# Konfigurieren der Geräteanmeldedaten im Cisco Business Dashboard

## Einführung

Das Cisco Business Dashboard bietet Tools, mit denen Sie Ihre Cisco Business-Geräte wie Switches, Router und Wireless Access Points (WAPs) 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.

Cisco Business Dashboard Network Management ist eine verteilte Anwendung, die aus zwei separaten Komponenten oder Schnittstellen besteht: eine oder mehrere Probes, die als Cisco Business Dashboard-Anfrage und als Cisco Business Dashboard bezeichnet werden.

Eine Instanz von Cisco Business Dashboard, die an jedem Standort im Netzwerk installiert ist, führt die Netzwerkerkennung durch und kommuniziert direkt mit jedem Cisco Gerät. In einem einzigen Standortnetzwerk können Sie eine eigenständige Instanz von Cisco Business Dashboard Testen ausführen. Wenn Ihr Netzwerk jedoch aus mehreren Standorten besteht, können Sie das Cisco Business Dashboard an einem geeigneten Ort installieren und jede Anfrage mit dem Dashboard 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 das Cisco Business Dashboard-Netzwerk das Netzwerk vollständig erkennen und verwalten kann, muss die Cisco Business Dashboard-Anfrage 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) zu authentifizieren. Wenn die Geräteanmeldedaten von der Standardeinstellung geändert wurden, müssen Sie dem Cisco Business Dashboard 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 Probe konfigurieren.

