

FindITネットワークプローブでのデバイス資格情報の設定

概要

Cisco FindITネットワーク管理は、Webブラウザを使用して、Cisco 100 ~ 500シリーズのネットワークデバイス(スイッチ、ルータ、ワイヤレスアクセスポイント(WAP)など)を簡単に監視、管理、設定できるツールを提供します。また、新しいファームウェア、デバイスステータス、ネットワーク設定の更新、および接続されたシスコデバイスに関する情報が提供され、保証もなくなったり、サポート契約の対象とされたりすることも通知されます。

FindITネットワーク管理は、2つの個別のコンポーネントまたはインターフェイスで構成される分散アプリケーションです。FindITネットワークプローブと呼ばれる1つ以上のプローブと、FindITネットワークマネージャと呼ばれる1つのマネージャです。

ネットワーク内の各サイトにインストールされたFindITネットワークプローブのインスタンスは、ネットワーク検出を実行し、各シスコデバイスと直接通信します。単一サイトネットワークでは、FindITネットワークプローブのスタンドアロンインスタンスを実行することを選択できます。ただし、ネットワークが複数のサイトで構成されている場合は、便利な場所にFindIT Network Managerをインストールし、各プローブをマネージャに関連付けることができます。マネージャインターフェイスから、ネットワーク内のすべてのサイトのステータスの概要ビューを取得し、特定のサイトにインストールされているプローブに接続して、そのサイトの詳細情報を表示できます。

FindITネットワークがネットワークを完全に検出して管理するには、FindITネットワークプローブに、ネットワークデバイスで認証するためのクレデンシャルが必要です。デバイスが最初に検出されると、プローブはデフォルトのユーザ名とパスワード、およびSimple Network Management Protocol(SNMP)コミュニティを使用してデバイスの認証を試みます。デバイスのクレデンシャルがデフォルトから変更されている場合は、FindITに正しいクレデンシャルを入力する必要があります。この試行が失敗すると、通知メッセージが生成され、有効なクレデンシャルがユーザから提供される必要があります。

目的

このドキュメントの目的は、Cisco Network Probeでデバイスのクレデンシャルを設定する方法を示すことです。

該当するデバイス

- FindITプローブ

[Software Version]

