高於 HA 系統，則必須使用更高版本軟體的更新 OVA 檔案來重新部署 HA 系統，或者更新 HA 系統。
附註 若要更新 HA 系統，請先備份虛擬機器。如需詳細資料，請參閱[使用 VMware vCenter 來建立備份](#)。
- 步驟 4 如果需要 HA 更新，請在部署 HA 系統之後，於連線至 HA 系統的瀏覽器上選取更新。
- 步驟 5 從 Cisco 下載適當的更新檔案：
[下載軟體](#)
將更新檔案放在可供 HA 系統使用的本地磁碟或資料存放區上。
- 步驟 6 在連線至 HA 系統的瀏覽器上選取繼續。
- 步驟 7 將 CD/DVD 光碟機連線至 HA 系統的「管理」虛擬機器中的 ISO 更新檔案。
請參閱[連接 CD/DVD 光碟機中的 ISO 映像檔](#)。
- 步驟 8 勾選我已連線至 ISO 檔案且已做好繼續的準備，然後選取繼續。
注意 選取繼續後，您將無法停止更新程序。如果在更新程序中發生問題，且未順利完成更新，則必須使用備份檔案來還原系統。
更新程序最多可能需要一小時的時間。請勿關閉此瀏覽器視窗，因為您將無法返回此頁面。
更新完成後，便會顯示新的對話方塊，來確認更新成功。
- 步驟 9 選取重新啟動。
重新啟動系統後，便會顯示已建立 HA 的系統頁面，並帶有指示更新成功的訊息。

下一步動作

在主系統上的 Cisco WebEx 管理中，將此高可用性系統新增至主系統。

新增高可用性系統



附註

高可用性系統上的大多數功能都被禁止。例如，您無權存取高可用性系統上的升級、SNMP 設定、儲存空間存取及電子郵件伺服器。您可以檢視系統屬性，但禁止修改。



附註

請在主系統上完成下列程序。

開始之前

- 請在次要虛擬機器上從 OVA 檔案安裝 Cisco WebEx，用作您的高可用性系統。



附註

您的高可用性系統大小必須與主系統大小相同。

- 您的高可用性系統必須使用與主系統相同的 OVA 和修補程式進行設定。如果您的主系統和高可用性系統的版本不符，則會指示您升級至較高的版本。
- 複製高可用性虛擬機器的完整網域名稱(FQDN)。您必須瞭解FQDN，才能新增高可用性系統。
- 驗證所有虛擬機器是否正常運作。透過檢視系統監視器來確定虛擬機器狀態，如[關於儀表板, 第 103 頁](#)中所述。
- 我們建議您先取得高可用性虛擬機器的快照，再執行此程序。如果發生錯誤，則重做此快照程序。

程序

步驟 1 登入「管理」網站。

步驟 2 選取開啟維護模式。

步驟 3 在主系統上的「系統」區段中，選取檢視更多鏈結。

步驟 4 選取新增高可用性系統。

步驟 5 遵循系統屬性頁面上的指示，以新增此 HA 系統。

步驟 6 輸入高可用性系統的管理網站虛擬機器的 FQDN，並選取繼續。
我們將為此新增 HA 程序驗證主系統和 HA 系統的準備度。

- 如果兩個系統都已準備就緒，則您會看到一個綠色**新增**按鈕。請勿選取它，直到您將系統置於維護模式中。
- 如果系統未準備就緒，則您會看到一條錯誤訊息。修正錯誤，然後再次嘗試新增高可用性程序。

步驟 7 選取新增。

附註 如果顯示錯誤「錯誤碼：資料庫 64」，請使用高可用性虛擬機器的快照來重複此程序。

您的高可用性系統已新增，且會自動設定為在主系統出現故障時充當備份。

- 步驟 8** 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，系統會重新開機。您可以在重新啟動完成後，重新登入管理網站。
-

測試系統

本節中列示一些在系統上執行的建議測試。您可以使用本產品支援頁面上提供的兩個診斷工具，來完成這些測試並驗證您的系統：「會議測試」及「系統資源測試」。

測試升級的系統時，您可以保留原始系統直到您完成測試升級的系統為止（但您無法同時開啓兩個系統）。對升級的系統測試結果感到滿意後，您可以移除（永久）原始系統。移除或刪除現有系統時，請確定您的升級系統正在執行。這樣可以避免意外移除基本虛擬機器磁碟 (VMDK) 檔案，升級系統可能會存取該檔案。

- 新增、編輯、啟動及停用使用者。
- 排定和舉行場會議。
- 重新排定現有會議。
- 刪除一系列會議或未來的會議。
- 開啓會議附件。
- 播放會議錄製檔。



第 8 章

將系統擴充為較大的系統大小

- [準備系統擴充, 第 77 頁](#)
- [準備系統更改程序, 第 78 頁](#)
- [使用自動部署來擴充系統, 第 79 頁](#)
- [使用手動部署來擴充系統, 第 83 頁](#)
- [測試系統, 第 86 頁](#)

準備系統擴充

本節說明系統擴充的先決條件。

系統擴充要求在擴充系統上重新主控現有的系統授權。（請參閱[在軟體升級或系統擴充之後重新主控授權](#)）。

判斷新系統的大小

請考慮以下幾項：

- 任何其他硬體的預算
- 未來幾個月的預期並行會議數及其平均大小

取得系統擴充所需的資訊

- 取得用於安裝現有系統版本的 OVA 檔案。
- 完成擴充檢查清單。

欄位名稱	系統的目前值
WebEx 網站 URL	
管理網站 URL	

欄位名稱	系統的目前值
私人 VIP 位址	
公用 VIP 位址	

準備系統更改程序

本節說明如何準備主系統更改程序：透過建立系統備份，擴充系統、新增高可用性系統、啓用公開存取、更新或升級系統等。

儘管您可以選擇這樣做，但是擴充或升級系統無需備份。在擴充或升級期間，要部署新系統並將現有系統的資料傳送給新系統。如果擴充或升級有問題，則可以關閉新系統的電源並繼續使用現有系統。



注意

由於此程序需要以獨佔方式存取系統，因此使用者無法存取會議的系統。請務必將此程序排定在對使用者干擾最少的時間進行。

其他系統管理員不應在進行此程序期間存取系統。如果他們這樣做，系統不會儲存其變更，並且結果可能難以預料。他們必須等到此程序完成，然後再登入 Cisco WebEx 管理以執行其作業。



附註

在開始系統更改程序之前，請務必與其他系統管理員協調。



注意

如果您不需要建立虛擬機器的備份，則不需要完成此程序。但是，Cisco 建議的最佳作法是建立備份。備份可讓您在程序失敗時還原系統。

程序

步驟 1 登入 Cisco WebEx 管理網站。

步驟 2 選取開啟維護模式。

步驟 3 使用 VMware Data Recovery (自 vSphere 5.1 版起稱為 VMware vSphere Data Protection) 來建立每個虛擬機器的備份。

備份可協助您將虛擬機器恢復為系統更改程序之前的狀態。如需進一步資訊，請參閱 [使用 VMware vCenter 來建立備份, 第 4 頁](#)。如需此備份的完整詳細資訊，請參閱《VMware Data Recovery 管理指南》或《vSphere Data Protection 管理指南》。

附註 如果您準備進行擴充或升級，請移除現有系統上的所有 VMware 快照。這樣可以避免意外移除 Hard disk 4 的基本 VMDK 檔案，擴充或升級系統可能會存取該檔案。

步驟 4 重新登入 Cisco WebEx 管理網站，但不關閉維護模式。

步驟 5 繼續執行系統更改程序。

使用自動部署來擴充系統

在開始之前



附註

將擴充前的系統稱為原始系統。將擴充後的系統稱為擴充系統。

將系統擴充排定在對使用者干擾最少的時間進行。

請先將主要系統設定為維護模式，然後再開始系統擴充。



注意

由於此程序需要以獨佔方式存取系統，因此使用者無法存取會議的系統。請務必將此程序排定在對使用者干擾最少的時間進行。

開始系統更改程序之前，請與其他系統管理員協調。其他系統管理員不應在進行此程序期間存取系統。如果他們這樣做，則系統不會儲存其變更，並且結果可能無法預期。

擴充系統之前的考量

- 在開始擴充程序之前，務必先移除原始系統上的所有 VMware 快照。
- 可以在擴充系統中重複使用原始虛擬機器的相同主機名稱和 IP 位址。但是，只能將原始系統或擴充系統開啓電源；這兩個系統不能同時開啓且在執行中。
- 如果原始系統上具有 HA，則部署擴充系統後，必須將 HA 新增至擴充系統。無法重複使用 HA 系統，因為它未在擴充後保留。
- 可以在完成對擴充系統的測試之前保留原始系統。在測試完成後，如果您對擴充系統滿意，則可以移除原始（擴充前）系統。
- 原始系統和擴充系統的內部虛擬機器必須位於同一個子網路上。
- 如果您已新增公開存取，則原始系統和擴充系統的「網際網路反向 Proxy」虛擬機器必須位於同一個子網路上。
- 當您對系統新增虛擬機器時，您的現行安全憑證及公開和私密金鑰都將變成無效且需要更新，除非您使用自我簽署的憑證。
憑證包含主機名稱與 URL。憑證與金鑰會變成無效的原因是它們不包含新的虛擬機器。如需關於憑證與金鑰的完整資訊，請參閱[管理憑證](#)。
- 確保擴充系統可以存取原始系統管理虛擬機器的磁碟。您會將 Hard disk 4 複製到擴充系統。
- 移除或刪除原始系統時，請確保擴充系統已啓動且在執行中。這樣可以防止意外移除 Hard disk 4 的基本 VMDK 檔案，因為擴充系統可能會存取該檔案。

擴充系統

擴充系統的整體作業為：

- 1 建立原始系統的備份。
- 2 使用部署原始系統所使用的相同 OVA 檔案，將管理虛擬機器部署為新的系統大小。
- 3 將資料從原始系統複製到擴充系統的「管理」虛擬機器。
- 4 將任何其他虛擬機器部署為新的系統大小。
- 5 測試擴充系統。
- 6 重新主控授權。

使用自動部署來擴充系統的作業摘要



附註

此表格包含指向《Cisco WebEx Meetings Server 管理指南》其他小節的鏈結。這些小節分別會提供有關特定作業的詳細資訊。在您完成每個作業之後，可回到此表格以完成下一個作業。（使用 Adobe Acrobat 中的「前一檢視」與「後一檢視」，可在此表格與個別作業程序之間輕鬆移動。）

作業	描述	如需取得詳細資訊，請參閱
1	準備要進行擴充的原始系統。	您在本章前面已完成此作業。表格中包含此作業是為了完整性。
2	準備執行系統更改程序。	您在本章前面已完成此作業。表格中包含此作業是為了完整性。
3	從原始系統的管理網站起始擴充程序。	擴充系統大小
4	使用 VMware vSphere 用戶端，在原始系統的虛擬機器上選取 Power > Shut Down Guest 。	
5	使用 vSphere 用戶端，將管理虛擬機器部署為新的系統大小。	透過 VMware vSphere 用戶端部署 OVA 檔案, 第 16 頁
6	將 Hard disk 4 從原始系統的「管理」虛擬機器附加到擴充系統的「管理」虛擬機器。	將現有 VMDK 檔案附加至新虛擬機器, 第 6 頁
7	開啟擴充系統的「管理」虛擬機器，並記下部署 URL。	
9	在 Web 瀏覽器中輸入該部署 URL，並繼續部署擴充系統。	
10	為部署擴充系統選取偏好語言。	選取用於設定的語言, 第 28 頁

作業	描述	如需取得詳細資訊，請參閱
11	確認系統大小。（此系統大小必須大於或等於原始系統。）	確認您的系統的大小, 第 29 頁
13	選取安裝主要系統。	選擇要安裝的系統, 第 29 頁
14	選取自動部署。	選擇系統部署的類型, 第 30 頁
15	輸入您的 vCenter 認證，以便我們可以為您部署虛擬機器。	提供 VMware vCenter 認證, 第 30 頁
16	為媒體虛擬機器選取 ESXi 主機、資料存放區及虛擬機器連接埠群組。	選擇用於您的「媒體」虛擬機器的 vCenter 設定, 第 31 頁
17	輸入媒體虛擬機器的完整網域名稱。（如果您已使用擴充系統的項目更新您的 DNS 伺服器，則我們將為您查詢 IP 位址。）	輸入「媒體」虛擬機器的網路資訊, 第 31 頁
18	如果您想要擴充系統的公開存取，請確定已勾選建立網際網路反向 Proxy 虛擬機器勾選方塊。否則，請取消勾選此勾選方塊。 附註 如果您尚未啟用公開存取，請跳到作業 19。	新增公開存取, 第 32 頁
19	如果您已新增公開存取，請為「網際網路反向 Proxy」虛擬機器選取 ESXi 主機、資料存放區及虛擬機器連接埠群組。	選擇用於您的網際網路反向 Proxy 的 vCenter 設定, 第 32 頁
20	輸入網際網路反向 Proxy 的主機名稱和網路資訊。	輸入網際網路反向 Proxy 的網路資訊, 第 33 頁
21	輸入 WebEx 網站 URL 的公用 VIP 位址。 附註 可以輸入您用於原始系統의相同公用 VIP 位址，或變更為新的 IP 位址。如果確實需要變更，請在 DNS 伺服器中進行必要更新。	輸入公用 VIP 位址, 第 33 頁
22	輸入 WebEx 管理 URL 的專用 VIP 位址。 附註 可以輸入您用於原始系統의相同專用 VIP 位址，或變更為新的 IP 位址。如果確實需要變更，請在 DNS 伺服器中進行必要更新。	輸入專用 VIP 位址, 第 34 頁

作業	描述	如需取得詳細資訊，請參閱
23	<p>輸入 WebEx 網站 URL。參加者存取此 URL 來主持和出席會議。（此 URL 解析為專用 VIP 位址或公用 VIP 位址，視您是否使用水平分割 DNS 而定。）</p> <p>附註 可以輸入您用於原始系統的相同 WebEx 網站 URL，或變更為新的 URL。如果確實需要變更，請在 DNS 伺服器中進行必要更新。</p> <p>確定您在 DNS 伺服器上保留原始網站 URL。將您的原始網站 URL 重新導向至新網站 URL。如果使用者嘗試使用原始 URL，但您沒有將它重新導向至新的 URL，他們將無法主持或加入會議。</p>	輸入 WebEx 網站和管理 URL, 第 36 頁
24	<p>輸入 WebEx 管理 URL，管理員可透過該 URL 存取 Cisco WebEx 管理，內部參加者可透過該 URL 主持或出席會議（僅限使用水平分割 DNS 時）。（此 URL 解析為專用 VIP 位址。）</p> <p>附註 可以輸入您用於原始系統的相同 WebEx 管理 URL，或變更為新的 URL。如果確實需要變更，請在 DNS 伺服器中進行必要更新。</p>	輸入 WebEx 網站和管理 URL, 第 36 頁
25	檢查是否已進行系統所需的所有網路、DNS 伺服器及防火牆設定變更。	確認您的網路已正確設定, 第 36 頁
26	成功部署虛擬機器後，請選取下一步以繼續進行系統檢查。	部署您的虛擬機器
27	在進行系統檢查的同時，我們會以任何所需更新來更新已擴充系統，以符合原始系統在擴充之前的軟體版本。（此更新最多可能需要一小時。）完成後，系統便會重新啟動。	檢查您的系統
28	登入 Cisco WebEx 管理。	
29	測試擴充系統。如果擴充失敗，則請關閉擴充系統的電源，並開啟原始系統的電源。請聯絡 Cisco TAC 以取得進一步協助。	測試系統
30	重新主控適合於擴充系統的授權。	關於授權在軟體升級或系統擴充之後重新主控授權

使用手動部署來擴充系統

在開始之前



附註

將擴充前的系統稱為原始系統。將擴充後的系統稱為擴充系統。

將系統擴充排定在對使用者干擾最少的時間進行。

請先將主要系統設定為維護模式，然後再開始系統擴充。



注意

由於此程序需要以獨佔方式存取系統，因此使用者無法存取會議的系統。請務必將此程序排定在對使用者干擾最少的時間進行。

開始系統更改程序之前，請與其他系統管理員協調。其他系統管理員不應在進行此程序期間存取系統。如果他們這樣做，則系統不會儲存其變更，並且結果可能無法預期。

擴充系統之前的考量

- 在開始擴充程序之前，務必先移除原始系統上的所有 VMware 快照。
- 可以在擴充系統中重複使用原始虛擬機器的相同主機名稱和 IP 位址。但是，無論何時，只能是原始系統或擴充系統中的一個處於開啓狀態。這兩個系統不能同時處於開啓和執行狀態。
- 如果已將 HA 系統新增至原始系統，則部署擴充系統之後，必須新增 HA 系統。無法重複使用原始 HA 系統，因為它未在擴充後保留。
- 可能想要在完成對擴充系統的測試之前保留原始系統。在測試完成後，如果您對擴充系統滿意，則可以移除原始（擴充前）系統。
- 原始系統和擴充系統的內部虛擬機器必須位於同一個子網路上。
- 如果已新增公開存取，則原始系統和擴充系統的「網際網路反向 Proxy」虛擬機器必須位於同一個子網路上。
- 當您對系統新增虛擬機器時，您的現行安全憑證及公開和私密金鑰都將變成無效且需要更新，除非您使用自我簽署的憑證。
憑證包含主機名稱與 URL。憑證與金鑰會變成無效的原因是它們不包含新的虛擬機器。如需有關憑證與金鑰的完整資訊，請參閱[管理憑證](#)，第 207 頁。
- 確保擴充系統可以存取原始系統管理虛擬機器的磁碟。您將把 Hard disk 4 複製到擴充系統。
- 移除或刪除原始系統時，請確保擴充系統已啓動且在執行中。這樣可以防止意外移除 Hard disk 4 的基本 VMDK 檔案，擴充系統可能會存取該檔案。

擴充系統

擴充系統的整體作業為：

- 1 建立原始系統的備份。

- 2 使用部署原始系統所使用的相同 OVA 檔案，將管理虛擬機器部署為新的系統大小。
- 3 將資料從原始系統複製到擴充系統的「管理」虛擬機器。
- 4 使用 OVA，將任何其他虛擬機器部署為新的系統大小。
- 5 測試擴充系統。
- 6 重新主控授權。

使用手動部署擴充系統的作業摘要



附註

此表格包含指向《Cisco WebEx Meetings Server 管理指南》其他小節的鏈結。這些小節分別會提供有關特定作業的詳細資訊。在您完成每個作業之後，可回到此表格以完成下一個作業。（使用 Adobe Acrobat 中的「前一檢視」與「後一檢視」，可在此表格與個別作業程序之間輕鬆移動。）

作業	描述	如需取得詳細資訊，請參閱
1	準備要進行擴充的原始系統。	您在本章前面已完成此作業。表格中包含此作業是為了完整性。
2	準備執行系統更改程序。	您在本章前面已完成此作業。表格中包含此作業是為了完整性。
3	從原始系統的管理網站起始擴充程序。	擴充系統大小
4	使用 VMware vSphere 用戶端，在原始系統的虛擬機器上選取 Power > Shut Down Guest 。	
5	使用 vSphere 用戶端，將管理虛擬機器部署為新的系統大小。 附註 此時，您還可以為系統建立其他虛擬機器。	透過 VMware vSphere 用戶端部署 OVA 檔案, 第 16 頁
6	將 Hard disk 4 從原始系統的「管理」虛擬機器附加到擴充系統的「管理」虛擬機器。	將現有 VMDK 檔案附加至新虛擬機器, 第 6 頁
7	開啟擴充系統的「管理」虛擬機器，並記下部署 URL。 附註 此時，您還可以開啟系統中其他虛擬機器的電源。請確定所有虛擬機器的電源已順利開啟。	
9	在 Web 瀏覽器中輸入該部署 URL，並繼續部署擴充系統。	
10	為部署擴充系統選取偏好語言。	選取用於設定的語言, 第 28 頁

作業	描述	如需取得詳細資訊，請參閱
11	確認系統大小。（此系統大小必須大於或等於原始系統。）	確認您的系統的大小, 第 29 頁
12	選取安裝主要系統。	選擇要安裝的系統, 第 29 頁
13	選取手動部署。	選擇系統部署的類型, 第 30 頁
14	如果您想要擴充系統的公開存取，請確定已勾選建立網際網路反向 Proxy 虛擬機器勾選方塊。否則，請取消勾選此勾選方塊。	新增公開存取, 第 32 頁
15	輸入 WebEx 網站 URL 的公用 VIP 位址。 附註 可以輸入您用於原始系統的相同公用 VIP 位址，或變更為新的 IP 位址。如果確實需要變更，請在 DNS 伺服器中進行必要更新。	輸入公用 VIP 位址, 第 33 頁
16	輸入 WebEx 管理 URL 的專用 VIP 位址。 附註 可以輸入您用於原始系統的相同專用 VIP 位址，或變更為新的 IP 位址。如果確實需要變更，請在 DNS 伺服器中進行必要更新。	輸入專用 VIP 位址, 第 34 頁
17	輸入 WebEx 網站 URL。參加者存取此 URL 來主持和出席會議。（此 URL 解析為專用 VIP 位址或公用 VIP 位址，視您是否使用水平分割 DNS 而定。） 附註 可以輸入您用於原始系統的相同 WebEx 網站 URL，或變更為新的 URL。如果確實需要變更，請在 DNS 伺服器中進行必要更新。 確定您在 DNS 伺服器上保留原始網站 URL。將您的原始網站 URL 重新導向至新網站 URL。如果使用者嘗試使用原始 URL，但您沒有將它重新導向至新的 URL，他們將無法主持或加入會議。	輸入 WebEx 網站和管理 URL, 第 36 頁
18	輸入 WebEx 管理 URL，管理員可透過該 URL 存取 Cisco WebEx 管理，內部參加者可透過該 URL 主持或出席會議（僅限使用水平分割 DNS 時）。（此 URL 解析為專用 VIP 位址。） 附註 可以輸入您用於原始系統的相同 WebEx 管理 URL，或變更為新的 URL。如果確實需要變更，請在 DNS 伺服器中進行必要更新。	輸入 WebEx 網站和管理 URL, 第 36 頁

作業	描述	如需取得詳細資訊，請參閱
19	檢查是否已進行系統所需的所有網路、DNS 伺服器及防火牆設定變更。	確認您的網路已正確設定, 第 36 頁
20	成功部署虛擬機器後，請選取下一步以繼續進行系統檢查。	部署您的虛擬機器
21	在進行系統檢查的同時，我們會以任何所需更新來更新已擴充系統，以符合原始系統在擴充之前的軟體版本。（此更新最多可能需要一小時。）完成後，系統便會重新啟動。	檢查您的系統
22	登入 Cisco WebEx 管理。	
23	測試擴充系統。如果擴充失敗，則請關閉擴充系統的電源，並開啓原始系統的電源。請聯絡 Cisco TAC 以取得進一步協助。	測試系統
24	重新主控適合於擴充系統的授權。	關於授權在軟體升級或系統擴充之後重新主控授權

測試系統

本節中列示一些在系統上執行的建議測試。您可以使用本產品支援頁面上提供的兩個診斷工具，來完成這些測試並驗證您的系統：「會議測試」及「系統資源測試」。

測試升級的系統時，您可以保留原始系統直到您完成測試升級的系統為止（但您無法同時開啓兩個系統）。對升級的系統測試結果感到滿意後，您可以移除（永久）原始系統。移除或刪除現有系統時，請確定您的升級系統正在執行。這樣可以避免意外移除基本虛擬機器磁碟 (VMDK) 檔案，升級系統可能會存取該檔案。

- 新增、編輯、啟動及停用使用者。
- 排定和舉行場會議。
- 重新排定現有會議。
- 刪除一系列會議或未來的會議。
- 開啓會議附件。
- 播放會議錄製檔。



第 9 章

更新系統

- [更新系統, 第 87 頁](#)
- [連接 CD/DVD 光碟機中的 ISO 映像檔, 第 88 頁](#)
- [繼續更新程序, 第 89 頁](#)
- [完成更新, 第 90 頁](#)

更新系統

由於更新程序需要以獨佔方式存取系統，因此使用者無法存取會議的系統。務必將更新排定在對使用者造成最少干擾的期間。

其他系統管理員不應在進行此程序期間存取系統。如果他們這麼做，將不會儲存其變更項目且結果無法預測；他們必須等到此程序完成之後才能登入 Cisco WebEx 管理網站。

視系統大小和資料庫大小而定，完整的更新程序（包括備份虛擬機器）最多可能需要一小時的時間。

開始之前

從 Cisco 取得最新的更新檔案：

[Cisco 軟體下載（外部）](#)

用於系統的更新套件包含 ISO 映像檔。不能跳過軟體的某些版本。例如，必須安裝 Cisco WebEx Meetings Server 1.1 版（建置編號 1.1.1.9.A）或 1.5 版（建置編號 1.5.1.6.A），然後才能套用 1.5 MR2。

程序

- 步驟 1 登入 Cisco WebEx 管理網站。
- 步驟 2 選取開啟維護模式。
- 步驟 3 選取系統標籤，然後選取升級。
- 步驟 4 選取更新。
- 步驟 5 在 VMware vSphere 用戶端中，對系統中的每個虛擬機器選取 **Power > Shut Down Guest**。

如需使用 vSphere 的完整詳細資訊，請參閱 VMware ESXi 和 vCenter Server 文件。

- 步驟 6** 關閉虛擬機器之後，使用 VMware Data Recovery（或隨附於 vSphere 5.1 版的 VMware vSphere Data Protection）來建立每個虛擬機器的備份。
必要時，備份會將虛擬機器回復為更新之前的狀態。如需進一步資訊，請參閱[使用 VMware vCenter 來建立備份, 第 4 頁](#)。如需此備份的完整詳細資訊，請參閱《VMware Data Recovery 管理指南》或《vSphere Data Protection 管理指南》。

附註 您也可以擷取快照，但應該在大約 24 小時內刪除所有快照，否則可能會遇到資料效能問題。如需相關資訊，請參閱[使用 VMware vCenter 來擷取快照](#)。

注意 建立所有虛擬機器的備份，因為更新程序會變更現有虛擬機器，而且一旦開始更新程序，就無法復原更新。

- 步驟 7** 在 VMware vSphere 用戶端中，開啓系統中每個虛擬機器的電源。

- 步驟 8** 登入 Cisco WebEx 管理網站，但不關閉維護模式。

- 步驟 9** 選取系統標籤，然後選取升級。

- 步驟 10** 選取更新，以返回更新系統頁面。

下一步動作

請移至[連接 CD/DVD 光碟機中的 ISO 映像檔](#)。

連接 CD/DVD 光碟機中的 ISO 映像檔

爲了讓更新快速完成，Cisco 建議您將 ISO 映像掛接在 vCenter 資料存放區中。但是，如果將它置於 vSphere 用戶端上的本地磁碟中，請確保 vSphere 用戶端具有對公司內部網路的實體連線（不是透過 VPN）。

若要将 ISO 映像檔放入 vCenter 資料存放區並連接 CD/DVD，請完成下列步驟：

開始之前

從 Cisco 取得需要的 ISO 映像檔：

[下載軟體](#)

確認您具有適當的權限。

程序

- 步驟 1 為管理虛擬機器選取 ESXi 主機。選取 **Summary** 標籤，然後連按兩下 **Storage** 下方的 **datastore1** 名稱。
- 步驟 2 在 **Datastore and Datastore clusters** 視窗上，選取 **Browse this datastore**。
- 步驟 3 選取綠色向上箭頭圖示 (上傳檔案)，並載入更新 ISO 檔案。
- 步驟 4 選取 VMware vCenter 庫存中的「管理」虛擬機器。
- 步驟 5 選取管理虛擬機器的 **CD/DVD** 圖示。
- 步驟 6 選取本地磁碟或資料存放區上的 **CD/DVD drive 1 > Connect to ISO image**。
- 步驟 7 確認 CD/DVD 光碟機已連線。
 - a) 在 vCenter 庫存中的「管理」虛擬機器名稱上按一下滑鼠右鍵，然後選取 **Edit Settings...**。
 - b) 在 **Hardware** 標籤中，選取 **CD/DVD drive 1**。
 - c) 如果已取消勾選，請勾選 **Connected** 勾選方塊。
 - d) 選取確定。

繼續更新程序

開始之前

您已完成：

- [更新系統, 第 87 頁](#)
- [連接 CD/DVD 光碟機中的 ISO 映像檔, 第 88 頁](#)

程序

- 步驟 1 在連線更新 ISO 映像之後，選取位於 Cisco WebEx 管理網站的**更新系統**頁面下的**繼續**。
- 步驟 2 勾選我已連線至 **ISO** 檔案且已做好繼續的準備勾選方塊。
- 步驟 3 選取**繼續**。

注意 選取繼續後，您將無法停止更新程序。如果在更新程序中發生問題，且未順利完成更新，則您必須使用備份來還原系統。

更新程序最多可能需要一小時的時間。請勿關閉瀏覽器視窗，因為您會無法返回此頁面。

更新完成後，即會顯示新的頁面，以確認更新成功。

附註 更新成功完成時，會存在間歇性問題，但您看不到說明**系統已更新**和**重新啟動**按鈕的文字。如果更新未完成，且時間超過一小時，則您可以嘗試關閉維護模式。如果您無法關閉維護模式，則表示更新仍在進行中。更新完成後，從 vCenter 重新啟動所有虛擬機器。等待虛擬機器進入線上狀態，並在儀表板上驗證系統版本。
- 步驟 4 選取**重新啟動**以重新啟動系統。

本頁的預設逾時值為 90 分鐘。請務必在此時段內重新啟動系統，或將預設逾時值變更爲更長的時段。

下一步動作

繼續執行[完成更新](#), 第 90 頁。

完成更新

開始之前

這是[繼續更新程序](#), 第 89 頁的延續。

程序

- 步驟 1** 更新成功完成後，選取**重新啟動**。
系統重新啟動後，即會顯示 Cisco WebEx 管理網站登入頁。
 - 步驟 2** 登入 Cisco WebEx 管理。更新的版本會顯示在儀表板上。
 - 步驟 3** 檢查此更新的發行說明，並確定是否需要任何更新後作業。如果需要其他作業，請先完成這些作業，然後再將系統退出維護模式。
 - 步驟 4** 完成任何更新後設定之後，選取**關閉維護模式**。
 - 步驟 5** 測試並檢查系統。您可以使用本產品支援頁面上提供的兩個診斷工具，來完成這些測試並驗證您的系統：「會議測試」及「系統資源測試」。
 - 新增、編輯、啟動及停用使用者。
 - 排定和舉行場會議。
 - 重新排定現有會議。
 - 刪除一系列會議或未來的會議。
 - 開啓會議附件。
 - 播放會議錄製檔。
-

下一步動作

- 如果您發現問題，則請使用 VMware Data Recovery (vSphere Data Protection) 或系統快照，以還原爲先前的版本。請檢查 ISO 網路連線並確定沒有任何問題。
- 如果更新成功，請使用已更新的系統一段時間。感到滿意後，請務必先刪除建立的虛擬機器備份或快照，然後再進行更新。



第 10 章

升級系統

- 準備升級, 第 91 頁
- 自動升級系統, 第 92 頁
- 手動升級系統, 第 94 頁
- 測試系統, 第 96 頁
- 授權重新主控與升級, 第 96 頁

準備升級

您可以透過使用升級的 OVA（虛擬伺服器範本）檔案重新部署系統來完成升級作業。升級定義為更換系統以部署我們對系統所做的重大修改。例如，將目前執行 1.0 版的系統更換為執行 2.0 版，該版本包含對新作業系統的支援。如果要更新至維護 (MR) 版本或修補程式，請一律使用[更新系統](#)程序。在發行說明中檢查是否有正確的程序供使用。在這兩種情況下，原始系統的所有資料都會傳輸至更新的或升級的系統。

