郵箱自動修復功能13.0 AsyncOS及更高版本：本地交換、混合多租戶和鏈結查詢

目錄

簡介

本文介紹新增的郵箱自動補救(MAR)功能，該功能是為用於郵件安全的AsyncOS 13.0引入的。

必要條件

- 適用於ESA的AsyncOS 13.0或更高版本
- 用於檔案信譽和檔案分析的許可證金鑰
- MS Office365或MS Exchange現場實施

背景資訊

MAR是在AsyncOS 10.0中引入的，僅支援Office 365 Online。

13.0及更高版本的AsyncOS功能：

- Microsoft Exchange Online — 託管在Microsoft Office 365上的郵箱
- Microsoft Exchange內部部署 — 本地Microsoft Exchange伺服器
- 混合/多租戶配置 — 跨Microsoft Exchange Online和Microsoft Exchange內部部署配置的郵箱組合

初始設定步驟可以在O365的原始MAR設定指南中找到，同時還可以在13.0及更新版本的O365的更改附錄中找到。

原始文章仍然有效，包含對該功能的說明以及為O365 Azure實施、ESA設定和常規故障排除生成證書的步驟。

如何為ESA配置Azure AD和Office 365郵箱設定

對13.0的Azure side API許可權的新更改

當前的使用手冊提供了自動修正功能的更多詳細資訊。

章節：自動修正郵箱中的郵件

配置多個「帳戶配置檔案」。

ESA 13.0和更新版本支援使用Exchange Online、Exchange內部部署或同時使用這兩種工具建立多個帳戶配置檔案：

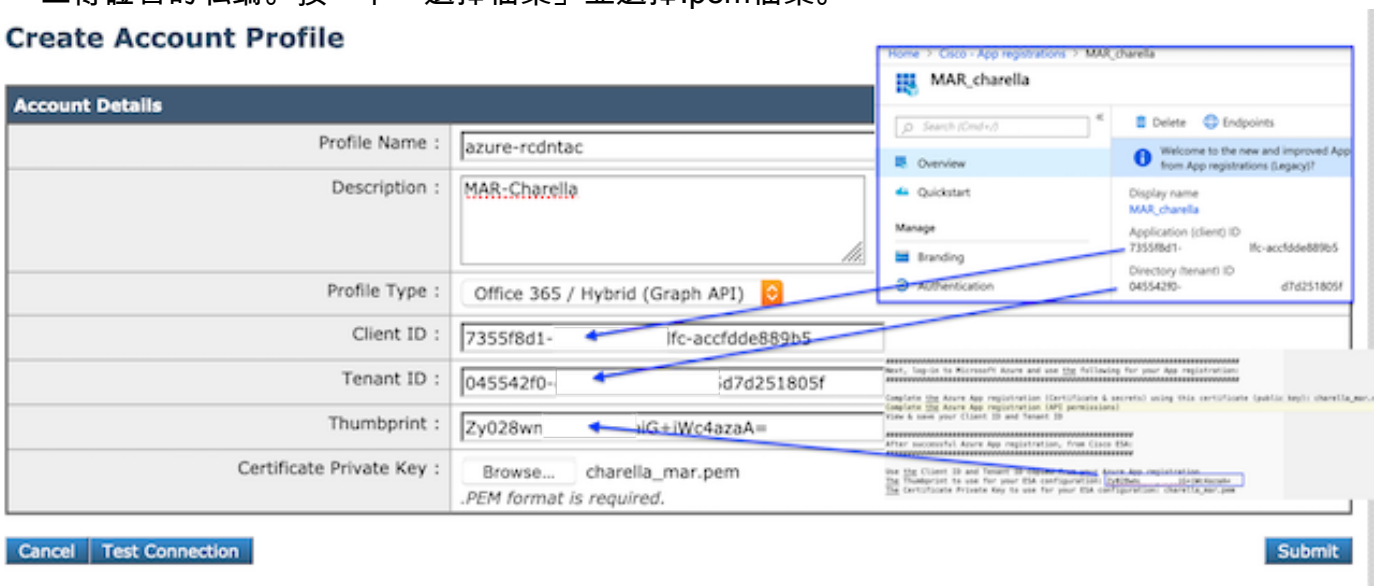
- 如果您的公司包括複雜的設定，其中域被隔離並駐留在不同的部署上
- 如果貴公司正在接受新收購，並希望將其域包含在內以使用MAR功能 然後，建立多個帳戶配置檔案將比以前的ESA功能具有更大的靈活性

