Cisco Prime IP Express的自帶裝置功能 — 白皮書

目錄

簡介

本白皮書介紹Cisco Prime IP Express(CPUBE)系統的BYOD功能的功能和配置。Cisco Prime IP Express BYOD註冊門戶是一個易於處理的自助服務Web門戶，用於註冊和管理裝置。它與Cisco Prime IP Express的DHCP、CDNS整合。詳細記錄了該系統所需的方法、架構和BYOD配置。您可以使用此白皮書作為指南，配置BYOD以註冊和管理裝置。

問題陳述

所有IP網路都面臨一組常見問題。這些與波士頓學院在開發其自動化Internet登入系統之前所面臨的類似，例如，需要：

- 為電腦提供使用者驅動的手動配置，以及正確的IP地址和網路設定。
- 在短時間內配置大量電腦
- 獲取有關網路上正在配置的電腦的資訊
- 控制對IP網路資源的訪問

- 收集資訊以幫助對網路和安全事件進行故障排除

BYOD功能 — 功能概述

您可以使用Cisco Prime IP Express系統的BYOD功能解決上面提到的每一個問題，因為它為員工提供全面的解決方案，讓他們以管理良好且安全的方式使用自己支援IP的裝置。它有效地消除了IT管理員在載入和跟蹤個人和公司裝置方面的挑戰。此功能的一些優勢包括：

- 提供使用者驅動的手動裝置配置，以及正確的IP地址和網路設定。
- 在短時間內配置大量裝置。
- 獲取有關網路上正在配置的裝置的資訊。

當使用者首次嘗試連線BYOD裝置時，Cisco Prime IP Express DHCP網路會自動將使用者重定向到BYOD註冊門戶，因為使用者必須使用現有的Active Directory憑證註冊其裝置。在註冊期間，通過自動檢測或手動輸入來捕獲有關使用者裝置的資訊，如其MAC地址/DUID和其他後設資料。此資訊用於將使用者對映到其裝置並跟蹤IP活動以進行稽核和合規性。BYOD註冊門戶與Cisco Prime IP Express的DHCP整合。

使用者的觀點：

BYOD功能提供簡單的流程，使終端使用者能夠啟用裝置並訪問Cisco Prime IP Express(CTPE)網路。具體步驟如下：

- 將裝置連線到網路
- 從瀏覽器請求http
- 您將自動重定向到BYOD註冊頁面
- 註冊頁面會填充裝置詳細資訊並提示您輸入使用者憑據
- 提供憑證，如使用者名稱、密碼
- 接受服務條款
- 按一下註冊按鈕
- 等待幾秒鐘，裝置將重新啟動。

