軟體定義的存取網狀架構佈建

規範性部署指南

2019 年 7 月

目錄

定義和設計：軟體定義存取 3
部署：SD-Access 網狀架構 4
程序：使用 Cisco DNA 中心進行初始網路設計和探索 6
程序：為 SD-Access 網路建立分段和原則 16
程序：為網路管理自動化做好準備 19
程序：佈建用於 SD-Access 的底層網路 31
程序：佈建 SD-Access 重疊網路 38
程序：將 SD-Access 無線整合到網狀架構中 52
附錄 A：產品清單 61
意見回饋 64

定義和設計：軟體定義存取

Cisco® 軟體定義存取 (SD-Access) 是從傳統園區區域網路設計，演變為直接實施組織意向的網路。SD-Access 須隨應用程式套件一併啟用，該應用程式套件以作為 Cisco DNA 中心軟體的一部分來執行，可用於設計、佈建和套用原則，並方便建立具有可靠性的智慧型園區有線和無線網路。

如同隨附的《軟體定義存取解決方案設計指南》中所述，本指南係用於部署管理基礎架構，包括 Cisco DNA 中心、Cisco Identity Services Engine (ISE) 以及思科無線區域網路控制器 (WLC)。如同隨附的《軟體定義存取網狀架構部署指南》中所述，本指南中提到的部署係指在部署思科軟體定義存取網狀架構之前使用。

如果您尚未從思科社群或設計專區下載本指南，請查看本指南的最新版本。

請造訪以下頁面，查看隨附的《軟體定義存取解決方案設計指南》、《軟體定義存取管理基礎架構規範性部署指南》、《分散式園區軟體定義存取規範性部署指南》等相關的部署指南、設計指南及白皮書：

- https://www.cisco.com/go/designzone
- https://cs.co/en-cvds

部署：SD-Access 網狀架構

如何讀取部署指令

針對輸入指令列介面 (CLI) 中的指令，本指南使用下列慣例。

須輸入 CLI 提示中的命令：

```
configure terminal
```

指定特定值或變數的指令（變數以粗斜體呈現）：

```
ntp server 10.4.0.1
```

具有須定義變數的指令（定義以粗體和斜體括起）：

```
class-map [highest class name]
```

CLI 或指令碼提示字元中的指令（輸入的指令以粗體顯示）：

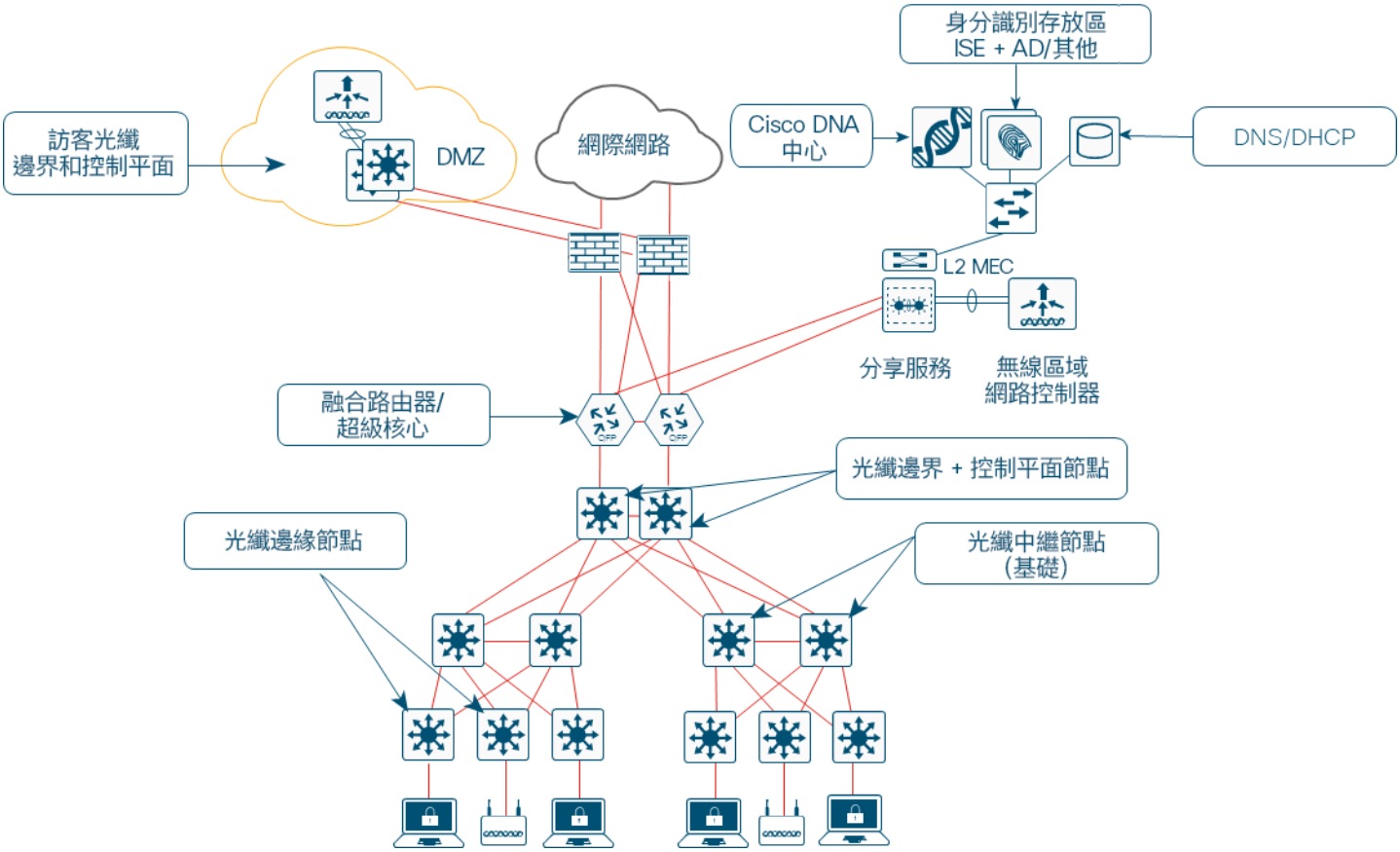
```
Router# enable
```

在列印頁面上換行的長指令（以一個指令的形式輸入加上底線的文字）：

```
police rate 1000 pps burst 10000
packets conform-action
```

如拓撲圖所示，將 SD-Access 管理元件部署到隨附的《軟體定義存取解決方案設計指南》中所述的拓撲之中。本指南假設已如同《軟體定義存取管理基礎架構部署指南》中所述，安裝並提供 Cisco DNA 中心、Cisco Identity Services Engine (ISE) 以及 Cisco Wireless LAN 控制器（WLC）管理基礎架構。

圖 1.
驗證拓撲



與所述的園區網狀架構部署整合的企業網路非虛擬化，並且執行增加型內部閘道通訊協定 (EIGRP) 作為路由通訊協定。來自園區（包括共用服務）的 IP 首碼必須同時用於網狀架構底層網路和重疊網路，同時維護重疊網路之間的隔離性。為了維持隔離，VRF-Lite 從網狀架構邊界節點擴展至融合路由器。融合路由器使用 BGP 路由目標匯入和匯出設定來執行 VRF 路由洩漏，並在企業網路中使用 EIGRP 執行相互重新分配，並使用 BGP 連線到園區網狀架構。動態標記和過濾重新分配路由的路由對應組態，提供一種簡單而動態的方式，以防止路由迴圈，同時在高可用性設計中容納多個重新分配點。

程序：使用 Cisco DNA 中心進行初始網路設計和探索

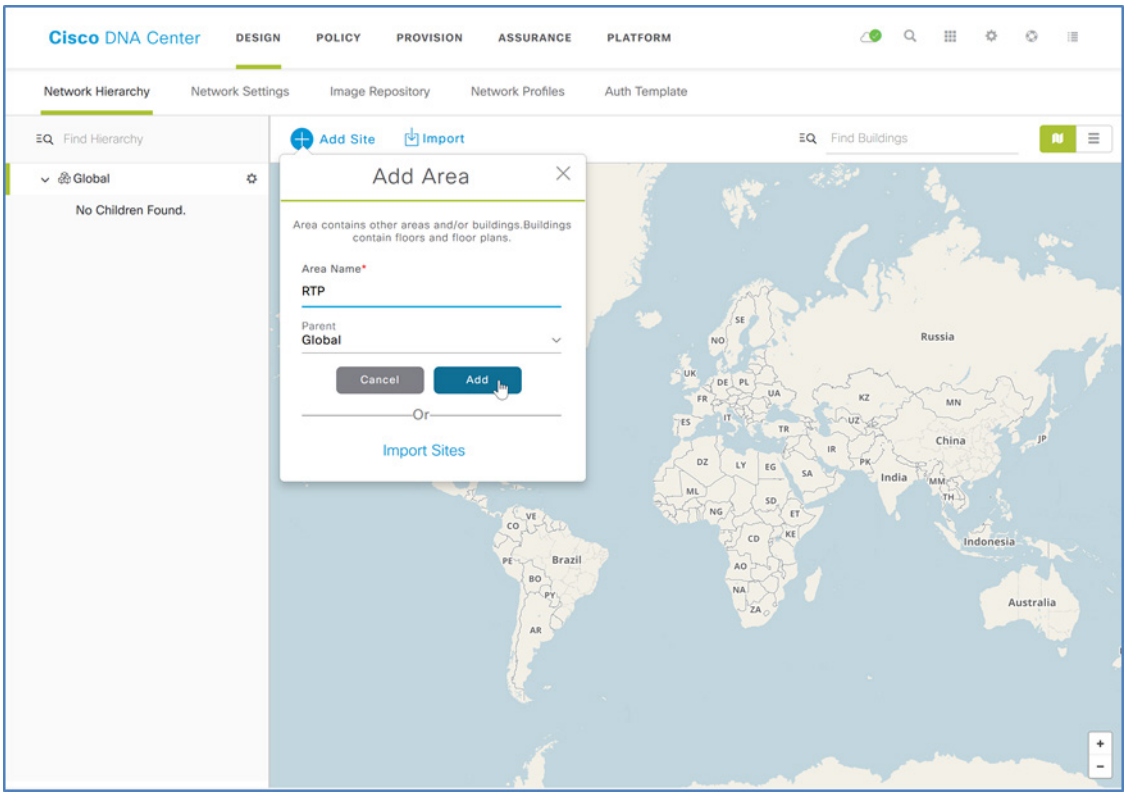
Cisco DNA 中心提供功能強大的設計應用程式，允許各種規模和大小的客戶輕鬆定義其實體網站和常用資源。使用直觀式易於使用的層級格式，設計應用程式無需在佈建裝置時從多個位置重新定義相同的資源，例如 DHCP、DNS 和 AAA 伺服器。在設計應用程式中建立的網路層級架構，應模仿實際部署的實體網路層級架構。

您可以使用 Cisco DNA 中心，來建立區域的網路層級架構，而且可以包含額外的區域或是區域中的建築物和樓層。裝置會對應到提供服務的建築和樓層。

程序 1.　建立網路網站

步驟 1.　登入 Cisco DNA 中心。從 Cisco DNA 中心的主控台，導覽至 Design > Network Hierarchy。

步驟 2.　按一下 **Add Site**，在下拉式功能表中選擇 **Add Area**，提供適當的**區域名稱**，然後按一下 **Add**。



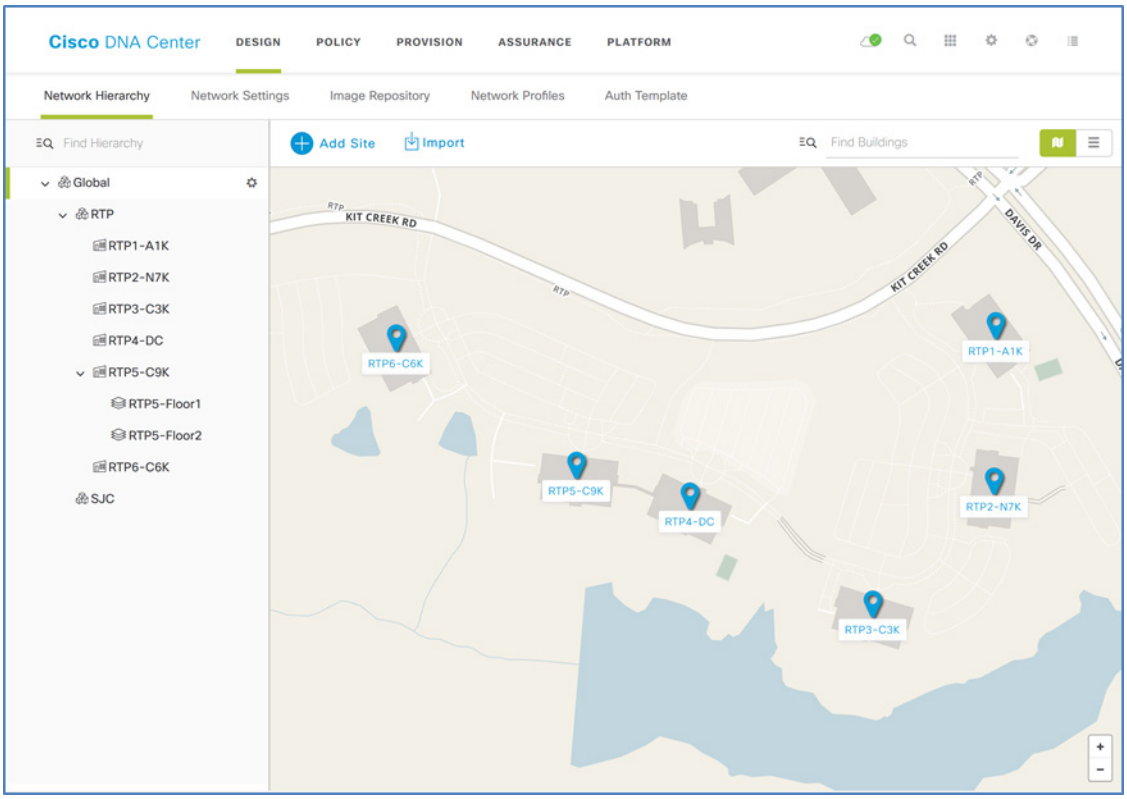
步驟 3.　按一下 **Add Site**，在下拉式功能表中選擇 **Add Building** 按鈕，提供適當的**建築物名稱**，選擇在上一步中建立的網站作為**父項**，完成精靈以指派位置，然後按一下 **Add**。

如要新增建築物，您可以在精靈內使用建築物附近約略的街道位址，如果需要，可按一下目標位置來調整地圖上的建築物位置。

步驟 4.　根據需要重複上一步，以新增網站和建築，建立您的組織可接受的層級架構。

步驟 5.　如果要將無線整合到建築物中，或者需要更精細地細分建築物內的網路選項，請選擇地圖上的建築（或選擇層級架構中建築物旁邊的齒輪圖示），選擇 **Add Floor** 並完成精靈的詳細資料。

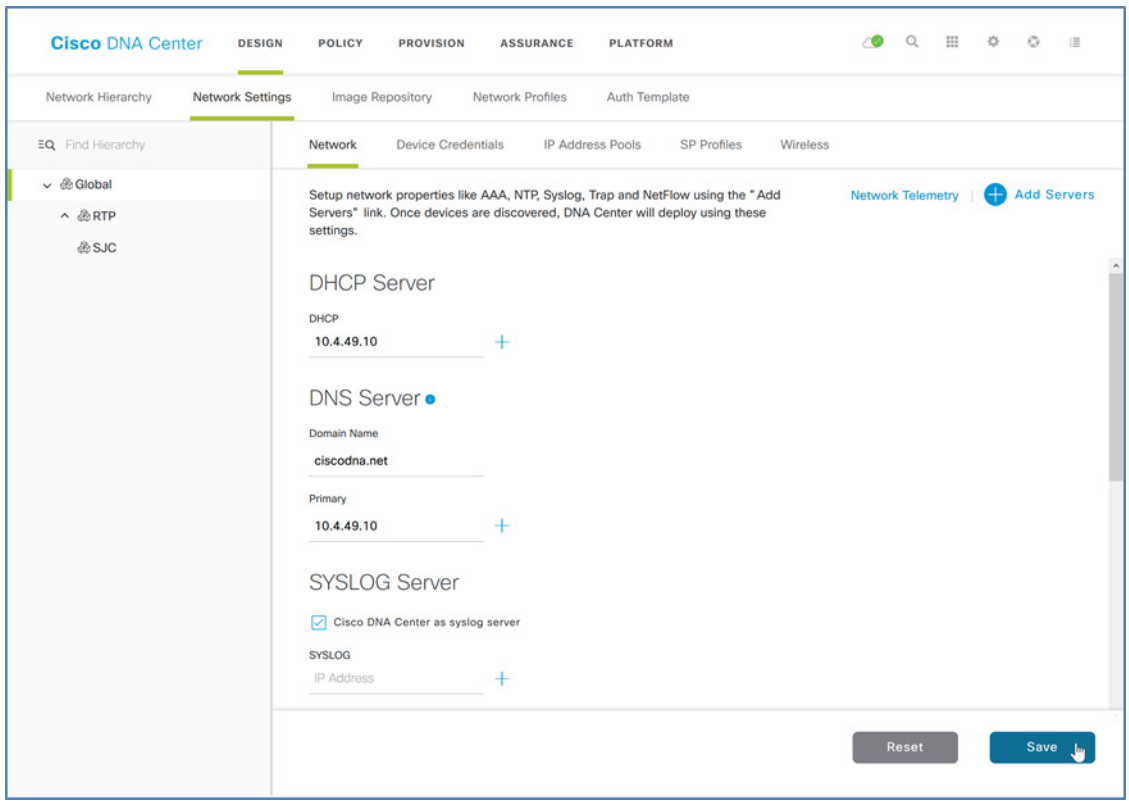
在無線佈建期間參考各個樓層。如果您有 DXF、DWG、JPG、GIF 或 PNG 格式的樓層地圖圖表，請將其新增到任何已定義的樓層，作為無線部署的有用元件，以顯示 AP 位置和覆蓋範圍。您可以按照《軟體定義存取解決方案設計指南》中所述的限制新增數百個網站。



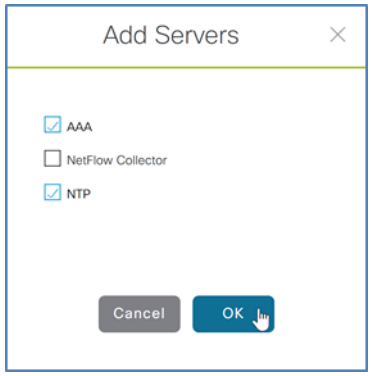
程序 2.　為站台設定網路服務

設定與 Cisco DNA 中心的層級架構一致的 AAA、DHCP 及 DNS 服務。如果服務在整個層級架構中使用相同的伺服器，則可以進行全域設定，並以層級架構的繼承屬性提供適用於所有網站的全域設定。然後，可以逐一網站套用各個網站的差異。此程序會在全域顯示設定。

步驟 1.　在 Cisco DNA 中心，導覽至 **DESIGN > Network Settings > Network**。在網站層級架構的左窗格中，選擇適當的層級（範例：全域），填寫 **DHCP 伺服器** IP 位址（範例：10.4.49.10），在 DNS 伺服器下填寫網域名稱（範例：ciscodna.net）和伺服器**主要** IP 位址（範例：10.4.49.10），新增備援或額外的伺服器（您可以保留此預設選項，使用 Cisco DNA 中心作為 SYSLOG 和 SNMP 伺服器），然後按一下 **Save**。



步驟 2. 在頂端附近，按一下 **Network Telemetry** 旁邊的 **+ Add Servers** 按鈕，選擇 **AAA** 和 **NTP** 核取方塊，然後按一下 **OK**。



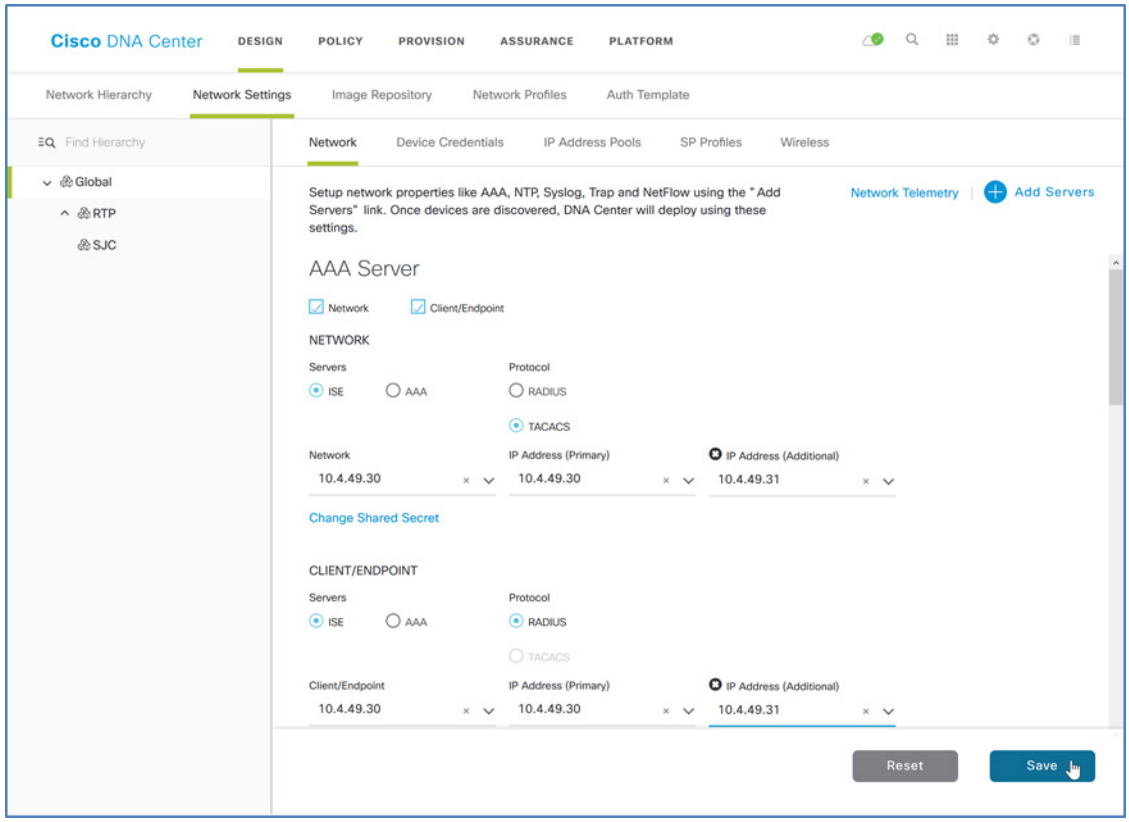
設定窗格會隨 **AAA 伺服器**和 **NTP 伺服器**更新為可用的設定區段。您可以為網路基礎架構裝置管理和連線到基礎架構的用戶端端點設定 AAA 服務。本範例則是使用高可用性的獨立 ISE 節點。

技術提示
許多組織使用 TACACS 進行基礎架構裝置管理支援。如果要在用於 RADIUS 用戶端身份驗證的同一 ISE 伺服器上啟用 TACACS，則在此步驟中，您還可以使用 **View Advanced Settings** 下拉式功能表將其與 Cisco DNA 中心整合。您可以透過在 ISE 導覽至 **Work Centers > Device Administration > Overview**，找到用於啟用 TACACS 整合的 ISE 設定資訊。

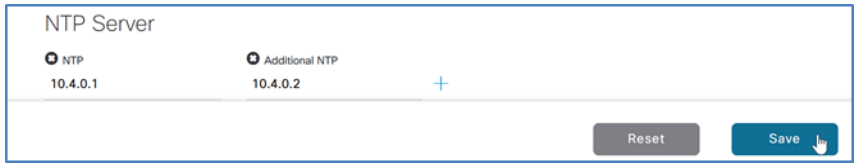
步驟 3. 在 **AAA 伺服器**下，選取 **Network** 和 **Client/Endpoint** 核取方塊，在 **Network** 下，選擇 **ISE** 單選按鈕，在 **Network** 下，使用下拉式功能表以選取預先填入的 ISE 伺服器（範例：10.4.49.30），在 **Protocol** 下，選擇 **TACACS** 單選按鈕，在 **IP Address (Primary)** 下，使用第二個下拉式功能表選擇主要 ISE 伺服器（範例：10.4.49.30），按一下加號（**+**）按鈕，然後在 **IP Address (Additional)** 下拉式功能表下方選擇備援 ISE 伺服器節點（範例：10.4.49.31）。

為確保已正確啟用 ISE 伺服器備援，請先驗證主要 IP 位址和額外的 IP 位址是否與所選的網路位址一併顯示，然後再繼續。

步驟 4. 在 **CLIENT/ENDPOINT** 和 **Servers** 下，選擇 **ISE** 單選按鈕，在 **Client/Endpoint** 下，使用下拉式功能表選擇預先填入的 ISE 伺服器。在 **Protocol** 下，選擇 **RADIUS** 單選按鈕，在 **IP Address (Primary)** 下使用下拉式功能表選擇主要 ISE 伺服器，按一下加號（**+**）按鈕，然後在 **IP Address (Additional)** 下使用下拉式功能表，選擇備援 ISE 伺服器節點，然後按一下 **Save**。



步驟 5. 在同一個畫面上，向下捲動到 **NTP Server**，新增 NTP 伺服器的 **IP 位址**（範例：10.4.0.1），如果您有一或多個額外的 NTP 伺服器，請選擇加號（**+**）按鈕，然後在 **Additional NTP** 中新增備援 NTP 伺服器的 IP 位址（範例：10.4.0.2），然後按一下 **Save**。



用於網站層級架構中所選級別的適用於 AAA 的 ISE 伺服器以及適用於 DHCP、DNS 和 NTP 的伺服器均儲存以便在網狀架構佈建期間使用。

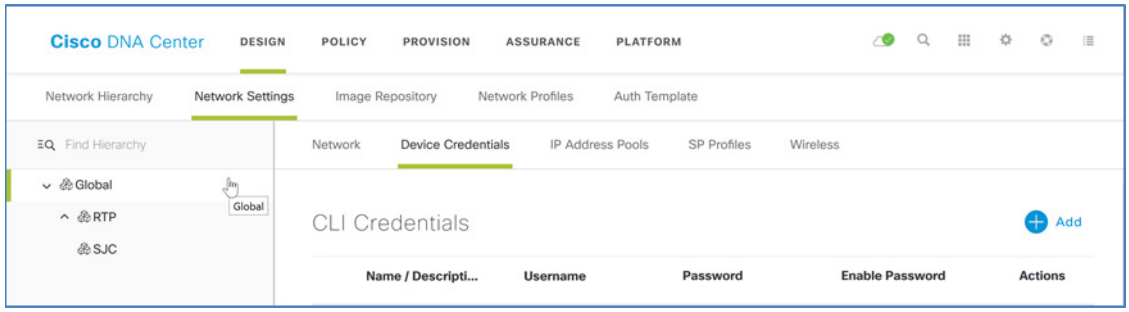
程序 3.　新增探索及管理所需的裝置憑證

當您使用已設定且 Cisco DNA 中心可存取網路的裝置部署 SD-Access 底層網路時，您可以透過提供 CLI 和簡易網路管理通訊協定 (SNMP) 憑證來探索和管理裝置。