配置Exchange Online/O365配置檔案

- 為O365/Azure建立帳戶配置檔案包含在「背景」部分中上面列出的2個連結中。

Office 365/混合(Graph API) — 選擇此項以配置在Exchange online上部署的郵箱，並輸入以下詳細資訊：

- 在Azure管理門戶上註冊的應用程式的客戶端ID和租戶ID。
- 證書的指紋（值為$base64Thumbprint）。
- 上傳證書的私鑰。按一下「選擇檔案」並選擇.pem檔案。

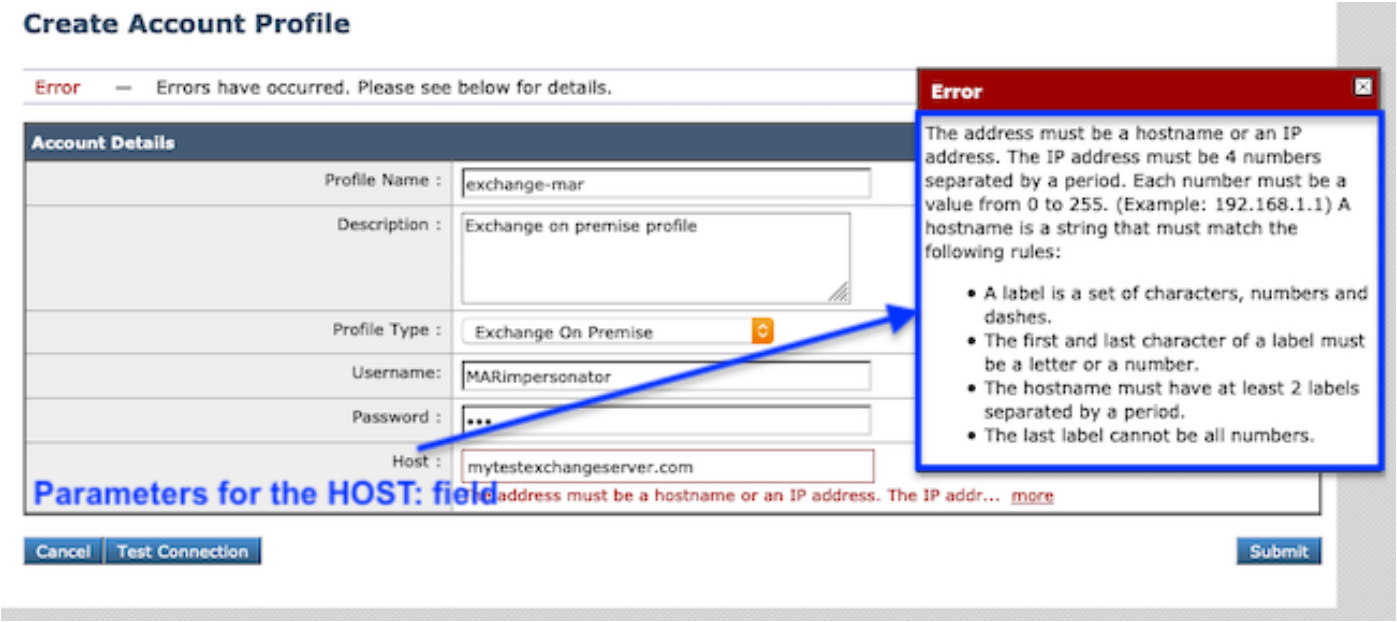


連線到O365的示例配置檔案

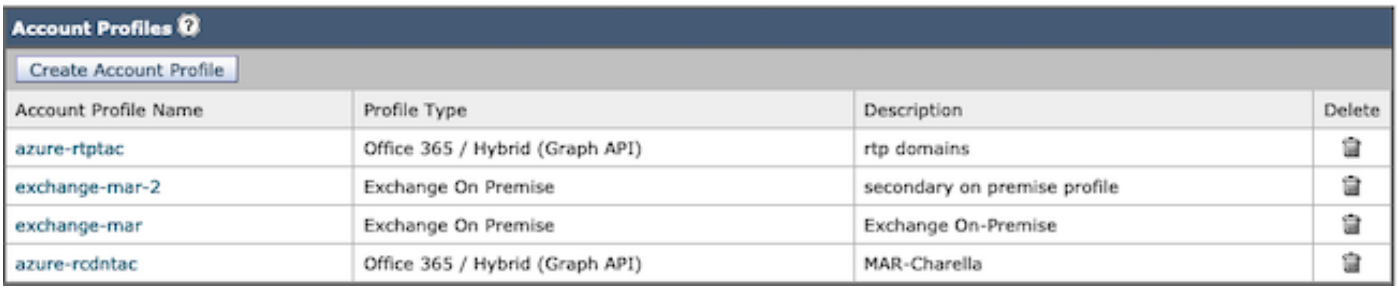
配置Exchange內部部署配置檔案

- 為內部部署Exchange例項建立帳戶配置檔案要簡單得多。
- 此方法需要一個具有ApplicationImpersonation的使用者帳戶。
- 使用以下格式瀏覽到Exchange管理中心，替換為您的值。https://mail.yourdomain.com/ecp/
- 登入後，導航到Permissions > Admin Roles > +以新增新配置檔案。如果您具有現有角色，可以將指定的使用者帳戶新增到成員中。
- 建立名稱和說明。向下滾動至「角色：+"新增角色。向下滾動，突出顯示「ApplicationImpersonation」，新增，確定
- 返回到新建立的配置檔案，選擇「成員：+"查詢並新增您指定用於ESA的使用者帳戶。
- 提交所有更改。
- 更詳細的說明需要管理員在MS支援頁面上進行研究。

- 然後登入ESA WebUI並導航至Account Settings。
- 建立帳戶配置檔案、名稱和說明。
- 選擇下拉選項「Profile Type:內部交換。」
- 填寫使用者名稱/密碼和主機：價值.
- 主機可接受的引數：值包括在影象中。
- 提交和提交更改。



