將ECE與PCCE整合到12.0及更高版本中

目錄

簡介

本檔案介紹將企業版聊天與電子郵件(ECE)與12.0及更高版本中的套裝客服中心企業版(PCCE)整合的步驟

必要條件

需求

思科建議您瞭解以下主題：

- 企業版聊天與電子郵件(ECE)12.x
- 套裝客服中心企業版(PCCE)12.x

採用元件

本檔案中的資訊是根據以下軟體版本：

- 歐洲經委會12.5(1)
- PCCE 12.5(1)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

PCCE版本12.0引入了新的管理介面，稱為單一管理平台(SPOG)。現在，幾乎所有聯絡中心和相關應用程式的管理都在此介面中執行。為了正確整合ECE和PCCE，您必須完成此整合獨有的幾個步驟。本文檔將指導您完成此過程。

技術

在本文檔中，將使用這些術語。

- 企業版聊天與電子郵件(ECE)- ECE產品允許以與語音呼叫相同的方式將電子郵件和聊天請求路由到聯絡中心座席。
- 單一窗格(SPOG)- SPOG是12.0版及更高版本中完成PCCE管理的方式。SPOG是對在12.0之前的版本中使用的CCE管理工具的完整重寫。
- 證書頒發機構(CA) — 根據公開金鑰基礎架構(PKI)模型頒發數位證書的實體。

  您可以遇到兩種型別的CA。

  - 公共CA — 公共CA是大多數瀏覽器和作業系統都包含其根證書和中間證書的CA。一些常見的公共CA包括IdenTrust、DigiCert、GoDaddy和GlobalSign。
  - 專用CA — 專用CA是公司內部存在的專用CA。某些私有CA由公有CA簽署，但大多數情況下，這些私有CA是獨立CA，且它們頒發的憑證僅受該組織中的電腦信任。

  在這兩種CA型別中的任一種中，都有兩種型別的CA伺服器。

  - 根CA伺服器 — 根CA伺服器簽署自己的證書。在標準的多層PKI部署中，根CA處於離線狀態且無法訪問。此模型中的根CA也只向另一個稱為中間CA的CA伺服器頒發證書。有些公司選擇僅使用單層CA。在此模型中，根CA會頒發供另一個CA伺服器之外的實體使用的證書。
  - 中間CA伺服器 — 中間CA伺服器或發佈CA伺服器頒發供其他CA伺服器之外的實體使用的證書。
- Microsoft管理控制檯(MMC)- Microsoft Windows附帶的一個應用程式，允許載入各種管理單元。您可以使用管理單元構建用於伺服器管理的自定義控制檯。Windows中包括許多不同的管

理單元。示例的簡短清單包括Certificates 、 Device Manager 、 Disk Management 、 Event Viewer和Services。

- 網路負載均衡器(NLB) — 向終端使用者提供具有公共物理名稱的多個物理資源的裝置或應用程式。NLB在Web應用程式和服務中非常常見。NLB可以多種方式實施。當與ECE一起使用時，NLB的配置方式必須確保使用者會話使用cookie-insert或等效方法返回到同一物理後端Web伺服器。這稱為使用cookie-insert的粘滯會話。粘滯會話只是指負載均衡器將使用者會話返回到同一物理後端伺服器進行所有互動的能力。
    - 安全套接字層(SSL)直通 — SSL直通是在終端使用者裝置和分配使用者會話的物理Web伺服器之間存在SSL會話的一種方法。SSL傳輸不允許cookie插入，因為HTTP會話始終以物理方式加密。大多數NLB通過使用粘滯表支援使用SSL Passthrough的粘滯會話，粘滯表用於監視會話設定的伺服器呼叫和客戶端呼叫部分，並將唯一值儲存在表中。當向NLB提交匹配這些值的下一個請求時，可以使用stick表將會話返回到同一後端伺服器。
    - SSL解除安裝 — 當為SSL解除安裝配置NLB時，任何給定終端使用者會話都存在兩個SSL會話或隧道。第一個介於終端使用者裝置和在NLB上為網站配置的虛擬IP(VIP)之間。第二個地址位於NLB的後端IP與分配使用者會話的物理Web伺服器之間。SSL解除安裝支援Cookie插入，因為HTTP流已完全解密，而在NLB上可以插入其他HTTP cookie並執行會話檢查。當Web應用程式不需要SSL而是出於安全考慮，通常使用SSL解除安裝。ECE的當前版本不支援在非SSL會話中訪問應用程式。

前提步驟

開始整合這兩個系統之前，必須完成幾個前提條件。

- 最低PCCE修補程式級別
    - 版本12.0(1)- ES37
    - 版本12.5(1) — 目前沒有基本功能的最低要求
- ECE最低補丁級別

  建議ECE運行最新的工程特別計畫(ES)。

    - 版本12.0(1)- ES3 + ES3_ET1a
    - 版本12.5(1) — 目前沒有基本功能的最低要求
- 配置專案

  確保將ECE_Email、ECE_Chat和ECE_Outbound Media Routing Domains(MRD)與正確的應用程式例項相關聯。

    - 對於PCCE 2000代理部署模型，應用例項為MultiChannel，並且在部署PCCE時進行了預配置。
    - 對於PCCE 4000/12000代理部署模型，應用程式例項可以是任意名稱，必須由執行整合的人員建立。最佳實踐是使用{site}_{peripheral_set}_{application_instance}的形式。如果您安裝的PCCE的站點名稱是Main，外圍裝置設定為PS1，應用例項設定為Multichannel，則應用例項名稱為Main_PS1_Multichannel。

注意：應用程式例項名稱區分大小寫。將ECE Web伺服器新增到清單時，請確保正確鍵

入名稱。

整合步驟

本檔案所有步驟的細節在歐洲經委會和太平洋經濟合作委員會的檔案中都有論述，但它們既沒有列入清單，也沒有列入同一檔案。如需其他詳細資訊，請參閱本文結尾包含的連結。

步驟 1.配置SSL證書

必須生成證書供ECE Web伺服器使用。您可以使用自簽名證書，但使用CA簽名證書通常更為容易。自簽名證書的安全性不亞於CA簽名的證書，初始建立證書的步驟較少，但是當需要替換證書時，必須記住將新證書上載到所有PCCE管理資料伺服器上的Java金鑰庫。如果使用CA簽名的證書，則只需將根證書和中間證書（如果存在）上傳到金鑰庫。

