

Konfigurieren der Geräteanmeldedaten auf der FindIT Network-Probe

Einführung

Das Cisco FindIT Network Management bietet Tools, mit denen Sie Ihre Cisco Netzwerkgeräte der Serien 100 bis 500 wie Switches, Router und WAPs (Wireless Access Points) über Ihren Webbrowser problemlos überwachen, verwalten und konfigurieren können. Darüber hinaus werden Sie über Geräte- und Cisco Support-Benachrichtigungen informiert, wie z. B. die Verfügbarkeit neuer Firmware, den Gerätestatus, Netzwerkeinstellungen-Updates und aller angeschlossenen Cisco Geräte, für die keine Garantie mehr besteht oder die ein Support-Vertrag besteht.

FindIT Network Management ist eine verteilte Anwendung, die aus zwei separaten Komponenten oder Schnittstellen besteht: eine oder mehrere Probes, die als FindIT Network Probe und ein einziger Manager mit dem Namen FindIT Network Manager bezeichnet werden.

Eine Instanz von FindIT Network Probes, die an jedem Standort im Netzwerk installiert ist, führt die Netzwerkerkennung durch und kommuniziert direkt mit jedem Cisco Gerät. In einem einzelnen Standortnetzwerk können Sie eine eigenständige Instanz von FindIT Network Probe ausführen. Wenn Ihr Netzwerk jedoch aus mehreren Standorten besteht, können Sie FindIT Network Manager an einem geeigneten Ort installieren und jede Anfrage mit dem Manager verknüpfen. Über die Manager-Schnittstelle können Sie einen allgemeinen Überblick über den Status aller Standorte in Ihrem Netzwerk erhalten und eine Verbindung mit der Probe herstellen, die an einem bestimmten Standort installiert ist, wenn Sie detaillierte Informationen zu dieser Site anzeigen möchten.

Damit FindIT Network das Netzwerk vollständig erkennen und verwalten kann, muss die FindIT Network Probe über Anmeldeinformationen für die Authentifizierung mit den Netzwerkgeräten verfügen. Wenn ein Gerät zum ersten Mal erkannt wird, versucht die Probe, sich mithilfe des Standardbenutzernamens und -kennworts sowie der SNMP-Community (Simple Network Management Protocol) mit dem Gerät zu authentifizieren. Wenn die Geräteanmeldedaten von der Standardeinstellung geändert wurden, müssen Sie FindIT die richtigen Anmeldeinformationen zuweisen. Wenn dieser Versuch fehlschlägt, wird eine Benachrichtigungsmeldung generiert, und der Benutzer muss gültige Anmeldeinformationen angeben.

Ziel

In diesem Dokument wird erläutert, wie Sie die Geräteanmeldedaten auf der Cisco Network Probe konfigurieren.