Exchange內部部署配置檔案示例



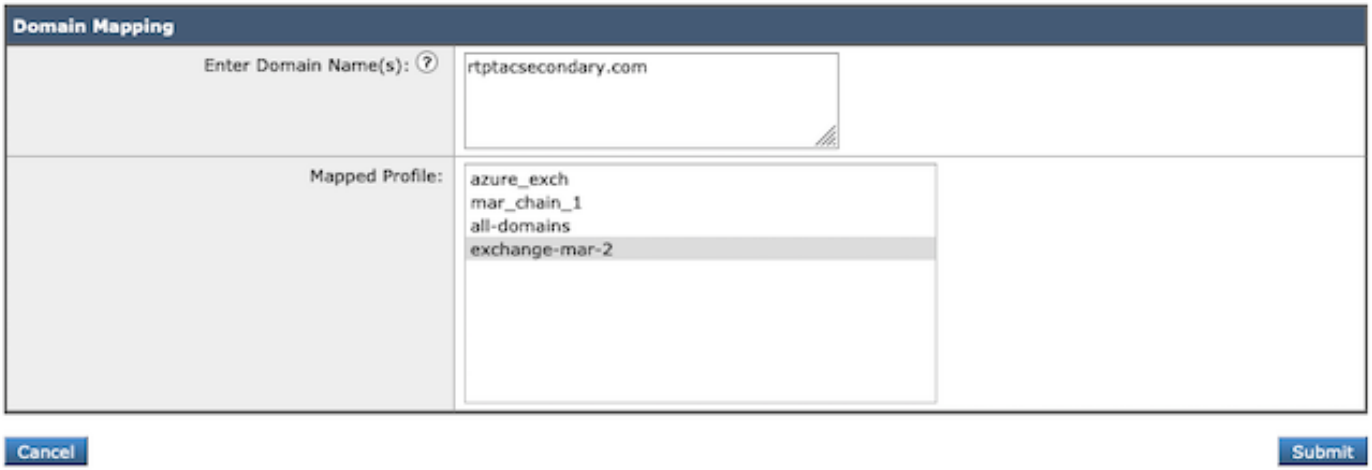
MAR帳戶配置檔案示例

配置域對映

域對映是將域分配給帳戶配置檔案。

每個實施至少需要一個域對映：

1. WebUI導航到系統管理>帳戶設定>建立域對映。