此過程通常只需大約三分鐘。完成後，將啟用裝置並在DHCP伺服器中建立客戶端。

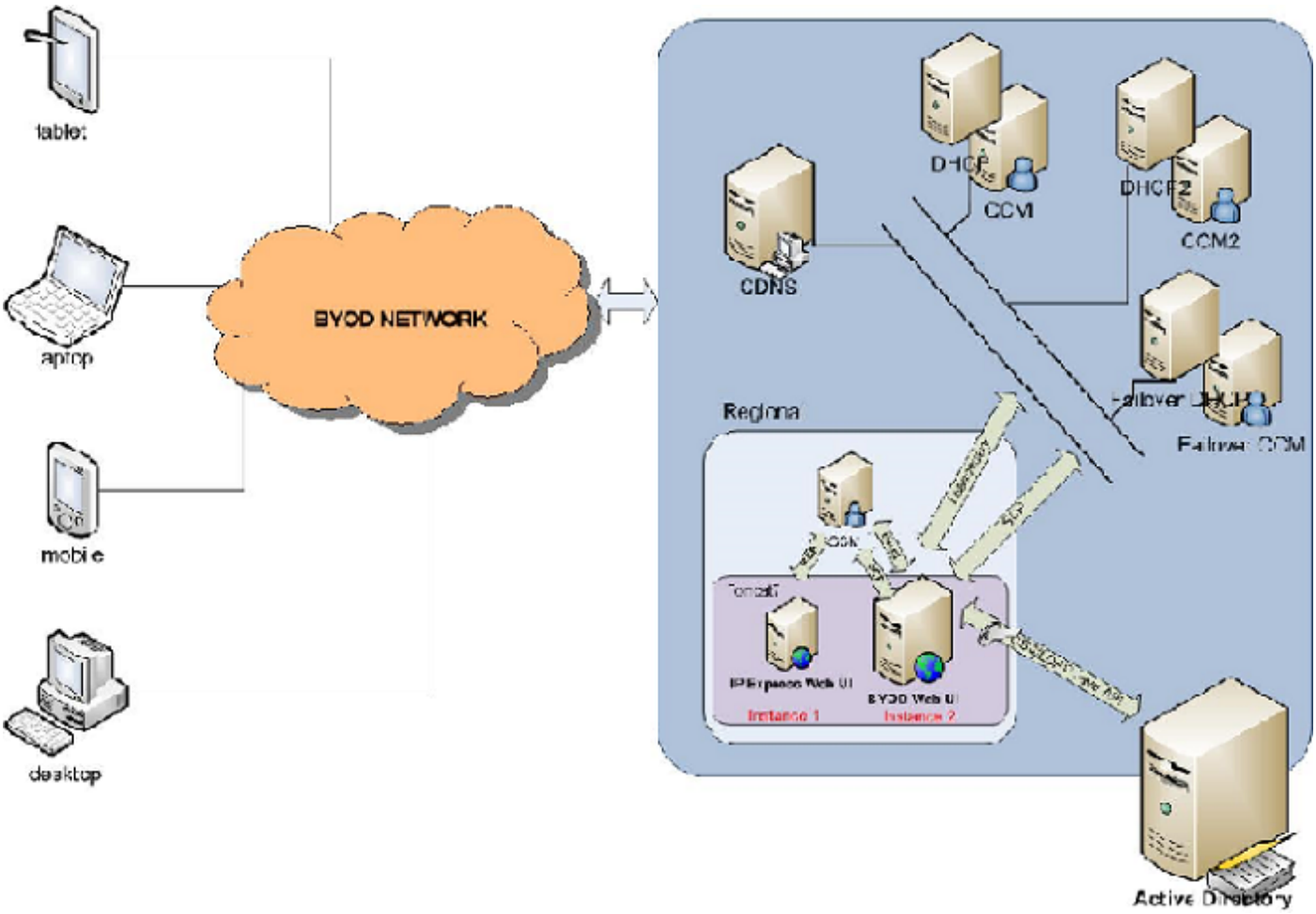
管理員的觀點：

此系統是一個易於使用的自助服務Web門戶，取代了許多耗時且容易出錯的過程。該自助服務系統的管理非常簡單。

- 安裝Cisco Prime IP Express Web Server
- 配置BYOD（DHCP、CDNS伺服器）
- 指導使用者如何註冊其裝置
- 指導使用者如何使用使用者登入頁面管理裝置

功能架構

該功能的架構至少需要四個主要元件：本地DHCP伺服器、CDNS伺服器、區域伺服器和Active Directory。在區域伺服器中，運行新的tomcat例項以支援BYOD。標準CDNS伺服器配置有帶ACL清單的域重定向規則，這可確保從特定地址範圍的所有HTTP查詢解析為BYOD Web伺服器地址。下面顯示了功能體系結構圖。



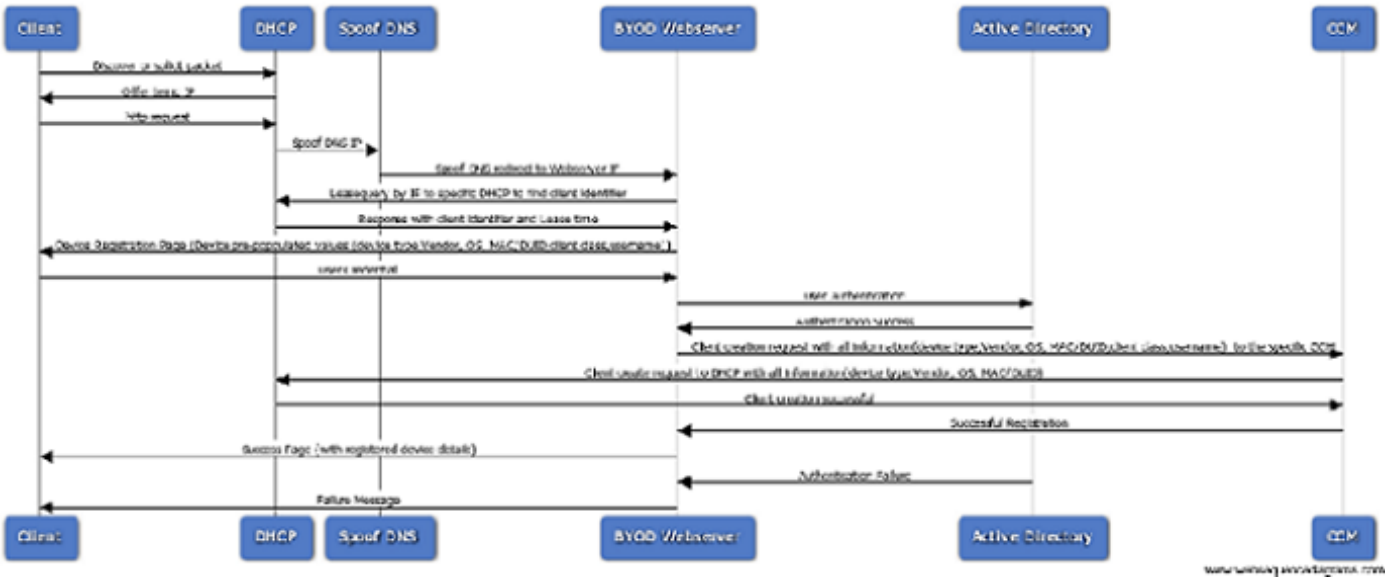
流程

下圖描述當使用者/客戶端將BYOD連線到網路時Web UI的流程。

- 當客戶端將新裝置連線到網路時，DHCPDISCOVER/SOLICIT資料包將傳送到DHCP。
- DHCP提供臨時IP並返回選項6（對於DHCPv4）或選項23（對於具有CDNS伺服器地址的DHCPv6）。
- 客戶端向CDNS伺服器傳送DNS解析查詢。
- CDNS域重定向規則為未註冊的BYOD裝置提供BYOD Web伺服器IP，並重定向到裝置註冊頁面。
- BYOD Web伺服器從http報頭資料獲取客戶端IP，並檢查匹配的子網/字首以查詢客戶端DHCP伺服器地址。
- 如果未找到匹配的子網/字首，則將SCP請求傳送到區域CCM以查詢為該客戶端提供服務的