如果部署中有多個Web伺服器，則必須檢視這些准則。配置網路負載均衡器所需的具體步驟不屬於本文檔的範圍。如有需要，請與您的負載平衡器供應商聯絡以獲得幫助。

- 雖然不需要，但負載均衡器可大大簡化實施
- 無論使用哪種負載均衡器方法，訪問每個Web伺服器上的ECE應用程式都必須使用SSL
- 負載均衡器可以配置為SSL傳遞或SSL解除安裝
- 如果選擇SSL直通：
    - 您必須從一個伺服器執行所有證書操作
    - 正確配置證書後，必須匯出證書並確保將私鑰包含在個人資訊交換(PFX)檔案中
    - 您必須將PFX檔案複製到部署中的所有其他Web伺服器，然後將證書匯入IIS
- 如果選擇SSL解除安裝，則可以使用各自的SSL證書配置每個Web伺服器

註：如果您有多台Web伺服器並選擇Web伺服器上的SSL直通，或者如果您希望所有伺服器上都有一個公用證書，則必須選擇一台Web伺服器執行上的步驟1，然後將證書匯入到所有其他Web伺服器。
如果選擇SSL解除安裝，則必須在所有Web伺服器上執行這些步驟。您還必須生成要在負載平衡器上使用的證書。

步驟 1.1.生成證書

如果您已建立或獲取證書，則可以跳過此部分，否則請選擇以下兩個選項之一。

選項 1.使用自簽名證書

1. 導航到IIS管理。
2. 在左側的「連線」樹中選擇伺服器名稱。
3. 在中心窗格中找到Server Certificates，然後按兩下將其開啟。
4. 從右側的Actions窗格中選擇Create Self-Signed Certificate...。

5. 在「Create Self-Signed Certificate」視窗中，在「Specify a friendly name for the certificate:」框中選擇並輸入名稱。此名稱是憑證在下一個主要步驟中的選取流程中出現的方式。此名稱無需與證書的公用名稱匹配，也不影響證書對終端使用者的顯示方式。
6. 確保在Select a certificate store for the new certificate: 下拉框中選擇了Personal。
7. 選擇OK以建立證書。
8. 請繼續執行下一個主要步驟「將證書繫結到網站」。

選項 2.使用CA簽名的證書

CA簽署的憑證要求您產生憑證簽署請求(CSR)。CSR是文字檔案，會傳送到已簽署其CA的CA，然後傳回已簽署的憑證以及所需的CA憑證，且CSR已履行。您可以選擇通過IIS管理或通過Microsoft管理控制檯(MMC)執行此操作。IIS Administration（IIS管理）方法非常簡單，不需要特殊知識，但僅允許您配置包括在證書的Subject（主題）屬性中的欄位並更改位長度。MMC需要執行其他步驟，並且您對有效CSR中所需的全部欄位具有透徹的瞭解。強烈建議您僅在建立和管理證書方面具備中等到專業經驗時才使用MMC。如果您的部署要求使用多個完全限定名稱來訪問ECE，或者如果您需要更改證書的任何部分（主題和位長度除外），則必須使用MMC方法。

1. 通過IIS管理

   使用以下步驟通過IIS管理器生成證書簽名請求(CSR)。

   1. 導航到IIS管理。
   2. 在左側的「連線」樹中選擇伺服器名稱。
   3. 在中心窗格中找到Server Certificates，然後按兩下將其開啟。
   4. 從右側的Actions窗格中選擇Create Certificate Request...。系統將顯示Request Certificate嚮導。
   5. 在「Distinguished Name Properties」頁面上，在表格中輸入系統的值。必須輸入所有欄位。選擇Next繼續。
   6. 在「加密服務提供程式屬性」頁上，保留加密服務提供程式的預設選擇：。將「Bit length:(位長度：)」下拉選單更改為最小為2048。選擇Next繼續。
   7. 在「File Name」頁面上，選擇要儲存CSR檔案的位置。
   8. 向CA提供檔案。收到已簽名的證書後，將其複製到Web伺服器並繼續下一步。
   9. 在IIS管理器的同一位置，在「操作」窗格中選擇「完成證書請求」。此時將顯示嚮導。
   10. 在「Specify Certificate Authority Response」頁面上，選擇您的CA提供的證書。在友好名稱框中指定名稱。此名稱是憑證在下一個主要步驟中的選取流程中出現的方式。確保「Select a certificate store for the new certificate:」下拉選單已設定為「Personal」。
   11. 選擇OK以完成證書上傳。
   12. 請繼續執行下一個主要步驟「將證書繫結到網站」。
2. 通過Microsoft管理控制檯(MMC)

   使用以下步驟通過MMC生成CSR。此方法允許您自訂CSR的每一方面。

   1. 按一下右鍵「Start（開始）」按鈕，然後選擇「Run（運行）」。
   2. 在運行框中鍵入mmc，然後選擇OK。
   3. 將證書管理單元新增到MMC視窗。
      1. 依次選擇檔案和新增/刪除管理單元……將出現新增或刪除管理單框。

2. 在左側清單中，找到Certificates，然後選擇Add >。此時會顯示「證書」管理單元框。
3. 選擇Computer account選項，然後選擇Next >。
4. 確保在「Select Computer（選擇電腦）」頁面上選擇「Local computer：（此控制檯所在的電腦）」(Local computer:(此電腦位於此控制檯上)，然後選擇「Finish」(完成)。
5. 選擇OK以關閉新增或刪除管理單元框。

