ForeScout CounterACT®

單機版 CounterACT 裝置

《快速安裝手冊》

版本 8.0

目錄

歡迎使用 CounterACT 8.0 版

CounterACT 平臺可提供基礎設施和設備可視性、政策管理、業務流程和工作流簡化，加強網絡安全。CounterACT 為企業提供即時的網絡設備和用戶情境資訊。政策在使用此情境資訊的 CounterACT 中界定，幫助確保合規、修復、適當的網絡訪問和簡化服務操作。

本手冊主要介紹單機版 CounterACT 裝置的安裝方法。

更詳細的資訊或關於部署多個裝置在企業範圍內實施網絡保護的資訊，請參閱*《CounterACT 安裝手冊》*和 *《CounterACT 管理手冊》*。請參閱 其他 CounterACT 文檔瞭解有關如何查看此類手冊的資訊。

另外，您也可以導航至支援網站：http://www.forescout.com/support，查看最新的文檔、知識庫文章和裝置的相關更新。

CounterACT 包裝清單

CounterACT 包裝中包含下列組件：

- CounterACT 裝置
- 前面板
- 導軌套件（安裝支架）
- 電源線
- DB9 控制台連接線纜（僅用於串列連接）
- 《企業產品安全、環境和監管資訊》
- 《入門手冊》文檔（僅限 51xx 裝置）

概述

按照下列步驟裝配 CounterACT：

1.制定部署計畫

2.設置交換機

3.連接網線並接通電源

4.配置裝置

5.遠端管理

6.驗證連接

7.設置 CounterACT 控制台

1.制定部署計畫

安裝之前，應該確定部署裝置的位置並瞭解裝置的介面連接。

確定部署裝置的位置

選擇安裝裝置的正確網絡位置，對成功部署 CounterACT 和確保其最佳性能極為重要。正確的位置取決於您的實施目標和網絡訪問政策。該裝置應該能夠監控與所需政策相關的流量。例如，如果您的政策依賴於在企業認證伺服器的端點監控授權活動，則需要安裝此裝置，以便它能夠監測流入認證伺服器的端點流量。

更多關於安裝和部署的資訊，請參閱*《CounterACT 安裝手冊》*。請參閱 其他 CounterACT 文檔瞭解有關如何查看此手冊的資訊。

裝置介面連接

該裝置通常配置有三個連接網絡交換機的介面連接。

管理介面

管理介面方便您管理 CounterACT 並對端點進行查詢和深層檢測。該介面必須連接至可訪問所有網絡端點的交換機端口。

每台裝置需要一個單獨的管理介面來連接網絡。此連接需要本地 LAN 上的 IP 地址和來自運行 CounterACT 控制台管理應用程式的機器的 13000/TCP 端口訪問。管理端口必須可以訪問其他網絡服務。

網絡接入要求

端口	服務	接入或接出 CounterACT	功能
22/TCP	SSH	接出	允許遠端監測 OS X 和 Linux 端點。 允許 CounterACT 與網絡交換機和路由器通信。
		接入	允許接入 CounterACT 命令行介面。
2222/TCP	SSH	接入	（高可用性）允許訪問作為高可用性對一部分的 CounterAC 實體裝置。 使用 22/TCP 訪問該對的共用（虛擬）IP 地址。
25/TCP	SMTP	接出	允許 CounterACT 訪問企業郵件轉發。
53/UDP	DNS	接出	允許 CounterACT 解析內部 IP 地址。
80/TCP	HTTP	接入	允許 HTTP 重定向。

