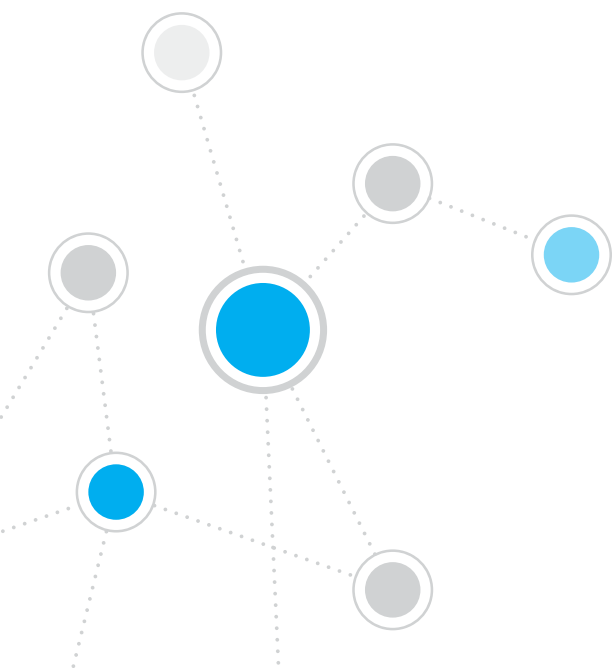




ForeScout CounterACT[®] 7

單一 CounterACT 設備

快速安裝指南



目錄

歡迎使用 ForeScout CounterACT® 7 版	3
CounterACT 包裝內容	3
概述	4
1. 建立部署計畫	5
決定設備部署位置	5
設備介面連接	5
2. 設定交換機	8
A. 交換機連接選擇	8
B. 交換機設定說明	9
3. 連接網路線並開機	10
A. 拆除包裝並連接纜線	10
B. 記錄介面分配	11
C. 開啟設備電源	11
4. 組態設備	12
網路連接要求	14
5. 遠端管理	15
iDRAC 設定	15
6. 驗證管理介面連接	19
驗證管理介面連接	19
驗證交換機/設備連接情況	19
執行 Ping 測試	20
7. 設定 CounterACT 控制台	21
安裝 CounterACT 控制台	21
登入	22
執行初始設定	22
聯絡資訊	24

歡迎使用 ForeScout CounterACT® 7 版

ForeScout CounterACT 是一套實體或虛擬安全設備，當有網路裝置與應用程式式連接到您的網路時，它能以動態方式立即進行識別並評估。由於 CounterACT 並不需要代理，因此它能夠搭配您的裝置運作 — 無論是受管或無受管、已知或未知、PC 或行動裝置、嵌入式或虛擬裝置均可。CounterACT 可快速判斷使用者、擁有者、作業系統、裝置組態、軟體、服務、修補程式狀態，以及是否存在安全性代理。接下來，它可對這些在網路上來來去去的裝置提供修補、控制與持續監控的能力。它還能在與您現有的 IT 基礎設施完全整合的前提下完成上述所有功能。



本指南描述了單一獨立式 CounterACT 設備的安裝。

如需更多詳情，或需要為企業級網路防護部署多部設備的資訊，請參閱《CounterACT 安裝指南》和《控制台使用者手冊》。這些文件位於 CounterACT 光碟的 /docs 目錄中。

此外，您還可以瀏覽支援網站：<https://www.forescout.com/support> 獲取設備的最新文件、知識庫文章和軟件更新。

CounterACT 包裝內容

- CounterACT 設備
- 快速安裝指南
- CounterACT 光碟（含控制台軟件、CounterACT 控制台使用者手冊和安裝指南）
- 保證書
- 安裝支架
- 電源線
- DB9 控制台連接線（僅用於串列連接）

概述

執行以下步驟設定 CounterACT:

1. 建立部署計畫
2. 設定交換機
3. 連接網路線並開機
4. 組態設備
5. 遠端管理
6. 驗證連接情況
7. 設定 CounterACT 控制台

1. 建立部署計畫

執行安裝前，應決定設備的部署位置以及瞭解設備介面連接。

決定設備部署位置

為設備選擇正確的網路位置對於 CounterACT 的成功部署和最佳性能是非常重要的。而正確位置則取決於所需實施目標和網路存取政策。本設備應能監測與所需政策相關的資訊流量。例如，如果您的政策依賴於監測從端點到企業驗證伺服器的授權事件，則需要將本設備安裝在能看到流向驗證伺服器的端點資訊流量的位置。

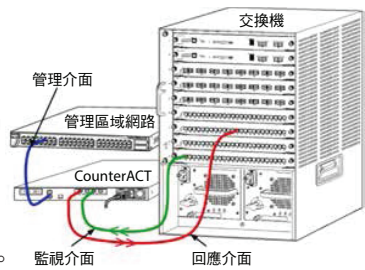
如需更多關於安裝和部署的資訊，請參閱此包裝隨附 CounterACT 光碟中的《CounterACT 安裝指南》。