4. 產生CSR
    1. 在左窗格中，依次展開證書（本地電腦）和個人，然後選擇證書資料夾。
    2. 按一下右鍵Certificates資料夾並導航到All Tasks > Advanced Operations >，然後選擇Create Custom Request...。系統將顯示Certificate Enrollment嚮導。
    3. 在簡介螢幕中選擇Next。
    4. 在Select Certificate Enrollment Policy頁面上，選擇Proceed without enrollment policy(在Custom Request下列出)，然後選擇Next。
    5. 在Custom request頁面上，確保所選Template是(No template)CNG鍵，並且Request format適合您的CA。PKCS #10可與Microsoft CA配合使用。選擇Next以進入下一頁。
    6. 在「Certificate Information」頁面上，選擇「Details」字詞旁邊的下拉選單，然後選擇「Properties」按鈕。系統將顯示Certificate Properties窗體。
    7. 提供「憑證屬性」表單的所有選項，這超出了本文件的范圍。有關詳細資訊，請參考Microsoft文檔。以下是關於此表單的一些備註和提示。
        - 確保在Subject：頁籤的Subject name：部分中填寫所有必需值
        - 確保在Alternative name：一節中還提供了為Common name提供的值
        - 將Type:設定為DNS，在Value:框中鍵入URL，然後選擇Add >按鈕
        - 如果您要使用多個URL訪問ECE，請在此同一欄位中提供每個備用名稱，並在每個備用名稱后選擇Add >
        - 請確保將Private Key頁籤上的Key size設定為大於1024的值。
        - 如果您計畫匯出要在多個Web伺服器上使用的證書（通常在HA安裝中完成），請確保選擇Make private key exportable。如果未能執行此操作，將導致無法在以後匯出證書
        - 您輸入的值和所做的選擇不會被驗證。必須確保提供所有所需的資訊，否則CA無法完成CSR
    8. 選擇所有選項後，OK返回嚮導。選擇Next以進入下一頁。
    9. 在要將離線請求儲存到何處？頁面上，選擇您能夠訪問的位置中的檔名。對於大多數CA，必須選擇Base 64作為格式。
    10. 向您的CA提供檔案。在他們簽名並將證書返回給您後，將證書複製到Web伺服器並繼續執行最後步驟。
    11. 在MMC的證書管理管理單元中，導航到證書（本地電腦）> Personal，按一下右鍵Certificates，然後選擇All Tasks > Import...。系統將顯示Certificate Import Wizard。
    12. 在介紹性螢幕上選擇Next。
    13. 在「File to import」螢幕上，選擇您的CA已簽名的證書，然後選擇Next。
    14. 確保選擇將所有證書放入以下儲存。
    15. 確保在Certificate store:框中選擇了Personal，然後選擇Next。
    16. 檢視最終螢幕，然後選擇完成完成匯入。
    17. 關閉MMC控制檯。如果系統提示您儲存主控台設定，請選擇否。這不會影響憑證

匯入。

18. 請繼續執行下一個主要步驟「將證書繫結到網站」。

步驟 1.2.將證書繫結到網站

⚠ 注意：必須確保主機名欄位留空，並且在「編輯站點繫結」框中未選擇「需要伺服器名稱指示」選項。如果其中任何一項已配置，則SPOG在嘗試與ECE通訊時失敗。

1. 開啟Internet Information Services(IIS)管理器（如果您以前沒有這樣做）。
2. 在左側的Connections窗格中，導航到Sites，然後選擇Default Web Site。

   如果選擇使用預設網站以外的網站名稱，請確保選擇正確的網站名稱。

3. 從右側的操作窗格中選擇Bindings...。出現Site Bindings框。
   1. 如果沒有具有Type、https和Port、443的行，請完成以下操作。否則，請繼續執行下一個主要步驟。
      1. 選擇Add...按鈕，將顯示Add Site Binding框。
      2. 在「Type:」下拉選單中選擇https。
      3. 確保IP address:下拉選單顯示All Unassigned，且Port:欄位為443。
      4. 確保將Host name：欄位留空，並取消選擇Require Server Name Indication選項。
      5. 在「SSL certificate:」下拉清單中，選擇與先前所建立的憑證名稱相對應的憑證名稱。
         - 如果您不確定要選擇哪個證書，請使用選擇……按鈕檢視和搜尋伺服器上存在的證書
         - 使用View...按鈕檢視所選證書並驗證詳細資訊是否正確
      6. 選擇OK以儲存您的選擇。
   2. 選擇在「型別」列中顯示https的行，然後選擇「編輯……」按鈕。出現Edit Site Binding框。
      1. 確保IP address:下拉選單顯示All Unassigned，且Port:欄位為443。
      2. 確保Host name：欄位留空，並且未選擇Require Server Name Indication選項。
      3. 在「SSL certificate:」下拉清單中，選擇與先前所建立的憑證名稱相對應的憑證名稱。
         - 如果您不確定要選擇哪個證書，請使用選擇……按鈕檢視和搜尋伺服器上存在的證書
         - 使用View...按鈕檢視所選證書並驗證詳細資訊是否正確
      4. 選擇OK以儲存您的選擇。
   3. 選擇Close以返回到IIS管理器。
4. 關閉IIS管理器。

步驟 2.配置分割槽管理員SSO

分割槽管理員SSO配置允許ECE為在SPOG中開啟ECE小工具的管理員自動建立分割槽級別使用者帳戶。

✎ 注意：即使不計畫啟用代理或主管SSO，也必須配置分割槽管理員SSO。

步驟 2.1.獲取Active Directory(AD)證書並建立金鑰庫。

可能需要執行此步驟才能解決Microsoft最近宣佈的安全更改。如果未應用更新且未對域進行更改，則可以跳過此過程。

有關詳細資訊，請參閱Microsoft KB4520412詳細資訊。

1. 從您在「分割槽管理員配置」表單中提供的AD伺服器獲取Base 64格式的SSL證書。這裡展示了一種方法。
    1. 使用工作站從OpenSSL下載並安裝用於Windows的OpenSSL副本。Light版已經足夠了。
    2. 啟動OpenSSL命令提示符。
    3. 運行此命令。將伺服器名稱替換為全域性編錄域控制器的完全限定名稱。
       openssl s_client -connect gcdcsrv01.example.local:3269
    4. 在輸出中，找到伺服器證書行。

```
C:openssl s_client -connect 14.10.162.6:3269
CONNECTED(00000003)
depth=1 DC = com, DC = massivedynamic, CN = MassiveDynamic Enterprise CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:
   i:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
 1 s:/DC=com/DC=massivedynamic/CN=MassiveDynamic Enterprise CA
   i:/C=US/OU=pki.uclabservices.com/O=Cisco Systems Inc/CN=UCLAB Services Root
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIH1DCCBbygAwIBAgITJwAAAAbAAn/HKFuWCQAAAAAABjANBgkqhkiG9w0BAQsF
ADBcMRMwEQYKCZImiZPyLGQBGRYDY29tMR4wHAYKCZImiZPyLGQBGRYObWFzc2l2
ZWR5bmFtaWMxJTAjBgNVBAMTHE1hc3NpdmVEeW5hbWljIEVudGVycHJpc2UgQ0Ew
HhcNMjAwNDE1MDAxNDM0WhcNMjEwNDE1MDAxNDM0WjAAMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAxFajhqjrWqQHfqTXg+SXP5pzvNVrTHIigrAam8DO
```

