

在思科業務控制面板上配置裝置憑證

簡介

Cisco Business Dashboard提供工具，幫助您使用Web瀏覽器輕鬆監控、管理和配置交換機、路由器和無線接入點(WAP)等思科業務裝置。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。

Cisco Business Dashboard 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：一個或多個探測器（稱為Cisco Business Dashboard Probe）和單個控制面板（稱為Cisco Business Dashboard）。

安裝在網路中每個站點的Cisco Business Dashboard 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Cisco Business Dashboard Probe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Cisco Business Dashboard，並將每個探測功能與控制面板相關聯。從Manager介面，您可以獲得網路中所有站點的狀態的高級檢視，並在要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。

為了使Cisco Business Dashboard Network能夠完全發現和管理網路，Cisco Business Dashboard Probe必須具有憑證才能通過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的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，則您需要向Cisco Business Dashboard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 Probe上配置裝置憑證。

適用裝置 | 軟體版本

- 思科業務控制面板 | 2.2

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Cisco Business Dashboard GUI，然後選擇**Administration** > Device Credentials。

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log

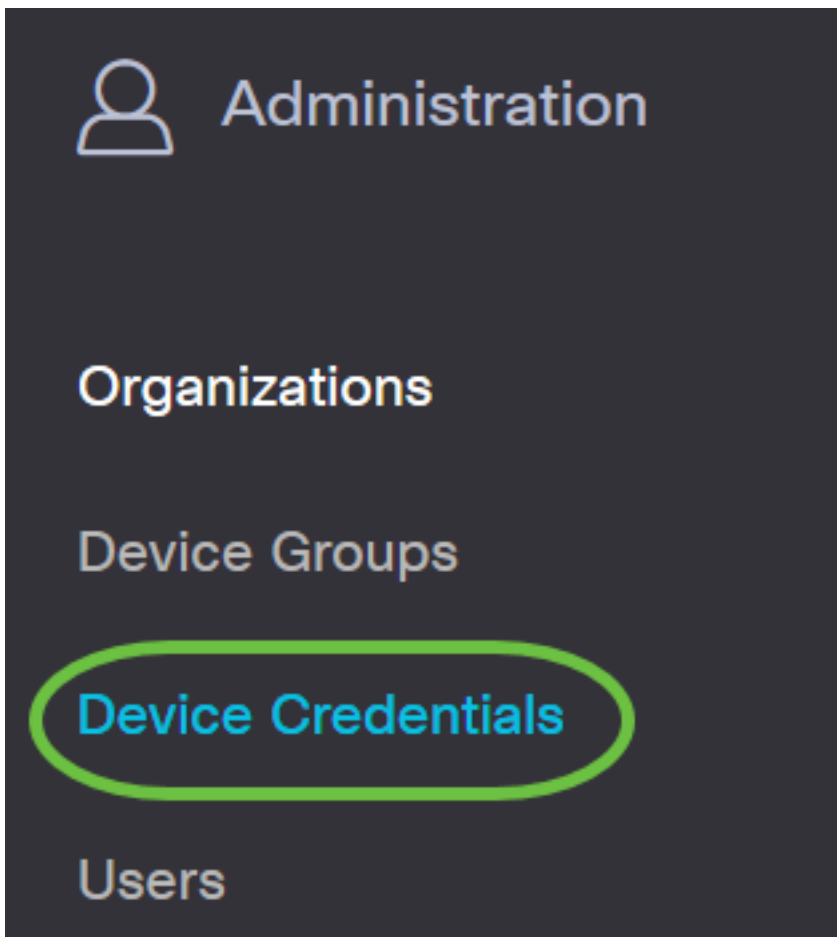


Reports



Administration





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。

Add New Credentials

Enter one or more sets of credentials in the fields below. When applied, each credential will be tested against any devices of of credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

cisco	●●●●●●●●	🗑️ +
cisco		🗑️

步驟3.在密碼欄位中，輸入密碼。

Add New Credentials

Enter one or more sets of credentials in the fields below. When applied, each credential will be tested against any devices of of credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

cisco	●●●●●●●●	🗑️ +
cisco		🗑️

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。

The screenshot shows a configuration form for SNMPv3. At the top, there is a text input field containing 'cisco' and a password field with masked characters. Below these are two rows of community string entries. The first row contains 'public' with a green checkmark and a trash icon. The second row also contains 'public' with a green checkmark and a trash icon. This second row is highlighted with a green oval. Below the community strings are two authentication method dropdown menus. The first is set to 'SHA' and the second is set to 'AES'. Both have corresponding masked password fields.

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。

This screenshot is identical to the one above, showing the same SNMPv3 configuration form. In this version, the 'public' entry in the second row of the community string list is highlighted with a green oval, indicating it is the selected user name.

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	●●●●●●●●●●●●●●	●●●●●●●●●●●●●●	🗑️

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

public	✓	🗑️
public	✓	🗑️
SHA	●●●●●●●●●●●●●●	🗑️
AES	●●●●●●●●●●●●●●	🗑️

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

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


public ✓



public ✓



SHA

AES

步驟10. (可選) 按一下該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。



 



 



SHA

AES

步驟11. 按一下「Apply」。


 

SHA







AES



現在，您應該已經在Cisco Business Dashboard Probe上成功配置裝置憑證。

檢視網路上的裝置

下表顯示了思科業務控制面板探測功能發現的裝置。

Device	Type	Organization	Network	Credential	Status	Last Used	Last Used Successfully	Action
SG300-10PP	Switch	Branch Offices	Branch 1	SNMPv2/*****	N/A	Aug 5 2020 10:47:33	Aug 5 2020 10:47:33	 
SG300-10PP	Switch	Branch Offices	Branch 1	cisco/*****	N/A	Aug 4 2020 13:42:48	Aug 4 2020 13:42:48	 
switch0294f9	Switch	Branch Offices	Branch 1	SNMPv2/*****	N/A	Aug 5 2020 10:47:30	Aug 4 2020 13:12:12	 

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。