設備介面連接

本設備通常組態了三個連接網路交換機的連接。

管理介面

透過此介面可管理 CounterACT 和執行端點查詢與深入檢查。此介面必須與能夠存取所有網路端點的交換機埠相連接。



每個設備都需要與網路建立單一管理連接。此連接需要本地區域網路的一個 IP 位址和執行 CounterACT 控制台管理應用程式的機器的 13000/TCP 埠存取許可權。該管理介面必須具有以下網路的存取許可權：

埠	服務	至或自 CounterACT	功能
22/TCP	SSH	至	允許存取 CounterACT 命令行介面。
2222/TCP			2222/TCP (高可用性) 允許存取屬於高可用性叢集的 CounterACT 物理裝置。 使用 22/TCP 存取該叢集的共用 (虛擬) IP 位址。
25/TCP	SMTP	自	自用於從 CounterACT 發送郵件
53/UDP	DNS	自	允許 CounterACT 解析內部 IP 位址。

埠	服務	至或自 CounterACT	功能
80/TCP	HTTP	至	允許 HTTP 重定向。
123/UDP	NTP	自	允許 CounterACT 存取 NTP 時間伺服器。CounterACT 預設使用 ntp.foreScout.net。
135/TCP	WMI	自	允許 CounterACT 使用 WMI 執行 Windows 端點的深入研究和控制。
139/TCP	SMB、MS-RPP	自	允許對 Windows 端點進行遠端檢查（針對執行 Windows 7 與較早版本的端點）。
445/TCP			允許對 Windows 端點進行遠端檢查。
161/UDP	SNMP	自	<p>允許 CounterACT 與網路基礎設施裝置通訊。例如，交換機和路由器。</p> <p>如需組態 SNMP 的資訊，請參閱《CounterACT 控制台使用者手冊》。</p>
162/UDP	SNMP	至	<p>允許 CounterACT 接收來自網路基礎設施裝置的 SNMP 陷阱。例如，交換機和路由器。</p> <p>如需組態 SNMP 的資訊，請參閱《CounterACT 控制台使用者手冊》。</p>
443/TCP	HTTPS	至	允許使用 SSL 進行 TLS 重定向。
2200/TCP	Secure Connector	至	允許 SecureConnector 從 Macintosh/Linux 機器建立與本設備的安全（加密 SSH）連接。當主機連接到網路時，SecureConnector 則為可管理 Macintosh 與 Linux 端點的指令集型代理。
10003/TCP	Secure Connector for Windows	至	<p>允許 SecureConnector 從 Windows 機器建立與本設備的安全（加密 TLS）連接。當主機連接到網路時，SecureConnector 則為可管理 Windows 端點的指令集型代理。請參閱《CounterACT 控制台使用者手冊》，以獲得有關 SecureConnector 的詳細資訊。</p> <p>當 SecureConnector 連接到設備或 Enterprise Manager 時，將重定向至其主機所指派的設備。請確認已向所有設備與 Enterprise Manager 開放此埠，以便組織內能獲得透明的行動性。</p>
13000/TCP	CounterACT	至	<p>允許控制台連接到本設備。</p> <p>對於具有多個 CounterACT 設備的系統，允許控制台連接到企業管理器以及企業管理器連接到每個設備。</p>

監視介面

此連接允許本設備監視和追蹤網路資訊流量。

資訊流量會鏡像至交換機的一個埠，由本設備進行監視。根據被鏡像的 VLAN 的數量，資訊流量可能有或沒有標記的 802.1Q VLAN。

- **單一 VLAN（無標記）：**如果監視的資訊流量是由單一的 VLAN 產生，鏡像的資訊流量則不需要是有標記的 VLAN。
- **多個 VLAN（有標記）：**如果監視的資訊流量是由一個以上的 VLAN 產生，鏡像的資訊流量則必須是有標記的 802.1Q VLAN。

當兩個交換機當成備援對連接時，本設備必須監視來自這兩個交換機的資訊流量。

監視介面不需要 IP 位址。

回應介面

本設備使用此介面對資訊流量做出回應。回應資訊流量用於防禦惡意活動和執行 NAC 政策行動。這些行動可能包含的範例有重定向網頁瀏覽器或執行防火牆阻攔。相關的交換機埠組態取決於要監測的資訊流量。