    5. 將輸出從「BEGIN CERTIFICATE」-----開始-----複製到「-----END CERTIFICATE-----」。確保包括BEGIN CERTIFICATE和END CERTIFICATE行。
    6. 將複製的資訊貼上到新的文本檔案中，然後將其以crt副檔名儲存到電腦。
2. 將證書檔案複製到其中一個應用程式伺服器。
3. 開啟與複製證書的應用程式伺服器的RDP會話。
4. 建立新的Java金鑰庫。
    1. 在應用伺服器上開啟命令提示符。
    2. 轉到ECE Java Development Kit(JDK)bin目錄。
    3. 運行此命令。根據需要替換這些值。
       keytool -import -trustcacerts -alias mydomaincontroller -file C:\temp\domainctl.crt -keystore c:\ece\pcce\mydomain.jks -storepass MyP@ssword
5. 在12.6之前的版本中，將金鑰庫複製到環境中所有其他應用程式伺服器上的同一路徑。在12.6版中，將金鑰庫複製到您配置ECE的工作站可訪問的位置。

步驟 2.2.使用AD輕型目錄訪問協定(LDAP)訪問資訊配置ECE。

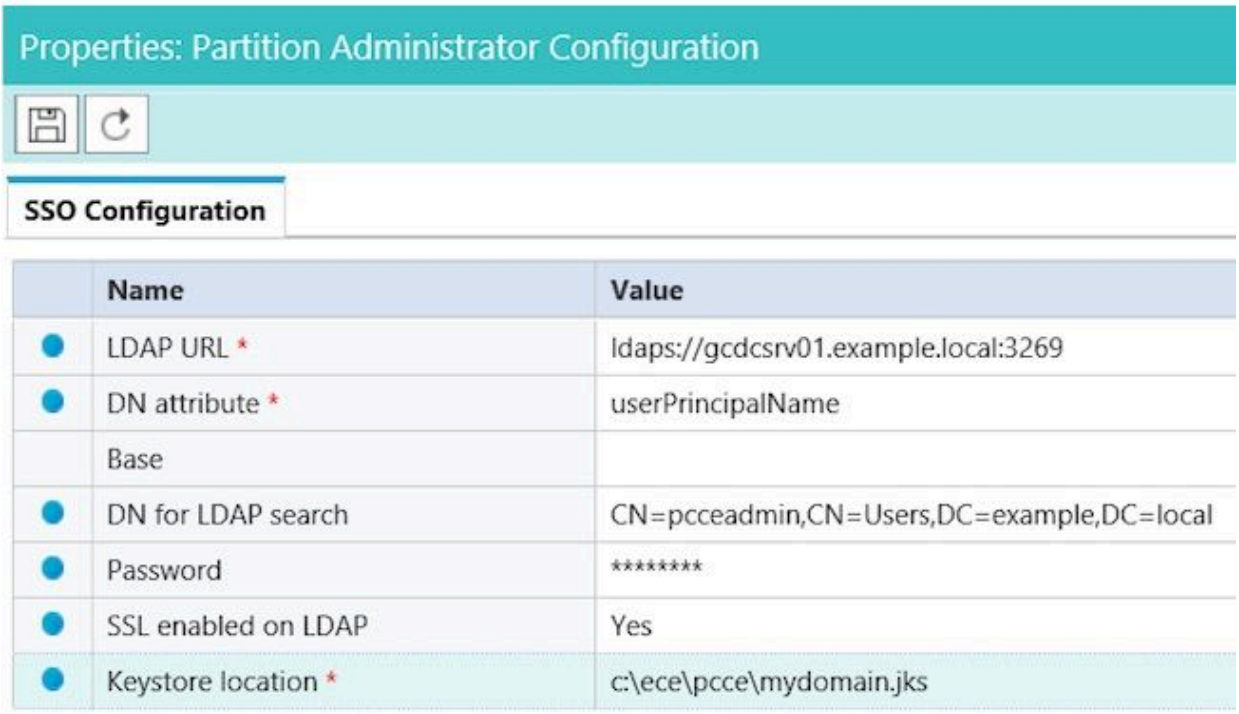
1. 從使用Internet Explorer 11的工作站或電腦上，導航到業務分割槽URL。

> 提示：業務分割槽也稱為分割槽1。對於大多數安裝，可通過 https://ece.example.com/default類似的URL訪問業務分割槽。

2. 以pa身份登入，並提供系統的密碼。
3. 成功登入後，在初始控制檯上選擇Administration連結。
4. 導航到SSO Configuration資料夾，Administration > Partition: default > Security > SSO and Provisioning。
5. 在右側的頂部窗格中，選擇Partition Administration Configuration條目。
6. 在右側的底部窗格中，輸入輕量級目錄訪問協定(LDAP)和AD的值。
    1. LDAP URL — 作為最佳實踐，請使用全域性編錄(GC)域控制器的名稱。
       如果不使用GC，則在ApplicationServer日誌中會看到錯誤，如下所示。
       LDAP身份驗證<@>中存在異常
       javax.naming.PartialResultException：未處理的繼續引用；剩餘名稱「
       DC=example，DC=com」
        - 非安全全域性目錄埠為3268
        - 安全全域性目錄埠為3269
    2. DN屬性 — 必須為userPrincipalName。
    3. Base — 如果使用GC，則不需要此過程，否則必須提供基本正確的LDAP格式。
    4. 用於LDAP搜尋的DN — 除非您的域允許匿名繫結，否則您必須提供能夠繫結到LDAP並搜尋目錄樹的使用者的可分辨名稱。

    > 提示：為使用者找到正確值的最簡單方法是使用Active Directory使用者和電腦工具。以下步驟顯示如何查詢此值。

        1. 從View選單中選擇Advanced Features選項。
        2. 導航到使用者對象，然後按一下右鍵並選擇屬性。
        3. 選擇屬性頁籤。
        4. 選擇Filter按鈕，然後選擇Only show attributes with values。
        5. 在清單中查詢distinquishedName，然後按兩下以檢視值。
        6. 突出顯示顯示的值，然後將其複製並貼上到文本編輯器。
        7. 將文本檔案中的值複製並貼上到DN for LDAP搜尋字段中。
           該值必須類似，CN=pcceadmin、CN=Users、DC=example、DC=local
    5. Password — 提供指定使用者的密碼。
    6. 在LDAP上啟用SSL — 對於大多數客戶來說，此欄位可視為必填欄位。
    7. 金鑰庫位置 — 這必須是從AD匯入SSL證書的金鑰庫位置。在本例中，這是c:\ece\pcce\mydomain.jks，如下圖所示：