### Anwendbare Geräte | Softwareversion

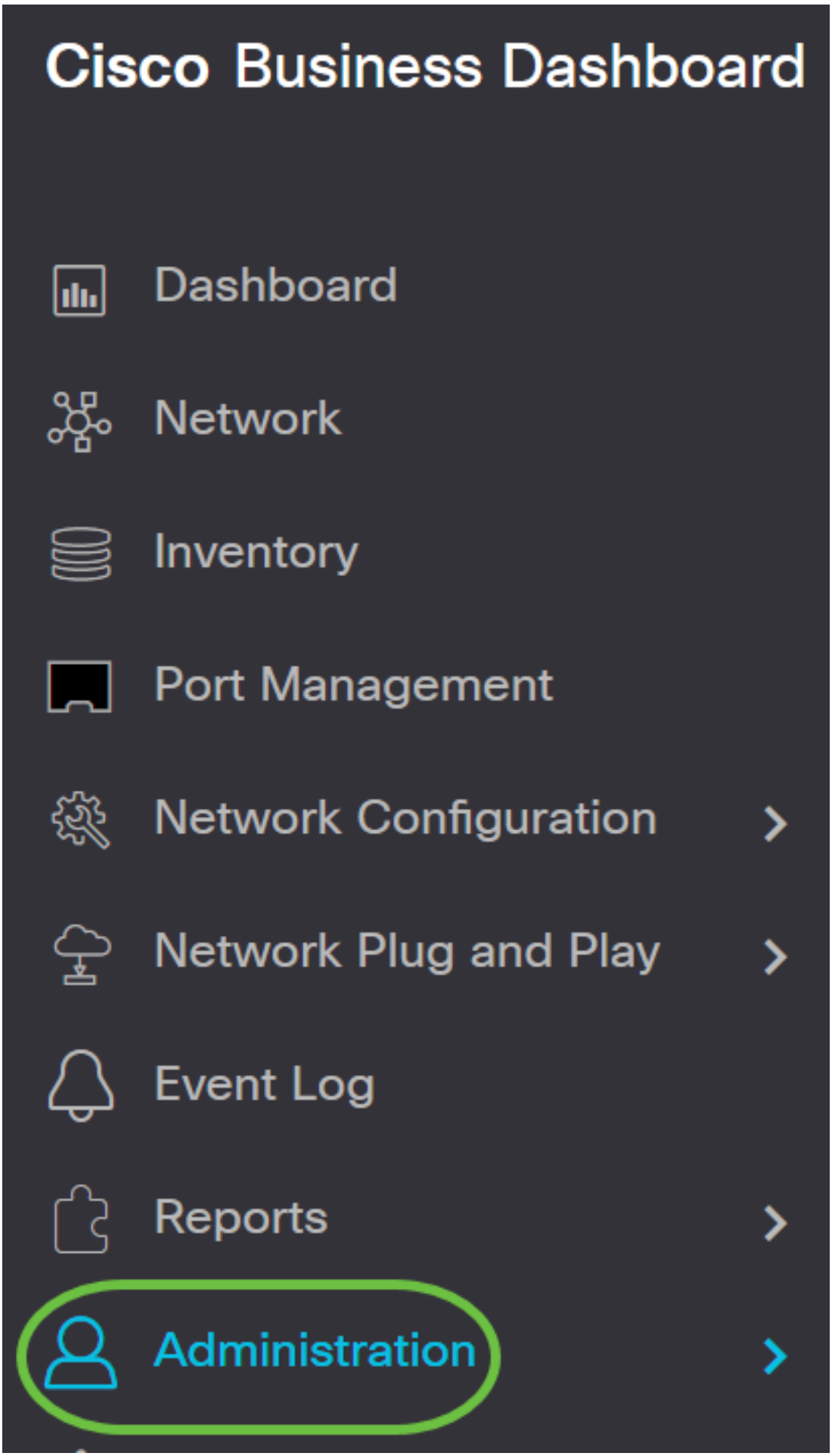
- Cisco Business Dashboard | 2,2

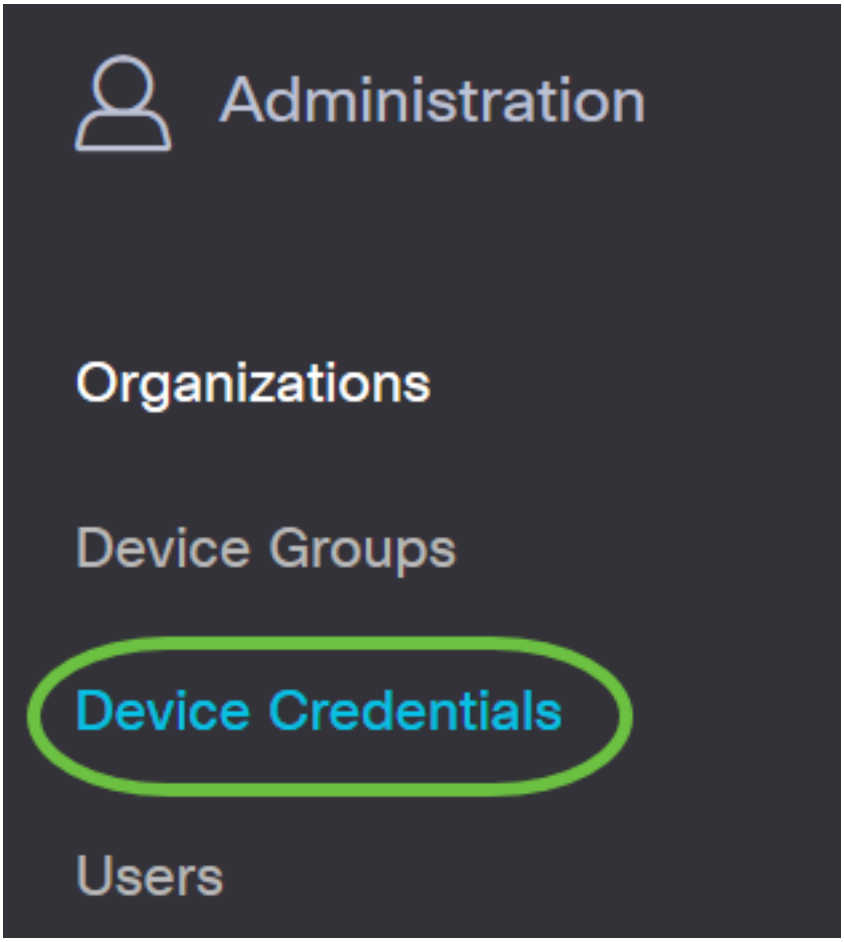
## Konfigurieren der Geräteanmeldedaten

### 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.

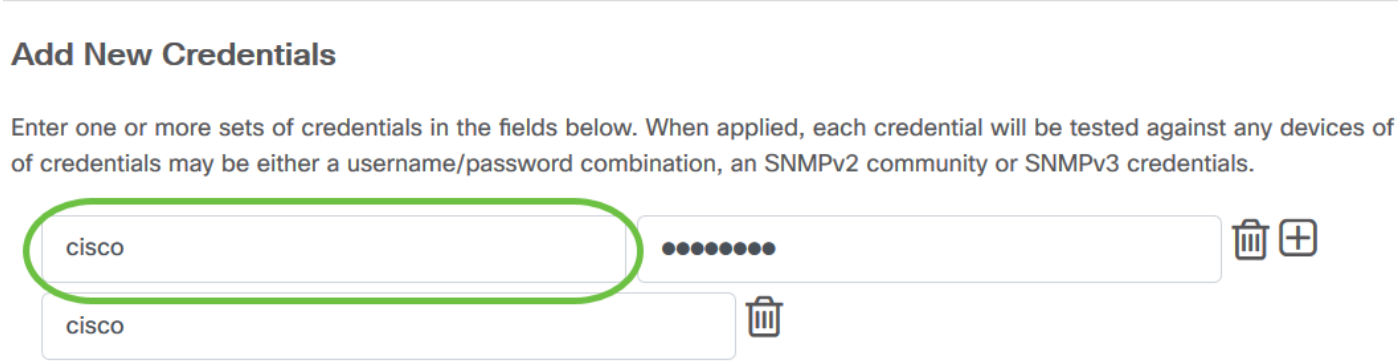
Schritt 1: Melden Sie sich bei der Benutzeroberfläche des Cisco Business Dashboard an, und wählen Sie **Administration > Device Credentials (Verwaltung > Geräteanmeldedaten)**.