可以自動或手動升級系統。我們建議您使用自動過程升級系統。

升級時：

- 可以升級至應用程式的下一個完整版本。例如，將系統從 1.5 升級至 2.0。將系統從 1.1 更新至 1.5；請勿嘗試將系統升級至增量版本。
- 升級 Cisco WebEx Meeting Server 時，儲存在原始系統上的日誌擷取不會傳送至更新的 Cisco WebEx Meeting Server 系統。因此，開始升級前，應該從原始系統擷取和下載您需要的任何日誌及日誌擷取。
- 對於 Cisco WebEx Meetings Server 2.0 版的新安裝，則具有「管理」虛擬機器的 ESXi 主機（Cisco UCS 伺服器）需要 1.5 TB 磁碟空間。不具有「管理」虛擬機器的 ESXi 主機（Cisco UCS 伺服器）需要 1 TB 磁碟空間。使用現有 Cisco UCS 伺服器從 Cisco WebEx Meetings Server 1.x 版升級至 2.0 版時，如果 UCS 伺服器僅具有「管理」虛擬機器（主要系統或 HA 系統），則 ESXi 主機將需要 1118 GB 的可用磁碟空間；如果 UCS 伺服器具有一個「管理」虛擬機器和一個「媒體」虛擬機器（主要系統或 HA 系統），則將需要 990 GB 的可用磁碟空間。磁碟空間可以是

本端 (DAS) 或外部 (SAN 或 NAS)。如需完整詳細資料，請參閱[系統需求](#)中的「Cisco WebEx Meetings Server 和 ESXi 主機使用的資源」小節。



附註

我們將起始升級前未改變的系統稱為原始系統。升級後的系統稱為升級的系統。

開始自動或手動升級之前

自動或手動升級系統之前，應該先解決下列問題：

- 取得升級所需 OVA 檔案。
- 為原始（現有）系統上的各虛擬機器建立備份。（請參閱[使用 VMware vCenter 來建立備份](#)。）
- 計劃一次維護性中斷。升級程序期間，原始系統置於維護模式且需要以獨佔方式存取系統；在此時間段，使用者無法存取會議的系統。將升級的這部分排定在對使用者造成最少干擾的時間。
- 請為資料存放區規劃增加的大小，因為原始系統及升級系統會共用資料存放區，直到完成升級系統測試並移除原始系統。
- 升級的系統中會重新使用原始系統主機名稱和 IP 位址。這兩個系統的內部虛擬機器位於同一子網路。如果您已新增公開存取，則原始系統和升級的系統的網際網路反向 Proxy 虛擬機器應位於相同的子網路。

自動升級系統

開始自動升級之前

使用自動程序升級系統之前，應該先解決下列問題：

- 通知其他系統管理員，在升級期間他們不應存取原始系統或對其做出變更，因為其變更可能會產生無法預測的結果。
- 提供并設定一個額外的 IP 位址，該位址將暫時用於升級的系統。
- 請勿手動開啓或關閉任一系統。
- 確定升級系統可以存取用於原始系統之管理虛擬機器的磁碟。

使用自動升級

此表格列出了完成自動升級所需的高層次作業。其中包含《*Cisco WebEx Meetings Server* 管理手冊》的各節鏈結，它們提供完成每個作業所需的詳細步驟。（選取 Adobe Acrobat 中的「前一檢視」與「後一檢視」，可在此表格與個別作業之間輕鬆移動。）

作業	描述	如需取得詳細資訊，請參閱
1	透過選取系統 > 檢視更多 > 管理授權，來移至原始系統上的 License Manager，並產生授權請求。License Manager 會在新標籤中開啓。 選取產生授權請求。此時會出現一個包含授權請求文字的快顯功能表。複製文字並將授權請求儲存在方便的位置，因為使用手動重新主控程序收回授權時可能需要。此資訊也可以協助 Cisco 找到您的授權。	透過使用 License Manager 來履行授權
2	使用 vSphere 用戶端，透過選取具有 Auto-upgrade 尾碼的配置（例如， 250 Users Admin Auto-upgrade ）來部署升級系統的「管理」虛擬機器。	
3	開啓升級系統管理虛擬機器的電源，然後記下虛擬機器主控台上顯示的部署 URL。	
4	在 Web 瀏覽器 URL 欄位中輸入部署 URL。	
5	輸入管理和 vCenter URL 及認證，以便我們為您部署虛擬機器。	提供 VMware vCenter 認證
6	若要部署任何額外的虛擬機器，請選取繼續。（直到您開始設定升級的系統且原始系統處於維護模式，使用者可主持會議，但管理員不得修改原始系統虛擬機器。）	升級進度會顯示在升級系統的部署 URL 上，及主要系統管理虛擬機器所連接的 VMware 主控台上。
7	記下 vCenter 中所列出自動建立的虛擬機器的名稱。 虛擬機器名稱的格式如下： CWMS_hostname_MMDDHHmm 其中 mm=分鐘 升級完成後，虛擬機器不會顯示。若要尋找 CWMS 升級過程中建立的虛擬機器，您可以根據此格式搜尋。	VMware 主控台提供了執行升級程序期間，瀏覽器視窗意外關閉時要使用的部署 URL。
8	若要自動將系統置於維護模式並開始設定升級的系統，請選取繼續。啓用「維護模式」時，會顯示一則訊息，說明可能需要長達 30 分鐘。	
9	若要啓動升級的 Cisco WebEx 管理網站，請選取登入管理網站。	
10	在升級的系統上關閉維護模式。系統重新啓動。	可能需要幾分鐘的時間，會議服務才能變為可用。如果系統內容頁面上列出的所有虛擬機器都顯示「良好」狀態（綠色），則系統已備妥，使用者可以順利地開始會議。如需相關資訊，請參閱 開啓或關閉維護模式 。

作業	描述	如需取得詳細資訊，請參閱
11	測試升級的系統。如果升級失敗，請關閉升級系統的電源，開啓原始系統的電源，然後聯絡 Cisco TAC。	測試系統
12	重新主控並更新適合於升級系統的授權版本。在 180 天內，免費授權的寬限期應該會到期。如果原始系統具有有效的授權，則必須在 180 天的時間內重新主控這些授權。如果原始系統是在免費授權寬限期內作業，則剩餘的未到期天數會轉移至升級系統。	關於授權在軟體升級或系統擴充之後重新主控授權

手動升級系統

開始手動升級之前

升級系統之前，應該先解決下列問題：

- 移除原始（現有）系統的所有 VMware 快照。
- 請勿同時開啓兩個系統的電源並執行，因為原始虛擬機器的主機名稱和 IP 位址均用於升級的系統。
- 確定升級系統可以存取用於原始系統之管理虛擬機器的磁碟。（Hard disk 4 將從原始系統複製到升級的系統。）

手動升級系統的作業

此表格的部分工作包含指向《Cisco WebEx Meetings Server 管理指南》其他小節的鏈結。這些小節提供該工作的詳細資訊。（選取 Adobe Acrobat 中的「前一檢視」與「後一檢視」，可在此表格與個別作業之間輕鬆移動。）

作業	描述	如需取得詳細資訊，請參閱
1	透過選取系統 > 檢視更多 > 管理授權，來移至原始系統上的 License Manager，並產生授權請求。License Manager 會在新標籤中開啓。 選取產生授權請求。此時會出現一個包含授權請求文字的快顯功能表。複製文字並將授權請求儲存在方便的位置，因為使用手動重新主控程序收回授權時可能需要。此資訊也可以協助 Cisco 找到您的授權。	關於授權
2	登入原始系統的管理網站。	
3	移至「系統」標籤並選取升級。	
4	選取主要升級。	
5	選取繼續以實現原始系統資料並將系統置於維護模式。	

作業	描述	如需取得詳細資訊，請參閱
6	使用 VMware vSphere 用戶端，在原始系統的虛擬機器上選取 Power > Shut Down Guest 。	
7	部署所有已升級的系統虛擬機器，包括 HA 和 IRP 虛擬機器。	透過 VMware vSphere 用戶端部署 OVA 檔案
8	將資料從原始系統複製到升級系統的「管理」虛擬機器。	將現有 VMDK 檔案附加至新虛擬機器
9	開啓升級管理虛擬機器的電源，然後記下虛擬機器主控台上所顯示的部署 URL。如果系統將包含高可用性 (HA)，請勿從「HA 管理部署」設定 HA 虛擬機器；請允許升級 Script 探索 HA 虛擬機器。（請參閱 配置高可用性系統 。）	
10	開啓其他升級的虛擬機器的電源。	
11	在 Web 瀏覽器中輸入部署 URL。	
12	選取繼續以啓動系統設定。	升級進度會顯示在升級系統的部署 URL 上，及主要系統管理虛擬機器所連接的 VMware 主控台上。 VMware 主控台提供了執行升級程序期間，瀏覽器視窗意外關閉時要使用的部署 URL。
13	選取關閉維護模式及繼續以進行確認。	可能需要幾分鐘的時間，會議服務才能變為可用。如果系統內容頁面上列出的所有虛擬機器都顯示「良好」狀態（綠色），則系統已備妥，使用者可以順利地開始會議。如需相關資訊，請參閱 開啓或關閉維護模式 。
14	系統設定完成時，選取登入管理網站。	
15	測試升級的系統。 當您的升級系統令人滿意地執行時，您可以刪除原始系統以釋放原始系統資源。保持升級系統執行，同時刪除原始系統以防止意外移除 Hard disk 4 基礎 VMDK 檔案，升級系統可能會存取該檔案。 如果升級失敗，請聯絡 Cisco TAC，關閉升級系統的電源，然後開啓原始系統的電源。	測試系統

作業	描述	如需取得詳細資訊，請參閱
16	重新主控並更新適合於升級系統的授權版本。在 180 天內，免費授權的寬限期應該會到期。如果原始系統具有有效的授權，則必須在 180 天的時間內重新主控這些授權。如果原始系統是在免費授權寬限期內作業，則剩餘的未到期天數會轉移至升級系統。	關於授權在軟體升級或系統擴充之後重新主控授權

測試系統

本節中列示一些在系統上執行的建議測試。您可以使用本產品支援頁面上提供的兩個診斷工具，來完成這些測試並驗證您的系統：「會議測試」及「系統資源測試」。

測試升級的系統時，您可以保留原始系統直到您完成測試升級的系統為止（但您無法同時開啓兩個系統）。對升級的系統測試結果感到滿意後，您可以移除（永久）原始系統。移除或刪除現有系統時，請確定您的升級系統正在執行。這樣可以避免意外移除基本虛擬機器磁碟 (VMDK) 檔案，升級系統可能會存取該檔案。

- 新增、編輯、啓動及停用使用者。
- 排定和舉行場會議。
- 重新排定現有會議。
- 刪除一系列會議或未來的會議。
- 開啓會議附件。
- 播放會議錄製檔。

授權重新主控與升級

重新主控允許在升級系統上使用原始系統授權達一段有限的時間。如果授權未重新主控，則無法完整升級。在 180 天內，寬限期應該會到期。在軟體升級後：

- 如果原始系統是在沒有授權的情況下作業，而且是在免費授權寬限期內，則剩餘的免費授權天數會轉移至升級系統。
- 如果原始系統具有有效授權，則這些授權的有效天數最多為 180 天，然後便必須重新主控（請參閱[在軟體升級或系統擴充之後重新主控授權](#)）及更新。

存取 GLO 請求表單

若要顯示「廣域授權作業 (GLO)」請求表單，請選取「產品授權註冊」頁面上的聯絡我們(<https://tools.cisco.com/SWIFT/LicensingUI/Quickstart>)。在「GLO 支援聯絡資訊」頁面上，選取請求。

開始之前

請準備提供下列資訊：

- 聯絡人資訊
- 問題說明
- 產品名稱及授權活動（例如重新傳送授權資訊或升級授權）
- 權益資訊（例如產品序號）

在軟體升級或系統擴充之後重新主控授權

CWMS 軟體升級或擴充且測試完成後，下一步是重新主控授權。重新主控的授權會在原始系統上自動失效。開始重新主控前，請保留來自原始系統的授權請求，以備重新主控授權之需。

重新主控授權時，您可以重新主控的授權數目限制為原始系統上的授權數目。重新主控授權的偏好方法是透過「產品授權註冊入口網站」。

如果原始系統具有授權，則升級系統會為您提供 180 天的寬限期，可讓您先測試升級系統，然後在升級系統上重新主控原始授權，之後才會要求授權。可以透過使用「產品授權註冊入口網站」<http://cisco.com/go/license> 來完成重新主控（請參閱[存取 GLO 請求表單](#)）。如果原始系統已經在寬限期內運作，則升級系統寬限期等於更新時原始系統上存在的寬限期量。如果原始系統由於缺乏授權而鎖定，則也將會鎖定升級系統。

儲存授權請求

若要獲得原始系統的授權請求：

程序

-
- 步驟 1 從原始系統管理視窗，選取系統視窗。
 - 步驟 2 選取（在「授權」下方）檢視更多 > 管理授權。
 - 步驟 3 選取產生授權請求。
 - 步驟 4 將請求儲存至 PC 上的本端資料夾。
-

註冊要重新主控的授權

使用「產品授權註冊」入口網站：

程序

-
- 步驟 1 登入「產品授權註冊」入口網站，網址為：<https://tools.cisco.com/SWIFT/LicensingUI/Quickstart>。
 - 步驟 2 登入用來履行原始系統授權的 cisco.com 帳戶。

如果此帳戶不可用或如果您登入但找不到與此帳戶關聯的授權，請向 Cisco 開啓案例（請參閱[存取 GLO 請求表單](#)）。

- 步驟 3** 選取要轉移的授權 - 起始（位於轉移功能表中）。此時會出現指定授權來源視窗。
- 步驟 4** 選取要從中重新主控授權之系統 UUID 旁邊的勾選方塊。例如，1.x 系統的 UUID。如果具有多個系統，但不知道所要重新主控的系統 UUID，請返回原始系統並啓動 License Manager。在授權視窗的檔名欄中尋找授權字串，例如 c8be79aeeccaba5922955b53679527463_201311182150051080。從字串開頭到底線字元 () 分隔符號之間的字元是 UUID。
- 步驟 5** 回到「產品授權註冊」入口網站。
- 步驟 6** 選取要重新主控的授權並選取下一步。此時會顯示指定目標和選項視窗。
- 步驟 7** 在目標系統授權請求欄位中貼上授權請求，並選取下一步。目標系統是您要將授權移入其中的系統。如果這是軟體升級，則目標是升級系統。如果這是系統擴充，則目標是較大的系統。如果這是災害復原，則目標是復原後的系統。此時會出現複查視窗。
- 步驟 8** 選取我同意授權協議的條款勾選方塊，然後按一下提交。
系統會向您傳送一封包含所重新主控授權的電子郵件。請注意，如果在軟體升級的程序中執行重新主控作業，則必須在 2.0 系統上重新主控（請參閱[在軟體升級或系統擴充之後重新主控授權](#)）並更新 1.0 授權。升級系統的管理網站上可能會顯示錯誤訊息，例如對現行部署使用的授權檔案無效。這符合預期。訊息中包含了指出將停用系統的到期日。請在到期日之前升級授權，否則將停用系統。

下一步動作

安裝在升級系統上的重新主控授權，和原始系統上的授權版本相同。例如，從 1.X 升級至 2.0 時，會向您傳送可以在 2.0 系統上辨識的 1.X 授權。安裝授權時，會顯示錯誤：對現行部署使用的授權檔案無效。如果這種情況繼續，則將於 *mm/dd/yy* 停用系統。這符合預期。（此訊息也可能透過電子郵件傳送給系統管理員。）

重新主控授權後，請在所顯示的日期之前完成授權升級，以確保系統的使用不會中斷。（請參閱[透過使用 License Manager 來履行授權](#)。）

軟體升級後升級授權

軟體升級後，將在升級的系統上從原始系統重新主控授權。（如需詳細資訊，請參閱[在軟體升級或系統擴充之後重新主控授權](#)。）重新主控授權後，可升級授權以在升級的系統上使用。

若要使用 eFulfilment 升級授權：

- 1 從供應商取得「產品授權金鑰 (PAK)」代碼。
- 2 從系統視窗選取（在授權）檢視更多>管理授權>授權>從 PAK 完成授權。隨即顯示從 PAK 完成授權。
- 3 輸入 PAK 代碼並選取下一步。
- 4 使用 cisco.com 帳戶認證登入。隨即顯示從 PAK 完成授權。
- 5 按一下「安裝」欄選取您要安裝的授權數目。
- 6 指示要安裝的授權數目，然後選取儲存。從 PAK 進行 eFulfilment 時，在系統上安裝授權。



附註

可以安裝的授權數目受限於升級 PAK 所提供的授權數目，並且不能超出已從原始系統重新主控的授權數目。

若要從授權檔案升級您的授權：

- 1 透過使用 cisco.com/go/license 從 Cisco 取得授權檔案。
- 2 從系統視窗選取（在授權）檢視更多>管理授權>授權>從檔案履行授權。隨即顯示安裝授權檔案視窗。
- 3 瀏覽授權檔案。檔案顯示在授權視窗。

授權便會自動更新。



第 **II** 部分

Cisco WebEx Meetings Server 設定指南

- [使用儀表板, 第 103 頁](#)
- [管理使用者, 第 117 頁](#)
- [設定系統, 第 137 頁](#)
- [配置設定, 第 167 頁](#)
- [管理報告, 第 225 頁](#)
- [使用支援功能, 第 231 頁](#)



第 11 章

使用儀表板

此模組說明 Cisco WebEx Server 儀表板上的功能以及如何使用這些功能。

- [關於儀表板, 第 103 頁](#)
- [檢視和編輯警報, 第 105 頁](#)
- [檢視資源歷史記錄, 第 107 頁](#)
- [檢視會議趨勢, 第 108 頁](#)
- [檢視會議清單, 第 109 頁](#)
- [排定維護時段, 第 110 頁](#)
- [變更排定的維護時段, 第 111 頁](#)
- [關於維護模式, 第 112 頁](#)
- [開啓或關閉維護模式, 第 114 頁](#)

關於儀表板

本節說明儀表板上的功能及如何使用這些功能。儀表板是管理網站的首頁，提供主要監視功能的數個參數和圖形。

儀表板包括以下區段：

- **系統監視器** — 顯示系統狀態和時間戳記，並且包括下列子區段：

會議和使用者 — 進行中會議的狀態及使用情況。顯示目前進行中的會議數目，以及參加會議的使用者數目（使用情況）。狀態 LED 指出進行中會議及使用情況是小於還是大於所配置的警報閾值。綠色狀態 LED 指出小於所配置的閾值，而紅色指出大於所配置的閾值。如需配置警報的相關資訊，請參閱[檢視和編輯警報, 第 105 頁](#)。

警報圖示 — 選取「警報」圖示來檢視及編輯所配置的警報閾值設定。警報閾值是以數字格式顯示在警報頁面上。依預設，警報閾值是以百分比形式顯示。如需配置警報的相關資訊，請參閱[檢視和編輯警報, 第 105 頁](#)。

您可以針對以下幾項設定警報：

進行中的會議 — 當目前會議遇到問題時指示。

使用情況 — 目前使用系統的使用者總數。

CPU — 虛擬機器的 CPU 使用率，及此系統中所有虛擬機器中的最高 CPU 使用率。

記憶體 — 具有最高記憶體負載的一個虛擬機器所使用的大約記憶體數量。



附註

LED 在短時間內顯示為紅色時，並不表示系統處於嚴重狀態或者需要立即注意。高記憶體使用率可能指出存在其他系統效能問題。如果記憶體使用量在一段較長的時間內超過了 90%，則我們建議您檢查 vCenter 記憶體使用量及 CPU 統計資料。如果發現這些統計資料超出範圍，請考慮修改您的系統以減少負載。

網路 — 已使用的系統頻寬總計。

儲存空間 — 已使用的錄製檔與資料庫備份儲存空間。



附註

如果您已設定儲存伺服器，即會出現儲存警報。如需相關資訊，請參閱[設定儲存伺服器](#), 第 148 頁。



附註

如果儲存體使用率大於閾值，則會停用會議錄製檔。

CPU、記憶體、網路及儲存體 — 顯示所使用資源的百分比和實際數量，及每個資源的狀態 LED。綠色狀態 LED 指出小於所配置的閾值，而紅色指出大於所配置的閾值。如需配置警報的相關資訊，請參閱[檢視和編輯警報](#), 第 105 頁。

選取「CPU、記憶體、網路或儲存體」鏈結，以存取[資源歷史記錄](#)或[儲存體歷史記錄](#)頁面。

•會議趨勢圖和會議清單 — 此圖形顯示系統上在指定時段內舉行的會議數目。使用開始和結束欄位，來設定會議趨勢資訊的時段及會議清單中所顯示會議的時段。可以選取「會議趨勢」圖形上的一個點，來列出會議清單中，於圖形上所指定時間段內發生的會議。若要檢視當日特定時間內發生的會議，請將滑鼠移至圖形上方並選取所需的時間。會議清單顯示所選時段內發生的會議總數、會議主題、主持人、參加者人數及會議狀態。可以排序會議清單中資訊的每一欄，並且會議會依狀態按順序顯示：進行中、已結束及未開始。

•維護 — 可讓您排定維護時段來配置系統或變更設定，以及開啓或關閉維護模式。如需相關資訊，請參閱[排定維護時段](#), 第 110 頁和[關於維護模式](#), 第 112 頁。

•前次系統備份 — 前次取得備份的時間和日期；備份的檔名、大小和位置；及下一個備份的日期與時間。它還會在備份失敗時通知您，以及如果尚未建立備份則通知您嘗試進行第一次備份的日期。



附註

僅在您已設定儲存伺服器時才會出現。

- 系統 — 顯示可以同時參加會議的使用者數目上限、版本號碼、產品 URL、是否允許進行公開存取、是否為高可用性系統以及使用者授權數目。如果是使用 Cisco WebEx Server 的免費試用版，且剩餘試用期不超過 30 天，則此區段也會指出試用期結束前剩餘的天數。選取[檢視更多](#)以移至 [設定系統](#), 第 137 頁。
- 使用者 — 顯示作用中使用者總數、是否配置了目錄整合、何時進行下一次同步（如果配置的話）及選定類型的驗證。選取[檢視更多](#)以移至 [編輯使用者](#), 第 124 頁。
- 設定 — 顯示每個會議中所允許的參加者人數上限、音訊類型及是否啓用了 WebEx HQ 視訊。選取[檢視更多](#)以移至 [配置設定](#), 第 167 頁。

相關主題

[檢視資源歷史記錄](#), 第 107 頁

[使用「進行中的會議」圖表解決會議問題](#), 第 107 頁

[排定維護時段](#), 第 110 頁

[開啓或關閉維護模式](#), 第 114 頁

檢視和編輯警報

程序

步驟 1 登入「管理」網站。

步驟 2 選取儀表板 > 警報。

即會出現警報頁面，其中顯示目前的警報閾值。

步驟 3 選取編輯。

即會出現編輯警報頁面。選取百分比 % 以百分比方式檢視警報閾值，或選取數量 # 以數字方式檢視警報閾值。預設設定為百分比 %。

步驟 4 選取您要啓用的警報的勾選方塊，並為每個已啓用的警報選取時間間隔。

選項	描述
進行中的會議	<p>顯示進行中會議的閾值。</p> <ul style="list-style-type: none"> •如果設定為百分比 %，請移動選取器條欄，從百分之 2 到 99 進行設定。 •如果設定為數量 #，請輸入百分之 2 到 99 之間的數字。 <p>預設： 已選取時間間隔 1 小時。</p>

選項	描述
使用情況	<p>顯示目前系統閾值。</p> <ul style="list-style-type: none"> •如果設定為百分比 %，請移動選取器條欄，從百分之 2 到 99 進行設定。 •如果設定為數量 #，請輸入使用者數目。 <p>預設：已選取時間間隔 12 小時。</p>
CPU	<p>顯示目前 CPU 閾值（以 MHz 為單位）。</p> <ul style="list-style-type: none"> •如果設定為百分比 %，請移動選取器條欄，從百分之 2 到 99 進行設定。 •如果設定為數量 #，請輸入 MHz 數目。 <p>預設：未選取。時間間隔為 1 小時。</p>
記憶體	<p>顯示目前記憶體閾值（以 GB 為單位）。</p> <ul style="list-style-type: none"> •如果設定為百分比 %，請移動選取器條欄，從百分之 2 到 99 進行設定。 •如果設定為數量 #，請輸入 GB 數目 <p>預設：未選取。時間間隔為 1 小時。</p> <p>附註 「記憶體」計量器顯示具有最高記憶體負載之虛擬機器所用的大致記憶體容量。當計量器在短時間內顯示在紅色區域中時，並不是表示系統處於嚴重狀態或者需要立即注意。記憶體使用量高可能指示應該解決其他系統效能問題。如果記憶體使用量在一段較長的時間內超過了 90%，則我們建議您檢查 vCenter 記憶體使用量及 CPU 統計資料。如果發現這些統計資料超出範圍，請考慮修改您的系統以減少負載。</p>
網路	<p>顯示目前網路頻寬閾值（以 Mbps 為單位）。</p> <ul style="list-style-type: none"> •如果設定為百分比 %，請移動選取器條欄，從百分之 2 到 99 進行設定。 •如果設定為數量 #，請輸入 Mbps 數目。 <p>預設：未選取。時間間隔為 1 小時。</p>
儲存空間	<p>顯示目前儲存空間閾值（以 GB 為單位）。最大儲存空間閾值計算方式為：總空間 - 錄製檔緩衝區大小，其中錄製檔緩衝區大小為 1 GB（微型）、5 GB（小型）、16 GB（中型）及 40 GB（大型）。</p> <ul style="list-style-type: none"> •如果設定為百分比 %，請移動選取器條欄，從百分之 2 到 99 進行設定。 •如果設定為數量 #，請輸入 GB 數目。 <p>預設：未選取。時間間隔為 1 小時。</p> <p>附註 只有在您設定儲存伺服器後，才會出現此區段。如需相關資訊，請參閱設定儲存伺服器, 第 148 頁。</p>

當警報超出臨界值時，會傳送電子郵件給管理員。時間間隔用於隱藏指定的時間內的多個警報，以避免就相同問題傳送過多的電子郵件。每個警報的時間間隔可以是：

- 1 小時
- 6 小時
- 12 小時
- 24 小時

步驟 5 選取儲存。

即會儲存您的警報設定，且警報頁面會以您的變更進行更新。

檢視資源歷史記錄

您的資源歷史記錄包含系統上設定的每個警報的詳細圖表。系統狀態、會議、參加者和儲存體的目前值顯示在右側面板中。如需取得您可以設定的警報的更多資訊，請參閱[檢視和編輯警報](#)。

若要檢視資源歷史記錄，則可以選取警報 **CPU**、記憶體或網路鏈結（位於儀表板視窗上）。例如，選取 **CPU** 鏈結即會出現資源歷史記錄視窗。

如果配置了儲存伺服器，則可以透過選取儀表板視窗上的儲存體鏈結來檢視儲存體歷史記錄。儲存體歷史記錄頁面會顯示儲存伺服器上已使用的空間，並且會顯示一個圖形，此圖形會顯示過去六個月所使用的儲存體空間。將滑鼠移至藍色的使用情形圖形，來查看過去六個月內某些天和時間使用的空間百分比。

使用「進行中的會議」圖表解決會議問題

當您收到電子郵件指出會議出現問題，請執行下列步驟以判定原因。

程序

步驟 1 選取您收到的會議問題電子郵件中的鏈結。

步驟 2 登入「管理」網站。

步驟 3 在儀表板上，選取 **CPU**、記憶體、或網路鏈結。
此時，會顯示資源歷史記錄。

步驟 4 在資源圖形右側顯示的側面板上，選取正在進行的會議鏈結。

步驟 5 可選擇性地選取檢視選項或者行事曆圖示，以顯示特定時段的會議。

步驟 6 可選擇性地選取顯示未來會議勾選方塊，以將未來的排定會議併入到會議清單中。

步驟 7 按一下參加者或會議圖形上的資料點，以顯示會議資訊。

您可以使用表格中顯示的詳細資訊，協助判定所收到電子郵件中描述的問題原因。會議清單會顯示對應於所選資料點的會議詳細資料。存在效能問題的會議在「狀態」欄中顯示為紅色或黃色。

在上表的欄位中輸入搜尋詞，以過濾會議清單。可透過選取關鍵字欄的標題來排序會議清單。

步驟 8 目前系統狀態會顯示在頁面的右欄。選取此行來回到儀表板。
系統狀態可能是：

- 良好 - 系統上的所有服務均在作業中。
- 關閉 - 系統上的所有服務均不在執行中。請聯絡「Cisco 技術協助中心 (TAC)」以尋求協助。
如需相關資訊，請參閱[使用支援功能](#)。

步驟 9 選取右欄的警報狀態方塊，以查看警報的「資源歷史記錄」。如需相關資訊，請參閱[檢視資源歷史記錄](#)。

步驟 10 如果已配置儲存伺服器，則會在頁面的右欄中顯示儲存空間量。如需相關詳細資訊，請參閱[檢視和編輯警報](#), 第 105 頁。

檢視會議趨勢

程序

步驟 1 登入「管理」網站。

步驟 2 選取儀表板。

步驟 3 在會議趨勢圖形上方，透過選取開始和結束日期與時間來設定趨勢期間。

- 排在午夜之前及延伸至第二天的會議，會依會議開始日期顯示在圖上。
- 如果某會議由於系統問題而中斷連線，然後又重新連線，則此會議會在會議趨勢圖上計算兩次。
- 由於一個月與六個月的會議趨勢資料檢視是以格林威治標準時間 (GMT) 為根據，因此無法準確地顯示 24 小時內的資料。例如，如果您的系統在給定的某一天主控了 200 個會議，則資料庫會根據 GMT（而非當地時間）來記錄這些會議項目。一天與一週的會議趨勢資料檢視是基於使用者的時區。
- 綠色軌道指出會議正在進行中或已結束。未來的會議顯示為黃色。
- 如果所選時間範圍為 24 小時，則已過去或進行中會議的資料點是使用五分鐘的間隔，並且未來會議則是使用一小時的間隔。
- 如果所選時間範圍長於一天，但短於或等於一週，則已過去、進行中或未來會議的資料點則會使用一小時的間隔顯示。
- 如果所選時間範圍長於一週，則已過去、進行中或未來會議的資料點則會使用一天的間隔顯示。

會議趨勢圖形會顯示所選時段內發生的會議總數。圖形下方的會議清單會列出所選趨勢期間的所有會議。

附註 部分會議趨勢項目可能顯示為重複項目，因為它們具有相同的名稱。每次開始會議時都會建立一個項目。因此，如果會議已開始、停止並重新啟動，則會顯示多個具有相同會議名稱的項目。

步驟 4 若要檢視特定時間發生的會議清單：

- a) 按一下會議趨勢圖形上的特定位置，以在圖形下方的會議清單中，列出在所選時間的 5 分鐘內發生的會議。如需相關資訊，請參閱[檢視會議清單, 第 109 頁](#)。
- b) 選取開始和結束欄位下方的圖形符號，以顯示「開始」和「結束」期間內所發生會議的日期與時間清單。然後從下拉清單中選取日期。