端口	服務	接入或接出 CounterACT	功能
123/UDP	NTP	接出	允許 CounterACT 訪問本地時間伺服器或 ntp.forescout.net。 CounterACT 默認訪問 ntp.foreScout.net
135/TCP	MS-WMI	接出	允許遠端監測 Windows 端點。
139/TCP	SMB，MS-RPC	接出	允許遠端監測 Windows 端點（對於運行 Windows 7 或較早版本的端點）。
445/TCP			允許遠端監測 Windows 端點。
161/UDP	SNMP	接出	允許 CounterACT 與網絡交換機和路由器通信。 有關配置 SNMP 的資訊，請參閱*《CounterACT 管理手冊》*。
162/UDP	SNMP	接入	允許 CounterACT 從網絡交換機和路由器接收 SNMP 陷阱。 有關配置 SNMP 的資訊，請參閱*《CounterACT 管理手冊》*。
389/TCP (636)	LDAP	接出	允許 CounterACT 與活動目錄通信。 允許與基於 CounterACT 網絡的門戶通信。
443/TCP	HTTPS	接入	允許使用 TLS 進行 HTTP 重定向。
2200/TCP	用於 Linux 的 SecureConnector	接入	允許 SecureConnector 在 Linux 機器上創建安全的（加密的 SSH）連接以連接至該裝置。*SecureConnector* 是個基於腳本的代理，它在連接網絡時可進行 Linux 端點管理。
10003/TCP	用於 Windows 的 SecureConnector	接入	允許 SecureConnector 在 Windows 機器上創建安全的（加密的 TLS）連接以連接至該裝置。*SecureConnector* 是個代理，它在連接網絡時可進行 Windows 端點管理。請參閱*《CounterACT 管理手冊》*瞭解更多關於 SecureConnector 的資訊。 SecureConnector 連接至裝置或企業管理器時，它會被重定向至主機分配到的裝置。確保此端口對所有裝置和企業管理器開放，從而確保在組織內部實現透明的移動性。
10005/TCP	用於 OS X 的 SecureConnector	接入	允許 SecureConnector 在 OS X 機器上創建安全的（加密的 TLS）連接以連接至該裝置。*SecureConnector* 是個代理，它在連接網絡時可進行 OS X 端點管理。請參閱*《CounterACT 管理手冊》*瞭解更多關於 SecureConnector 的資訊。 SecureConnector 連接至裝置或企業管理器時，它會被重定向至主機分配到的裝置。確保此端口對所有裝置和企業管理器開放，從而確保在組織內部實現透明的移動性。

端口	服務	接入或接出 CounterACT	功能
13000/TCP	CounterACT	接入/接出	對於只有一台裝置的環境——從控制台連接到裝置。 對於有多台 CounterACT 設備的環境——從控制台連接到 CounterACT 設備，再從一台 CounterACT 設備連接到另一台。CounterACT 設備通信包括使用 TLS 與企業管理器和恢復企業管理器通信。

監控介面

監控介面允許裝置監控並追蹤網絡流量。任何可用介面都可用作監控介面。

流量鏡像至交換機的端口並由該裝置監控。802.1Q VLAN 標記的使用取決於被鏡像的 VLAN 數量。

- ***單一 VLAN***：監控的流量由單一的 VLAN 生成時，鏡像流量不需要添加 VLAN 標記。
- ***多重 VLAN***：如果監控的流量來自於多個 VLAN，鏡像流量必須添加 802.1Q VLAN 標記。

當兩個交換機作為冗余對連接時，該裝置必須同時監控兩個交換機的流量。

監控介面無需 IP 地址。

回應介面

該裝置使用回應介面對流量作出回應。回應流量用於防止惡意行為及執行政策措施。這些措施可能包括，例如，重定向網頁流覽器或進行會話阻塞。相關的交換機端口配置取決於正被監控的流量。

任何可用介面都可用作回應介面。

- ***單一 VLAN***：監控的流量由單一的 VLAN 生成時，回應端口必須屬於同一個 VLAN。在這種情況下，該裝置在該 VLAN 上必須有單一的 IP 地址。
- ***多個 VLAN***：如果監控的流量來自多個 VLAN，響應端口也必須為相同的 VLAN 配置 802.1Q VLAN 標記。該裝置則要求每個被監控 VLAN 有一個 IP 地址。

2.設置交換機

A. 交換機連接選項

該裝置旨在與多種多樣的網絡環境無縫整合。若要成功地將裝置整合到您的網絡中，請驗證交換機是否設定為監控所需的流量。

有幾個選項可用於將該裝置連接至您的交換機。

1 標準部署（分開管理、監控和響應介面）

推薦部署使用三個獨立的端口。這些端口在 裝置介面連接有說明。

2 被動式內聯分接頭

該裝置可使用被動式內聯分接頭，不需要連接至交換機監控端口。

被動式內聯分接頭需要兩個監控端口（一個用於上游流量，而另一個用於下游流量），除非是在有*重組*分接頭的情況下，它會將兩個雙工流結合在單個端口中。注意，如果連接分接頭的端口上的流量已作出 802.1Q VLAN 標記，那麼回應端口也必須作出 802.1Q VLAN 標記。