Anwendbare Geräte

- FindIT Probe

Softwareversion

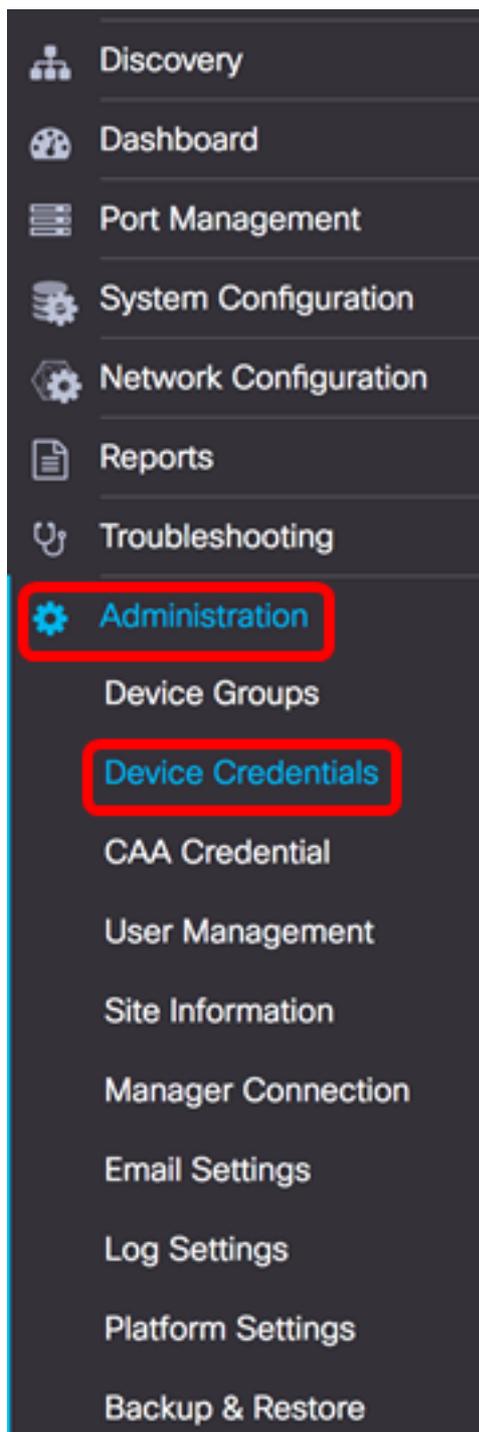
- 1,1

Konfigurieren der Geräteanmeldedaten

Neue Anmeldeinformationen hinzufügen

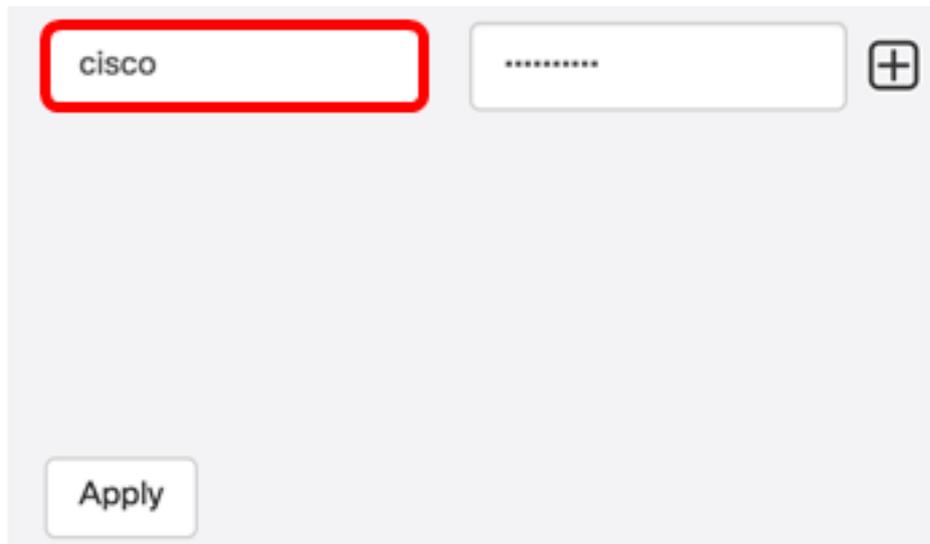
Geben Sie in die Felder unten einen oder mehrere Berechtigungssätze ein. Bei Anwendung werden alle Zertifikate mit Geräten des entsprechenden Typs getestet, für die keine Arbeitsanmeldeinformationen verfügbar sind. Ein Satz von Anmeldeinformationen kann entweder eine Kombination aus Benutzername und Kennwort, eine SNMPv2-Community oder SNMPv3-Anmeldeinformationen sein.

Schritt 1: Melden Sie sich bei der Administratorbenutzeroberfläche von FindIT Network Probe Administrator an, und wählen Sie **Administration > Device Credentials (Administration > Geräteanmeldedaten)** aus.



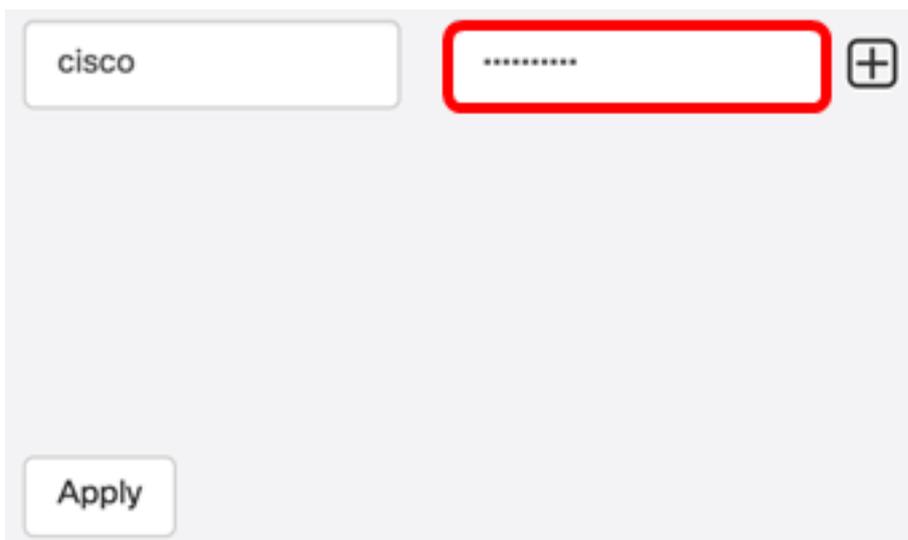
Schritt 2: Geben Sie im Bereich Add New Credentials (Neue Anmeldeinformationen hinzufügen) im Feld *Username* (Benutzername) einen Benutzernamen für die Geräte im Netzwerk ein. Der Standard-Benutzername und das Kennwort lautet cisco.