附註 下拉功能表中顯示的資料點，和圖形中顯示的那些資料點相同。之所以使它們可存取，主要是為了方便具有鍵盤和螢幕閱讀器的使用者。

附註 將滑鼠置於圖形上，以查看那個時候發生的會議總數。

檢視會議清單

程序

步驟 1 登入「管理」網站。

步驟 2 選取儀表板。

步驟 3 在會議趨勢圖形上方，透過選取開始和結束日期與時間來設定趨勢期間。如需相關資訊，請參閱[檢視會議趨勢, 第 108 頁](#)。

- 附註
- 依預設，會議清單會顯示目前 24 小時期間的會議。
 - 未按排定時間開始的排定會議不會併到會議趨勢圖形或會議清單中。

會議清單會顯示會議總數，並列出所選趨勢期間排定、進行中或結束的所有會議。依下列狀態的順序來顯示會議：進行中、已結束、未開始。會議清單中顯示的資訊包含：

- 在趨勢圖表中選取的時間範圍
- 會議主題
- 主持人
- 參加者人數
- 會議的狀態：進行中、已結束、未開始

附註 狀態為進行中或已結束的會議會在第一欄中顯示綠色、黃色或紅色 LED，以指出會議的狀態為良好、一般或不良。一般（黃色）指出會議期間發生的音訊/視訊延遲或抖動已達到次要閾值，並且應該加以監視和調查以判定原因。不良（紅色）指出會議期間發生的音訊/視訊延遲或抖動已達到主要閾值，並且管理員應該聯絡 Cisco 技術協助小組 (TAC) 以取得協助。

步驟 4 選擇性地選取欄標題來排序會議。

步驟 5 使用分頁功能來檢視下一頁或上一頁。

附註 •每個頁面上最多會顯示 10 個會議。

•在任何趨勢期間，可顯示的會議總數上限為 125。如果給定期間內存在許多會議，請將趨勢期間分成較小的時段。

•可能會在會議清單中看到重複的會議項目。每次開始會議時都會建立一個會議項目。因此，如果會議已開始、停止及重新啟動，則清單中會顯示多個同名的會議項目。

排定維護時段

執行系統維護前，應該排定維護時段。維護時段生效時的唯一限制是使用者無法排定維護時段內或者與維護時段重疊的會議。例如，管理員想要關閉系統大約一小時以進行維護（例如上午 5:00 到上午 6:00，此時段內似乎沒有排定任何會議）。如果已排定會議，則管理員必須聯絡每個會議主持人，告訴他們在他們的會議時間內排定了維護時段。設定維護時段後，使用者便無法在此時間內排定會議。但是，使用者可以使用**現在開會**功能來開始即時會議。

開啓維護模式後，會結束目前正在進行的所有會議，並且「現在開會」功能會因此無法再使用。假設您判定應該需要大約兩小時來進行必要的系統變更。您需要執行的其中一個作業是上傳新的憑證授權單位 (CA) 憑證，這可能會要求您在關閉維護模式後執行系統重新開機作業。您計劃在上午 4:00 左右開始系統維護。若要排定維護時段，請指定開始時間 2014 年 4 月 15 日上午 3:30，持續時間為 3 小時 30 分鐘。這表示維護時段將從上午 3:30（這容許結束所有會議，並且在管理員打算開始系統維護之前的 30 分鐘內並未排定會議）生效，直到上午 7:00。此時段容許在開啓維護模式後可能進行的重新開機作業之後，系統可完全運作之前所需的額外時間，以及在使用者可以排定並主持會議之前，管理員啟動一個以上即時會議來測試所修改設定的時間。

雖然部分系統維護作業並不要求您開啓維護模式，但請注意，不要求系統處於維護模式的作業，在您關閉維護模式後，將需要額外的時間來完成重新啟動或重新開機。系統重新啟動只需要幾分鐘（大約 3 到 5 分鐘），但重新開機大約需要 30 分鐘。記住在排定維護時段時要考量讓系統可完全運作所需的這段額外時間。如需相關詳細資訊，請參閱[開啓或關閉維護模式](#)，第 114 頁。

程序

步驟 1 登入「管理」網站。

步驟 2 選取排定維護。

此時會顯示**排定維護時段**。

步驟 3 使用行事曆工具和時間下拉功能表來選取維護時段的日期和開始時間。

步驟 4 透過指定小時數和分鐘數來輸入維護時段的持續時間。

步驟 5 選取**排定**。

「維護」窗格中會顯示排定的維護時段日期、開始時間和持續時間。

附註 維護時段開始時，如果使用者嘗試排定的會議落在排定維護時段的範圍內，則使用者會收到一則錯誤訊息。

下一步動作

- 如需開啓維護模式的相關資訊，請參閱[開啓或關閉維護模式](#)。
- 如需通知使用者系統維護的詳細資料，請參閱[傳送電子郵件給使用者](#)。

變更排定的維護時段

排定維護時段後，可以重新排定日期與時間或者將其刪除。

程序

步驟 1 登入「管理」網站。

步驟 2 選取**儀表板**。

步驟 3 選取顯示的系統維護日期與時間。

步驟 4 在**排定維護時段**上，您可以執行下列作業：

- 輸入不同的開始日期與時間。
- 修改持續時間（小時和分鐘）。
- 選取**刪除**以移除維護時段。

附註 如果提前完成系統維護，則可以縮短持續時間，也可以選取**排定維護時段**上的**刪除**。

下一步動作

記住先開啓維護模式，再修改系統內容。如需哪些系統內容要求開啓維護模式的相關資訊，請參閱[關於維護模式](#)，第 112 頁。

關於維護模式

許多設定變更都需要將系統進入維護模式。由於維護模式會關閉會議活動，因此您需要排定維護時段，以確保將使用者的停機時間減至最少。雖然我們建議在開啟維護模式之前排定維護時段，但這不是必要的。隨時都可以開啟維護模式。開啟維護模式按鈕位於儀表板頁面上。

在決定要執行系統維護的時間後，使用排定維護功能（位於儀表板頁面）來排定維護時段。如需詳細資料，請參閱[排定維護時段](#), 第 110 頁。然後應該選取傳送電子郵件給使用者功能，提前通知您的使用者，他們將無法在維護時段加入或主持會議。如需相關資訊，請參閱[傳送電子郵件給使用者](#), 第 135 頁。

開啟維護模式後，應該會出現下列情況：

- 結束目前正在進行的會議。
- 使用者無法排定或主持新會議。
- 使用者無法從網頁、Microsoft Outlook 外掛程式或行動裝置應用程式登入 WebEx 網站。
- 系統會繼續將自動通知電子郵件傳送給使用者和管理者。

使用下表來判斷需要您開啟維護模式的作業，及關閉維護模式後系統所執行的動作。如果嘗試執行這些作業，但未先開啟維護模式，則系統會提供提醒訊息。

作業	參考	需要維護模式	在關閉維護模式後，系統會重新開機或重新啟動
新增和移除高可用性系統	配置高可用性系統 , 第 138 頁	是	重新開機
透過部署或移除網際網路反向 Proxy 新增和移除公開存取權	新增對系統的公開存取 , 第 142 頁和 移除公開存取 , 第 143 頁	是	重新啟動
變更系統預設語言	設定您的公司資訊 , 第 168 頁	是	重新啟動
變更您的主持人或管理員帳戶 URL	變更網站設定 , 第 145 頁	是	重新啟動
變更您的郵件伺服器	設定郵件伺服器 , 第 146 頁	否	不適用
變更虛擬 IP 位址	變更虛擬 IP 位址 , 第 141 頁	是	重新開機
設定及變更品牌設定	配置您的品牌設定 , 第 169 頁	否	不適用

作業	參考	需要維護模式	在關閉維護模式後，系統會重新開機或重新啟動
配置及變更許多音訊設定	關於設定音訊設定, 第 172 頁	是	重新啟動
設定並變更撥入存取號碼、顯示名稱、呼叫者 ID 音訊設定。	配置您的音訊設定, 第 175 頁	否	不適用
設定及變更服務品質設定	設定服務品質 (QoS), 第 178 頁	否	不適用
設定及變更 SNMP 設定	設定 SNMP 設定, 第 151 頁	是	重新啟動
設定憑證	管理憑證, 第 207 頁	是	重新啟動或重新開機（由系統決定）
設定及變更災害復原設定	使用災害復原功能, 第 149 頁	是	重新啟動
設定符合 FIPS 標準的加密	啟用與 FIPS 相容的加密, 第 222 頁	是	重新啟動
設定儲存伺服器	設定儲存伺服器, 第 148 頁	是	重新啟動
設定虛擬機器安全性	設定虛擬機器安全性, 第 221 頁	是	重新開機
擴充系統大小	擴充系統大小, 第 144 頁	是	重新啟動
執行次要更新、主要升級及擴充系統	更新系統, 第 87 頁	是	重新啟動
更新共用金鑰	管理憑證, 第 207 頁	是	重新啟動
使用系統資源測試	使用系統資源測試, 第 234 頁	是	重新啟動

每個虛擬機器都有一個主控台視窗，指示它是否處於維護模式。您可以在 vCenter 庫存欄中開啟主控台視窗（用於導覽）。主控台視窗提供系統的 URL、系統類型（主要、高可用性或公開存取權）、部署類型（50、250、800 或 2000 個使用者系統），及現行系統狀態（包括開啟還是關閉維護模式）。

與系統狀態變更的時間)。顯示的時間在您的「公司資訊」設定中配置。如需相關資訊，請參閱[設定您的公司資訊](#)，第 168 頁。

完成系統維護作業

完成修改系統配置後，可以關閉維護模式。視執行的作業而定，系統會執行下列動作：

- 快速進入作業狀態，因為更新不需要維護模式。
- 顯示一則訊息以指出所做的變更要求系統重新啟動，而此程序只需幾分鐘。
- 顯示一則訊息以指出所做的變更要求系統重新開機，此程序大約要花費 30 分鐘，取決於系統的大小。

系統重新啟動需要幾分鐘，但系統重新開機可能需要長達 30 分鐘的時間。在此期間，無法進行會議活動。當您關閉維護模式時，系統會判定所需的動作，並顯示適當的訊息。

關閉維護模式後，會重新整理儀表板頁面。如果系統內容頁面上列出的所有虛擬機器都顯示「良好」狀態（綠色），則系統已備妥，使用者可以順利地開始會議。如需相關資訊，請參閱[開啟或關閉維護模式](#)，第 114 頁。

如果維護模式已關閉，但排定的維護時段仍生效，則使用者將能夠主持並出席先前排定的會議，但是將無法排定新會議，除非維護時段已結束。

針對系統升級開啟和關閉維護模式

在針對升級系統部署虛擬機器後，如果手動升級系統以將 Cisco WebEx Meetings Server 1.x 版更新為 2.0 版，則在應該開啟維護模式時，會顯示一則訊息。必須手動開啟維護模式。

如果選擇自動升級程序，則會在適當的時間自動開啟維護模式，並且會顯示一則訊息，讓您瞭解此情況的發生時間。

完成手動或自動升級程序時，可以在升級的 Cisco WebEx Meetings Server 2.0 版系統上手動關閉維護模式。可能需要幾分鐘的時間，會議服務才能變為可用。

相關主題

[排定維護時段](#)，第 110 頁

[開啟或關閉維護模式](#)，第 114 頁

開啟或關閉維護模式

在修改系統配置之前，應該排定維護時段，並通知使用者排定的系統維護時間。如需詳細資料，請參閱[排定維護時段](#)，第 110 頁。



附註

開啟維護模式後，使用者無法排定、主持或出席會議。將結束目前正在進行的會議。

開始之前

如果開啟維護模式，則會關閉會議活動並阻止使用者登入 WebEx 網站、排定或加入會議以及播放會議錄製檔。關閉維護模式時，系統會判斷是需要重新啟動（大約需要 3 到 5 分鐘）還是重新開機

（大約需要 30 分鐘）並顯示適當的訊息。如需哪些系統作業要求開啟維護模式的相關資訊，請參閱[關於維護模式](#)。

程序

-
- 步驟 1** 登入「管理」網站。
 - 步驟 2** 選取開啟維護模式。
此時會顯示開啟維護模式對話方塊。確保瞭解開啟維護模式時系統的狀況。
 - 步驟 3** 準備好啟動系統維護時，選取繼續。
此時會顯示一則訊息，指出系統處於維護模式。此時會顯示關閉維護模式按鈕。
 - 步驟 4** （選用）備份虛擬機器。
 - 步驟 5** 完成系統配置後，請選取關閉維護模式。
視所修改的系統內容而定，可能需要幾分鐘或者大約 30 分鐘，使用者才能登入並繼續會議活動。
 - 步驟 6** （選用）若要判斷系統是否可完全運作，請選取儀表板 > 系統 > 檢視更多（在「系統」區段中）。如果所列出所有虛擬機器的狀態都是良好（綠色），則會議活動可以繼續進行。
-

下一步動作

如果在關閉維護模式且系統完成重新啟動或重新開機後排定的維護時段仍在生效中，則使用者可透過選取現在開會（位於會議頁面上）來開始即時會議。請參閱《使用者指南》（位於http://www.cisco.com/en/US/products/ps12732/tsd_products_support_maintain_and_operate.html）中的「開始即時會議」。



第 12 章

管理使用者

本章說明如何管理系統上的使用者。

- [關於管理使用者, 第 117 頁](#)
- [關於逗號和 Tab 分隔的檔案, 第 118 頁](#)
- [新增使用者, 第 124 頁](#)
- [編輯使用者, 第 124 頁](#)
- [啟動使用者, 第 125 頁](#)
- [停用使用者, 第 125 頁](#)
- [使用匯入停用使用者, 第 126 頁](#)
- [匯入使用者, 第 126 頁](#)
- [匯出使用者, 第 127 頁](#)
- [使用匯出檔案將使用者匯入至新系統, 第 127 頁](#)
- [設定追蹤碼, 第 128 頁](#)
- [設定目錄整合, 第 129 頁](#)
- [同步化使用者群組, 第 133 頁](#)
- [使用 CUCM 配置 AXL Web 服務及目錄同步, 第 134 頁](#)
- [使用 CUCM 來配置 LDAP 整合與驗證, 第 135 頁](#)
- [傳送電子郵件給使用者, 第 135 頁](#)

關於管理使用者

您可以逐個新增使用者，或者匯入逗號或 Tab 分隔的檔案中儲存的使用者清單。

您可以新增和停用使用者帳戶，但無法將其刪除。停用可讓您使使用者處於非使用中狀態，但您可以稍後根據需要重新啟動使用者。重新啟動的使用者帳戶可重新取得其在被停用之前所具有的會議、錄製檔及其他資料的存取權。

系統在生命週期中最大可支援 400,000 個使用者帳戶。此數目代表處於使用中和非使用中狀態的使用者帳戶總數。此生命週期最大數目足以符合使用者資料庫的預期成長需求。

若要阻止未經授權登入系統，請務必停用離開組織的任何使用者。您可以透過以下方式停用使用者：

- 如果您的系統未使用整合的 SSO，則您可以逐個停用使用者，或者透過匯入逗號或 Tab 分隔的檔案（對於要停用的每位使用者，「ACTIVE」欄位均設定為「N」）來停用。如需相關資訊，請參閱[停用使用者](#)，第 125 頁和[關於逗號和 Tab 分隔的檔案](#)，第 118 頁。
- 如果您的系統使用整合的 SSO，則必須透過將使用者從 SAML 2.0 iDP 中的企業目錄中移除來將其停用。此程序並非由此產品執行。
- 使用密碼設定功能可在經過指定的時間後停用使用者。如需相關資訊，請參閱[配置您的一般密碼設定](#)，第 180 頁。

關於逗號和 Tab 分隔的檔案

若要使用試算表應用程式（例如，Microsoft Excel）來整理您的使用者資料，請以逗號或 Tab 分隔 (CSV) 檔儲存或匯出您的試算表。系統支援 UCS 轉換格式 — 8 位元 (UTF-8)。您只能在檔案中輸入 UTF-8 中指定的字元。如果您的檔案包含非 ASCII 字元，請驗證該檔案使用的是 Unicode 的逗號或 Tab 分隔符號。

若要順利匯入逗號或 Tab 分隔檔，必需提供表格中列出的所有欄位。欄位值可以為空。如果遺漏欄位，則會出現錯誤訊息。例如，「檔案格式不正確。需要 Custom10」。

最多可以定義十個追蹤碼群組。追蹤碼群組名稱應該是唯一的，並且您不應該使用預先定義的欄位名稱（USERID、ACTIVE、FIRSTNAME、LASTNAME、EMAIL、LANGUAGE、HOSTPRIVILEGE、TIMEZONE）。

欄位名稱	描述	值的大小和類型
USERID	使用者 ID。 附註 此欄位由系統自動產生，且必須在匯入 CSV 檔時留空。	1 至 19 個英數字元
ACTIVE	此使用者是否處於使用中狀態。	Y 或 N
FIRSTNAME	使用者名字。	1 至 32 個字元字串
LASTNAME	使用者姓氏。	1 至 32 個字元字串
EMAIL	使用者的電子郵件地址。	1 至 192 個英數字元字串

欄位名稱	描述	值的大小和類型
LANGUAGE	使用者的語言。如需相關資訊，請參閱 CSV 檔案欄位值 。	1 至 64 個字元字串
HOSTPRIVILEGE	主持人特權。	ADMN 或 HOST
TIMEZONE	使用者所在的時區。如需相關資訊，請參閱 CSV 檔案欄位值 。	時區名稱
DIVISION	使用者的分部。適用於追蹤碼群組 1。此欄位可在「追蹤碼」頁上設定。如需相關資訊，請參閱 設定追蹤碼 。	1 至 128 個字元字串
DEPARTMENT	使用者的部門。適用於追蹤碼群組 2。此欄位可在「追蹤碼」頁上設定。如需相關資訊，請參閱 設定追蹤碼 。	1 至 128 個字元字串
PROJECT	使用者的專案。適用於追蹤碼群組 3。此欄位可在「追蹤碼」頁上設定。如需相關資訊，請參閱 設定追蹤碼 。	1 至 128 個字元字串
OTHER	其他資訊。適用於追蹤碼群組 4。此欄位可在「追蹤碼」頁上設定。如需相關資訊，請參閱 設定追蹤碼 。	1 至 128 個字元字串
CUSTOM5	自訂欄位 5。	1 至 128 個字元字串
CUSTOM6	自訂欄位 6。	1 至 128 個字元字串
CUSTOM7	自訂欄位 7。	1 至 128 個字元字串
CUSTOM8	自訂欄位 8。	1 至 128 個字元字串
CUSTOM9	自訂欄位 9。	1 至 128 個字元字串
CUSTOM10	自訂欄位 10。	1 至 128 個字元字串

CSV 檔案欄位值

語言欄位值

下面是您可以在 CSV 檔中使用的國碼值的範例。

欄位值	語言
en-us	美國英文

欄位值	語言
zh-cn	簡體中文
zh-tw	繁體中文
jp	日文
ko	韓文
fr	法文
de	德文
it	義大利文
es-me	卡斯提爾西班牙文
es	拉丁美洲西班牙文
nl	荷蘭文
pt-br	葡萄牙文
ru	俄文

時區欄位值

以下是您可以在 CSV 檔中設定的時區 (TIMEZONE) 欄位值。

欄位值	GMT
馬紹爾群島	-12 小時
薩摩亞	-11 小時
檀香山	-10 小時
安克雷奇	-9 小時
舊金山	-8 小時
提娃那	-8 小時
亞歷桑那	-7 小時
丹佛	-7 小時

欄位值	GMT
奇瓦瓦	-7 小時
芝加哥	-6 小時
墨西哥市	-6 小時
薩克其萬	-6 小時
特古西加爾巴	-6 小時
波哥大	-5 小時
巴拿馬	-5 小時
紐約	-5 小時
印地安納州	-5 小時
加拉卡斯	-4.5 小時
聖地牙哥	-4 小時
哈利法克斯	-4 小時
紐芬蘭	-3.5 小時
波西里亞	-3 小時
布魯諾斯愛麗斯	-3 小時
累西腓	-3 小時
努克	-3 小時
大西洋中部	-2 小時
亞速爾	-1 小時
雷克雅維克	0 小時
倫敦	0 小時
卡薩布蘭卡	0 小時
西非	1 小時

欄位值	GMT
阿姆斯特丹	1 小時
柏林	1 小時
馬德里	1 小時
巴黎	1 小時
羅馬	1 小時
斯德哥爾摩	1 小時
雅典	2 小時
開羅	2 小時
比勒陀利亞	2 小時
赫爾辛基	2 小時
特拉維夫	2 小時
安曼	2 小時
伊斯坦堡	2 小時
利雅德	3 小時
奈洛比	3 小時
德黑蘭	3.5 小時
莫斯科	4 小時
阿布達比	4 小時
巴古	4 小時
喀布爾	4.5 小時
伊斯蘭馬巴德	5 小時
孟拜	5.5 小時
可倫坡	5.5 小時

欄位值	GMT
伊卡特林堡	6 小時
阿馬提	6 小時
加德滿都	6.75 小時
曼谷	7 小時
北京	8 小時
伯斯	8 小時
新加坡	8 小時
台北	8 小時
吉隆坡	8 小時
東京	9 小時
首爾	9 小時
愛德蘭	9.5 小時
達爾文	9.5 小時
亞庫茲克	10 小時
布里斯本	10 小時
雪梨	10 小時
關島	10 小時
霍巴特	10 小時
海參威	11 小時
索羅門群島	11 小時
惠靈頓	12 小時
斐濟	12 小時

新增使用者

程序

- 步驟 1 登入「管理」網站。
 - 步驟 2 選取使用者 > 新增使用者。
 - 步驟 3 選取您的帳戶類型（主持人或管理員）。
 - 步驟 4 將使用者的資訊填入欄位。標有星號的欄位必填。
 - 步驟 5 選取儲存。
Cisco WebEx Meetings Server 會向使用者傳送一封包含建立密碼鏈結的電子郵件。使用者必須建立密碼，才能登入 WebEx 網站。
- 附註 「建立密碼」鏈結會在 72 小時後過期。

編輯使用者

您可以變更使用者資訊，以及使用編輯使用者功能啟動或停用使用者帳戶。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取使用者。
即會出現使用者清單。每個頁面上顯示的使用者預設數量為 50 個。您也可以選取每頁顯示的使用者數量下拉功能表，並將設定變更為 50 或 100。
- 步驟 3 選取要編輯的使用者。
- 步驟 4 變更可編輯的欄位。標有星號的欄位必填。
- 步驟 5 （選用）選取強制此使用者在下次登入時變更密碼勾選方塊。
附註 如果系統上已啟用 SSO，則此功能不適用於主持人帳戶。
- 步驟 6 也可以啟動或停用使用者帳戶：
 - 選取啟動，可重新啟動非使用中的帳戶。
 - 選取停用，可停用帳戶。

附註 啟動或停用帳戶不會儲存您對帳戶所做的任何其他變更。您必須選取儲存才能儲存變更。
- 步驟 7 選取儲存。這會儲存變更，而不會改變帳戶的狀態。

啟動使用者

新增或匯入主持人和管理員帳戶後，預設即會啟動它們。使用此功能重新啟動非使用中的使用者。或者您還可以在[編輯使用者](#)頁面啟動帳戶。如需相關資訊，請參閱[編輯使用者](#), 第 124 頁。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取使用者。
- 步驟 3 選取您要啟動的任何非使用中使用者的勾選方塊。
- 步驟 4 選取動作 > 啟動。
選取的帳戶已啟動，且每個帳戶的狀態現在應該是「活動」。

停用使用者

您可以停用主持人和管理員帳戶。停用帳戶可防止帳戶的所有者執行以下操作：

- 從網頁、Outlook 外掛程式及行動裝置應用程式登入
- 主持或出席會議
- 管理系統（若使用者是管理員）

您也可以在[編輯使用者](#)頁面上停用帳戶。如需相關資訊，請參閱[編輯使用者](#), 第 124 頁。



附註

管理員無法停用自己的帳戶。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取使用者。
- 步驟 3 選取要停用的任何使用中的使用者的勾選方塊。
- 步驟 4 選取動作 > 停用，然後選取確定進行確認。
選取的帳戶已停用，每個帳戶的狀態現在應該是「非使用中」。

使用匯入停用使用者

您可以使用匯入功能停用使用者帳戶。

程序

-
- 步驟 1** 登入「管理」網站。
 - 步驟 2** 選取使用者 > 匯入/匯出使用者 > 匯出。
等待顯示下載匯出的 **csv** 檔案鏈結。
 - 步驟 3** 選取下載匯出的 **csv** 檔案，並將 CSV 檔儲存到您的硬碟中。
 - 步驟 4** 開啓 CSV 檔。在 ACTIVE 欄中進行下列變更：
 - a) 針對要停用的每個使用者輸入 N。
 - b) 針對您不想變更的使用者，刪除所有記錄。
 - 步驟 5** 選取使用者 > 匯入/匯出使用者 > 匯入。
 - 步驟 6** 選取瀏覽，選取您更新的 CSV 檔，選取逗號，然後選取匯入。
更新的使用者記錄將被覆寫，而選取的使用者帳戶將被停用。
-

匯入使用者

開始之前

準備包含您的使用者資訊的以逗號或 Tab 分隔的檔案。如需相關資訊，請參閱[關於逗號和 Tab 分隔的檔案](#), 第 118 頁。

程序

-
- 步驟 1** 登入「管理」網站。
 - 步驟 2** 選取使用者 > 匯入/匯出使用者。
即會出現「匯入/匯出使用者」頁。
 - 步驟 3** 選取匯入。
即會出現「匯入使用者」頁。
 - 步驟 4** 選取瀏覽，然後選取要匯入的以逗號分隔或以 Tab 分隔的檔案。
 - 步驟 5** 選取 **Tab** 或逗號圓鈕，指示要匯入的類型。
 - 步驟 6** 選取匯入。
即會匯入您的檔案。在匯入完成後，系統會傳送一封電子郵件，指出成功匯入的記錄數目及失敗的記錄數目。
-

下一步動作

選取**使用者**，以查看您系統上的使用者。確定您的使用者已正確匯入。

匯出使用者

程序

-
- 步驟 1** 登入「管理」網站。
 - 步驟 2** 選取**使用者 > 匯入/匯出使用者**。
 - 步驟 3** 選取**匯出**。
您的使用者資料將匯出為 CSV 檔案。系統會向管理員傳送電子郵件，其中含有可下載匯出檔案的鏈結。
-

使用匯出檔案將使用者匯入至新系統

執行以下步驟，可使用匯出檔案將使用者匯入至新系統。

程序

-
- 步驟 1** 登入您要從中匯出使用者的系統上的管理網站。
 - 步驟 2** 選取**使用者 > 匯入/匯出使用者**。
 - 步驟 3** 選取**匯出**。
您的使用者資料將匯出為以逗號或 Tab 分隔的檔案。
 - 步驟 4** 開啓匯出的檔案，刪除檔案中的所有 USERID，然後重新儲存檔案。
 - 步驟 5** 登入您要匯入使用者至其中的系統上的管理網站。
 - 步驟 6** 選取**使用者 > 匯入/匯出使用者**。
即會出現「匯入/匯出使用者」頁。
 - 步驟 7** 選取**匯入**。
即會出現「匯入使用者」頁。
 - 步驟 8** 選取**瀏覽**，然後選取您上面匯出的檔案。
 - 步驟 9** 選取 **Tab** 或 **逗號** 圓鈕，指示要匯入的類型。
 - 步驟 10** 選取**匯入**。
即會匯入您的檔案。在匯入完成後，系統會傳送一封電子郵件，指出成功匯入的記錄數目及失敗的記錄數目。
-

下一步動作

選取**使用者**，以查看您系統上的使用者。確定您的使用者已正確匯入。

設定追蹤碼

您可以設定追蹤碼，來追蹤指定群組中主持人的使用情形。例如，您可以設定專案或部門的追蹤碼。當您新增或編輯使用者時，您設定的追蹤碼會顯示為選項。

您可以為每個追蹤碼設定下列內容：

- **追蹤碼群組** – 設定您的追蹤碼群組。在新增和編輯使用者時，使用追蹤碼群組。預設值為「分部」、「部門」、「專案」、「其他」及「自訂 5」至「自訂 10」。



附註 追蹤碼群組名稱應該是唯一的，並且您不應該使用預先定義的欄位名稱（USERID、ACTIVE、FIRSTNAME、LASTNAME、EMAIL、LANGUAGE、HOSTPRIVILEGE、TIMEZONE）。

- **輸入模式** – 選取**文字欄位**或**下拉功能表**。
- **使用情況** – 選取**未被使用**、**可選**或**必要**。

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取**使用者 > 追蹤碼**。
- 步驟 3** 也可以輸入您要在**追蹤碼群組**欄中設定的各追蹤群組名稱。如果您打算使用預設值，則無需變更任何欄位。
- 步驟 4** 在**輸入模式**欄中，為各追蹤碼選取**文字輸入**或**下拉功能表**。
如果您選取**文字輸入**，則可在文字欄位中輸入追蹤碼名稱。如果您選取**下拉功能表**，則輸入模式欄位旁會出現**編輯清單**鏈結。選取**編輯清單**鏈結在下拉功能表中為該追蹤碼設定值。如需相關資訊，請參閱[編輯追蹤碼](#)，第 129 頁。
附註 如果您為其中一個追蹤碼群組選取**下拉功能表**，則必須選擇**編輯清單**，並為關聯的下拉功能表輸入一或多個選項。
- 步驟 5** 在**使用情況**欄中，為各追蹤碼選取**未被使用**、**可選**或**必要**。
附註 在您設定下拉功能表清單後，應僅將「使用情況」變更為**必要**或**可選**。如果您試圖設定**未被使用**之外的使用設定，而沒有先設定追蹤碼群組和輸入模式，則會出現一則錯誤訊息。
- 步驟 6** 選取**儲存**。
您的追蹤碼設定已儲存。

編輯追蹤碼

依預設，追蹤碼顯示為文字方塊。如果您要顯示下拉功能表中的追蹤碼選項，必須設定選項清單。選取下拉功能表(從輸入模式下拉功能表) 後，即會出現編輯清單鏈結。

開始之前

若要編輯追蹤碼，您必須選取使用者 > 追蹤碼，然後選取下拉功能表(針對您的輸入模式)。

程序

-
- 步驟 1** 選取編輯清單鏈結。
即會出現編輯追蹤碼清單對話方塊。
- 步驟 2** 設定編輯追蹤碼清單對話方塊中的欄位。
- a) 選取僅顯示使用中的代碼，可在您開啓此對話方塊時僅顯示使用中的追蹤碼。取消選取此選項則可顯示所有追蹤碼。請注意，第一次為每個輸入模式設定追蹤碼時，無法選取此選項。
 - b) 選取移至第一個空的追蹤碼，可移至具有空代碼欄位的第一個頁面。
 - c) 依預設，已選取使用中。您可以取消勾選使用中，以使追蹤碼成為非使用中。非使用中追蹤碼不會出現在此追蹤碼群組的下拉功能表上。勾選使用中，可啟動非使用中的追蹤碼。
 - d) 在代碼文字方塊中輸入功能表項目名稱。限制：128 個字元。
 - e) 選取預設圓鈕，可使此功能表項目成為下拉功能表的預設選項。
 - f) 選取再新增 20 行，可再新增 20 行可設定的追蹤碼。如果要顯示 20 行以上，可新增導覽鏈結（下一頁、上一頁及頁碼）。限制：500 行（25 頁）。
 - g) 選取排序圓鈕，可設定追蹤碼的排序方式（不排序、遞增排序、遞減排序）。請注意，排序僅對目前頁面起作用。
- 步驟 3** 選取更新，可儲存您的設定。
您的設定會儲存，且編輯追蹤碼清單頁面會關閉。
-

設定目錄整合

目錄整合使您的系統能夠使用 Cisco Unified Communications Manager (CUCM) 使用者資料庫移入及同步化您的 Cisco WebEx Meetings Server 使用者資料庫，然後與 LDAP 目錄整合。

目錄整合使用下列某種方式簡化使用者設定檔的管理：

- 從 CUCM 將使用者設定檔匯入 Cisco WebEx Meetings Server。
- 使用 CUCM 資料庫中新的或修改的使用者屬性定期更新 Cisco WebEx Meetings Server 資料庫，包括每個使用者的名、姓及電子郵件地址。Cisco WebEx Meetings Server 透過使用者的電子郵件地址來區分使用者，因此如果使用者的名與姓相同，但電子郵件地址不同，則 Cisco WebEx Meetings Server 將其視為不同的使用者。