3 主動式（可插入）內聯分接頭

該裝置可使用主動式內聯分接頭。如果分接頭可以插入，該裝置會將監控端口和回應端口結合在一起，這樣就無需在交換機上配置單獨的回應端口。無論是上游還是下游交換機配置類型，均可使用此選項。

4 IP 層回應（第 3 層交換機安裝）

該裝置可以使用自帶的管理介面對流量作出回應。儘管這個選項可與任何受監控的流量一起使用，但還是建議只在裝置監控並非任何 VLAN 一部分的多個端口且無法使用其他任何交換機端口對監控的流量作出回應時使用。這在監控兩個路由器之間的鏈路時最常出現。這個選項無法對地址解析通訊協定 (ARP) 請求作出回應，這會限制該裝置探測針對所監控的子網包含的 IP 地址的掃描的能力。兩個路由器之間的流量受到監控時，此限制將不適用。

B. 交換機設置注意事項

VLAN (802.1Q) 標記

- ***監控單一 VLAN***：如果受監控流量來自于單一 VLAN，那麼該流量不需要 802.1Q VLAN 標記。
- ***監控多個 VLAN***：如果受監控的流量來自於兩個或多個 VLAN，那麼被監控端口和回應端口都必須啟用 802.1Q VLAN 標記。推薦監控多個 VLAN，因為它在最大限度減少鏡像端口數量的同時，也提供最佳的整體覆蓋。
- 如果交換機無法在鏡像端口上使用 802.1Q VLAN 標記，那麼請執行下列操作中的一項：

  - 僅鏡像單一 VLAN
  - 鏡像單一、未加標記的上行鏈路端口
  - 使用 IP 層回應選項
- 如果交換機只能鏡像一個端口，則鏡像單一上行鏈路端口。這可能會被添加標記。一般而言，如果交換機去掉 802.1Q VLAN 標記，您就必須使用 IP 層回應選項。

其他指引

- 在下列情況下，您只能鏡像一個介面（允許傳送/接收）：
  - 如果交換機無法鏡像傳輸和接收的流量
  - 如果交換機無法鏡像所有交換機流量
  - 如果交換機無法鏡像 VLAN 的所有流量
- 請確認您的鏡像端口沒有過載。
- 有些交換機（例如 Cisco 6509）在進入新的配置之前，可能會要求完全刪除當前的端口配置。未刪除舊有的端口資訊通常會導致交換機去掉 802.1Q 標記。

3.連接網線並接通電源

A. 打開設備包裝並連接電纜

1. 將裝置和電力電纜從集裝箱上搬下來
2. 取出與裝置一起收到的導軌套件。
3. 在裝置上安裝導軌套件並將裝置安裝在支架上。
4. 連接裝置後面板上的網絡介面和交換機端口之間的網線。

   後面板樣板——CounterACT 設備

您可以使用經 ForeScout 測試及認證的 Finisar SFP 替換 ForeScout 提供的 SFP。請參閱*《CounterACT 安裝手冊》*瞭解更多詳細資訊。

B. 記錄介面分配

在資料中心完成裝置安裝及安裝 CounterACT 控制台之後，您將收到登記介面分配的提示。這些分配，也稱為*通道定義*，要在您首次登錄控制台時打開的初始設置嚮導中輸入。

在下方記錄實際的介面分配，並在控制台上完成通道設置時使用它們。

Eth 介面	介面分配（例如，管理、監控和回應）
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	

C. 接通裝置的電源

1. 將電力電纜連線到裝置後面板上的電源連接器上。

2. 將電力電纜的另一端連接到接地的交流電插座上。
3. 將鍵盤和顯示器與裝置相連，或者設置裝置的串列連接。請參閱*《CounterACT 安裝手冊》*瞭解更多資訊。
4. 在前面板上打開裝置的電源。

4.配置裝置

在您配置裝置之前，請準備好下列資訊。

裝置主機名稱	
CounterACT 管理員密碼	將密碼保存在安全的位置
管理介面	
裝置 IP 地址	
網絡掩碼	
默認網關 IP 地址	
DNS 域名	
DNS 伺服器地址	

打開電源之後，您將被提示開始配置下列資訊：

```
CounterACT 裝置啟動完成。
按下 <Enter> 鍵以繼續。
```

1. 按下 **Enter** 鍵如果您的設備是 51xx CounterACT，則會顯示下列菜單：

```
CounterACT 8.0.0-<build> 選項：

1) 配置 CounterACT

2) 還原保存的 CounterACT 配置

3) 識別並對網絡介面重新編號

4) 配置鍵盤佈局

5) 關閉機器

6) 重啟機器

選擇 (1-6)：1
```