Cisco Business Dashboard
Dashboard
Network
Inventory
Port Management
Network Configuration
Network Plug and Play
Event Log
Reports
Administration

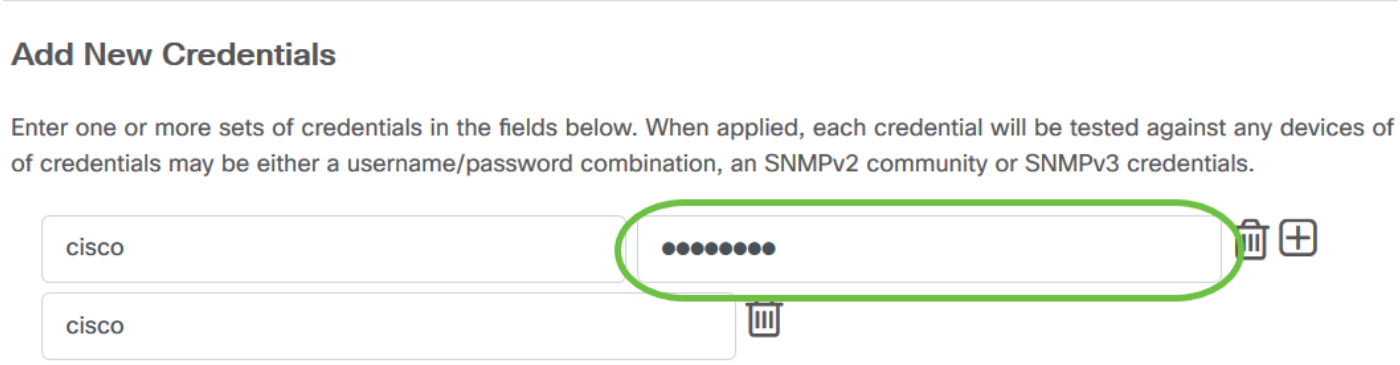



Schritt 2: Geben Sie im Bereich Add New Credentials (Neue Anmeldeinformationen hinzufügen) im Feld *Username* (Benutzername) einen Benutzernamen für die Geräte im Netzwerk ein. Der Standard-Benutzername und das Kennwort lautet cisco.

