

在FindIT网络探测功能上配置设备凭证

简介

Cisco FindIT网络管理提供的工具可帮助您使用Web浏览器轻松监控、管理和配置Cisco 100至500系列网络设备，如交换机、路由器和无线接入点(WAP)。它还会通知您有关设备和思科支持的通知，如新固件的可用性、设备状态、网络设置更新以及不再在保修期内或支持合同覆盖的任何已连接思科设备。

FindIT网络管理是一个分布式应用，由两个独立的组件或接口组成：一个或多个探测功能（称为FindIT Network Probe）和一个称为FindIT Network Manager的管理器。

安装在网络中每个站点的FindIT网络探测实例执行网络发现，并直接与每台思科设备通信。在单站点网络中，您可以选择运行FindIT网络探测功能的独立实例。但是，如果网络由多个站点组成，您可以在方便的位置安装FindIT Network Manager，并将每个探测功能与Manager相关联。从Manager界面，您可以获得网络中所有站点状态的概要视图，并在您希望查看该站点的详细信息时连接到安装在特定站点的探测功能。

要使FindIT网络能够完全发现和管理网络，FindIT网络探测功能必须具有凭证才能向网络设备进行身份验证。首次发现设备时，探测功能将尝试使用默认用户名和密码和简单网络管理协议（SNMP社区）与设备进行身份验证。如果设备凭证已从默认值更改，则需要为FindIT提供正确的凭证。如果此尝试失败，将生成通知消息，并且用户必须提供有效的凭证。

目标

本文档旨在向您展示如何在思科网络探测功能上配置设备凭证。

适用设备

- FindIT探测

软件版本

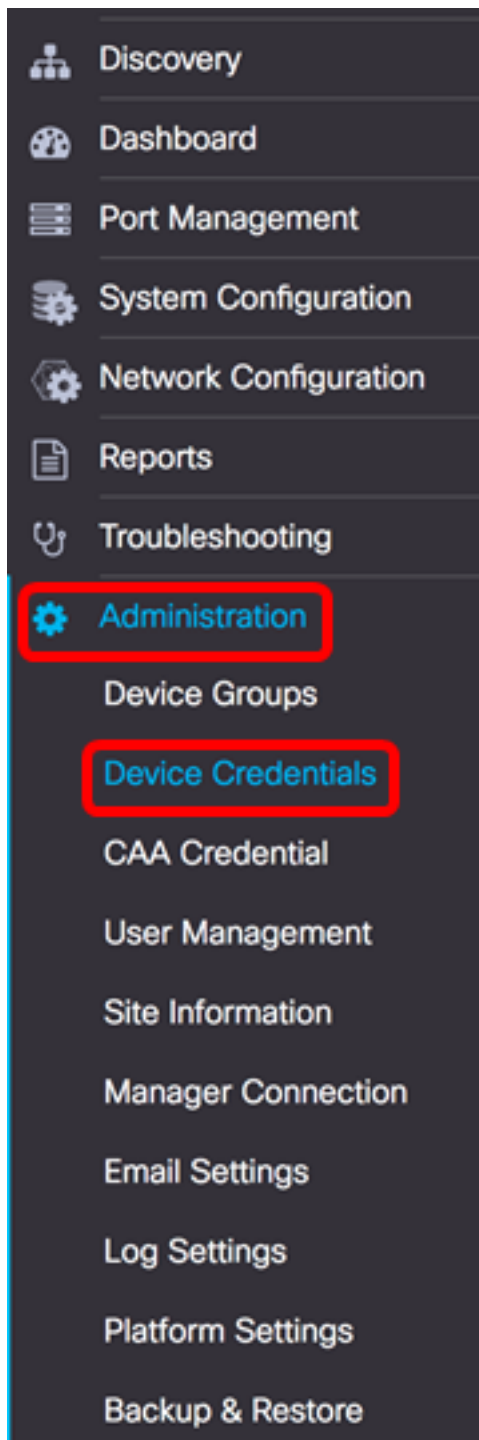
- 1.1

配置设备凭证

添加新凭据

在以下字段中输入一组或多组凭据。应用时，将针对工作凭证不可用的任何类型的设备测试每个凭证。一组凭证可以是用户名/密码组合、SNMPv2社区或SNMPv3凭证。

步骤1. 登录FindIT Network Probe Administrator GUI并选择Administration > Device Credentials(管理)。



步骤2.在Add New Credentials区域中，在Username字段中输入要应用于网络中设备的用户名。默认用户名和密码为cisco。

注意：在本例中，使用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. Below these fields is an 'Apply' button.

步骤3.在password字段中，输入密码。

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. Below these fields is an 'Apply' button.

步骤4.在SNMP Community字段中，输入Community Name。它是用于验证SNMP Get命令的只读社区字符串。社区名称用于从SNMP设备检索信息。默认SNMP社区名称为Public。

注意：在本例中，使用Public。

A screenshot of a configuration interface. At the top, there is a text input field containing the word 'Public', which is highlighted with a red rectangular border. To the right of this field is a plus sign icon in a square. Below this field is another text input field containing the text 'SNMPv3 User Name', also with a plus sign icon to its right. Below these are two rows of 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'.