如果您的設備是 CT-xxxx CounterACT，則會在菜單頂部看到列示的版本是 CounterACT 7.0.0 或 CounterACT 8.0.0。

– 如果您看到的是 CounterACT 7.0.0，則可以升級或者直接安裝版本 8.0.0。請參閱 *《CounterACT 安裝手冊》* 瞭解詳細資訊。升級至或安裝版本 8.0.0 之後，您將會看到上述菜單。

– 如果您看到的是 CounterACT 8.0.0，菜單則會提供安裝 CounterACT 7.0.0 或配置 CounterACT 8.0.0 的選項，如下所示。如果您選擇 CounterACT 7.0.0，將無法透過 Configuration（配置）菜單重新安裝 CounterACT 8.0.0。請參閱*《CounterACT 版本 7.0.0 安裝手冊》*瞭解配置 CounterACT 7.0.0 的詳細資訊。

```
CounterACT 8.0.0-<build> 選項：

1) 安裝 CounterACT 7.0.0-<build>

2) 配置 CounterACT 8.0.0-<build>

3) 還原保存的 CounterACT 配置

4) 識別並對網絡介面重新編號

5) 配置鍵盤佈局

6) 關閉機器

7) 重啟機器

選擇 (1-7)：
```

如果配置被中斷或者如果您選擇的 CounterACT 版本錯誤，則需要使用相關版本的 ISO 文件重置裝置映像。請參閱《CounterACT 安裝手冊》瞭解更多重置裝置映像的資訊。

2. 選擇 **Configure CounterACT（配置 CounterACT）**。出現提示時：

   繼續：（yes/no（是/否））？

   按下 **Enter** 鍵以啟動設置。

3. High Availability Mode（高可用性模式）提示框打開。按下 **Enter** 鍵，選擇 Standard Installation（標準安裝）。

4. 顯示 CounterACT Initial Setup（CounterACT 初始設置）提示框。按下 **Enter** 鍵以繼續。

5. Select CounterACT Installation Type（選擇 CounterACT 安裝類型）提示框打開。鍵入 **1**，然後按下 **Enter** 鍵，安裝標準的 CounterACT 裝置。

   設置被初始化。這可能需要一點時間。

6. Select Licensing Mode（選擇許可模式）提示框打開。選擇您的部署使用的許可模式。許可模式在購買過程中決定。***確認您的部署使用的許可模式之前，請勿鍵入任何值***。聯絡您的 ForeScout 代表驗證您的許可模式或者驗證您是否輸入了錯誤的模式。

7. 在 Enter Machine Description（輸入機器描述）提示框中，輸入識別該設備的短文本，然後按下 **Enter** 鍵。

   顯示下列介面：

```
>>>>>> 設置管理員密碼 <<<<<<
```

此密碼將用於以「 根 」的身份登錄機器操作系統並以「 管理員」 的身份登錄 CounterACT 控制台。 密碼的長度必須為 6 到 15 個字符，而且應至少包含一種非字母字符。 管理員密碼：

8. 在 Set Administrator Password（設置管理員密碼）提示框中，鍵入密碼字符串（這個字符串不會在螢幕上顯示），然後按下 **Enter** 鍵。您將會收到確認密碼的提示。密碼的長度必須為 6 到 15 個字符，而且至少要包含一種非字母字符。

   以 root（根）*的身份登錄裝置，然後以* admin（管理員）*的身份登錄控制台。*

9. 在 Set Host Name（設置主機名稱）提示框中，鍵入主機名稱，然後按下 **Enter** 鍵。主機名稱可在登錄控制台時用到，而且會顯示在控制台上，以幫助您識別正在查看的 CounterACT 裝置。主機名稱不得超過 13 個字符。

10. Configure Network Settings（配置網絡設置）介面會提示一系列配置參數。在每個提示框中鍵入一個值，然後按下 **Enter** 鍵以顯示下一個提示框。

    – CounterACT 元件透過管理介面通信。列示的管理介面數量取決於裝置型號。

    – **Management IP address（管理 IP 地址）**是 CounterACT 元件通信所使用介面的地址。只有當用於在 CounterACT 元件之間通信的介面連接至已添加標記的端口時，才需要為此介面添加 VLAN ID。