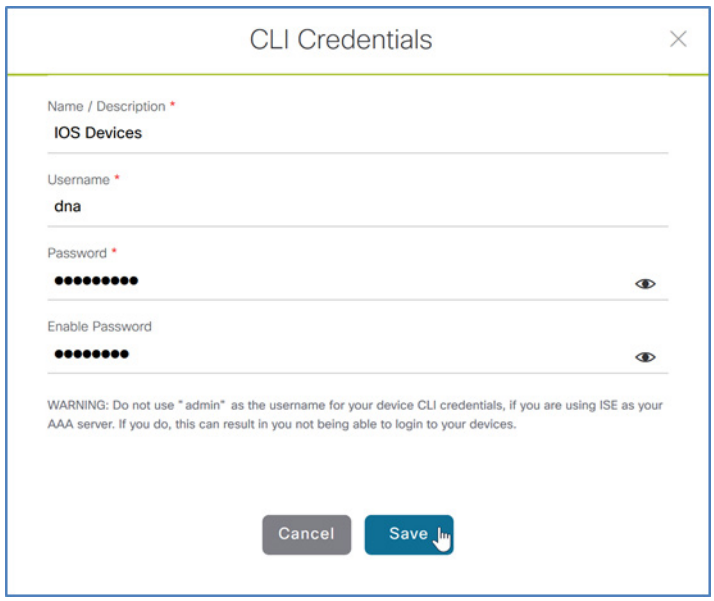
您可以選擇使用 Cisco DNA 中心區域網路自動化功能，將無現有設定的區域網路交換器部署到底層網路中。Cisco Network Plug and Play (PnP) 是為支援的交換器提供連線和初始設定的機制。如果要進行 LAN 自動化部署，您也可以提供 CLI 和 SNMP 憑證來存取和準備一或多個支援的 PnP 種子裝置，例如分佈層和核心層的 Cisco Catalyst 9500 系列交換器。LAN 自動化會使用 Cisco Discovery Protocol 發掘直接連線到所選的種子裝置介面的交換器及其直接相鄰的交換器，所有這些交換器都必須執行 PnP 代理程式，並且先前並未設定。提供的憑證可讓 Cisco DNA 中心和種子裝置協同工作，以便為發掘到的裝置進行設定，並將其新增到受管庫存中。

新增裝置憑證，以管理在設計中建立的網站層級架構的範圍。這些憑證可啟用網路發掘和管理。

步驟 1.　在 Cisco DNA 中心，導覽到 **Design > Network Settings > Device Credentials**，然後在左側窗格中選擇適當層級的網站層級架構（範例：「Global」是指可用於所有層級架構的通用憑證）。



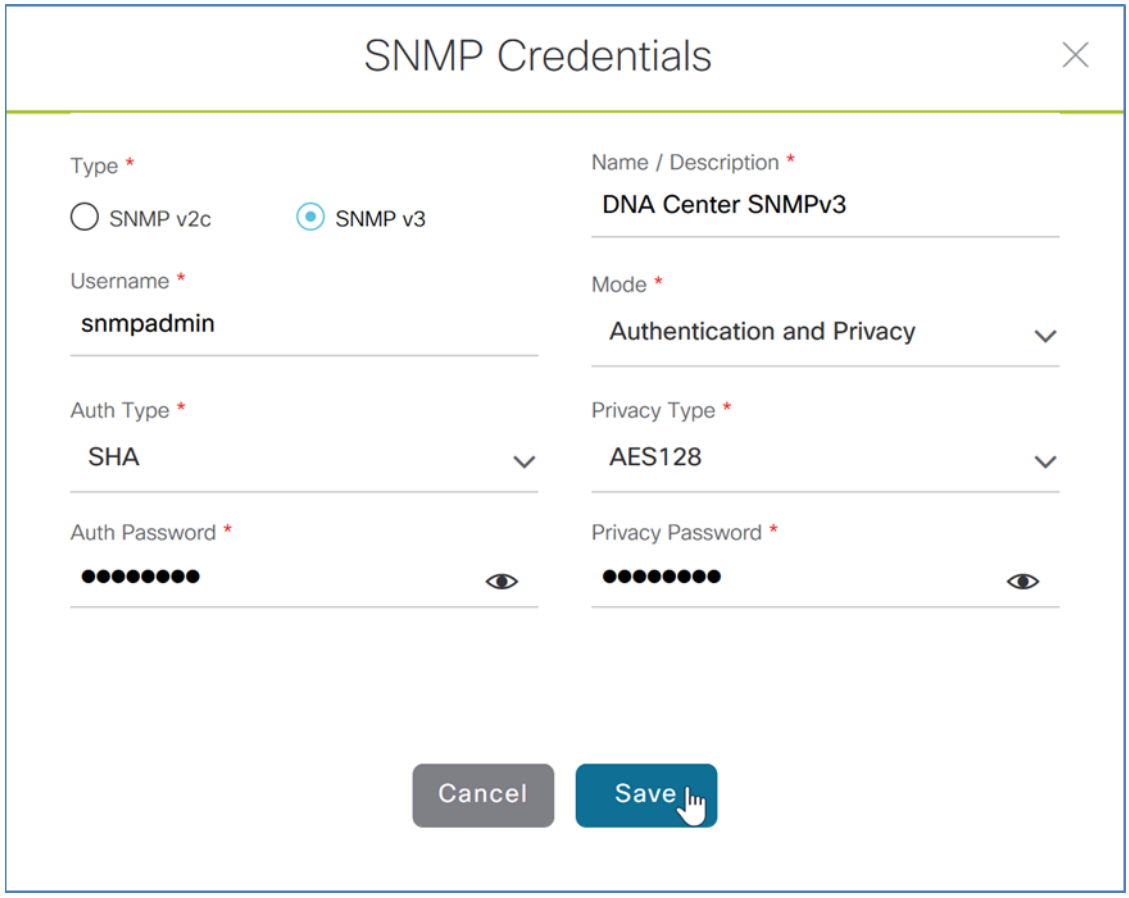
步驟 2.　在 **CLI Credentials** 區段的頂端，按一下 **Add**，填寫 **Name / Description**（範例：IOS 裝置）、**Username**、**Password** 和 **Enable Password** 欄位，然後按一下 **Save**。



注意

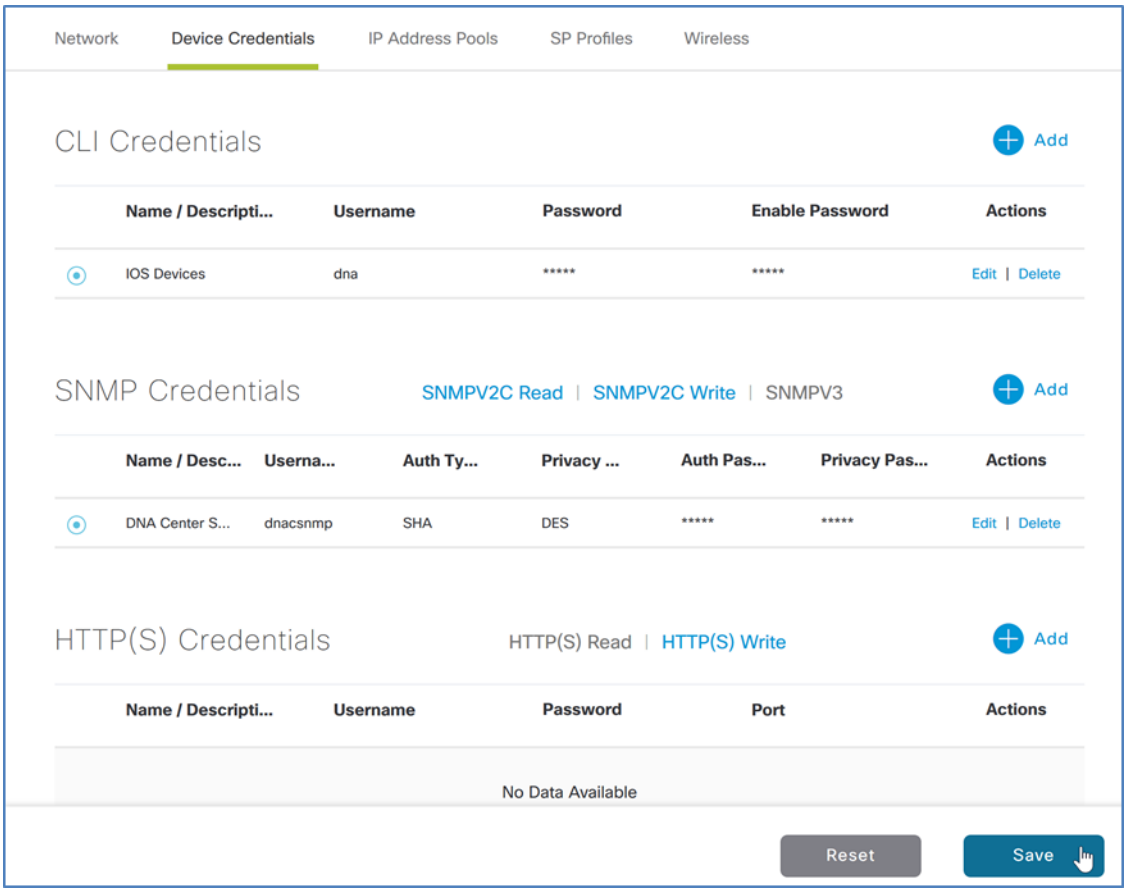
如果您使用 ISE 作為 AAA 伺服器，則應避免使用 **admin** 作為裝置 CLI 憑證的使用者名稱，以免造成使用者名稱與 ISE 管理員登入衝突，而無法登入裝置。

步驟 3. 在 **SNMP Credentials** 區段的頂端，選擇要更新的 SNMP 憑證類型（範例：SNMPV3）。按一下 **Add**，選擇要更新的憑證旁邊的行中的單選按鈕（每次一行一個憑證），填寫憑證詳細資訊（建議設 12 個字元的密碼，以便與 Cisco WLC 相容），然後按一下 **Save**。



步驟 4. 針對層級架構中所需的任何其他憑證，重複步驟 2 和 3。**CLI 憑證**和 **SNMPV3**，或 **SNMPV2C 讀取**和 **SNMPV2C 寫入**，這些是最常見的要求。

步驟 5. 針對指定的每個 CLI 和 SNMP 憑證，請按一下建立的每個指派旁邊的所有單選按鈕。每次選取後在裝置憑證畫面底部，按一下 **Save**。如果您使用了多個 SNMP 憑證類型，請透過切換至每個 SNMP 憑證選項來重複此步驟，按一下選項旁邊的單選按鈕，然後按一下 **Save**。



隨即將會顯示已成功建立常見設定的確認訊息。現在您可在 Cisco DNA 中心使用裝置憑證來進行網路探索和管理。

程序 4. 定義全域 IP 位址池

透過在 Cisco DNA 中心手動指派網路來定義您網路的 IP 位址。或者，透過將 API 整合 IPAM，將 IP 位址分派推送給 IP 位址管理員 (IPAM) （範例：Infoblox、Bluecat）。您可以透過導覽至 **System Settings > Settings > IP Address Manager** 並使用 IPAM 供應商的詳細規格來填寫表單來與 IPAM 進行整合。本範例不使用 IPAM 整合，您需要手動設定 IPAM 伺服器上的 IP 定址和 DHCP 範圍，以便與 Cisco DNA 中心中的指派相對應。

DHCP 伺服器上設定的 DHCP 範圍，應支援位址分配以及使裝置正常運作所需的任何其他 DHCP 選項。例如，一些 IP 網路電話供應商需要特定的 DHCP 選項，來使其裝置正常運作（範例：用於設定供 TFTP 伺服器進行設定的 DHCP 選項150）。請查看產品說明文件，以滿足您的部署要求。

此程序顯示如何手動定義在集區保留程序中使用的 IP 位址集區。這些集區指派給您網路中的網站，並且需要執行手動和整合 IPAM 部署的指派步驟。您可以靈活地建立更大的全域集區，然後在網站較低的層級架構保留部分的集區。IP 位址集區僅能在全域層級建立，您只能在全域之外的層級保留集區中的位址。

本指南中介紹的部署使用列在表格中的全域位址集區。為了便於理解，與企業組織通常的部署（例如 /16 或更大的位址空間）相比，大多數全域位址集區使用較小的位址空間。如員工範例所示，較大的全域位址集區在整個網站層級架構中支援許多較小的位址空間保留項目。雖然每個集區中的 IP 閘道的位址指派是必需的，但是 SD-Access 在建立重疊網路時僅使用該閘道。表格中還包括適用於手動 LAN 底層網路和單獨的自動化 LAN 底層網路以及多點傳送對等處理的範例集區。

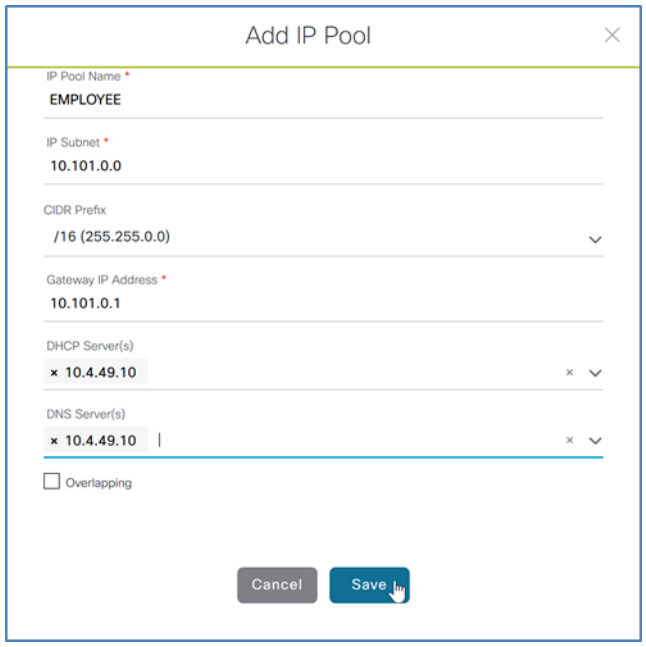
表 1. 全域位址集區範例

集區名稱	網路/遮罩	IP 閘道	DHCP 伺服器	DNS 伺服器
員工	10.101.0.0/16	10.101.0.1	10.4.49.10	10.4.49.10
BUILDING_CONTROL	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10
訪客	10.103.114.0/24	10.103.114.1	10.4.49.10	10.4.49.10
LAN_UNDERLAY	10.4.14.0/24	10.4.14.1	10.4.49.10	10.4.49.10
LAN_AUTOMATION	10.5.100.0/24	10.5.100.1	10.4.49.10	10.4.49.10
BORDER_HANDOFF	172.16.172.0/24	172.16.172.1	–	–
MULTICAST_PEER	172.16.173.0/24	172.16.174.1	–	–
ACCESS_POINT	172.16.174.0/24	172.16.173.1	10.4.49.10	10.4.49.10

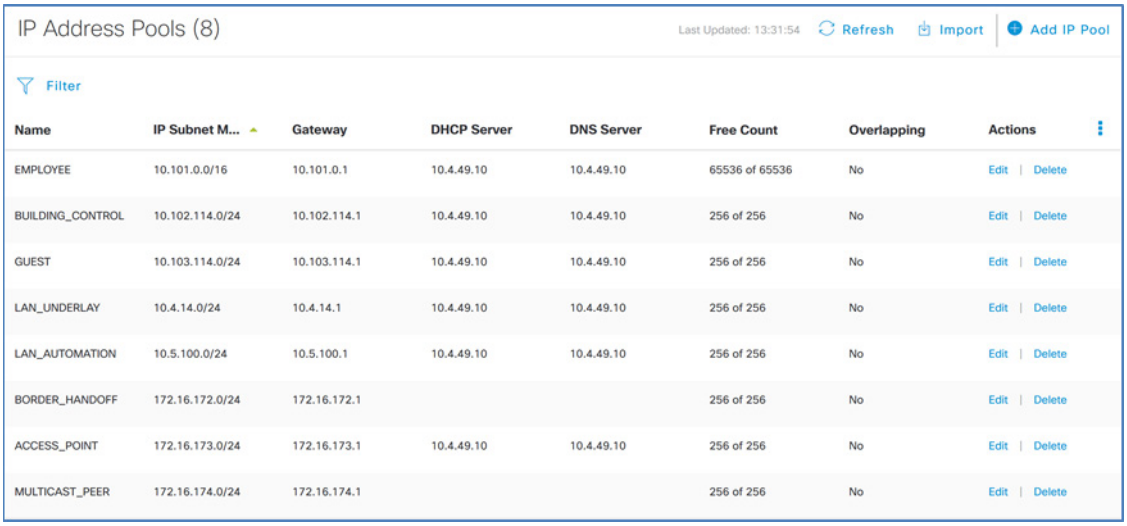
表 2. 來自員工全域集區的位址集區保留範例

集區名稱	網路/遮罩	IP 閘道	DHCP 伺服器	DNS 伺服器
EMPLOYEE-DATA-RTP5	10.101.114.0/24	10.101.114.1	10.4.49.10	10.4.49.10
EMPLOYEE-PHONE-RTP5	10.101.214.0/24	10.101.214.1	10.4.49.10	10.4.49.10

步驟 1. 在 Cisco DNA 中心新增專用於 SD-Access 網狀架構邊界節點連線佈建的全域集區。在 Cisco DNA 中心，導覽至 **DESIGN > Network Settings > IP Address Pools**。在左側的網站層級架構中，選擇 **Global**，然後按一下 **+ Add IP Pool**。填寫 **IP 集區名稱**、**IP 子網路**、**CIDR 首碼**和**閘道 IP 位址**。如果該集區具有端點用戶端，請使用下拉式功能表指派 **DHCP 伺服器**和 **DNS 伺服器**。請勿選擇 **Overlapping**。完成後，按一下 **Save**。



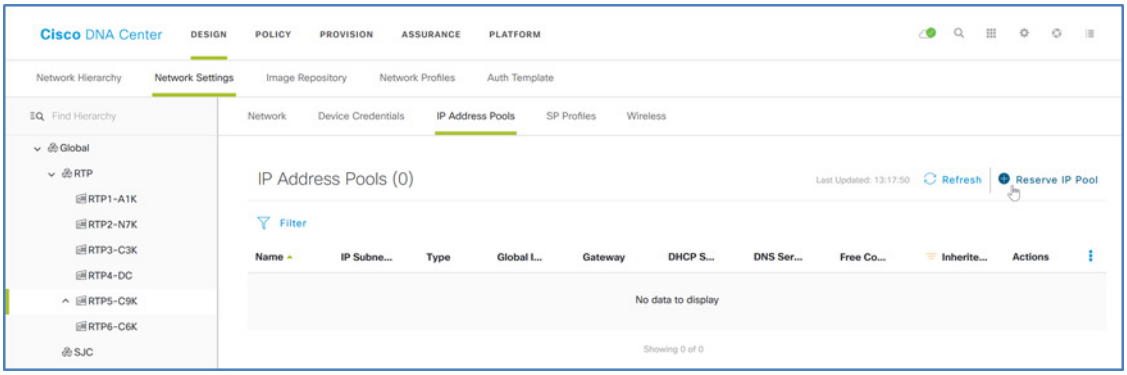
步驟 2. 針對在網站和建築物層級包含子網路的任何其他全域 IP 集區，重複上述步驟。這些集區將新增到全域集區清單中。



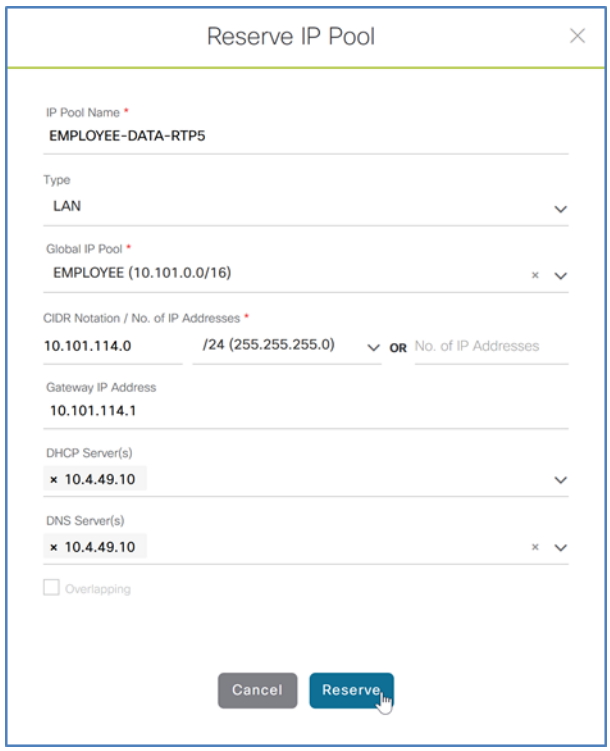
程序 5. 保留 IP 位址集區

使用定義的全域 IP 位址集區，透過網路層級架構為設計中的網站保留 IP 位址。如果是單一網站部署，可以為該網站保留完整集合的全域 IP 位址集區。當您從已定義的全域 IP 位址集區保留位址時，DNS 和 DHCP 伺服器可在這些保留項目中使用，也可以被覆蓋。

步驟 1. 在 Cisco DNA 中心中，導覽至 **DESIGN > Network Settings > IP Address Pools**，在網站層級架構的左側，為 IP 位址集區保留項目選擇一個網站或更低層級（範例：RTP5-C9K），然後在右上角按一下 **Reserve IP Pool**。



步驟 2. 填寫 **IP 集區名稱**（範例：EMPLOYEE-DATA-RTP5），在 **Type** 下方選取 **LAN**，選擇用於保留的**全域 IP 集區**來源（範例：「EMPLOYEE」），在 **CIDR Notation / No. of IP Addresses** 下方，選取要使用的位址空間部分（範例：10.101.114.0/24），指派**閘道 IP 位址**（範例：10.101.114.1），使用下拉式功能表指派 **DHCP 伺服器**和 **DNS 伺服器**，然後按一下 **Reserve**。



步驟 3. 對每個網站的層級架構中需要保留的所有全域集區位址區塊重複上述步驟。

層級架構顯示指派的位址集區。此範例顯示 RTP5-C9K 大樓層級的 RTP 網站內的集區保留。

程序：為 SD-Access 網路建立分段和原則

作為針對您的 SD-Access 網路部署準備的設計決策的一部分，您需要確定組織的網路分段原則。巨集分段在網狀架構中使用其他重疊網路（虛擬網路），而微分段使用可擴充群組標記將原則運用於使用者裝置設定檔群組。

使用群組原則透過分段輕鬆容納所需的原則應用結果。在大學的範例中，學生和教職員機器都可以存取列印資源，但學生電腦不得直接與教職員電腦通訊，而且列印裝置不得與其他列印裝置通訊。

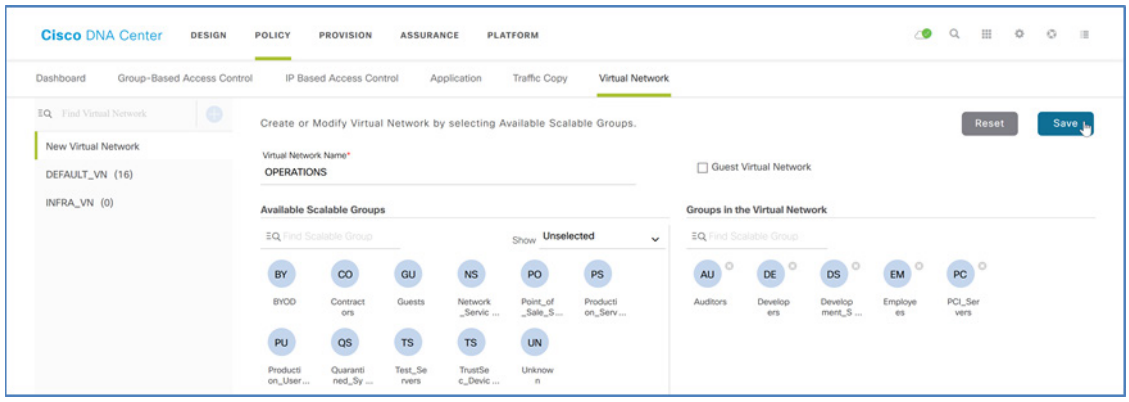
其他情況下則需要更進一步隔離。在零售商店範例中，銷售點電腦一律不得與視訊監控網路基礎架構通訊，而該監控架構則不得與建築的 HVAC 系統進行通訊。在隔離需要從網路邊緣一路延伸到網路核心，以存取集中式服務的情況下，使用虛擬網路的巨集分段是最佳選擇。政府和業界合規性要求以及組織的風險原則通常會提高使用巨集分段的選擇。

如需透過使用案例深入探索如何為 SD-Access 設計分段，請至 Cisco.com 上參閱《軟體定義的存取分段設計指南》。

使用這些程序作為部署巨集和微分段原則的範例。

程序 1.　為軟體定義存取網路新增重疊 VN

步驟 1.　從 Cisco DNA 中心主要儀表板，導覽至 **POLICY > Virtual Network**，按一下 **+**（加號）以建立新的虛擬網路，輸入**虛擬網路名稱**（範例：OPERATIONS），從 **Available Scalable Groups** 集區中將可擴充群組拖曳至 **Groups in the Virtual Network** 集區（範例：Auditors、Developers、Development_Servers、Employees 以及 PCI_Servers），然後按一下 **Save**。



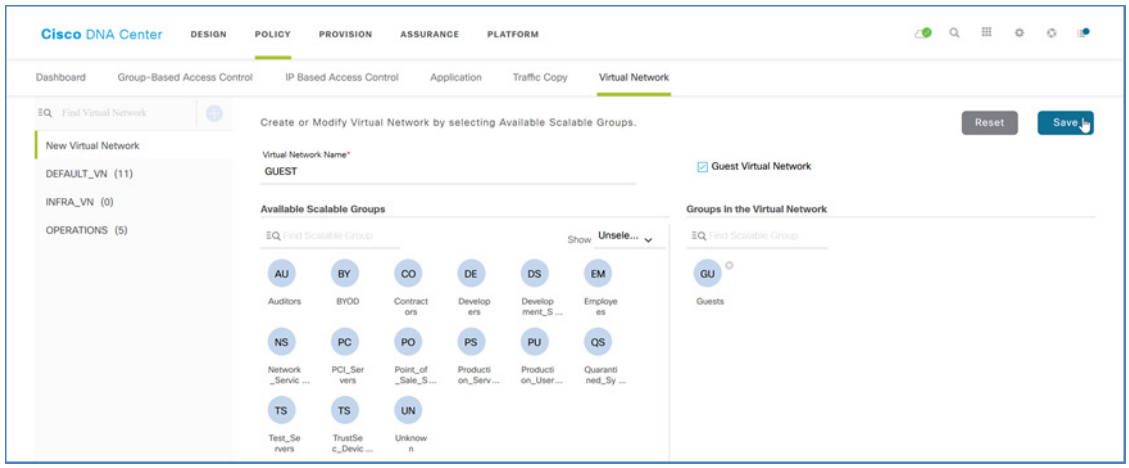
關聯群組的虛擬網路已定義，並且會顯示在定義的虛擬網路清單中。這些虛擬網路定義可用於佈建網狀結構。

技術提示
如果您沒有看到任何群組，則可能是因為 Cisco DNA 中心與 ISE 之間的 pxGrid 連線尚未完全開始運作。在這種情況下，請查看與 Cisco DNA 中心的 ISE 整合程序，並確保已從 Cisco DNA 中心核准 ISE 的 pxGrid 連線請求。

步驟 2.　如果您的組織需要與預設群組不同的群組，請透過導覽至 **POLICY > Group-Based Access Control > Scalable Groups** 來建立自訂群組，然後按一 下**Add Groups** 以建立新群組和 SGT。