- **單一 VLAN（無標記）：**如果監視的資訊流量是由單一的 VLAN 產生，回應介面則必須組態成為相同 VLAN 的一部分。在此情況下，本設備需要該 VLAN 上的一個 IP 位址。
- **多個 VLAN（有標記）：**如果監視的資訊流量是來自一個以上的 VLAN，回應介面則必須組態具有相同 VLAN 的 802.1Q 標記。本設備對於每個受保護的 VLAN 都需要一個 IP 位址。

2. 設定交換機

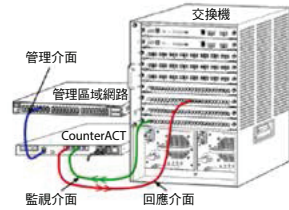
A. 交換機連接選擇

本設備的設計無縫整合至廣泛的網路環境中。若要將本設備成功整合至網路中，請驗證交換機是否設定用於監視所需資訊流量。

可選擇幾種方式將本設備連接到交換機。

1. 標準部署（單獨的管理、監視和回應介面）

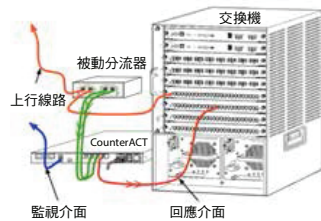
建議部署使用三個單獨的埠。關於這些埠的描述請參閱設備介面連接。



2. 被動內聯分流器

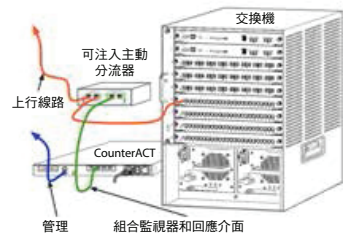
設備可使用一個被動內聯分流器來代替連接到一個交換機監視埠。

被動內聯分流器需要兩個監視埠，「重組」分流器除外，這會把兩個雙工流組合至一個埠。分流埠和回應介面的資訊流量必須以相同的方式組態。例如，如果分流埠的資訊流量是有標記的 VLAN (802.1Q)，那麼回應介面必須也是有標記的 VLAN 埠。



3. 主動（可注入）內聯分流器

當本設備使用可注入內聯分流器，可結合監視和回應介面。這不需要在交換機上組態一個單獨的回應介面。此選擇可用於任何類型的上游或下游交換機組態。



4. IP 層回應（適用於 3 層交換機裝置）

本設備可使用自己的管理介面對資訊流量做出回應。儘管此選擇可用於任何監視的資訊流量，但建議在本設備監視的埠不屬於任何 VLAN 時使用，這樣本設備不能使用任何其他交換機埠對監視的資訊流量做出反應。這種監視連接兩個路由器的鏈結是很普遍。

此選擇不能對位址解析協議 (ARP) 請求做出回應，這會限制本設備針對監視子網中的 IP 位址進行檢測掃描的能力。此限制不適用於監視兩個路由器之間的資訊流量。

B. 交換機設定說明

VLAN (802.1Q) 標記

- **監視單一 VLAN（無標記的資訊流量）** 如果監視的資訊流量來自單一的 VLAN，則資訊流量不需要 802.1Q 標記。
- **監視多個 VLAN（有標記的資訊流量）** 如果監視的資訊流量來自兩個或多個 VLAN，則監視和回應介面都必須啟用 802.1Q 標記。建議採用「監視多個 VLAN」選擇，因為它能在儘量減少鏡像埠的同時提供最佳的全面覆蓋。
- 如果交換機在鏡像埠上不能使用 802.1Q VLAN 標記，則執行下列步驟之一：
 - 只鏡像單一 VLAN
 - 鏡像單一沒有標記的上行線路埠
 - 使用 IP 層回應選擇
- 如果交換機只能鏡像一個埠，則鏡像單一行線路埠。這可能有標記。一般來說，如果交換機去除 802.1Q VLAN 標記，則需要使用 IP 層回應選擇。

其他說明

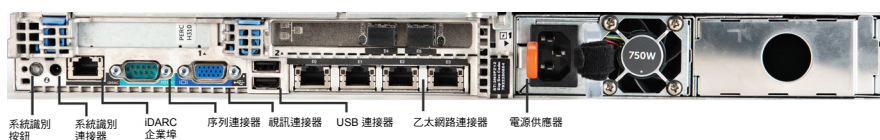
- 如果交換機對收/發資訊流量都無法鏡像，則需監視整個交換機、完整的 VLAN（提供收/發）或就一個介面（允許收/發）。請確認鏡像埠不會超載。
- 一些交換機（例如 Cisco 6509）在採用新組態前可能需要完全清除以前的埠組態。不清除舊埠資訊的最常見結果是交換機會去除 802.1Q 標記。

3. 連接網路線並開機

A. 拆除包裝並連接纜線

1. 將設備和電源線從包裝箱中取出。
2. 將設備隨附的導軌套件取出。
3. 將導軌套件安裝在設備上，然後將設備安裝在支架上。
4. 使用網路線連接設備後面板的網路介面與交換機埠。