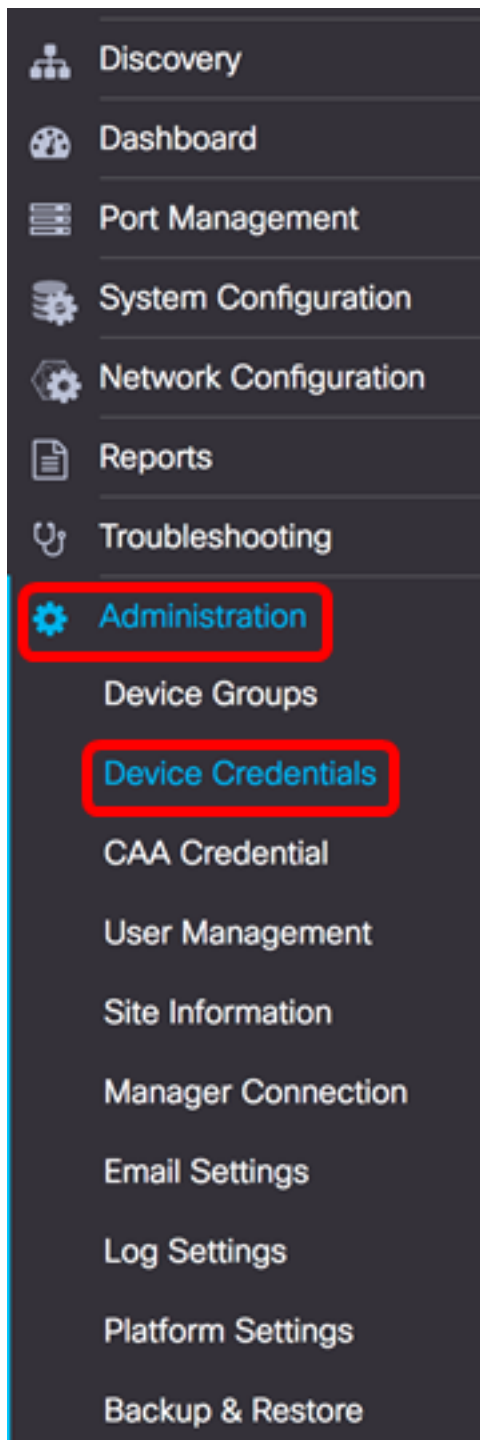
- 1.1

デバイス資格情報の設定

新しい資格情報の追加

次のフィールドに1つ以上の資格情報セットを入力します。適用されると、各クレデンシャルは、作業クレデンシャルが使用できない適切なタイプのデバイスに対してテストされます。クレデンシャルのセットは、ユーザ名/パスワードの組み合わせ、SNMPv2コミュニティ、またはSNMPv3クレデンシャルのいずれかです。

ステップ1:FindITネットワークプロープの管理者GUIにログインし、[Administration] > [Device Credentials]を選択します。



ステップ2:[Add New Credentials (新しい資格情報の追加)]領域で、[Username (ユーザ名)]フィールドにネットワーク内のデバイスに適用するユーザ名を入力します。デフォルトのユーザ名とパスワードはciscoです。

注：この例では、ciscoが使用されています。

A screenshot of a configuration form. 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 the input fields is a button labeled 'Apply'.

ステップ3 : パスワードフィールドにパスワードを入力します。

A screenshot of a configuration form. 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 the input fields is a button labeled 'Apply'.

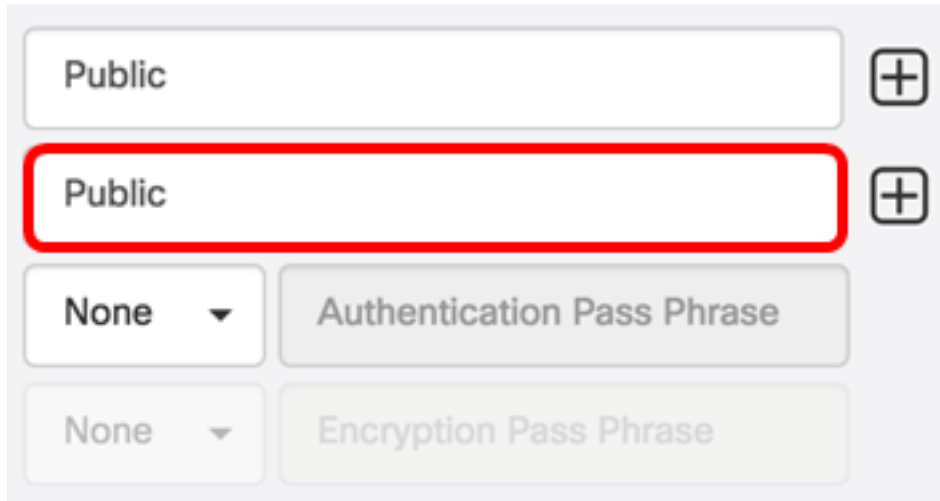
ステップ4:[SNMP Community]フィールドに、*[Community Name]*を入力します。これは、SNMP Getコマンドを認証するための読み取り専用コミュニティストリングです。コミュニティ名は、SNMPデバイスから情報を取得するために使用されます。デフォルトのSNMPコミュニティ名は[Public]です。

注 : この例では、Publicを使用しています。

A screenshot of a configuration form. 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 labeled 'SNMPv3 User Name' 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 labeled 'Authentication Pass Phr' with a green checkmark. The second row has a dropdown menu with 'None' selected and a text field labeled 'Encryption Pass Phrase'.