步驟 3.　對每個重疊網路重複前兩個步驟。您還可以在佈建網狀架構後回到這些步驟，以建立更多重疊網路。

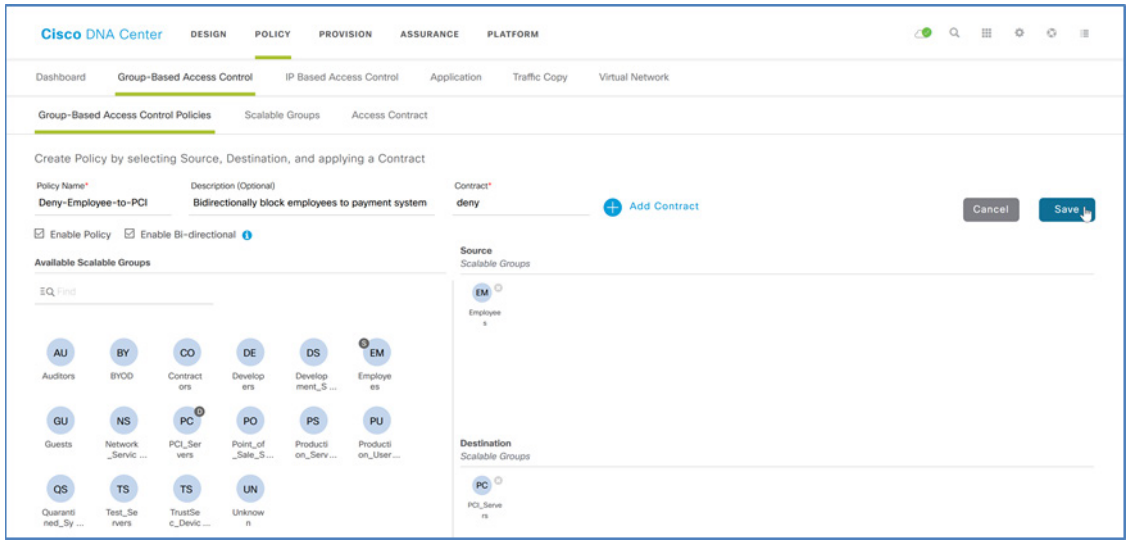
步驟 4.　許多網路需要為無線使用者提供訪客服務，可以建立訪客虛擬網路以支援此功能。從 Cisco DNA 中心儀表板，導覽至 **POLICY > Virtual Network**，按一下 **+**（加號）以建立新的虛擬網路，輸入**虛擬網路名稱**（範例：GUEST），選取 **Guest Virtual Network** 旁的核取方塊，請將 **Guests** 可擴充群組從 **Available Scalable Groups** 集區中拖曳到 **Groups in the Virtual Network** 集區，然後按一下 **Save**。



程序 2. 使用 SGT 建立微分段原則

為組織的部署自訂微分段原則。此簡單範例顯示可用於拒絕員工群組中的使用者與 PCI_Servers 群組通訊的基本原則。當身份驗證設定檔適當地將 SGT 指派給端點或使用者時，ISE 會擷取此原則的意圖並將其呈現在網路中。

步驟 1. 從 Cisco DNA 中心主要儀表板，導覽至 **POLICY > Group-Based Access Control > Group-Based Access Control Policies**，按一下 **+ Add Policy**，從 **Available Scalable Groups** 窗格中，將 **Employees** 群組拖放至 **Source** 窗格中，將 **PCI_Servers** 群組拖曳至到 **Destination** 窗格中，輸入**原則名稱**（範例：Deny-Employee-to-PCI），輸入**說明**，選取 **Enable Policy**，然後選擇 **Enable Bi-directional**，按一下 **+ Add Contract**，選擇 **deny**，按一下 **OK**，然後按一下 **Save**。



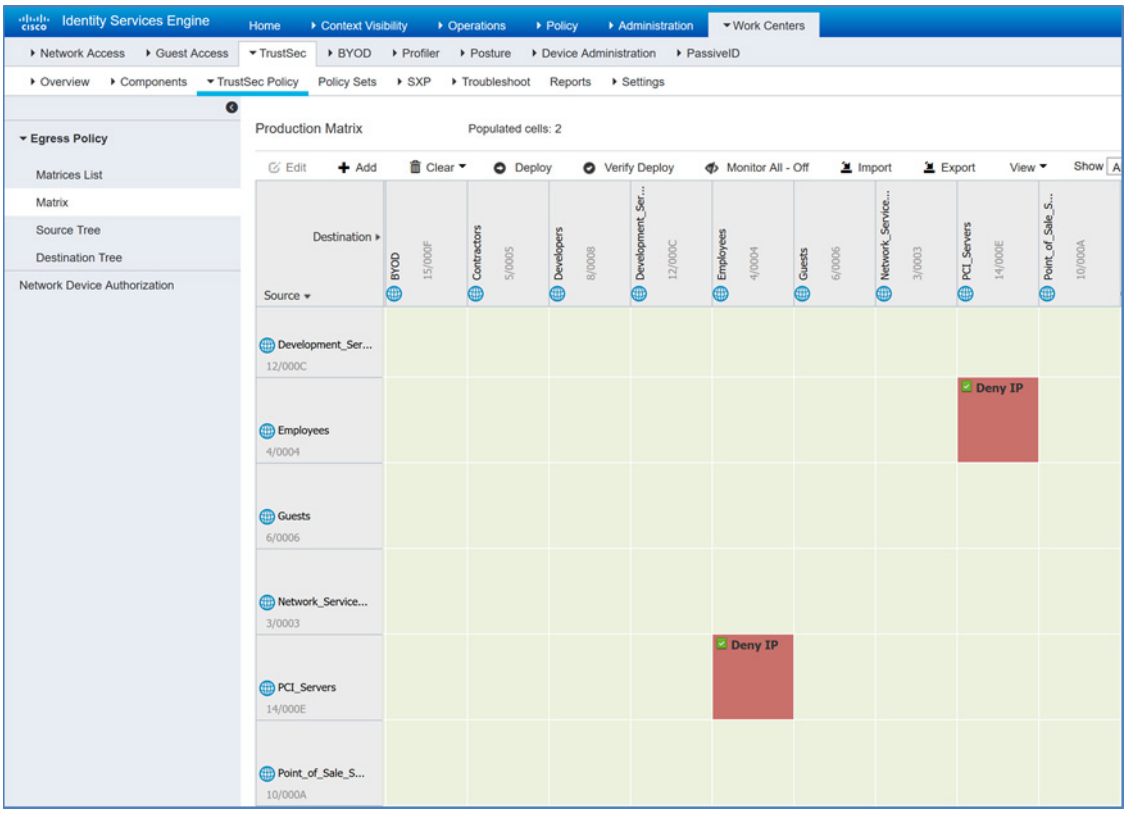
該原則已建立並列為 **CREATED** 的狀態。由於選擇了雙向選項，因此也會建立反向原則。

步驟 2. 選取已建立的原則，然後按一下 **Deploy**。

狀態變更為 **DEPLOYED**，且原則可套用在 Cisco DNA 中心建立的 SD-Access 網狀架構和 ISE，可使用 Cisco TrustSec 原則對照表查看。

步驟 3. 按一下右上角的 **Advanced Options**。該連結是登入 ISE 的捷徑，請導覽至 **Work Centers > TrustSec > TrustSec Policy**，然後在左側選擇 **Matrix**。您將被重新導向登入 ISE，然後重新導向瀏覽器並顯示 TrustSec 原則對照表。

驗證原則是否已更新到 ISE，以呈現在網路中。



程序：為網路管理自動化做好準備

透過建立一個正常運作的網路底層網路（包括裝置管理連線），為部署網路設計和原則做好準備。如同在隨附的《分散式園區軟體定義存取規範部署指南》中所示，ISE 會透過 TACACS 基礎架構裝置管理支援進行設定，並作為 ISE 與 Cisco DNA 中心整合的一部分。對於 TACACS 設定，Cisco DNA 中心會修改探索到的裝置，以便依預設使用來自 ISE 和本機容錯移轉服務的身份驗證和計量服務。ISE 必須做好準備，以支援在探索過程中推送到裝置的裝置管理設定。

程序 1.　使用 Cisco IOS XE CLI 設定底層網路裝置管理

為取得最大恢復能力和頻寬，請使用每台裝置上的回送介面，並啟用第三層連線，以進行 Cisco DNA 中心頻內探索和管理。下列步驟使用 IS-IS 作為路由通訊協定設定裝置之間的點對點乙太網路連線，並使用裝置回送介面設定 SSHv2 以進行裝置設定。SNMP 設定會在後續程序中進行推送，以作為裝置探索的一部分。

請勿將設定新增到您打算使用 LAN 自動化進行探索和設定的任何裝置，作為後續程式的一部分。不得使用 LAN 自動化設定具有現有設定的裝置。此範例顯示在 Cisco Catalyst 交換器上使用 Cisco IOS XE 的設定。

步驟 1.　使用裝置 CLI 設定主機名稱，使其易於識別裝置和停用未使用的服務。

```
hostname [hostname]
no service config
```

步驟 2.　設定本機登入名和密碼。

```
username dna privilege 15 algorithm-type scrypt secret [password]
! older software versions may not support scrypt (type 9)
! username dna privilege 15 secret [password]
enable secret [enable password]
service password-encryption
```

步驟 3.　將安全性殼層 (SSH) 設定為 CLI 管理存取的方法。

```
ip domain-name ciscodna.net
! generate key with choice of modulus, required by some switches
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 15
  login local
  transport input ssh
  transport preferred none
```

步驟 4.　將交換器設定為支援乙太網器巨型框架。選擇的 MTU 允許額外的網狀架構標頭以及與大多數交換器的最高通用值的相容性，而且在設定和故障排除時，捨入的整數應可方便記憶。

```
system mtu 9100
```

技術提示
在路由器上使用 Cisco IOS XE 的底層網路連線要求在介面設定層級使用 **mtu** 指令，而 Cisco Catalyst 和 Cisco Nexus® 交換器不使用 Cisco IOS XE，而是在全域設定層級使用 **system jumbo mtu** 指令。

步驟 5. 設定交換器迴路位址，並指派 SSH 管理來使用。

介面迴圈 ***0***

IP 位址 ***[裝置迴圈 IP 位址]*** 255.255.255.255

IP SSH 來源介面迴圈 ***0***

程序 2. 為路由存取連線設定底層網路連結

如果您的底層網路已使用路由存取網路部署模式進行設定，請跳過此程序。通常第二層部署需要執行此程序。

請勿將設定新增到您打算使用 LAN 自動化功能探索和設定的任何裝置。目前已有設定的裝置，除非將裝置重設為原本的預設值，否則不能線上使用 LAN 自動化來設定。

步驟 1. 在底層網路基礎架構內設定交換器連線。對網狀架構底層網路中相鄰交換器的每個連結重複此步驟。如果底層網路裝置將被佈建為網狀架構邊界節點，並且使用此連線作為從網狀架構到外部基礎架構的遞交，則請改為執行下一個步驟。

```
interface TenGigabitEthernet1/0/1
 no switchport
 ip address [Point-to-point IP address] [netmask]
```

步驟 2. 啟用 IP 路由，並啟用交換器上的 IS-IS 路由通訊協定。

```
! ip routing is not enabled by default on some switches
ip routing
ip multicast-routing
ip pim register-source Loopback0
ip pim ssm default
router isis
 net 49.0000.0100.0400.0001.00
 domain-password [domain password]
 metric-style wide
 nsf ietf
 log-adjacency-changes
 bfd all-interfaces
```

技術提示

IS-IS 中常見的慣例是將迴圈 IP 位址內嵌到唯一的網路或系統 ID 中。例如，迴圈 IP 位址 ***10.4.32.1*** (***010.004.032.001***) 會重新分組為 ***0100.0403.2001***，附加 ***.00*** 的尾碼，並在前面加上區域 ID（例如 ***49.0000***），因而得到 NET ***49.0000.0100.0403.2001.00***。

步驟 3. 除了在下一個程序中設定的邊界遞交介面外，在底層網路中所有已設定的基礎架構介面上啟用 IS-IS 路由。啟用回送介面以共用管理 IP 位址，並啟用實體介面，以便與連線的基礎架構共用路由資訊。

```
interface Loopback0
! ip address assigned in earlier step
 ip router isis
 ip pim sparse-mode
```

```
interface range TenGigabitEthernet1/0/1-2、 TenGigabitEthernet2/0/1-2
! routed ports with ip addresses assigned via earlier steps
 ip router isis
 isis network point-to-point
 ip pim sparse-mode
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 dampening
```

程序 3. 在邊界啟用面向外部路由器芳鄰的路由連線

如果您已將底層網路設定為路由存取網路，並使用 BGP 透過 802.1 Q 遞交與網路其他部分整合，請略過此程序。大多數部署都需要執行此程序。

要將邊界節點裝置連線到您的網路，您可以使用 VRF-lite（使用 802.1 Q VLAN 標記來分隔 VRF）在設定的介面之間建立連線。在沒有直接連接到 SD-Access 網路節點的情況下，透過將現有的企業網路擴展到邊界處的底層網路，來連接邊界節點外可用的通用網路服務（例如 DNS、DHCP、WLCs 和 Cisco DNA 中心管理）。若要進行其他佈建，則需要連線到 Cisco DNA 中心。

處理多個虛擬網路和全域路由執行個體之間路由作業的外部裝置將充當這些網路的融合路由器。使用由 802.1 Q 標記的介面連線到邊界的 VRF （又稱為 VRF-lite），藉此來維護連線的獨立性。使用 BGP 建立底層網路連線，可讓 Cisco DNA 中心使用此連結來管理初始探索和設定，然後根據需要使用與其他標記和 BGP 作業階段擴增的相同連結進行重疊 VN 連線。

步驟 1. 針對每個邊界節點，如果您要設定支援 VLAN trunk 介面的交換器（例如 Cisco Catalyst 9000、3800 或 6800 系列交換器），則必須在已連線的介面上使用專用 VLAN 設定主幹，以便為與融合路由器對等路由建立底層網路連線。

```
vlan 100
interface vlan100
 ip address [IP address] [netmask]
 ip pim sparse-mode
 no shutdown
interface FortyGigabitEthernet1/0/24
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 100
 no shutdown
```

步驟 2. 針對每個邊界節點，如果要設定支援 802.1 Q VLAN 標記的裝置（例如 ASR 或 ISR 路由器），請使用替代的子介面組態（而非交換器主幹介面）來建立與融合路由器的底層網路連線。

```
interface TenGigabitEthernet0/1/0
 no shutdown
!
interface TenGigabitEthernet0/1/0.100
```

```
 encapsulation dot1Q 100
 ip address [IP address] [netmask]
 ip pim sparse-mode
 no shutdown
```

步驟 3. 將備援邊界節點一併與至少一個路由介面連線，以進行底層網路通訊和後續的 BGP 對等互連。隨即會顯示整合到 IS-IS 通訊協定中的組態。為連線邊界節點的每個介面重複此步驟。

```
interface FortyGigabitEthernet1/0/23
 no switchport
 ip address [Point-to-point IP address] [netmask]
 ip router isis
 isis network point-to-point
 ip pim sparse-mode
 logging event link-status
 load-interval 30
no shutdown
```

步驟 4. 啟用通往融合路由器的 BGP 路由，以便連線到網狀架構外部的網路，並在連線介面上啟動 BGP。設定 BGP 以允許 Cisco DNA 中心管理存取底層網路裝置，同時允許對介面上的虛擬網路進行進一步佈建，並大幅降低網路連線中斷。對每個邊界節點重複此步驟。

```
router bgp [underlay AS number]
 bgp router-id [loopback 0 IP address]
 bgp log-neighbor-changes
! fusion router is an eBGP neighbor
 neighbor [fusion interface IP address] remote-as [external AS number]
! redundant border is an iBGP neighbor
 neighbor [redundant border Lo0 address] remote-as [underlay AS number]
 neighbor [redundant border Lo0 address] update-source Loopback0
 !
 address-family ipv4
  network [Lo0 IP address] mask 255.255.255.255
 ! advertise underlay IP network summary in global routing table
  aggregate-address [underlay IP network summary] [netmask] summary-only
  redistribute isis level-2
  neighbor [fusion interface IP address] activate
  neighbor [redundant border Lo0 address] activate
  maximum-paths 2
 exit-address-family
```

程序 4. 將共用的服務子網路重新分配到底層網路 IGP

存取點無法使用底層網路的預設路由來觸及 WLC。在存取點連線以建立連線的每個節點的全域路由表中，必須存通往 WLC IP 位址的更為具體的路由（例如 /24 子網路或 /32 主機路由）。使用此程序將邊界上的共用服務路由重新分配到底層網路 IGP 路由程序，藉此來允許對從 BGP（範例：10.4.174.0/24 和 10.4.48.0/21）到底層網路所需的 WLC 和 DHCP 共用服務設定更為具體的路徑。使用此程序時，使用的首碼須與 BGP 路由表中的首碼相符。

步驟 1. 連線到每個邊界節點，並為用於共用服務的子網路新增首碼清單和路由圖。

```
ip prefix-list SHARED_SERVICES_NETS seq 5 permit 10.4.48.0/21
ip prefix-list SHARED_SERVICES_NETS seq 10 permit 10.4.174.0/24
route-map GLOBAL_SHARED_SERVICES_NETS permit 10
 match ip address prefix-list SHARED_SERVICES_NETS
```

步驟 2. 在每個邊界節點上，將首碼重新分配到底層網路路由通訊協定中。此範例假設為 ISIS。

```
router isis
 redistribute bgp [underlay AS number] route-map GLOBAL_SHARED_SERVICES_NETS metric-type external
```

程序 5. 在外部融合路由器上啟用面向邊界芳鄰的連線

連線到網狀架構邊界路由器的融合路由器需要針對與先前程序一致的底層網路連線的 CLI 組態。在連線到邊界的每個外部融合路由器裝置上執行此過程。

範例中的融合路由器設定了包含橫跨整個企業全域路由的 VRF 和在邊界上的全域路由表之間的路由對等互連， 以達到網狀架構底層網路的連線能力，而無需使用融合路由器全域路由表。

或是在融合路由器跨企業全域路由表和邊界上的全域路由表之間對應，而不使用 VRF。

步驟 1. 在每個外部融合路由器上，建立與邊界的初始管理連線的 VRF、路由識別碼和路由目標。

```
vrf definition VRF-GLOBAL_ROUTES
 rd 100:100
 !
 address-family ipv4
  route-target export 100:100
  route-target import 100:100
exit-address-family
```

步驟 2. 針對從外部融合路由器到 SD-Access網狀架構邊界的每個連線，啟用介面、VLAN 標記的子介面和 IP 定址。此範例在具有子介面的路由器上使用 802.1 Q VLAN 標記。針對需要主幹埠組態的交換器，請配對先前設定的另一端。

```
interface TenGigabitEthernet0/1/7
 description to Border
 mtu 9100
 no ip address
 no shutdown
interface TenGigabitEthernet0/1/7.100
 encapsulation dot1Q 100
```

```
 vrf forwarding VRF-GLOBAL_ROUTES
 ip address [IP network] [netmask]
```

在融合路由器與邊界節點之間的 802.1 Q 標記連線上，現已為 VLAN （範例：100）啟用 IP 連線。

步驟 3. 建立路由圖以標記路由，並避免在使用多個連結進行連線時，並且在網路的其他部分中使用的 IGP 和 BGP之間進行重新分配時，避免路由迴圈。IGP 須視情況而定。範例中顯示的是 EIGRP，完成從 IS-IS、BGP 到 EIGRP 的路由連線。

```
route-map RM-BGP-TO-EIGRP permit 10
 set tag 100
!
route-map RM-EIGRP-TO-BGP deny 10
 match tag 100
route-map RM-EIGRP-TO-BGP permit 20
```

步驟 4. 啟用從備援融合路由器到邊界節點的 BGP 對等互連，並重新分配用於到達融合路由器之外的網路的 IGP。

```
router bgp [external AS number]
 bgp router-id [loopback IP address]
 bgp log-neighbor-changes
 !
address-family ipv4 vrf VRF-GLOBAL_ROUTES
  redistribute eigrp 100 route-map RM-EIGRP-TO-BGP
  neighbor [redundant fusion IP] remote-as [external AS number]
  neighbor [redundant fusion IP] activate
  neighbor [border IP address] remote-as [underlay AS number]
  neighbor [border IP address] activate
  maximum-paths 2
  default-information originate
 exit-address-family
```

步驟 5. 將 BGP 重新分配到 IGP 中以啟用連線能力。IGP 須視情況而定。範例中所示為用於命名模式 EIGRP。

```
router eigrp LAN
 !
 address-family ipv4 unicast vrf VRF-GLOBAL_ROUTES autonomous-system 100
  topology base
   redistribute bgp [external AS number] metric 1000000 1 255 1 9100 route-map RM-BGP-TO-EIGRP
  exit-af-topology
  network [external IP network address] [netmask]
  eigrp router-id [loopback IP address]
 exit-address-family
```

程序 6. 在非受管中繼裝置上設定 MTU

選用

由 Cisco DNA 中心管理網狀架構網域中的所有裝置有其優點。Cisco DNA 中心已管理網狀架構邊緣節點和邊界節點；但是，如果您在網狀架構中的部分中繼裝置並非由 Cisco DNA 中心管理（範例：在 Cisco DNA 中心並不提供硬體或軟體支援），則這些裝置仍必須符合透過這些傳輸網狀架構中繼節點傳輸 SD-Access 流量的要求。主要要求是：

- 必須是主動參與其他網狀架構底層網路裝置中的路由拓撲的第三層裝置。
- 必須能夠傳輸網狀架構封裝技術提供的巨型框架。

針對於非受管網狀架構中繼節點裝置，您必須設定適當的 MTU （範例：9100），並藉由底層網路中的其他裝置手動設定路由。此情況的設定指南須視裝置而有所不同，本指南中不會對此進行討論。

請勿將設定新增到您打算使用 LAN 自動化進行探索和設定的任何裝置，作為後續程式的一部分。不得使用 LAN 自動化設定具有現有設定的裝置。

程序 7. 探索和管理網路裝置

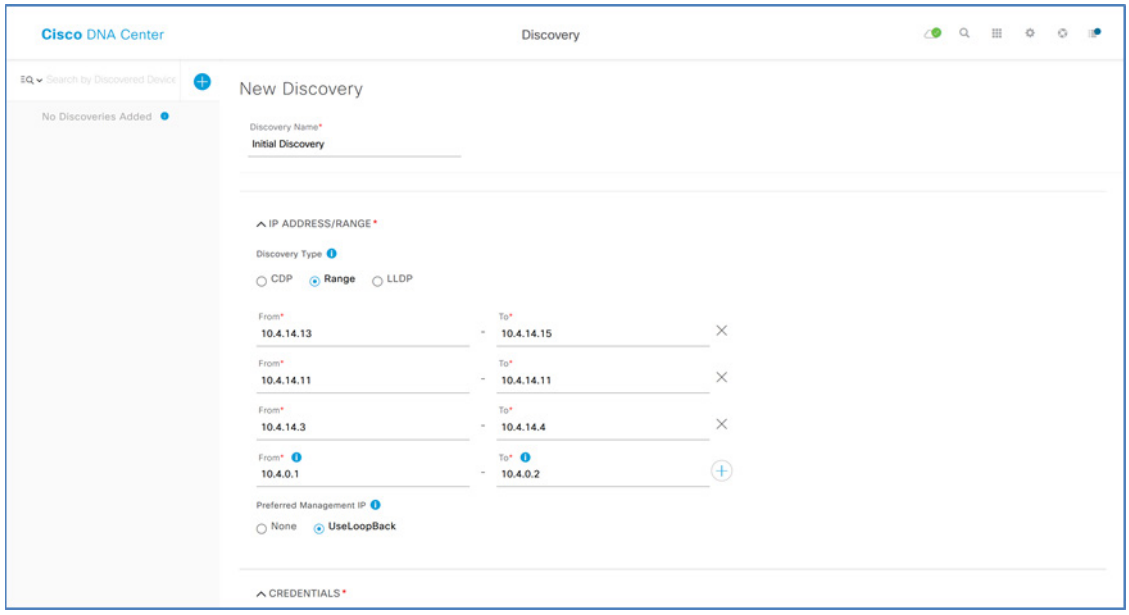
透過啟用與裝置的 IP 連線並將管理憑證提供給 Cisco DNA 中心，您可以使用 Cisco DNA 中心探索並管理底層網路裝置以進行 SD-Access。將此程序用於所有未計畫在下一個程序中使用 LAN 自動化來探索和管理的 LAN 自動化種子裝置和所有其他裝置。

這些步驟顯示如何透過提供 IP 位址範圍或用於掃描網路裝置的多個範圍來起始探索，進而限制探索並可能節省時間。或者您可以針對不使用 LAN 自動化上線的裝置，提供初始裝置以進行探索，並引導 Cisco DNA 中心使用 Cisco Discovery Protocol 來尋找連線的芳鄰。使用 Cisco Discovery Protocol 時，請將預設躍點數降至一個合理的數字，以加快探索速度。

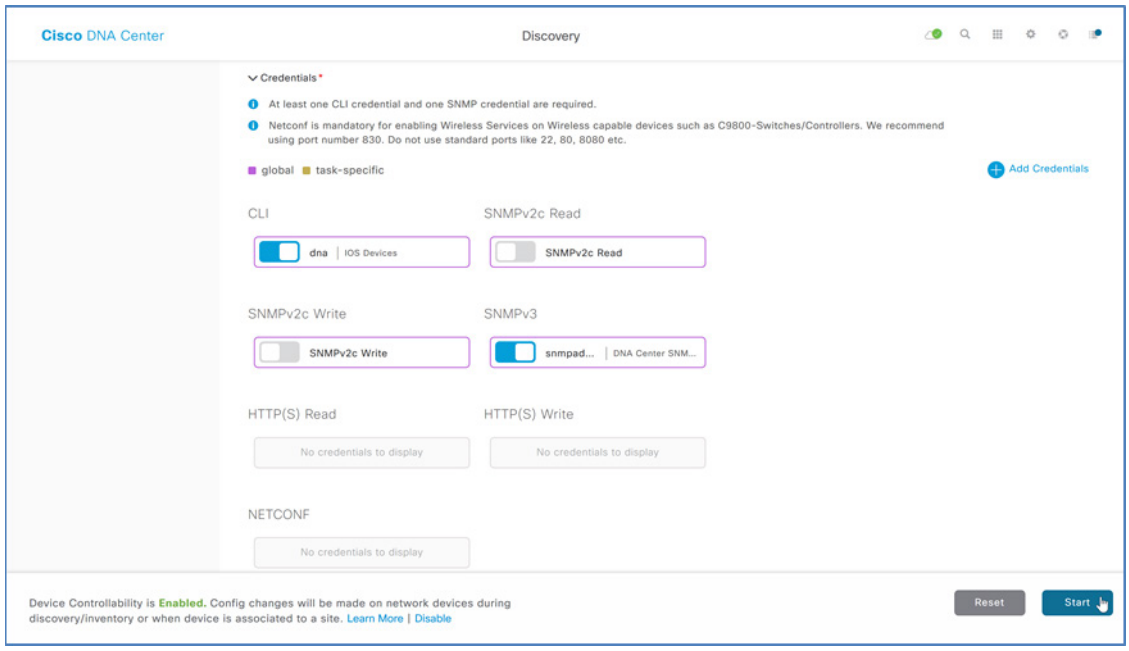
步驟 1. 導覽至主 Cisco DNA 中心控制台，捲動至 **Tools** 區段，按一下 **Discovery** 並提供**探索名稱**。選擇 **Range** 並在 **IP Ranges** 中輸入開始和結束 IP 迴路位址（如要涵蓋單一位址，請輸入該範圍開頭和結尾的位址）。對於 **Preferred Management IP**，如果裝置具有用於管理的回送介面，則選擇 **UseLoopBack**。