DHCP伺服器，並更新BYOD記憶體中的子網/字首資訊。

- 將帶有地址的租賃查詢（根據RFC 4388 for DHCPv4和根據RFC 5007 for DHCPv6）傳送到相應的DHCP伺服器以獲取客戶端識別符號（裝置ID），並在裝置註冊頁面中填寫其他詳細資訊，如裝置供應商、作業系統等。
- 客戶端提供Active Directory憑證並提交登入表單。
- BYOD Web伺服器根據Active Directory對憑證進行身份驗證。
- 在身份驗證成功時，BYOD Web伺服器將SCP請求傳送到DHCP群集或故障轉移對，以便在DHCP客戶端資料庫中建立客戶端條目（客戶端類名稱、身份驗證截止時間、裝置型別、供應商、作業系統、MAC/DUID、使用者名稱）。如果已配置LDAP，則只會在LDAP資料庫中建立客戶端。
- 最後，BYOD Web伺服器向客戶端傳送成功註冊消息，其中包含他/她註冊的所有裝置的詳細資訊。
- 如果身份驗證失敗，BYOD Web伺服器將用失敗身份驗證消息回應要求客戶端。



BYOD配置

要構建支援BYOD功能的系統，您必須修改Cisco Prime IP Express配置的出廠設定以啟用伺服器的一些高級功能。您可以使用Cisco Prime IP Express區域伺服器中的BYOD設定嚮導輕鬆完成此過程（BYOD配置設定）。

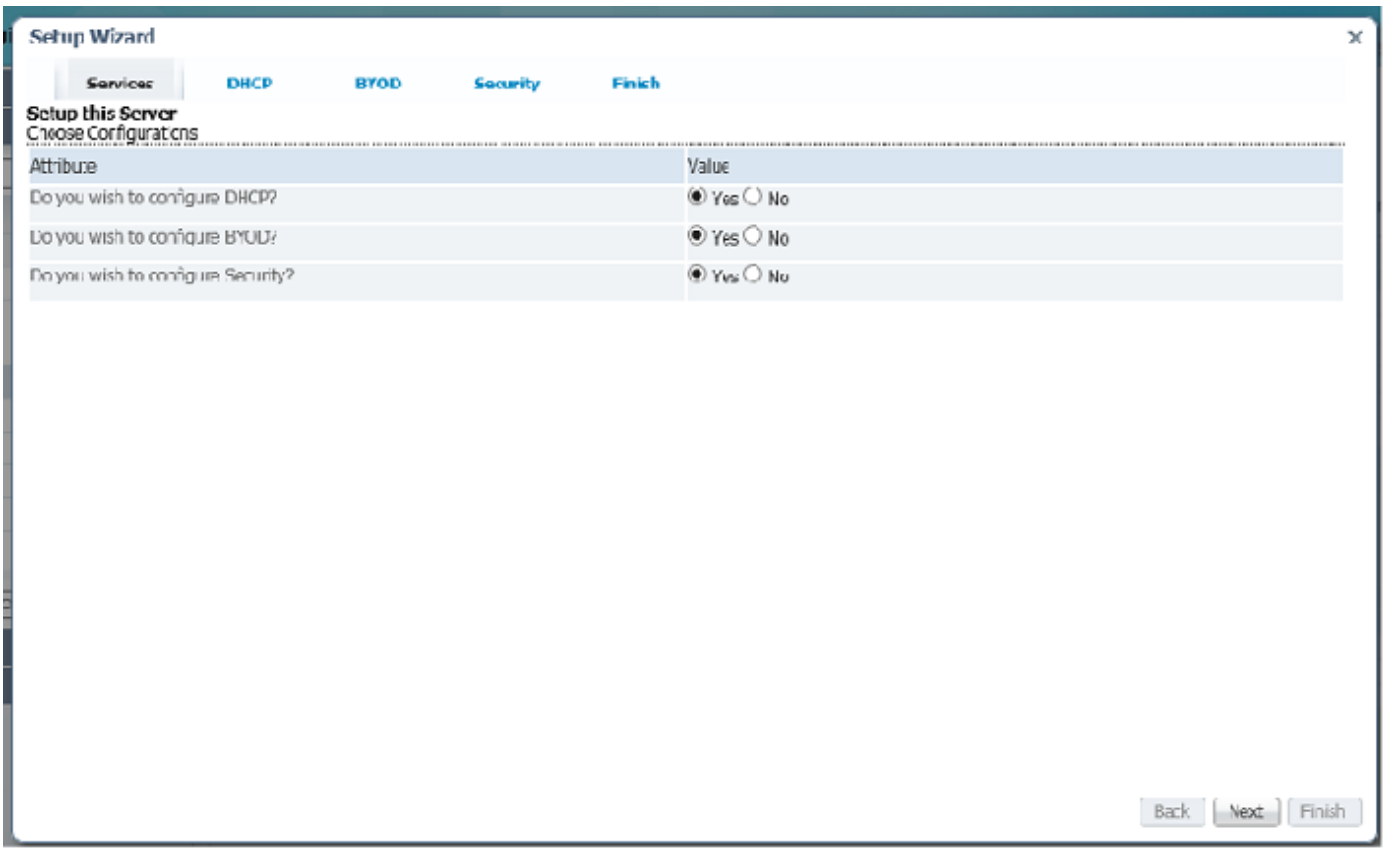
有關如何安裝Cisco Prime IP Express的資訊，請參閱《Cisco Prime IP Express安裝指南》。