- 定期檢查 CUCM 資料庫的非作用中的使用者項目，並從 Cisco WebEx Meetings Server 資料庫停用其使用者設定檔。
- 支援系統使用 LDAP 認證來針對外部目錄驗證 Cisco WebEx Meetings Server 目錄整合使用者。
- 在 CUCM 及 LDAP 伺服器上啟用安全 LDAP (SLDAP) 時支援完全加密 LDAP 整合。
- CUCM 中配置的所有使用者將同步至 Cisco WebEx Meetings Server，並啟用他們的帳戶。您可以選擇在完成同步後停用帳戶。CUCM 中所有作用中的使用者都將同步至 Cisco WebEx Meetings Server。非作用中的使用者將不會匯入 Cisco WebEx Meetings Server。

開始之前

繼續目錄整合之前，請確定滿足下列必要條件：

- 我們建議您在離峰時段或在週末安排同步化，以最小化對使用者的影響。
- 請確定您有受支援的 Cisco Unified Communications Manager (CUCM) 版本。如需相關資訊，請參閱《[Cisco WebEx Meetings Server 系統需求](#)》。
- 取得 CUCM 管理使用者認證（需要為目錄整合新增 CUCM 伺服器）。
- 您必須先在 CUCM 上設定 AXL 與 LDAP 目錄服務，然後才能使用目錄整合功能。需要 CUCM 才能將使用者匯入您的 Cisco WebEx Meetings Server 系統。使用 CUCM 執行下列動作：

啟用 Cisco AXL Web 服務

啟用 Cisco 目錄同步化

配置 LDAP 整合

配置 LDAP 驗證

請參閱[使用 CUCM 配置 AXL Web 服務及目錄同步](#)及[使用 CUCM 來配置 LDAP 整合與驗證](#)。如需其他資訊，請參閱 [CUCM 說明文件](#)。

- 請確定 CUCM 中有需要主持人特權的所有使用者。不在 CUCM 中的使用者將無法登入及主持會議（所有使用者都可以作為訪客加入）。若有必要，建立僅包含您要從 CUCM 匯入之使用者的 CUCM 群組或過濾器。



附註

如果不使用 CUCM 群組，則在首次目錄同步期間，會將所有作用中的 CUCM 使用者都匯入 Cisco WebEx Meetings Server。非作用中的 CUCM 使用者不會匯入。後續同步化期間將只匯入作用中的新使用者與修改的使用者。您必須在 Cisco WebEx Meetings Server 中停用不想授予其主持人存取權的使用者帳戶。請注意，僅當使用者實際主持會議時才會在 Cisco WebEx Meetings Server 中耗用一個主持人授權。不主持會議的帳戶不耗用授權。如需授權使用的相關資訊，請參閱《[設定系統](#)》中的「管理授權」。

- 沒有電子郵件地址的使用者將不匯入。
- 如果使用者具有多個帳戶，這些帳戶使用相同名字和姓氏，但在 CUCM 上獲指派不同的電子郵件地址，則將這些使用者匯入 Cisco WebEx Meetings Server 時，會將這些位址作為不同的使用者進行處理。CUCM 使用者具有唯一的使用者名稱，因此管理員可以使用同一個電子郵件地址

來建立多個使用者帳戶。但是，Cisco WebEx Meeting Server 上的帳戶具有唯一的電子郵件地址。因此，如果多個 CUCM 使用者帳戶具有同一個電子郵件地址，則 CUCM 管理員應該手動編輯這些使用者帳戶，以使電子郵件地址成為唯一，然後再將這些帳戶匯入 Cisco WebEx Meetings Server。

- 如果啟用 LDAP 驗證，則當您選取**現在同步**，或者勾選**下一次同步**選項並輸入日期與時間時，Cisco WebEx Meetings Server 會使用連接埠 8443 來連線至 CUCM。

程序

步驟 1 登入您的 Cisco WebEx Meetings Server 管理網站。

步驟 2 （選用）選取**開啟維護模式**及**繼續**，以進行確認。

附註 執行目錄整合不需要維護模式，但大型同步可能影響系統效能。您可以將系統置於維護模式，以避免使用者在同步化期間使用系統。

步驟 3 選取**使用者 > > 目錄整合**。

步驟 4 若尚未輸入您的 CUCM 伺服器資訊，請先輸入：

- IP 位址或標準域名 (FQDN)
- 使用者名稱
- 密碼

使用者名稱及密碼可以是您的 CUCM 管理員或 AXL 使用者名稱及密碼。配置 CUCM 資訊之後，CUCM 伺服器的 IP 位址或 FQDN 出現在 CUCM 圖示下。

附註 如果您已配置了 CUCM 設定，則此步驟非必要，您可以繼續至下一步。配置 CUCM 資訊之後，對其進行變更是一個複雜的過程，可能會導致使用者同步化問題，因此不建議這麼做。

步驟 5 選取**要過濾的 CUCM 使用者群組**，只將所選「CUCM 使用者群組」中的那些使用者新增至 Cisco WebEx Meeting Server。

步驟 6 將您的 Cisco WebEx Meetings Server 系統與 LDAP 目錄服務同步化。您可以透過以下方式執行同步化：

- 選取**立即同步**，立即執行同步。

附註 在同步開始之後無法取消。

- 選取**下一次同步**勾選方塊，並輸入日期、時間及重複機制來排定將來的同步。

如果選取**立即同步**，則系統會立即執行同步。此過程所需的時間視同步的使用者人數而定。當同步完成後，您將收到電子郵件。**立即同步**後不會通知系統上的其他管理員。如果安排同步，則在指定日期與時間發生。安排的同步化完成後，所有管理員都會收到電子郵件。如果要阻止將來同步，則可以取消選取**下一次同步**。

在同步過程中會對映下列屬性：

CUCM 屬性	Cisco WebEx Meetings Server 屬性
名字	名字

CUCM 屬性	Cisco WebEx Meetings Server 屬性
姓氏	姓氏
郵件 ID	電子郵件地址

附註 Cisco WebEx Meetings Server 中的名與姓是顯示給使用者的全名的一部分。

一般使用者無法更新 Cisco WebEx Meetings Server 中的對映屬性。

如果同步失敗，則會在頁面上顯示錯誤訊息，並向管理員傳送包含錯誤相關資訊的電子郵件。選取**檢視日誌**以查看錯誤的詳細說明。提供的日誌包含停用的使用者報告、失敗的使用者報告及摘要。

執行至少一次同步之後，會顯示前次同步的摘要，指出該同步是否已完成、完成的日期與時間（使用您「公司資訊」設定中配置的日期與時間）、使用者變更項目清單，包括下列內容：

- 新增 — 新增的新使用者人數。
- 停用 — 停用的使用者人數。

步驟 7 如果您已配置或變更您的同步日程表或管理員通知設定，請選取**儲存**。

步驟 8 選取**使用者標籤**，並確定已同步化正確的使用者。

- a) 在下拉功能表上選取**遠端使用者**，以過濾使用者清單。請確保清單中列出您要同步的使用者。遠端使用者透過目錄同步匯入 Cisco WebEx Meetings Server。如果先本端建立使用者，然後透過目錄同步改寫，則該使用者將變成遠端使用者，而不是本端使用者。
- b) 選取**本端使用者**以查看未包含在同步中的使用者。本端使用者由 Cisco WebEx Meetings Server 管理員在本端建立。可以手動新增或使用 CSV 檔匯入本端使用者。

步驟 9 請確定您的 CUCM 與 Cisco WebEx Meetings Server 同步日程表為順序。必須先進行 CUCM 同步，然後再立即進行 Cisco WebEx Meetings Server 同步。

步驟 10 （選用）選取或取消選取**同步完成時通知管理員**，然後選取**儲存**。依預設，此選項已選取，且僅在安排同步後通知管理員。

步驟 11 選取**啟用 LDAP 驗證**。

附註 如果系統配置為使用 SSO，則必須先停用 SSO。如需相關資訊，請參閱**停用 SSO**。如果系統未配置為使用 SSO，則使用其預設驗證直到啟用 LDAP 驗證為止。

啟用 LDAP 之後，我們建議管理員使用 Active Directory 伺服器來進行使用者管理，包括新增、停用及修改使用者。啟用 LDAP 驗證之後，所有參加者都必須使用其 LDAP 認證才能登入 WebEx 網站。但是，管理員仍然使用他們的 Cisco WebEx Meetings Server 認證登入管理網站。

步驟 12 請確定您的使用者可以使用其 AD 域認證登入系統。

步驟 13 如果已將系統置於維護模式，請選取**關閉維護模式**。

步驟 14 （選用）如果您已執行同步，則可以選取**立即通知**，以便在您的 Cisco WebEx Meetings Server 系統上建立帳戶或帳戶變更時透過電子郵件通知使用者。您也可以選取**自動傳送通知**，以便在每次同步後新增使用者時向您自動傳送電子郵件。驗證設定有任何變更（例如，啟用 LDAP）之後，會傳送「使用者 - 密碼變更」電子郵件給受影響的使用者。

當您選取**立即通知**時

- 所有使用者僅在其生命週期內接受一次通知。後續同步不會導致傳送其他電子郵件。
- 「需要通知的使用者」指出所有作用中但尚未被通知的使用者。
- 不會向非作用中的使用者或本端使用者傳送任何通知。
- 在 Cisco WebEx Meetings Server 上新增本端使用者會傳送電子郵件給該使用者。不過，必須先在 CUCM Active Directory 伺服器上新增該使用者，然後他才能登入 WebEx 網站。
- 您只能傳送通知給使用同步功能新增的使用者。
- 傳送電子郵件通知給使用者需要數分鐘時間。此延遲因 Cisco WebEx Meetings Server 系統外部的數個因素所致，包括電子郵件伺服器、網路連線問題，及個別電子郵件帳戶的垃圾郵件擷取程式。

您的系統會傳送下列電子郵件：

- 「AD 啟用電子郵件」，當在同步中首次將使用者匯入系統時，會向此類使用者傳送該郵件。使用者在後續同步時不會收到此電子郵件。
- 「使用者密碼 - 已變更」電子郵件會傳送給系統上本端建立的使用者。

如需自訂這些電子郵件範本的相關資訊，請參閱[關於電子郵件範本](#)。

附註 如果您是將「目錄整合」與 LDAP 驗證一起使用，則 CUCM 中配置的使用者會同步到 Cisco WebEx Meeting Server 作為主持人，並使用其 LDAP 認證來登入 WebEx 網站。但是，如果將所匯入使用者的帳戶類型從主持人變更為管理員，則使用者會收到一封包含「建立密碼」鏈結的電子郵件。使用者選取此鏈結，並為 Cisco WebEx Meetings Server 輸入新密碼。使用者將使用這個新建的密碼來登入管理網站，但將繼續使用 LDAP 認證來登入 WebEx 網站。

同步化使用者群組

管理員可以在 CUCM 中建立使用者群組。例如，管理員可建立由可以使用 Cisco WebEx Meetings Server 之使用者組成的使用者群組。管理員可以從 CWMS 選取特定的使用者群組，以過濾並匯入某些使用者。

開始之前

使用 CUCM 來建立使用者群組。如需相關資訊，請參閱《Cisco Unified Communications Manager 管理指南http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html》中的「使用者管理設定」一節。

程序

-
- 步驟 1** 登入您的 Cisco WebEx Meetings Server 管理網站。
- 步驟 2** 選取使用者 > > 目錄整合。
- 步驟 3** 選取用於過濾的 CUCM 群組鏈結。
- 步驟 4** 勾選要同步的使用者群組。
 附註 如果未選取任何群組，則目錄整合將會同步所有使用者群組。
- 步驟 5** 選取儲存。
- 步驟 6** 選取「立即同步」來執行同步。此過程所需的時間視同步的使用者人數而定。
 附註 系統會記住之前同步過哪些使用者群組。如果沒有選取之前已同步的使用者群組，則未選使用者群組中的使用者將在同步過程中被停用。當同步完成時，系統會顯示新增及停用的使用者數目。
- 步驟 7** 如需在同步過程中匯入或停用之使用者的摘要資訊，請選取檢視日誌。
-

使用 CUCM 配置 AXL Web 服務及目錄同步

使用 CUCM 配置 AXL Web 服務及目錄同步。

開始之前

請在使用「目錄整合」功能之前執行此程序。如需相關資訊，請參閱[設定目錄整合, 第 129 頁](#)。

程序

	命令或動作	目的
步驟 1	登入您的 CUCM 帳戶。	
步驟 2	從右上角的下拉功能表選取 Cisco Unified 可服務性 ，然後選取執行。	
步驟 3	選取工具 > 啟動服務。	
步驟 4	選取 Cisco AXL Web 服務 與 Cisco DirSync ，然後選取儲存。	

下一步動作

如果您尚未使用 CUCM 來配置 LDAP 整合與驗證，請先配置。如需相關資訊，請參閱[使用 CUCM 來配置 LDAP 整合與驗證, 第 135 頁](#)。

使用 CUCM 來配置 LDAP 整合與驗證

使用 CUCM 來配置 LDAP 整合與驗證。



附註

如果為「目錄整合」配置了 CUCM，則可以選擇使用 SSO、LDAP 或本端驗證。

開始之前

請在使用「目錄整合」功能之前執行此程序。如需相關資訊，請參閱[設定目錄整合](#)。

程序

	命令或動作	目的
步驟 1	登入您的 CUCM 帳戶。	
步驟 2	從右上角的下拉功能表選取 Cisco Unified CM 管理 ，然後選取執行。	
步驟 3	選取檔案 > LDAP > LDAP 系統 。	
步驟 4	選取啟用 LDAP 伺服器同步 ，選取 Microsoft Active Directory 作為 LDAP 伺服器類型，選取 SAM 帳戶名稱 作為使用者 ID 的 LDAP 屬性，然後選取儲存。	
步驟 5	選取 LDAP 伺服器的勾選方塊，然後選取新增。	
步驟 6	填寫「LDAP 目錄」頁面上的欄位並選取儲存。	
步驟 7	在「LDAP 驗證」頁面上，選取對最終使用者使用 LDAP 驗證 勾選方塊，填寫頁面上的欄位，然後選取儲存。	

下一步動作

如果尚未使用 CUCM 配置 Cisco AXL Web 服務及 Cisco 目錄同步，請先配置。如需相關資訊，請參閱[使用 CUCM 配置 AXL Web 服務及目錄同步](#)。

傳送電子郵件給使用者

使用此工具可將電子郵件傳送給您的使用者。

程序

步驟 1 登入「管理」網站。

步驟 2 選取使用者 > 傳送電子郵件給使用者。

步驟 3 在收件者欄位中，輸入目標使用者電子郵件地址或電子郵件別名。

步驟 4 （選用）在密件副本欄位中輸入電子郵件地址。

步驟 5 在主旨欄位中輸入主旨。

步驟 6 在訊息欄位中輸入訊息。

步驟 7 選取傳送。

此時會傳送您的電子郵件。

附註 可能需要數分鐘時間，使用者才能收到您的電子郵件。此延遲可能是因 Cisco WebEx Meetings Server 系統外部的數個因素所致，包括電子郵件伺服器、網路連線速度，及個別電子郵件帳戶的垃圾郵件擷取程式。



第 13 章

設定系統

此模組說明如何使用管理員頁面來設定您的系統。

- [設定系統內容, 第 137 頁](#)
- [設定一般設定, 第 145 頁](#)
- [設定伺服器, 第 146 頁](#)
- [設定 SNMP 設定, 第 151 頁](#)
- [管理授權, 第 158 頁](#)

設定系統內容

透過選取「系統」區段中的「系統」和「檢視更多」來設定系統內容。

變更您的虛擬機器設定

使用此功能變更您的虛擬機器設定。



附註

請勿使用 VMware vCenter 來編輯您的虛擬機器設定。

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取系統並在「系統」區段中選取檢視更多。
- 步驟 3** 選取開啟維護模式及繼續以進行確認。
- 步驟 4** 若要修改虛擬機器的設定，請在「主系統」或「高可用性系統」區段中選取虛擬機器名稱鏈結。
- 步驟 5** 您可以修改下列虛擬機器設定：

- 完整網域名稱 — 您系統的 FQDN。
- 虛擬機器 — 您的虛擬機器 IP 位址。
- 主要 DNS 伺服器
- 次要 DNS 伺服器
- 子網路遮罩/首碼
- 閘道

附註 您可以使用 IPv4 或 IPv6 虛擬機器設定來配置您的系統。部署期間，您可以僅設定 IPv4 設定，但您可以在此頁面上將您的虛擬機器更新為 IPv6。

步驟 6 選取儲存。
您的變更已儲存，虛擬機器會重新開機。

步驟 7 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

下一步動作

如果您對任何虛擬機器進行變更，則必須取得系統上每個虛擬機器的新憑證，除非您在相同網域中對系統使用萬用字元憑證。如需相關資訊，請參閱[管理憑證](#)，第 207 頁。

配置高可用性系統

高可用性系統是在主要系統失敗時提供備份的備援系統。



附註

在新增或移除高可用性系統之前開啓維護模式。如果排定維護時段來執行此作業，請注意在您關閉維護模式時，系統會執行系統重新開機作業。系統重新開機大約會花費 30 分鐘，取決於系統的大小。

新增高可用性系統



附註

高可用性系統上的大多數功能都被禁止。例如，您無權存取高可用性系統上的升級、SNMP 設定、儲存空間存取及電子郵件伺服器。您可以檢視系統屬性，但禁止修改。



附註

請在主系統上完成下列程序。

開始之前

- 請在次要虛擬機器上從 OVA 檔案安裝 Cisco WebEx，用作您的高可用性系統。



附註 您的高可用性系統大小必須與主系統大小相同。

- 您的高可用性系統必須使用與主系統相同的 OVA 和修補程式進行設定。如果您的主系統和高可用性系統的版本不符，則會指示您升級至較高的版本。
- 複製高可用性虛擬機器的完整網域名稱(FQDN)。您必須瞭解 FQDN，才能新增高可用性系統。
- 驗證所有虛擬機器是否正常運作。透過檢視系統監視器來確定虛擬機器狀態，如[關於儀表板, 第 103 頁](#)中所述。
- 我們建議您先取得高可用性虛擬機器的快照，再執行此程序。如果發生錯誤，則重做此快照程序。

程序

步驟 1 登入「管理」網站。

步驟 2 選取開啟維護模式。

步驟 3 在主系統上的「系統」區段中，選取檢視更多鏈結。

步驟 4 選取新增高可用性系統。

步驟 5 遵循系統屬性頁面上的指示，以新增此 HA 系統。

步驟 6 輸入高可用性系統的管理網站虛擬機器的 FQDN，並選取繼續。

我們將為此新增 HA 程序驗證主系統和 HA 系統的準備度。

- 如果兩個系統都已準備就緒，則您會看到一個綠色**新增**按鈕。請勿選取它，直到您將系統置於維護模式中。
- 如果系統未準備就緒，則您會看到一條錯誤訊息。修正錯誤，然後再次嘗試新增高可用性程序。

步驟 7 選取新增。

附註 如果顯示錯誤「錯誤碼：資料庫 64」，請使用高可用性虛擬機器的快照來重複此程序。

您的高可用性系統已新增，且會自動設定為在主系統出現故障時充當備份。

步驟 8 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，系統會重新開機。您可以在重新啟動完成後，重新登入管理網站。

移除高可用性系統

開始之前

您目前必須已將備用系統設定為高可用性系統。

程序

步驟 1 登入「管理」網站。

步驟 2 選取開啟維護模式。

步驟 3 在「系統」區段中，選取檢視更多鏈結。

步驟 4 選取移除高可用性系統。

即會出現**移除高可用性系統**頁面，顯示高可用性系統的完整網域名稱 (FQDN)。

步驟 5 選取繼續。

附註 移除高可用性系統後，您就無法再將相同的高可用性系統重新新增回您的網站。若要重新設定高可用性，必須透過 OVA 檔案重新部署高可用性系統來從頭開始。如需相關資訊，請參閱[新增高可用性系統](#)，第 69 頁。

即會移除您的高可用性系統。

步驟 6 開啟 VMware vCenter，然後使用 **從磁碟刪除** 命令移除高可用性系統。

步驟 7 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，系統會重新開機。您可以在重新啟動完成後，重新登入管理網站。

元件故障時的系統行為

當虛擬機器上執行的特定媒體和平台元件故障時，系統會自動重新啟動這些元件。受影響的會議會容錯移轉至系統中相同或另一個虛擬機器中的其他可用資源（適用於獨立式 50 個使用者的系統以外的系統）。

高可用性系統

在高可用性 (HA) 系統上，Cisco WebEx Meetings Server 將在發生單一元件故障時恢復這些元件：

- 一個虛擬機器上的單一服務。
- 虛擬機器。
- 單一實體伺服器或刀片式伺服器，可主控最多兩個虛擬機器（只要虛擬機器佈局符合《Cisco WebEx Meetings Server 系統需求》和《Cisco WebEx Meetings Server 規劃指南》中所列的規格。）
- 單一網路鏈結，假設以完全冗餘的方式佈建網路。
- 單一 Cisco Unified Communications Manager (CUCM) 節點，假設以冗餘的方式佈建 CUCM。

單一元件故障後，Cisco WebEx Meetings Server 系統的行為如下：

- 在最長三分鐘的時間內，應用程式共用、使用電腦進行的音訊語音連線及視訊都可能會中斷。Cisco WebEx Meetings Server 需要三分鐘來偵測故障，並自動重新連線所有受影響的會議用戶端。使用者無需關閉其會議用戶端和重新加入會議。
- 部分故障可能會導致通信會議音訊連線中斷。如果發生該情況，使用者需要手動重新連線。重新連線應該會在兩分鐘內完成。
- 關於部分故障，並非所有用戶端和會議都會受影響。通常會跨多個虛擬機器和主機重新分配會議連線。

適用於 2000 個使用者的系統的額外資訊

2000 個使用者的系統無需新增 HA 系統，即可提供部分高可用性功能。對於不具高可用性的 2000 個使用者的系統：

- 系統在遺失任何網路或媒體虛擬機器之後都仍然能夠運作，但系統容量將受影響。
- 遺失管理虛擬機器則會導致系統無法使用。

對於具高可用性的 2000 個使用者的系統：

- 遺失任何虛擬機器（管理、媒體或網路）都不會影響系統。即使遺失任何主控主要虛擬機器（管理和媒體或網路和媒體）的實體伺服器或 HA 虛擬機器（管理和媒體或網路），系統也仍然能以完整容量執行。
- 故障的虛擬機器重新啟動後會重新加入系統，且系統會回到正常的工作狀態。
- 當媒體虛擬機器故障時，該伺服器上主控的會議會短暫中斷，但會議會容錯移轉至替代的媒體虛擬機器。使用者必須手動重新加入桌面音訊和視訊階段作業。
- 當 Web 虛擬機器故障時，該虛擬機器上主控的現有網路階段作業也會失敗。使用者必須重新登入 Cisco WebEx 網站，並建立將在候補網路虛擬機器上主控的新瀏覽器階段作業。
- 當管理虛擬機器故障時，任何現有的管理員階段作業也會失敗。管理員必須重新登入管理網站，並建立將在候補管理虛擬機器上主控的新瀏覽器階段作業。此外，任何現有管理員或最終使用者會議階段作業都可能會出現短暫中斷。

變更虛擬 IP 位址

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取開啟維護模式及繼續以進行確認。
- 步驟 3** 選取系統並在「系統」區段中選取檢視更多。
- 步驟 4** 在「虛擬 IP 位址」區段的「類型」欄中，選取一個鏈結。

範例：

選取專用取得專用虛擬 IP 位址。

步驟 5 在「VIP IPv4 位址」對話方塊中，輸入您的新虛擬 IP 位址。

步驟 6 選取儲存。

步驟 7 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，系統會重新開機。您可以在重新啟動完成後，重新登入管理網站。

附註 系統大約需要 30 分鐘才能完成系統重新開機。針對包含此作業的系統維護排定維護時段時，如果指定所排定維護時段的持續時間，則務必將系統重新開機時段考慮在內。如需相關資訊，請參閱[排定維護時段](#), 第 110 頁。

設定公開存取

公開存取使您的網路外部的人員可以透過網際網路或行動裝置主持或出席線上會議。移除公開存取將移除您 WebEx 網站 URL 的「公用虛擬 IP 位址」設定，並終止對您網站的外部存取。

新增對系統的公開存取

開始之前

若要啟用公開存取，您必須先設定網際網路反向 Proxy 虛擬機器以充當公開存取系統。

啟動 VMware vCenter 並執行以下操作：

- 使用 VMware Data Recovery (vSphere 5.0) 或 VMware vSphere Data Protection (vSphere 5.1) 備份虛擬機器。這可讓您在必要時還原變更。如需相關資訊，請參閱[使用 VMware vCenter 來建立備份](#), 第 4 頁。
- 使用用於部署您的管理員虛擬機器的相同 OVA 檔案，來部署網際網路反向 Proxy 虛擬機器。您的網際網路反向 Proxy 虛擬機器必須位於與虛擬 IP 位址相同的子網路上。如需相關資訊，請參閱[新增公開存取](#), 第 32 頁。



附註 如果您有高可用性系統，您也必須為高可用性系統部署網際網路反向 Proxy 虛擬機器。

程序

步驟 1 登入「管理」網站。

步驟 2 選取開啟維護模式及繼續以進行確認。

步驟 3 選取系統，然後選取「系統」區段中的檢視更多鏈結。

步驟 4 選取新增公開存取。

步驟 5 在 FQDN 欄位中輸入網際網路反向 Proxy 虛擬機器。

附註 如果您的系統設定為高可用性，會有兩個完整網域名稱(FQDN)欄位。在第二個欄位中輸入您的高可用性 FQDN。

步驟 6 選取偵測虛擬機器。

- 如果您的系統未設定為高可用性，則會出現表格，其中顯示網際網路反向 Proxy 虛擬機器。
- 如果您的系統設定為高可用性，則會出現表格，其中顯示主要系統網際網路反向 Proxy 虛擬機器和高可用性網際網路反向 Proxy 虛擬機器。

如果您系統的任何更新與您用於建立網際網路反向 Proxy 虛擬機器的 OVA 版本不相容，您會收到一條錯誤訊息，且無法繼續，直到您使用與主要系統上的更新相容的合適 OVA 檔案重新部署網際網路反向 Proxy 虛擬機器。

步驟 7 選取繼續。**步驟 8 在公用 (VIP) 虛擬 IPv4 位址欄位中，輸入用於設定網際網路反向 Proxy 虛擬機器的相同子網路的 IP 位址，然後選取儲存。**

即會更新您的系統並設定公開存取。請確保在整個過程中保持瀏覽器視窗開啟。

如果主要系統需要與用於建立網際網路反向 Proxy 虛擬機器的 OVA 版本相容的次要更新，則會自動套用至網際網路反向 Proxy 虛擬機器。

步驟 9 如果您的系統需要次要更新，在更新完成後會提示您選取重新啟動。如果不需要任何更新，請繼續下一步。

在系統重新啟動後，您會收到一條確認訊息，指示您已新增公開存取。

步驟 10 驗證您的設定。如果感到滿意，您可以先刪除設定的虛擬機器備份，然後再執行此程序。**步驟 11 選取完成。****步驟 12 驗證您的安全性憑證是否仍然有效。由於此程序會變更您的虛擬機器，因此可能會影響您的憑證。如有必要，您的系統會提供自我簽署憑證以保持系統運作，直到您可以重新設定憑證為止。如需相關資訊，請參閱[管理憑證](#), 第 207 頁。****步驟 13 對您的 DNS 伺服器進行必要的變更。****步驟 14 選取關閉維護模式及繼續以進行確認。**

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

移除公開存取**開始之前**

使用 VMware Data Recovery (vSphere 5.0) 或 VMware vSphere Data Protection (vSphere 5.1) 備份虛擬機器。這樣可讓您在必要時還原變更。如需相關資訊，請參閱[使用 VMware vCenter 來建立備份](#), 第 4 頁。請務必在備份完成後開啟虛擬機器的電源。

程序

-
- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取開啟維護模式及繼續以進行確認。
- 步驟 3** 選取系統，然後選取「系統」區段中的檢視更多鏈結。
- 步驟 4** 選取所需的網站，選取**移除公開存取**，然後選取繼續。
即會從網站移除公開存取。
- 附註** 從您的網站移除公開存取後，您就無法再將相同的網際網路 Proxy 虛擬機器新增回該網站。若要重新設定公開存取，必須透過從 OVA 檔案重新部署網際網路反向 Proxy 虛擬機器來從頭開始。如需相關資訊，請參閱[新增對系統的公開存取](#), 第 142 頁。
- 步驟 5** 選取完成。
- 步驟 6** 開啓 VMware vCenter，關閉網際網路反向 Proxy 機器（以及高可用性網際網路反向 Proxy 機器，若已部署的話）的電源，並將其從您的系統中刪除。
- 步驟 7** 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啓動。您可以在重新啓動完成後，重新登入管理網站。
-

擴充系統大小

開始之前

開始執行系統擴充之前，請參閱[將系統擴充為較大的系統大小](#)，它說明您在使用本功能之前應該採取的所有必要步驟，以及如何使用自動或手動部署擴充系統。

程序

-
- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取開啟維護模式及繼續以進行確認。
- 步驟 3** 選取系統，然後選取「系統」區段中的檢視更多鏈結。
- 步驟 4** 選取擴充系統大小。
- 步驟 5** 選取繼續。
您的系統會檢查虛擬機器的連線。如果一或多個虛擬機器存在連線問題，您必須先修復問題然後才能繼續。如果沒有連線問題，您的系統會執行自動備份。在備份完成後，系統會通知您可以繼續進行擴充。
- 步驟 6** 使用以下其中一種方式部署 OVA 檔案：
- [使用自動部署來擴充系統](#)
 - [使用手動部署來擴充系統](#)

擴充完成後，系統便會通知您。

步驟 7 選取**重新啟動**。

步驟 8 登入「管理」網站。

步驟 9 選取**關閉維護模式**及**繼續**以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

設定一般設定

若要存取一般設定，請選取「設定」>「一般設定」下的**系統**和**檢視更多**鏈結。一般設定包括下列功能：

- 網站設定** — 使用此功能來配置或變更網站 URL。此功能還可顯示您的網站私人虛擬 IP 位址和網站公用虛擬 IP 位址。
- 管理設定** — 使用此功能可設定或變更您的管理網站 URL。此功能還可顯示您的管理網站私人虛擬 IP 位址。

變更網站設定

使用此功能變更您的網站 URL。部署時您可以設定您的原始網站 URL。如需網站 URL 設定及命名慣例的詳細資訊，請參閱 [WebEx 網站](#)和 [WebEx 管理 URL](#)，第 34 頁。

開始之前

確定您在 DNS 伺服器上保留原始網站 URL。將您的原始網站 URL 重新導向至更新的網站 URL。如果使用者嘗試使用原始 URL，但您未將其重新導向至新 URL，則他們無法主持或加入會議或從網頁、生產力工具及行動裝置應用程式登入。

程序

步驟 1 登入「管理」網站。

步驟 2 選取**開啟維護模式**及**繼續**以進行確認。

步驟 3 選取**系統**>**設定**>**一般設定**>**檢視更多**。

步驟 4 在「網站設定」區段中選取**編輯**。

步驟 5 在對話框中輸入您的新網站 URL，然後選取**儲存**。

步驟 6 選取**關閉維護模式**及**繼續**以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

下一步動作

更新您的網站憑證，以確保安全存取。如需相關資訊，請參閱[管理憑證, 第 207 頁](#)。

變更管理設定

部署時您可以設定您的原始管理網站 URL。如需管理網站設定及命名慣例的詳細資訊，請參閱[WebEx 網站和 WebEx 管理 URL, 第 34 頁](#)。

開始之前

請確定您在 DNS 伺服器上保留了原始管理網站 URL。請將您的原始管理網站 URL 重新導向至更新的管理網站 URL。如果使用者嘗試使用原始 URL，但您未將其重新導向至新 URL，則他們無法主持或加入會議或從網頁、生產力工具及行動裝置應用程式登入。