Hinweis: In diesem Beispiel wird cisco verwendet.



The screenshot shows a web interface for adding credentials. It features two input fields at the top: the first contains the text 'cisco' and is highlighted with a red rectangular border; the second contains a series of dots representing a password. To the right of the password field is a plus sign icon in a square. At the bottom left of the form is a button labeled 'Apply'.

Schritt 3: Geben Sie im Kennwortfeld ein Kennwort ein.



The screenshot shows the same web interface as in Step 2. In this step, the password field, which contains a series of dots, is highlighted with a red rectangular border. The 'Username' field now contains the text 'cisco'. The plus sign icon and the 'Apply' button remain in the same positions.

Schritt 4: Geben Sie im Feld *SNMP Community* (SNMP-Community) den Community-Namen ein. Der schreibgeschützte Community-String authentifiziert den SNMP Get-Befehl. Der Community Name wird verwendet, um die Informationen vom SNMP-Gerät abzurufen. Der standardmäßige SNMP-Community-Name ist Public.

Hinweis: In diesem Beispiel wird Public verwendet.

Schritt 5: Geben Sie im Feld *SNMPv3-Benutzername* einen Benutzernamen für SNMPv3 ein.

Hinweis: In diesem Beispiel wird Public verwendet.

Schritt 6: Wählen Sie im Dropdown-Menü Authentifizierung einen Authentifizierungstyp aus, den SNMPv3 verwenden soll. Folgende Optionen stehen zur Verfügung:

- Keine - Es wird keine Benutzerauthentifizierung verwendet. Dies ist die Standardeinstellung. Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 11 fort](#).
- MD5 - Verwendet eine 128-Bit-Verschlüsselungsmethode. Der MD5-Algorithmus verwendet ein öffentliches Kryptosystem, um Daten zu verschlüsseln. Wenn diese Option ausgewählt ist, müssen Sie eine Authentifizierungs-Kennzeichenfolge eingeben.
- SHA - Secure Hash Algorithm (SHA) ist ein unidirektionaler Hash-Algorithmus, der einen 160-Bit-Digest erzeugt. SHA berechnet langsamer als MD5, ist aber sicherer als MD5. Wenn diese Option ausgewählt ist, müssen Sie eine Authentifizierungs-Kennzeichenfolge eingeben und ein Verschlüsselungsprotokoll auswählen.

Hinweis: In diesem Beispiel wird SHA verwendet.

The image shows a configuration interface with two 'Public' labels and two plus signs on the right. Below them is a dropdown menu with 'SHA' selected and highlighted in blue. To the right of the dropdown are two input fields: 'Authentication Pass Phrase' and 'Encryption Pass Phrase'.

Schritt 7: Geben Sie im Feld *Authentication Pass Phrase* (Authentifizierungskennzeichenfolge) ein Kennwort für SNMPv3 ein.

The image shows the same configuration interface as in Step 7. The 'Authentication Pass Phrase' field is now filled with asterisks and has a green checkmark next to it, indicating it is valid. The 'SHA' dropdown is still selected. The 'Encryption Pass Phrase' field is still empty.

Schritt 8: Wählen Sie im Dropdown-Menü Verschlüsselungstyp eine Verschlüsselungsmethode aus, um die SNMPv3-Anforderungen zu verschlüsseln. Folgende Optionen stehen zur Verfügung:

- Keine: Es ist keine Verschlüsselungsmethode erforderlich.
- DES - Data Encryption Standard (DES) ist eine Verschlüsselung symmetrischer Blöcke, die einen 64-Bit-gemeinsamen geheimen Schlüssel verwendet.
- AES128 - Advanced Encryption Standard, der einen 128-Bit-Schlüssel verwendet.