有關如何使用GUI的詳細資訊，請參閱《快速入門手冊》和《使用手冊》。

您可以在以下位置找到所有其他Cisco Prime IP Express生產文檔：http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-ip-express/tsd-products-support-series-home.html

BYOD安裝嚮導

以下各節介紹Cisco Prime IP Express區域伺服器中的BYOD設定嚮導工作流程。整個過程包括配置DHCP和CDNS伺服器。對於簡單的設定，預設客戶端用於未註冊的自帶裝置裝置，而對於複雜的設定；使用client-class-lookup-id和client-lookup-expression。詳細資訊在使用者文檔/部署指南中提供。



DHCP配置

要配置DHCP伺服器，請完成以下步驟：

- 為故障切換選擇值No。
- 為DHCPv4選擇值Yes。
- 為DHCPv6選擇值No，然後按一下Next。
- 「DHCPv4設定嚮導」頁面開啟。
- 按一下新增範圍模板以建立範圍。
- 在「名稱」框中輸入作用域模板名稱，然後按一下「新增DHCP作用域模板」按鈕。
- 按一下「儲存」以儲存範圍模板，然後按一下「下一步」移動到下一頁。
- 在Scope Name Expression文本框中輸入（與「byod — 」子網相關）。
- 在「範圍表達式」文本框中輸入(create-range first-addr last-addr)，然後按一下「儲存」以儲存頁面。按「Next」（下一步）。
- 按一下新增子網以建立子網。

- 在地址文本框中輸入子網IP，例如10.76.206.0，然後按一下新增子網按鈕。
- 按一下「推送」圖示將子網推送到本地群集。
- 從Cluster或Failover下拉選單中，選擇要將子網推入的本地群集主機名。
- 從Scope Template下拉選單中選擇範圍模板。
- 按一下「按子網」按鈕。
- 按一下下一步轉到「BYOD設定」頁。

BYOD配置

您可以使用「BYOD設定」頁面捕獲有關建立域重定向規則（欺騙DNS）的CDNS伺服器配置的詳細資訊以及未註冊裝置的租用時間。

1. 下面提到的策略和客戶端類是在區域伺服器中建立的，並在安裝嚮導頁面中進一步使用：BYOD策略名稱：BYOD_Unregistered。新增DHCPv4 dhcp-lease-time選項(51)並設定DHCPv6 valid-lifetime和preferred-lifetime。為DHCPv4選擇域名伺服器選項6，為DHCPv6選擇選項23。BYOD客戶端類名稱：BYOD_Registered設定排除的選擇標準 — BYOD_Unregistered。BYOD客戶端類名稱：BYOD_Unregistered。設定選擇條件 — BYOD_Unregistered。Set Policy -BYOD_Unregistered。
2. 要配置BYOD，請執行以下步驟……從下拉選單中選擇CDNS伺服器。指定未註冊的客戶端的時間，然後按一下按一下「下一步」，轉到「策略」頁。按一下推送圖示，從「可用」清單中選擇本地群集主機名，使用後退箭頭將其新增到目標群集，然後按一下「將資料推入群集」按鈕。按一下「關閉」按鈕關閉「檢視推送資料包表」。按一下下一步以移動到「客戶機類」頁，按一下推送圖示，然後按一下將資料推送到集群按鈕。通過按一下「關閉」按鈕關閉「檢視推送資料包告」，然後按一下「下一步」轉到「範圍建立」頁。在值下的文本框中指定百分比，以定義未註冊客戶端的IP範圍。預設情況下，值為10。按一下「下一步」轉到「報告」頁，此頁顯示分配給特定客戶端的IP範圍以及其他詳細資訊，如範圍、集群、子網和IP範圍，如下圖所示。按一下「下一步」轉到https配置頁面。

區域伺服器 — Https配置

安裝嚮導頁面可用於Https配置；自帶裝置Web伺服器需要這些詳細資訊。

要配置Https，請執行以下步驟：

- 使用「選擇檔案」按鈕上傳Keystore檔案，並在「Keystore密碼」文本框中輸入金鑰庫密碼，按一下「上傳」按鈕，然後按一下「下一步」轉到「重新載入伺服器頁面」。