技術提示
如果您使用的是具有超大型組態的 Cisco Catalyst 6800 系列交換器，則可以在設定模式中將以下指令新增到該交換器，以避免探索逾時： `snmp mib flash cache`

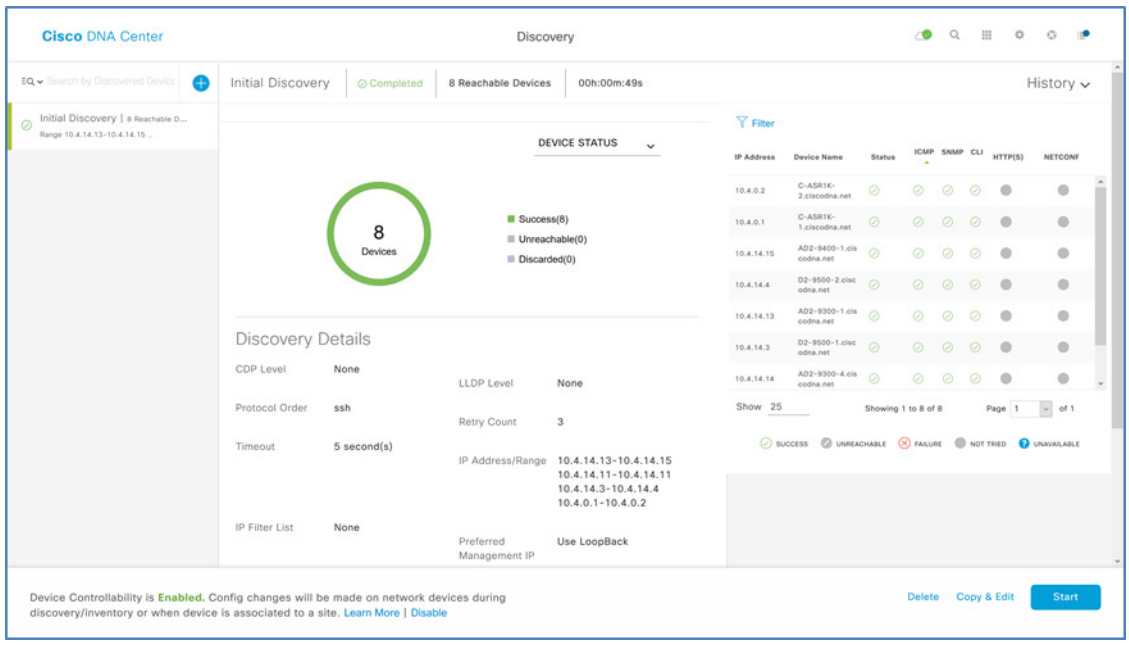
步驟 2. 如果您有任何額外的範圍，請按一下第一個範圍旁邊的 **+**（加號），輸入其他範圍，並對剩餘的範圍重複此操作。



步驟 3. 向下捲動，以驗證用於探索的 CLI 憑證，以及透過 Cisco DNA 中心裝置可控性功能將其推送到裝置的 SNMP 憑證設定，然後按一下底部的 **Start**。



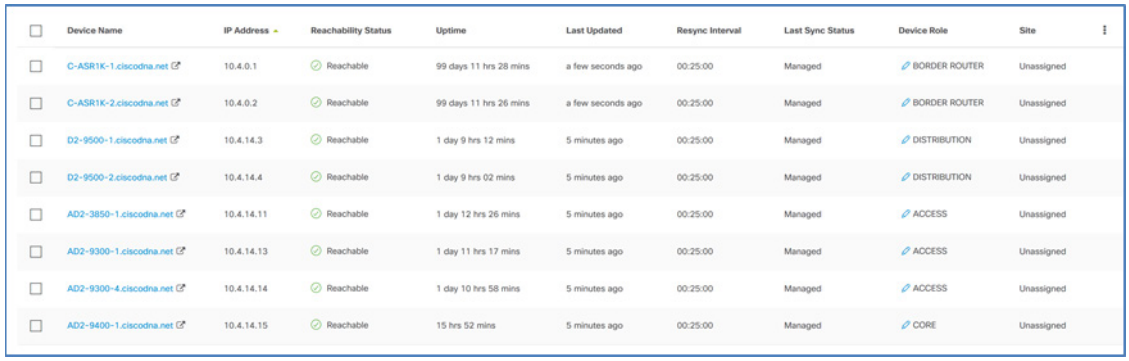
在執行探索時，畫面上會顯示探索詳細資訊。



在已啟用裝置可控性的裝置探索完成時，使用 CLI 指派並存放在本機裝置上的憑證將用來作為備份。僅當失去與 ISE 的連線時，才會使用本機憑證來存取主要集中憑證。

步驟 4. 如果存在任何探索失敗，請檢查裝置清單、解決問題，並重新啟動這些裝置的探索以及要新增到庫存的任何其他裝置的探索。

步驟 5. 成功完成所有探索任務後，請導覽至主要 Cisco DNA 中心儀表板，然後在 **Tools** 區段下，按一下 **Inventory**。螢幕上會顯示已探索的裝置。在庫存收集完成後，每台裝置都會顯示 **Managed** 同步狀態，表明 Cisco DNA 中心維持內部模型鏡像裝置實體部署。



Cisco DNA 中心現在可以存取裝置，同步設定庫存 ，並在裝置上進行設定變更。

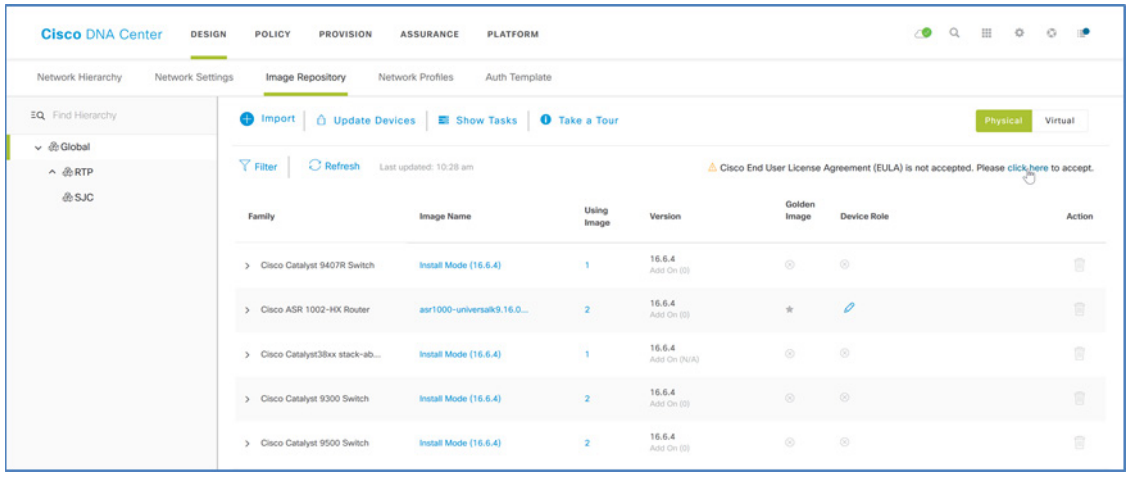
技術提示
您可以在庫存表的標題列右側，調整要顯示的列。使用 **Device Role** 欄查看藉由探索根據裝置類型所指派的裝置角色，以便將角色調整至最能反映裝置實際部署的角色（例如存取、分佈、核心或邊界路由器），其中在此顯示的邊界路由器是通用的非網狀架構裝置角色。現在調整角色就可以改善初始拓撲圖的外觀，而不必在後續程序中調整角色。

程序 8.　管理庫存中裝置的軟體映像檔

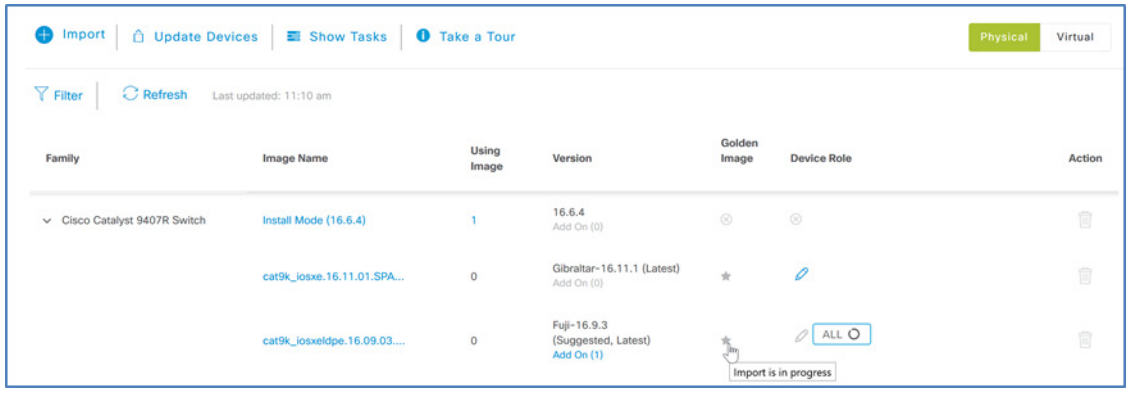
為了實現 SD-Access 的完整功能，Cisco DNA 中心的 SD-Access 套件具有其佈建裝置的最低軟體版本要求。內置於 Cisco DNA 中心的軟體映像檔管理功能可用於升級未執行建議映像檔版本的裝置。您可以使用 Cisco.com 上的 SD-Access 硬體和軟體相容性對照表尋找推薦用於 SD-Access 的映像檔。用於驗證的映像檔在附錄 A：產品清單中列出。

使用以下步驟將映像檔和軟體維護更新 (SMUs) 的軟體更新套用於裝置，方法是匯入所需的映像檔，將映像檔標示為金色，並將映像檔套用於裝置。

步驟 1.　導覽至主 Cisco DNA 中心控制台，按一下 **Design**，然後按一下 **Image Repository**。如果是第一次使用本軟體，則在右上的 **Cisco End User License Agreement** 通知中，選擇 **click here**，然後按一下 **Accept License Agreement**。



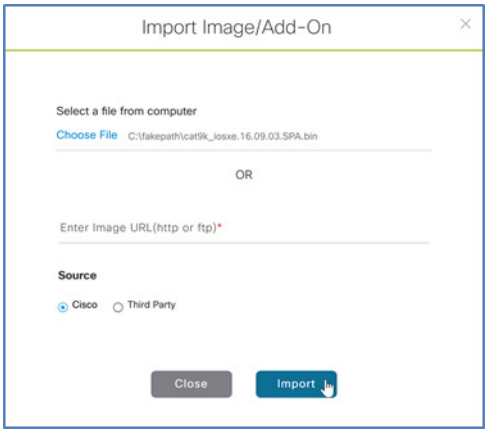
步驟 2.　如果您選擇讓 Cisco DNA 中心下載新映像檔以套用於裝置，則在 **Image Name** 欄下方按一下列為裝置系列的映像檔旁邊的向下箭頭，然後按一下 **Golden Image** 星號，將相應的映像檔標記為該平台的偏好設定。



尚未匯入的映像檔將會使用 Cisco.com 憑證自動匯入。您可以使用 **Settings**（齒輪圖示） **> System Settings > Settings > Cisco Credentials** 來更新 Cisco.com 憑證。

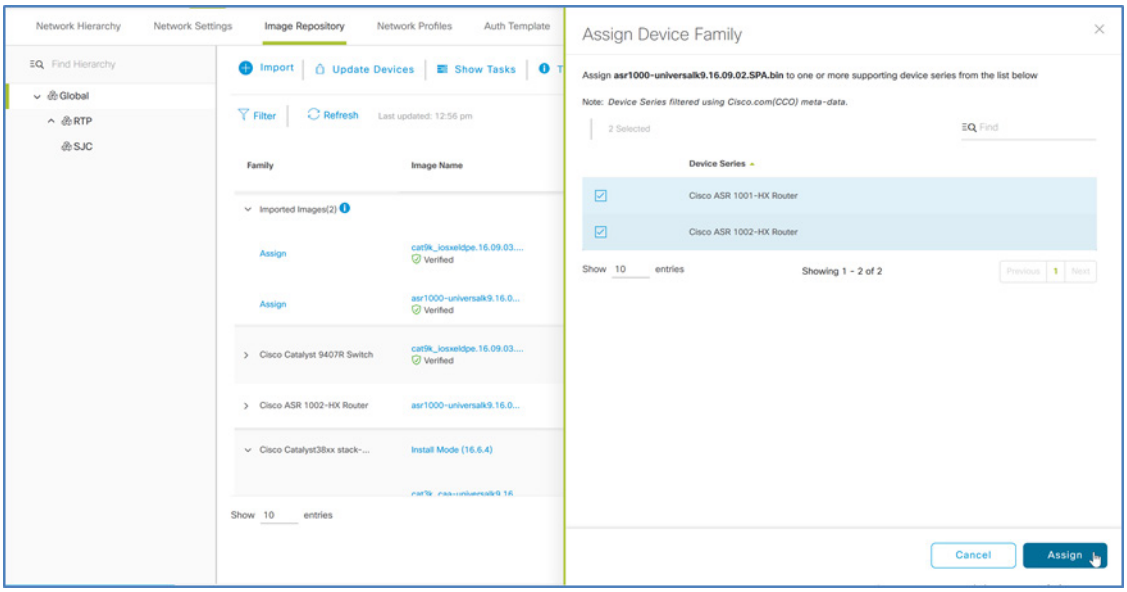
步驟 3.　重複匯入並將映像檔標記為金色，直到所有裝置都標有適當的映像檔。

步驟 4.　如果您選擇從本機電腦匯入映像檔，請按一下「Import Image/Add-On」對話方塊中的 **+ Import**，選擇一個檔案位置，然後按一下 **Import**。



隨即開始將映像檔匯入 Cisco DNA 中心。

步驟 5. 匯入完成後，將匯入的映像檔指派給裝置。在匯入的映像檔旁邊，按一下 **Assign**，選擇要使用映像檔的裝置，然後在快顯視窗中按一下 **Assign**。



該映像檔位於存放庫中，並可用於將這些裝置標記為金色。

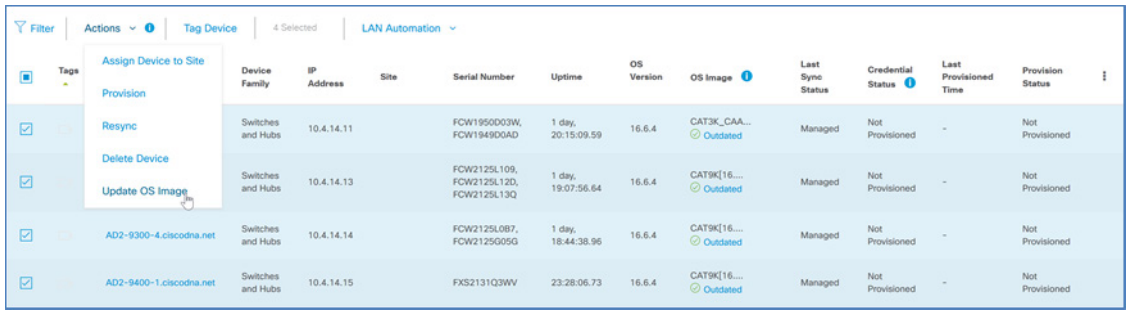
步驟 6. 針對具有新指派映像檔的每部裝置，按一下 **Golden Image** 星號，將相應的映像檔標記為平台的偏好設定。

步驟 7. 針對您希望使用 Cisco DNA 中心部署的所有映像檔重複這些步驟。具有已指派金色映像檔的所有裝置類型均已準備就緒，可用於發佈軟體映像檔。

程序 9. 使用軟體映像檔管理以更新裝置軟體

Cisco DNA 中心對庫存中的裝置執行合規性檢查，與標記為金色的映像檔進行比較。與金色映像檔不符的裝置會在庫存中標記為 **Outdated**。將映像檔更新為標記為金色的版本。庫存收集必須已成功完成，且裝置必須處於 **Managed** 狀態，然後才能繼續。您首先要發佈軟體映像檔，並排程或手動啟動具有已發佈映像檔的裝置。

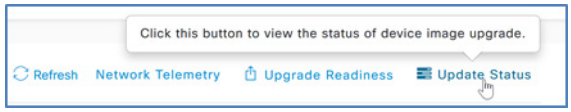
步驟 1. 導覽至 **PROVISION > Devices > Inventory**，選擇標記為 **Outdated** 的所有裝置，然後在 **Actions** 選單中，按一下 **Update OS Image**。為了提高對更新的控制，請在可以重新開機的裝置上啟動作業系統更新，而不影響與您正在更新的其他裝置的連線。



步驟 2. 在顯示的滑出項中，在 **Distribute > When** 下方選擇 **Now**，按 **Next**，在 **Activate** 下方選擇 **Schedule Activation after Distribution is completed**，按 **Next**，然後按一下 **Confirm** 下方的 **Confirm** 按鈕。

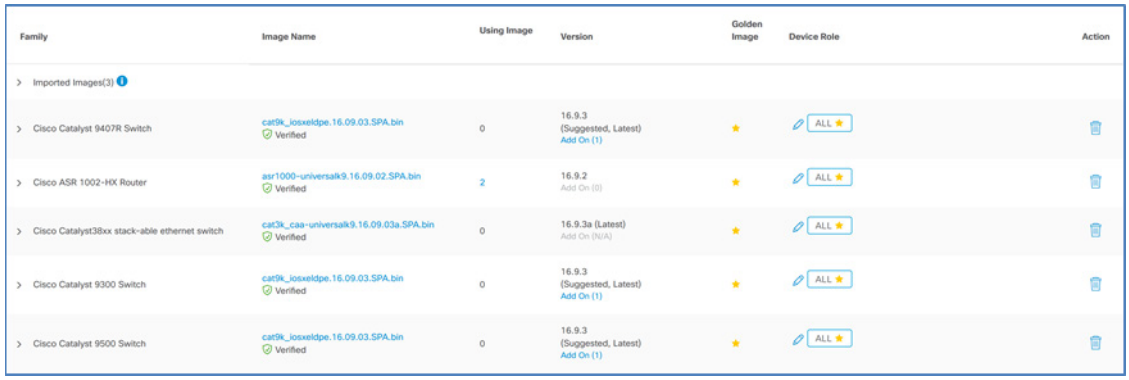
映像檔將被發佈至所選裝置。

步驟 3. 在右上角，按一下 **Update Status**。



狀態螢幕會提供比主畫面更多的詳細資訊，包括對任何失敗的解讀。當 **In Progress** 狀態變更為 **Successful** 時，請使用 **Refresh** 按鈕進行觀察。

步驟 4. 根據需要重複此程序，將裝置軟體更新為網路部署所需的版本。完成後，要部署的所有裝置都與金色映像檔相關聯，並已安裝映像檔。



程序：佈建用於 SD-Access 的底層網路

在 Cisco DNA 中心探索並對執行用於 SD-Access 的相應軟體版本的裝置進行管理控制後，請使用 Cisco DNA 中心以便在底層網路中佈建裝置。

程序 1.　使用 LAN 自動化功能佈建底層網路交換器

選用

如果使用 Cisco DNA 中心的 LAN 自動化功能將全新未設定的 LAN 交換器部署到底層網路中，請使用此程序。使用上述程序設定一或多個種子裝置（與全新未受管網路連線的受管裝置）、藉由 PnP 推送的裝置 CLI 和 SNMP 憑證，以及用於連線且可透過網路存取的 IP 位址集區。雖然這並不是嚴格要求，但每個種子裝置通常是在後續程序中指派作為邊界的交換器，並且必須具有適當的 VTP 模式和 MTU 設定（範例：VTP 透明模式、系統 MTU 9100）。連線到要探索裝置的種子裝置上的連接埠必須位於第 2 層模式（存取埠與路由埠），且種子裝置連接埠不能是專用的頻外 (OOB) 管理連接埠。

技術提示

LAN 自動化允許從支援的種子裝置探索支援的交換器（在本驗證中使用的交換器在附錄中列出）。已探索的交換器會直接連線到所選的種子裝置介面（在 LAN 自動化裝置啟動期間無法連線 OOB 管理連接埠，因為會封鎖非 OOB 連接埠上的 LAN 自動化），以及最多額外一個躍點的連線交換器，總計距離種子裝置兩個躍點。提供的憑證可讓 Cisco DNA 中心和種子裝置協同工作，以便為發掘到的裝置進行設定，並將其新增到受管庫存中。由於已探索的裝置必須執行沒有先前設定的 PnP 代理程式，因此必須將先前設定的任何交換器恢復到 PnP 代理程式正在執行的狀態，透過使用以下設定模式和執行模式指令來完成：

```
(config)#config-register 0x2102
(config)#crypto key zeroize
(config)#no crypto pki certificate pool
delete /force vlan.dat
delete /force nvram:*.cer
delete /force nvram:pnp*
delete /force flash:pnp*
delete /force stby-nvram:*.cer
delete /force stby-nvram:*.pnp*
! previous two lines only for HA systems
write erase
reload
```

請勿儲存重新載入程序的設定。如果要準備交換器堆疊以實現 LAN 自動化，請對堆疊中的每台交換器使用相同的還原指令。

交換器堆疊要求不會為 LAN 自動化進行變更，堆疊中的所有交換器都必須執行相同的軟體授權和支援 IP 路由功能的版本，並且應處於安裝模式（而非套件模式）。如果您希望提高對連接埠編號和堆疊行為的控制，則您可以在開始 LAN 自動化程序之前，調整交換器堆疊編號，同時影響交換器，使其成為堆疊內作用中的角色，方法是透過在執行模式下使用下列指令來提高優先順序：

```
switch [switch stack number] renumber [new stack number]
switch [switch stack number] priority 15
```

找出庫存中由 Cisco DNA 中心管理的一或兩個裝置，以指派給網站上的種子裝置角色。相同的種子可用於執行多項 LAN 自動化功能，允許將已探索的裝置指派給每次執行的不同建築物或樓層。

步驟 1.　在主 Cisco DNA 中心儀表板中，導覽至 **PROVISION > Devices > Inventory**。選擇最多兩個種子裝置，在 **Actions** 下拉式功能表中，按一下 **Assign Device to Site**，在 **Assign Device to Site** 的畫面中，選擇裝置網站指派，然後按一下 **Apply**。

步驟 2. 如果您使用的是 Catalyst 6800 系列種子裝置，請使用介面設定模式指令將通往已探索裝置的連接埠變更為第 2 層連接埠。

```
switchport
```

儲存設定變更後，透過導覽至主 Cisco DNA 中心儀表板重新同步裝置，在 **Tools** 下方選擇 **Inventory**，選擇已修改的 Catalyst 6800 交換器，然後在頂端 **Actions** 下拉式功能表中，選擇 **Resync**。

技術提示

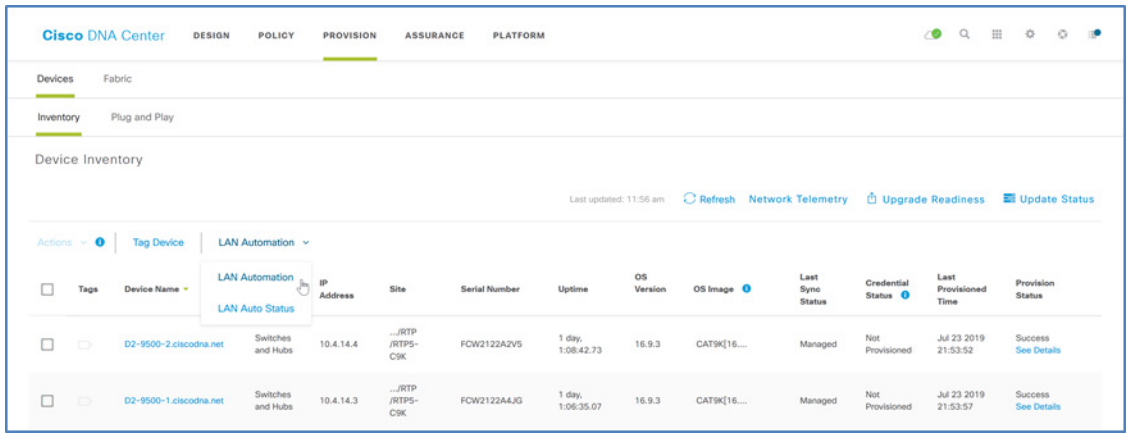
用於 LAN 自動化的 IP 集區的大小應調整為明顯大於要探索的裝置數。集區分為兩半，一半用於種子裝置提供的 VLAN 1 DHCP 服務。集區的另一半會被再次分為兩半，留出總位址空間的四分之一作為點對點連結定址，另外的四分之一作為迴圈定址。端點不得插入交換器中，因為可能會耗去用於 PnP 佈建的 IP 集區 DHCP。

LAN 自動化集區中的位址需要由 Cisco DNA 中心存取，以成功完成佈建，並且不得用於網路中的其他位置。如果您的 Cisco DNA 中心將可選的專用管理網路用於 web 存取埠，而不是使用預設路由的單一連接埠，則必須確保可透過企業網路基礎架構連接埠使用通往 LAN 自動化 IP 集區的路由。如果 IP 集區未包含在 Cisco DNA 中心設定的路由中，請使用 SSH 埠 2222 連線到 Cisco DNA 中心，然後以 maglev 身份登入並執行以下指令：