程序

-
- 步驟 1 登入「管理」網站。
 - 步驟 2 選取開啟維護模式及繼續以進行確認。
 - 步驟 3 選取系統 > 設定 > 一般設定 > 檢視更多。
會顯示一般設定頁面。
 - 步驟 4 在「管理設定」區段中選取編輯。
 - 步驟 5 在對話方塊中輸入您的新管理網站 URL，然後選取儲存。
 - 步驟 6 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。
-

下一步動作

更新您的網站憑證，以確保安全存取。如需相關資訊，請參閱[管理憑證, 第 207 頁](#)。

設定伺服器

使用以下功能來設定伺服器：

- SMTP 伺服器 — SMTP 伺服器負責將電子郵件從 Cisco WebEx Meeting Server 傳送至目標。
- 儲存伺服器 — NFS 伺服器是儲存所有會議錄製檔的儲存伺服器。

設定郵件伺服器

設定郵件伺服器，使您的系統能夠向使用者傳送會議邀請及其他通訊。



附註

您的郵件伺服器必須一直處於運作狀態。電子郵件是與您的使用者通訊的主要方式，包括錄製通知、會議資訊變更、帳戶狀態和其他許多重要公告。



附註

變更這些內容並不要求開啓維護模式。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取系統並在「伺服器」區段選取檢視更多。
- 步驟 3 在「郵件伺服器」區段中選取編輯。
- 步驟 4 輸入您的郵件伺服器主機名稱，然後選擇性地選取 **TLS 已啟用** 勾選方塊。
- 步驟 5 輸入您的郵件伺服器連接埠號碼，然後選擇性地選取 **伺服器驗證已啟用** 勾選方塊。
- 步驟 6 選取繼續。

設定 SMTP 伺服器

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取系統。
- 步驟 3 在「伺服器」下，選取檢視更多鏈結。
- 步驟 4 選取開啟維護模式及繼續以進行確認。
- 步驟 5 在「SMTP 伺服器」下，選取編輯鏈結。
- 步驟 6 填寫 SMTP 伺服器欄位：
 - 主機名稱 – 您的 SMTP 伺服器的主機名稱。
 - 連接埠 – 您的 SMTP 伺服器的連接埠號碼。
 - 使用者名稱 – 電子郵件用戶端的使用者名稱。
 - 密碼 – 使用者的密碼。
- 步驟 7 選擇性地選取 **TLS 已啟用** 和 **伺服器驗證已啟用** 勾選方塊。
- 步驟 8 選取儲存。
- 步驟 9 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啓動。您可以在重新啓動完成後，重新登入管理網站。

設定儲存伺服器

使用您的儲存伺服器備份系統並儲存會議錄製檔。「災害復原」（請參閱[使用災害復原功能](#)）期間，可以使用這些備份來還原系統。目前支援的儲存方法是網路檔案系統 (NFS)。確保可從所有內部虛擬機器存取您的儲存伺服器。（VMware 隨附的 VMware Data Recovery 功能也可以用來備份虛擬機器。如需相關資訊，請參閱 http://www.vmware.com/pdf/vdr_11_admin.pdf。）



附註

您無需將儲存伺服器連接至外部虛擬機器，例如網際網路反向 Proxy (IRP) 伺服器。

您的儲存伺服器每日都會備份下列內容：

- 特定系統設定
- 使用者資訊
- 會議資訊
- 上傳至系統的 SSL 憑證
- 網站 URL

每日會執行備份，且初始設定為當地時間上午 4:20。Cisco WebEx Meetings Server 在備份程序期間執行，而不會中斷會議、錄製檔或其他功能。系統不會移除之前的備份，直至完成下列每日備份，以確保備份可用。

您的系統大約需要 5 分鐘來備份 500 MB。備份系統所需的時間視儲存速度、NFS 速度及其他因素而定。備份 70 GB 資料庫大約需要 1 小時，且需 10 分鐘將其轉換為 NFS。轉換時間為 12 MB/秒，以允許其他網路通訊和確保產品持續運作。

開始之前

請務必設定您的 Unix 存取特權，以便您的系統可以儲存使用者產生的內容及系統備份。

在 Linux 型儲存系統上，這取決於您的「網路檔案系統 (NFS)」要使用之特定目錄的匿名使用者讀寫權限的配置。

在 Windows 型儲存系統上，這取決於網路存取：讓 **Everyone** 權限套用到匿名使用者設定。此外，您還必須向 Everyone 使用者群組提供 NFS 的讀寫權限。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取開啟維護模式及繼續以進行確認。
- 步驟 3 選取系統。
- 步驟 4 在「伺服器」區段，選取檢視更多。

如果您的系統上存在儲存伺服器，則儲存伺服器會顯示在此頁上。如果您的系統不存在任何儲存伺服器，則會為您提供設定儲存伺服器的選項。

- 步驟 5** 在「儲存伺服器」區段，選取**立即新增儲存伺服器**。
- 步驟 6** 輸入 NFS 掛接點，然後選取**儲存**。
系統會確認您的 NFS 掛接點。
- 步驟 7** 選取**繼續**。
您會收到一則確認訊息告知您的儲存伺服器已新增。
- 步驟 8** 選取**完成**。
- 步驟 9** 可以選擇性地變更每日備份的預設時間。在「儲存體伺服器」區段中，按一下「系統備份排程時間」，並從下拉功能表中選取另一時間。然後選取**儲存**。
每日備份發生於您所選取的時間，而不是您最初設定的當地時間上午 4:20。
- 步驟 10** 選取**關閉維護模式及繼續**以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

下一步動作

設定您的系統以在下列情況下使用儲存伺服器：

- 會議錄製檔。
- 災害復原。如需相關資訊，請參閱[使用災害復原功能](#)，第 149 頁。

若要確保您的儲存伺服器正確運作，請確定

- 是否可從 Cisco WebEx Meetings Server 之外存取儲存伺服器。
- 儲存伺服器是否已開啓。
- 儲存伺服器是否有網路連線。
- 是否可從非 Cisco WebEx Meetings Server 機器掛載/存取。
- 您的儲存伺服器是否已滿。



附註

如果使用者不小心從 **Cisco WebEx 會議錄製檔** 頁面刪除了某個錄製檔，但該錄製檔儲存在「網路檔案系統 (NFS)」儲存伺服器上，請聯絡 Cisco 技術協助中心 (TAC) 取得回復錄製檔的協助。

使用災害復原功能

使用災害復原功能，在系統故障或其他災害後復原您的部署。災害可以是網路損毀、伺服器故障、資料中心中斷，或其他令系統無法使用的活動。有以下兩種災害復原：

- 一個資料中心災害復原 — 如果您具有單一資料中心且您的系統變得無法使用，您可以在相同資料中心重新安裝您的系統，並將系統還原為相同的狀態。

- 兩個資料中心災害復原 — 如果您具有兩個資料中心且您的系統在第一個資料中心變得無法使用，則可以在第二個資料中心存取系統，並將第一個資料中心還原為相同的狀態。

在配置儲存伺服器之後，每日都會備份系統。系統備份通知會出現在儀表板上，並且包含最新備份的相關資訊。一次僅會在儲存空間中保留一個備份系統。執行升級或更新後，會保留舊版 Cisco WebEx Meetings Server 中的備份。我們建議您不要對不同的 Cisco WebEx Meetings Server 安裝使用相同的儲存目錄。

請注意，災害復原的下列特性：

- 需要 30 分鐘以上
- 以最新備份的設定覆寫您的設定
- 需要您執行其他步驟，將服務還原給您的使用者（此章節中下一步做什麼進行了詳細說明）

此程序備份特定系統設定、使用者資訊、會議資訊、上傳至系統的 SSL 憑證及網站 URL。備份程序不會為個別虛擬機器儲存 VMware 認證或 IP 位址資訊。（VMware 隨附的 VMware Data Recovery 功能也可以用來備份虛擬機器。如需相關資訊，請參閱 http://www.vmware.com/pdf/vdr_11_admin.pdf。）如果執行災害復原，您必須手動重新套用特定設定，包括下列內容：

- 特定外部元件的連線（例如，Cisco Unified Communications Manager (CUCM)）
- SSL 憑證（如果災害復原系統的主機名稱不同於原始系統中的主機名稱）
- 在部署一個資料中心時，可以選擇使用相同的 IP 位址或主機名稱。在部署兩個資料中心時，可以選擇對主要系統使用相同的 IP 位址或主機名稱。

發生災害且無法使用系統後，請執行下列程序。

開始之前

執行災害復原程序：

- 儲存伺服器必須已設定。如果您未設定儲存伺服器，則災害復原選項不可用，且不會建立任何備份。如需相關資訊，請參閱**設定儲存伺服器**。
- 您必須對可以在其中還原您的部署的系統具有存取權。請參閱下面有關一個資料中心災害復原和兩個資料中心災害復原的資訊。
- 您的復原系統的部署大小和軟體版本必須與原始系統相同。

對於高可用性系統，必須先設定災難復原，然後才能在該系統上配置高可用性。如果您的系統需要從災害復原，則必須先還原系統，然後在還原的系統上配置高可用性。如需高可用性的相關資訊，請參閱**新增高可用性系統**。

程序

-
- 步驟 1** 在您可以從可用於還原您的部署的系統上，登入管理網站。
 - 步驟 2** 選取**開啟維護模式**及繼續以進行確認。
 - 步驟 3** 選取**系統 > 伺服器 > 新增儲存伺服器**。
 - 步驟 4** 在**NFS 掛接點欄位**中輸入您儲存伺服器的名稱，然後選取**儲存**。

範例：

192.168.10.10:/CWMS/backup。

步驟 5 選取**繼續**以繼續進行災害復原。

如果復原系統部署大小和軟體版本與原始系統相符，您可以繼續進行災害復原。如果系統的部署大小或軟體版本不同，則您無法繼續直到在復原系統上重新部署應用程式以便部署大小及軟體版本符合原始部署為止。IP 位址或主機名稱不必符合原始部署。

步驟 6 選取以下其中一個動作以繼續：

- 取消** — 在新增儲存伺服器之前備份既存的系統。備份系統後，您會返回此頁面，且可以選取**繼續**以繼續進行。
- 繼續** — 覆寫您既有的系統，並繼續執行災害復原。

災害復原過程將開始。如果關閉瀏覽器，您無法重新登入系統，直到此過程完成。

步驟 7 選取**關閉維護模式及繼續**以進行確認。

在關閉維護模式後，您的系統會重新啓動。您可以在重新啓動完成後，重新登入管理網站。

下一步動作

您必須執行以下程序，將服務還原給您的使用者：

- 重新設定通信會議設定。請參閱《規劃指南》中的「設定 CUCM」，以瞭解更多資訊。
- 重新設定您的 SSO 設定。如需相關資訊，請參閱[配置同盟單一登入 \(SSO\) 設定](#)。
- 重新設定您的 SNMP 設定。如需相關資訊，請參閱[設定 SNMP 設定](#)。
- 重新設定您的憑證。如果您的 SSL 憑證與復原系統上設定的 SSL 憑證不相符，則可能必須重新載入您的 SSL 憑證。如需相關資訊，請參閱[還原 SSL 憑證](#)。
- 復原的系統最初配置為免費授權模式，該模式將在 180 天後到期。請在復原的系統上重新主控先前的系統授權。如需相關資訊，請參閱[在軟體升級或系統擴充之後重新主控授權及關於授權](#)。
- 設定您的 DNS 設定，使您的網站 URL 指向目前的 VIP。還原系統上的 VIP 可能與原始系統上的不同。您必須完成您的 DNS 設定，使最終使用者能夠使用其原始鏈結登入或加入還原系統上的會議。如需相關資訊，請參閱[變更虛擬 IP 位址](#)。
- 如果您的系統已設定目錄整合，並啓用了 LDAP 驗證，請驗證您的 CUCM 認證是否工作。取消系統的維護模式並完成系統重新開機之後，請登入管理網站，選取**使用者 > 目錄整合**，然後選取**儲存**。如果 CUCM 認證不正確，則會收到**無效認證錯誤**訊息。如果接收到此錯誤訊息，請輸入正確的認證，然後再選取**儲存**。如需相關資訊，請參閱[設定目錄整合](#)。

設定 SNMP 設定

您可以設定以下 SNMP 設定：

- 社群字串 — SNMP 社群字串會驗證對 MIB 物件的存取並充當內嵌密碼。
- USM 使用者 — 設定基於使用者的安全性模型 (USM)，以提供額外的訊息層級安全性。請選取現有 USM 設定以進行編輯，或新增其他 USM 設定。除預設 USM 使用者 `serveradmin`（對 MIB 資訊具有讀寫特權）以外，您設定的所有新 USM 使用者僅對 MIB 資訊具有唯讀特權。
- 通知目標 — 使用此功能可設定陷阱/通知接收者。

設定社群字串

您可以新增和編輯社群字串及社群字串存取特權。

新增社群字串

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取開啟維護模式及繼續以進行確認。
- 步驟 3 選取系統，然後選取 SNMP 區段中的檢視更多鏈結。
- 步驟 4 在「社群設定」區段中選取新增。
- 步驟 5 填寫新增社群字串頁面上的欄位。

選項	描述
社群字串名稱	輸入您的社群字串名稱。最大長度：256 個字元。
存取特權	<p>設定社群字串的存取特權。選項包括：</p> <ul style="list-style-type: none"> •唯讀 •讀寫 •讀寫通知 •僅通知 •無 <p>預設：唯讀</p>
主機 IP 位址資訊	<p>選取您的主機 IP 位址資訊類型。（預設：接受來自任何主機的 SNMP 封包）</p> <p>如果您選取接受來自以下主機的 SNMP 封包，則選項下面會顯示一個對話方塊。輸入主機名稱和 IP 位址，以逗號分隔。</p>

選取新增。

社群字串已新增至您的系統。

- 步驟 6** 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啓動。您可以在重新啓動完成後，重新登入管理網站。

編輯社群字串

程序

- 步驟 1** 登入「管理」網站。
步驟 2 選取開啟維護模式及繼續以進行確認。
步驟 3 選取系統，然後選取 SNMP 區段中的檢視更多鏈結。
步驟 4 選取「社群字串」區段中的社群字串名稱鏈結。
步驟 5 變更編輯社群字串頁面上所需的欄位。

選項	描述
社群字串名稱	變更您的社群字串名稱。最大長度：256 個字元。
存取特權	設定社群字串的存取特權。選項包括： <ul style="list-style-type: none"> •唯讀 •讀寫 •讀寫通知 •僅通知 •無 <p>預設：唯讀</p>
主機 IP 位址資訊	選取您的主機 IP 位址資訊類型。 <p>預設：接受來自任何主機的 SNMP 封包</p> <p>如果您選取接受來自以下主機的 SNMP 封包，則選項下面會顯示一個對話方塊。輸入主機名稱和 IP 位址，以逗號分隔。</p>

選取編輯。

您的社群字串資訊會變更。

- 步驟 6** 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啓動。您可以在重新啓動完成後，重新登入管理網站。

設定 USM 使用者

您可以新增和編輯您的 USM 使用者。

新增 USM 使用者

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取系統，然後選取 SNMP 區段中的檢視更多。
- 步驟 3 選取開啟維護模式及繼續以進行確認。
- 步驟 4 在「USM 使用者」區段中選取新增。
- 步驟 5 填寫新增 USM 使用者頁面上的欄位。

選項	描述
USM 使用者名稱	輸入您要設定的 USM 使用者名稱。最多 256 個字元。
安全性層級	<p>選取安全性層級。您選取的安全性層級可確定您可以為使用者設定的演算法和密碼。選項包括：</p> <ul style="list-style-type: none"> •noAuthNoPriv — 不為使用者設定驗證演算法和密碼，也不設定私密演算法和密碼。 •authPriv — 可讓您為使用者設定驗證演算法和密碼及私密演算法和密碼。 •authNoPriv — 可讓您為使用者設定驗證演算法和密碼。 <p>預設： noAuthNoPriv</p>
驗證演算法	<p>為使用者選取驗證演算法。</p> <p>附註 僅在安全性層級設定為 authPriv 或 authNoPriv 時才會顯示此選項。</p> <p>預設： SHA</p>
驗證密碼	<p>輸入使用者的驗證密碼。</p> <p>附註 僅在安全性層級設定為 authPriv 或 authNoPriv 時才會顯示此選項。</p>
私密演算法	<p>為使用者選取私密演算法。</p> <p>附註 僅在安全性層級設定為 authPriv 時才會顯示此選項。</p> <p>預設： AES128</p>

選項	描述
私密密碼	輸入使用者的私密密碼。 附註 僅在安全性層級設定為 authPriv 時才會顯示此選項。

步驟 6 選取新增。
USM 使用者已新增至您的系統。

步驟 7 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

編輯 USM 使用者



附註 預設 USM 使用者 **serveradmin** 是在內部使用的，該使用者只能變更密碼，但不能變更安全性層級、驗證及私密演算法。

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取系統，然後選取 SNMP 區段中的檢視更多。
- 步驟 3** 選取開啟維護模式及繼續以進行確認。
- 步驟 4** 選取「USM 使用者」區段中的 USM 使用者。
- 步驟 5** 變更編輯 USM 使用者頁面上所需的欄位。

選項	描述
USM 使用者名稱	變更 USM 使用者名稱。最多 256 個字元。
安全性層級	選取安全性層級。您選取的安全性層級可確定您可以為使用者設定的演算法和密碼。選項包括： <ul style="list-style-type: none"> •noAuthNoPriv — 不為使用者設定驗證演算法和密碼，也不設定私密演算法和密碼。 •authPriv — 可讓您為使用者設定驗證演算法和密碼及私密演算法和密碼。 •authNoPriv — 可讓您為使用者設定驗證演算法和密碼。 <p>預設： noAuthNoPriv</p>

選項	描述
驗證演算法	為使用者選取驗證演算法。 附註 僅在安全性層級設定為 authPriv 或 authNoPriv 時才會顯示此選項。 預設: SHA
驗證密碼	變更使用者的驗證密碼。 附註 僅在安全性層級設定為 authPriv 或 authNoPriv 時才會顯示此選項。
私密演算法	為使用者選取私密演算法。 附註 僅在安全性層級設定為 authPriv 時才會顯示此選項。 預設: AES128
私密密碼	變更使用者的私密密碼。 附註 僅在安全性層級設定為 authPriv 時才會顯示此選項。

步驟 6 選取**編輯**。
USM 使用者資訊會變更。

步驟 7 選取**關閉維護模式**及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

設定通知目標

您可以在系統上設定虛擬機器，以針對下列情況產生 SNMP 通知或陷阱：

- 虛擬機器啟動（冷啟動陷阱）
- 所有警報條件

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取系統，然後選取 SNMP 區段中的檢視更多鏈結。
- 步驟 3** 選取開啟維護模式及繼續以進行確認。
- 步驟 4** 選取通知目標下的新增通知目標。
- 步驟 5** 針對您的通知目標設定下列欄位：

選項	描述
目標主機名稱 / IP 位址	您想要設定為通知目標的虛擬機器的主機名稱或 IP 位址。
連接埠號碼	您虛擬機器的連接埠號碼。 預設： 162
SNMP 版本	您的 SNMP 版本。 預設： V3
通知類型	選取 Inform 或 Traps 。 預設： Traps
USM 使用者 附註 只有在「SNMP 版本」設定為 V3 時，才會出現此選項。	選取 USM 使用者。如需相關資訊，請參閱 設定 USM 使用者, 第 154 頁 。
社群字串 附註 此選項僅在「SNMP 版本」未設定為 V3 時才會出現。	選取社群字串。如需相關資訊，請參閱 設定社群字串, 第 152 頁 。

步驟 6 選取新增。
已新增您的通知目標。

步驟 7 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

編輯通知目標

設定通知目標

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取系統，然後選取 SNMP 區段中的檢視更多鏈結。
- 步驟 3** 選取開啟維護模式及繼續以進行確認。
- 步驟 4** 從通知目標清單中選取通知目標鏈結。
- 步驟 5** 您可以針對您的通知目標編輯下列欄位：

選項	描述
目標主機名稱 / IP 位址	您想要設定為通知目標的虛擬機器的主機名稱或 IP 位址。
連接埠號碼	您虛擬機器的連接埠號碼。 預設：162
SNMP 版本	您的 SNMP 版本。 預設：V3
通知類型	選取 Inform 或 Traps 。 預設：Inform
USM 使用者 附註 只有在「SNMP 版本」設定為 V3 時，才會出現此選項。	選取 USM 使用者。如需相關資訊，請參閱 設定 USM 使用者, 第 154 頁 。
社群字串 附註 此選項僅在「SNMP 版本」未設定為 V3 時才會出現。	選取社群字串。如需相關資訊，請參閱 設定社群字串, 第 152 頁 。

步驟 6 選取儲存。
您的通知目標變更即已儲存。

步驟 7 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

管理授權

購買此產品時，您可以享有六個月免費試用期。在免費試用期到期後，您需要為您的使用者購買授權。

可以使用內嵌的 Cisco Enterprise License Manager（請參閱[透過使用 License Manager 來履行授權](#)）、eFulfilment（請參閱[使用 eFulfilment 來訂購授權](#)）或者聯絡 TAC（請參閱[透過聯絡 TAC 來履行授權](#)）來取得授權。

關於授權

關於基於使用者的授權

本產品具有「基於主機的授權」。要求您為想要主持會議的每個使用者購買一個授權。瞭解下列詞彙很重要：

- **參加者** — 此人會出席會議，但不排定或主持會議，並且對主持人功能（例如呈現內容）沒有控制權，除非此參加者已由主持人指定為主講者。
- **會議主持人** — 排定會議，在主持人有空的時間內出席會議，並且對所選功能（例如識別主講者或將其他參加者靜音）具有控制權。
- **候補主持人** — 會議主持人不在時排定成且指定為擔當會議主持人角色的人員。如果排定會議的會議主持人未出席，則候補主持人會獲授與會議主持人對大部分功能具有的控制權。如果指定為候補主持人的個人及會議主持人都出席了會議，則從授權角度而言，候補主持人的狀態為參加者。
- **在主持人之前加入 (JBH)** — 允許參加者在主持人或候補主持人到達之前加入會議。
- **重疊會議** — 由同一個主持人排定在同一時間進行的兩個或多個會議。如果會議主持人或候補主持人開始重疊會議，則可能會耗用其他授權。個人可以排定重疊會議，但個人無法同時主持多個會議。如果一個會議的主持人離開該會議以開始另一個會議，而第一個會議會繼續（由其他擔任主持人的個人指導），則會發生重疊會議。
- **寬限期** — 15 分鐘重疊時段。只有在啟用 JBH 且由非主持人出席者開始會議時，才會套用寬限期。

每個月進行一次授權使用情況計算，例如，從 1 月 1 日到 31 日計算一次，從 2 月 1 日到 28 日計算一次，依此類推。計算授權的方式如下所示：

- **排定會議永不耗用授權。** 排定會議時，會議主持人可以指定候補主持人。指定候補主持人或者代表其他人排定會議並不會耗用授權。出席會議時，排定會議的個人依預設會指定為會議主持人。
- **參加者永不耗用授權。** 如果某個人這個月內一律以參加者身分出席會議，而且永不擔任主持人角色，則此人不耗用任何授權。
- **某個人第一次在給定月份開始會議時會耗用一個授權，而此授權會與個人產生關聯，並且將他們會指定為該會議的主持人。** 如果這個月內該人員開始更多的非重疊會議，則不會耗用其他授權。如果此人在接下來的一個月內沒有以主持人身分參加任何會議，則此人在這個月內不會耗用任何授權。該個人可以使用參加者的身分出席會議，而不耗用授權。
- **如果該個人以會議主持人身分出席每個重疊會議，則會額外耗用一個授權並與此個人產生關聯。** 單一個人所耗用的授權總數，是由此人所主持的重疊會議數目上限所決定。如果個人於同一時段內在主持人有空的時間內出席兩個會議，則會耗用兩個授權，並且這個月內都與這兩個授權相關聯。如果此人開始三個會議且重疊了同一個時段，則會耗用三個授權。依此類推。如果此人以主持人身分出席會議，第一個會議還沒有結束就離開，然後在主持人有空的時間內出席另一個會議，則此人需要兩個授權。
- **如果指定為候補主持人且在這個月內尚未耗用任何授權的個人開始會議，並且會議主持人加入會議，則不會耗用其他授權。**
- **如果這個月內尚未耗用授權的候補主持人在主持人有空的時間內出席一個會議，而排定該會議的會議主持人未能加入該會議，則此候補主持人會耗用一個授權並與此授權產生關聯。**

如果您要對系統執行主要升級或災害復原程序，則必須配置新的虛擬機器和重新主控授權。（請參閱[在軟體升級或系統擴充之後重新主控授權](#)）。

系統每個月會統計每個使用者的授權使用情況一次，如表格中的範例情境所示。表格中的情境假設在每個範例中，使用者在這個月內都是首次主持會議。

情境	會議日期	會議時間	耗用的授權
使用者 A 排定會議，但永不開始會議。	1 月 1 日	上午 09:00 到上午 10:00	0
使用者 B 開始一個會議。	1 月 2 日	上午 09:00 到上午 10:00	1
使用者 C 主持了兩個或多個不重疊的會議。	1 月 3 日 1 月 3 日 1 月 4 日	上午 09:00 到上午 10:00 下午 2:00 到下午 2:30。 上午 10:00 到上午 11:00	1
使用者 D 出席兩個重疊相同日期與時間的會議。	1 月 6 日 1 月 6 日	上午 09:00 到上午 10:00 上午 09:30 到上午 10:00	2
使用者 E 開始兩個重疊相同日期與時間的會議。主持人開始兩個會議，而候補主持人主持第二個會議。	1 月 6 日 1 月 6 日	上午 09:00 到上午 10:00 上午 09:30 到上午 10:00	3 一個授權由開始每個會議的主持人耗用，而另一個授權由候補主持人耗用。
使用者 F 在相同的日期開始兩個會議，然後離開這兩個會議。候補主持人主持每個會議。	1 月 7 日 1 月 7 日	上午 09:00 到上午 10:00 上午 09:00 到上午 10:00	2 對於原始主持人，則為每個會議一個；而且對於繼續其中一個會議的候補主持人，則為一個。
使用者 G 開始一個會議，並在會議期間將主持權轉交給另一位參加者。第一個會議的主持人隨後會開始第二個會議，此會議與第一個會議同時進行。	1 月 8 日 1 月 8 日	上午 09:00 到上午 10:00 上午 09:30 到上午 10:00	2 對於原始主持人，則為每個會議一個；而且對於繼續其中一個會議的候補主持人，則為一個。
使用者 H 開始一個啓用了在主持人之前加入的會議。主持人加入會議。第一個使用者隨後排定第二個會議（與第一個會議同時進行），但第二個會議的所有參加者均僅加入通信會議（而未加入網路部分）且選取了這個選項。	1 月 11 日 1 月 11 日	上午 09:00 到上午 10:00 上午 09:00 到上午 10:00	2

情境	會議日期	會議時間	耗用的授權
使用者 J 排定會議。已啓用在主持人之前加入。參加者加入會議，但會議主持人和候補主持人都未出席會議，並且所有參加者都離開會議。	1 月 11 日	上午 09:00 到上午 10:00	1
使用者 K 開始一個啓用了在主持人之前加入的會議。JBH 出席者代表主持人開始第二個會議。主持人在寬限期到期之前離開並結束了第一個會議。	1 月 12 日 1 月 12 日	上午 09:00 到上午 10:00 上午 9:10 到上午 10:00	1
使用者 L 使用帳戶 1、帳戶 2 與帳戶 3 在相同日期但不同時間開始三個個人會議（非網路部分）。	1 月 12 日 1 月 12 日 1 月 12 日	上午 09:00 到上午 10:00 上午 10:00 到上午 11:00 上午 11:00 到中午 12:00	1
使用者 M 使用帳戶 1、帳戶 2 與帳戶 3 在相同日期及時間開始三個個人會議（非網路部分）。	1 月 14 日	上午 09:00 到上午 10:00	3
在啓用了在主持人之前加入的情況下，使用者 N 在相同日期，但於不同時間開始一個會議及個人會議（非網路部分）。	1 月 14 日 1 月 14 日	上午 09:00 到上午 10:00 上午 11:00 到中午 12:00	1
在啓用了在主持人之前加入的情況下，使用者 P 在相同日期與時間開始一個會議及個人會議（非網路部分）。	1 月 15 日 1 月 15 日	上午 09:00 到上午 10:00 上午 09:00 到上午 10:00	2
使用者 Q 開始個人會議（而不是網路部分），並緊接著啓動重疊的網路部分。	1 月 16 日 1 月 16 日	上午 9:00 到上午 10:00 （個人會議） 上午 9:15 到上午 10:00 （「網路會議」與「個人會議」一起啓動）	1

您可以從**報告**頁面取得提供該月耗用的授權總數的報告。此外，我們還建議您檢視「PDF 摘要報告」，以按月顯示授權耗用趨勢。透過檢視整體授權趨勢，您可以更有效地規劃將來如何購買授權，以因應您公司內對此系統不斷成長的採用率。

**注意**

您的系統允許授權耗用量超過系統上安裝的授權數。管理員收到**授權超額使用**電子郵件，且儀表板通知會提示他們必須減少授權耗用量或在六個月內購買更多授權。在這六個月期間內，您的系統仍將對您的使用者繼續正常運作。如果在六個月後仍未減少授權耗用量或未購買更多授權，則系統將對所有使用者關閉，直到管理員安裝更多授權為止。

當系統關閉時，使用者無法排定、主持、出席會議，或存取會議錄製檔。使用者在 WebEx 網站上看到一則**網站維護**中訊息。管理網站正常運作，因此管理員可以登入並新增授權，來解決此授權數超出的狀況。安裝其他授權後，使用者便可以存取 WebEx 網站、主持會議、結束會議和存取錄製檔。

六個月免費試用期

在您首次登入本產品並完成首次體驗精靈後，即開始您的六個月免費試用。在免費試用期間，管理員可以設定系統，而您的使用者可以排定、主持及出席會議。管理網站頂部會出現一個橫幅，指示您的免費試用期剩餘月數。在試用期結束之前的一個月，您會收到一封電子郵件通知您必須購買和安裝授權，否則您的系統將被停用。

在免費試用結束之後，您的系統將被停用。新增授權之前，您可以登入系統，但無法使用任何其他功能。如需管理授權的相關資訊，請參閱**管理授權**小節（位於《Cisco WebEx Meetings Server 管理指南》）。

重新主控授權

升級 CWMS 軟體或擴充現有系統後，重新主控授權允許在所升級或擴充的系統上使用有效的舊授權。請參閱**在軟體升級或系統擴充之後重新主控授權**（位於《Cisco WebEx Meetings Server 管理指南》）。

取得授權

請聯絡您的 Cisco 銷售代表，為您的系統訂購授權。當您聯絡您的銷售代表時，將需要指定所需的授權數目。您組織中將要主持會議的每一個員工都將需要一個授權。

有數種方式可判定所需的授權數目。您可以使用您的儀表板來檢視使用情況、資源歷史記錄和會議趨勢，以判定您系統上主持和出席會議的使用者數目。在使用本產品數個月之後，即可使用每月摘要報告和自訂的詳細資訊報告，來幫助您判定所需的授權數。您的每月摘要報告會顯示有關服務採用和使用者授權使用情況的統計資料。服務採用統計資料顯示新使用者對您系統的採用率（以前三個月的採用率顯示），並預測未來三個月的成長率。使用者授權統計資料顯示前三個月的授權使用情況和未來三個月的預期成長率。