後面板範例— CounterACT 裝置



B. 記錄介面分配

在資料中心完成設備安裝和安裝 CounterACT 控制台後，您將被提示記錄介面分配。當您首次登入控制台時，可在開啟的 Initial Setup Wizard（初始設定精靈）中輸入這些分配，稱為通道定義。

在下方記錄實體介面分配，並於控制台中完成通道設定時使用它們。

乙太網介面	介面分配 (例如，管理、監視、回應)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. 開啟設備電源

1. 使用電源線連接設備後面板的電源連接器。
2. 將電源線的另一端連接到接地的交流電插座。
3. 將鍵盤和監視器連接到設備上或設定設備的串列連接。請參閱 CounterACT 光碟上的《CounterACT 安裝指南》。
4. 從設備前面板開機。

重要資訊：拔插頭前必先關閉機器。

4. 組態設備

組態設備前，請準備以下資訊。

<input type="checkbox"/> 設備主機名稱	
<input type="checkbox"/> CounterACT 管理員密碼	將密碼儲存在安全位置
<input type="checkbox"/> 管理介面	
<input type="checkbox"/> 設備 IP 位址	
<input type="checkbox"/> 網路遮罩	
<input type="checkbox"/> 預設閘道 IP 地址	
<input type="checkbox"/> DNS 網域名稱	
<input type="checkbox"/> DNS 伺服器地址	

開機後，您將被以下訊息提示開始組態。

CounterACT 設備啟動完成。
按 <Enter> 繼續。

1. 按 **Enter** 顯示以下功能表：

1) 組態 **CounterACT**
2) 還原已儲存的 **CounterACT** 組態
3) 標識網路介面並重新編號
4) 組態鍵盤配置
5) 關機
6) 重新開機
選擇 (1-6) : 1

2. 選擇 **1** - 組態 **CounterACT**。出現提示時：

繼續：(是/否)？

按 **Enter** 開始設定。

3. 將開啟 **High Availability Mode** (高可用性模式) 功能表。按 **Enter** 選擇標準安裝。
4. 將顯示 **CounterACT Initial Setup** (CounterACT 初始設定) 提示。
按 **Enter** 繼續。
5. 將開啟 **Select CounterACT Installation Type** (選擇 CounterACT 安裝類型) 功能表。輸入 **1**，按 **Enter** 安裝標準 CounterACT 設備。設定將初始化。這可能需要一些時間。


6. 出現 **Enter Machine Description**（輸入機器描述）提示時，輸入標識該設備的簡短文字，按 **Enter**。
將顯示以下內容：

>>>>>> 設定管理員密碼 <<<<<<

此密碼用於以「根使用者」身份登入機器的作業系統和以「管理員」身份登入 CounterACT 控制台。

密碼應為 6 - 15 個字元，應包含至少一個非字母字元。

管理員密碼：

7. 出現 **Set Administrator Password**（設定管理員密碼）提示時，輸入密碼字串（不是螢幕的應答字串），然後按 **Enter**。您將被提示確認密碼。密碼必須為 6 - 15 個字元，應包含至少一個非字母字元。
 以使用者身份登入設備，以管理員身份登入控制台。
8. 出現 **Set Host Name**（設定主機名稱）提示時，輸入一個主機名稱，然後按 **Enter**。主機名稱可在登入控制台時使用，並顯示在控制台上，協助您識別正在查看的 CounterACT 設備。
9. **Configure Network Settings**（組態網路設定）螢幕會提示您輸入一系列組態參數。按照每個提示輸入一個值，按 **Enter** 繼續。
- CounterACT 元件透過管理介面通訊。列出的管理介面數量取決於設備型號。
 - **Management IP address**（管理 IP 位址）是 CounterACT 元件通訊介面的位址。只用於在連接到有標記埠的 CounterACT 元件之間通訊的情況下為此介面新增一個 VLAN ID。
 - 如果有一個以上的 **DNS 伺服器地址**，用空格隔開每個位址——大多數內部 DNS 伺服器可解析外部和內部位址，但您可能需要包含一個外部解析 DNS 伺服器。因為設備執行的所有 DNS 查詢幾乎都是內部位址，所以外部 DNS 伺服器應列在最後。
10. 將顯示 **Setup Summary**（設定摘要）螢幕。系統將提示您執行一般連接測試、重新組態設定或完成設定。輸入 **D** 完成設定。

授權

安裝後，您必須安裝 CounterACT 代表提供的初始展示授權。此授權在初始控制台設定時安裝。此初始展示授權具有一定天數的有效期。您必須在有效期結束前安裝一個永久授權。我們將透過電子郵件向您通知到期日。此外，控制台的 Appliances/ Devices（設備/裝置）窗格也會顯示關於到期日和授權狀態的資訊。