重新載入伺服器

配置完成後，可以使用重新載入伺服器頁面重新載入DHCP伺服器、CDNS伺服器和BYOD Web伺服器，

為此，請遵循以下步驟：

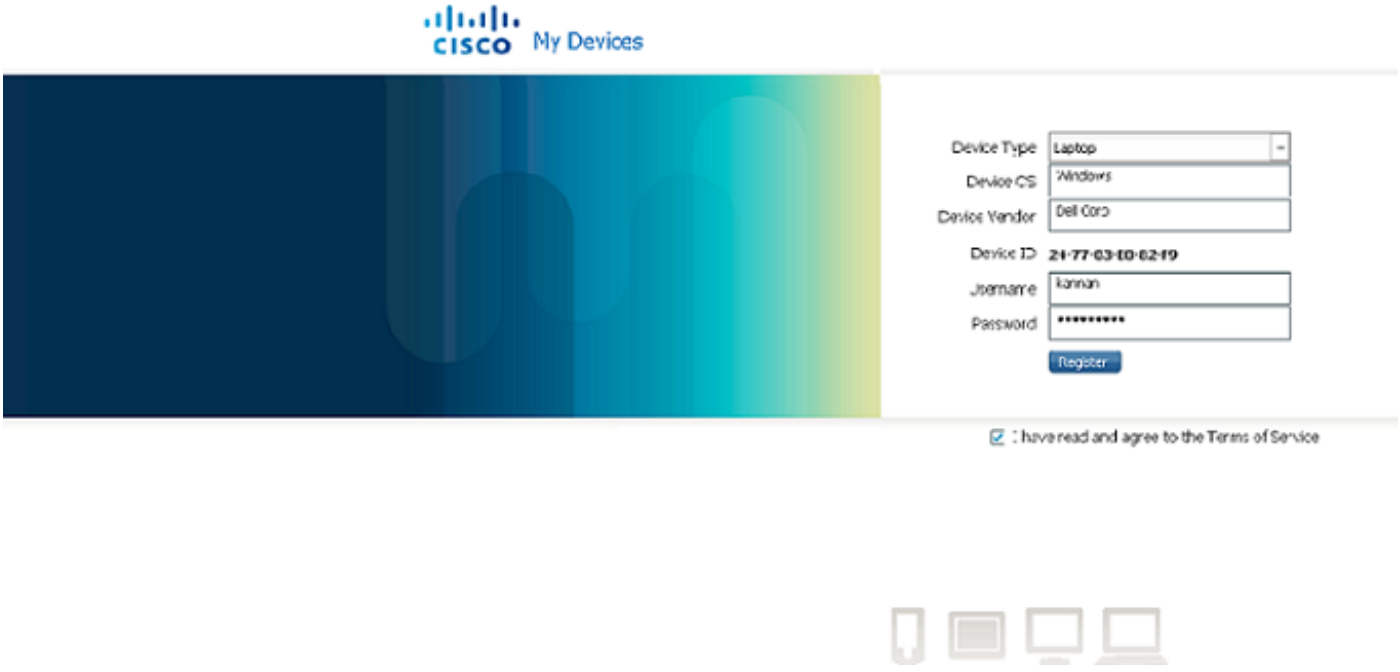
- 在「是」或「否」中指定值以重新啟動BYOD Web伺服器、CDNS Web伺服器和DHCP伺服器/故障轉移對，按一下「重新載入伺服器」按鈕，然後按一下「下一步」，將開啟「安全」頁。
- 從Value下拉選單中選擇身份驗證型別值Active Directory。
- 按一下「儲存並下一步」並移動到「Active Directory頁」，然後按一下「儲存」。
- 在各自的文本框中輸入IP地址、主機名和埠，例如IP=10.76.206.5、hostname= tmh2-chn-cnrent-AD1和埠= 389，然後按一下新增地址。
- 在「域」文本框中輸入域名CPIPE.COM。
- 按一下「下一步，成功配置頁面」開啟。按一下「完成」完成配置設定過程。

裝置註冊頁面

Device registration page允許使用者註冊其裝置。在此頁面中，某些欄位（如裝置型別、裝置作業系統、裝置供應商和裝置/MAC ID）已預先填充，並且允許使用者編輯詳細資訊。但是，使用者需要輸入其憑證，例如：