**Hinweis:** In diesem Beispiel wird cisco verwendet.

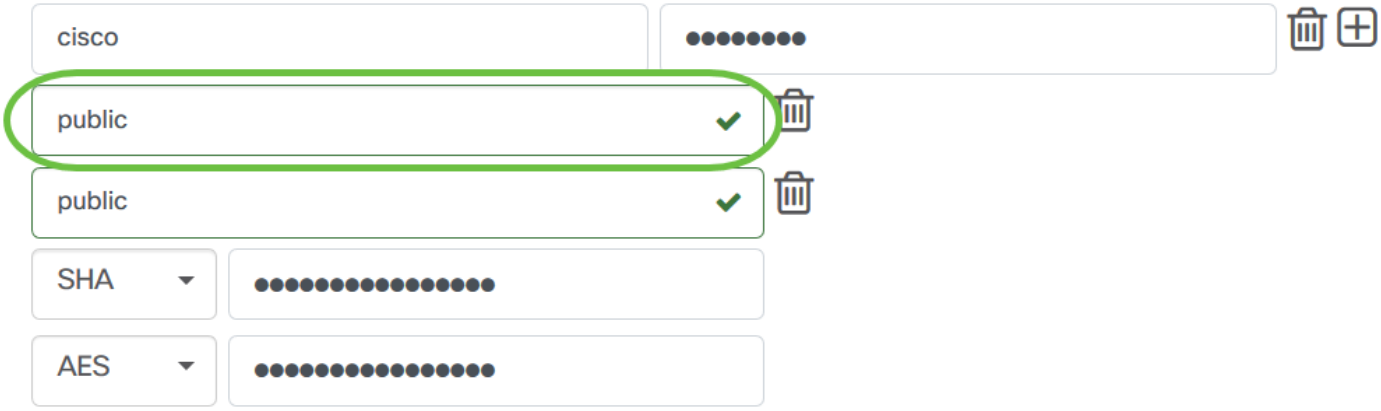



Schritt 3: Geben Sie im Kennwortfeld ein Kennwort ein.



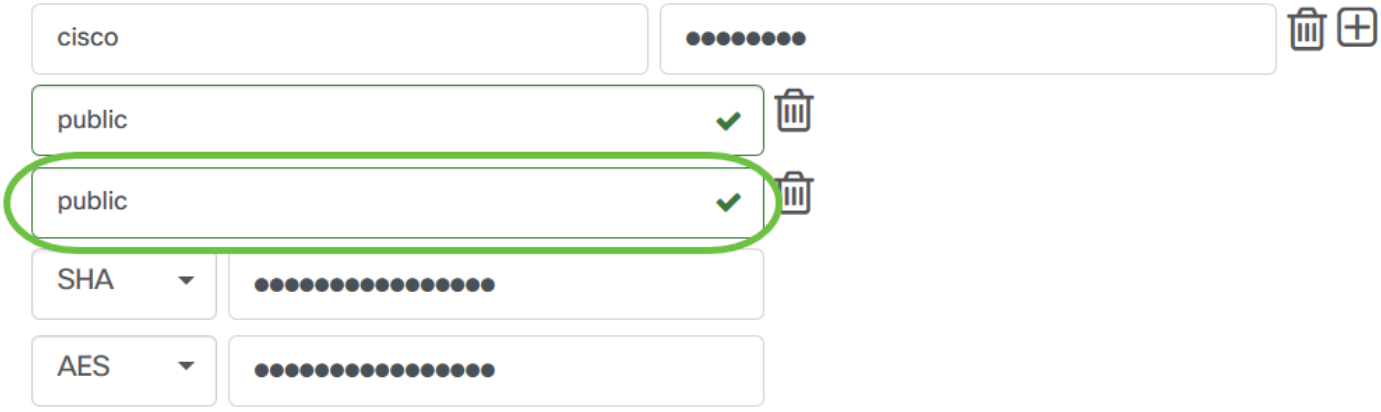
Schritt 4: Geben Sie im Feld *SNMP Community* (SNMP-Community) den Community-Namen ein. Der schreibgeschützte Community-String authentifiziert den SNMP Get-Befehl. Der Community Name wird verwendet, um die Informationen vom SNMP-Gerät abzurufen. Der standardmäßige SNMP-Community-Name ist Public.