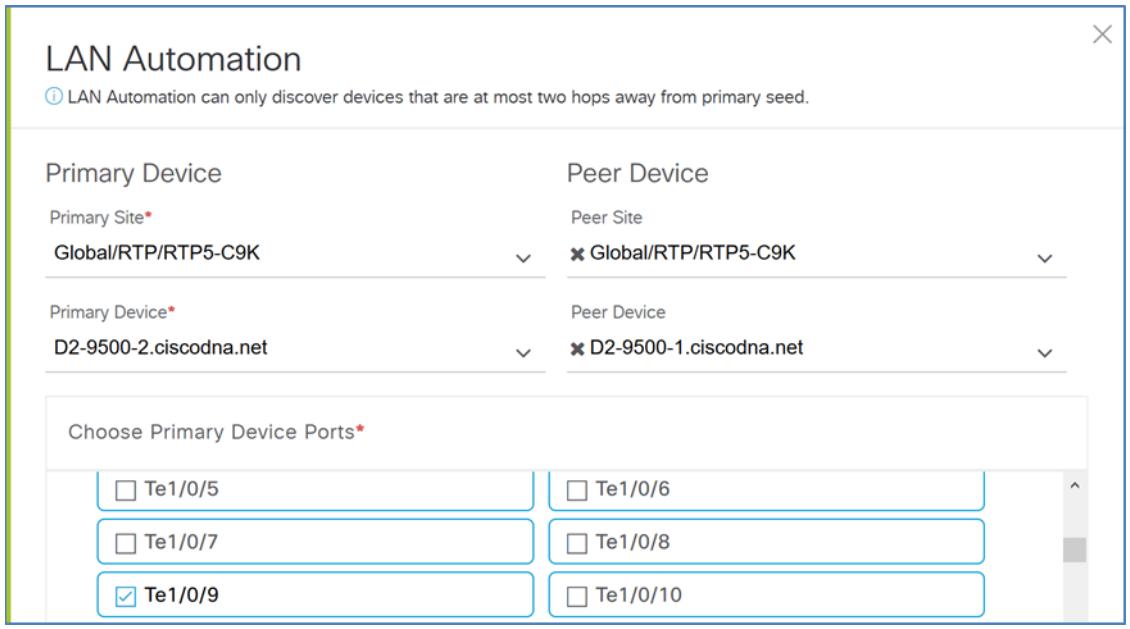
```
sudo maglev-config update
```

在啟動 LAN 自動化之前，請使用設定精靈將靜態路由設定為在適當的網路介面卡上包含 IP 集區。

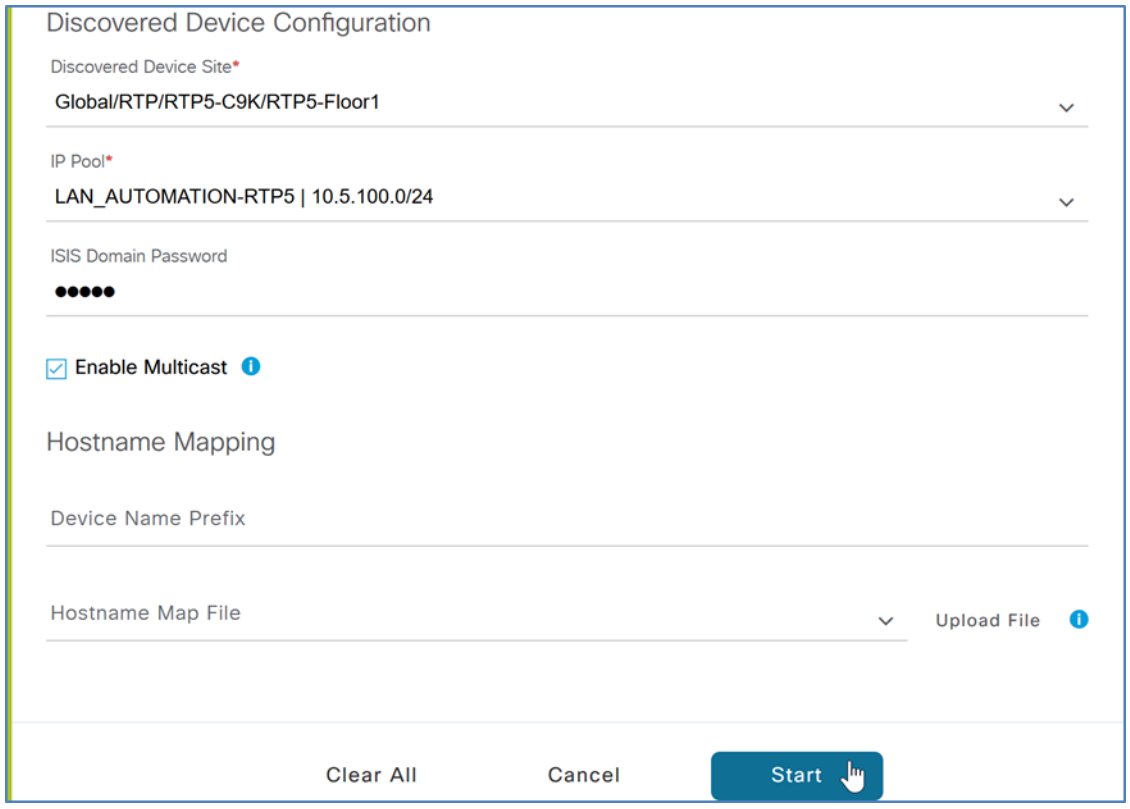
步驟 3. 導覽至 **PROVISION > Devices > Inventory**。在頂部，按一下 **LAN Automation** 下拉式功能表，然後按一下 **LAN Automation**。



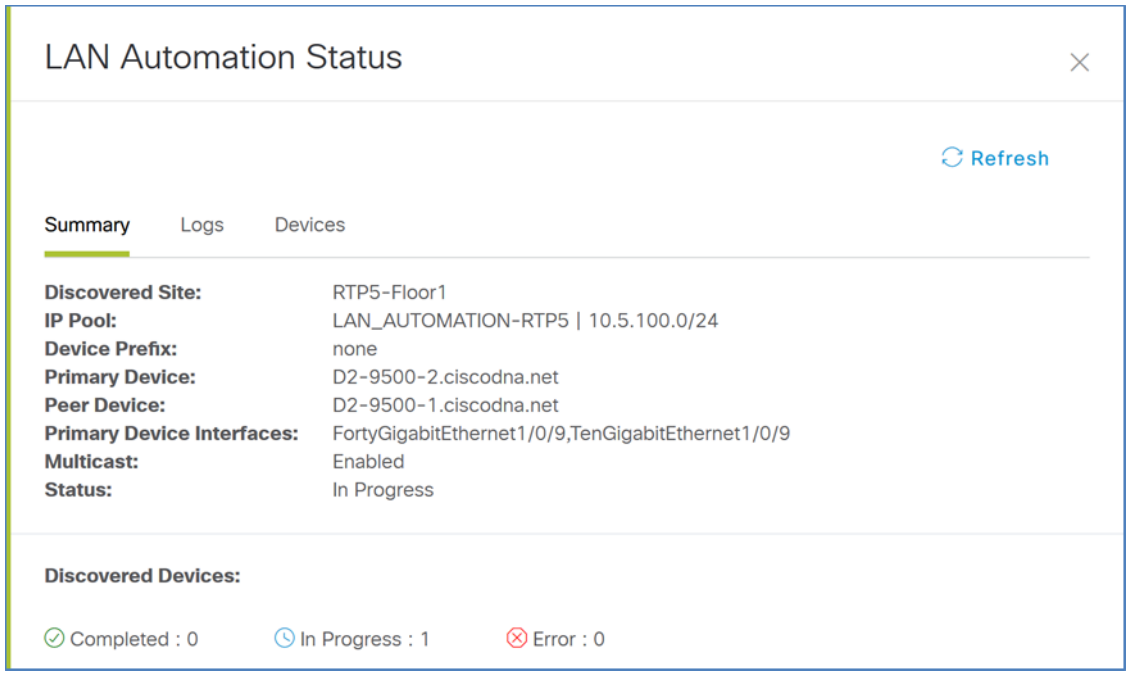
步驟 4. 在「LAN Automation」滑出項的右側，填寫用於探索的參數。在 **Primary Device** 下，提供**主網站 *、主要裝置 *、選擇主裝置埠 ***，在 **Peer Device** 下提供**對等裝置網站**和**對等裝置**。



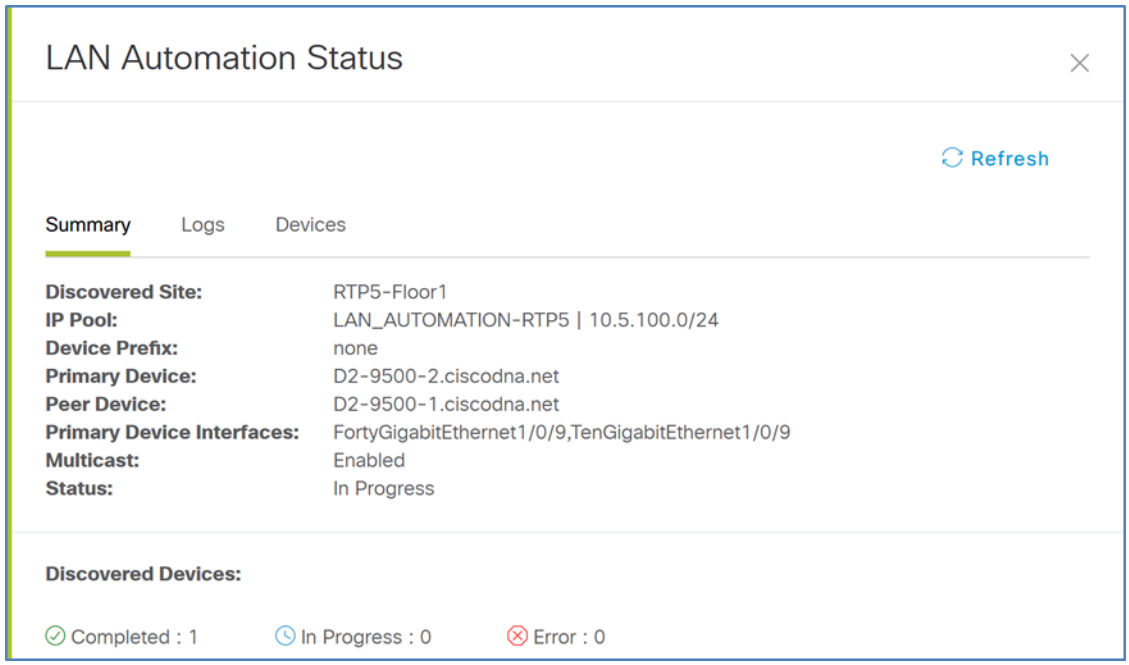
步驟 5. 在「LAN Automation」滑出項的右側，繼續填寫用於探索的參數。在 **Discovered Device Configuration** 下，提供**已探索的裝置網站 *** 、**IP 集區 ***，如果已使用則請提供 **ISIS 網域密碼**，選擇 **Enable Multicast**，然後按一下 **Start**。



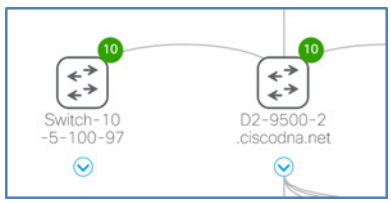
步驟 6. 在頂部，按一下 **LAN Automation** 下拉式功能表，然後按一下 **LAN Auto Status** 以查看進度。



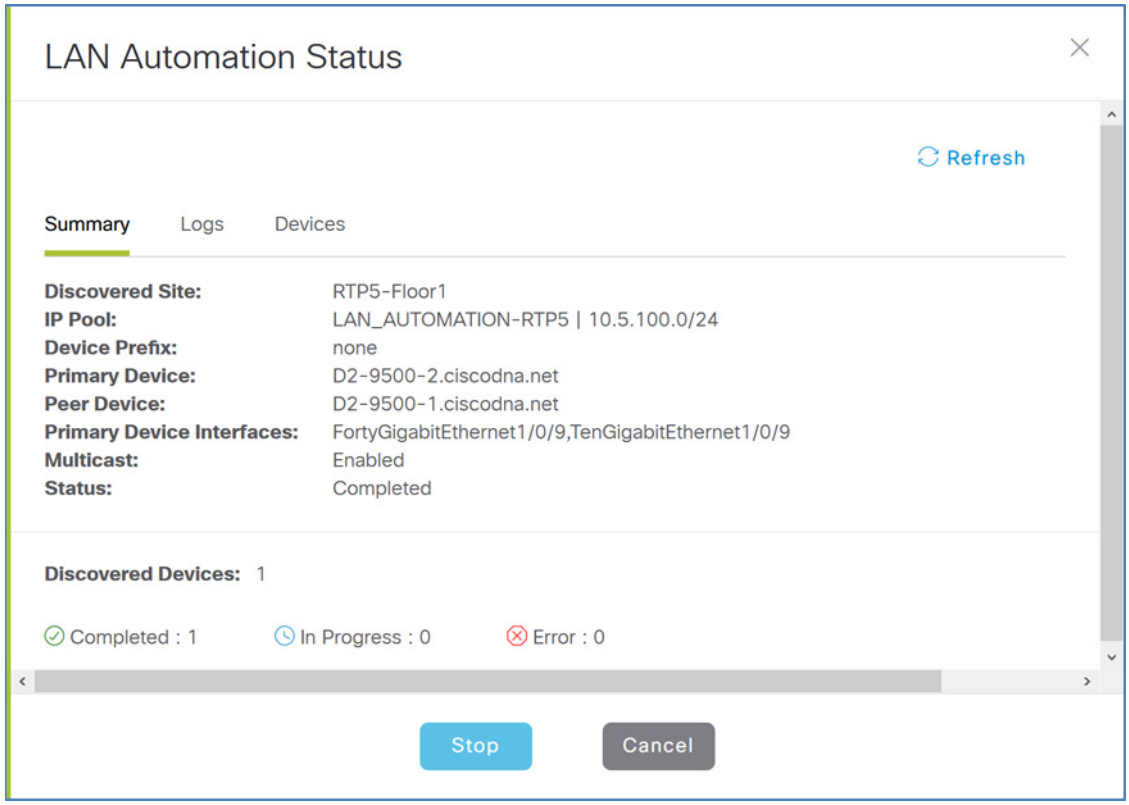
請勿在此步驟中按下 **Stop**。等到所有裝置均顯示 **Completed** 狀態，然後繼續進行下一個驗證步驟。過早停止 PnP 程序會使探索處於需要手動介入進行恢復的狀態。探索距離種子裝置多一個躍點的裝置可能需要更長的時間才能完成。



步驟 7. 導覽至主 Cisco DNA 中心儀表板，在 **Tools** 下選擇 **Topology**。所有連結均應探索。如果拓撲中缺少任何連結，請驗證實體連線。



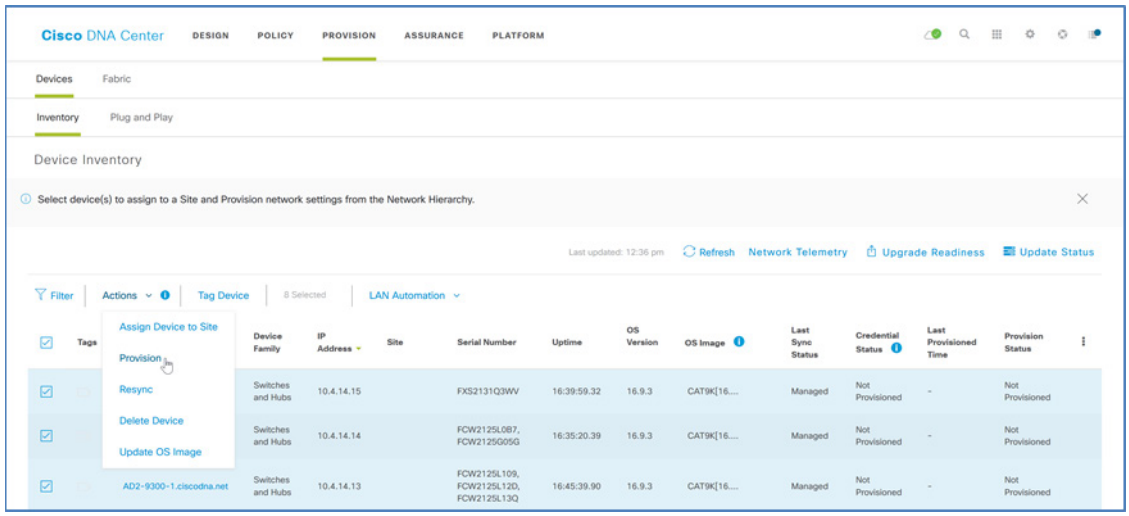
步驟 8. 導覽至 **PROVISION > Devices > Inventory**。在頂部，按一下 **LAN Automation** 下拉式功能表，按一下 **LAN Auto Status**。在裝置探索全部均已達到 **Completed** 狀態後，按一下 **Stop**。LAN 自動化在 VLAN 1 上關閉所有第 2 層連線，底層網路 IS-IS 路由程序可用於通往路由網路的連線，而裝置則受管於庫存中。



程序 2. 佈建裝置並指派到網站以準備進行 SD-Access

佈建網路裝置，然後將裝置指派到網站，以整合到 SD-Access 網路中。

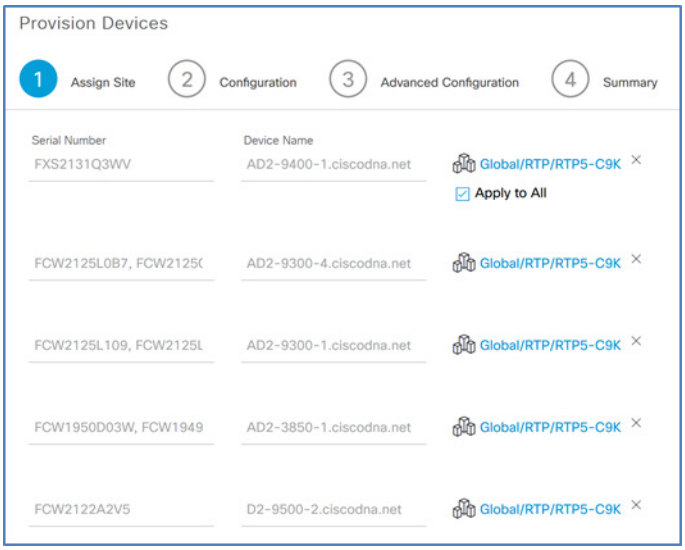
步驟 1. 在 Cisco DNA 中心中，導覽至 **PROVISION > Devices > Inventory**，選擇相同類型的裝置（範例：所有交換器）以佈建到網路中，按一下 **Actions**，然後按一下 **Provision**。



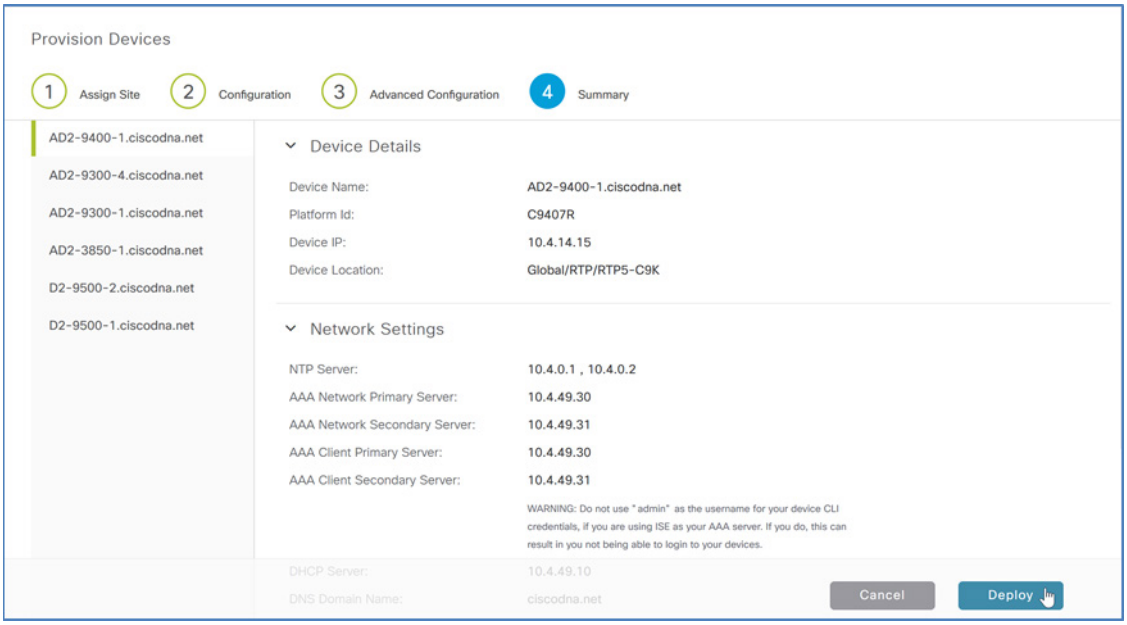
隨即將顯示 **Provision Devices** 精靈畫面。

技術提示
裝置必須是屬於相同類型（範例：所有路由器）才能同時佈建。您可以根據需要將佈建作業分組為多個小型批次，以進行常見的網站指派。

步驟 2. 在第一個精靈畫面中，為裝置選取網站指派，然後按一下畫面底部的 **Next**。



步驟 3. 按 **Next** 兩次以跳過 **Configuration** 和 **Advanced Configuration** 畫面，在 **Summary** 畫面中查看每個裝置的詳細資訊，然後按一下 **Deploy**。

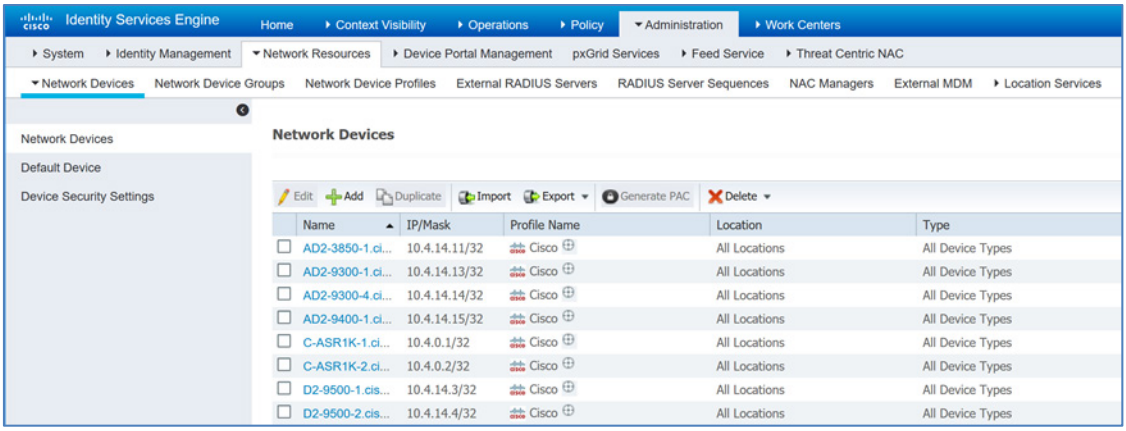


步驟 4. 在快顯畫面上，保留 **Now** 的預設選項，然後按一下 **Apply**。

隨即開始每個裝置的設定，並在每個裝置成功佈建時顯示狀態訊息。裝置庫存畫面會更新 **Provision Status** 和 **Sync Status**。使用 **Refresh** 按鈕更新最終狀態。

步驟 5. 對於新增的每一批裝置，重複 Cisco DNA 中心佈建步驟。Cisco DNA 中心 pxGrid 整合會更新 ISE 中的裝置。

步驟 6. 登入 ISE 並導覽至 **Administration > Network Resources > Network Devices**，以驗證 ISE 整合功能。隨即將會顯示佈建的裝置。



程序：佈建 SD-Access 重疊網路

在 Cisco DNA 中心使用已新增到庫存並佈建到網站的已探索裝置建立網狀架構重疊網路。Cisco DNA 中心可自動執行支援 SD-Access 重疊網路的額外裝置設定。

SD-Access 解決方案支援佈建下列網狀架構結構：

- 網狀架構網站：獨立的網狀架構，包括控制平面節點和邊緣節點功能，使用網狀架構邊界節點以輸出網狀架構網站，通常包括 ISE PSN 和網狀架構模式 WLC
- 中繼網站：也稱為傳輸網路，將網狀架構網站連線到外部網路（IP 型傳輸）或連線到一或多個網狀架構網站，並原生保留分段（SD-Access 傳輸）
- 網狀架構網域：包含一或多個網狀架構網站以及任何相應的傳輸網站

IP 型傳輸網路將網狀架構連線到外部網路，通常使用 VRF 進行 IP 連線。SD-Access 傳輸會傳送 SGT 和 VN 資訊，在網狀架構網站之間傳輸原則和分段，進而建立一個分散式園區。此設定

技術提示

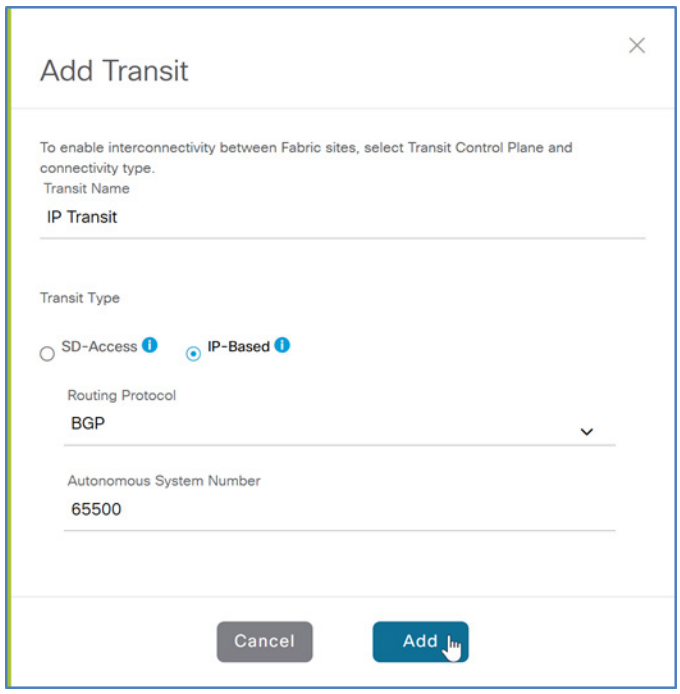
附錄中列出的 Cisco DNA 中心軟體和 Cisco IOS 軟體不包括對 SD-Access 傳輸的驗證，這些功能會在軟體定義的分散式園區規範性部署指南中介紹。您可以透過搜尋 Cisco.com 上的 SD-Access 硬體和軟體相容性對照表，尋找可能支援其他選項的備用軟體版本。

附錄中列出的 Cisco DNA 中心軟體和 Cisco IOS 軟體不包括對 SD-Access 傳輸的驗證，這些功能會在軟體定義的分散式園區規範性部署指南中介紹。您可以透過搜尋 Cisco.com 上的 SD-Access 硬體和軟體相容性對照表，尋找可能支援其他選項的備用軟體版本。

程序 1.　建立 IP 型傳輸網站、網狀架構網域和網狀架構網站

IP 型傳輸網站代表 BGP 遠端自主系統 (AS)。本機 BGP AS 會在後續步驟中設定為網狀架構邊界佈建的一部分。

步驟 1.　使用 Cisco DNA 中心，導覽至 **PROVISION > Fabric**，在右上角按一下 **+ Add Fabric or Transit**，按一下 **Add Transit**，在滑出項提供**中繼名稱**（範例：IP_Transit），選擇 **IP-Based**，針對 **Routing Protocol** 選擇 **BGP**，輸入遠端 BGP AS 的**自主系統編號**（範例：65500），然後按一下 **Add**。

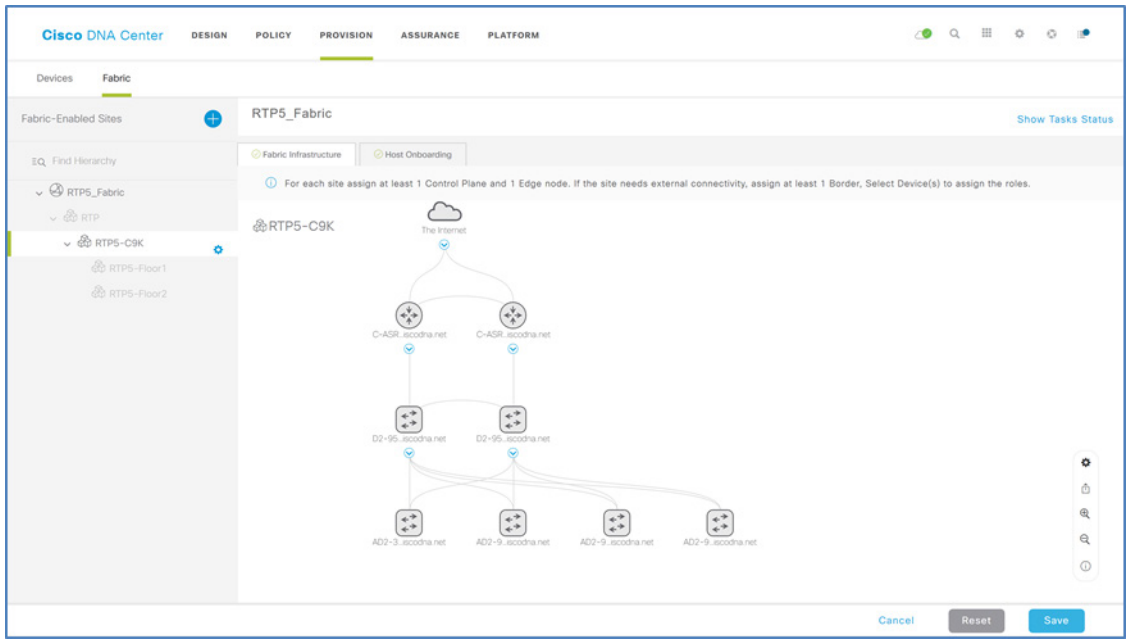


系統將顯示狀態訊息，並建立傳輸。

步驟 2. 導覽至 **PROVISION > Fabric**，在右上角按一下 **+ Add Fabric or Transit**，按一下 **Add Fabric**，在滑出項提供**網狀架構名稱**（範例：RTP5_Fabric），使用網站層級架構以選取一個位置（包括網站）以啟用網狀架構（範例：RTP5-C9K），然後按一下 **Add**。