您可以使用內嵌的 Cisco Enterprise License Manager 或 eFulfilment，或者聯絡 TAC 來取得授權。如需管理授權的相關資訊，請參閱**管理授權**小節（位於《Cisco WebEx Meetings Server 管理指南》）。

超出您的授權數

當您購買授權並在系統上進行設定後，必須確定您有足夠的授權提供給您系統上的所有使用中主持人。系統每隔一個月會檢查，以確定是否有足夠的授權提供給每一個使用中的主持人。每個行事曆月份會重設授權計數。如果您系統上的使用中主持人數目超出授權數，則會傳送一封電子郵件給管理員，通知他已超出授權數。您有六個月寬限期來減少授權使用數或增加您系統上的授權數，使其

符合或超出使用中的主持人數。如果您在六個月寬限期結束之前未減少授權使用數或購買足夠的授權來符合使用情況，您的系統將被停用。發生此情況時，會有電子郵件通知管理員停用日期。

系統會檢查並調整管理網站上顯示的授權數。審核管理程式每天執行一次（在凌晨 2 點），以在必要時調整使用的授權數。在每月結束時，系統會檢查授權使用情況。如果主持人數低於授權數，則此授權數超出的狀況結束。如果使用中的主持人數仍然超出授權數，則會每月向您的管理員傳送一封新電子郵件，通知他授權數超出的狀況仍然存在以及系統停用的日期。

如果連續六個月仍有授權數超出的狀況，您的系統將被停用，且管理員會收到一封電子郵件通知他該狀況。系統停用之後，您的使用者將無法在您的系統上排定、主持或出席會議，或是存取錄製檔。管理網站仍將正常運作，所以管理員還是可以登入和新增授權。管理員對系統新增授權後，使用者將重新取得排定、主持和出席會議，以及存取錄製檔的能力。

臨時授權

如果您在系統上設定了臨時授權，則您的臨時授權狀態會顯示在管理網站每一頁的橫幅上。橫幅會通知您設定了多少臨時授權數，以及這些臨時授權到期的時間。當臨時授權到期時，您的系統將回到其先前的授權狀態。

到期授權

如果您要升級系統，還必須更新您的授權。升級系統之後，會傳送一封電子郵件給您的管理員，通知他有六個月的寬限期來更新授權。如果您在六個月寬限期結束之前未更新授權，您的系統將被停用。發生此情況時，會有電子郵件通知管理員停用日期。

系統會檢查並調整管理網站上顯示的授權數。審核管理程式每天執行一次（在凌晨 2 點），以在必要時調整到期授權數目。在每個月結束時，系統會檢查授權是否已從前一個期間更新。如果授權已更新，則到期授權狀況結束。如果尚未更新授權，則會每月向您的管理員傳送一封新電子郵件，通知他到期授權狀況仍然存在以及系統停用的日期。

如果在六個月後仍有到期授權狀況，您的系統將被停用，且管理員會收到一封電子郵件通知他該狀況。系統停用之後，您的使用者將無法在您的系統上排定、主持或出席會議，或是存取錄製檔。管理網站將正常運作，所以管理員可以登入和更新授權。管理員更新授權後，使用者將重新取得排定、主持和出席會議，以及存取錄製檔的能力。

Prime License Manager (PLM) 連線中斷

當您購買授權時，使用內嵌的 PLM 工具來輸入 PAK 並註冊授權。PLM 每隔 12 小時執行一次同步，以更新授權狀態和前次符合時間。如果兩天未連線至 PLM，則會傳送一封電子郵件給管理員，通知他 PLM 無法與系統同步。將有六個月的寬限期來重新連線至 PLM。如果系統在六個月寬限期結束之前未重新連線至 PLM，則會停用系統。發生此情況時，會有電子郵件通知管理員停用日期。

在系統無法連線至 PLM 的每個月月尾時，會傳送一封新電子郵件給管理員，向管理員通知系統的停用日期。如果系統在六個月寬限期到期之前重新連線至 PLM，則此狀況結束。

如果系統在六個月後仍然無法連線至 PLM，則系統會停用，且管理員會收到所發生狀況的電子郵件通知。如果停用系統，則使用者無法排定、主持或出席會議，也無法存取系統上的錄製檔。管理網站會正常運作，因此管理員可以登入系統，但系統必須重新連線至 PLM，才能結束此狀況並且恢復讓使用者排定、主持和出席會議以及存取錄製檔的能力。

需要新授權的動作

下列系統更改動作需要您安裝新授權：

- 擴充 — 如需相關資訊，請參閱[將系統擴充為較大的系統大小](#)。
- 升級 — 如需相關資訊，請參閱[升級系統](#)。
- 災害復原 — 如需相關資訊，請參閱[使用災害復原功能](#)。

透過使用 **License Manager** 來履行授權

請使用內嵌的 Cisco Enterprise License Manager 來取得授權：

開始之前

請聯絡您的 Cisco 銷售代表，為您的系統訂購授權。您的銷售代表將向您傳送一封電子郵件，其中含有您的產品授權金鑰 (PAK)。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取系統，然後選取「授權」區段中的檢視更多鏈結。
- 步驟 3 選取**管理授權**
瀏覽器會開啓一個新標籤或視窗，其中包含 Cisco Prime License Manager (PLM)。
附註 此版本的 PLM 內嵌在 Cisco WebEx Meetings Server 中。PLM 不是外部網站。
- 步驟 4 選取**授權管理 > 授權**。
- 步驟 5 選取**產生授權請求**。
即會出現**授權請求和後續步驟對話方塊**。
- 步驟 6 複製欄位中選取的文字，然後選取 **Cisco 授權註冊**。
- 步驟 7 登入您的 Cisco 帳戶。
- 步驟 8 在**產品授權金鑰**欄位中輸入您從 Cisco 銷售代表收到的 PAK，然後選取**下一步**。
即會出現**履行 PAK 頁**。
- 步驟 9 將您在前面複製的授權請求的內容貼到欄位中，輸入您所購買的授權數量，然後選取**下一步**。
- 步驟 10 複查頁面，然後選取**我同意授權條款**。
- 步驟 11 確定聯絡人電子郵件地址正確無誤。也可以選擇變更**傳送給**欄位中的聯絡人電子郵件地址。
- 步驟 12 選取**取得授權**
即會出現**授權請求狀態對話方塊**。
- 步驟 13 透過以下其中一種方式取得您的授權檔案：
 - 選取**下載**，以下載您的授權檔案 (.bin)。
 - 從透過電子郵件傳送給您的 ZIP 歸檔中解壓縮授權檔案 (.bin)。
- 步驟 14 返回管理網站並選取系統，然後選取「授權」區段中的檢視更多鏈結。
- 步驟 15 選取**管理授權**。

瀏覽器會開啓一個新標籤或視窗，其中包含 Cisco Prime License Manager (PLM)。

步驟 16 選取安裝授權檔案。

步驟 17 選取瀏覽，然後選取您下載或從您的電子郵件 ZIP 檔中解壓縮的授權檔案 (.bin)。

步驟 18 選取安裝。

即會安裝您的授權檔案。檢查所顯示的授權資訊，以確定其正確無誤。

步驟 19 在「履行日期」欄中選取目前。

此時會出現授權履行頁面。確認履行的授權區段中顯示的資訊正確。

使用 eFulfilment 來履行授權

可以在 License Manager 中輸入「產品授權金鑰 (PAK)」(而不使用網站)來履行授權訂單。

開始之前

請聯絡您的 Cisco 銷售代表，為您的系統訂購授權。您的銷售代表將向您傳送一封電子郵件，其中含有您的產品授權金鑰 (PAK)。

eFulfilment 要求可以在系統和 Cisco Systems, Inc. 之間建立網路連線。確認系統並非位在不允許存取的防火牆後面。如果不允許存取，請使用檔案型履行(請參閱[透過使用 License Manager 來履行授權](#))或者聯絡 TAC 以開啓案例來訂購授權(請參閱[透過聯絡 TAC 來履行授權](#))。

程序

步驟 1 登入「管理」網站。

步驟 2 選取系統，然後選取「授權」區段中的檢視更多鏈結。

步驟 3 選取管理授權

瀏覽器會開啓一個新標籤或視窗，其中包含 Cisco WebEx Meetings Server 中的內嵌 Cisco Prime License Manager (PLM)。(PLM 網站不是外部網站。)

步驟 4 選取從 PAK 履行授權。

此時會出現從 PAK 履行授權精靈。

步驟 5 在產品授權金鑰欄位中輸入您從 Cisco 銷售代表收到的 PAK，然後選取下一步。

即會出現履行 PAK 頁。

步驟 6 選取從新 PAK 新增授權。

步驟 7 在 *PAK 代碼方塊中輸入 PAK 代碼，然後選取下一步。

步驟 8 使用 cisco.com 使用者 ID 和密碼來登入。

此時會出現**履行授權**視窗，其中會指出可用的授權數目。

步驟 9 在**動作**欄中選取**履行**。

步驟 10 按一下**安裝**欄以編輯值。

步驟 11 輸入要針對此系統履行的授權數。如果 PAK 支援局部履行，則此範圍介於 1 到 PAK 中剩餘的授權數之間。

步驟 12 選取**儲存**。

步驟 13 選取**確定**。

此時會出現**履行授權**視窗。**安裝**欄中的值會顯示您選擇履行的授權數。

步驟 14 選取**下一步**。

此時會出現**複查內容**視窗。**現行值**欄會顯示作用中的授權數。**履行後**欄會顯示 eFulfillment 完成時您將具有的授權數。

步驟 15 選取**下一步**。

步驟 16 選取透過勾選此方塊，我確認已閱讀、瞭解並同意「最終使用者授權協議」條款和條件的限制。

步驟 17 選取**完成**。

當 License Manager 連線至 Cisco 以履行授權時，會顯示連線至授權伺服器進度列。eFulfillment 完成時，授權視窗中會新增一行。**履行日期**欄會顯示現行日期，其後緊跟著 - **現行**。可以選取此鏈結以顯示授權的詳細資料，包括此系統上所安裝的授權類型和數目。

透過聯絡 TAC 來履行授權

開始之前

取得您的註冊 ID 號碼。您可以透過開啓「企業授權管理」工具並選取**關於**，來尋找註冊 ID 號碼。

程序

步驟 1 登入「管理」網站。

步驟 2 選取**支援**並透過所列的號碼呼叫 TAC。

步驟 3 提交案例，請求您想要的額外授權數。

Cisco 會處理您的請求，並在您的系統上啓用額外授權。

步驟 4 選取**系統**。

步驟 5 檢查「授權」區段，確認已新增授權。



第 14 章

配置設定

此模組說明如何設定您的設定。

- [設定您的公司資訊, 第 168 頁](#)
- [配置您的品牌設定, 第 169 頁](#)
- [設定您的會議設定, 第 170 頁](#)
- [關於設定音訊設定, 第 172 頁](#)
- [設定您的視訊設定, 第 177 頁](#)
- [設定您的行動裝置設定, 第 177 頁](#)
- [設定服務品質 \(QoS\), 第 178 頁](#)
- [設定密碼, 第 179 頁](#)
- [配置您的電子郵件設定, 第 183 頁](#)
- [設定您的下載設定, 第 206 頁](#)
- [管理憑證, 第 207 頁](#)
- [產生 SSL 憑證, 第 208 頁](#)
- [匯入 SSO IdP 憑證, 第 215 頁](#)
- [匯入安全通信會議憑證, 第 215 頁](#)
- [設定使用者階段作業安全性, 第 217 頁](#)
- [配置同盟單一登入 \(SSO\) 設定, 第 217 頁](#)
- [設定您的雲端功能, 第 220 頁](#)
- [設定虛擬機器安全性, 第 221 頁](#)

設定您的公司資訊

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 如果要變更語言設定，請選取開啟維護模式和繼續以便確認。
附註 修改公司資訊頁面上的其他設定時，不必開啓維護模式。
- 步驟 3** 選取設定。如果您檢視其中一個其他設定頁面，您還可以在「設定」區段下選取公司資訊。
- 步驟 4** 填寫頁面上的欄位並選取儲存。

選項	描述
公司名稱	您的公司或組織名稱。
地址 1	地址行 1。
地址 2	地址行 2。
縣/市	您所在的城市。
省	您所在的州或省名稱。
郵遞區號	ZIP 或其他郵遞區號。
國家/地區	您所在的國家或地區名稱。
業務電話	含國家代碼的下拉功能表和含區碼的工作電話號碼欄位。
時區	您所在的時區。
語言	您的語言。語言設定會影響下列項目： <ul style="list-style-type: none"> • 管理員第一次啟動管理員帳戶時看到的登入頁面。 • 為撥入通信會議使用者播放的預設音訊提示。
地區設定	您的地區設定。地區設定會影響時間、日期、貨幣及數字的顯示。

- 步驟 5** 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，您的系統會重新啓動。您可以在重新啓動完成後，重新登入管理網站。

配置您的品牌設定

開始之前

請在配置您的品牌設定之前準備下列項目：

- 包含您公司標誌的 120x32 PNG、GIF 或 JPEG 影像
- 您公司的隱私權聲明 URL
- 您公司的服務條款聲明 URL
- 您公司的支援 URL

程序

步驟 1 登入「管理」網站。

步驟 2 選取設定 > 品牌。

步驟 3 填寫頁面上的欄位並選取儲存。

選項	描述
公司標誌	瀏覽至您的標誌檔案。您的標誌必須為 PNG、JPEG 或 GIF 格式。最大尺寸為 120x32 像素，最大檔案大小為 5 MB。
隱私權聲明	輸入您公司的隱私權聲明 URL。
服務條款	輸入您公司的服務條款 URL。
自訂頁尾文字	您輸入的文字將是系統傳送的所有最終使用者和管理員電子郵件的頁尾。
頁首背景色彩	選擇此選項關閉預設背景色彩。請注意：這將影響所有瀏覽器列和電子郵件。
支援聯絡 URL	輸入您公司支援網頁的 URL。

移除公司標誌

開始之前

請建立透明的 120x32 PNG 或 GIF 檔案。

程序

-
- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取設定 > 品牌。
- 步驟 3** 對於「公司標誌」欄位，選取瀏覽，然後選擇透明的 120x32 PNG 或 GIF 檔案。
- 步驟 4** 選取儲存。
- 您的空白 PNG 或 GIF 檔案會取代您先前的公司標誌。請確認原始標誌已移除。
-

設定您的會議設定

設定您的會議設定以控制參加者可以使用的功能。設定下列功能：

- 加入會議設定
- 每個會議的參加者人數上限（會議大小）



附註

此設定受部署期間設定的系統大小限制。如需相關資訊，請參閱[確認您的系統的大小](#), 第 29 頁。

- 參加者特權

程序

-
- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取設定 > 會議。
- 步驟 3** 在「加入會議設定」區段，選取您的選項。
- 預設設定為允許參加者在主持人之前加入會議、允許參加者在主持人之前加入通信會議及第一個加入的參加者將成為主講者。如果選取了允許參加者在主持人之前加入會議及允許參加者在主持人之前加入通信會議，則參加者最多可以在開始時間之前 15 分鐘加入會議。也可以選取任何人都可以在會議中做簡報。
- 附註 如果您取消選取允許參加者在主持人之前加入會議，則會自動取消選取第一個加入的參加者將成為主講者功能。

步驟 4 透過拖曳滑桿，選取每場會議的參加者人數上限。您系統的參加者人數上限在部署時即已設定。以下為系統大小設定和對應的最大會議大小。

系統大小	最大會議大小
50	50
250	100
800	100 (不具有 HA)，250 (具有 HA)
2,000	100 (不具有 HA)，250 (具有 HA)

步驟 5 在「參加者特權」區段中選取您的選項。預設會選取聊天、民意調查、文件複查與簡報及共用和遠端控制。所選的參加者特權會出現在使用者控制項中。

預設會停用錄製。選取錄製以在您的儲存伺服器上錄製和儲存會議。

附註 您必須設定儲存伺服器以啟用錄製。如需相關資訊，請參閱[設定儲存伺服器](#)，第 148 頁。

步驟 6 選取儲存。

關於會議安全性

Cisco WebEx Meetings Server 根據下列因素啟用不同會議安全性功能：

- 使用者類型：主持人、候補主持人使用者 (已登入) 及訪客。
- 會議有密碼或無密碼。
- 會議邀請中隱藏或顯示密碼。
- 電子郵件會議邀請中隱藏或顯示密碼。
- 行為顯示在會議加入頁 (請參閱下表)。

表 1：排定會議時已排除密碼

使用者類型	密碼顯示在電子郵件邀請和提醒中	會議詳細資訊頁
主持人	是	是
候補主持人	是	是
邀請的出席者	否	否
轉寄的出席者	否	否

表2: 排定會議時已包含密碼

使用者類型	密碼顯示在電子郵件邀請和提醒中	會議詳細資訊頁
主持人	是	是
候補主持人	是	是
邀請的出席者	是	是
轉寄的出席者	是	是

•在主持人之前加入已開啓/關閉。

開啓：出席者/訪客/受邀出席者可在主持人之前且排定開始時間前 15 分鐘加入會議。

關閉：出席者/訪客受邀出席者不能在主持人之前加入會議。主持人或候補主持人可開始會議，然後出席者才可加入。

•在主持人之前加入通信會議已開啓/關閉。

開啓：如果主持人未在會議用戶端開始通信會議，則出席者可在主持人之前加入通信會議。

關閉：如果主持人未在會議用戶端開始通信會議，則出席者無法在主持人之前加入通信會議。

•第一位出席者可主講已開啓/關閉。

開啓：若已設定「在主持人之前加入」,則第一位出席者為主講者。

關閉：主持人始終擁有球。

關於設定音訊設定

第一次設定音訊設定時，精靈會引導您完成過程，協助您設定 CUCM SIP 設定和撥入存取號碼。在您完成精靈並設定初始音訊設定之後，可以設定所有其他音訊設定。

首次配置您的音訊設定

首次配置您的音訊設定時，必須指定您想要的功能，您必須配置您的 CUCM 設定。精靈會引導您完成首次安裝程序。

開始之前

您必須先啓用通信會議並設定 CUCM，才能繼續音訊設定。如果您計劃向通信會議提供高可用性，則必須在兩個系統上設定 CUCM。請參閱《規劃指南》，以瞭解更多資訊。若要繼續，您必須取得下列資訊：

- 準備您的參加者用於撥入會議的撥入存取號碼清單。
- 您的 CUCM IP 位址。
- （選用）如果您計劃使用 TLS/SRTP 通信會議加密，請取得有效的安全會議憑證。如需相關資訊，請參閱[匯入安全通信會議憑證](#)。



附註 俄羅斯或土耳其未提供此功能。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取開啟維護模式及繼續以進行確認。
- 步驟 3 選取設定 > 音訊。
即會出現音訊頁面，且會顯示您的目前音訊功能。
- 步驟 4 選取下一步。
即會出現 **SIP** 設定頁面。此頁面會顯示您設定 CUCM 所需的 SIP 設定資訊，包括每種伺服器類型的 IP 位址和連接埠號碼。
- 步驟 5 選取下一步。
啟用通信會議： **CUCM** 設定頁面會出現，顯示您的目前設定。
- 步驟 6 選取編輯以變更您的設定。
即會出現 **CUCM (Cisco Unified Communications Manager)** 對話方塊。
- 步驟 7 填寫 **CUCM (Cisco Unified Communications Manager)** 對話方塊中的欄位，如下所示：
 - a) 為 CUCM 1 IP 位址和（可選）CUCM 2 IP 位址輸入 IP 位址。
這些 IP 位址必須對應於主要及選用的次要 CUCM 節點，而這些節點屬於「Cisco Unified Communications Manager 群組」，如同 CUCM 中「應用程式點 SIP 主幹連線」上配置的裝置集區所設定。如需更多詳細資料，請參閱《規劃指南》中的「配置應用程式點的 SIP 主幹連線」。
附註 CUCM 2 不是必要的，但建議使用以取得通信會議高可用性。
 - b) 輸入系統的連接埠號碼。連接埠號碼必須與 CUCM 中指定的連接埠號碼相符。（預設：5062）
 - c) 使用傳輸下拉功能表，為您的系統選擇傳輸類型。（預設：TCP）
附註 如果您選取 TLS 作為傳輸類型，則必須為每個 CUCM 伺服器匯入有效的安全會議憑證，匯出 SSL 憑證並將其上傳至 CUCM，以及在每個 CUCM 伺服器上將系統的完整網域名稱 (FQDN) 設定為 SIP 網域名稱。如需匯入憑證的相關資訊，請參閱[匯入安全通信會議憑證](#)；如需 CUCM 的相關資訊，請參閱《規劃指南》中的「設定 CUCM」。
 - d) 選取繼續。
 您的新或更新的 CUCM 設定會出現在啟用通信會議： **CUCM** 設定頁面上。
- 步驟 8 選取下一步。

啟用通信會議： 存取號碼設定頁面會顯示。

步驟 9 選取編輯。

即會出現撥入存取號碼對話方塊。

步驟 10 選取新增以新增撥入存取號碼。

對話方塊中會為電話標籤和號碼新增一行。每次您選取新增，對話方塊中都會顯示額外的一行。

步驟 11 為您新增的每個存取號碼輸入電話標籤和電話號碼，然後在您新增完號碼之後選擇繼續。

附註 確保您僅新增在 CUCM 中設定的號碼。您新增的號碼會出現在電子郵件邀請和 Cisco WebEx Meetings 用戶端中。

範例：

輸入「總部」作為電話標籤，並輸入電話號碼「888-555-1212」。

您輸入的存取號碼已新增至您的系統，您已返回啟用通信會議：存取號碼設定頁面。該頁面現在會指示已設定的存取號碼數目。

步驟 12 選取儲存。

精靈會通知您，您已成功設定通信會議功能。

步驟 13 (可選) 在顯示名稱對話方塊中輸入顯示名稱。

步驟 14 (可選) 在呼叫者 ID 對話方塊中輸入有效的呼叫者 ID。

附註 呼叫者 ID 限制為數字字元和破折號 (-)，最大長度為 32 個字元。

步驟 15 (可選) 設定您的「WebEx 撥我電話」設定 (預設：按 1 以連線至會議)。也可以選取此選項以略過按 1 連線至會議的要求。

附註 不建議選取此選項，除非您的電話系統不能傳送數字 1。

步驟 16 (可選) 選取您的電話的進入與退出聲音。

- 嘀嗒聲 (預設)
- 無聲音
- 播報姓名

步驟 17 (可選) 如果已在系統上設定 IPv6，請將您的 IPv6 通信會議設定，設定為開啟或關閉。(預設：關閉。關閉設定表示 IPv4 為設定值。)

附註 IPv6 通信會議選項不適用於未設定為 IPv6 的系統。

步驟 18 選取使用者撥入 Cisco WebEx 會議的音訊部分或使用「撥我電話」服務時能夠聽到的系統音訊語言。

步驟 19 選取儲存。

步驟 20 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

配置您的音訊設定

開始之前

如果您未配置您的音訊設定，請參閱[首次配置您的音訊設定](#)，第 172 頁。



附註

配置或變更「撥入存取號碼」、「顯示名稱」、「呼叫者 ID」音訊設定時，不需要開啓維護模式。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取開啟維護模式及繼續以進行確認。
- 步驟 3 選取設定 > 音訊。
- 步驟 4 配置您的編輯音訊功能設定。

選項	描述
WebEx 音訊	<ul style="list-style-type: none"> •使用者「撥入」和「撥我電話」服務 – 可讓使用者透過撥打指定的電話號碼或接聽系統「撥我電話」來電，出席通信會議。 •撥入 – 可讓使用者透過撥打指定電話號碼的方式出席通信會議。 •關閉 – 停用所有呼叫功能。
使用電腦進行語音連線	<ul style="list-style-type: none"> •開啓 •關閉

- 步驟 5 在「編輯通信會議設定」區段中，選取 CUCM (Cisco Unified Communications Manager) 下的編輯鏈結，變更您的設定。

選項	描述
CUCM 1 IP 位址	輸入您 CUCM 1 系統的主機名稱或 IP 位址。
CUCM 2 IP 位址	(可選) 輸入您 CUCM 2 (負載平衡服務) 系統的主機名稱或 IP 位址。 附註 CUCM 2 不是必要的，但建議使用以取得通信會議高可用性。
連接埠號碼	請輸入有效的連接埠號碼。請確定連接埠號碼與 CUCM 中的設定相符。 預設: 5062

選項	描述
傳輸	<p>選取傳輸類型。</p> <p>附註 如果您選取 TLS 作為傳輸類型，則必須為每個 CUCM 伺服器匯入有效的安全會議憑證，匯出 SSL 憑證並將其上傳至 CUCM，以及在每個 CUCM 伺服器上將系統的完整網域名稱 (FQDN) 設定為 SIP 網域名稱。請參閱匯入安全通信會議憑證, 第 215 頁，以取得匯入憑證的相關資訊；參閱《Cisco WebEx Meetings Server 規劃指南》中的「配置 CUCM」，以取得 CUCM 的相關資訊。</p> <p>預設：TCP</p>

即會出現 CUCM (Cisco Unified Communications Manager) 對話方塊。填寫欄位並選取繼續。

步驟 6 在「編輯通信會議設定」區段，選取「撥入存取號碼」下的編輯鏈結，以新增、變更或刪除您的存取號碼。

- a) 選取**新增**並為您要新增的每一個新存取號碼輸入電話標籤和電話號碼。
- b) 若要刪除號碼，請選取行末的刪除鏈結。
- c) 針對您要變更的任何存取號碼，在電話標籤和電話號碼欄位中輸入更新的資訊。
- d) 完成後選取繼續。

附註 確保您僅新增在 CUCM 中設定的號碼。您新增的號碼會出現在電子郵件邀請和 Cisco WebEx Meetings 用戶端中。

步驟 7 在顯示名稱對話方塊內輸入顯示名稱。

步驟 8 在呼叫者 ID 對話方塊內輸入有效的呼叫者 ID。

附註 呼叫者 ID 限制為數字字元和破折號 (-)，最大長度為 32 個字元。

步驟 9 配置您的「WebEx 撥我電話」設定（預設：按 1 以連線至會議）。也可以選取此選項以略過按 1 連線至會議的要求。

附註 Cisco 不建議選取此選項，除非您的電話系統不能傳送數字 1。

步驟 10 選取您的電話的進入與退出聲音。

- 嘀嗒聲（預設）
- 無聲音
- 播報姓名

步驟 11 如果已在系統上設定 IPv6，請將您的 IPv6 通信會議設定，設定為開啟或關閉。（預設：關閉。關閉設定表示 IPv4 為設定值。）

附註 IPv6 通信會議選項不適用於未設定為 IPv6 的系統。

步驟 12 選取儲存。

步驟 13 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

設定您的視訊設定

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取設定 > 視訊。
- 步驟 3 選取開啟或關閉，然後選取儲存。(預設： 開啟)。

設定您的行動裝置設定



附註

Cisco WebEx Meetings Server 2.0 及更高版本支援 Android。依預設，會啓用 iOS 和 Android WebEx 應用程式。

開始之前

若要設定行動裝置設定，您必須於部署期間在系統上新增公開存取。如需相關資訊，請參閱[新增對系統的公開存取](#)。

請注意，如果系統配置為允許多個撥入存取號碼，則系統會假設第一個號碼是免費存取號碼，並且行動裝置應用程式預設為先嘗試這個號碼。如果無法從行動網路存取這個號碼，則應用程式將無法連線。請確保可從行動網路存取這個號碼。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取設定 > 行動裝置。
- 步驟 3 透過選取您的系統支援的行動裝置平台來配置您的行動裝置設定，然後選取儲存。(預設： iOS WebEx 應用程式和 Android WebEx 應用程式已選定)

附註

- 必須具有 DMZ 網路，才能使用 iOS 或 Android 行動裝置來存取會議。如果不具有 DMZ 網路，則 iOS WebEx 應用程式選項和 Android WebEx 應用程式選項會變成灰色。

- iOS 和 Android WebEx 應用程式的運作方式，與 Cisco WebEx 桌面應用程式相同；從內部網路或外部網際網路。

設定服務品質 (QoS)

區別服務 (DiffServ) 代碼點 (DSCP) 設定可決定音訊和視訊媒體訊號的 QoS，如 RFC 2475 定義。Cisco 建議您保留預設值。當網路需要不同的 DSCP 設定時（很少出現此情況），可使用其他值。如需更多資訊，請參閱適用於您的 Cisco Unified Communications Manager 版本之 Cisco Unified Communications Solution Reference Network Design (SRND) 的「Network Infrastructure」章節，網址是 http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html。

以下是預設值：

•WebEx 音訊（媒體）

IPv4 QoS 標記：**EF DSCP 101110**

IPv6 QoS 標記：**EF DSCP 101110**

•WebEx 音訊（訊號）

IPv4 QoS 標記：**CS3（優先順序 3）DSCP 011000**

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取設定 > 服務品質。
- 步驟 3 使用適當的下拉功能表選取 QoS 標記設定，然後選取儲存。

關於 QoS 標記

請參閱下面的表格，以取得某些部署（其流量流經網際網路反向 Proxy 伺服器）與某一部署（其流量不流經網際網路反向 Proxy 伺服器）的 QoS 標記資訊。

Cisco WebEx Meetings Server 系統（流量流經網際網路反向 Proxy 伺服器）上的 QoS 標記

流量	QoS 標記
SIP 音訊—媒體—CWMS 至端點	是
SIP 音訊—訊號—CWMS 至端點	是
PC 音訊—媒體—CWMS 至用戶端	否
PC 音訊—訊號—CWMS 至用戶端	否
PC 音訊—媒體—用戶端至 CWMS	否
PC 音訊—訊號—用戶端至 CWMS	否

流量	QoS 標記
PC 視訊—媒體—CWMS 至用戶端	否
PC 視訊—訊號—CWMS 至用戶端	否
PC 視訊—媒體—用戶端至 CWMS	否
PC 視訊—訊號—用戶端至 CWMS	否

Cisco WebEx Meetings Server 系統（流量不流經網際網路反向 Proxy 伺服器）上的 QoS 標記

流量	QoS 標記
SIP 音訊—媒體—CWMS 至端點	是
SIP 音訊—訊號—CWMS 至端點	是
PC 音訊—媒體—CWMS 至用戶端	是
PC 音訊—訊號—CWMS 至用戶端	是
PC 音訊—媒體—用戶端至 CWMS	否
PC 音訊—訊號—用戶端至 CWMS	否
PC 視訊—媒體—CWMS 至用戶端	是
PC 視訊—訊號—CWMS 至用戶端	是
PC 視訊—媒體—用戶端至 CWMS	否
PC 視訊—訊號—用戶端至 CWMS	否

設定密碼

您可以針對以下幾項設定密碼設定：

- 一般密碼 — 用於控制密碼有效期限，可讓您強制使用者立即或按指定的時間間隔變更其密碼。
- 使用者密碼 — 可讓您為使用者帳戶設定密碼強度，包括大小寫混合、長度、字元類型和使用、動態網頁文字控制項，以及設定不可接受的密碼清單。
- 會議密碼 — 可讓您強制會議使用密碼並為會議設定密碼強度，包括大小寫混合、長度、字元類型和使用、動態網頁文字控制項，以及設定不可接受的密碼清單。



