

Cisco Business Dashboardでのデバイスクレデンシャルの設定

概要

Cisco Business Dashboardは、Webブラウザを使用して、スイッチ、ルータ、ワイヤレスアクセスポイント(WAP)などのシスコビジネスデバイスを簡単に監視、管理、および設定するための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。

Cisco Business Dashboard Network Managementは、次の2つ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。Cisco Business Dashboard Probeと呼ばれる1つ以上のプローブと、Cisco Business Dashboardと呼ばれる1つのダッシュボードです。

ネットワーク内の各サイトにインストールされたCisco Business Dashboard Probe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。単一のサイトネットワークで、Cisco Business Dashboard Probe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Cisco Business Dashboardをインストールし、各プローブをダッシュボード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。

Cisco Business Dashboard Networkがネットワークを完全に検出して管理するには、Cisco Business Dashboard Probe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と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、Cisco Business Dashboard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 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 | ソフトウェアバージョン

- Cisco Businessダッシュボード | 2.2

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: Cisco Business Dashboard GUIにログインし、[Administration] > [Device Credentials]を選択します。

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports



Administration





Administration

Organizations

Device Groups

Device Credentials

Users

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。

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 credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

cisco	●●●●●●●●	🗑️ +
cisco		🗑️

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。

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 credentials may be either a username/password combination, an SNMPv2 community or SNMPv3 credentials.

cisco	●●●●●●●●	🗑️ +
cisco		🗑️

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。

The screenshot shows a configuration form for SNMP. At the top, there are two input fields: one containing 'cisco' and another with masked characters. Below these are two rows of 'Community Name' entries, each with a checkmark and a trash icon. The first 'public' entry is highlighted with a green oval. Below the community names are two dropdown menus for 'Authentication' (set to 'SHA') and 'Encryption' (set to 'AES'), each followed by a masked password field.

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

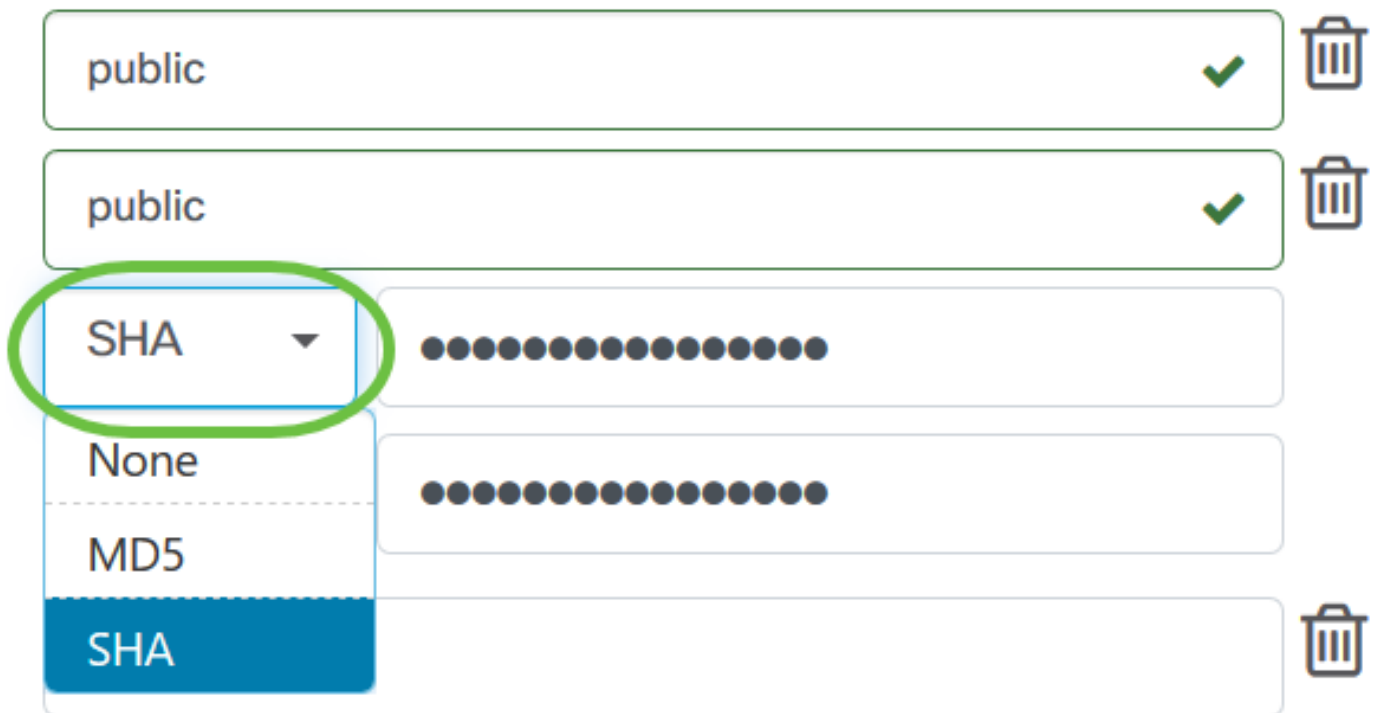
注：この例では、Publicを使用しています。

This screenshot is similar to the previous one, showing the configuration for the SNMPv3 user name. The 'User Name' field is highlighted with a green oval and contains 'public'. The rest of the interface, including the authentication and encryption settings, is identical to the previous screenshot.

