Modifier les informations d'identification des périphériques à partir de Cisco Catalyst Center pour les périphériques filaires et sans fil pour les scénarios de réseau SDA et non SDA

Table des matières

Introduction

Informations générales

Résumé

Solution (Meilleure pratique)

- Exigences
- Conditions préalables

Procédure de modification des informations d'identification de Cisco Catalyst Center

- Sites avec AAA géré par Cisco Catalyst Center
  - Il est obligatoire de modifier le mot de passe de l'utilisateur (pas de modification du mot de passe actif)
  - Vous devez modifier le mot de passe de l'utilisateur et le mot de passe enable
- Sites avec Cisco Catalyst Center AAA non géré
  - Il est obligatoire de modifier le mot de passe de l'utilisateur (pas de modification du mot de passe actif)
  - Vous devez modifier le mot de passe de l'utilisateur et le mot de passe enable

Introduction

Ce document décrit les étapes de la procédure de modification des informations d'identification à partir de Cisco Catalyst Center (anciennement Cisco DNA Center) pour les périphériques filaires et sans fil pour les scénarios de réseau de fabric et non de fabric.

Informations générales

Ce document s'applique également aux sites avec Dynamic Network Access Control (Cisco Catalyst Center) géré ou non géré Authentication, Authorization and Accounting (AAA).

Résumé

Ce document traite de la situation dans laquelle il existe une exigence réseau de mise à jour des identifiants utilisés par Cisco Catalyst Center pour l'automatisation. Les périphériques gérés sont détectés par Cisco Catalyst Center avec un nom d'utilisateur et un mot de passe, et ces mêmes informations d'identification sont utilisées par Cisco Catalyst Center pour les connexions SSH aux périphériques gérés (pour l'automatisation/la collecte d'inventaire, etc.). Ce document présente les

meilleures pratiques pour modifier le mot de passe des périphériques gérés après leur détection par Cisco Catalyst Center.

Solution (Meilleure pratique)

Exigences

1. Pour les sites avec AAA géré par Cisco Catalyst Center

- Vous devez modifier le mot de passe de l'utilisateur (pas de modification du mot de passe actif).
- Vous devez modifier le mot de passe de l'utilisateur et le mot de passe enable.

2. Pour les sites avec Cisco Catalyst Center AAA non géré

- Vous devez modifier le mot de passe de l'utilisateur (pas de modification du mot de passe actif).
- Vous devez modifier le mot de passe de l'utilisateur et le mot de passe enable.

Conditions préalables

- Assurez-vous que AAA n'est pas configuré dans Cisco Catalyst Center pour tous les sites non SDA.
- Utilisez un script Python pour valider si tous les commutateurs Catalyst 9k (SDA ou non-SDA) utilisent RADIUS vers ISE pour les connexions SSH aux lignes VTY. Corrigez tous les périphériques qui utilisent des informations d'identification locales.
- Pour les noeuds étendus
    - Pour mettre à jour les lignes vty 0 à 4, utilisez ces commandes de configuration (il peut s’agir de la toute première étape pour les noeuds étendus).

```
line vty 0 4
authorization exec VTY_author
login authentication VTY_authen
```

Procédure de modification des informations d'identification de Cisco Catalyst Center

