

在FindIT網路探測上配置裝置憑證

簡介

Cisco FindIT Network Management提供的工具可幫助您使用Web瀏覽器輕鬆監控、管理和配置Cisco 100至500系列網路裝置，例如交換機、路由器和無線接入點(WAP)。它還通知您有關裝置和思科支援通知，例如新韌體的可用性、裝置狀態、網路設定更新，以及任何不再在保修範圍內或受支援合約覆蓋的已連線思科裝置。

FindIT Network Management是一個分散式應用程式，由兩個獨立的元件或介面組成：一個或多個稱為FindIT網路探測的探測和一個稱為FindIT網路管理器的管理器。

安裝在網路中每個站點的FindIT Network Probe例項執行網路發現，並與每個思科裝置直接通訊。在單個站點網路中，您可以選擇運行FindIT網路探測的獨立例項。但是，如果您的網路由多個站點組成，您可以在方便的位置安裝FindIT Network Manager，並將每個探測與Manager相關聯。從Manager介面，您可以獲得網路中所有站點的狀態的高級檢視，並要在檢視特定站點的詳細資訊時連線到安裝在特定站點的探測器。

為使FindIT網路能夠完全發現和管理網路，FindIT網路探測必須具有憑證才能向網路裝置進行身份驗證。首次發現裝置時，探測功能將嘗試使用預設使用者名稱和密碼以及簡單網路管理協定 (SNMP社群) 對裝置進行身份驗證。如果裝置憑證已從預設更改，則需要向FindIT提供正確的憑證。如果此嘗試失敗，將生成通知消息並且使用者必須提供有效的憑據。

目標

本文檔旨在向您展示如何在Cisco Network Probe上配置裝置憑證。

適用裝置

- FindIT探測

軟體版本

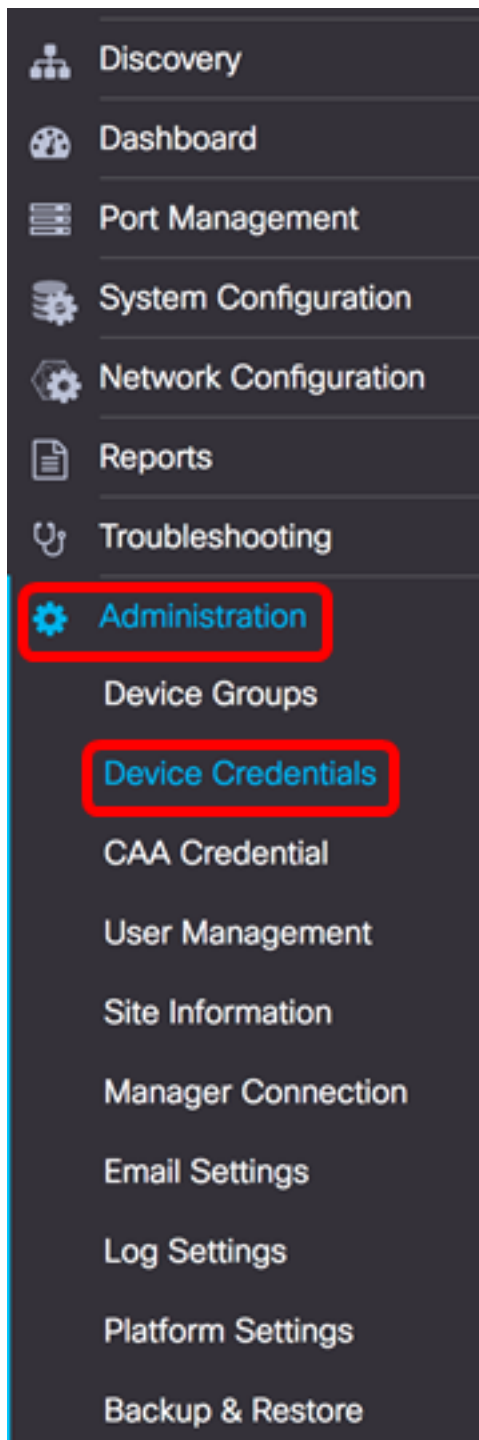
- 1.1

配置裝置憑證

新增新憑據

在下面的欄位中輸入一組或多組憑據。應用時，將對沒有工作憑據的相應型別的任何裝置進行測試。一組憑證可以是使用者名稱/密碼組合、SNMPv2社群或SNMPv3憑證。

步驟1. 登入到FindIT Network Probe Administrator GUI，然後選擇**Administration > Device Credentials**。



步驟2.在Add New Credentials區域，在*Username*欄位中輸入要應用於網路中裝置的使用者名稱。預設使用者名稱和密碼為cisco。

附註：在本範例中使用的是cisco。

A screenshot of a configuration interface. At the top, there are two input fields. The first field contains the text 'cisco' and is highlighted with a red rectangular border. The second field contains a series of dots representing a password. To the right of the second field is a plus sign icon in a square box. Below these fields is an 'Apply' button.

步驟3.在密碼欄位中，輸入密碼。

A screenshot of a configuration interface. At the top, there are two input fields. The first field contains the text 'cisco'. The second field contains a series of dots representing a password and is highlighted with a red rectangular border. To the right of the second field is a plus sign icon in a square box. Below these fields is an 'Apply' button.

步驟4.在SNMP Community欄位中，輸入Community Name。它是用於驗證SNMP Get命令的只讀社群字串。團體名稱用於從SNMP裝置檢索資訊。預設SNMP社群名稱為Public。

附註：在此示例中，使用Public。

A screenshot of a configuration interface. At the top, there is a large input field containing the text 'Public', which is highlighted with a red rectangular border. To the right of this field is a plus sign icon in a square box. Below this field is another input field containing the text 'SNMPv3 User Name', also with a plus sign icon to its right. Below these are two rows of configuration options. The first row has a dropdown menu with 'SHA' selected and a text field containing 'Authentication Pass Phr' with a green checkmark. The second row has a dropdown menu with 'None' selected and a text field containing 'Encryption Pass Phrase'.