建立新的園區網狀架構。

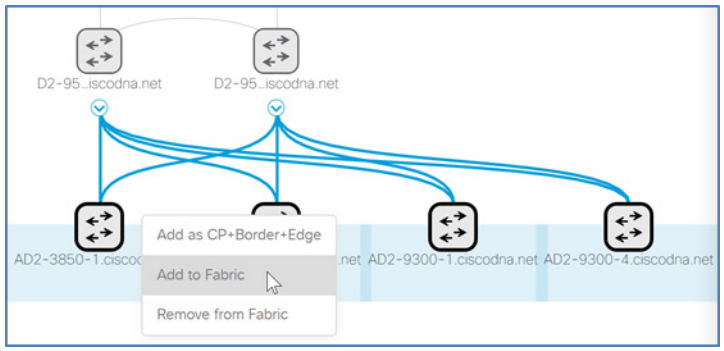
步驟 3. 按一下剛建立的網狀架構網域名稱（範例：RTP5_Fabric），在左側的 **Fabric-Enabled Sites** 層級架構中，選擇在上一步中新增的網站（範例：RTP5-C9K）。顯示網狀架構和相關網站的檢視圖。



如果顯示的網狀架構拓撲圖未模仿已部署的兩層（分佈/存取）或三層（核心/分佈/存取）拓撲，請透過導覽至 **Tools > Inventory** 來修正拓撲，庫存表的標題列右側上調整要顯示的欄位以包括 **Device Role**，然後調整角色以反映裝置的實際部署。在修改已更新檢視的裝置角色後，返回網狀架構網域拓撲檢視圖。

程序 2.　建立網狀架構覆蓋

步驟 1.　在網狀架構域拓撲檢視圖中，按住 shift 鍵，按一下作為網狀架構邊緣節點的所有節點，然後在快顯方塊中，按一下 **Add to Fabric**。



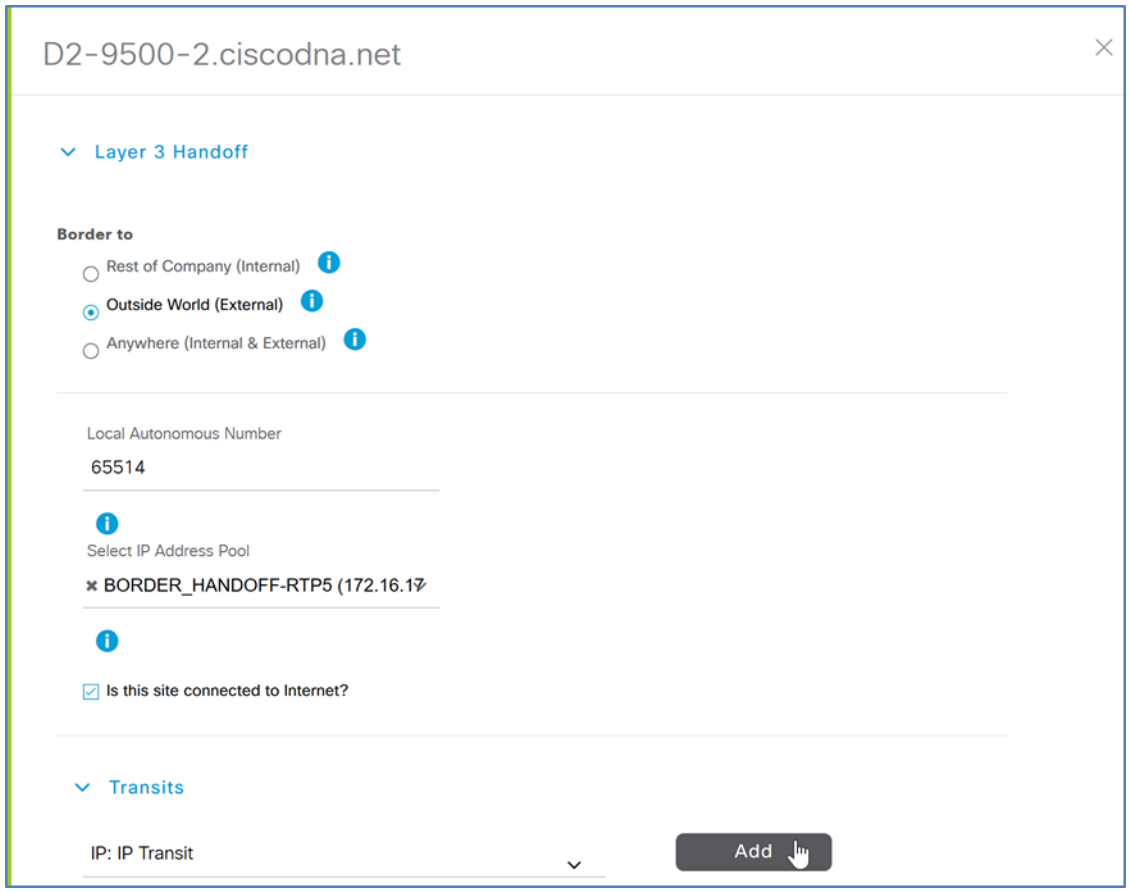
隨即顯示藍色圖示邊界和網狀架構角色符號，表示裝置的預期目標行為。

步驟 2.　如果您擁有的網狀架構節點專用於不具有邊界功能的控制平面節點的角色，請按一下該節點，然後在快顯方塊中，按一下 **Add as CP**（控制平面）。

對不具邊界功能的備援專用控制平面節點重複此步驟。

技術提示
如果邊界節點是使用列於「附錄 A：產品清單」中軟體的 Cisco Nexus 7700 系列交換器，則請使用專用控制平面節點、將其直接連線到 7700 系列，並設定為外部邊界節點。如果您的 NX 版本需要，請啟用 MPLS 授權。將實體連結上的 MPLS LDP 設定為控制平面節點，以支援控制平面連線。

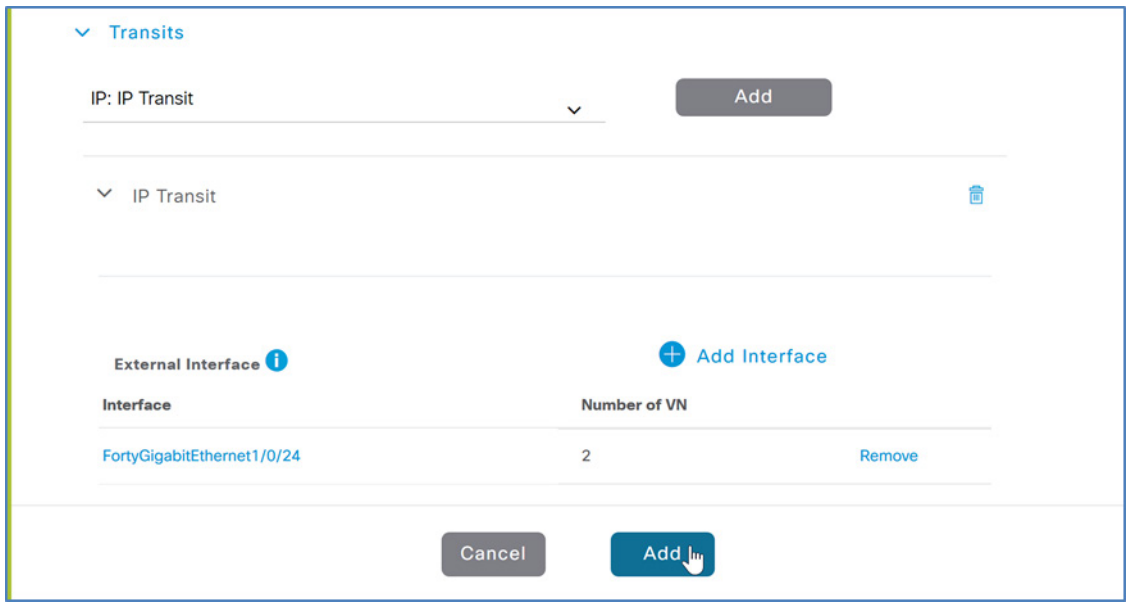
步驟 3.　按一下裝置以執行網狀架構邊界角色，在快顯方塊中按一下 **Add as Border** 或 **Add as CP+Border**（如果跳過上一步）並填寫其他滑出的對話方塊。在 **Layer 3 Handoff** 下，選擇**邊界**至（範例：Outside World (External)），提供**BGP 本機自主編號**（範例：65514），在 **Select IP Address Pool** 下，選擇先前為邊界連線功能設定的全域集區（範例：BORDER_HANDOFF-RTP5），針對外部邊界選擇 **Is this site connected to the Internet?**，在 **Transit** 選單中選取傳輸（範例：IP: IP Transit），然後按一下傳輸旁邊的灰色 **Add** 按鈕。



隨即將顯示其他 **IP Transit** 區段。

技術提示
如果邊界是將結束網狀架構連線到網路其餘部分的唯一路徑，則應選擇外部邊界。在具有組合控制平面和邊界節點功能，且節點使用內部邊界功能的情況下，在使用「附錄 A：產品清單」中所示已驗證版本時，可能需要進行其他控制平面過濾。

步驟 4. 按一下 **IP Transit** 內容，按一下顯示的 **+ Add Interface**，在滑出方塊中選擇連線到網狀架構外部的融合路由器的介面，在顯示的網狀架構外部裝置的 BGP **Remote AS Number** 下， 展開 **Virtual Network** 選擇面板，選取網狀架構中使用的每個 VN，以包含在網狀架構外部的第 3 層遞交中（範例：INVRA_VN，OPERATIONS），按一下 **Save**，然後按一下 **Add**。

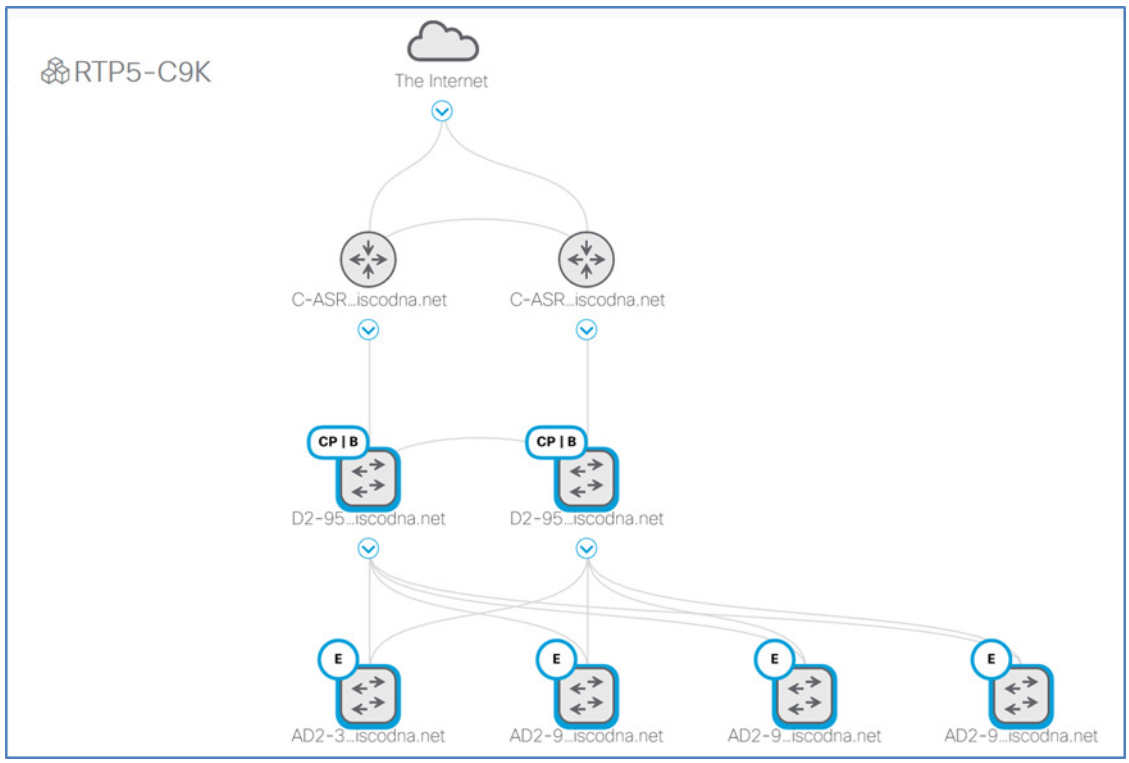


確認其他資訊快顯視窗。

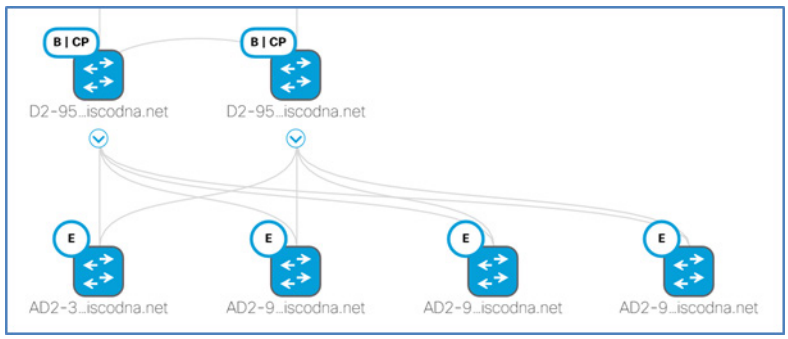
步驟 5. 如果有額外的網狀架構邊界節點，請對其重複先前的兩個步驟。

技術提示
如要設定從邊界到網路其餘部分的 VRF-Lite 遞交介面，則需要使用 802.1 Q 標記的介面。如同在將管理設定至邊界裝置以進行網路探索的程序中所述，如果要使用要轉換的備援連結上的頻內連線來管理邊界，請先透過標記介面進行連線。當使用本指南中驗證的 SD-Access 版本時，如果介面已包含非標記設定，則佈建不會成功。

步驟 6. 將所有要求的角色指派到網狀架構中的節點後，按一下底部的 **Save**，使用 **Now** 的預設選項，然後按一下 **Apply**。您的園區網狀架構網域已完成建置。



網狀架構圖示將變為藍色，表達您建立網狀架構的意圖。佈建裝置實際上可能需要更長時間才能完成。



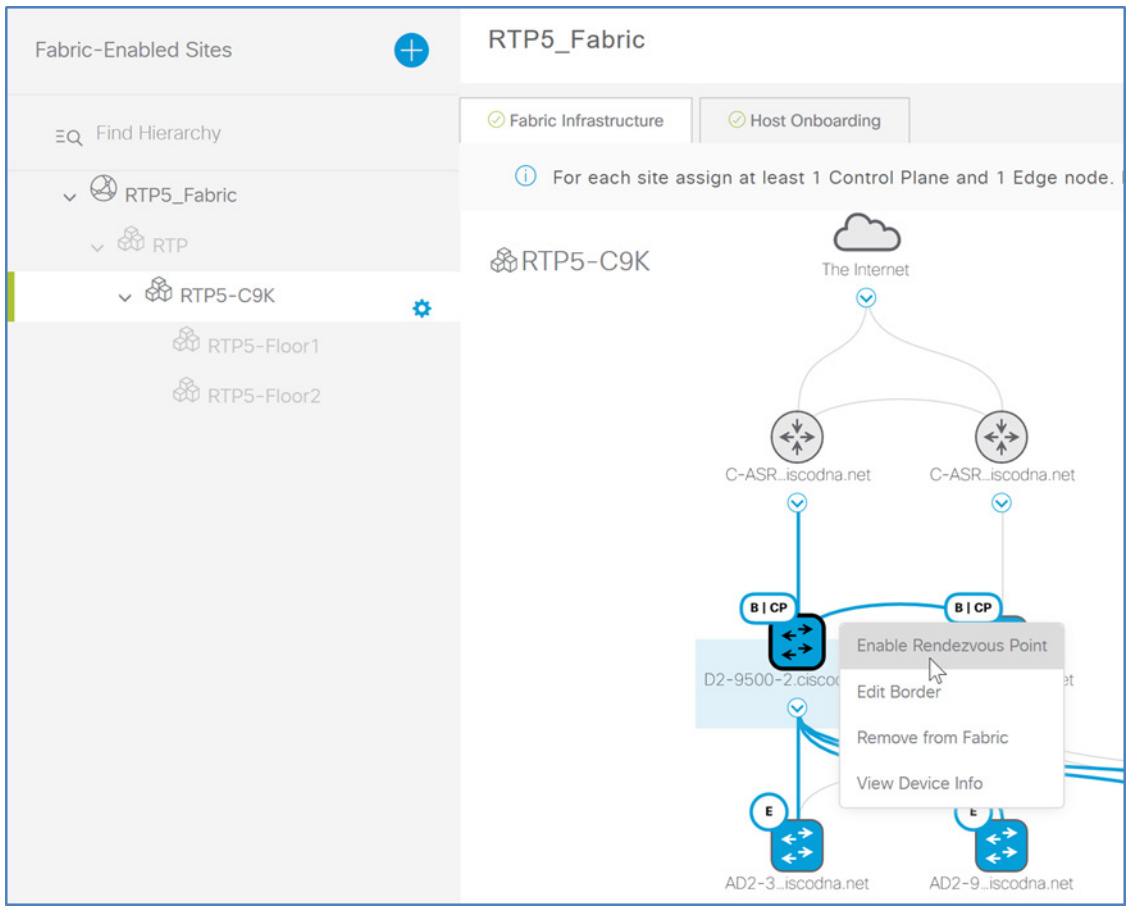
程序 3. 為網狀架構啟用多點傳送

使用此程序以在網狀架構覆蓋層中設定多點傳送支援。

SD-Access 網狀架構可支援任何來源多點傳送 (ASM) 和特定來源的多點傳送 (SSM)。來源可以位於網狀架構內或網狀架構外，而集結點設定僅限在網狀架構邊界節點上取得。PIM 訊息在邊界節點和網狀架構邊緣之間進行單點傳送，並將多點傳送封包複製到面向網狀架構邊緣節點的前端網狀架構邊界裝置上。

步驟 1. Cisco DNA 中心中專用於單點傳送 IP 介面的全域集區，可用於為已啟用多點傳送的每個 VN 設定多點傳送。如果不存在全域集區，請重新造訪「Define Global IP Address Pools」程序來建立一個。

步驟 2. 從 Cisco DNA 中心儀表板，導覽至 **PROVISION > Fabric**，在 **Fabrics** 下按一下已建立的網狀架構網站（範例：RTP5_Fabric），在左側導覽窗格中，按一下網狀架構網站（範例：RTP5-C9K），按一下頂部的 **Fabric Infrastructure** 索引標籤，按一下網狀架構邊界節點，然後選擇 **Enable Rendezvous Point**。



步驟 3. 在右側的 **Associate Multicast Pools to VNs** 快顯視窗中，在關聯虛擬網路下，選擇 VN （範例：OPERATIONS），在**Select IP Pools**下，選擇為多點傳送建立的集區（範例：MULTICAST_PEER-RTP5），然後按 **Next**，選取一個 VN （範例：OPERATIONS），然後按一下 **Enable**。

步驟 4. 對其他網狀架構邊界節點重複上一步。在畫面底部，按一下 **Save**，然後按一下 **Apply**。

Cisco DNA 中心將多點傳送設定推送到網狀架構節點，並為邊界節點之間的集結點 (RP) 狀態通訊建立迴圈和多點傳送來源探索協定 (MSDP) 對等連線。

步驟 5. 如果面向融合路由器的邊界外需要進行多點傳送通訊，請在每台裝置上啟用下列指令。

Global:

```
ip multicast-routing
ip pim rp address [RP Address]
ip pim register-source Loopback0
ip pim ssm default
```

Interface or subinterface (for each virtual network):

```
ip pim sparse-mode
```

步驟 6. 在使用網狀架構設定的網站左側導覽面板中，按一下網站名稱旁邊的齒輪圖示，按一下 **Enable Native Multicast for IPv4**，在底部按一下 **Save**，在滑出視窗中，保留預設選取的 **Now**，然後按一下 **Apply**。

部署重疊的多點傳送設定，以使用底層網路多點傳送進行有效率的基礎架構通訊。

程序 4. 在芳鄰（融合）到邊界路由器上啟用 VN 的 eBGP 連線

Cisco DNA 中心的 SD-Access 應用程式可設定通往外部網路的網狀架構邊界節點 BGP 遞交。在所述的 SD-Access 版本中，您使用相容的 VRF Lite 和 BGP 對等連線資訊來手動設定邊界裝置的外部網路對等體。

步驟 1. 使用 CLI 登入邊界裝置，觀察由 Cisco DNA 中心 SD-Access應用程式建立的邊界外 IP 連線的自動設定。下列部分指令可能會有所幫助。

```
show running-config brief
show running-config | section vrf definition
show running-config | section interface Vlan
show running-config | section router bgp
```

技術提示

透過在邊界節點與融合路由器之間的直接連線部署復原的一對邊界節點，以防止邊界節點和融合路由器之間出現連線失敗。若要啟用自動流量重新導向，請在邊界節點之間為每個已設定的 VN 建立 iBGP 鄰居關係。使用交換器上的主幹連接埠設定和路由器上的子介面，支援使用 802.1 Q 標記的多邏輯連線。

步驟 2. 使用邊界組態設定指南登入連線到邊界的網狀架構外部的每個融合裝置，並按照在邊界上建立的虛擬網路所需的方式設定 VRF。VRF 會在網狀架構內的介面群組與虛擬網路環境之間區隔通訊。

```
vrf definition [VRF name]
 rd [Route Distinguisher]
 address-family ipv4
  route-target export [Route Target]
  route-target import [Route Target]
 exit-address-family
```

例如，如果在邊界上佈建下列的設定：

```
vrf definition OPERATIONS
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
```

為融合路由器設定相同的組態。

對於每個虛擬網路脈絡（包括訪客 VRF，如果已設定的話）重複此步驟，與邊界節點設定保持一致。

技術提示

在融合路由器上設定的 VRF 名稱、路由識別碼和路由目標應與邊界節點上的設定相符。

步驟 3. 對芳鄰設定每一個介面。部分裝置直接在主幹上支援 VLAN 子介面設定，而其他裝置則需要建立 VLAN 介面並將其與主幹建立關聯。為邊界的每個對等裝置上的每一個芳鄰重複相鄰介面設定。

```
interface [Peer physical interface]
 switchport mode trunk
```

```
interface [VLAN interface]
 vrf forwarding [VN/VRF name]
 ip address [Peer point-to-point IP address]
```

例如，如果在邊界上佈建下列的設定：

```
vlan 3003
vlan 3004
interface FortyGigabitEthernet1/0/24
 switchport mode trunk
interface Vlan3003
 description vrf interface to External router
 vrf forwarding OPERATIONS
 ip address 172.16.172.9 255.255.255.252
interface Vlan3004
 description vrf interface to External router
 ip address 172.16.172.13 255.255.255.252
```

為融合路由器設定相容的連線和定址。沒有關聯的 VRF 轉移陳述式的 VLAN 介面可用於與全域路由表的 INFRA_VN 通訊。

```
vlan 3003
vlan 3004
interface FortyGigabitEthernet1/0/7
 switchport mode trunk
interface Vlan3003
 description vrf interface to External router
 vrf forwarding OPERATIONS
 ip address 172.16.172.10 255.255.255.252
interface Vlan3004
 description vrf interface to External router
 ip address 172.16.172.14 255.255.255.252
```

步驟 4. 設定面向邊界的 BGP IPv4 單點傳送路由，以支援與網狀架構中每個 VN 關聯的每個 VRF 的連線。

```
router bgp [Local BGP AS]
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor [Border VLAN IP Address] remote-as [Fabric BGP AS]
 neighbor [Border VLAN IP Address] update-source [VLAN interface]
 ! repeat for any additional neighbors
address-family ipv4
  network [Loopback IP Address] mask 255.255.255.255
  neighbor [Border VLAN IP Address] activate
! repeat for any additional neighbors
  maximum-paths 2
 exit-address-family
```

```
 address-family ipv4 vrf [VN/VRF name]
  neighbor [Border VLAN IP Address] remote-as [Fabric BGP AS]
  neighbor [Border VLAN IP Address] update-source [VLAN interface]
  neighbor [Border VLAN IP Address] activate
! repeat for any additional neighbors
 exit-address-family
```

例如，如果在邊界上佈建下列的設定：

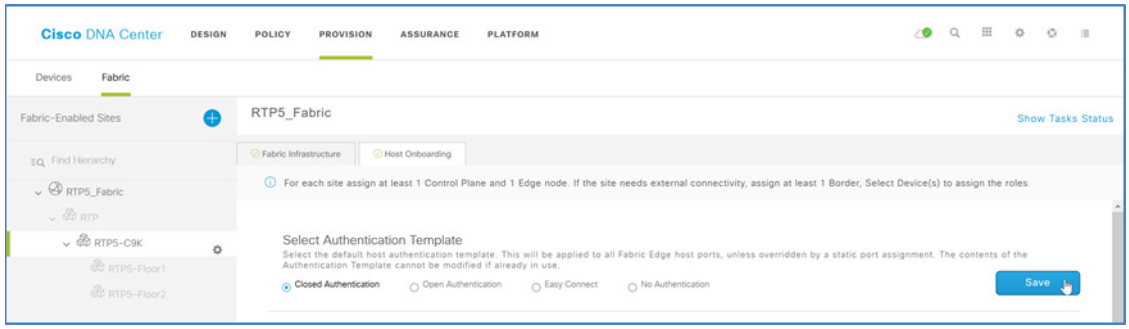
```
router bgp 65514
 bgp router-id interface Loopback0
 neighbor 172.16.172.14 remote-as 65500
 neighbor 172.16.172.14 update-source Vlan3004
 !
 address-family ipv4
  network 172.16.173.1 mask 255.255.255.255
  aggregate-address 172.16.173.0 255.255.255.0 summary-only
  neighbor 172.16.172.14 activate
exit-address-family
 !
 address-family ipv4 vrf OPERATIONS
  neighbor 172.16.172.10 remote-as 65500
  neighbor 172.16.172.10 update-source Vlan3003
  neighbor 172.16.172.10 activate
exit-address-family
```

在融合路由器上設定下列內容：

```
router bgp 65500
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor 172.16.172.13 remote-as 65514
 neighbor 172.16.172.13 update-source Vlan3004
 !
 address-family ipv4
  neighbor 172.16.172.13 activate
 exit-address-family
 !
 address-family ipv4 vrf OPERATIONS
  neighbor 172.16.172.9 remote-as 65500
  neighbor 172.16.172.9 update-source Vlan3003
  neighbor 172.16.172.9 activate
exit-address-family
```