一旦您獲得了永久授權，ForeScout 授權伺服器會每天對它驗證一次。Device Details（裝置詳情）窗格會顯示授權提醒警告和違規。

達一個月不再有效的授權將被撤回。請參閱《CounterACT 安裝指南》瞭解更多關於授權的資訊。

網路連接要求

至少一個 CounterACT 裝置（設備或企業管理器）必須能夠存取網際網路。此連接被 ForeScout 授權伺服器用來驗證 CounterACT 授權。

無法完成延期驗證達一個月的授權將被撤回。CounterACT 會每天發送一封說明與伺服器有通訊錯誤的警告電子郵件。

5. 遠端管理

iDRAC 設定

整合戴爾遠端控制器 (iDRAC) 是一個整合伺服器系統解決方案，讓您可透過本地區域網路或網際網路遠端存取 CounterACT 設備/企業管理器，且不受位置/作業系統限制。使用此模組可執行 KVM 存取、開機/關機/重置和執行故障檢修與保養工作。

使用 iDRAC 模組執行以下任務：

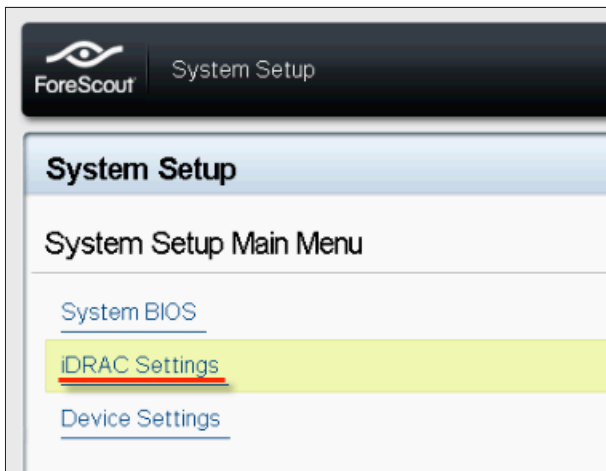
- 啟用和組態 iDRAC 模組
- 將模組連接至網路
- 登入 iDRAC

啟用和組態 iDRAC 模組

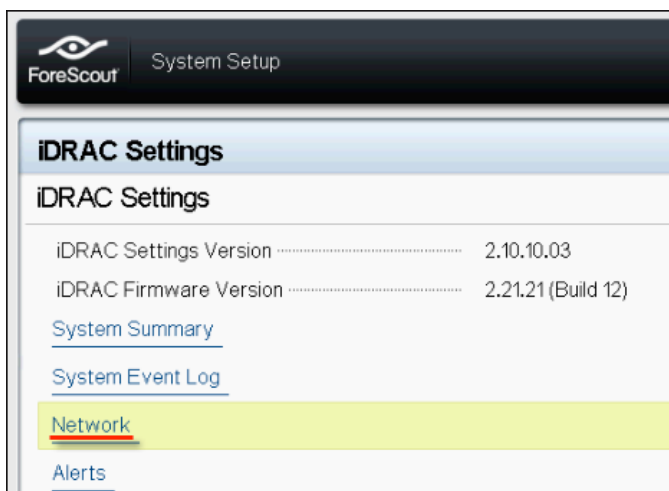
變更 iDRAC 設定，在 CounterACT 裝置上啟用遠端存取。此節描述了與 CounterACT 一起使用的所需基本整合設定。

組態 iDRAC：

1. 開啟受管理的系統。
2. 在開機自我測試 (POST) 時按 F2。
3. 在 System Setup Main Menu (系統設定主功能表) 頁面上，選擇 **iDRAC Settings** (iDRAC 設定)。