7. 選擇磁片的圖示以儲存更改。

步驟 3.驗證配置檔案

對於所有12.0安裝，必須完成本部分。對於12.0以外的任何版本，都可以跳過此部分。
對於所有版本，可能還需要執行此步驟的兩個其他方案。第一種是將ECE安裝在高可用性設定中時。第二種情況（也更常見）是Web伺服器的主機名與用於訪問ECE的名稱不匹配。例如，如果您在主機名為UCSVRECEWEB.example.com的伺服器上安裝ECE Web伺服器，但使用者使用URL chat.example.com訪問ECE網頁，則必須完成此部分。如果伺服器主機名與用於訪問ECE的URL相同，並且安裝了版本12.5或更高版本，則可以跳過此步驟並完成部分。

將{ECE_HOME}替換為已安裝ECE的物理位置。例如，如果已在C:\Cisco安裝ECE，則在每個位置將{ECE_HOME}替換為C:\Cisco。

提示：使用記事本等文本編輯器++而不是記事本或寫字板，因為這些文本編輯器無法正確解釋行尾。

---

1. 開啟與部署中的所有ECE Web伺服器的遠端案頭會話。
2. 導航到此路徑:{ECE_HOME}\eService\templates\finesse\gadget\spog。
3. 找到spog_config.jsfile，並在安全位置製作備份副本。
4. 在文本編輯器中，開啟當前的spog_config.jsfile。
5. 找到這兩個行並更新它們以匹配您的部署。
   web_server_protocol必須是https，如果需要，請更新。
   更新web_server_name以匹配您分配用於訪問ECE的完全限定名稱。示例：
   ece.example.com
   - var web_server_protocol = "https";
   - var web_server_name = "ece.example.com";
6. 儲存更改。
7. 在部署中的所有其他Web伺服器上重複上述操作。

步驟 4.將ECE新增到PCCE清單

自12.0起，PCCE有3種不同的部署選項：2000座席（2K座席）、4000座席（4K座席）和12000座席（12K座席）。這三個部署選項可分為兩個組：2K Agent和4K/12K Agent。它們以這種方式分開，因為它們在SPOG中的外觀存在一些根本的差異。在這段之後，對這兩種方法進行非常高級別的比較。本文檔未提供向清單新增元件的特定步驟。請參閱本文檔末尾的連結，瞭解此流程的具體詳細資訊。本部分介紹在將ECE新增到PCCE時必須驗證的特定詳細資訊。本文檔還假定您的PCCE安裝已完成，並且您可以訪問和配置解決方案的其他方面。

- 2K代理部署
  - PCCE元件的初始配置完全通過CCE管理完成，並且是自動的
  - 新元件通過彈出框新增到資產頁面中，您可以在其中輸入詳細資訊（如IP或主機名以及任何必要的憑證或元件特定配置）
- 4K和12K代理部署
  - 大部分初始配置都反映了用於UCCE的步驟
  - 元件通過從CCE管理下載的逗號分隔值(CSV)檔案新增，按照您的特定安裝進行填充，然後上傳
  - 初始部署要求將某些特定元件包括在第一個CSV檔案中
  - 最初設定系統時未新增的元件將通過包含所需資訊的CSV檔案新增

步驟 4.1.將ECE Web伺服器證書上傳到Java金鑰庫

1. 如果使用自簽名證書
   1. 開啟與主A端管理資料伺服器(ADS)的遠端案頭連線。
   2. 以管理員身份開啟Internet Explorer 11並導航到ECE業務分割槽。
   3. 選擇URL欄右側的掛鎖圖示，然後選擇View Certificates。
   4. 在Certificate框中，選擇Details頁籤。
   5. 選擇靠近頁籤底部的Copy to File...。
   6. 在「Certificate Export Wizard」中，選擇「Next」，直到進入「Export File Format」頁面。確保選擇Base-64 encoded X.509(.CER)格式。
   7. 將證書儲存到ADS伺服器上c:\Temp\certificates等位置以完成匯出。
   8. 將證書複製到所有其他ADS伺服器。
   9. 開啟管理命令提示符。
   10. 轉到Java主目錄，然後轉到bin目錄。可以使用以下方法訪問Java主目錄。 cd %JAVA_HOME%\bin
   11. 備份當前的cacerts檔案。將cacerts檔案從%JAVA_HOME%\lib\security複製到其他位置。
   12. 運行此命令以匯入之前儲存的證書。如果您的金鑰庫密碼不是「changeit」，請更新命令以匹配您的安裝。
       keytool -keystore ../lib/security/cacerts -storepass changeit -import -alias <ECE伺服器的FQDN> -file <儲存證書的位置>
   13. 重新啟動ADS伺服器。
   14. 在其他ADS伺服器上重複步驟8-12。
2. 如果使用CA簽名的證書
   1. 獲取DER/PEM格式的根證書和中間證書，並將它們複製到所有ADS伺服器上的C:\Temp\certificates位置。

> 注意：請與您的CA管理員聯絡以獲取這些證書。

2. 開啟與主A端ADS的遠端案頭連線。
3. 開啟管理命令提示符。
4. 轉到Java主目錄，然後轉到bin目錄。可以使用以下方法訪問Java主目錄。 cd %JAVA_HOME%\bin
5. 備份當前的cacerts檔案。將cacerts檔案從%JAVA_HOME%\lib\security複製到其他位置。
6. 運行此命令以匯入之前儲存的證書。如果您的金鑰庫密碼不是「changeit」，請更新命令以匹配您的安裝。
   keytool -keystore ../lib/security/cacerts -storepass changeit -trustcacerts -import -alias <CA根的名稱> -file <儲存根證書的位置>
7. 重複步驟6。並匯入中間證書（如果存在）。
8. 重新啟動ADS伺服器。
9. 在所有其他ADS伺服器上重複步驟2-12。

步驟 4.2.將ECE資料伺服器新增到庫存

- 雖然資料伺服器必須存在於系統清單中，但是PCCE ADS和資料伺服器之間不會進行直接通訊
- 在1500代理部署中部署ECE時，資料伺服器是服務伺服器
- 在HA配置中安裝ECE時，僅新增A端服務伺服器