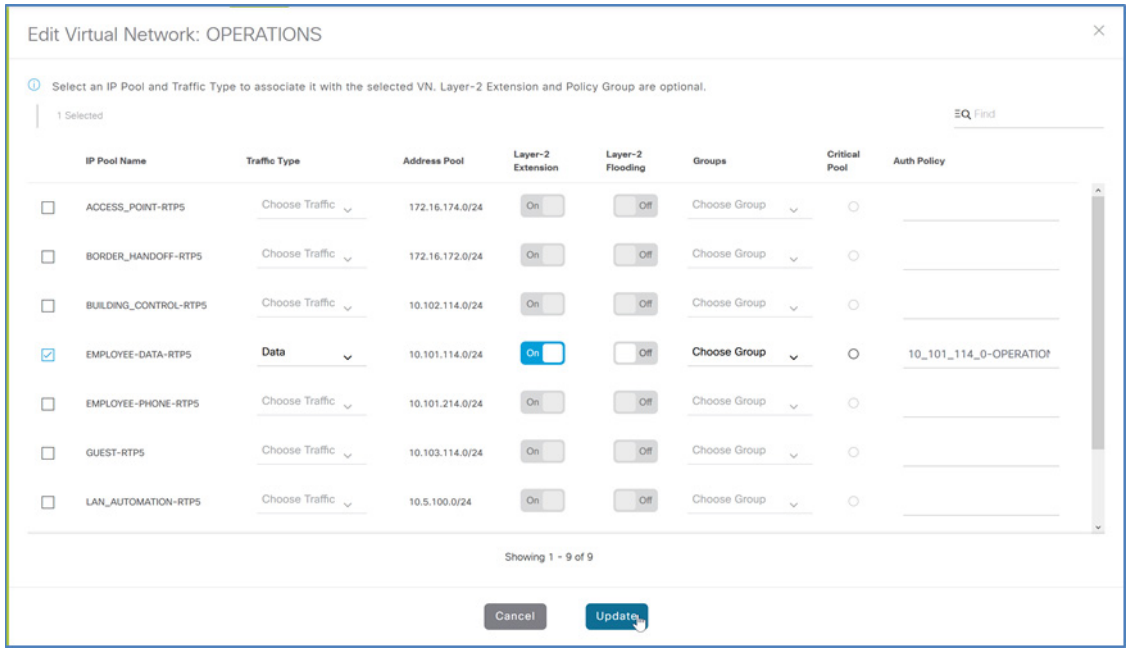
程序 5.　將有線用戶端指派到 VN 並啟用連線

步驟 1.　從 Cisco DNA 中心儀表板，導覽至 **PROVISION > Fabric**，在 **Fabrics** 下按一下已建立的網狀架構網站（範例：RTP5_Fabric），在左側導覽窗格中，按一下網狀架構網站（範例：RTP5-C9K），按一下頂部的 **Host Onboarding** 索引標籤，在 **Select Authentication template** 下選擇 **Closed Authentication**，按一下區段頂端的 **Save**，然後按一下 **Apply**。



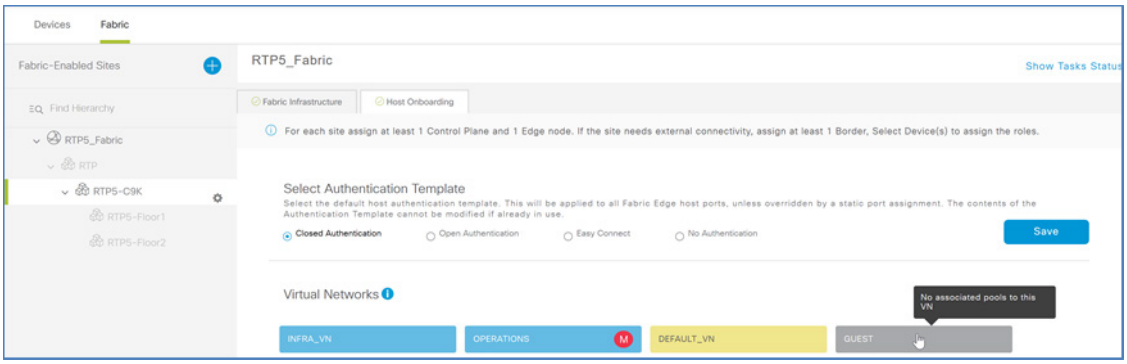
將關閉的身份驗證設定為主機連接埠的預設值，需要端點的 802.1x 身份驗證才能連線到網狀架構；此設定可由連接埠覆寫，以用於其他用途，例如用於 AP 連接埠。

步驟 2.　在 **Virtual Networks** 下，選取要用於有線用戶端的 VN （範例：OPERATIONS），在 **Edit Virtual Network:*OPERATIONS*** 滑出窗格中，選擇要新增到 VN 的 **IP 集區**的名稱（範例：EMPLOYEE-DATA-RTP5），選擇 **Data** 的 **Traffic Type**，驗證 **Layer 2 Extension** 是否為 **On**，可選擇將 **Auth Policy** 名稱變更為對網站有意義的內容，按一下 **Update**，然後按一下 **Apply**。

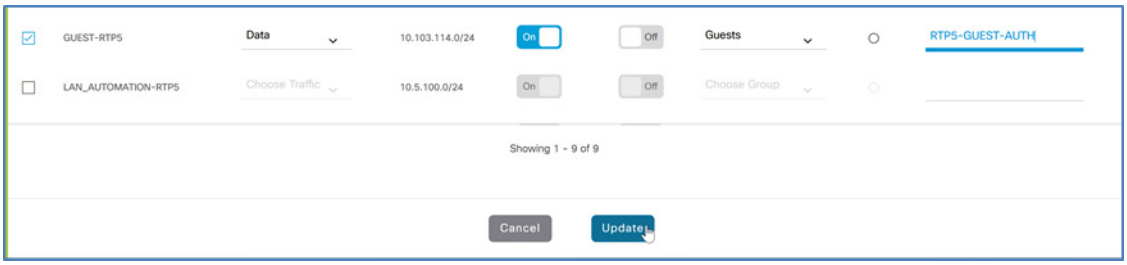


畫面上會顯示狀態訊息，然後會顯示 **Host Onboarding** 畫面。

步驟 3.　如果您已建立訪客虛擬網路，請將 IP 集區與訪客服務建立關聯。在 **Virtual Networks** 下，選擇要用於訪客無線用戶端的 VN （範例：GUEST）。



步驟 4. 在 **Edit Virtual Network:*GUEST*** 滑出窗格中，選擇要新增到 VN 的 **IP 集區**的名稱（範例：EMPLOYEE-Data-RTP5），選擇 **Data** 的 **Traffic Type**，驗證 **Layer 2 Extension** 是否為 **On**，或者可選擇將 **Auth Policy** 名稱變更為對網站有意義的名稱，按一下 **Update**，然後按一下 **Apply**。



畫面上會顯示狀態訊息，然後會顯示 **Host Onboarding** 畫面。

程序 6. 啟用用於用戶端啟動的網狀架構邊緣連接埠

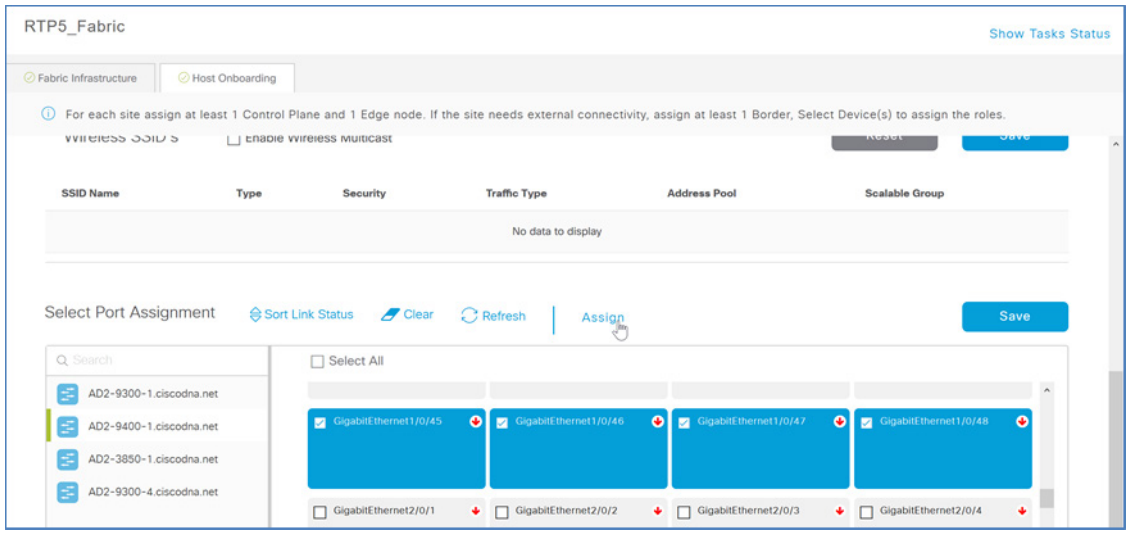
選用

當連線的裝置不支援 802.1x，或使用其他身份驗證方法（例如物聯網裝置的 MAB 身份驗證），或者當手動將位址集區指派給連接埠，請覆寫在上一個程序中指派的預設身份驗證範本（關閉的身份驗證）。

針對連線到網狀架構邊緣連接埠（要求覆寫預設身份驗證範本）的用戶端，對於每個網狀架構邊緣交換器重複此程序。

步驟 1. 導覽至 **PROVISION > Fabric**，在 **Fabrics** 下，按一下建立的網狀架構網站（範例：RTP5_Fabric），在左側導覽窗格中，按一下網狀架構網站（範例：RTP5-C9K），按一下頂端的 **Host Onboarding** 索引標籤，然後在 **Select Port Assignment** 區段下的左側欄中，選擇一個交換器。

步驟 2. 在交換器埠清單中，選擇一組要參與網狀架構 VN 的有線網狀架構邊緣連接埠，然後按一下 **Assign**。



步驟 3. 在滑出視窗中，選擇適當的**連線裝置類型**（範例：使用者裝置 (ip-phone、computer、laptop)），選擇**位址集區**（範例：10_101_114_0(EMPLOYEE-DATA-RTP5)），選擇**群組**（範例：Employees），選擇一個**語音集區**（如果需要），選擇一個**身份驗證範本**（範例：No Authentication），然後按一下 **Update**。

步驟 4. 在 **Select Port Assignment** 區段的右側，選擇 **Save**，保留預設選擇的 **Now**，然後按一下 **Apply**。

步驟 5. 對新增的每個額外的交換器重複上述步驟。

現在，裝置可以使用所建立的有線網路重疊和身份驗證方法，在網狀架構邊緣連接埠連線。

技術提示
如果網狀架構邊緣連接埠未使用身份驗證伺服器動態接收其指派，則使用群組指派來靜態設定群組，這對於組織中使用的某些類型的裝置非常實用。如果選擇「No Authentication」作為身份驗證方法，則 Cisco DNA 中心會推送在畫面頂端「Select Authentication template」區段中選擇的全域預設身份驗證範本。當您選擇「Closed Authentication」，或選擇「Open Authentication」時，Cisco DNA 中心會推送連接埠設定。

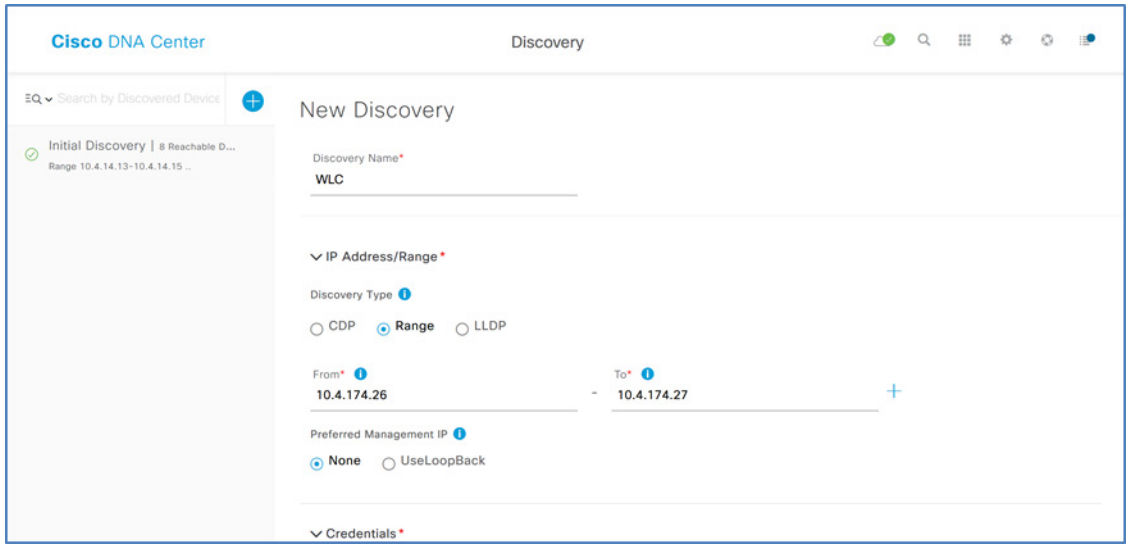
程序：將 SD-Access 無線整合到網狀架構中

安裝用於 SD-Access 的無線局域網路控制器的程序會在《分散式園區軟體定義存取規範部署指南》中介紹。此無線整合過程假定控制器可使用 Cisco DNA 中心整合到網狀架構中。

程序 1.　將無線控制器新增到庫存中，並建立 HA SSO 配對

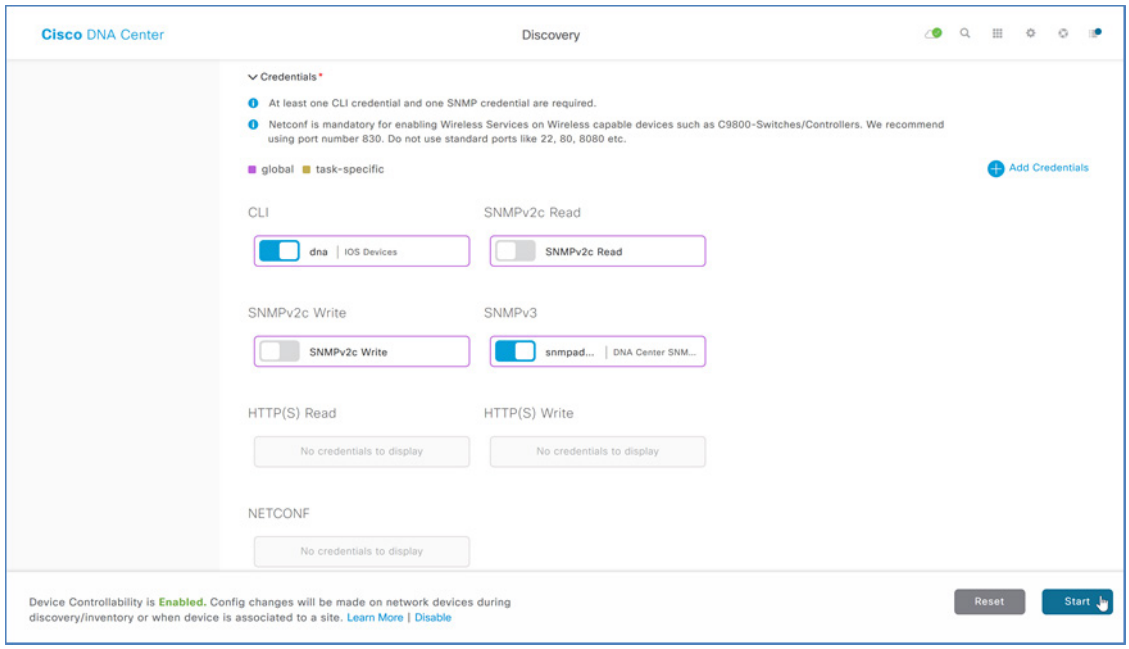
如果無線區域網路控制器不在 Cisco DNA 中心庫存中，您必須在無線整合之前新增。為提供恢復能力，您還應使用同一類型的兩個 WLC 來建立高可用性的 SSO 配對。

步驟 1.　導覽至主 Cisco DNA 中心控制台，捲動至 **Tools** 區段，按一下 **Discovery** 並提供**探索名稱**。選擇 **Range** 並在 **IP Ranges** 中輸入開始和結束 IP 迴路位址（如要涵蓋單一位址，請輸入該範圍開頭和結尾的位址）。對於 **Preferred Management IP**，請使用 **None**。

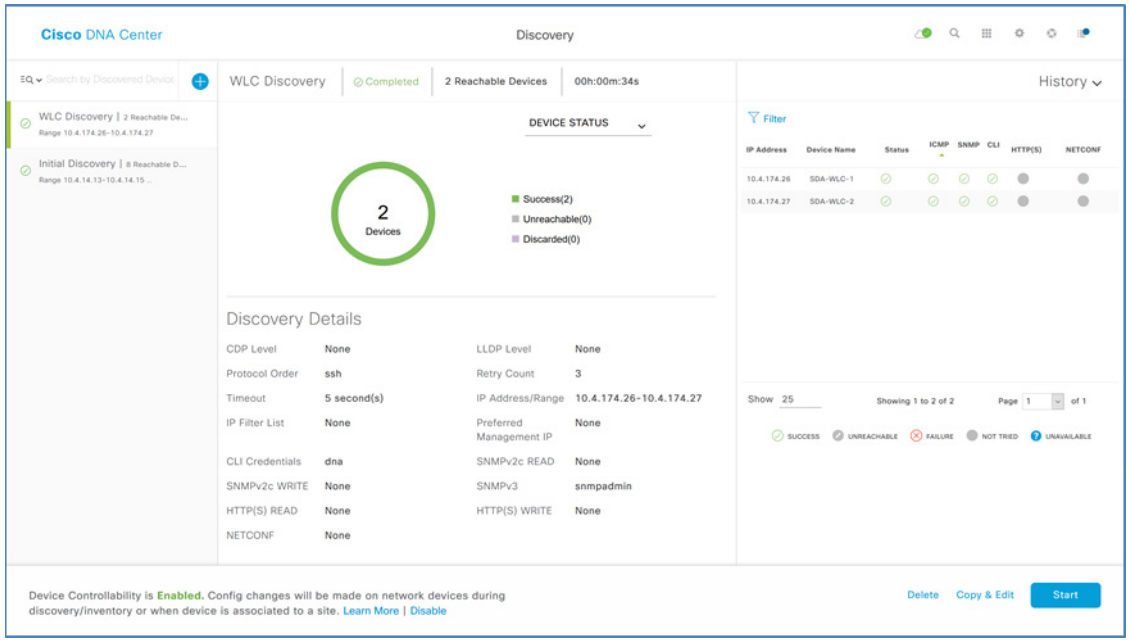


步驟 2.　如果您有任何額外的範圍，請按一下第一個範圍旁邊的 **+**（加號），輸入其他範圍，並對剩餘的範圍重複此操作。

步驟 3.　向下捲動以驗證用於探索的 CLI 憑證，以及透過 Cisco DNA 中心裝置可控性功能推送到裝置的 SNMP 憑證設定。如果您有裝置的特定探索唯一憑證，請按一下 **+ Add Credentials** 新增每個新的憑證，儲存後按一下底部的 **Start**。



在執行探索時，畫面上會顯示探索詳細資訊。



步驟 4. 如果存在任何探索失敗，請檢查裝置清單、解決問題，並重新啟動這些裝置的探索以及要新增到庫存的任何其他裝置的探索。

步驟 5. 成功完成所有探索任務後，請導覽至主要 Cisco DNA 中心儀表板，然後在 **Tools** 區段下，按一下 **Inventory**。螢幕上會顯示已探索的裝置。在庫存收集完成後，每台裝置都會顯示 **Managed** 同步狀態，表明 Cisco DNA 中心維持內部模型鏡像裝置實體部署。

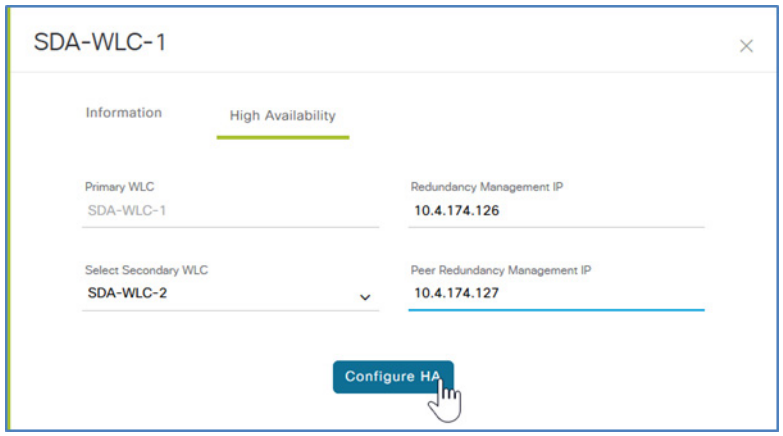
Cisco DNA 中心現在可以存取裝置，同步設定庫存 ，並在裝置上進行設定變更。

技術提示

您可以在庫存表的標題列右側，調整要顯示的列。使用 **Device Role** 欄查看藉由探索根據裝置類型所指派的裝置角色，以便將角色調整至最能反映裝置實際部署的角色（例如存取、分佈、核心或邊界路由器），其中在此顯示的邊界路由器是通用的非網狀架構裝置角色。現在調整角色就可以改善初始拓撲圖的外觀，而不必在後續程序中調整角色。針對 WLC，指派到核心角色會讓裝置更靠近這些裝置的通常位置。

在繼續之前，請使用 **Refresh** 按鈕更新 **Last Inventory Collection Status**，直至其處於 **Managed** 狀態。

步驟 6. 如果要使用目前未配對的一組控制器建立高可用性 SSO 配對，請前往主 Cisco DNA 中心儀表板，導覽至 **PROVISION > Devices > Inventory**，按一下主 WLC 的**裝置名稱**內容（範例：SDA-WLC1），在頂端快顯視窗的右側選擇 **High Availability**，在 **Select Secondary WLC** 下，選擇 HA SSO 配對中的次要 WLC（範例：SDA-WLC-2），提供**備援管理 IP** 和**對等備援管理 IP**（範例：10.4.174.126、10.4.174.127），按一下 **Configure HA**，然後在重新開機警告快顯視窗中，按一下 **OK**。



在瀏覽器中，隨即會顯示警告訊息。

```
Configuring HA for Primary. Please do not Refresh the page..
Configuring HA for Secondary...
```

重新設定和重新啟動可能需要幾分鐘時間。

步驟 7. 使用顯示畫面頂端的重新整理按鈕，以重新整理顯示畫面，直至高可用性模式下的 WLC 顯示為一台裝置。若要檢查高可用性狀態，請按一下主 WLC 的**裝置名稱**內容（範例：SDA-WLC1），在頂端的快顯視窗右側選擇 **High Availability**，並檢查 **Redundancy State** 是否為 **SSO** 且 **Sync Status** 為 **Complete**。

在 HA 設定完成後，繼續執行下一步。

步驟 8. 前往主 Cisco DNA 中心儀表板，導覽至 **DESIGN > Image Repository**。尋找裝置系列並檢查軟體版本。如果 WLC 映像檔的版本正確無誤，則請繼續。如果需要更新映像檔，並且已列出映像檔，請按一下映像檔旁邊的星號以將該映像檔標記為金色，並更新軟體。如果您需要未列出的映像檔，請按一下頂端的「Import Image/SMU」，按照說明匯入，重新整理畫面，使用該裝置的下拉功能表將映像檔標記為金色。

步驟 9. 如果要升級裝置，請導覽至 **PROVISION > Devices > Inventory**，選擇標記為 **Outdated** 的 WLC，然後在 **Actions** 選單中選擇 **Update OS Image**。確認選擇要更新的裝置，使用預設的 **When** 選項中的 **Now** 並按一下 **Apply**，然後在彈出關於重新開機裝置的警告中，按一下 **OK**。

映像檔將被發佈到所選裝置，然後在映像檔發佈完成後，裝置會重新開機以立即啟動新的映像檔。使用 **Refresh** 按鈕查看何時移除 **In Progress** 的狀態。

程序 2.　為存取點建立 IP 位址集區

驗證 Cisco DNA 中心的全域集區是否可用於對要由網路管理的 AP 進行位址指派。

步驟 1.　導覽至 **DESIGN > Network Settings > IP Address Pools**。在左側的網站層級架構中，選擇 **Global**，然後檢查專用於 AP 基礎架構的集區 IP 位址集區清單（範例：ACCESS_POINT）。

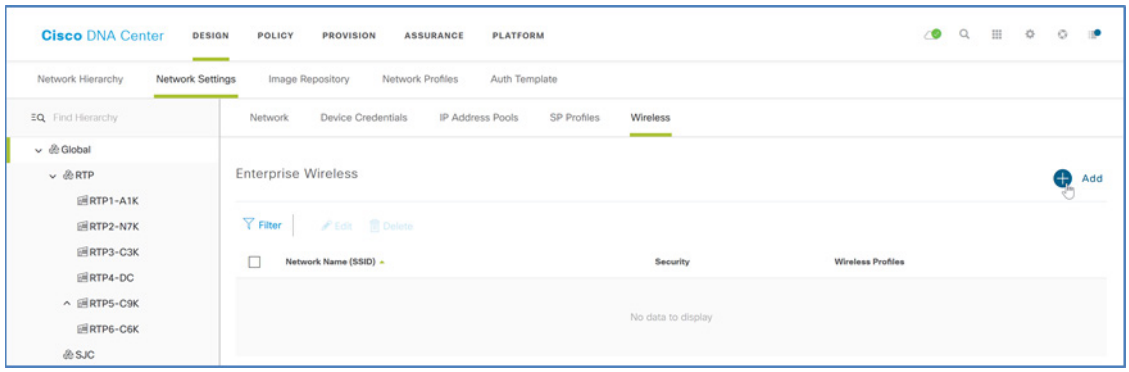
步驟 2.　如果存取點的集區不存在，請按一下 **+ Add IP Pool**，填寫 **IP 集區名稱**、**IP 子網路**、**CIDR 首碼**和**閘道 IP 位址**（範例：ACCESS_POINT、172.16.173.0、/24、172.16.173.1），選擇 **DHCP 伺服器**和 **DNS 伺服器**，然後按一下 **Save**。

步驟 3.　導覽至 **DESIGN > Network Settings > IP Address Pools**，在網站層級架構左側，為 IP 位址集區保留項目選擇一個網站或更低層級（範例：RTP5-C9K）。如果尚未保留集區，請在右上角按一下「Reserve IP Pool」。

步驟 4.　如果要保留集區，請填寫 **IP 集區名稱**（範例：ACCESS_POINT-RTP5），在 **Type** 下選取 **LAN**，選擇用於保留的 **Global IP Pool** 來源，在 **CIDR Notation / No. of IP Addresses** 下，選取要使用的位址空間部分，指派**閘道 IP 位址**、**DHCP 伺服器**和 **DNS 伺服器**，然後按一下 **Reserve**。

程序 3.　設計網狀架構企業無線 SSID

步驟 1.　在 Cisco DNA 中心儀表板中，導覽至 **DESIGN > Network Settings> Wireless**，在左側層級架構窗格中，選擇 **Global** 層級，在 **Enterprise Wireless** 區段中按一下 **+ Add**。



系統將會顯示 **Create an Enterprise Wireless Network** 精靈。

步驟 2.　使用 **Create an Enterprise Wireless Network** 精靈以提供下列資訊：

- 輸入**無線網路名稱(SSID)**（範例：Employee）
- 在 **TYPE OF ENTERPRISE NETWORK** 下，選擇語音和資料以及快速通道
- 選擇或確認 **WIRELESS OPTION**
- 對於 **LEVEL OF SECURITY**，請選擇一個選項（範例：WPA2 Enterprise）
- 在 **ADVANCED SECURITY OPTIONS** 下，選擇「Adaptive」