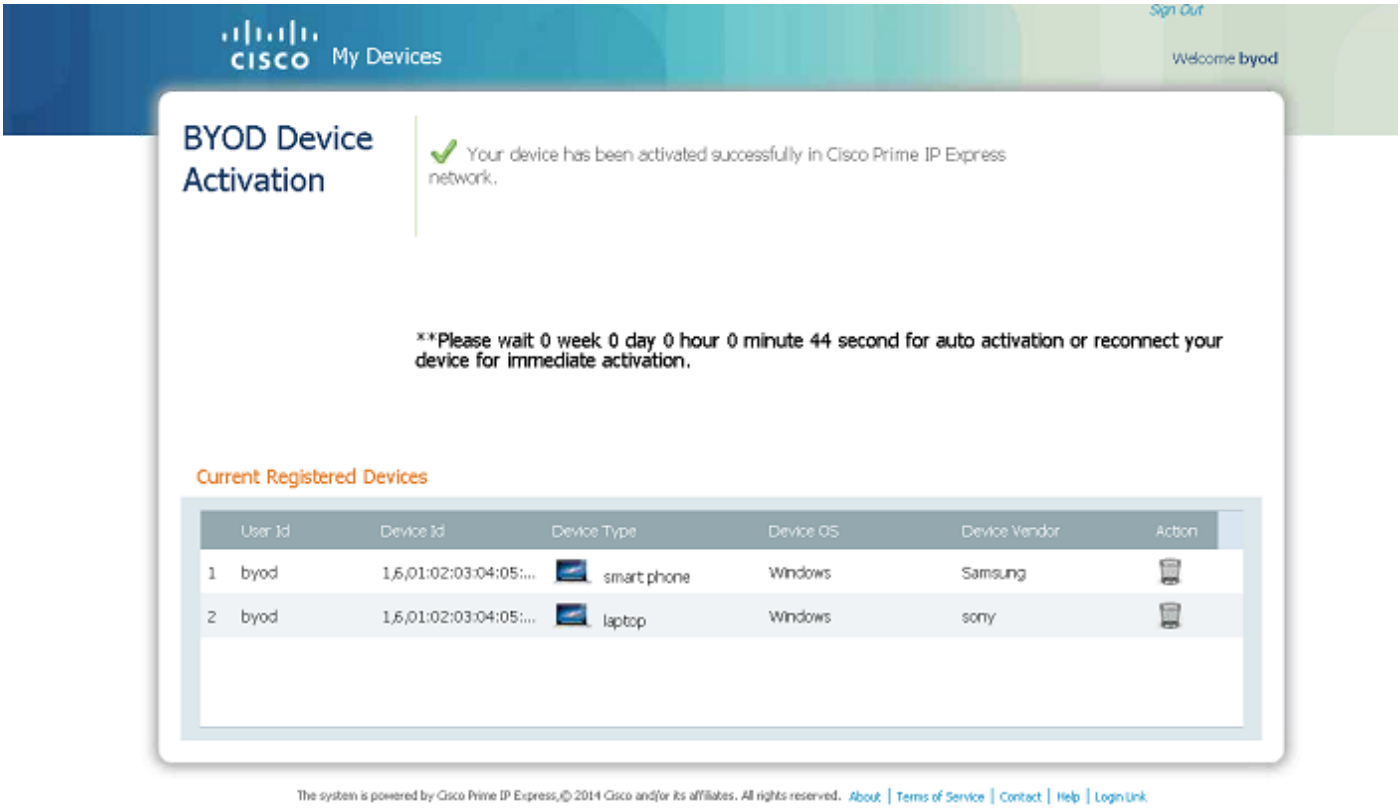
頁面

- 使用者名稱
- 密碼
- 服務條款



啟用成功頁

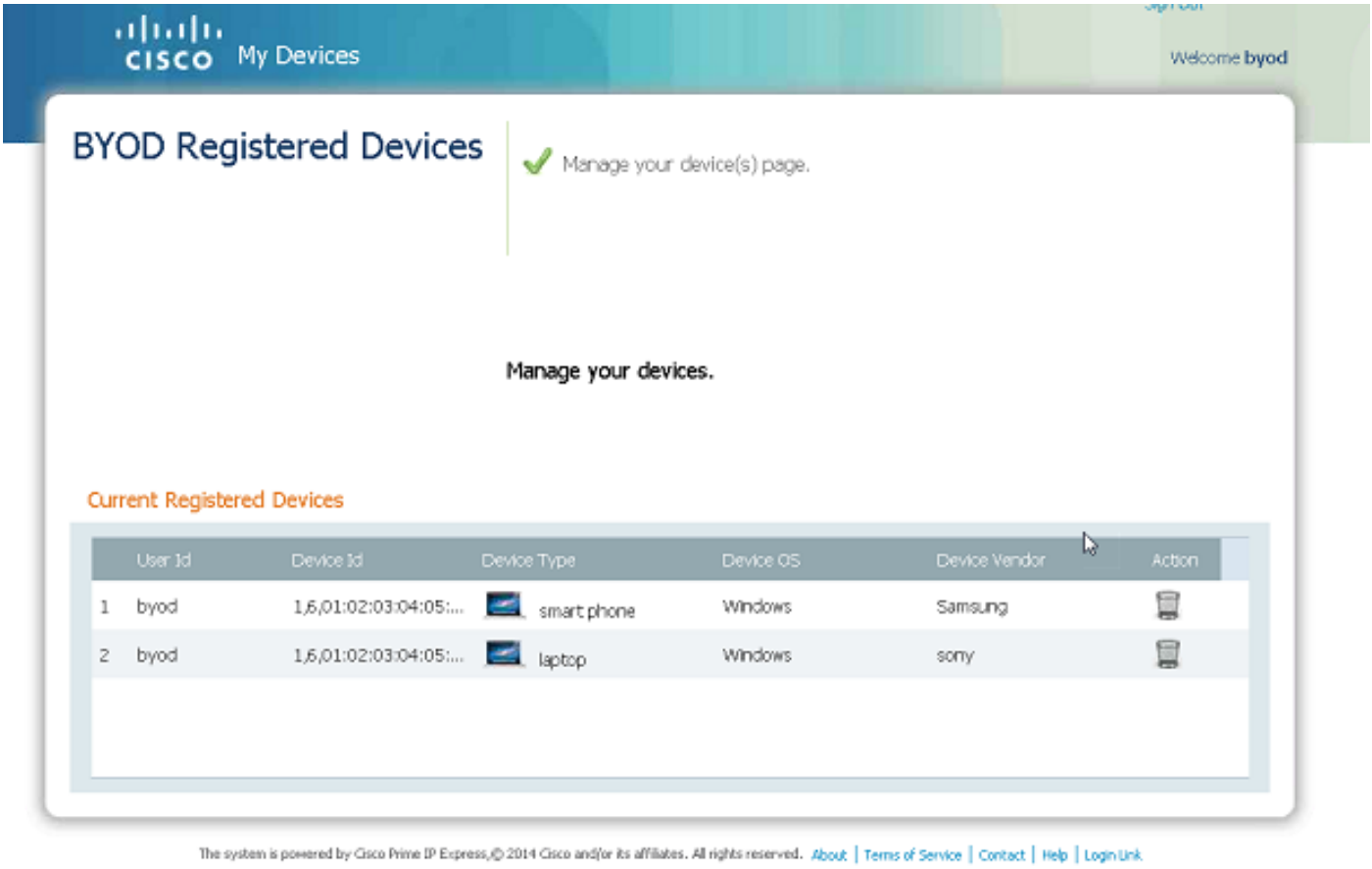
成功註冊後，啟用成功頁面將顯示包含自動啟用的租用時間的消息以及立即生效的重連線消息，如下圖所示。啟用成功頁面還顯示同一使用者的當前和先前註冊裝置的清單。使用者可通過按一下刪除圖示刪除裝置。