**Hinweis:** In diesem Beispiel wird Public verwendet.




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

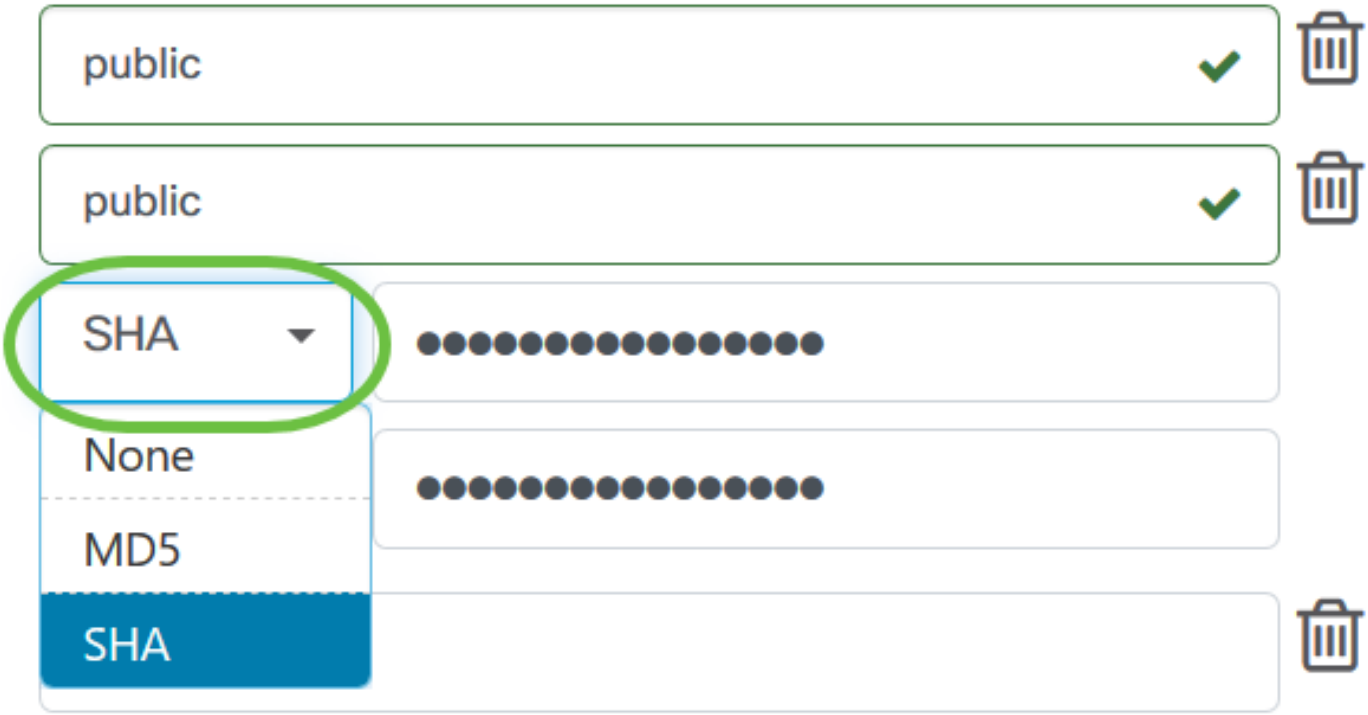
**Hinweis:** In diesem Beispiel wird Public verwendet.