Hinweis: In diesem Beispiel wird AES ausgewählt.

The screenshot shows a configuration interface with two rows of 'Public' entries. Below these, there are two rows of encryption settings. The first row has 'SHA' selected in a dropdown and a field containing '.....' with a green checkmark. The second row has 'AES' selected in a dropdown and a field containing 'Encryption Pass Phrase'. The 'AES' dropdown and its corresponding field are highlighted with a red border.

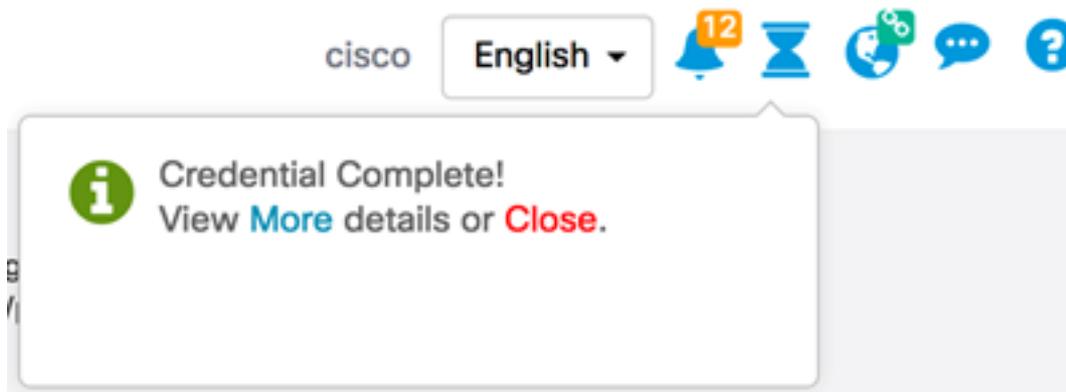
Schritt 9: Geben Sie im Feld *Encryption Pass Phrase* (Verschlüsselungskennzeichenfolge) einen 128-Bit-Schlüssel ein, der von SNMP für die Verschlüsselung verwendet wird.

This screenshot shows the same configuration interface as the previous one. The 'Encryption Pass Phrase' field in the second row is now filled with '.....' and has a green checkmark next to it. This field is highlighted with a red border.

Schritt 10: (Optional) Klicken Sie auf die  Schaltfläche, um einen neuen Eintrag für Benutzername und Titel zu erstellen. Je nach Anmeldeinformationen können Sie bis zu ein oder zwei zusätzliche Einträge hinzufügen.

[Schritt 11](#): Klicken Sie auf **Übernehmen**.

Unter dem Stundengläser-Symbol wird ein Fenster angezeigt, das Sie darüber informiert, dass die erforderlichen Konfigurationen angewendet wurden.



Sie sollten jetzt die Geräteanmeldedaten auf der FindIT Network-Probe erfolgreich konfiguriert haben.

Anzeigen von Geräten im Netzwerk

In der folgenden Tabelle werden die von Cisco FindIT Network Probe erkannten Geräte aufgeführt.

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

- Gerät - Der Name des Geräts, das im Netzwerk erkannt wird. Ein Gerätenamen kann je nach dem Typ der Anmeldeinformationen, für die der Service verfügbar ist, mehrere Male erscheinen.
- Anmeldeinformationstyp - Dies kann entweder Admin-Benutzer-ID/Kennwort oder SNMP

sein. Dies wird verwendet, um Informationen vom Gerät abzurufen.

- Anmeldeinformationen OK? — Es kann ein Häkchen oder ein rotes X angezeigt werden, um festzustellen, ob die in den obigen Feldern eingegebenen Anmeldeinformationen auf das richtige Gerät angewendet wurden. Durch Klicken auf das rote X in der Geräteliste wird die Konfiguration für die Geräteanmeldeinformationen angezeigt.
- Fehlergrund - In der Spalte "Fehlerursache" wird ein Fehlergrund angezeigt, wenn ein Gerät nicht mit der Probe kommunizieren kann. Mögliche Meldungen sind "Invalid Credential" (Ungültige Anmeldeinformationen) oder "SNMP disabled" (SNMP deaktiviert).

Hinweis: Es wird empfohlen, SNMP auf dem Gerät zu aktivieren, um eine genauere Netzwerktopologie zu erhalten.

Sie sollten jetzt die Identität der Geräte im Netzwerk und den entsprechenden Zertifikatstyp erfolgreich überprüft haben.