用於管理裝置的使用者登入頁

使用者登入頁面允許使用者刪除其註冊裝置。要登入到「使用者登入」頁面，使用者需要提供其登入憑證（如使用者名稱、密碼），還需要接受服務條款。成功登入後，將開啟BYOD註冊裝置頁面。此頁用於管理註冊裝置，如刪除裝置。

- 使用者名稱
- 密碼
- 服務條款



查詢表達式

查詢表達式標識裝置是現有裝置還是未註冊裝置。它確定DHCP伺服器的client-class-lookup-id屬性的客戶端類，並且伺服器在每個傳入資料包上執行此表達式，以確定資料包的客戶端類。它根據指定的表達式值返回一個字串（資料包的client-class名稱，或指示客戶端請求未考慮任何client-class值的區分字串）。「查詢」表達式用於確保每個客戶端通過同一網路接收其相應的服務類別。

設定查詢表達式

配置BYOD後，可通過以下步驟設定查詢表達式：

- 按一下Expert進入Expert模式。
- 「開啟清單/新增DHCP客戶機類」頁，(導航：設計> DHCP設定>客戶端類)
- 在左側的「客戶端類」窗格中建立或選擇已建立的類。
- 在「編輯DHCP客戶端類」建立的客戶端頁的「建立新的嵌入式策略」下，在client-lookup-id和override-client-id中輸入expression，例如，在client-lookup-id文本框中輸入request option "relay-agent-info" "remote-id"，在override-client-id文本框中輸入request option "relay-agent-info" "remote-id")。
- 按一下儲存以儲存設定。
- 開啟「管理伺服器」頁(導航：操作>伺服器>管理伺服器)
- 在左側的Manage Servers窗格中按一下Local DHCP Server連結。

- 點選Edit Local DHCP Server頁籤。
- 在client-class-lookup-id文本框中輸入建立的客戶機類名稱。
- 重新啟動本地DHCP伺服器以使這些更改生效。

LDAP客戶端建立支援

當使用LDAP客戶端選項啟用IP Express DHCP伺服器時，BYOD Web伺服器啟用「LDAP客戶端建立」支援。

如果DHCP伺服器在LDAP中啟用客戶端查詢，則BYOD需要區域伺服器LDAP配置才能在LDAP中建立客戶端。

要在區域伺服器中建立和配置LDAP客戶端，請按照以下步驟操作：

- 按一下Expert進入Expert模式。
- 開啟「清單/新增LDAP遠端伺服器」頁，(導航：部署> DHCP > LDAP)
- 按一下左側的LDAP窗格中的Add LDAP圖示，將開啟Add DHCP LDAP Server視窗。
- 在名稱和主機名文本框中輸入LDAP名稱和主機名，然後按一下新增DHCP LDAP伺服器。在左側的LDAP窗格中新增DHCP LDAP伺服器，該伺服器具有給定的名稱。
- 按一下左側的LDAP窗格中新新增的LDAP連結，「編輯LDAP遠端伺服器」(Edit LDAP Remote Server)頁面開啟，在此頁面中，名稱和主機名將自動填充。
- 在相應的文本框中輸入addr、埠值以及使用者名稱和密碼。
- 將「enable」的值設定為True。
- 設定「可以建立」的值。
- 設定「can-query」的啟用值。
- 設定啟用的「can-update」的值。
- 在查詢下，輸入「搜尋路徑」值。
- 在查詢下，輸入「搜尋路徑」值。
- 在「查詢」下，保留「search-scope」的預設值SUBTREE
- 在建立設定下，輸入「dn-create-format」值
- 在建立設定下，輸入「create-dictionary」值
- 在建立設定下，輸入create-object-classes值
- 按一下儲存以儲存設定。
- 開啟「管理伺服器」頁。(導航：操作>伺服器>管理伺服器)