附註

如果您的系統上已啟用 SSO，則一般密碼和使用者密碼頁面上的設定及編輯使用者頁面上的密碼變更控制項將不再適用於主持人帳戶。

配置您的一般密碼設定

您的一般密碼設定可讓您設定帳戶停用和密碼使用期限限制。此頁面上的所有密碼設定均為可選，且可開啓（勾選）或關閉（未勾選）。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取設定 > 密碼管理 > 一般密碼。
- 步驟 3 （可選）選取在主持人帳戶處於非使用狀態 數字 天後將其停用勾選方塊，然後在文字欄位中輸入天數。（預設：已勾選且設定為 90 天）
如果您使用預設值，而使用者未主持或排定會議連續 90 天，則會停用使用者。
附註 此功能僅適用於主持人帳戶。您無法使用此功能停用管理員帳戶。若要停用管理員帳戶，請參閱[停用使用者](#), 第 125 頁。
- 步驟 4 （可選）選取強制所有使用者每隔 數字 天變更一次密碼勾選方塊，然後在文字欄位中輸入天數。（預設：未勾選）
- 步驟 5 （可選）選取強制所有使用者在下次登入時變更密碼。（預設：未勾選）
- 步驟 6 選取儲存。

設定您的使用者密碼設定

設定您的使用者密碼要求和限制。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取設定 > 密碼管理 > 使用者密碼。
- 步驟 3 設定頁面上的欄位來變更您的使用者密碼設定。

選項	描述
要求為使用者帳戶使用強密碼	選取此選項以啓用剩餘選項。 預設：已選取
最小字元長度	最少字元要求。 預設：已選取和 6 個字元
最少字母字元數	最少字母（非數字、非特殊字元）數。 預設：已選取和 1 個字元

選項	描述
最少數字字元數	最少數字（非字母、非特殊字元）數。 預設：已選取和 1 個數字
最少特殊字元數	最少特殊字元（非字母、非數字字元）數。 預設：未選取和 1 個字元
必須包含大小寫混合	密碼必須包含大寫和小寫字母字元。 預設：已選取
不允許任何字元重複出現超過 3 次	一個字元（字母、數字或特殊字元）不得重複三次以上。 預設：已選取
不可接受的密碼的清單	管理員指定的無法使用的密碼清單。 預設：未選取
公司名稱、網站名稱、使用者電子郵件地址和主持人姓名永遠不可接受	請勿使用這些特定名稱。 預設：已選取
不能包含先前使用的 n 個密碼	請勿使用先前用過的密碼。從下拉功能表中選取一個數字，以指定不能使用的先前密碼的個數。 預設：已選取 預設數字：5

步驟 4 選取儲存。

設定您的會議密碼

使用此功能來設定會議密碼參數。下表描述在設定會議時，哪些使用者必須輸入密碼。

設定密碼	在電子郵件邀請中排除密碼	會議建立者登入	主持人登入	受邀者登入	訪客登入	訪客不登入
否	不適用	不需要密碼。	不需要密碼。	不需要密碼。	不需要密碼。	不需要密碼。
是	是	不需要密碼。	不需要密碼。	不需要密碼。	需要密碼。	需要密碼。

設定密碼	在電子郵件邀請中排除密碼	會議建立者登入	主持人登入	受邀者登入	訪客登入	訪客不登入
是	否	不需要密碼。	不需要密碼。	不需要密碼。	需要密碼。 可以預先填入密碼。	需要密碼。 可以預先填入密碼。

程序

步驟 1 登入「管理」網站。

步驟 2 選取設定 > 密碼管理 > 會議密碼。

步驟 3 透過設定頁面上的欄位，來變更您的會議密碼設定。

附註 依預設，所有選項都未選取。

選項	描述
所有會議都必須有密碼	要求所有會議都具有密碼。
要求為會議使用強密碼	選取此選項以啓用剩餘選項。
最少字元長度	最少字元要求。 預設： 6
最少字母字元數	最少字母（非數字、非特殊字元）數。 預設： 1
最少數字字元數	最少數字（非字母、非特殊字元）數。 預設： 1
最少特殊字元數	最少特殊字元（非字母、非數字字元）數。 預設： 1
不能包含這些特殊字元 (空格、\、'、"、/、&、<、>、=、[、])	選取此選項可禁止使用這些字元。
必須包含大小寫混合	密碼必須包含大寫和小寫字母字元。
不可接受的密碼的清單	管理員指定的無法使用的密碼清單。
公司名稱、網站名稱、使用者電子郵件地址、主持人姓名和會議主題永遠不可接受	選取此選項可禁止使用這些字詞或字串。

步驟 4 選取儲存。

配置您的電子郵件設定

您可以配置您的電子郵件設定和範本。您的電子郵件範本具有預設設定，您也可以加以變更。

程序

步驟 1 登入「管理」網站。

步驟 2 選取設定 > 電子郵件。
會顯示變數頁面。

步驟 3 輸入您的寄件者姓名、寄件者電子郵件地址、回覆電子郵件地址，然後選取儲存。
附註 如果在「變數」頁面上的「寄件者姓名」中輸入人名，但會議邀請將反映主持人的電子郵件地址。

步驟 4 選取範本。如需各範本類型的說明，請參閱[關於電子郵件範本](#)，第 183 頁。
會顯示範本頁面。請選取通用或會議標籤。通用為預設值。

步驟 5 若要設定電子郵件範本，請選取通用和會議標籤上想要的範本鏈結。

步驟 6 對您選取的電子郵件範本做出變更（如有），然後選取儲存。

範例：

選取「通用」標籤上的帳戶已被重新啟動範本鏈結。對帳戶已被重新啟動對話方塊中的欄位做出變更，然後選取儲存。

預設寄件者姓名、寄件者電子郵件地址與回覆值取自您在變數頁面配置的設定。

附註 如果在變數頁面上輸入寄件者姓名的人名，則系統會自動將人名取代為所有會議邀請的 WebEx 網站 URL。

關於電子郵件範本

使用電子郵件範本將重要活動傳達給使用者。各電子郵件範本均有您必須設定的變數。請參閱下表瞭解各範本中的變數描述。

有兩種電子郵件範本：

- 通用 – 包括遺失密碼、主持人和受邀者通知、錄製檔可用性及其他一般通知。
- 會議 – 包括會議邀請、取消、更新、提醒及資訊通知。

表3: 通用電子郵件範本

標題	描述	變數
AD 啟用	啟用AD帳戶後傳送給使用者。	<ul style="list-style-type: none"> •%SiteURL% •%DisplayName% •%SSOSignINLink% •%OrgLogo% •%Participants% •%Support% •%CustomFooterText% •%Year%
AD 同步失敗	同步失敗後傳送給管理員。	<ul style="list-style-type: none"> •%FullName% •%Failure_Reason% •%DownloadLogURL% •%Sync_Start_Time% •%Sync_Completion_Time% •%Users_Added% •%Users_Deactivated% •%Users_Failed_to_Sync% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
AD 同步成功	同步成功後傳送給管理員。	<ul style="list-style-type: none"> •%FullName% •%DownloadLogURL% •%Sync_Start_Time% •%Sync_Completion_Time% •%Users_Added% •%Users_Deactivated% •%Users_Failed_to_Sync% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
帳戶已被重新啟動	在管理員重新啟動使用者的帳戶後傳送給使用者。	<ul style="list-style-type: none"> •%DisplayName% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
忘記密碼 – 密碼已變更	在使用者已從最終使用者網站重設密碼後，傳送至使用者。	<ul style="list-style-type: none"> •%SiteURL% •%DisplayName% •%OrgLogo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
忘記密碼 - 重設密碼	在使用者已從最終使用者網站重設密碼後，傳送至使用者。此電子郵件會要求使用者建立新密碼。	<ul style="list-style-type: none"> •%SiteURL% •%DisplayName% •%OrgLogo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
PT PCN 會議邀請 - 受邀者	在 PCN 帳戶使用生產力工具排定會議後傳送給會議受邀者。	<ul style="list-style-type: none"> •%HostName% •%Topic% •%TeleconferencingInfo% •%Meeting Link% •%Meeting Number% •%Meeting Password% •%Meeting Space% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
PT PCN 會議通知 - 主持人	在 PCN 帳戶使用生產力工具排定會議後傳送給會議主持人。	<ul style="list-style-type: none"> •%HostName% •%Topic% •%TeleconferencingInfo% •%Meeting Link% •%Meeting Number% •%Meeting Password% •%Meeting Space% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
PT — 主持人通知	在使用生產力工具排定會議後傳送給會議主持人。	<ul style="list-style-type: none"> •%Topic% •%HostName% •%Meeting Link% •%Meeting Number% •%Meeting Password% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText%
PT — 受邀者通知	在使用生產力工具排定會議後傳送給會議受邀者。	<ul style="list-style-type: none"> •%Topic% •%HostName% •%Meeting Link% •%Meeting Number% •%Meeting Password% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText%
錄製檔可用（針對主持人）	向主持人傳送會議錄製檔的鏈結。	<ul style="list-style-type: none"> •%SiteURL% •%OrgLogo% •%DisplayName% •%Topic Name% •%Duration% •%Recording Time% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
SSO 啟動電子郵件	在啟用單一登入 (SSO) 後傳送。	<ul style="list-style-type: none"> •%SiteURL% •%DisplayName% •%OrgLogo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
傳送電子郵件給所有使用者	向系統上的所有使用者傳送電子郵件。	<ul style="list-style-type: none"> •%SiteURL% •%Subject% •%OrgLogo% •%AttendeeName% •%Body% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
安裝 Cisco WebEx – Android	通知使用者 Android 版 Cisco WebEx 應用程式，並提供該應用程式的下載鏈結。	<ul style="list-style-type: none"> •%SiteURL% •%Subject% •%OrgLogo% •%DisplayName% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
安裝 Cisco WebEx – iPhone/iPad	通知使用者 iPhone/iPad 版 Cisco WebEx 應用程式，並提供該應用程式的下載鏈結。	<ul style="list-style-type: none"> •%SiteURL% •%Subject% •%OrgLogo% •%DisplayName% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
共用錄製檔	向選取的會議出席者傳送會議錄製檔的鏈結。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%OrgLogo% •%AttendeeName% •%HostName% •%Topic Name% •%Duration% •%Recording Time% •%Personalized Message% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
從 MC 共用錄製檔	向選取的會議出席者傳送會議錄製檔的鏈結。在選取離開會議後，由 Meeting Center 中的主持人選取的出席者。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%OrgLogo% •%AttendeeName% •%Topic Name% •%Duration% •%Recording Time% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
使用者 — 密碼已變更	當使用者密碼變更後向其傳送電子郵件。	<ul style="list-style-type: none"> •%SiteURL% •%OrgLogo% •%DisplayName% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
歡迎電子郵件	在建立新管理員的帳戶後傳送給他或她。	<ul style="list-style-type: none"> •%SiteURL% •%DisplayName% •%SiteURL% •%Support% •%participants% •%CustomFooterText% •%Year%

表4: 會議電子郵件範本

標題	描述	變數
進行中會議的邀請（針對出席者）	當主持人邀請使用者加入會議（會議在進行中）時傳送給使用者。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%Topic% •%AttendeeName% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%MeetingNumber% •%MeetingPassword% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
即時會議的邀請（針對主持人）	當主持人選取現在開會時傳送給主持人和出席者。	<ul style="list-style-type: none"> •%SiteURL% •%Topic% •%HostName% •%Topic_HTML% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%MeetingNumber% •%MeetingPassword% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
會議已取消（針對出席者）	通知使用者排定的會議已被取消。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%Topic% •%AttendeeName% •%HostName% •%Topic_HTML% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%Write% •%SiteURL% •%CustomFooterText% •%Year%
會議已取消（針對主持人）	傳送給會議的主持人以確認會議取消。	<ul style="list-style-type: none"> •%SiteURL% •%Topic% •%HostName% •%Topic_HTML% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%Write% •%SiteURL% •%CustomFooterText% •%Year%

標題	描述	變數
會議資訊已更新（針對候補主持人）	在會議設定變更後為候補主持人提供會議資訊。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%Topic% •%OrgLogo% •%AlternateHostName% •%MeetingTime% •%HostName% •%Duration% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
會議資訊已更新（針對出席者）	在會議設定變更後為會議受邀者提供會議資訊。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%Topic% •%AttendeeName% •%HostName% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%MeetingNumber% •%MeetingPassword% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
會議資訊已更新（針對主持人）	在會議設定變更後為主持人提供會議資訊。	<ul style="list-style-type: none"> •%SiteURL% •%Topic% •%HostName% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
會議提醒（針對候補主持人）	向會議的候補主持人傳送會議提醒。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%Topic% •%OrgLogo% •%AlternateHostName% •%MeetingTime% •%HostName% •%Duration% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
會議提醒（針對主持人）	向會議的主持人傳送會議提醒。	<ul style="list-style-type: none">•%SiteURL%•%Topic%•%OrgLogo%•%HostName%•%MeetingTime%•%HostName%•%Duration%•%MeetingNumber%•%MeetingPassword%•%HostNumber%•%TeleconferencingInfo%•%SiteURL%•%Support%•%CustomFooterText%•%Year%

標題	描述	變數
已重新排定會議（針對候補主持人）	向候補主持人傳送更新的會議資訊。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%Topic% •%AlternateHostName% •%HostName% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
已重新排定會議（針對出席者）	向出席者傳送更新的會議資訊。	<ul style="list-style-type: none">•%HostName%•%HostEmail%•%Topic%•%AttendeeName%•%HostName%•%MeetingDateOrRecurrence%•%MeetingTime%•%TimeZone%•%MeetingNumber%•%MeetingPassword%•%TeleconferencingInfo%•%SiteURL%•%Support%•%CustomFooterText%•%Year%

標題	描述	變數
會議資訊（針對候補主持人）	向候補主持人傳送會議確認。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%Topic% •%AlternateHostName% •%HostName% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
會議資訊（針對出席者）	向出席者傳送會議邀請。	<ul style="list-style-type: none"> •%HostName% •%HostEmail% •%Topic% •%AttendeeName% •%HostName% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%MeetingNumber% •%MeetingPassword% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%
會議資訊（針對主持人）	向主持人傳送會議確認。	<ul style="list-style-type: none"> •%SiteURL% •%Topic% •%HostName% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%TeleconferencingInfo% •%SiteURL% •%Support% •%CustomFooterText% •%Year%

標題	描述	變數
PCN 會議自動提醒 — 主持人	向會議主持人傳送自動會議提醒 (僅限 PCN 帳戶)。	<ul style="list-style-type: none"> •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%SiteURL% •%Support%
PCN 會議邀請 — 受邀者	傳送會議邀請給受邀者 (僅限 PCN 帳戶)。	<ul style="list-style-type: none"> •%AttendeeName% •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%SiteURL% •%Support%

標題	描述	變數
PCN 會議手動提醒 — 主持人	向會議主持人傳送手動會議提醒 (僅限 PCN 帳戶)。	<ul style="list-style-type: none"> •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%SiteURL% •%Support%
PCN 會議手動提醒 — 受邀者	傳送手動會議提醒給受邀者 (僅限 PCN 帳戶)。	<ul style="list-style-type: none"> •%AttendeeName% •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%SiteURL% •%Support%

標題	描述	變數
PCN 會議通知 — 主持人	傳送會議通知給主持人 (僅限 PCN 帳戶)。	<ul style="list-style-type: none"> •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%SiteURL% •%Support%
PCN 會議即時邀請 — 主持人	傳送即時會議通知給主持人 (僅限 PCN 帳戶)。	<ul style="list-style-type: none"> •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%SiteURL% •%Support%

標題	描述	變數
PCN 會議進行中邀請 — 受邀者	傳送即時會議通知給受邀者（僅限 PCN 帳戶）。	<ul style="list-style-type: none"> •%AttendeeName% •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%SiteURL% •%Support%
PCN 會議排定變更 — 主持人	傳送排定變更通知給主持人（僅限 PCN 帳戶）。	<ul style="list-style-type: none"> •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%HostNumber% •%SiteURL% •%Support%

標題	描述	變數
PCN 會議排定變更 — 受邀者	傳送排定變更通知給受邀者（僅限 PCN 帳戶）。	<ul style="list-style-type: none"> •%AttendeeName% •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%SiteURL% •%Support%
PCN 會議重排 — 受邀者	傳送會議重排通知給受邀者（僅限 PCN 帳戶）。	<ul style="list-style-type: none"> •%AttendeeName% •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%TeleconferencingInfo% •%MeetingInfoURL% •%MeetingNumber% •%MeetingPassword% •%SiteURL% •%Support%

標題	描述	變數
PCN 會議取消 — 主持人	傳送會議取消通知給主持人（僅限 PCN 帳戶）。	•%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%Write% •%SiteURL%
PCN 會議取消 — 受邀者	傳送會議取消通知給受邀者（僅限 PCN 帳戶）。	•%AttendeeName% •%HostName% •%Topic% •%MeetingDateOrRecurrence% •%MeetingTime% •%TimeZone% •%Write% •%SiteURL%

設定您的下載設定

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取設定 > 下載。
- 步驟 3 選取自動更新「WebEx 生產力工具」勾選方塊，以設定定期自動更新。（預設：已勾選。）
 附註 如果計劃手動將「WebEx 生產力工具」推送至使用者，則建議您取消勾選此選項。
- 步驟 4 選取您的下載方式：
 - 允許使用者下載 WebEx 桌面應用程式
 - 手動將 WebEx Meetings 和生產力工具推送至使用者的桌面

如果您選取允許使用者下載 WebEx 桌面應用程式，您可以選取儲存完成您的下載設定。無需執行進一步動作。如果您選取手動將 WebEx Meetings 和生產力工具推送至使用者的桌面，請繼續下一步。

如果您選取手動將 WebEx Meetings 和生產力工具推送至使用者的桌面，頁面上會出現「WebEx Meetings 應用程式」、「生產力工具」及「WebEx 網路型錄製檔播放程式」區段。

- 步驟 5** 對於您要下載及安裝的每一個應用程式，選取下載並選取儲存，以將 ZIP 檔儲存至包含對應應用程式之安裝程式的系統。
每一個 ZIP 檔都包含所有受支援的語言及平台的應用程式安裝程式。
- 步驟 6** 選取儲存以儲存您的下載設定。

關於下載

在使用者具有及沒有管理員特權的 Windows PC 上，都可以使用此產品。本節提供有關下載的基本資訊。如需有關設定下載的詳細資訊，請參閱《規劃指南》的「關於下載」。

在沒有管理員特權的 PC 上：

- 建議您先將 WebEx Meetings 應用程式和「生產力工具」離線推送至最終使用者桌面，然後再通知最終使用者已為他們建立使用者帳戶。這可確保您的使用者第一次登入時，可以從其 Web 瀏覽器和 Windows 桌面開始並加入會議。
- 您可以從管理網站上的設定 > 下載頁面取得用於各個項目的 .MSI 安裝程式。如需相關資訊，請參閱[設定您的下載設定](#)，第 206 頁。
- 如果您決定不推送應用程式給您的使用者，您的使用者仍然可以從最終使用者下載頁存取這些應用程式。但是，如果其 PC 禁止安裝下載的應用程式，他們將無法完成安裝過程。
- 在使用者使用 Web 瀏覽器加入會議時（仍然可以隨選下載 WebEx Meetings 應用程式），他們可以成功加入會議。此外，WebEx Meetings 應用程式會嘗試執行安裝，以加快開始或加入未來會議的過程。這會因為其 PC 沒有管理員特權而失敗。

在具有管理員特權的 PC 上：

- 使用者可以從最終使用者下載頁下載及安裝 WebEx Meetings 應用程式和「生產力工具」。不需要管理員採取其他動作。
- 建議使用者在第一次登入時安裝「生產力工具」。
- 在使用者第一次加入會議時，會隨選下載 WebEx Meetings 應用程式，並以無訊息方式安裝在使用者的 PC 上。

管理憑證

憑證用於確保系統元件間的通訊。第一次部署系統時，使用自我簽署憑證進行設定。雖然自我簽署憑證最長可以持續五年，但我們強烈建議您設定憑證授權單位驗證的憑證。憑證授權單位可確保虛擬機器間的通訊已經過驗證。請注意，您必須為系統上的每部虛擬機器安裝一個憑證。

以下是支援的憑證類型：

- SSL — 所有系統皆需要。
- SSO IdP — 適用於具有身份識別提供者 (IdP) 憑證的 SSO。
- 安全通信會議 — TLS 通信會議需要。您可以設定最多兩個安全的通信會議憑證，您選擇設定的每個 CUCM 系統各一個。

所有系統都必須具有 SSL 憑證。此產品支援以下 SSL 憑證：

- 自我簽署
- 由憑證授權單位簽署
- 由外部憑證授權單位簽署

您無法更新憑證。如果您將虛擬機器新增至系統或變更任何現有虛擬機器，則必須為系統上的每部虛擬機器產生新憑證。

由於以下原因，SSL 憑證可能變為無效：

- 您的系統大小已擴充，因此需部署新的虛擬機器。原始 SSL 憑證中不存在這些新虛擬機器的完整網域名稱 (FQDN)。
- 已新增高可用性系統，因此需部署新的虛擬機器。原始 SSL 憑證中不存在這些新虛擬機器的 FQDN。
- Cisco WebEx 網站 URL 已變更。原始 SSL 憑證中不存在此 URL。
- 管理網站 URL 已變更。原始 SSL 憑證中不存在此 URL。
- 管理虛擬機器的 FQDN 已變更。原始 SSL 憑證中不存在此 FQDN。
- 您目前的 SSL 憑證已到期。

如果由於任何原因您的 SSL 憑證成為無效，您的系統會自動產生新的自我簽署憑證，且管理網站頁頂部的全球警告訊息會通知您此變更，指示 SSL 已成為無效。

產生 SSL 憑證

您的系統必須已設定 SSL 憑證。此產品支援以下 SSL 憑證類型：

- 自我簽署
- 由憑證授權單位簽署
- 由外部憑證授權單位簽署

產生憑證簽署請求 (CSR)

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取開啟維護模式及繼續以進行確認。
- 步驟 3** 選取設定 > 安全性 > 憑證 > 產生 CSR。
- 步驟 4** 填寫產生 CSR（憑證簽署請求）頁面上的欄位。

選項	描述
一般名稱	選取主體別名憑證或萬用字元憑證。
主體別名 附註 只有在您為「一般名稱」類型選取主體別名時，才會出現此選項。	您的管理網站和虛擬機器名稱。如果您已選取萬用字元一般名稱，則不需要主體別名。
組織	輸入您的組織名稱。
部門	輸入您的部門名稱。
縣/市	輸入城市。
省	輸入省。
國家/地區	選取您的國家/地區。
金鑰大小	從以下選項中選取您的金鑰大小： •2048 預設： 2048（建議）

- 步驟 5** 選取產生 CSR。
即會出現下載 CSR 對話方塊。
- 步驟 6** 選取下載。
您會收到一個 ZIP 檔案，其中包含 CSR 和相關聯的私密金鑰。CSR 檔案名稱爲 csr.pem，私密金鑰檔案名稱爲 csr_private_key.pem。
- 步驟 7** 使用 VMware Data Recovery (vSphere 5.0) 或 VMware vSphere Data Protection (vSphere 5.1) 備份系統。
如需相關資訊，請參閱[使用 VMware vCenter 來建立備份](#)，第 4 頁。
附註 備份系統會保留私密金鑰，以備您還原系統之用。
- 步驟 8** 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，您的系統會重新啓動。您可以在重新啓動完成後，重新登入管理網站。

匯入 SSL 憑證

您可以使用此功能來匯入 SSL 憑證。Cisco WebEx Meetings Server 支援採用 PEM 和 DER 編碼的 X.509 憑證以及 PKCS12 歸檔。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取開啟維護模式及繼續以進行確認。
- 步驟 3 選取設定 > 安全性 > 憑證 > 更多選項 > 匯入 SSL 憑證/私密金鑰。
如果您已安裝憑證，系統會警告您匯入新的憑證將覆寫已安裝的憑證。
- 步驟 4 選取繼續。
- 步驟 5 選取瀏覽，然後選擇您的憑證檔案。
您必須選擇與 X.509 相容的憑證或憑證鏈。有效類型包括：

- PEM/DER 編碼的憑證：.CER/.CRT/.PEM/.KEY
- PKCS12 加密的憑證：.P12/.PFX

您可以使用 PKCS#12 檔案或 PEM 區塊的單一檔案，來匯入憑證鏈。如果使用 PEM 檔案，它必須格式化如下：

- （選用）如果您要上傳私密金鑰，私密金鑰必須是檔案中的第一個區塊。它可以加密或取消加密。它應該是 PKCS#8 格式、PEM 編碼。如果它已加密，您必須在複雜密碼欄位中輸入密碼，以將其解密。
- 下一個元素必須是中繼憑證授權單位的憑證，該單位是以 PEM 編碼的 X.509 格式發出您的憑證。
- 您可以包括您在基礎結構中使用的所有中繼憑證。根憑證授權單位的憑證則不應包括在內。如果您使用的是私密憑證授權單位，必須確定已將根憑證分發給所有用戶端。

所有憑證都必須一起上傳在一個檔案中。您不能上傳一個憑證，稍後再新增中繼憑證。如果您使用的是採用中繼憑證的憑證授權單位，且中繼憑證未分發在其用戶端中，則您可能要上傳中繼憑證。上傳憑證將防止憑證警告。

PKCS#12 檔案必須具有 .p12 副檔名。它們應該僅包含憑證和私密金鑰（選用）。

- 步驟 6 選取上傳。
在選取上傳後，系統將判斷您的憑證是否有效。憑證可能會因為下列原因而無效：
 - 憑證檔案不是有效的憑證檔案。
 - 您選取的憑證檔案已到期。

- 您的公開金鑰必須至少為 2048 個位元。
- 憑證中的伺服器網域不符合網站 URL。
- 由系統自動產生的私密金鑰與該憑證不相容。

如果憑證有效，將繼續進行下一步。如果憑證無效，您將無法進行上傳。您必須先選取有效的憑證，然後才能繼續。

步驟 7 (選用) 在複雜密碼欄位中輸入複雜密碼。

附註 需要複雜密碼才能解密 PKCS12 歸檔或加密的私密金鑰（若已上傳含有私密金鑰的 .pem 檔案）。

步驟 8 選取繼續。

系統會匯入您的 SSL 憑證，並在可捲動的憑證檔案對話方塊中顯示該憑證。

步驟 9 選取完成。

步驟 10 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

匯出 SSL 憑證

程序

步驟 1 登入「管理」網站。

步驟 2 選取設定 > 安全性 > 憑證 > 更多選項 > 匯出 SSL 憑證。

步驟 3 儲存憑證檔案。

下一步動作

確定管理員和最終使用者都能夠登入管理頁或網頁，而不會看到任何網站不受信任的瀏覽器警告。

匯出適用於行動裝置的 SSL 憑證

執行 Apple iOS 5.0 或更新版本的 Apple iPhone 或 iPad 具有內建的授信根憑證。如果公司使用自我簽署憑證，或者 Cisco WebEx Meetings Server 上安裝的根憑證不在 Apple 授信憑證授權單位清單上，則您必須匯出 SSL 憑證並使用電子郵件將此 SSL 憑證傳送給使用者以安裝在他們的行動裝置上，然後才能加入 WebEx 會議。



附註

只有在使用自我簽署憑證時，才需要匯出 SSL 憑證。如果是使用授信憑證授權單位簽署的憑證，則不需要匯出 SSL 憑證。

開始之前

確認使用者 Apple iPhone 或 iPad 上預先安裝的授信根憑證，位於 Apple 授信憑證授權單位清單上。如需詳細資料，請參閱<http://support.apple.com/kb/ht5012>。



附註

使用者的行動裝置必須具有作用中高速網際網路連線。

程序

- 步驟 1 登入管理網站。
- 步驟 2 選取設定 > 安全性 > 憑證。
- 步驟 3 從 SSL 憑證區段複製憑證名稱。
- 步驟 4 選取更多選項 > 匯出 SSL 憑證。
- 步驟 5 將憑證檔案儲存至本端硬碟。
- 步驟 6 將儲存的憑證檔案附加到電子郵件，並將其傳送至每個使用者的 iOS 電子郵件帳戶。
- 步驟 7 使用者在行動裝置上開啓此電子郵件，並儲存檔案。
- 步驟 8 使用者在其行動裝置上安裝憑證檔案：
 - a) 點選安裝（位於安裝設定檔頁面上）。
 - b) 點選「未簽署的設定檔」對話方塊上的立即安裝。
 - c) 輸入使用者的 iOS 密碼。
 - d) 點選下一步。
 - e) 點選完成。

下載您的 CSR 和私密金鑰

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取設定 > 安全性 > 更多選項 > 下載 CSR。
即會現對話方塊，並要求您儲存檔案 CSR.zip，此檔案包含 CSR 和私密金鑰。
- 步驟 3 選取在您的系統上儲存此檔案的位置，然後選取確定。
- 步驟 4 備份您的私密金鑰檔案 csr-private-key.pem，以供您稍後需要時使用。

產生自我簽署憑證

在部署系統之後，會自動產生自我簽署憑證。我們建議您安裝由憑證授權單位簽署的憑證。您可以隨時使用此功能來產生新的自我簽署憑證。



附註

除非用戶端管理員已將其系統設定為使用自我簽署憑證，否則如果系統使用自我簽署憑證，使用者在加入會議時可能會遇到問題。

程序

步驟 1 登入「管理」網站。

步驟 2 選取開啟維護模式及繼續以進行確認。

步驟 3 選取設定 > 安全性 > 憑證 > 更多選項 > 產生自我簽署憑證。

步驟 4 完成一般自我簽署憑證頁面上的欄位。

選項	描述
憑證名稱	輸入您的自我簽署憑證的名稱。（必填）
X.509 主體名稱	您的系統的主機名稱。（不可設定）
組織	輸入您的組織名稱。
部門	輸入您的部門名稱。
縣/市	輸入您的市/縣名稱。
省	輸入您的州或省的名稱。
國家/地區	選取您的國家/地區名稱。

步驟 5 選取產生憑證和私密金鑰。

附註 如果您需要在主要升級之後使用相同的 SSL 憑證，則必須上傳載入用於取得憑證之 CSR 產生的私密金鑰。私密金鑰必須是憑證檔中的第一個區塊。即會產生並顯示您的憑證檔案。

步驟 6 選取完成。

步驟 7 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

還原 SSL 憑證

在您的憑證變成無效或在系統上執行了災害復原的事件中，您可以使用此功能還原 SSL 憑證。Cisco WebEx Meetings Server 支援採用 PEM 和 DER 編碼的 X.509 憑證以及 PKCS12 歸檔。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取開啟維護模式及繼續以進行確認。
- 步驟 3 選取設定 > 安全性 > 憑證 > 更多選項 > 匯入 SSL 憑證。
如果您已安裝憑證，系統會警告您匯入新的憑證將覆寫已安裝的憑證。
- 步驟 4 選取繼續。
- 步驟 5 選取瀏覽，然後選擇您的憑證檔案。
您必須選擇與 X.509 相容的憑證或憑證鏈。有效類型包括：

- PEM/DER 編碼的憑證：.CER/.CRT/.PEM/.KEY
- PKCS12 加密的憑證：.P12/.PFX

您可以使用 PKCS#12 檔案或 PEM 區塊的單一檔案，來匯入憑證鏈。如果使用 PEM 檔案，它必須格式化如下：

- （選用）如果您要重新套用災害復原的前一個私密/公開金鑰組，請將公開金鑰檔 (csr_private_key.pem) 與從憑證授權單位 (CA) 接收到的憑證合併至一個檔案中。私密金鑰必須是檔案中的第一個區塊，後面接著公開金鑰。它可以加密或取消加密。它應該是 PKCS#8 格式及 PEM 編碼。如果它已加密，您必須在複雜密碼欄位中輸入密碼，以將其解密。
- 下一個元素必須是中繼憑證授權單位的憑證，該單位是以 PEM 編碼的 X.509 格式發出您的憑證。
- 您可以包括您在基礎結構中使用的所有中繼憑證。根憑證授權單位的憑證則不應包括在內。如果您使用的是私密憑證授權單位，必須確定已將根憑證分發給所有用戶端。