2. 輸入以逗號分隔的域名（Image1中列出了可接受域格式的完整清單）。
3. 如果整個配置中只有一個帳戶配置檔案，則填充域名：**全部。**
4. 域只能使用一次。



域對映示例

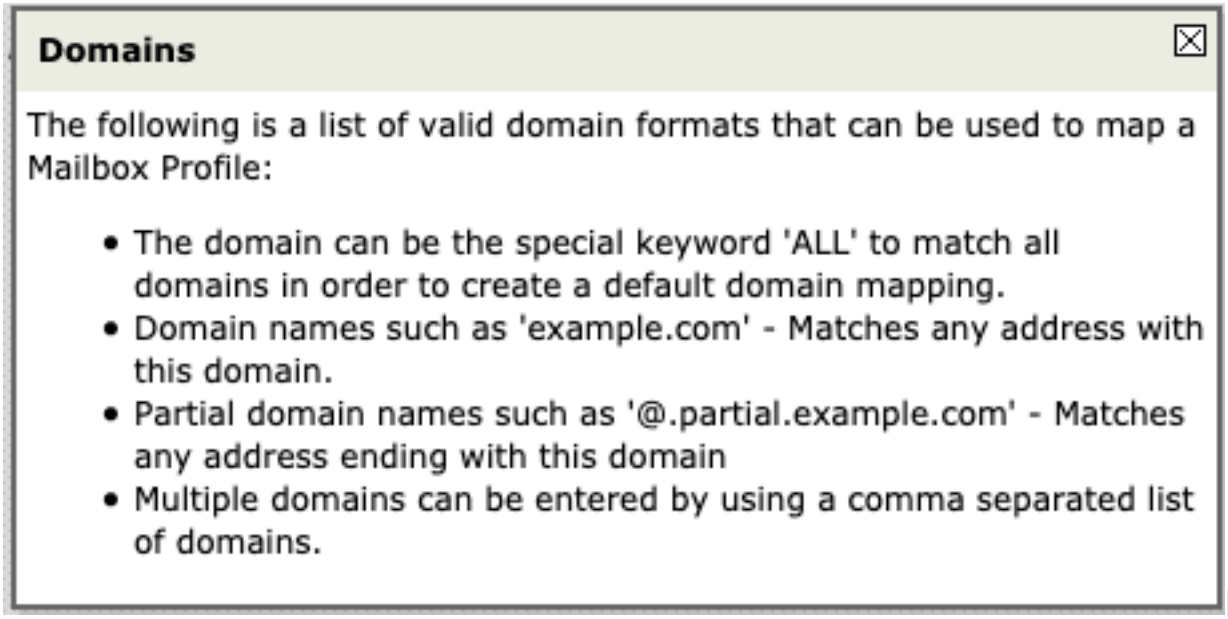
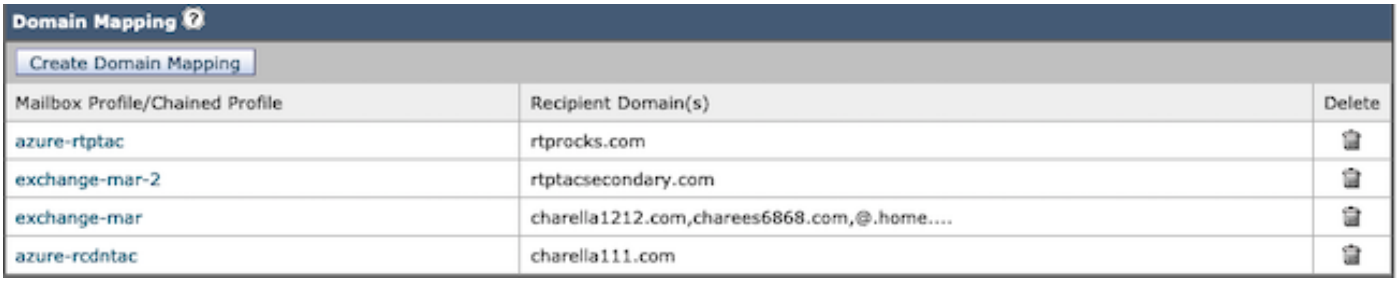