ステップ5:[SNMPv3 User Name]フィールドに、SNMPv3で使用するユーザ名を入力します

注：この例では、Publicを使用しています。

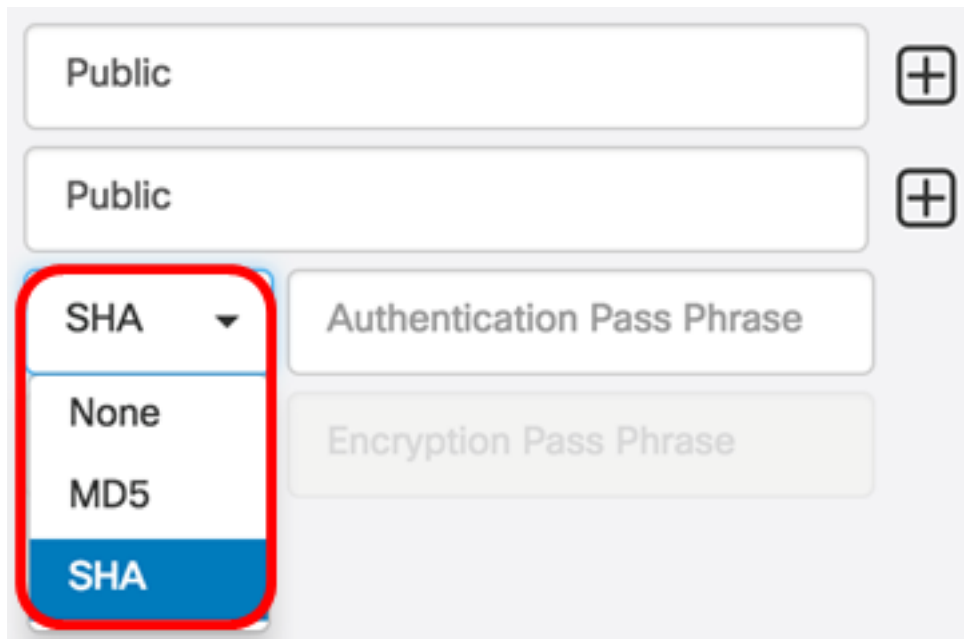


The image shows a configuration interface with a list of entries. The first entry is 'Public' and the second entry is also 'Public' and is highlighted with a red rectangular border. To the right of each entry is a plus sign icon. Below the list are two dropdown menus, both currently set to 'None'. To the right of the first dropdown is a text input field labeled 'Authentication Pass Phrase'. To the right of the second dropdown is a text input field labeled 'Encryption Pass Phrase'.

ステップ6:[Authentication]ドロップダウンメニューから、SNMPv3で使用する認証タイプを選択します。次のオプションがあります。

- None：ユーザ認証は使用されません。これはデフォルトです。このオプションを選択した場合は、ステップ[11に進みます](#)。
- MD5:128ビット暗号化方式を使用します。MD5アルゴリズムは、公開暗号システムを使用してデータを暗号化します。これを選択すると、認証パスフレーズの入力が必要になります。
- SHA:Secure Hash Algorithm(SHA)は、160ビットのダイジェストを生成する一方向のハッシュアルゴリズムです。SHAはMD5より低速ですが、MD5より安全です。これを選択すると、認証パスフレーズを入力して暗号化プロトコルを選択する必要があります。

注：この例では、SHAが使用されています。



The image shows the same configuration interface as before, but the 'Authentication' dropdown menu is now open. The menu is highlighted with a red border and shows four options: 'SHA', 'None', 'MD5', and 'SHA'. The bottom 'SHA' option is highlighted in blue. The 'Authentication Pass Phrase' text input field is now visible and is the focus of the next step.