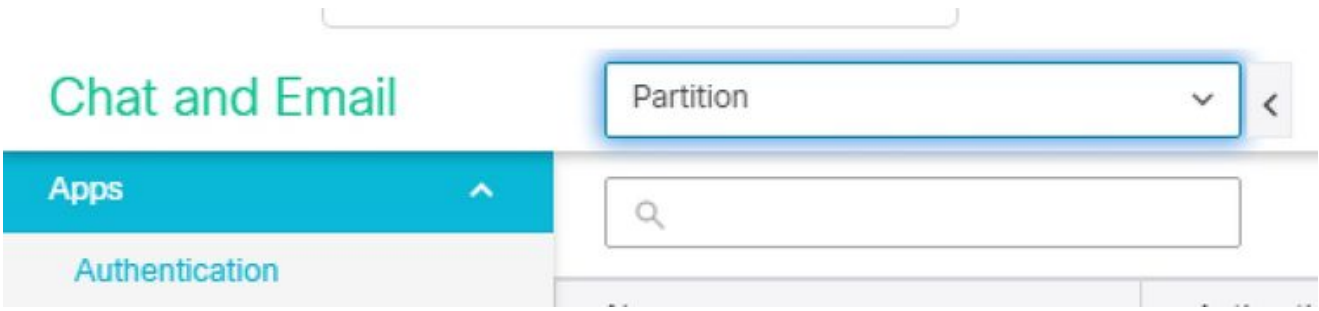
步驟 4.3.將ECE Web伺服器新增到清單

- 確保使用完全限定名稱新增Web伺服器
  - 此名稱必須與ECE證書中的公用名稱匹配，或者必須列為主題備用名稱(SAN)之一
  - 不能僅使用主機名或IP地址
- ECE的使用者名稱和密碼必須為pa登入憑據
- 確保應用程式例項正確
  - 應用程式例項名稱區分大小寫
  - 對於2000座席PCCE部署，應用例項為MultiChannel
  - 對於4000/12000代理PCCE部署，應用例項包含站點和外設集作為名稱的一部分
- 當ECE安裝有多個Web伺服器時，例如在1500代理部署或400代理HA部署中，您可以使用指向負載平衡器的URL或指向每個單個Web伺服器的URL作為Web伺服器的完全限定名稱。最佳實踐是使用負載均衡器。
- 如果您有多個ECE部署，或者如果您選擇在部署中新增多個單獨的Web伺服器，則在SPOG中開啟ECE小工具時，您只需選擇正確的Web伺服器。

步驟 5.將ECE與PCCE整合

1. 以管理員身份登入到CCE Administration。
2. 選擇Email and Chat卡，然後選擇Email and Chat連結，如下圖所示。

3. 在Device Name下拉選單中檢視當前選定的伺服器。如果在HA安裝中新增了兩個Web伺服器，則可以選擇其中一個Web伺服器。如果以後向系統中新增第二個ECE部署，請確保在繼續之前選擇適當的伺服器。
4. 在Chat and Email旁邊的下拉中，選擇Partition或Global，如下圖所示。



5. 在頂部選單中，選擇Integration，然後選擇Unified CCE旁邊的箭頭，然後選擇第二個Unified CCE，如下圖所示。

6. 填充安裝的AWDB Details頁籤中的值，然後選擇Save按鈕。
7. 選擇Configuration頁籤，然後按如下方式完成此操作。
    1. 選擇Application Instance旁邊的下拉選單，然後選擇為ECE建立的應用程式例項。

> 註：這不能是以UQ開頭的應用程式例項。

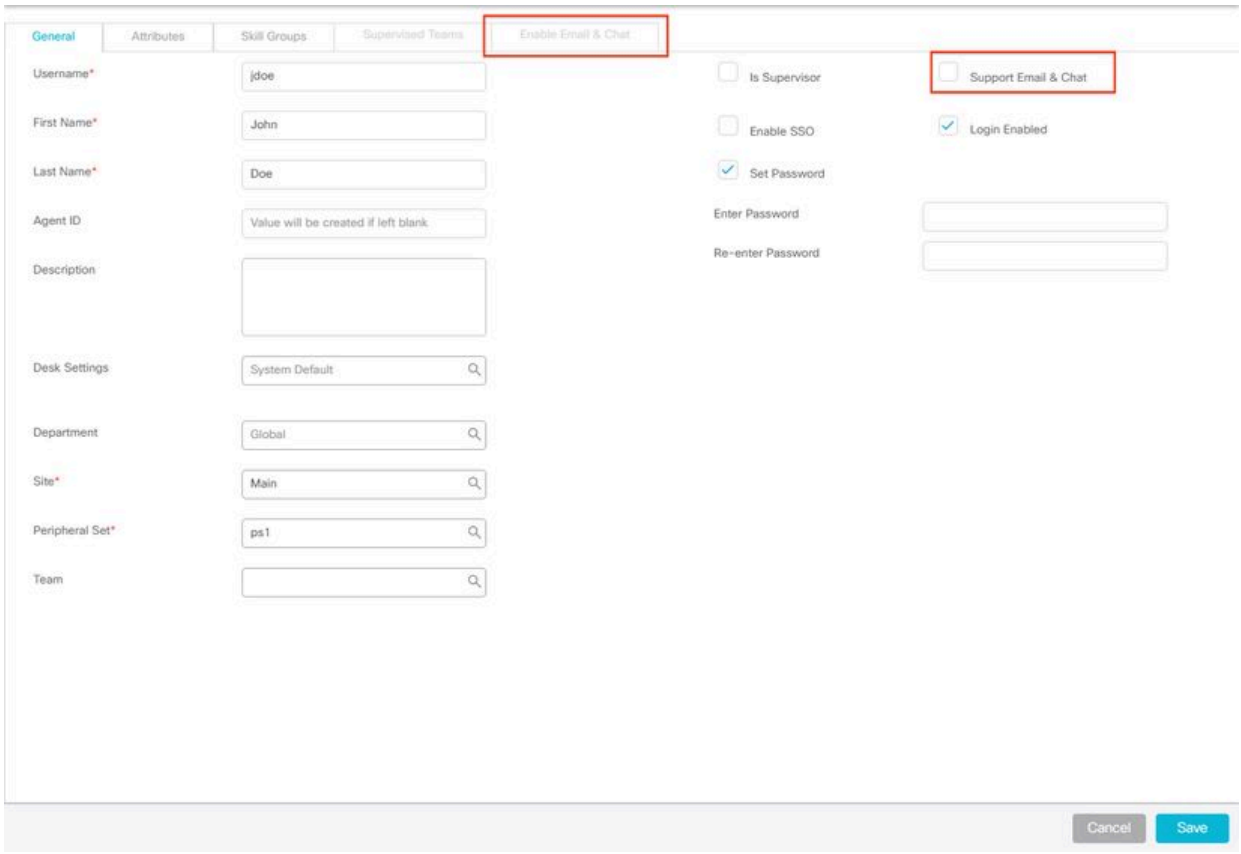
    2. 選擇帶白色加號的綠色圓圈按鈕，選擇Agent PG。
        1. 選擇座席PG（如果座席的PG不止一個）。
        2. 新增所有Agent PG後，選擇Save。