圖1.可接受的域格式



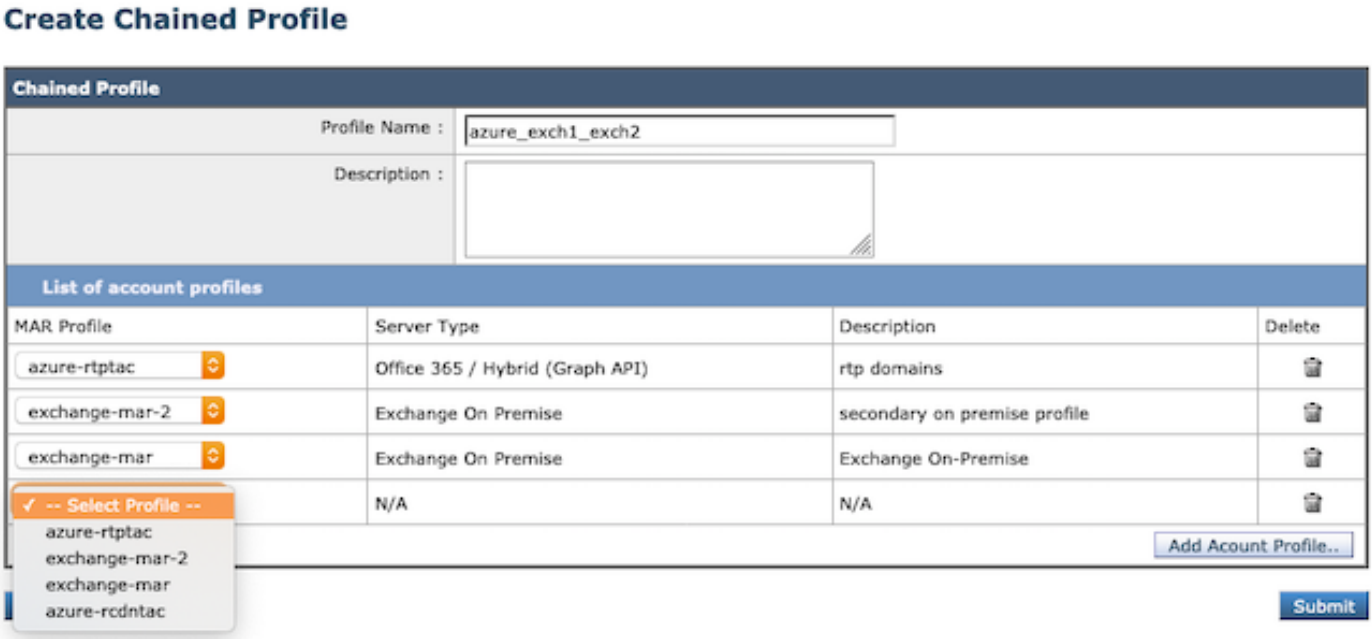
域對映示例

配置鏈結配置檔案

僅當要修復混合部署或多租戶部署上的郵箱中的郵件時，才需要執行此操作。

應首先以最高優先順序新增配置檔案。首先使用率最高的域配置檔案。

1. WebUI >導航至>系統管理>帳戶設定>建立鏈結配置檔案。
2. 新增配置檔名稱、說明。
3. 從Mar Profile中選擇域：下拉選單。
4. 選擇「Add Account Profile」（新增帳戶配置檔案）以新增另一個域配置檔案，直到選擇完成。
5. 提交和提交更改。



建立鏈配置檔案。

驗證每個帳戶配置檔案

在單個配置檔案中，選擇「測試配置檔案」按鈕確認每個帳戶配置檔案。

1. WebUI >導航>系統管理>帳戶設定>選擇其中一個帳戶配置檔案
2. 選擇左下方按鈕「測試連線」。
3. 填寫「電子郵件地址：欄位」並選擇「測試連線」。

測試每個配置檔案以驗證連線是否成功

疑難排解

日誌包含：

- mail_logs:最終補救行動和摘要
- mar_logs:執行補救的順序
- UI中的「測試連線」選項：用於驗證連線和許可權

通過「Account Settings（帳戶設定）」中的電子郵件測試可以確定許多資訊：

使用測試連線進行故障排除

- **SMTP地址沒有與之關聯的郵箱。** 正在使用的使用者郵箱不存在。
- **訪問被拒絕。請檢查憑據並重試。** 在Microsoft Azure中配置的應用程式沒有訪問Office 365郵箱所需的許可權。
- **在目錄<tenant_id>中找不到識別符號為「<client_id>」的應用程式。** 帳戶配置檔案設定頁面上的客戶端ID無效。
- **在資料儲存中找不到名為「<tenant_id>」的服務名稱空間。** 帳戶配置檔案設定頁面上的租戶ID無效。
- **驗證憑據時出錯。憑據驗證失敗。** 帳戶配置檔案頁上的證書指紋無效。用於訪問郵箱的配置檔