所有憑證都必須一起上傳在一個檔案中。您不能上傳一個憑證，稍後再新增中繼憑證。如果您使用的是採用中繼憑證的憑證授權單位，且中繼憑證未分發在其用戶端中，則您可能要上傳中繼憑證。上傳憑證將防止憑證警告。

PKCS#12 檔案必須具有 .p12 副檔名。它們應該僅包含憑證和私密金鑰（選用）。

- 步驟 6 選取上傳。
在選取上傳後，系統將判斷您的憑證是否有效。憑證可能會因為下列原因而無效：
- 憑證檔案不是有效的憑證檔案。
 - 您選取的憑證檔案已到期。
 - 您的公開金鑰必須至少為 2048 個位元。
 - 憑證中的伺服器網域不符合網站 URL。

- 由系統自動產生的私密金鑰與該憑證不相容。

如果憑證有效，將繼續進行下一步。如果憑證無效，您將無法進行上傳。您必須先選取有效的憑證，然後才能繼續。

步驟 7 （選用）在**複雜密碼欄位**中輸入複雜密碼。

附註 需要有複雜密碼才能解密 PKCS12 歸檔或加密的私密金鑰（若已上傳含有私密金鑰的 .pem 檔案）。

步驟 8 選取**繼續**。

系統會匯入您的 SSL 憑證，並在可捲動的憑證檔案對話方塊中顯示該憑證。

步驟 9 選取**繼續**（位於**SSL 憑證**頁面），以完成匯入。

步驟 10 選取**完成**。

步驟 11 選取**關閉維護模式及繼續**以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

匯入 SSO IdP 憑證

程序

步驟 1 登入「管理」網站。

步驟 2 選取**設定 > 安全性 > SSO IdP 憑證**。

步驟 3 選取**瀏覽**，然後選擇您的 SSO IdP 憑證。

步驟 4 選取**上傳**。

即會顯示您的憑證檔案。

步驟 5 選取**完成**以提交您的憑證。

匯入安全通信會議憑證

只有在啟用 TLS 會議時，才需要安全通信會議憑證。如果未啟用 TLS 會議，則此選項不可用。

開始之前

只有在於音訊設定中選取 TLS 作為傳輸類型時，您的 CUCM 伺服器才需要安全通信會議憑證。如需相關資訊，請參閱[關於設定音訊設定](#)，第 172 頁。

程序

步驟 1 登入「管理」網站。

步驟 2 選取開啟維護模式及繼續以進行確認。

步驟 3 選取設定 > 安全性 > 憑證。

「安全通信會議憑證」區段會顯示以下其中一個訊息：

- 此系統不需要安全通信會議憑證，因為 TLS 通信會議未啟用。
- CUCM 安全會議憑證對於在此系統上啟用的 TLS 通信會議是必要的。

如果需要安全通信會議憑證，則會針對必須設定的每台 CUCM 伺服器顯示匯入憑證按鈕。

步驟 4 為 CUCM 1 選取匯入憑證。

即會出現安全通信會議憑證頁面。

步驟 5 輸入憑證名稱。

步驟 6 選取瀏覽，然後選擇您的憑證檔案。

附註 如果 CUCM 使用自我簽署憑證，則使用 CallManager.pem 檔。如果 CUCM 使用協力廠商憑證，則使用「根憑證授權單位(CA)」憑證。請參閱《規劃指南》中的「下載 CUCM 憑證」，以取得如何將 CUCM 憑證下載至本端硬碟的更多詳細資料。

步驟 7 選取上傳。

在選取上傳後，系統將判斷您的憑證是否有效。

如果憑證有效，將繼續進行下一步。如果憑證無效，您將無法進行上傳。您必須先選取有效的憑證，然後才能繼續。

步驟 8 選取繼續。

系統會匯入您的 SSL 憑證，並在可捲動的憑證檔案對話方塊中顯示該憑證。系統會通知您已匯入 SSL 憑證。

步驟 9 選取完成。

步驟 10 返回步驟 4，並針對 CUCM 2 伺服器重複該過程。

步驟 11 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

設定使用者階段作業安全性

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取設定 > 安全性 > 使用者階段作業。
- 步驟 3** 填寫使用者階段作業頁面上的欄位，以設定網頁到期時間。

選項	描述
網頁到期時間	設定使用者自動登出之前的天數、小時數及分鐘數。 預設： 1 小時 30 分。
行動裝置存取或生產力工具到期 (SSO)	設定使用者自動登出之前的天數、小時數及分鐘數。 預設： 14 天 附註 此欄位僅在設定 SSO 後才會出現。

- 步驟 4** 選取儲存。

配置同盟單一登入 (SSO) 設定

設定 SSO 可讓您的最終使用者使用其公司認證登入系統，因而為您提供將產品與您公司目錄整合的方法。您也可以設定 SSO，以在使用者嘗試登入時，即時建立或管理使用者帳戶。



附註

設定 SSO 可能是一項複雜的作業，我們強烈建議您在繼續之前先聯絡 Cisco 通路合作夥伴或 Cisco 進階服務。

開始之前

- 啓用同盟單一登入功能前，您必須產生一組公開金鑰和私密金鑰，以及一個包含公開金鑰的 X.509 憑證。擁有公開金鑰或憑證之後，您必須在[管理憑證](#), 第 207 頁區段中將其上傳。



附註

您啓用 SSO 後，使用者認證由您的企業驗證系統管理。特定密碼管理功能不再適用於您的使用者。如需相關資訊，請參閱[設定密碼](#), 第 179 頁和[編輯使用者](#), 第 124 頁。請注意，即使管理員也是最終使用者，他們也不會使用 SSO 登入。他們使用此產品的管理員認證來登入。

- 設定 SSO IdP 憑證，以使用此功能。如需相關資訊，請參閱[匯入 SSO IdP 憑證](#), 第 215 頁。

程序

步驟 1 登入「管理」網站。

步驟 2 選取設定 > 安全性 > 同盟 SSO。

步驟 3 您產生公開和私密金鑰及 X.509 憑證後（如先決條件中所述），選擇繼續。

步驟 4 選擇您的啟動方式：

- 由 SP（服務提供者）起始 – 使用者選擇服務提供者鏈結，並會暫時重新導向至身份識別提供者進行驗證。然後，使用者會返回他們初始請求的鏈結。
- 由 IdP（身份識別提供者）起始 – 使用者在其身份識別提供者處啟動、登入，然後重新導向至服務提供者的登入頁面。

步驟 5 填寫欄位，並在 SSO 設定頁面選取您的選項：

附註 請參閱您的 IdP 設定檔案填寫 IdP 欄位。選取 **IdP 憑證鏈結**。

欄位	描述
由 SP（服務提供者）起始	選取此選項，以便服務提供者啟動登入。
簽名的驗證請求	選取此選項要求 AuthnRequest 訊息必須由服務提供者的私密金鑰簽章。 附註 如果您想要匯出的 SAML 中繼資料檔案包含您網站的 SSL 憑證，則必須選取此選項。
目標	IdP 的 SAML 2.0 實施 URL，可接收驗證請求以進行處理。 附註 此欄位僅在選取簽名的驗證請求後才會出現。
由 idP（身份識別提供者）起始	選取此選項，以便身份識別提供者啟動登入。
目標頁面 URL 參數名稱	SSO 成功後，您的系統會重新導向至此 URL。 預設：目標 附註 在已啟動 IdP 的系統上，URL 必須是以下格式的組合 URL：您的服務登入 URL、「?」或「&」、目標頁面 URL 參數、「=」（如果未出現）及目標 URL。
SAML 簽發者（SP ID）	輸入為 IdP 設定的相同 SP ID。參考 SAML2 通訊協定。
SAML 的簽發者（IdP ID）	輸入為 IdP 設定的相同 ID。參考 SAML2 通訊協定。

欄位	描述
客戶 SSO 服務登入 URL	IdP 中 SAML2 的判斷提示消耗 URL。
NameID 格式	<p>選取您在 IdP 中設定的相同 NameID 格式。NameID 是您從 Cisco WebEx 傳送判斷提示中的使用者 ID 及單一登出請求的格式。請參閱 SAML 通訊協定作為指導。</p> <p>我們建議您將電子郵件地址設定為您的名稱 ID。這樣做對於已在系統上根據其電子郵件地址設定帳戶的最終使用者，能夠方便地使用 SSO。</p> <p>支援使用其他名稱 ID 格式，但不建議。如果使用電子郵件位址以外的格式，則當 SSO 已停用時，使用者將無法再登入 WebEx 網站。</p> <p>預設：未指定的</p>
AuthnContextClassRef	<p>輸入在 IdP 中設定的值。AuthnContextClassRef 是出現在 AuthnRequest 訊息中的值。</p> <p>預設： urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</p>
預設 WebEx 目標頁面 URL	SSO 成功後，您的系統會重新導向至此 URL。預設頁面是 Cisco WebEx 會議頁面，與一般登入頁面相同。
客戶 SSO 錯誤 URL	SSO 失敗後，您的系統會重新導向至此 URL。依預設，錯誤頁面是一般 Cisco WebEx 錯誤頁面。
單一登出	<p>此選項可啟用 SAML2 通訊協定定義的單一登出。如果您已選取 SSO 選項但未選取「單一登出」選項，則「登出」選項將不會顯示在最終使用者頁面上。</p> <p>為 ADFS 2.0 取消選取此選項。</p> <p>附註 此版本中不支援已啟動 IdP 的 SLO。</p>
客戶 SSO 服務登出 URL	在 IdP 中輸入 SAML2 的判斷提示消耗 URL。
附註 此選項僅在選取「單一登出」後才會出現。	
自動建立帳戶	沒有 Cisco WebEx 帳戶的使用者無法登入。如果您選取此選項，則當使用者試圖登入時，會自動為新使用者建立一個帳戶。

欄位	描述
自動更新帳戶	如果您選取此選項，則當 SAML2 判斷提示「updateTimeStamp」中的最新使用者資訊比 Cisco WebEx 中的目前資料多時，會更新使用者資訊。
移除 Active Directory UPN 的 UID 網域尾碼	選取此選項以驗證沒有網域尾碼的使用者。 移除 Active Directory UPN 的 UID 網域尾碼 選項在下列情況下起作用： <ul style="list-style-type: none"> •NameId 格式為電子郵件，UID 格式為 X509 主體名稱或使用主體名稱 (UPN)。 •NameId 格式為 X509 主體名稱或 UPN。

- 步驟 6** 選取啟用 SSO。
- 會顯示複查 SSO 設定頁面。複查您的設定並選取儲存。

停用 SSO

開始之前

停用 SSO 會使您的使用者無法使用其公司認證登入。請確定您已通知使用者將停用 SSO，他們仍然可以使用 Cisco WebEx 認證登入。

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取設定 > 安全性 > 同盟 SSO。
- 步驟 3** 尋找句子「如果要停用 SSO，請按一下這裡」。選取按一下這裡鏈結。
- 步驟 4** 選取停用 SSO 以確認。
- 即會出現同盟 SSO 頁，並帶有確認您已停用 SSO 的橫幅。

設定您的雲端功能

您可以設定系統，讓使用者能夠將單一版本的「Cisco WebEx 生產力工具」與他們的 Cisco WebEx Meetings Server 及 SaaS WebEx 帳戶搭配使用，或檢視 Cisco WebEx 在線上託管的訓練視訊。



附註

系統支援 Cisco WebEx SaaS 發行版 WBS27、WBS28 及 Cisco WebEx Meetings 1.2。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取設定 > 安全性 > 雲端功能。
- 步驟 3 （可選）選取允許使用者從「WebEx 生產力工具」登入 SaaS WebEx 帳戶勾選方塊。
- 步驟 4 選取儲存。

設定虛擬機器安全性

您的虛擬機器安全性功能包括更新加密金鑰的能力，以及啟用或停用符合 FIPS 標準的加密。

更新加密金鑰

Cisco WebEx Meetings Server 使用內部產生的加密金鑰，來確保您系統上虛擬機器之間的所有通訊安全。使用此功能定期更新您的加密金鑰。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取開啟維護模式及繼續以進行確認。
- 步驟 3 選取設定 > 安全性 > 虛擬機器。
- 步驟 4 選取更新加密金鑰。
- 步驟 5 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。

關於 FIPS

聯邦資訊處理標準 (FIPS) 140 是指定加密編譯模組安全需求的美國和加拿大政府標準。加密編譯模組是「一組可實作核准的安全功能（包括加密編譯演算法和金鑰產生）的硬體、軟體和/或韌體，且包含在加密編譯界限內。」加密編譯模組是要驗證的內容。

FIPS 140 需求

在很高層級，FIPS 140 需求適用於下列模組特性：

- 實作 FIPS 核准的演算法
- 金鑰生命週期的特定管理
- 核准的隨機數字產生
- 加密編譯演算法、影像完整性和隨機數字產生器 (RNG) 的自我測試

Cisco WebEx Meetings Server 使用 CiscoSSL 2.0 來實現 FIPS 140-2 第 2 層級合規性。

啟用 FIPS

啟用 FIPS 可能會導致降低與常用 Web 瀏覽器和作業系統的相容性。症狀可能包括但不限於登入系統的問題、404 錯誤及開始和加入會議。

Cisco 建議您執行下列動作：

- 確定您的 Windows PC 執行的是至少 Windows XP SP3 或更高版本。
- 無論您的使用者所需的 Web 瀏覽器是 Internet Explorer、Mozilla Firefox 還是 Google Chrome，請將所有 Windows 電腦更新至 Microsoft Internet Explorer 8 或更高版本。您的使用者必須在所有電腦上提供 Internet Explorer 8，因為啟用 FIPS 的用戶端（Cisco WebEx Meetings、生產力工具和 WebEx 錄製檔播放程式）使用僅在 Internet Explorer 8 和更高版本上提供的啟用 FIPS 的系統資料庫。
- 將所有使用者電腦上的網際網路設定都設定為 TLS 加密。在您的 PC 桌面上，選取控制台 > 網際網路選項 > 進階 > 安全性 > 使用 TLS 1.0 和使用 TLS 1.2。我們建議選取這兩個選項，以取得最大相容性，但至少必須選取使用 TLS 1.0。
- 如果您的使用者打算為訪客（例如，非貴公司員工）主持會議，您必須通知您的訪客使用者先手動更新作業系統和瀏覽器（如上所述），然後再加入您的會議。如果他們未執行上述步驟，可能會遇到相容性問題。我們建議您將上述指示包含在會議邀請中。您可以編輯您的管理網站上可用的相應會議邀請（設定 > 電子郵件 > 範本）來完成此操作。

啟用與 FIPS 相容的加密

使用此功能可啟用與聯邦資訊處理標準 (FIPS) 相容的加密設定。

程序

-
- 步驟 1** 登入「管理」網站。
 - 步驟 2** 選取開啟維護模式及繼續以進行確認。
 - 步驟 3** 選取設定 > 安全性 > 虛擬機器。
 - 步驟 4** 選取啟用以啟用與 FIPS 相容的加密，然後選取繼續以進行確認。
您系統上即已設定與 FIPS 相容的加密。
 - 步驟 5** 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。
-

停用與 FIPS 相容的加密

使用此功能可在您系統上停用與聯邦資訊處理標準 (FIPS) 相容的加密。

程序

- 步驟 1 登入「管理」網站。
 - 步驟 2 選取開啟維護模式及繼續以進行確認。
 - 步驟 3 選取設定 > 安全性 > 虛擬機器。
 - 步驟 4 選取停用以停用與 FIPS 相容的加密，然後選取繼續以進行確認。
您系統上即已停用與 FIPS 相容的加密。
 - 步驟 5 選取關閉維護模式及繼續以進行確認。
在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。
-



第 15 章

管理報告

您可以檢視每月報告，以及針對特定的日期範圍自訂報告。報告使用您公司資訊頁面上設定的語言、地區設定及時區設定。如需相關資訊，請參閱[設定您的公司資訊](#)，第 168 頁。



附註

當您的系統全新部署或最近升級後，在第一個月結束之前，沒有資料可用於「自訂詳細資訊報告」以外的任何報告。在該情況下，本節所述的下載鏈結及所有其他報告，要到第一個月結束後才可使用。

- [下載每月報告](#)，第 225 頁
- [關於每月報告](#)，第 225 頁
- [產生自訂詳細資訊報告](#)，第 227 頁
- [關於自訂詳細資訊報告](#)，第 227 頁

下載每月報告

您可以透過此頁面檢視並下載每月摘要報告。報告是以 PDF 格式顯示。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取報告。
- 步驟 3 選取您要檢視的每月報告的下載鏈結。

關於每月報告

您的「每月摘要報告」包含下列區段：

系統摘要報告

您的「系統摘要報告」包含下列報告：

- 服務採用 — 此報告顯示一個圖，描繪前三個月的唯一主持人和出席者數目，及後三個月的預期增長率。
- 使用者授權 — 此報告顯示您所使用的已購授權百分比，及描繪前三個月使用的授權數目和後三個月的預期增長率的圖。您可以使用這些數目來預測將來的授權使用量，並據以調整您如何購買授權。如需相關資訊，請參閱[透過使用 License Manager 來履行授權](#), 第 164 頁。
- 系統大小 — 此報告顯示您的會議參加者尖峰值，及尖峰值使用的系統大小的百分比。該圖描繪前三個月的會議參加者尖峰值，及後三個月的預期增長率。
- 儲存空間 — 此報告顯示您的資料歸檔及錄製檔的儲存空間使用率，兩者都是以佔總體儲存空間的百分比及總計 GB 表示。該圖描繪前三個月的儲存空間總計，及後三個月的預期增長率。使用此報告可監視您的儲存空間使用情形。如果需要新增額外的儲存空間，則必須將現有儲存空間資料歸檔和錄製檔手動複製到新的儲存伺服器，然後才能啟動。



附註 只有在您設定儲存伺服器後，才會出現此報告。如需相關資訊，請參閱[設定儲存伺服器](#), 第 148 頁。

- 網路 — 此報告顯示下列內容：

您的網路頻寬消耗尖峰值 (Mbps)。

該圖描繪前三個月的網路頻寬消耗尖峰值 (Mbps)，及後三個月的預期增長率 (紅線指示網路頻寬上限)。

圓餅圖指示每個系統資源所消耗的頻寬的百分比。

- 系統計劃的停機時間和計劃外的中斷 — 此報告顯示下列內容：

- 前三個月的系統平均正常運行時間。
- 前三個月的計劃外系統中斷的平均時間。
- 前三個月由於系統中斷導致的會議中斷的平均次數。
- 該圖描繪前三個月的計劃停機時間和計劃外的中斷，及後三個月的預期增長率。



附註 停機時間增加有時反映出使用率增加。請務必必要將您的停機時間統計資料與其他報告中顯示的使用率統計資料相比較。

會議摘要報告

您的「會議摘要報告」包含下列報告：

- 會議狀態 — 此報告顯示的圖描繪上個月的會議狀態、遭遇問題的會議的百分比，及一個月內舉辦的會議總數。如需即時會議狀態，請參閱您的儀表板。如需相關資訊，請參閱[關於儀表板](#)，第 103 頁。
- 會議大小 — 此報告顯示的圖描繪了過去一個月您系統上所舉辦的會議的規模、會議大小的明細，及一個月內舉辦的最大規模會議的相關詳細資訊。
- 會議功能的使用狀況 — 此報告顯示下列內容：
 - 過去一個月使用次數最多的功能，包括使用功能的總計分鐘數。
 - 過去一個月您系統上使用率增長最快的功能，包括增長率。
 - 該圖描繪了您系統上每個功能的使用率 (以分鐘為單位)。
 - 該圖描繪了您系統上使用率增長最快的功能的增長率。
- 使用量最多的參加者電子郵件網域 — 此報告顯示下列內容：
 - 該圖描繪了使用量最多的參加者電子郵件網域。
 - 參加者電子郵件網域的明細。
 - 您系統上會議參加者使用最多的前三個電子郵件網域的清單。
- 尖峰時間（天和時段） — 此報告顯示兩個圖。第一個圖描繪了過去一個月每週最繁忙的一天。第二個圖描繪了過去一個月您系統上每天最忙的時間。

產生自訂詳細資訊報告

程序

-
- 步驟 1** 登入「管理」網站。
 - 步驟 2** 選取報告 > 自訂您的報告。
 - 步驟 3** 選取您想要檢視的報告的日期範圍，然後選取**提交**。
預設為最近的月份。您可以選取最長可往後延長六個月的日期範圍。

自訂報告請求已提交頁面會出現，其中顯示您的自訂報告的日期。您會收到一封電子郵件，其中含有 CSV 格式的自訂報告的鏈結。
 - 步驟 4** 選取完成。
-

關於自訂詳細資訊報告

當您產生自訂詳細資訊報告時，會收到一個包含歸檔的電子郵件，該歸檔包含 CSV 格式的下列報告：

•**欺詐企圖報告** — 此報告顯示所有失敗的電話存取企圖，在這些情況下呼叫者嘗試開始或加入個人會議時三次輸入錯誤的主持人或參加者存取碼或主持人 PIN 碼。這個報告包括下列欄位：

- 呼叫的存取碼** — 開始或加入個人會議時撥入的 Cisco WebEx 撥入號碼。
- 呼叫號碼** — 用於呼叫的電話號碼。
- 呼叫的開始時間** — 呼叫的日期與時間。
- 第一個嘗試的存取碼** — 呼叫者輸入的第一個無效存取碼。
- 第一個存取碼擁有者的電子郵件（如有）** — 如果第一個無效存取碼關聯有效的 Cisco WebEx Meetings Server 帳戶，則為與該存取碼關聯的使用者的電子郵件地址。
- 第二個嘗試的存取碼** — 呼叫者輸入的第二個無效存取碼。
- 第二個存取碼擁有者的電子郵件（如有）** — 如果第二個無效存取碼關聯有效的 Cisco WebEx Meetings Server 帳戶，則為與該存取碼關聯的使用者的電子郵件地址。
- 第三個嘗試的存取碼** — 呼叫者輸入的第三個無效存取碼。
- 第三個存取碼擁有者的電子郵件（如有）** — 如果第三個無效存取碼關聯有效的 Cisco WebEx Meetings Server 帳戶，則為與該存取碼關聯的使用者的電子郵件地址。

•**會議報告** — 此報告包含指定時段內進行的所有會議的相關資訊，並包含下列欄位：

- 會議 ID** — 排定會議時，系統產生的唯一會議 ID。
- 會議號** — Cisco WebEx Meetings 會議號。
- 主旨** — 主持人設定的會議名稱。
- 主持人姓名** — 會議的主持人。
- 開始時間** — 會議的開始日期與時間。
- 持續時間** — 會議的持續時間 (以分鐘為單位)。
- 參加者人數** — 包括主持人在內的參加者的人數。
- 狀態**
- 撥入音訊分鐘數**
- 回撥音訊分鐘數**
- VoIP 分鐘數**
- 視訊分鐘數**
- 錄製分鐘數**
- 錄製間隔** — 為會議期間建立的每個錄製檔指定開始時間和停止時間。
- Web 共用分鐘數** — 網路會議中所有參加者花費的分鐘數總計（例如，如果有三個參加者出席時長為 10 分鐘的會議的網路會議部分，則 Web 共用分鐘數為 30）。
- 參加者** — 會議的參加者清單。

- 主機平台/瀏覽器 — 主持人開始 Cisco WebEx 會議時，主機所使用的作業系統及瀏覽器版本。
- 主機 IP 位址 — 主持人開始 Cisco WebEx 會議時，主機所使用的 IP 位址。
- 追蹤碼 — 主持人排定會議時套用的追蹤碼。
- 網路頻寬使用量報告 — 此報告包含針對下列每個功能，在指定時段內每一天的網路頻寬消耗量清單：
 - 音訊最大消耗頻寬 (mbps)
 - 音訊 VoIP 最大消耗頻寬 (mbps)
 - 視訊最大消耗頻寬 (mbps)
 - Web 共用最大消耗頻寬 (mbps)

消耗量為 0 (零) 是指該日未使用此功能。如果指定日期的消耗量小於 1 Mbps，則顯示消耗量小於 1。

視訊的網路頻寬消耗量包括來自相機的視訊和網路會議共用的視訊檔案。如果您的網站已停用視訊，則您無法開啓相機接收視訊，但仍可共用視訊檔案。這將導致報告中包含的一些視訊對網路頻寬的消耗。對某網站停用視訊後，這是導致視訊消耗網路頻寬的唯一狀況。

- 儲存容量使用量報告 — 此報告顯示截至所列日期的已用磁碟空間總計，及每日進行的錄製會議數。



附註 只有在您設定儲存伺服器後，才會包含此報告。如需相關資訊，請參閱[設定儲存伺服器](#)。

- 參加者報告 — 此報告顯示會議歷史記錄、每個會議的開始時間及對每個會議套用的追蹤碼。
 - 會議 ID — 排定會議時，系統產生的唯一會議 ID。
 - 會議名稱 — 排定會議時，主持人在內容欄位中輸入的會議名稱。
 - 使用者名稱 — 主持人的使用者名稱。
 - 加入時間 — 使用者加入 Cisco WebEx 會議時的時間和日期。
 - 離開時間 — 使用者離開 Cisco WebEx 會議時的時間和日期。
 - 持續時間 — 使用者參加 Cisco WebEx 會議的時間量 (分鐘)。
 - 平台/瀏覽器 — 主持人開始 Cisco WebEx 會議時，主機所使用的作業系統及瀏覽器版本。
 - 用戶端 IP 位址 — 主持人或參加者用來開始或出席 Cisco WebEx 會議的 WebEx 用戶端 IP 位址。
 - 階段作業開始時間 — 階段作業的開始時間。
 - 階段作業結束時間 — 階段作業的結束時間。

階段作業的類型 — 階段作業類型可以是視訊（Web 共用）、VoIP（電話連線）、撥入或回撥。

階段作業持續時間 — 階段作業持續的時間長度。

電話號碼 — 用來呼叫 WebEx 會議的電話號碼。

電話 伺服器 — 電話伺服器。

•系統停機時間報告 — 此報告包含指定時段的系統停機時間資訊，並包括下列欄位：

類別 — 停止服務或維護。停止服務是指服務中斷。維護是指已計劃的維護時段。

服務 — 列出受影響的功能。

停機開始時間 — 開始停機的日期與時間。

停機結束時間 — 結束停機的日期與時間。

被中斷的會議數 — 列出被中斷的會議數目。對於「維護」停機時間，該欄位為空白，因為維護時間已事先計劃。如果在「無法服務」停機時段內未排定任何會議，則該數目為 0。

•使用者授權使用量報告 — 此報告有兩個版本。一個版本顯示過去 30 天的授權使用量，標題為 UserLicenseUtilizationReportForLastMonth.csv；另一個版本顯示當月（從本月第一天至今）的授權使用量，標題為 UserLicenseUtilizationForThisMonth.csv。這些報告分別都包含下列欄位：

使用者名稱 — 會議主持人的使用者名稱。

電子郵件地址 — 會議主持人的電子郵件地址。

會議 ID — 排定會議時，系統產生的唯一會議 ID。

會議號 — Cisco WebEx Meetings 會議號。

開始時間 — 開始會議的日期與時間。

同時進行的會議 — 相同使用者排定的同時進行的會議的數目。錄製的每一個同時進行的會議都會為排定該會議的使用者產生一個附加行，新增至此報告。



第 16 章

使用支援功能

- [自訂您的日誌, 第 231 頁](#)
- [設定遠端支援帳戶, 第 232 頁](#)
- [停用遠端支援帳戶, 第 233 頁](#)
- [使用會議測試, 第 234 頁](#)
- [使用系統資源測試, 第 234 頁](#)

自訂您的日誌

您可以產生日誌檔，日誌檔會顯示整個系統或特定會議的活動。使用日誌檔可排解問題，或在需要協助時將日誌檔提交至 Cisco 技術協助中心 (TAC)。



附註

建議您在非工作時間產生日誌檔。日誌檔案較大，可能影響系統效能。



附註

日誌資料會保留 30 天。但是，如果將 Cisco WebEx Meetings Server 1.x 版部署升級至 2.0 版，則 1.x 版中的日誌資料將不會傳送至 Cisco WebEx Meetings Server 2.0 系統，並因此在完成升級至 2.0 版後無法使用。

程序

- 步驟 1** 登入「管理」網站。
- 步驟 2** 選取支援 > 日誌。
- 步驟 3** 填寫自訂您的日誌頁面上的欄位，然後選取提交。

欄位	描述
(可選) 案例 ID	輸入您的 Cisco TAC 案例 ID。在 Cisco TAC 協助您處理案例時，可從 Cisco TAC 取得案例 ID。使用此功能可讓您將產生的日誌與案例 ID 關聯。
類型	選取日誌類型。您可以選取 整體系統日誌 或 特定會議日誌 。「整體系統日誌」包含系統的所有指定日誌資訊，「特定會議日誌」則會從資料庫中收集日誌及資料以進行 MATS 處理。 預設： 整體系統日誌
範圍	選取您的日誌的範圍。您必須為您的日誌指定開始和結束的日期與時間。限制為 24 小時。僅提供過去 30 天的日誌資料。 附註 若要產生超過 24 小時的日誌，您必須透過選取連續的日期時間範圍重複執行此作業。每個作業將建立一個獨立的日誌檔案。例如：若要產生從 1 月 1 日到 1 月 3 日的日誌，請先選取 1 月 1 日到 1 月 2 日作為日期範圍，選取 提交 並下載建立的日誌檔。然後，選取 1 月 2 日到 1 月 3 日作為日期範圍。選取 提交 並下載建立的日誌檔案。
包括	指定要包含在日誌中的資料。 預設： 所有活動

系統會產生日誌並向您傳送一封電子郵件，其中含有可下載日誌的鏈結。

設定遠端支援帳戶

如果您遇到技術問題需要聯絡 Cisco TAC 以尋求協助，您可以設定遠端支援帳戶，以授予 TAC 代表暫時存取您系統的權限。由於此產品未對管理員提供 CLI 存取權，因此需要 TAC 代表對一些問題進行疑難排解。

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取支援 > 遠端支援帳戶。
- 步驟 3 選取啟用遠端支援。
- 步驟 4 填寫遠端支援帳戶頁面上的欄位，然後選取建立帳戶。

欄位	描述
遠端支援帳戶名稱	輸入遠端支援帳戶的名稱（6 – 30 個字元）。
帳戶生命週期	指定帳戶的持續時間（小時）。最長時間為 720 小時（30 天）。
解碼器版本	選取 2 - Webex 會議伺服器 。 附註 如果您具有發佈 Cisco WebEx Meetings Server 1.5 版之前作用的遠端支援帳戶，則不必配置此設定。

此時會出現建立遠端支援帳戶對話方塊，並顯示您的通行碼。請聯絡 Cisco TAC 並提供遠端支援帳戶名稱和通行碼，以允許 Cisco 支援人員存取系統。

停用遠端支援帳戶

程序

- 步驟 1 登入「管理」網站。
- 步驟 2 選取支援 > 遠端支援帳戶。
- 步驟 3 在狀態訊息「遠端支援已啟用」旁，選取停用它鏈結。
您的遠端支援帳戶即已停用。

使用會議測試

程序

步驟 1 登入「管理」網站。

步驟 2 選取支援 > 會議測試。

步驟 3 選取下一步。

您的系統即會執行會議測試，並驗證其排定、開始及加入會議的能力。測試的結果會在數分鐘內出現。

使用系統資源測試

程序

步驟 1 登入「管理」網站。

步驟 2 選取開啟維護模式及繼續以進行確認。

步驟 3 選取支援 > 系統資源測試。

步驟 4 選取下一步。

系統會公佈以下幾項的測試結果：

- 系統上每個主機的 CPU、記憶體、網路及儲存空間
- 您的網站和管理 URL 的內部和外部連線檢查。

步驟 5 選取關閉維護模式及繼續以進行確認。

在關閉維護模式後，您的系統會重新啟動。您可以在重新啟動完成後，重新登入管理網站。