- 按一下左側的Manager Servers窗格中的Local BYOD Web Server連結。
- 通過按一下「重新啟動伺服器」圖示重新啟動本地BYOD Web伺服器以使更改生效。

DHCP指紋

DHCP指紋是用於識別特定作業系統或裝置型別的唯一識別符號。

BYOD Web伺服器讀取「dhcp_fingerprint.conf」，它包含指紋(PRL)和作業系統說明的「雜湊對映」。

通過DHCPv4租用查詢應答，BYOD Web伺服器獲取租用的使用者定義屬性值，並查詢適當的OS（說明值）和OS編號。使用作業系統編號可以找到相應的類定義，類的說明將提供裝置型別資訊。

如果無法使用指紋檔案識別作業系統供應商和裝置型別，則使用http標頭使用者代理資料。模式匹配是使用具有作業系統清單的主檔案完成的。

要配置DHCP指紋，請按照以下步驟操作：

- 按一下Expert進入Expert模式。
- 開啟「清單/新增DHCP擴展」頁，(導航：部署> DHCP >擴展)
- 按一下左側的Extensions窗格中的Add Extensions圖示，將開啟Add DHCP Server Extension視窗。
- 在相應的文本框中輸入副檔名「name」、「lang」、「file」和「entry」值。
- 按一下Add DHCP Server Extension（新增DHCP伺服器擴展），然後按一下Save（儲存）儲存設定，新增新的擴展。
- 按一下左側的Add Extension窗格中的Extension連結，此時將開啟Edit DHCP Extension頁。
- 按一下右側的「附加擴展點」圖示，此時將開啟「擴展點」視窗，如下圖所示。
- 在Attach Extension Points下，選擇post-packet-decode，然後按一下Save（儲存），如下圖所示。
- 或者按一下DHCP Extension Points頁籤，然後針對「post-packet-decode」選擇Attach下拉選單。 此視窗也可用於斷開連線的擴展連線。
- 開啟「管理伺服器」頁，(導航：操作>伺服器>管理伺服器)
- 按一下左側的Manager Servers窗格中的Local DHCP Server連結。
- 通過按一下「重新啟動伺服器」圖示重新啟動本地DHCP伺服器以使更改生效。

附註：只能在本地伺服器中配置指紋。

主題配置

此頁面允許BYOD管理員通過編輯主題屬性（如特定顏色或顏色代碼以及徽標/背景影象）來編輯

BYOD網頁的外觀和感覺，以與其自己的品牌相匹配。

有兩種型別的主題：不可自定義的預設思科主題和其他是可自定義的主題。

要配置主題，請按照以下步驟操作：

- 按一下Expert進入Expert模式。
- 開啟清單/新增自定義主題頁面，(導航：部署> BYOD >主題)
- 按一下左側主題窗格中的「新增主題」圖示，將開啟「新增自定義主題」視窗。
- 在相應的文本框中輸入主題名稱、背景顏色、登入頁面標題字型顏色和頁面標題字型顏色。
- 按一下「新增自定義主題」，將開啟包含您提供的詳細資訊的下一頁。

附註：您可以使用此頁面上載背景影象、通用頁面標題影象、登入頁面徽標和通用頁面徽標。

- 按一下Background Image Browse按鈕，然後按一下Upload以上傳背景影象。
- 重複相同步驟以上傳公用頁標題影象、登入頁日誌和公用頁徽標影象。
- 按一下儲存以儲存設定。

內容頁面

Content頁面允許BYOD管理員配置消息，如註冊/登入頁面消息、關於內容、服務條款、聯絡人和特定於客戶的幫助。

使用者輸入內容並提交或上傳(.html)檔案（表格）時。 它為BYOD Web內容目錄內的每個屬性生成具有特定檔名的特定html檔案，並且內容連結指向特定html檔案。

輸入的內容放置在html段落標籤之間，以確保內容以與輸入內容相同的格式顯示。

要配置內容頁面，請按照以下步驟操作：

- 按一下Expert進入Expert模式。
- 開啟內容頁面，(導航：部署>BYOD >內容)
- 在各自的文本框中輸入「註冊/登入頁面消息內容」、「關於內容」、「服務條款內容」、「聯絡內容」和「幫助內容」的內容。
- 或者按一下相應的瀏覽和載入按鈕以匯入內容。
- 按一下儲存以儲存設定。

IPS簽名提示

下面給出的清單描述了整個文檔中使用的術語的首字母縮寫。

自帶裝置：自帶裝置

AD:Active Directory

管道：Cisco Prime IP Express

DHCP:動態主機設定通訊協定

CDNS:快取域名系統

ACL:訪問控制清單

SCP:系統配置協定

CCM:中央組態管理員

RFC:指令請求

DUID:DHCP唯一識別符號

LDAP:輕量型目錄存取通訊協定