步驟 3.　按 **Next** 以繼續使用精靈，並提供下列資訊：

- 輸入**無線設定檔名稱**（範例：RTP5-Wireless）

- 在 **Fabric** 下，選擇 **Yes**
- 在 **Choose a site** 下，選擇 SSID 廣播的位置（範例：Global/RTP/RTP5-C9K），並包括要包含在 SSID 覆蓋範圍內的樓層（範例：Global/RTP/RTP5-C9K/ Floor 1）

步驟 4. 按一下 **Finish** 以繼續。隨即會顯示 **DESIGN > Network Settings> Wireless** 畫面。

步驟 5. 針對使用相同網路設定檔的其他 SSID，以及與 SSID 相關聯的任何新位置設定檔，重複此程序。

程序 4. 設計網狀架構訪客無線 SSID

步驟 1. 導覽至 **DESIGN > Network Settings> Wireless**，在 **Guest Wireless** 區段中，按一下 **Create a Guest Wireless Network** 精靈中的 **+ Add**，並提供以下資訊：

- 輸入**無線網路名稱(SSID)**（範例：Guest）
- 在 **LEVEL OF SECURITY** 選擇「Web Auth」
- 在 **AUTHENTICATION SERVER** 下選擇「ISE Authentication」

保留其他預設選擇，然後按 **Next** 以繼續操作精靈。

步驟 2. 在 **Wireless Profiles** 步驟中，選擇與部署位置對應的**設定檔名稱**（範例：RTP5-Wireless），在滑出面板中，保留預設 **Fabric** 選項的 **Yes**，保留其他預設資訊，在面板底部按一下 **Save**，然後按 **Next**。

步驟 3. 在 **Portal Customization** 步驟中，按一下 **+ Add**。隨即顯示 **Portal Builder** 畫面。

步驟 4. 提供**訪客入口網站**名稱（範例：GUEST-RTP5），進行所需的自訂，然後按一下畫面底部的 **Save**。系統會為網站產生訪客網頁身份驗證入口網站，並返回上一個畫面。

步驟 5. 按一下 **Finish**。

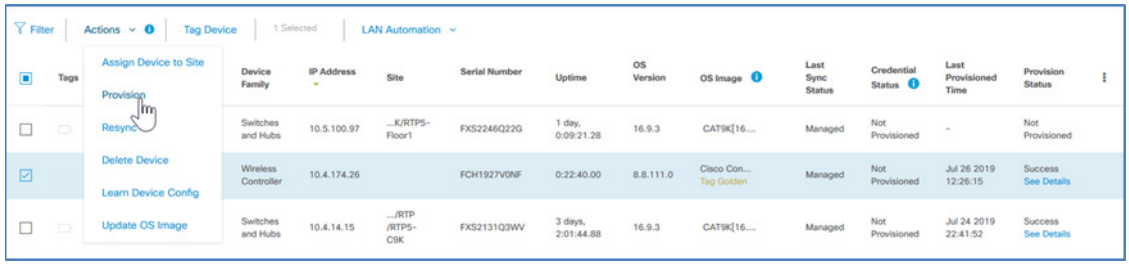
無線區域網站設計已建立並準備好部署。

程序 5. 佈建 SD-Access 無線網狀架構整合的 WLC

完成 SD-Access 無線設計後，將設定從設計應用程式推送到 WLC。

步驟 1. 導覽至「PROVISION > Devices > Inventory」，尋找 WLC 並選取旁邊的核取方塊，然後在「Actions」下拉式功能表下的畫面頂端，選擇「Provision」。系統會開啟佈建裝置精靈。

技術提示
當在 HA SSO 模式下設定一對 WLC 時，系統會在 Cisco DNA 中心庫存中顯示單一 WLC。您可以透過按一下裝置名稱，然後按一下 **High Availability** 索引標籤，來驗證是否已設定 HA SSO 配對。



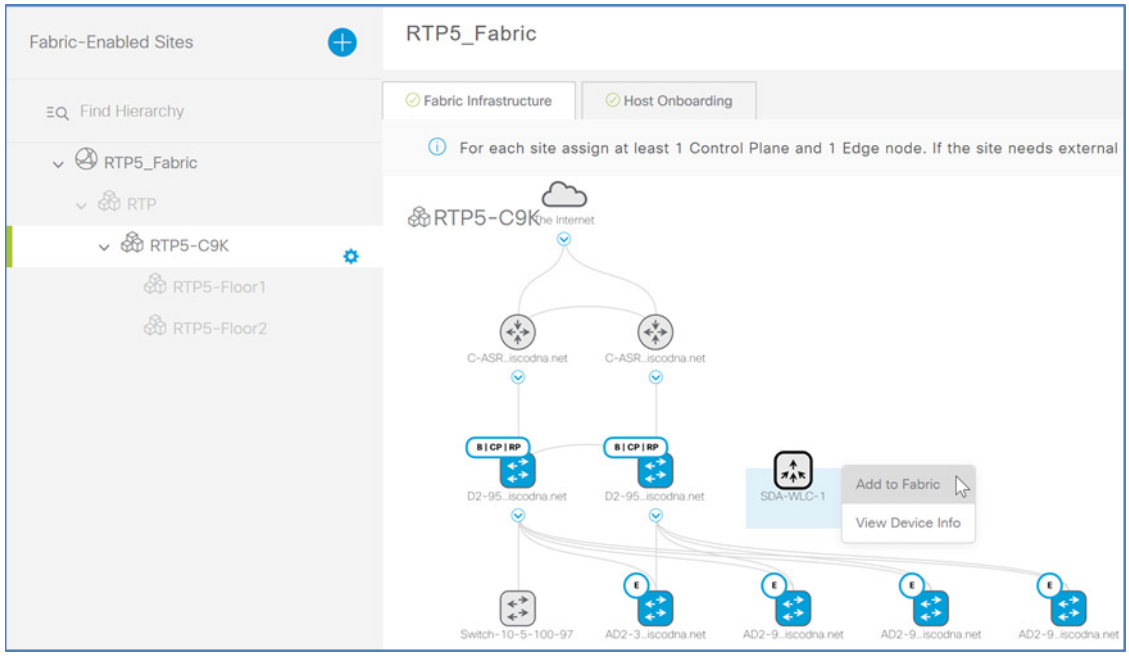
步驟 2. 指派網站（範例：Global/RTP/RTP5-C9K），按 **Next**，在 **Managed AP Location** 下的 **Configuration** 步驟中選擇由 WLC 管理的 AP 的其他樓層指派（範例：Global/RTP/RTP5-C9K/ Floor 1），按 **Next**，然後在 **Advanced Configuration** 步驟中按 **Next**。

步驟 3. 在 **Summary** 步驟中，查看設定，按一下 **Deploy**，在滑出面板中保留預設選項 **Now**，然後按一下 **Apply**。

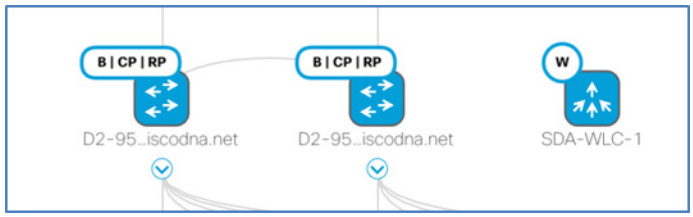
WLC 已指派到網站，並開始佈建。使用 **Refresh** 按鈕，直到 **Provision Status** 顯示 **Success**，然後再繼續。

程序 6. 將 SD-Access 無線佈建至網狀架構中

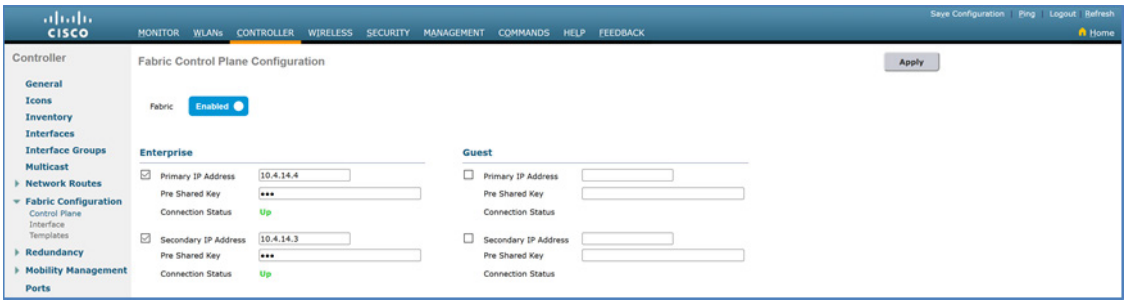
步驟 1. 從 Cisco DNA 中心控制台，導覽至 **PROVISION > Fabric**，在 **Fabric** 下，按一下建立的網狀架構網站（範例：RTP5_Fabric），按一下 **Fabric-Enabled Sites** 導覽左側的關聯網站（範例：Global/RTP/RTP5-C9K），按一下 WLC，然後在快顯方塊中按一下 **Add to Fabric**。



步驟 2. 在畫面底部，按一下 **Save**，在滑出選單中保留預設選項 **Now**，然後按一下 **Apply**。建立 WLC 設定以建立與網狀架構控制平面的安全連線。



您可以透過導覽至 **CONTROLLER > Fabric Configuration > Control Plane**，其中會顯示網狀架構整合已啟用，且連線狀態為開啟，以驗證 WLC 控制器配對已從 WLC 主控台整合到網狀架構中。



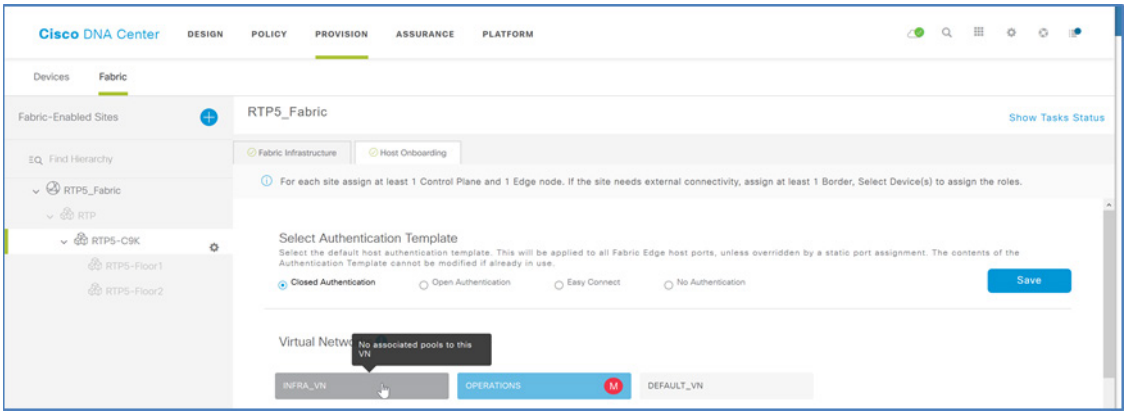
程序 7. 支援在無線網狀架構中啟動存取點

AP 是加入網狀架構並指派到名為 INFRA_VN 的 VN 的主機。此為針對基礎架構裝置（例如 AP）的特殊 VN，使用網狀架構控制平面以及位於網狀架構外部的 WLC （全域路由連線）作為全域路由連線的一部分，以實現網狀架構邊緣節點之間的無線存取點之間的管理通訊。

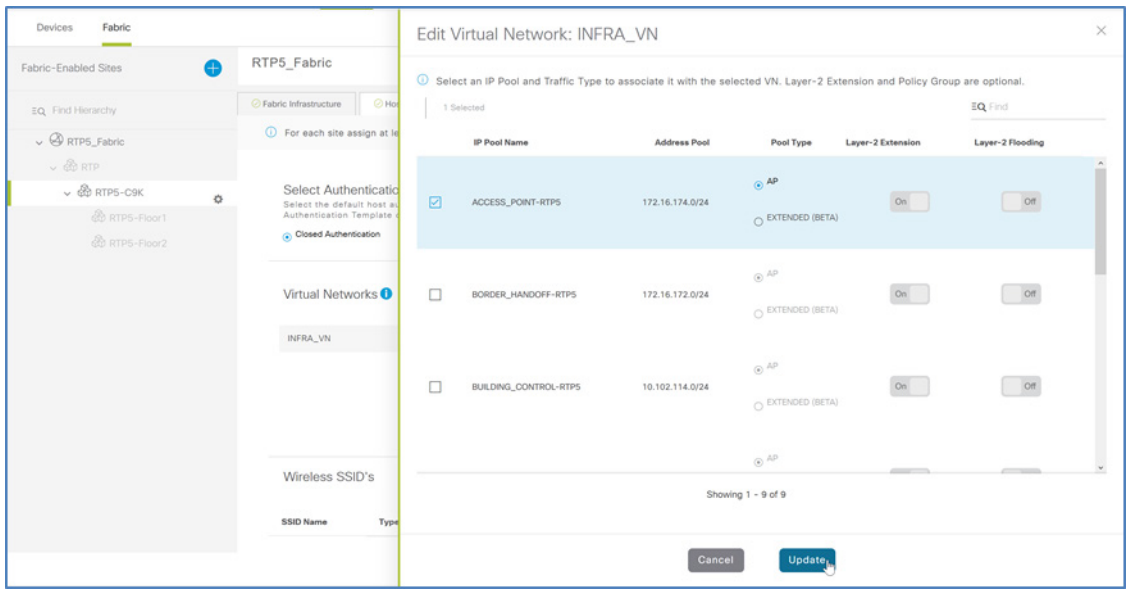
步驟 1. 將 AP 用來作為網狀架構，以連線到網狀架構中的邊緣節點。

步驟 2. 在 Cisco DNA 中心儀表板中，導覽至 **PROVISION > Fabric**，在 **Fabric Domains** 下按一下建立的網狀架構網站（範例：RTP5_Fabric），在 **Fabric-Enabled Sites** 導覽左側，按一下相關網站（範例：Global/RTP/RTP5-C9K），然後按一下 **Host Onboarding**。

步驟 3. 在 **Virtual Networks** 下，選擇 **INFRA_VN**。

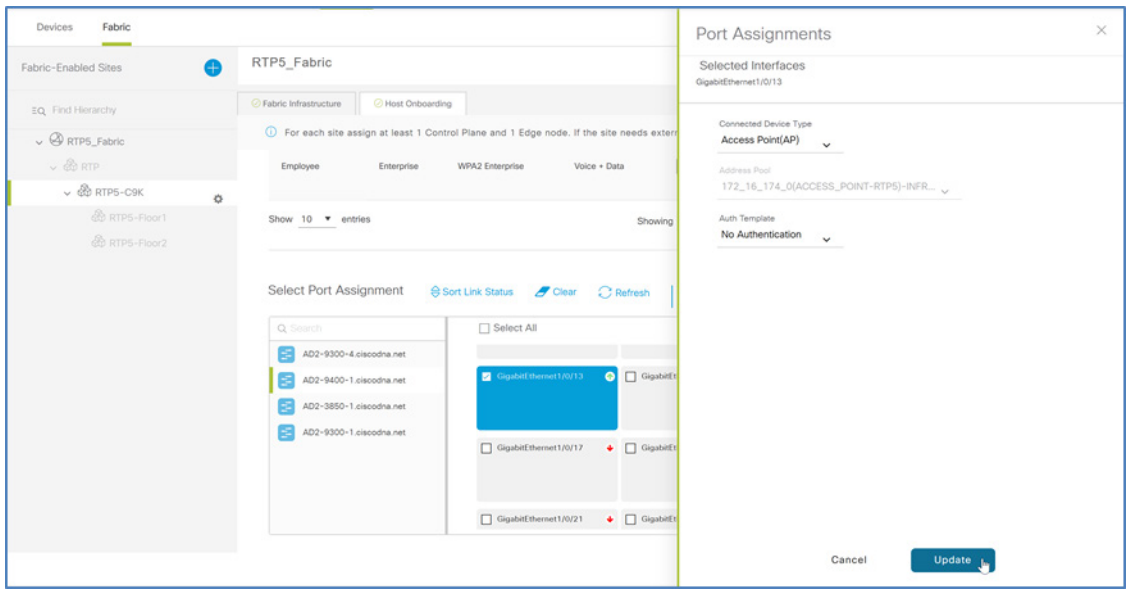


步驟 4. 為 AP 選擇 IP 集區名稱旁邊的核取方塊（範例：ACCESS_POINT-RTP5），在 **Pool Type** 下選擇 **AP**，然後按一下 **Update**。



步驟 5. 在「Modify Virtual Network」滑出面板中，保留預設選項 **Now**，然後按一下 **Apply**。

步驟 6. 在 **Select Port Assignment** 下，選擇一個交換器，選擇交換器上要用於 AP 的任何連接埠，選擇 **Assign**，在 **Port Assignments** 滑出視窗中，選取 **Connected Device Type** 下的 **Access Point (AP)**，保留預設的 **Address Pool** 選項，在 **Auth Template** 下選擇 **No Authentication**，然後按一下 **Update**。



技術提示

當身份驗證範本設定為 **No Authentication** 時，Cisco DNA 中心會透過在網狀架構邊緣交換器上佈建 CDP 巨集來實現存取點的自動啟動。或者您可以使用 Cisco DNA 中心中的交換器連接埠設定，為 AP 將連接埠指派給 IP 位址集區。

步驟 7. 針對具有用於 AP 的連接埠的任何其他交換器，重複上一個步驟。

步驟 8. 在選取所有支援 AP 的連接埠後，在 **Select Port Assignment** 區段的頂端，按一下 **Save**，保留預設選項 **Now**，然後按一下 **Apply**。

完成更新後，連線到 AP 的邊緣節點交換器連接埠將啟用裝置跟蹤設定識別 AP，並允許 AP 進行網路連線。

技術提示

存取點無法使用底層網路的預設路由來觸及 WLC。WLC IP 位址的更具體的路由（例如 /24 子網路或 /32 主機路由）必須存在於 AP 連線以建立連線的每個節點的全域路由表中。將邊界上的 WLC 路由重新發佈至底層網路 IGP 路由程序，以提高效率。或，您可以在支援 AP 的每個邊緣節點上建立靜態項目。

步驟 9. 在 **PROVISION > Devices > Inventory** 下導覽至主 Cisco DNA 中心儀表板，然後在頂端的 **Actions** 下拉式功能表中，選取 **Resync**。與 WLC 關聯的 AP 會新增到庫存中，而無需等待庫存重新整理。

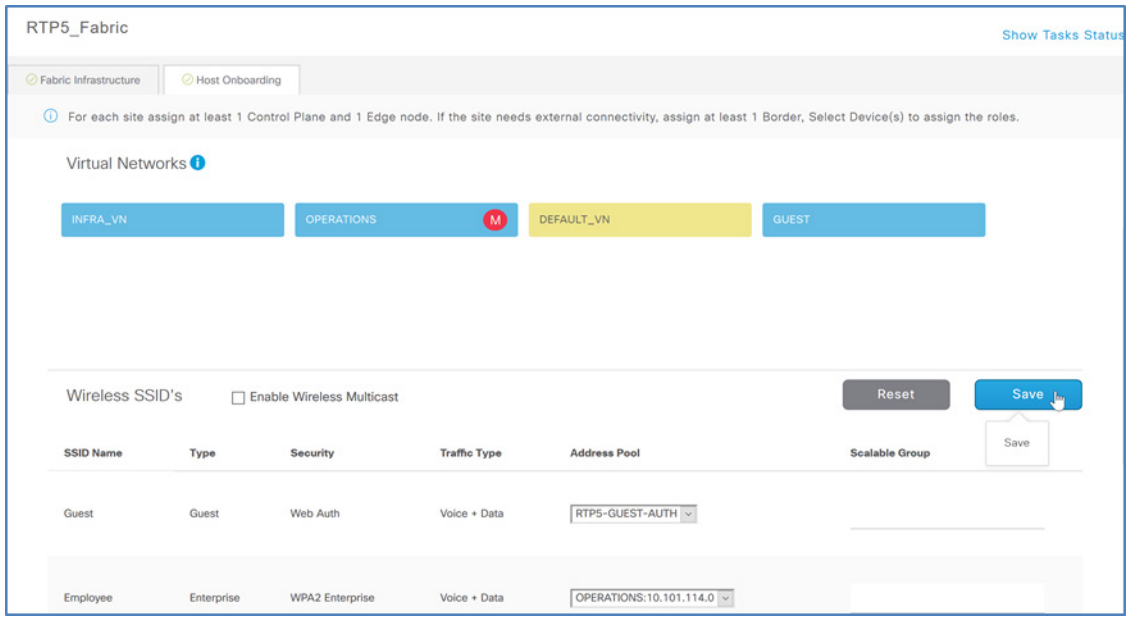
步驟 10. 導覽至主 Cisco DNA 中心儀表板，在 **PROVISION > Devices > Inventory** 下選擇要新增的 AP，然後在頂端的 **Actions** 下拉式功能表中選擇 **Provision**。

步驟 11. 在 **Provision Devices** 畫面上，將 AP 指派到特定樓層（範例：Global/RTP/RTP5-C9K/ Floor 1），按 **Next**，針對 **RF Profile**（如果您尚未建立自己的設定檔），選取 **TYPICAL**，按 **Next**，在 **Summary** 頁面中按一下 **Deploy**，然後在滑出面板中保留預設選項 **Now**，然後按一下 **Apply**。確認有關重新開機的任何警告。

程序 8. 將無線用戶端指派到 VN 並啟用連線

步驟 1. 在 Cisco DNA 中心儀表板中，導覽至 **PROVISION > Fabric**，在 **Fabric Domains** 下按一下建立的網狀架構網站（範例：RTP5_Fabric），在 **Fabric-Enabled Sites** 左側導覽，按一下相關網站（範例：Global/RTP/RTP5-C9K），然後按一下 **Host Onboarding** 索引標籤。

步驟 2. 在 **Wireless SSID** 區段下，為每個 **SSID 名稱**選擇一個關聯的**位址集區**，選擇任何關聯的**可擴充群組**，按一下 **Save**，保留預設選項 **Now**，然後按一下 **Apply**。



現在，裝置可以透過無線網路進行連線。

附錄 A：產品清單

以下產品和軟體版本包括在本部署指南中作為驗證的一部分，此驗證集並未包含所有可能性。其他硬體選項列在相關軟體定義的存取解決方案設計指南、SD-Access 產品相容性對照表中，且 Cisco DNA 中心資料表可能有除了已測試的內容之外的指引，以作為本指南的一部分。更新的 Cisco DNA 中心封裝檔會定期發佈並提供於套件與更新清單中。

表 3. Cisco DNA 中心

產品	裝置編號	軟體版本
Cisco DNA Center 設備	DN2-HW-APL-L （M5 型機箱）	1.2.10.4 （系統 1.1.0.754）

表 4. Cisco DNA 中心套件

在驗證過程中在 Cisco DNA 中心執行的所有套件均會列出，亦即並未將所有套件納入作為 SD-Access 驗證的測試的一部分。

套件	版本
套用原則	2.1.28.170011
可靠性 - 基礎	1.2.11.304
可靠性 - 感應器	1. 2.10.254
自動化 - 基礎	2.1.28.600244.9
自動化 - 智慧型擷取	2.1.28.60244
自動化 - 感應器	2.1.28.60244
Cisco DNA 中心 UI	1.2.11.19
指令執行程式	2.1. 28.60244
裝置啟動	2.1.18.60024
DNAC 平台	1.0.8.8
映像管理	2.1.28.60244
NCP - 基礎	2.1.28.60244
NCP - 服務	2.1.28.60244.9
網路控制器平台	2.1.28.60244.9
網路資料平台 - 基礎分析	1.1.11.8
網路資料平台 - 核心	1.1.11.77
網路資料平台 - 管理員	1.1.11.8

套件	版本
路徑追蹤	2.1.28.60244
軟體定義存取	2.1.28.60244.9

表 5. 身分辨識管理

功能區域	產品	軟體版本
思科 ISE 伺服器	思科身分識別服務引擎	2.4 修補程式 6

表 6. SD-Access 網狀架構邊界和控制平面

功能區域	產品	軟體版本
邊界和控制平面	Cisco Catalyst 9500 系列交換器	16.9.3
邊界和控制平面	Cisco Catalyst 9400 系列交換器	16.9.3
邊界和控制平面 - 小型網站	Cisco Catalyst 3850 XS 交換器（10 Gbps 網狀架構）	16.9.3
邊界和控制平面	Cisco 4000 系列整合服務路由器	16.9.2
邊界和控制平面 - 大規模	Cisco ASR 1000-X 和 1000-HX 系列聚合服務路由器	16.9.2
邊界	Cisco Catalyst 6807 7 插槽機箱，具有監督器引擎 6T 或監督器引擎 2T 和 6800 32 埠 10 GE，含雙整合 DFC4	15.5(1)SY2
邊界	Cisco Catalyst 6880-X 和 6840-X 交換器	15.5(1)SY2
外部邊界	Cisco Nexus 7700 交換器 2 插槽機箱，具有監督器 2 增強模組和 Cisco Nexus 7700 M3 系列 48 埠 1/10 Gigabit 乙太網路模組	8.3(2)
控制層面	Cisco 雲端服務路由器 1000V 系列	16.9.2

表 7. SD-Access 網狀架構邊緣

功能區域	產品	軟體版本
網狀架構邊緣	Cisco Catalyst 9300 系列 – 堆疊式	16.9.3
網狀架構邊緣	具監督器引擎-1 的 Cisco Catalyst 9400 系列 – 模組機箱	16.9.3

功能區域	產品	軟體版本
網狀架構邊緣	Cisco Catalyst 3850 系列 – 堆疊式	16.9.3
網狀架構邊緣	Cisco Catalyst 3650 系列 – 獨立式（可選用堆疊式）	16.9.3
網狀架構邊緣	具監督器 8-E 的 Cisco Catalyst 4500E 系列 – 模組機箱	3.10.2 E

表 8. SD-Access 無線

功能區域	產品	軟體版本
無線 LAN 控制器	Cisco 8540、5520 和 3504 系列無線控制器	8.8.111.0 (8.8 MR1)
網狀架構模式存取點	Cisco Aironet®1800、2800 和 3800 系列 (Wave 2)	8.8.111.0 (8.8 MR1)

表 9. 本指南測試的 LAN 自動化交換器（並未包括所有可能性）

功能區域	產品
Cisco Catalyst 9500 系列（標準效能版本）	種子裝置
Cisco Catalyst 3850 XS 交換器（10 Gbps 網狀架構）	種子裝置
Cisco Catalyst 9300 系列 – 堆疊式	已探索種子裝置的裝置
具監督器引擎-1 的 Cisco Catalyst 9400 系列 – 模組機箱	已探索種子裝置的裝置（10Gbps 介面）
Cisco Catalyst 3850 系列 – 堆疊式	已探索裝置
Cisco Catalyst 3650 系列 – 獨立式（可選用堆疊式）	已探索裝置
具監督器 8-E 的 Cisco Catalyst 4500E 系列 – 模組機箱	已探索裝置

意見回饋

如需有關本指南和相關指南的評論和建議，請加入 https://cs.co/en-cvds Cisco 社群上的討論。

美洲總部
Cisco Systems, Inc.
聖荷西加州

亞太總部
Cisco Systems (USA) Pte. Ltd.
新加坡

歐洲總部
Cisco Systems International BV Amsterdam,
荷蘭

思科在全球各地擁有超過 200 間分公司。 各分公司地址、電話及傳真號碼皆列於 Cisco 網站上，網址為 **www.cisco.com/go/offices**。