> 警告：選擇Save後，系統將永久連線到PCCE，並且無法撤消。如果本節中出錯，則必須完全解除安裝ECE並刪除所有資料庫，然後像全新安裝一樣安裝ECE。

步驟 6.驗證ECE整合

1. 在CCE管理中，檢查頂部狀態列中是否未顯示警報。 如果有警報，請選擇警報一詞並檢視「清單」頁，以確保沒有適用於ECE伺服器的警報。
2. 在左側導航欄中選擇Users，然後選擇Agents。

3. 從清單中選擇一個代理並驗證這一點。
    1. 現在，您可以在General頁籤上看到Support Email & Chat的新覈取方塊。
    2. 現在，您可以看到標有Enable Email & Chat的新索引標籤，如下圖所示。



4. 啟用ECE測試代理。
    1. 選中Support Email & Chat覈取方塊，並注意Enable Email & Chat頁籤現在可選中。
    2. 選擇Enable Email & Chat頁籤，並在Screen Name欄位中提供值。
    3. 選擇Save以更新使用者。
    4. 您會收到一條成功消息。
5. 驗證ECE是否已更新。
    1. 選擇Overview導航按鈕，然後選擇Email and Chat卡和連結。
    2. 在Chat and Email旁邊的下拉選單中，選擇與座席部門對應的名稱。

> 註:ECE中的服務部門儲存屬於PCCE中的全區域性門的所有對象。因此，部門名稱Service是保留值。

    1. 在頂部選單中，選擇User Management，然後在Chat and Email下的選單中選擇Users。
    2. 驗證您是否在清單中看到新代理。

疑難排解

建議您下載多個工具，並將其保留在ECE伺服器上。隨著時間的推移，這些功能使解決方案的故障排除和維護變得更為簡單。

- 文本編輯器，如記事本++

- 存檔工具，如7-Zip
- 眾多Tail for Windows程式之一
  下面是一些示例：
  - 赤尾
  - Win32的尾部

為了排除整合問題，您必須首先瞭解一些關鍵日誌檔案和每個日誌檔案的位置。

1. ECE上的檔名和位置

ECE系統上有許多日誌，當您嘗試解決整合問題時這些日誌非常有用。

日誌檔案	伺服器	名稱慣例	說明
應用伺服器	C/A	eg_log_{HOSTNAME}_ApplicationServer.log	來自Wildfly伺服器的日誌
外部代理分配	客戶/伺服器	eg_log_{HOSTNAME}_EAAS-process.log	與MR PG的互動
外部代理消息	客戶/伺服器	eg_log_{HOSTNAME}_EAMS-process.log	與CTI伺服器的互動
根日誌	抄送/抄送/抄送	egpl_root_{HOSTNAME}.log	進程間日誌、HazelCast、常規錯誤
元件狀態	抄送/抄送/抄送	eg_log_{HOSTNAME}_component-status.log	進程開始和檔案複製完成
進程啟動器	抄送/抄送	eg_log_{HOSTNAME}_ProcessLauncher.log	服務和進程啟動的一般日誌

	/抄送		
分散式服務管理員	客戶/伺服器	eg_log_{HOSTNAME}_DSMController.log	在Services伺服器上顯示進程啟動和停止的日誌

伺服器金鑰：

- C =並置伺服器
- A =應用程式伺服器
- S =服務伺服器
- M =郵件伺服器

大多數日誌檔案還有另外兩個與其關聯的日誌。

- eg_log_{SERVERNAME}_{PROCESS}.log — 主進程日誌
- eg_log_dal_connpool_{SERVERNAME}_{PROCESS}.log — 連線池使用情況
- eg_log_query_timeout_{SERVERNAME}_{PROCESS}.log — 查詢因超時而失敗時更新

2. PCCE上的檔名和位置

有關整合問題的PCCE日誌全部位於A側ADS。以下是排除整合問題時最重要的日誌。這些產品均位於C:\icm\tomcat\logs。

日誌檔案	名稱慣例	說明
CCBU	CCBU.{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	CCE Admin和所有相關Web應用程式的主日誌
CCBU錯誤	錯誤。{YYYY}-{MM}-{DD}T{hh}-{mm}-{ss}.{msec}.startup.log	CCE管理員和相關的Web應用程式看到的錯誤
卡塔利納	catalina.{YYYY}-{MM}-{DD}.log	Tomcat本機日誌，顯示證書錯誤
Tomcat stdout	tomcat9-stdout.{YYYY}-{MM}-{DD}.log	來自Tomcat的標準輸出日誌消息
Tomcat stderr	tomcat9-stderr.{YYYY}-{MM}-{DD}.log	來自Tomcat的標準錯誤日誌消息

在這些日誌中，前三個最常被請求和檢視。

使用以下步驟設定跟蹤級別並收集所需的日誌。

3. 跟蹤級別配置

本節僅適用於ECE。PCCE所需的日誌的跟蹤級別由思科設定，無法更改。

1. 從使用Internet Explorer 11的工作站或電腦上，導航到系統分割槽URL。

> 提示：系統分割槽也稱為分割槽0。對於大多數安裝，可以通過類似 https://ece.example.com/system的URL訪問系統分割槽

2. 以sa身份登入，並提供系統的密碼。
3. 成功登入後，在初始控制檯上選擇System連結。
4. 在「系統」頁面中，展開System > Shared Resources > Logger > Processes。
5. 在右上方的窗格中，找到要更改跟蹤級別的進程並選擇它。
   注意：在HA系統和具有多台應用伺服器的系統中，進程會多次列出。為確保捕獲資料，請為包含進程的所有伺服器設定跟蹤級別。
6. 在右下方的窗格中，選擇Maximum trace level下拉選單並選擇適當的值。
   ECE中定義了8個跟蹤級別。本清單中的4個為最常用的。
   - 2 — 錯誤 — 進程的預設跟蹤級別
   - 4 — 資訊 — 通常用於問題解決的跟蹤級別
   - 6 - Dbquery — 通常有助於在設定早期診斷問題或更複雜的問題
   - 7 — 調試 — 非常詳細的輸出，僅在最複雜的問題中需要