步骤5.在SNMPv3 User Name字段中，输入要在SNMPv3中使用的用户名

注意：在本例中，使用Public。

Public

Public

None

Authentication Pass Phrase

None

Encryption Pass Phrase

步骤6.从Authentication下拉菜单中，选择SNMPv3将使用的身份验证类型。选项有：

- 无 — 不使用用户身份验证。这是默认设置。如果选择此选项，请跳至[步骤11](#)。
- MD5 — 使用128位加密方法。MD5算法使用公共密码系统加密数据。如果选择此选项，则需要输入身份验证密码短语。
- SHA — 安全散列算法(SHA)是一种单向散列算法，可生成160位摘要。SHA计算速度比MD5慢，但比MD5更安全。如果选择此选项，则需要输入身份验证密码短语并选择加密协议。

注意：在本例中，使用SHA。

Public

Public

SHA

Authentication Pass Phrase

None

MD5

SHA

Encryption Pass Phrase

步骤7.在Authentication Pass Phrase字段中，输入SNMPv3要使用的密码。

Public

Public

SHA

.....

None

Encryption Pass Phrase

步骤8.从Encryption Type下拉菜单中，选择加密方法来加密SNMPv3请求。选项有：

- 无 — 不需要加密方法。
- DES — 数据加密标准(DES)是使用64位共享密钥的对称分组密码。
- AES128 — 使用128位密钥的高级加密标准。

注意：在本例中，选择AES。

Public

Public

SHA

.....

AES

None


DES

AES

Encryption Pass Phrase

步骤9.在Encryption Pass Phrase字段中，输入SNMP用于加密的128位密钥。

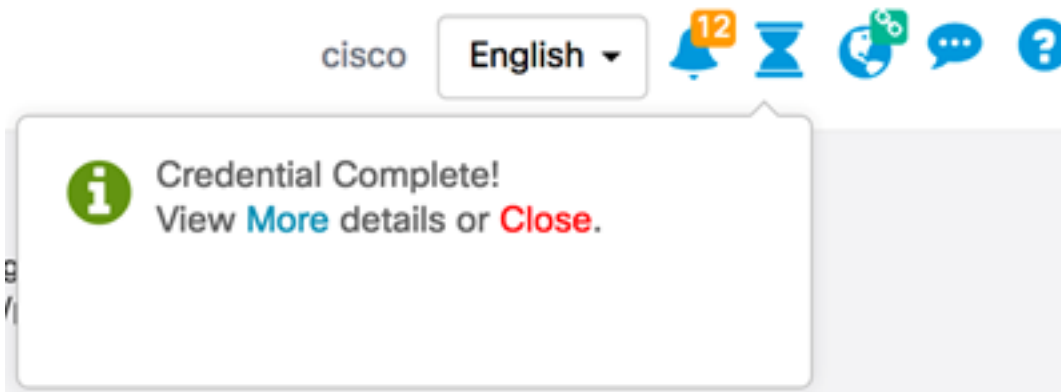
The screenshot shows a configuration panel with two 'Public' entries at the top, each with a '+' icon to its right. Below these are two rows for authentication methods. The first row has a 'SHA' dropdown and a masked password field with a green checkmark. The second row has an 'AES' dropdown and a masked password field with a green checkmark. The second row is highlighted with a red border.

步骤10. (可选) 单击按钮  为用户名和标题创建新条目。根据凭证类型，最多可添加一个或两个条目。

[步骤11.](#)单击“应用”。

This screenshot shows the same configuration interface as above, but with the 'Apply' button at the bottom left highlighted with a red border. The 'SHA' and 'AES' rows are still visible with their respective dropdowns and masked passwords.

此时，“小时玻璃”图标下方将显示一个窗口，通知您已应用必要的配置。



现在，您应该已成功配置FindIT网络探测功能上的设备凭证。

查看网络中的设备

下表显示了Cisco FindIT网络探测功能发现的设备。

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

- 设备 — 在网络上发现的设备的名称。设备名称可能会多次显示，具体取决于可服务的凭证类型。
- 凭证类型(Credential Type) — 这可以是管理员用户ID/密码(Admin Userid/Password)或SNMP。这用于从设备提取信息。
- 凭证是否正常？ — 勾选或红色X可能用于确定在上述字段中输入的凭证是否应用于正确的设备。点击设备列表上的红色X将显示设备凭证的配置。
- Failure Reason — 如果设备无法与探测通信，则故障原因出现在列中。可能的消息包括“凭证无效”或“SNMP已禁用”。

注意：建议在设备上启用SNMP，以使网络拓扑更准确。

现在，您应该已成功查看网络上设备的身份及其相应的凭证类型。