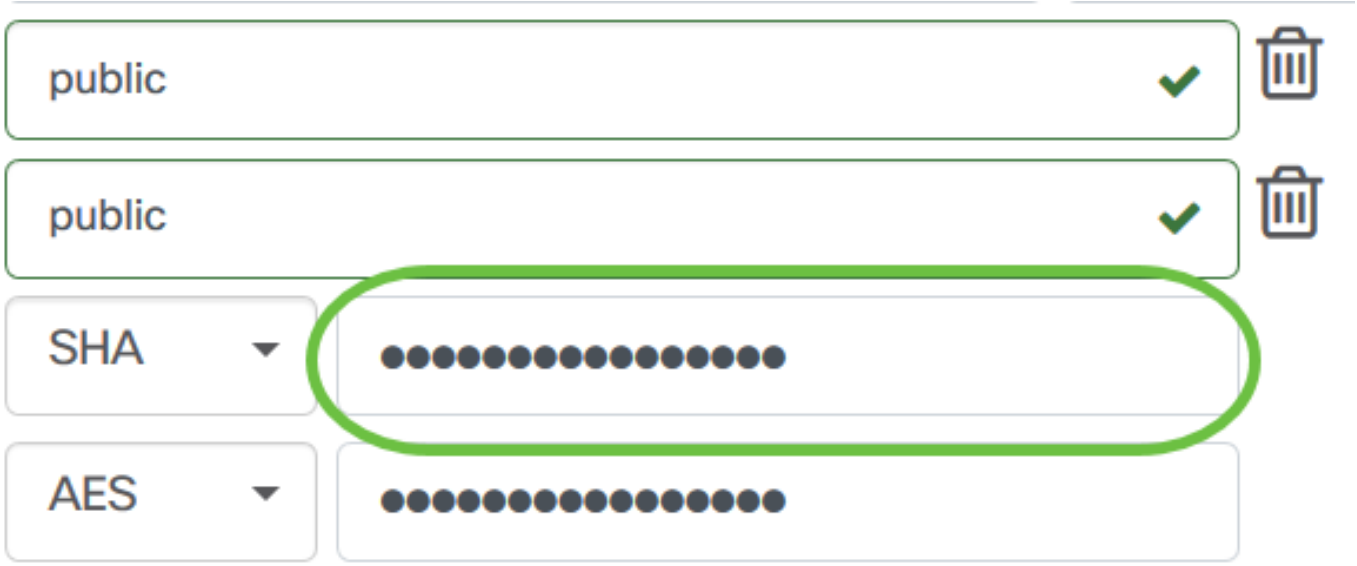

Schritt 6: Wählen Sie im Dropdown-Menü Authentifizierung einen Authentifizierungstyp aus, den SNMPv3 verwenden soll. Folgende Optionen stehen zur Verfügung:

- 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.