步驟5.在SNMPv3 User Name 欄位中，輸入要在SNMPv3中使用的使用者名稱

附註：在此示例中，使用Public。

Public

Public

None

Authentication Pass Phrase

None

Encryption Pass Phrase

步驟6.從Authentication下拉選單中，選擇SNMPv3將使用的身份驗證型別。選項包括：

- 無 — 不使用使用者身份驗證。這是預設設定。如果選擇此選項，請跳至[步驟11](#)。
- MD5 — 使用128位加密方法。MD5演算法使用公共密碼系統加密資料。如果選擇此選項，則需要輸入身份驗證口令。
- SHA — 安全雜湊演算法(SHA)是一種產生160位摘要的單向雜湊演算法。SHA的計算速度比MD5慢，但比MD5更安全。如果選擇此選項，則需要輸入身份驗證密碼短語並選擇加密協定。

附註：在此範例中，使用SHA。

Public

Public

SHA

Authentication Pass Phrase

None

MD5

SHA

Encryption Pass Phrase

步驟7.在Authentication Pass Phrase欄位中輸入要由SNMPv3使用的密碼。

Public

Public

SHA

.....

None

Encryption Pass Phrase

步驟8.從Encryption Type下拉選單中，選擇加密SNMPv3請求的加密方法。選項包括：

- 無 — 不需要加密方法。
- DES — 資料加密標準(DES)是使用64位共用金鑰的對稱分組密碼。
- AES128 — 使用128位金鑰的高級加密標準。

附註：在此範例中，選擇AES。

Public

Public

SHA

.....

AES

None


DES

AES

Encryption Pass Phrase

步驟9.在Encryption Pass Phrase欄位中，輸入SNMP用於加密的128位金鑰。

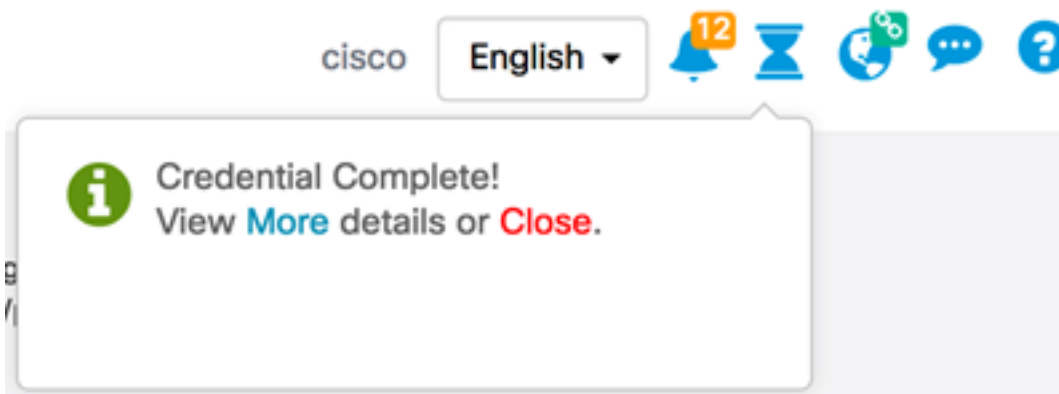
The screenshot shows a configuration interface with two 'Public' entries at the top, each with a '+' button to its right. Below these are two credential entries. The first entry is for 'SHA' with a dropdown arrow and a text field containing '.....' followed by a green checkmark. The second entry is for 'AES' with a dropdown arrow and a text field containing '.....' followed by a green checkmark. The 'AES' entry and its text field are highlighted with a red rectangular border.

步驟10。(可選) 按一下  按鈕為使用者名稱和標題建立新條目。根據憑據型別，最多可以新增一個或兩個附加條目。

步驟11. 按一下「Apply」。

This screenshot shows the same configuration interface as above, but with the 'Apply' button at the bottom left highlighted with a red rectangular border. The 'SHA' and 'AES' entries are still visible on the right side of the interface.

小時玻璃圖示下方將出現一個視窗，通知您已應用必要的配置。



現在，您應該已經在FindIT網路探測上成功配置裝置憑證。

檢視網路上的裝置

下表顯示Cisco FindIT網路探測發現的裝置。

Device	Credential Type	Credential Ok?	Failure Reason
WAP			
wap5e0940	Admin Userid/Password	✓	
wap5e0940	SNMP	✗	SNMP disabled
wampipti	Admin Userid/Password	✓	
wampipti	SNMP	✗	Invalid credential
WAP150	SNMP	✗	Invalid credential
WAP361	Admin Userid/Password	✗	Invalid credential

- 裝置 — 在網路上發現的裝置的名稱。裝置名稱可能顯示多次，具體取決於可服務的憑據型別。
- 憑據型別 — 這可以是管理員使用者ID/密碼或SNMP。用於從裝置提取資訊。
- 憑據是否正常？ — 可能會出現一個複選或紅色X以決定在以上欄位中輸入的憑證是否應用於正確的裝置。按一下裝置清單上的紅色X將顯示裝置憑據的配置。
- 失敗原因 — 如果裝置無法與探測功能通訊，則失敗原因將顯示在列中。可能的消息包括「Invalid credential」或「SNMP disabled」。

附註：建議在裝置上啟用SNMP以獲得更準確的網路拓撲。

現在，您應該已經成功檢視了網路中裝置的身份及其相應的憑證型別。