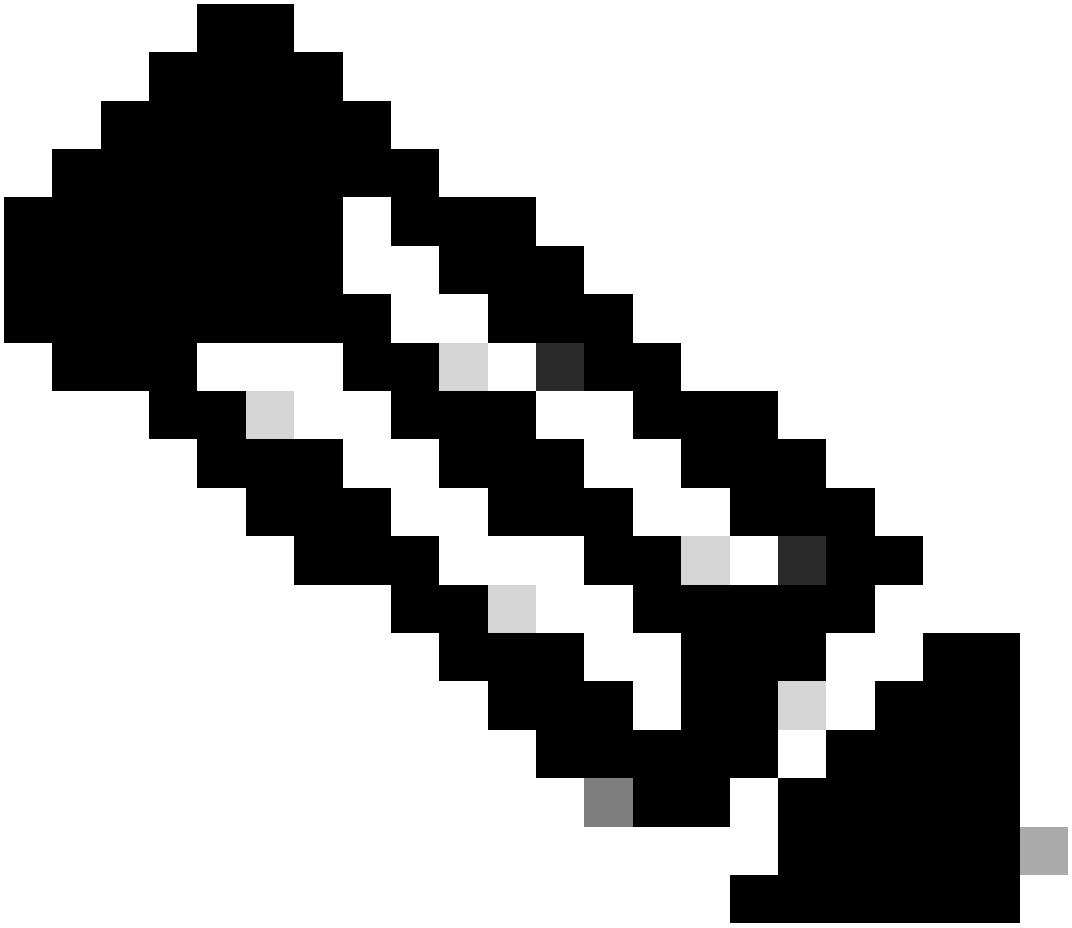
Sites avec AAA géré par Cisco Catalyst Center

Il est obligatoire de modifier le mot de passe de l'utilisateur (pas de modification du mot de passe actif)