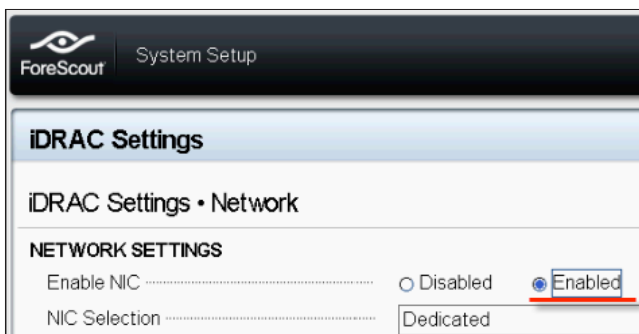


4. 在 iDRAC Settings (iDRAC 設定) 頁面上，選擇 **Network** (網路)。



5. 組態以下網路設定：

- **網路設定**。確認 **Enable NIC** (啟用 NIC) 欄位是否設定為 **Enabled** (啟用)。



- **普通設定**。在 DNS DRAC Name (DNS DRAC 名稱) 欄位中，您可以更新動態 DNS (可選)。

- **IPv4 設定**。確認 **Enable IPv4**（啟用 IPv4）欄位是否設定為 **Enabled**（啟用）。將 **Enable DHCP**（啟用 DHCP）欄位設定為 **Enabled**（啟用）使用動態 IP 位址分配或設定為 **Disabled**（禁用）使用靜態 IP 位址分配。如啟用，DHCP 會自動給 iDRAC 分配 IP 地址、網道和子網路遮罩。如禁用，在 **Static IP Address**（靜態 IP 地址）、**Static Gateway**（靜態網道）和 **Static Subnet Mask**（靜態子網路遮罩）欄位中輸入值。

ForeScout System Setup

iDRAC Settings

iDRAC Settings • Network

IPv4 SETTINGS

Enable IPv4	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Enable DHCP	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Static IP Address	192.168.1.103
Static Gateway	192.168.1.1
Static Subnet Mask	255.255.255.0
Use DHCP to obtain DNS server addresses	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Static Preferred DNS Server	192.168.1.2
Static Alternate DNS Server	0.0.0.0

- 選擇 **Back**（返回）。
- 選擇 **User Configuration**（使用者組態）。
- 組態以下使用者組態欄位：
 - **Enable User**（啟用使用者）。確認此欄位是否設定為 **Enabled**（啟用）。
 - **User Name**（使用者名稱）。輸入一個使用者名稱。
 - **LAN and Serial Port User Privileges**（本地區域網路和序列埠使用者許可權）。將許可權級別設定為 **Administrator**（管理員）。
 - **Change Password**（變更密碼）。設定使用者登入的密碼。

ForeScout System Setup Help | About | E...

iDRAC Settings

iDRAC Settings • User Configuration

User ID	2
Enable User	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
User Name	root
LAN User Privilege	Administrator
Serial Port User Privilege	Administrator
Change Password	

- 選擇 **Back**（返回），然後選擇 **Finish**（完成）。確認變更的設定。儲存網路設定後，重新啟動系統。

將模組連接至網路

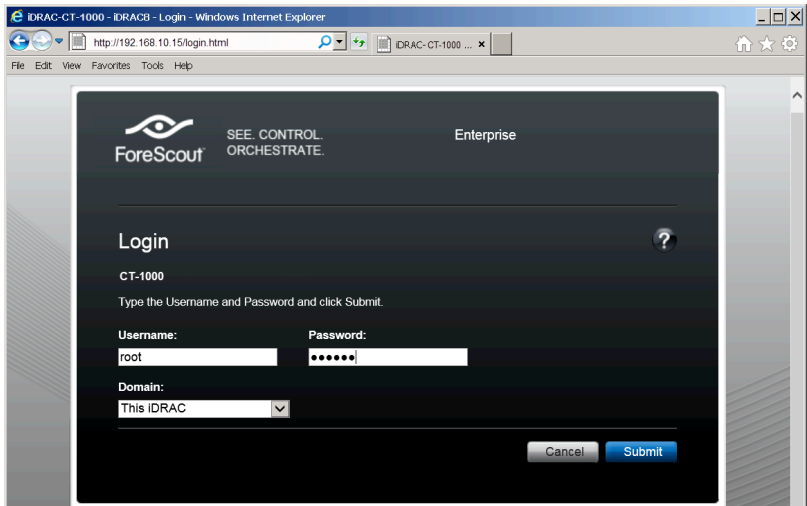
iDRAC 連接到乙太網網路。通常會將它連接到管理網路。下圖顯示了 CT-1000 設備後面板上的 iDRAC 埠位置。



登入 iDRAC

登入 iDRAC：

- 存取在 **iDRAC Settings**（iDRAC 設定）> **Network**（網路）中組態的 IP 位址或功能變數名稱。



- 輸入在 iDRAC 系統設定的 User Conguration（使用者組態）頁面中組態的使用者名稱和密碼。
- 選擇 **Submit**（提交）。

如需更多關於 iDRAC 的資訊，請參閱《[iDRAC 使用者指南](#)》。

更新預設憑據是重要。

6. 驗證管理介面連接

驗證管理介面連接

若要測試管理介面連接，登入設備，執行以下命令：

```
fstool linktest
```

將顯示以下資訊：

```
管理介面狀態
Ping 預設閘道資訊
Ping 統計資訊
執行功能變數名稱解析測試
測試摘要
```

驗證交換機/設備連接情況

離開資料中心前，請確認交換機已正確連接到設備。要執行此操作，在設備上為檢測的每個介面執行 `fstool ifcount` 命令。

```
fstool ifcount eth0 eth1 eth2
```