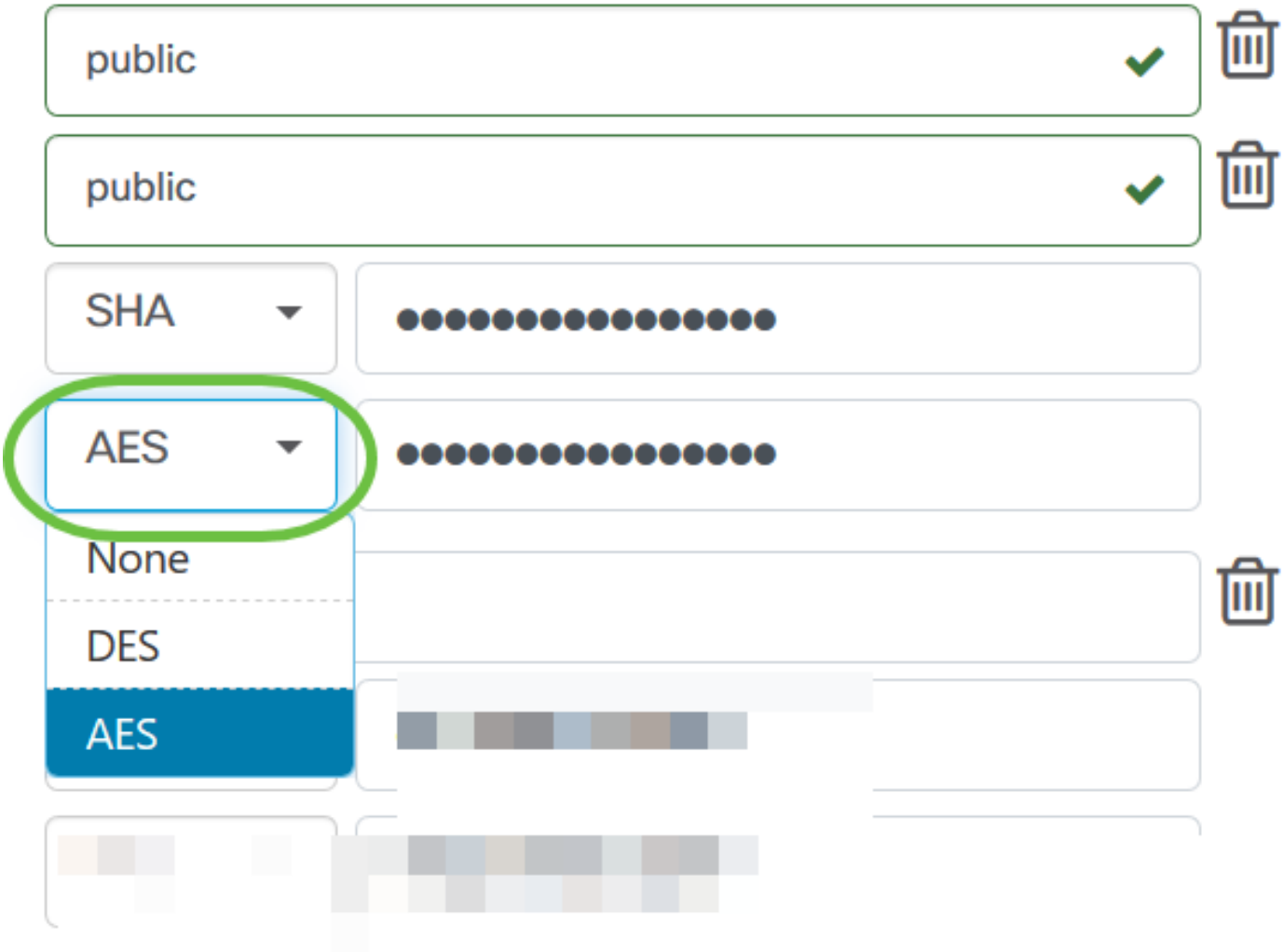

Schritt 7: Geben Sie im Feld *Authentication Pass Phrase* (Authentifizierungskennzeichenfolge) ein Kennwort für SNMPv3 ein.




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

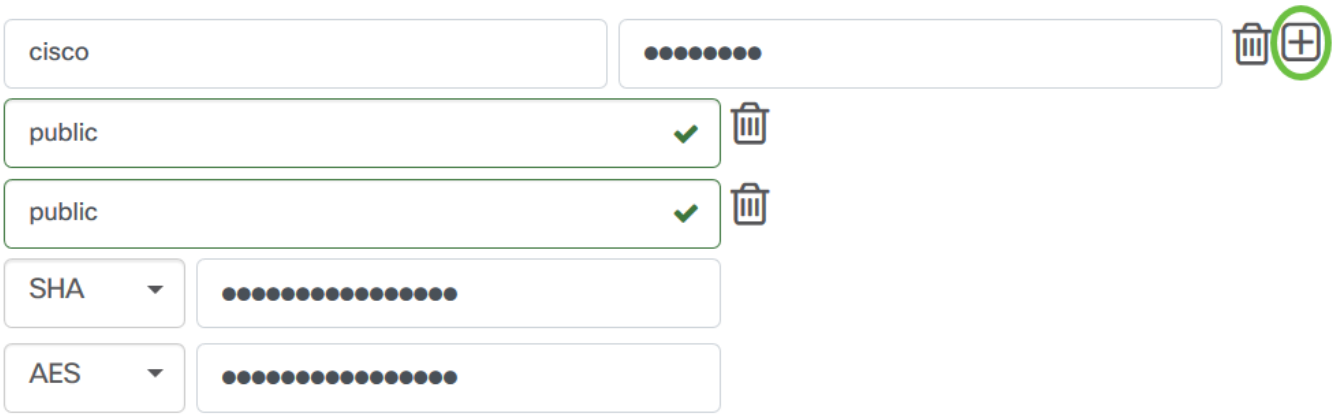
- Keine - Es ist keine Verschlüsselungsmethode erforderlich.
- DES - Data Encryption Standard (DES) ist eine symmetrische Blockchiffre, die einen 64-Bit-gemeinsamen geheimen Schlüssel verwendet.
- AES128 - Advanced Encryption Standard, der einen 128-Bit-Schlüssel verwendet.