    – 如果有多個 **DNS 伺服器地址**，則用空格將每個地址隔開。大部分內部 DNS 伺服器可解析外部和內部地址，但是您可能需要添加一台外部解析 DNS 伺服器。由於裝置執行的幾乎所有 DNS 查詢都將用於內部地址，因此，外部 DNS 伺服器應該列在最後。

11. Setup Summary（設置概要）介面將會顯示。您將被提示執行一般連接測試、重新配置設置或完成設置。鍵入 **D** 以完成設置。

許可證

配置之後，確保您的 CounterACT 設備擁有有效的許可證。CounterACT 設備的默認許可狀態取決於部署正在使用的許可模式。

- 如果 CounterACT 部署正在 ***Per-Appliance Licensing Mode（單一裝置許可模式）***下運行，您現在可以使用演示許可證開始工作，該許可證的有效期是 30 天。在此期間，您應該會收到 ForeScout 的永久性許可證，將它放在硬盤或網絡的可訪問資料夾中。在 30 天的演示許可證到期之前，從這個位置安裝許可證（如有必要，您可以申請演示許可證延期。）。

  如果您的演示許可證即將過期，您將收到透過各種方式發來的提示。請參閱*《CounterACT 管理手冊》*瞭解更多關於演示許可證提示的資訊。

  如果您正使用 CounterACT 虛擬系統：

  – 演示許可證不會在這個階段自動安裝。您必須安裝 ForeScout 代表透過電子郵件發送給您的演示許可證。

  – 至少應該有一台 CounterACT 設備可以訪問網絡。此連接用於在 ForeScout 許可證伺服器上驗證 CounterACT 許可證。未在一個月內驗證的許可證將被撤銷。CounterACT 將會每天發送一封警告郵件，提醒與伺服器之間的通信出錯。

    請參閱*《CounterACT 安裝手冊》*瞭解更多資訊。

- 如果 CounterACT 部署正在 ***Centralized Licensing Mode（集中許可模式）***下運行，當許可證權利已創建並可在 ForeScout 客戶門戶獲取時，*權利管理員*應該會收到一封電子郵件。許可證可以獲取之後，部署的 *CounterACT 管理員*就可在 CounterACT 控制台上激活許可證。許可證激活之前，CounterACT 功能無法正常運行。例如，將不會對政策進行評估，也不會執行操作。*演示許可證不會在系統安裝過程中自動安裝。*

請參閱*《CounterACT 管理手冊》*瞭解更多關於許可證管理的資訊。

5.遠端管理

iDRAC 設置

集成化戴爾遠端存取控制器 (iDRAC) 是一個集成化的伺服器系統解決方案，可透過 LAN 或互聯網對 CounterACT 裝置進行位置獨立/操作系統獨立的遠端存取。使用模組執行 KVM 訪問、開啟電源/關閉電源/重置以及執行故障排除和維護任務。

執行下列操作， 以便使用 iDRAC 模組：

- 啟用並配置 iDRAC 模組
- 將模組連接至網絡
- 登錄 iDRAC

啟用並配置 iDRAC 模組

更改 iDRAC 設置，以在 CounterACT 設備上啟用遠端存取。這個部分描述與 CounterACT 一起運行所需的基礎集成設置。

若要配置 iDRAC：

1. 打開管理的裝置。
2. 在啟動過程中選擇 F2。
3. 在 System Setup Main Menu（系統設置主菜單）頁面，選擇 **iDRAC Settings（iDRAC 設置）**。
4. 在 iDRAC Settings（iDRAC 設置）頁面，選擇 **Network（網絡）**。
5. 配置下列 Network（網絡）設置：
   - ***Network Settings（網絡設置）***。驗證 **Enable NIC（啟用 NIC）**欄位是否被設置為 **Enabled（已啟用）**。
   - ***Common Settings（常用設置）***。您可以在 DNS DRAC Name（DNS DRAC 名稱）欄位更新動態 DNS（可選）。
   - ***IPV4 Settings（IPV4 設置）***。驗證 **Enable IPv4（啟用 IPv4）**欄位是否被設置為 **Enabled（已啟用）**。

     將 **Enable DHCP（啟用 DHCP）**欄位設置為 **Enabled（已啟用）**，以使用動態 IP 地址，或者設置為 **Disabled（已禁用）**，使用靜態 IP 地址。如果被啟用，DHCP 將會為 iDRAC 自動分配 IP 地址、網關和子網掩碼。如果被禁用，在 **Static IP Address（靜態 IP 地址）**、**Static Gateway（靜態網關）**和 **Static Subnet Mask（靜態子網掩碼）**欄位輸入值即可。