ステップ7:[Authentication Pass Phrase]フィールドに、SNMPv3で使用するパスワードを入力します。

Public

Public

SHA

None

Encryption Pass Phrase

ステップ8:[Encryption Type]ドロップダウンメニューから、SNMPv3要求を暗号化する暗号化方式を選択します。次のオプションがあります。

- None : 暗号化方式は不要です。
- DES:Data Encryption Standard (DES ; データ暗号規格) は、64ビットの共有秘密キーを使用する対称ブロック暗号です。
- AES128:128ビットキーを使用するAdvanced Encryption Standard (AES ; 高度暗号化規格) 。

注 : この例では、AESが選択されています。

Public

Public

SHA

AES

None

DES

AES

Encryption Pass Phrase


ステップ9:[暗号化パスフレーズ]フィールドに、SNMPが暗号化に使用する128ビットキーを入力します。

Public


Public


SHA ▼ ✓


AES ▼ ✓

ステップ10: (オプション) ボタンをクリック  して、ユーザ名とタイトルの新しいエントリを作成します。クレデンシャルのタイプに応じて、追加エントリを1つまたは2つまで追加できます。

[ステップ11:](#) [Apply] をクリックします。

cisco 

Public 

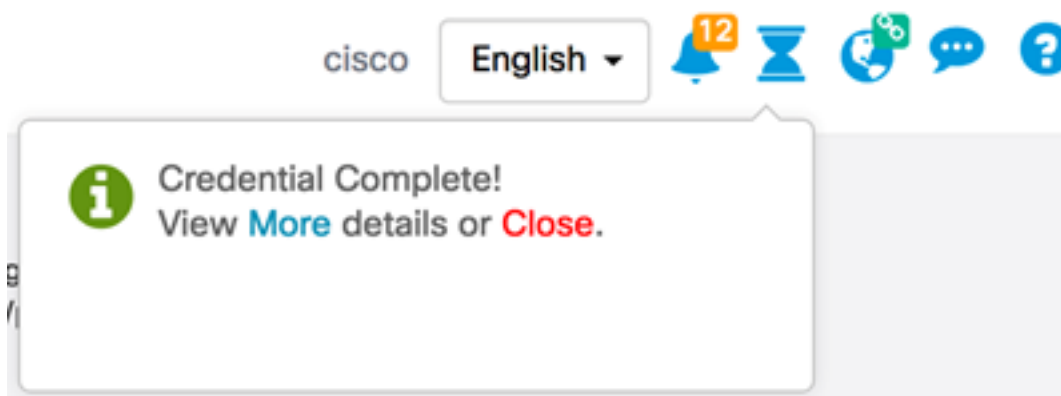
Public 

SHA ▼ ✓

AES ▼ ✓

Apply

時間ガラスアイコンの下にウィンドウが表示され、必要な設定が適用されたことが通知されます。



これで、FindITネットワークプローブのデバイス資格情報が正常に設定されました。

ネットワーク上のデバイスの表示

次の表に、Cisco FindITネットワークプローブによって検出されたデバイスを示します。

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

- Device : ネットワーク上で検出されたデバイスの名前。サービス対象のクレデンシャルのタイプによっては、デバイス名が複数回表示される場合があります。
- [Credential Type]:Admin Userid/PasswordまたはSNMPのいずれかです。これは、デバイスから情報を取得するために使用されます。
- クレデンシャルは正しいですか？ – 上記のフィールドに入力されたクレデンシャルが適切なデバイスに適用されているかどうかを確認するために、チェックまたは赤いXが表示されることがあります。デバイスリストの赤い[X]をクリックすると、デバイスのクレデンシャルの設定が表示されます。
- [Failure Reason] : デバイスがプローブと通信できない場合、障害の理由が列に表示されます。メッセージには、「Invalid credential」または「SNMP disabled」が含まれます。

注：より正確なネットワークトポロジを持つように、デバイスのSNMPを有効にすることを推奨します。

これで、ネットワーク上のデバイスのIDと、対応するクレデンシャルタイプが正常に表示されます。