**Hinweis:** In diesem Beispiel wird AES ausgewählt.

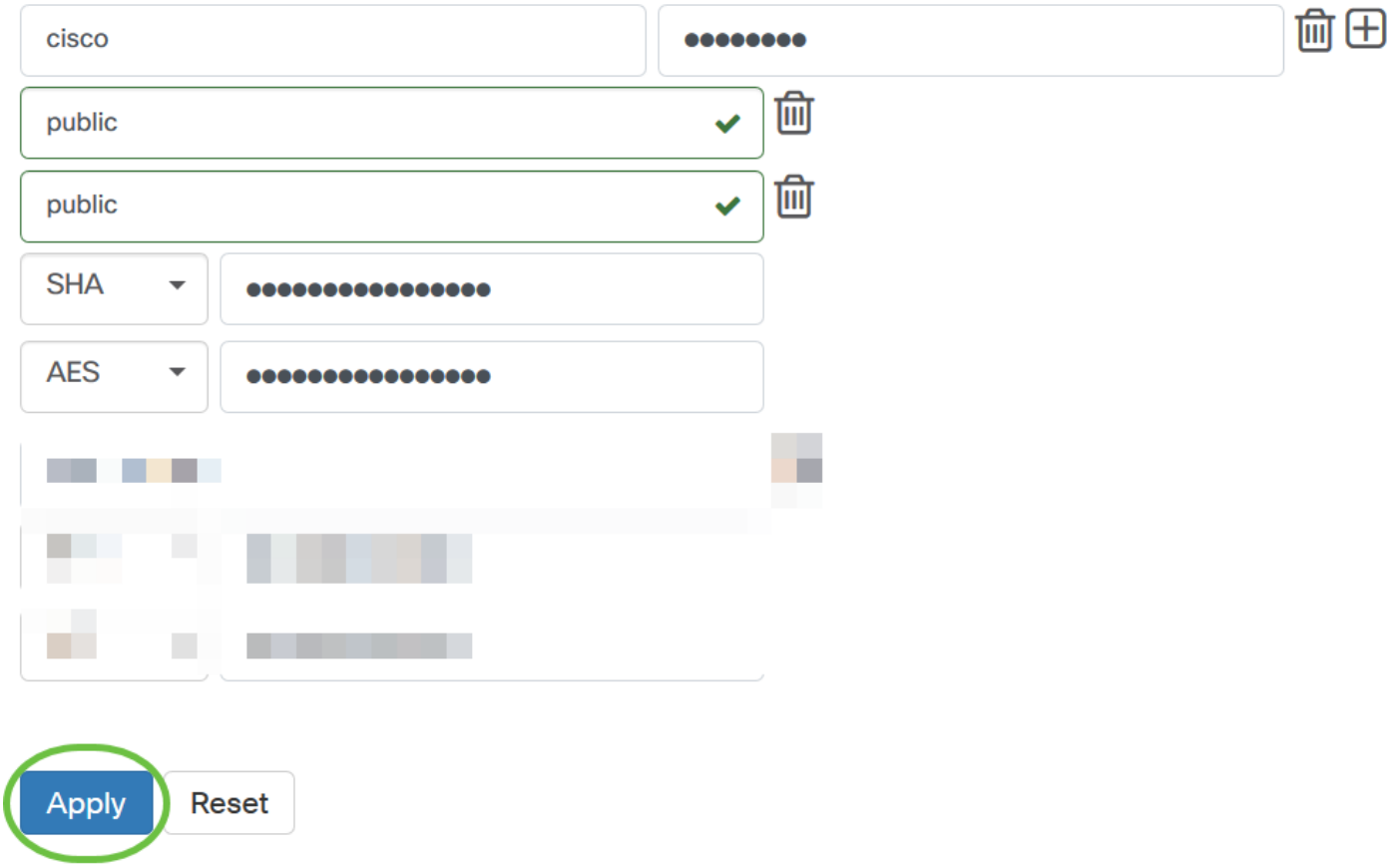



Schritt 9: Geben Sie im Feld *Encryption Pass Phrase* (Verschlüsselungskennzeichenfolge) einen 128-Bit-Schlüssel ein, der von SNMP für die Verschlüsselung verwendet wird.


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**.




Sie sollten jetzt die Geräteanmeldedaten für die Cisco Business Dashboard-Anfrage erfolgreich konfiguriert haben.

## Anzeigen von Geräten im Netzwerk

In der folgenden Tabelle werden die Geräte aufgeführt, die von Cisco Business Dashboard-Tests erkannt wurden.

| 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 | |

**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.