6. 選擇 **Back（後退）**。
7. 選擇 **User Configuration（用戶配置）**。
8. 為根用戶配置下列 User Configuration（用戶配置）欄位。
   - ***Enable User（啟用用戶）***。驗證這個欄位是否被設置為 Enabled（已啟用）。

     在此配置的用戶名跟 CounterACT 用戶名不一樣。

   - ***LAN and Serial Port User Privileges（LAN 和串行端口用戶權利）***。將權利級別設為 Administrator（管理員）。
   - ***Change Password（更改密碼）***。設置用戶登錄的密碼。
9. 選擇 **Back（後退）**，然後選擇 **Finish（完成）**。確認更改的設置。

   配置的設置會被保存，而且系統會重啟。

將模組連接至網絡

iDRAC 連接至乙太網。一般的慣例是將它連接到管理網絡。下圖顯示 CT-1000 裝置後面板上的 iDRAC 端口位置：

登錄 iDRAC

若要登錄 iDRAC：

1. 流覽至在 **iDRAC Settings（iDRAC 設置）** > **Network（網絡）**中配置的 IP 地址或域名。
2. 輸入在 iDRAC 系統設置的 User Configuration（用戶配置）頁面配置的 Username（用戶名）和 Password（密碼）。
3. 選擇 **Submit（提交）**。

更多關於 iDRAC 的資訊，請參閱*《iDRAC 用戶手冊》*。取決於部署使用的許可模式，您可以在下列位置查看本手冊：

- Per-Appliance Licensing Mode（單一裝置許可模式）——https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf
- Centralized Licensing Mode（集中許可模式）——客戶門戶，Documentation（文檔）頁面。

請參閱 其他 CounterACT 文檔（*在控制台識別您的許可模式*），瞭解您的部署正在使用的許可模式。

更新默認根密碼非常重要（如果您還沒有更新的話）。

6.驗證連接

驗證管理介面連接

若要測試管理介面連接，登錄該裝置並運行下列命令：

fstool linktest

則會顯示下列資訊：

```
管理介面狀態
正在 Ping 默認網關資訊
Ping 統計資料
正在執行名稱解析測試
測試總結
```

執行 Ping 測試

運行下列命令，以驗證從裝置到網絡桌面的連接：

Ping <network_desktop_IP_address>

7.設置 CounterACT 控制台

安裝 CounterACT 控制台

控制台是用於查看端點的詳細資訊並對其進行控制的 CounterACT 管理應用程式。此資訊由 CounterACT 設備收集。請參閱*《CounterACT 管理手冊》*瞭解更多資訊。

您必須提供存放 CounterACT 控制台應用程式軟件的機器。最低硬件要求：

- 非專用機器，運行：
  - Windows 7/8/8.1/10
  - Windows Server 2008/2008 R2/2012/2012 R2/2016
  - Linux RHEL/CentOS 7
- 記憶體 2GB
- 硬盤空間 1GB

可透過下列途徑執行控制台安裝：

使用裝置內置的安裝軟件。

1. 在控制台電腦上打開流覽器視窗。
2. 在流覽器地址行鍵入下列地址：

   http://<Appliance_ip>/install

   其中 Appliance_ip 是該裝置的 IP 地址。流覽器即會顯示控制台安裝視窗。
3. 按照介面上顯示的提示操作。

登錄

安裝完成之後，您可以登錄 CounterACT 控制台。

1. 在您創建的快捷方式位置選擇 CounterACT 圖標。
2. 在 **IP/Name（IP/名稱）**欄位輸入裝置的 IP 地址或主機名稱。
3. 在 **User Name（用戶名）**欄位，輸入管理員。
4. 在 **Password（密碼）**欄位，輸入您在安裝裝置過程中創建的密碼。
5. 選擇 **Login（登錄）**，啟動控制台。