（以空格隔開每個介面）。

此工具持續顯示指定介面的網路資訊流量。它以兩種模式工作：按介面或按 VLAN。模式可在顯示幕中進行變更。顯示以下每個資訊流量類別的位元/秒和百分比：

- 監視介面應主要看到 90 % 以上的鏡像資訊流量。
- 回應介面應主要看到廣播資訊流量。
- 監視和回應介面應都能看到預期的 VLAN。

命令選項：

- v** - 以 VLAN 模式顯示
- I** - 以介面模式顯示
- P** - 顯示上一個
- N** - 顯示下一個
- q** - 退出顯示

VLAN 模式：

```
update=[4]      [eth3: 14 vlans]
Interface/Vlan  Total   Broadcast   Mirrored   *To my MAC   *From my MAC
eth3.untagged   4Mbps    0.2%        99.8%      0.0%         0.0%
eth3.1          9Mbps    0.0%        100.0%     0.0%         0.0%
eth3.2          3Mbps    0.1%        99.9%      0.0%         0.0%
eth3.4          542bps   100.0%      0.0%       0.0%         0.0%
eth3.20         1Kbps    100.0%      0.0%       0.0%         0.0%
Show [v]lans [i]nterfaces <-[p]rev [n]ext->      [q]uit
```

介面模式：

```
update=[31]      [eth0: 32 vlans] [eth1: 1 vlans]
Interface         Total   Broadcast   Mirrored   *To my MAC   *From my MAC
eth0              3Kbps   42.3%       0.0%       14.1%        43.7%
eth1              475bps  0.0%        100.0%     0.0%         0.0%
```

*To my MAC — 目標 MAC 是設備的 MAC。

*From my MAC — 從此設備發送的資訊流量（來源 MAC 是設備的 MAC。
目標可能是廣播或單播）。

如果您看不到任何資訊流量，請確認該介面是否啟動。在設備上使用以下命令：

ifconfig [interface name] up

執行 Ping 測試

從設備向網路桌面執行一個 Ping 測試來驗證連接情況。

執行測試：

1. 登入設備。
2. 執行以下命令：**Ping [network desktop IP]** 預設情況下，設備本身不回覆 Ping。

7. 設定 CounterACT 控制台

安裝 CounterACT 控制台

CounterACT 控制台是用於查看、追蹤和分析本設備檢查的活動的中央管理應用程式。可使用此控制台定義 NAC、威脅防護、防火牆和其他政策。請參閱《CounterACT 控制台使用者手冊》瞭解更多資訊。

您必須提供一部執行 CounterACT 主控台應用程式軟體的機器。最低的硬體要求為：

- 非專用的機器，並執行：
 - Windows XP、Windows Vista 或 Windows 7
 - Windows Server 2003 或 Server 2008
 - Linux
- Pentium 3, 1 GHz
- 2 GB 的記憶體
- 1 GB 的磁碟空間

執行控制台安裝有兩種方法：

使用設備內置的安裝軟件。

1. 從控制台電腦開啟瀏覽器視窗。
2. 在瀏覽器網址列輸入
http://<Appliance_ip>/install
<Appliance ip> 指此設備的 IP 位址。此瀏覽器顯示控制台安裝視窗。
3. 遵循螢幕上的指示。

從 CounterACT CD-ROM (唯讀光碟) 安裝

1. 將 CounterACT CD ROM (唯讀光碟) 插入 DVD (數位視訊影碟) 光碟器中。
2. 使用瀏覽器開啟 CD ROM (唯讀光碟) 中的 **ManagementSetup.htm** 文件。
3. 遵循螢幕上的指示。