> 注意：請勿在6 - Dbquery或更高的時間內保留任何進程，通常只在TAC指導下保留。

   保持大多數進程跟蹤級別，2 — 錯誤。如果選擇級別7或8，還必須選擇最長持續時間。當達到最大持續時間時，跟蹤級別將返回到上一個級別集。
   設定系統後，將這四個進程更改為跟蹤級別4。

   - EAAS流程
   - EAMS流程
   - dx進程
   - rx-process
7. 選擇儲存圖示以設定新的跟蹤級別。

4. 日誌檔案收集

1. 開啟與需要進程日誌的伺服器的遠端案頭會話。
2. 導航到日誌檔案位置。
   1. ECE伺服器

      日誌的寫入方式如下。

- 預設情況下，日誌是最大大小為5MB的已寫入檔案
- 當一個日誌檔案達到配置的最大值時，將以{LOGNAME}.log.{#}格式重新命名該檔案
- ECE保留以前的49個日誌檔案加上當前檔案
- 當前日誌始終以.log結尾，且後面沒有數字
- 日誌既不存檔也不壓縮
- 大多數日誌具有公共結構
- 日誌檔案使用<@>分隔各個部分
- 日誌始終以GMT+0000時間寫入

根據特定安裝，ECE日誌位於不同位置。

1. 400代理部署
    1. 單面
        - 伺服器：並置伺服器
        - 位置: {ECE_HOME}\eService_RT\logs
    2. 高可用性
        - 伺服器：兩個並置的伺服器
        - 位置: {ECE_HOME}\eService\logs
        - 為分散式檔案系統(DFS)共用建立的目錄僅包含用於安裝和升級的日誌。
        - 只有擁有分散式系統管理器(DSM)角色的伺服器才能寫入屬於服務角色的元件的日誌
            - 可以在Windows工作管理員的「進程」頁籤上找到DSM角色所有者。此伺服器上有10-15個Java進程不在輔助伺服器上。
            - DSM下的元件包括EAAS、EAMS、Retriever、Dispatcher、Workflow等。
    2. 1500代理部署
        - 位於承載角色的伺服器上的日誌
        - 位置: {ECE_HOME}\eService\logs
        - 除服務伺服器外，所有伺服器都運行並寫入與該元件關聯的所有進程的日誌
        - 在高可用性部署中，服務伺服器以主用/備用配置運行
        - 只有擁有分散式系統管理器(DSM)角色的伺服器才能寫入日誌
        - DSM角色所有者可以通過Windows工作管理員中可見的進程數來標識。主伺服器上有10-15個Java進程，輔助伺服器上只有4個Java進程
2. PCCE伺服器
    - 來自PCCE的所需日誌位於C:\icm\tomcat\logs
    - Tomcat日誌不會被回滾或存檔
    - 日誌以本地伺服器時間寫入
3. 收集發現問題後建立或修改的所有日誌。

對日誌和所發現問題的完整說明不在本檔案的範圍之內。下面是一些常見問題、要檢查的內容以及一些可能的解決方案。

- 憑證相關問題
    - 未匯入證書

        - 行為：當您嘗試在SPOG中開啟ECE小工具時，會看到錯誤「載入頁面時出錯。請聯絡管理員。」
        - 檢查：Catalina在PCCE上記錄類似以下錯誤 javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX路徑生成失敗：sun.security.provider.certpath.SunCertPathBuilderException：無法找到指向請求目標的有效證書路徑
        - 解決方案：確保您已將ECE Web伺服器證書或適當的CA證書匯入到ADS上的金鑰庫中
    - 證書不匹配
        - 行為：當您嘗試在SPOG中開啟ECE小工具時，您會看到一個錯誤，表明證書的公用名或使用者替代名稱與配置的名稱不匹配。
        - 檢查：驗證SSL證書
        - 解析：確保主題中的「公用名」欄位或主題替代名稱中的一個DNS欄位包含您在SPOG中輸入的完全限定名稱作為Web伺服器名稱。
- 系統問題
    - 服務未啟動
        - 行為：當您嘗試在SPOG中開啟ECE小工具時，您會看到錯誤：「https://{url}上的網頁可能暫時關閉，或者它可能已永久移動到新地址。」
        - 檢查：確認除Web伺服器外，所有ECE伺服器上均啟動了Windows服務 — Cisco服務。檢視應用程式伺服器上的根日誌是否有錯誤
        - 解決方案：啟動所有ECE服務的思科服務。
- 組態問題
    - LDAP配置
        - 行為：當您嘗試在SPOG中開啟ECE小工具時，會看到錯誤「載入頁面時出錯。請聯絡管理員。」
        - 檢查：將應用程式伺服器的跟蹤級別提高到級別7 — 調試，然後再次嘗試登入並檢視應用程式伺服器日誌。搜尋LDAP一詞。
        - 解決方案：驗證分割槽管理員SSO的LDAP配置以確保其正確。

相關資訊

在開始任何ECE安裝或整合之前，您必須仔細閱讀這些關鍵文檔。這不是一份全面的歐洲經委會檔案清單。

⚠ 注意：大多數歐洲經委會檔案有兩個版本。請確保下載並使用適用於PCCE的版本。文檔標題在版本號之後為Packaged Contact Center Enterprise或（對於PCCE）或（對於UCCE和PCCE）。

在進行任何安裝、升級或整合之前，請務必檢視思科企業版聊天與電子郵件文檔的起始頁以瞭解任何更新。

https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-

email/series.html

- 12.0
  - 企業版聊天與電子郵件安裝及設定指南
  - 企業版聊天與電子郵件升級指南
  - 企業版聊天與電子郵件管理員指南
- 12.5
  - 企業版聊天與電子郵件安裝及設定指南
  - 企業版聊天與電子郵件升級指南
  - 企業版聊天與電子郵件管理員指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。