進行初始設置

首次登錄時，初始設置嚮導即會打開。該嚮導會指導您完成必要的配置步驟，以設置 CounterACT 並使其快速高效地運行。

開始初始設置之前

在您按照嚮導操作之前，請準備好下列資訊：

嚮導所需的資訊	值
您的組織所使用的 NTP 伺服器地址（可選）	
如果裝置不允許發送 SMTP 流量，允許發送郵件提醒的內部郵件轉發 IP 地址（可選）	
CounterACT 管理員電子郵箱地址	
監控和回應介面	
對於無 DHCP 的分段/VLAN，則是回應介面直接連接的網絡分段/VLAN，以及 CounterACT 在每個此類 VLAN 使用的永久性 IP 地址。	
此裝置將監控的 IP 地址範圍（所有內部地址，包括未使用的地址）	
LDAP 用戶帳戶資訊和 LDAP 伺服器 IP 地址	
域憑證，包括域管理帳戶名稱和密碼	
驗證伺服器，這樣 CounterACT 就可以確定哪些網絡主機已驗證成功	
交換機 IP 地址、供應商和 SNMP 參數	

請參閱*《CounterACT 管理手冊》*或線上幫助，瞭解操作嚮導有關的資訊。

其他 CounterACT 文檔

有關其他 CounterACT 功能和模組的資訊，請參閱下列資源：

- 文檔下載
- 文檔門戶
- CounterACT 幫助工具

文檔下載

文檔下載可從兩個 ForeScout 門戶中的其中一個訪問，這取決於部署使用的許可模式。

- ***Per-Appliance Licensing Mode（單一裝置許可模式）——***產品更新門戶
- ***Centralized Licensing Mode（集中許可模式）——***客戶門戶

也可以從這些門戶網站上下載軟件。

若要瞭解您的部署正在使用的許可模式，請參閱 在控制台上識別許可模式。

產品更新門戶

產品更新門戶提供轉至 CounterACT 版本發佈、基礎和內容模組、擴展模組以及相關文檔的連結。該門戶網站同時也提供一系列其他文檔。

若要訪問產品更新門戶：

1. 進入 https://updates.forescout.com/support/index.php?url=counteract。
2. 選擇您要查找的 CounterACT 版本。

客戶門戶

ForeScout 客戶門戶的 Downloads（下載）頁面提供轉至已購買 CounterACT 版本發佈、基礎和內容模組、擴展模組以及相關文檔的連結。如果您擁有軟件的許可證權利，軟件及相關的文檔則會顯示在 Downloads（下載）頁面。該門戶網站的 Documentation（文檔）頁面同時也提供一系列其他文檔。

若要查看 ForeScout 客戶門戶上的文檔：

1. 進入 https://forescout.force.com/support/。
2. 選擇 **Downloads（下載）**或 **Documentation（文檔）**。

文檔門戶

ForeScout 文檔門戶是可搜索的、基於網頁的文件庫，其中包含關於 CounterACT 工具、功能和集成的資訊。

如果部署正在使用 Centralized Licensing Mode（集中許可模式），您可能沒有訪問此門戶的憑證。

若要訪問文檔門戶：

1. 進入 www.forescout.com/docportal。
2. 使用您的客戶支援憑證登錄。
3. 選擇您要查找的 CounterACT 版本。

CounterACT 幫助工具

直接從 CounterACT 控制台查看資訊。

控制台幫助按鈕

使用情境敏感 *Help（幫助）*按鈕，快速查看關於您正在進行的任務或主題的資訊。

《CounterACT 管理手冊》

在 **Help（幫助）**菜單中選擇 **CounterACT Help（CounterACT 幫助）**。

插件幫助文件

1. 插件安裝之後，選擇 **Tools（工具）**菜單中的 **Options（選項）**，然後選擇 **Modules（模組）**。
2. 選中插件，然後選擇 **Help（幫助）**。

文檔門戶

在 **Help（幫助）**菜單中選擇 **Documentation Portal（文檔門戶）**。

在控制台上識別許可模式

如果您的企業管理器在控制台上列示有 *ForeScout CounterACT See（ForeScout CounterACT 查看）*許可證，那麼您的部署正在 Centralized Licensing Mode（集中許可模式）下運行。如果沒有，您的部署則在 Per-Appliance Licensing Mode（單一裝置許可模式）下運行。

選擇 **Options（選項）> Licenses（許可證）**，查看您是否有表格列示的 *ForeScout CounterACT See（ForeScout CounterACT 查看）*許可證。

如果您對識別許可模式有任何疑問，請聯絡您的 ForeScout 代表。

法律聲明

有關本文檔的評論或疑問，請發送至：support@forescout.com

2018 年 3 月 27 日 15:08:24 2018 年 3 月 27 日 15:08:24