案型別可能不正確。例如，使用Office 365配置檔案訪問內部郵箱。可能缺少訪問郵箱所需的許可權。

- **為Exchange伺服器輸入的使用者名稱或密碼無效。** 在配置檔案中輸入的模擬者帳戶使用者名稱和密碼無效。
- **該帳戶沒有模擬所請求使用者的許可權。** 未向配置檔案中配置的使用者帳戶分配模擬器角色許可權。
- **請檢查主機<hostname>是有效的exchange server地址。** 在配置檔案中輸入的本地Exchange伺服器主機名無效。
- **無法使用此配置檔案訪問郵箱，或者缺少所需的許可權。** 正在使用錯誤型別的配置檔案訪問有效的郵箱。使用o365配置檔案訪問的內部郵箱示例。

單個配置檔案的成功補救示例：

```
Fri Aug 30 11:57:30 2019 Info: Process ready for Mailbox Remediation
Fri Aug 30 12:29:54 2019 Info: MID: 782107 Attempting to remediate using `azure-rtptac` profile
for recipient testuser@rtprocks.com. Attempt number : 1
Fri Aug 30 12:29:54 2019 Info: MID: 782107 Trying to perform the forward and delete action on
Office 365 or Hybrid exchange for SHA256:
1e6f324 982d4eb71ad967e79261a6435aef928b57bc523dbb3e7de4ed65941ab recipient's
(testuser@rtprocks.com) mailbox.
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Message forwarded successfully to
admin_mar@rtprocks.com.
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Message deleted successfully from
testuser@rtprocks.com mailbox.
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Remediation succeeded with `azure-rtptac` profile for
recipient testuser@rtprocks.com.
```

鏈結配置檔案的成功修復示例：

```
Mon Oct 14 15:01:01 2019 Info: MID: 24 Attempting gto remediate using 'azurertptac' profile for
recipient charella@rtptacsecondary.com . Attempt number : 1
Mon Oct 14 15:01:01 2019 Info: MID: 24 Trying to perfrm the delete action on Office 365 or
Hybrid exchange for SHA256: 1e6f324982d4eb71ad967e79261a6435aef928b57bc523dbb3e7de4ed65941ab
recipients (charella@rtptacsecondary.com) mailbox
Mon Oct 14 15:01:09 2019 Info: MID: 24 Unable to read message(s) from the recipient's
(charella@rtptacsecondary.com ) mailbox. Error: The mailbox cannot be accessed using this
profile or the required
permissions may be missing
Mon Oct 14 15:01:09 2019 Info: MID: 24 Attempting to remediate using 'exchange-mar-2' profile
for recipient charella@rtptacsecondary.com . Attempt number : 1
Mon Oct 14 15:01:09 2019 Info: MID: 24 Trying to perform the delete action on On Premise
Exchange for SHA256: 1e6f324982d4eb71ad967e79261a6435aef928b57bc523dbb3e7de4ed65941ab
recipient's (charella@rtptacsecondary.com) mailbox.
Mon Oct 14 15:01:16 2019 Info: MID: 24 Message deleted successfully from
charella@rtptacsecondary.com mailbox.
Mon Oct 14 15:01:16 2019 Info: MID: 24 Remediation succeeded with 'exchange-mar-2' profile for
recipient charella@rtptacsecondary.com. Not trying further profile.
```

相關資訊

- 如何為ESA配置Azure AD和Office 365郵箱設定
- 技術支援與檔案 — Cisco Systems
- 思科電子郵件安全裝置 — 產品支援
- 思科電子郵件安全裝置 — 版本說明
- Cisco Email Security Appliance — 最終使用手冊
- 思科內容安全管理裝置 — 產品支援

- 思科內容安全管理裝置 — 版本說明
- 思科內容安全管理裝置 — 最終使用手冊