登入

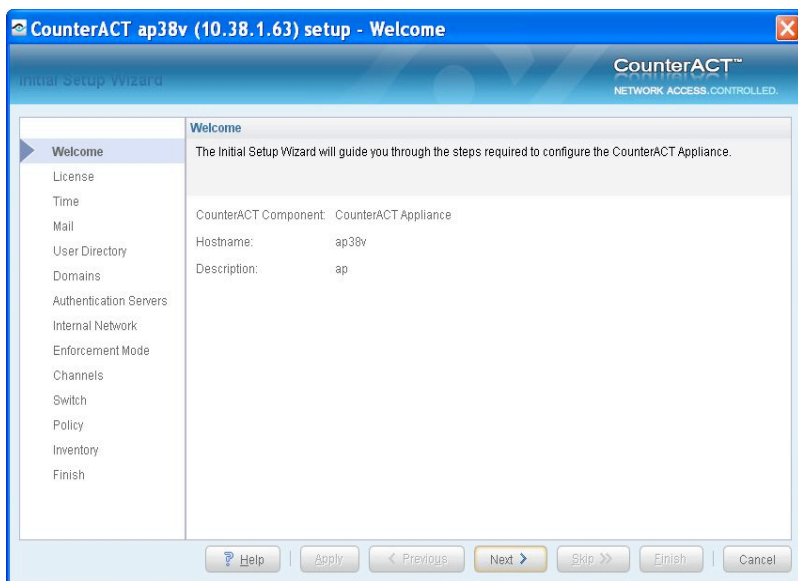
安裝完成後，您可登入 CounterACT 控制台。

1. 從建立的捷徑位置選擇CounterACT 圖示。
2. 在 **IP/Name**（IP/名稱）欄位中輸入設備的 IP 位址或主機名。
3. 在 **User Name**（使用者名稱）欄位中，輸入 **admin**。
4. 在 **Password**（密碼）欄位中，輸入在設備安裝過程中創建的密碼。
5. 選擇 **Login**（登入）啟動控制台。



執行初始設定

首次登入後，會顯示 Initial Setup Wizard（初始設定精靈）。本精靈將引導您完成必要的組態步驟，確保 CounterACT 快速有效地啟動執行。



開始初始設定前

使用此精靈前，請準備以下資訊：

資訊	值
<input type="checkbox"/> 您的組織使用的 NTP 伺服器位址（可選）。	
<input type="checkbox"/> 內部郵件轉送 IP 位址。如果設備不允許 SMTP 資訊流量，這可允許從 CounterACT 發送電子郵件（可選）。	
<input type="checkbox"/> CounterACT 管理員的電子郵件位址。	
<input type="checkbox"/> 在資料中心定義的監視和回應介面。	
<input type="checkbox"/> 對於沒有 DHCP 的網段或 VLAN，此網段或 VLAN 與監視介面直接連接，CounterACT 要對每個這樣的 VLAN 使用一個永久 IP 位址。企業管理器設定不需要此資訊。	
<input type="checkbox"/> 設備將保護的 IP 位址範圍（所有內部位址，包含未使用的位址）。	
<input type="checkbox"/> 使用者目錄帳戶資訊和使用者目錄伺服器 IP 地址。	
<input type="checkbox"/> 域證書，包含域管理帳戶名和密碼。	
<input type="checkbox"/> 驗證伺服器，使 CounterACT 可分析哪些網路主機得到成功驗證。	
<input type="checkbox"/> 核心交換機 IP 地址、供應商和 SNMP 參數。	

請參閱《CounterACT 控制台使用者手冊》或線上幫助瞭解使用此精靈的資訊。

聯絡資訊

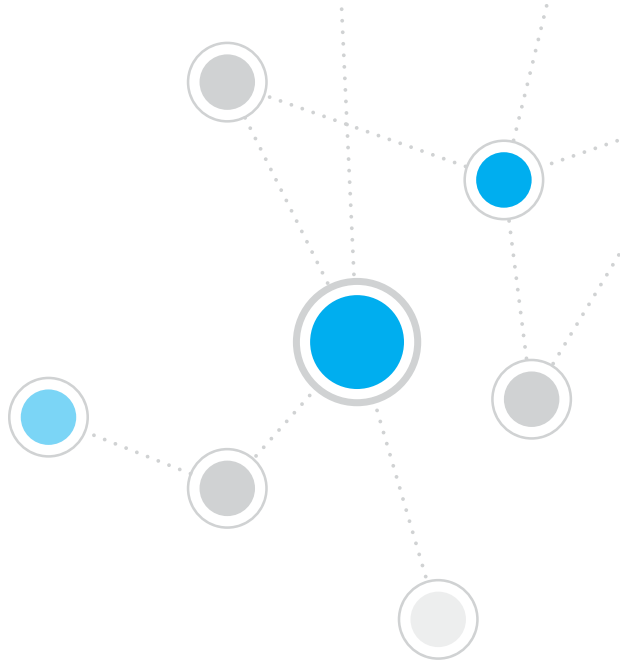
如需 ForeScout 技術支援，請發送郵件至 support@forescout.com 或致電。

- 免費電話（美國）：1.866.377.8771
- 電話（國際）：1.408.213.3191
- 支援：1.708.237.6591
- 傳真：1.408.371.2284

©2016 ForeScout Technologies, Inc. 產品受美國專利保護：#6,363,489、
#8,254,286、#8,590,004 和 #8,639,800。保留所有權利。

ForeScoutTechnologies 和 ForeScout 標誌是 ForeScout Technologies, Inc
的商標。所有其他商標為各自所有人所有。

使用任何 ForeScout 產品均應遵守 www.forescout.com/eula 上的 ForeScout
終端使用者許可協定的條款。



ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

免費電話（美國）：+1.866.377.8771

電話（國際）：+1.408.213.3191

支援：+1.708.237.6591

傳真：+1.408.371.2284

400-00020-01