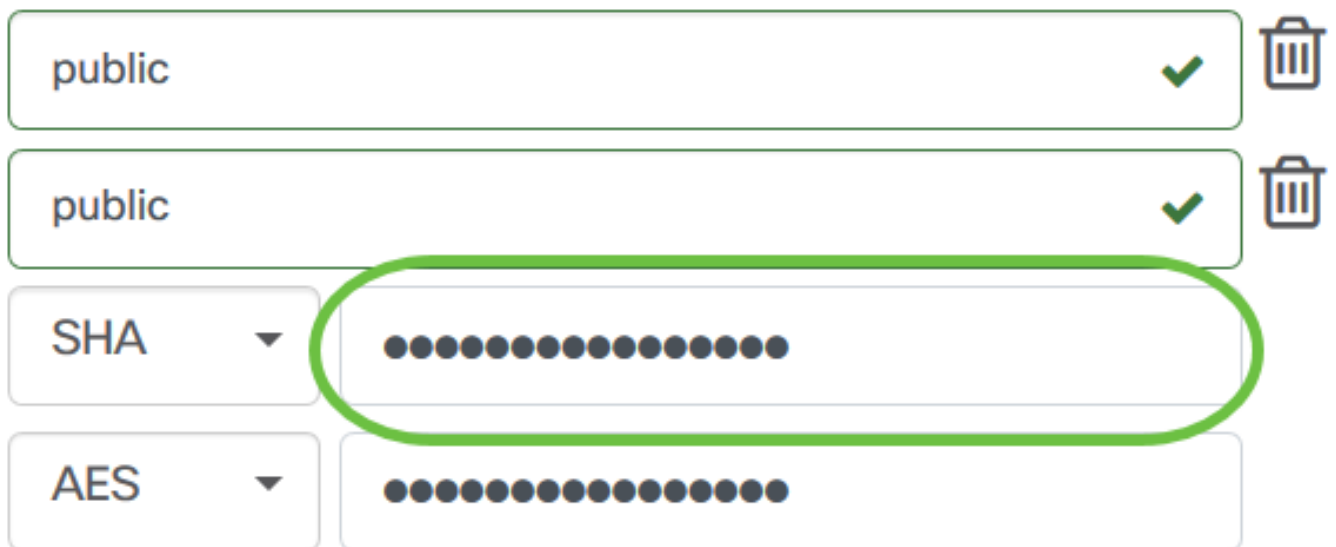
ステップ6:[Authentication]ドロップダウンメニューから、SNMPv3で使用する認証タイプを選択します。次のオプションがあります。

- 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。



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。



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。

- [なし(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。

The image shows a configuration interface with several rows. The first two rows are labeled 'public' and have a green checkmark and a trash can icon. The third row is labeled 'SHA' and has a field of 16 black dots. The fourth row is labeled 'AES' and has a field of 16 black dots; this row is highlighted with a green circle. Below this, a dropdown menu is open, showing options: 'None', 'DES', and 'AES'. The 'AES' option is selected and highlighted in blue. To the right of the 'None' and 'DES' rows is a trash can icon. Below the 'AES' row is a field with a blurred pattern of colored squares.

ステップ9:[暗号化パスワード]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。

The image shows a configuration interface similar to the one above. The first two rows are labeled 'public' and have a green checkmark and a trash can icon. The third row is labeled 'SHA' and has a field of 16 black dots. The fourth row is labeled 'AES' and has a field of 16 black dots; this row is highlighted with a green circle. Below this, a dropdown menu is open, showing options: 'None', 'DES', and 'AES'. The 'AES' option is selected and highlighted in blue. To the right of the 'None' and 'DES' rows is a trash can icon.

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。

🗑️ ⊕

✓ 🗑️

✓ 🗑️

SHA

AES

[ステップ11:](#) [Apply]をクリックします。

🗑️ ⊕

✓ 🗑️

✓ 🗑️

SHA

AES

Apply Reset

これで、Cisco Business Dashboard Probeのデバイス資格情報が正しく設定されました。

ネットワーク上のデバイスの表示

次の表に、Cisco Business Dashboard Probeによって検出されたデバイスを示します。

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	🗑️ 🔄

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。