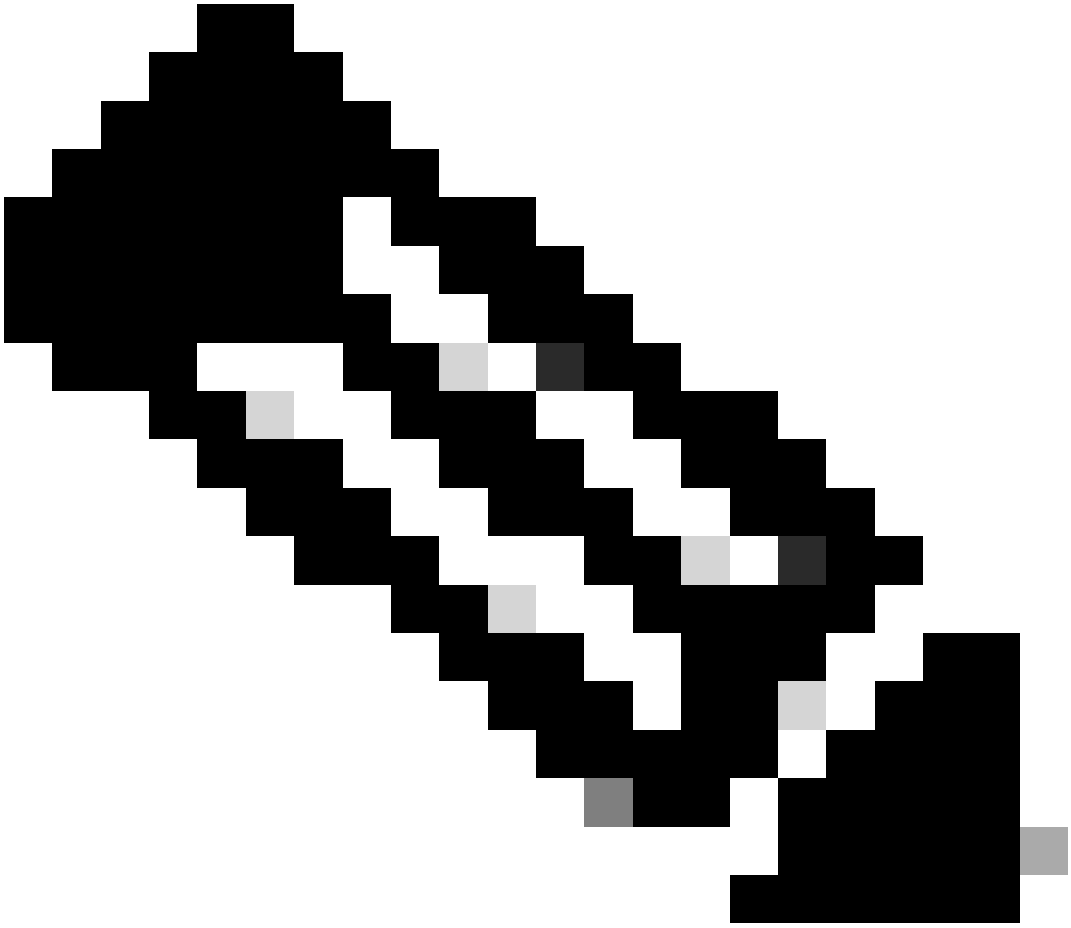
1. Mettez d'abord à jour les informations d'identification (mot de passe pour le nom d'utilisateur

approprié) dans ISE. Cela entraînera un échec de collecte d'inventaire et les états d'inventaire des périphériques gérés passeront à Inaccessible, Échec de collecte partielle ou Informations d'identification incorrectes.

2. Sur la page Provisionner > Inventaire, sélectionnez un ou plusieurs périphériques et sélectionnez Actions > Inventaire > Modifier le périphérique > onglet Informations d'identification. Ensuite, mettez à jour les informations d'identification « Add device specific credential » avec le nouveau nom d'utilisateur et/ou mot de passe (conservez le même mot de passe actif). À ce stade, Cisco Catalyst Center sera en mesure de se connecter aux périphériques avec les informations d'identification mises à jour et les états d'inventaire des périphériques reviendront à Géré.
3. Les informations d'identification locales des périphériques peuvent être mises à jour en tant que secours afin de s'assurer que Cisco Catalyst Center est en mesure de se connecter aux périphériques lorsque le serveur AAA externe est inaccessible. Les informations d'identification locales peuvent être mises à jour à l'aide de l'Éditeur de modèle de Cisco Catalyst Center, d'un script Python personnalisé ou manuellement.
4. La dernière étape consiste à mettre à jour ces mêmes informations d'identification sur la page Informations d'identification et de connexion globales. Cela permet de s'assurer que les périphériques récemment découverts ou ajoutés à l'aide de LAN Automation utilisent les informations d'identification mises à jour de la page Conception > Paramètres réseau > Informations d'identification des périphériques > Informations d'identification de l'interface de ligne de commande > modifier le nom d'utilisateur > mettre à jour le mot de passe de l'utilisateur sans modifier le mot de passe actif.



Remarque : la connexion SSH/Telnet est authentifiée par le serveur AAA externe. Les informations d'identification du périphérique local ne sont pas mises à jour.



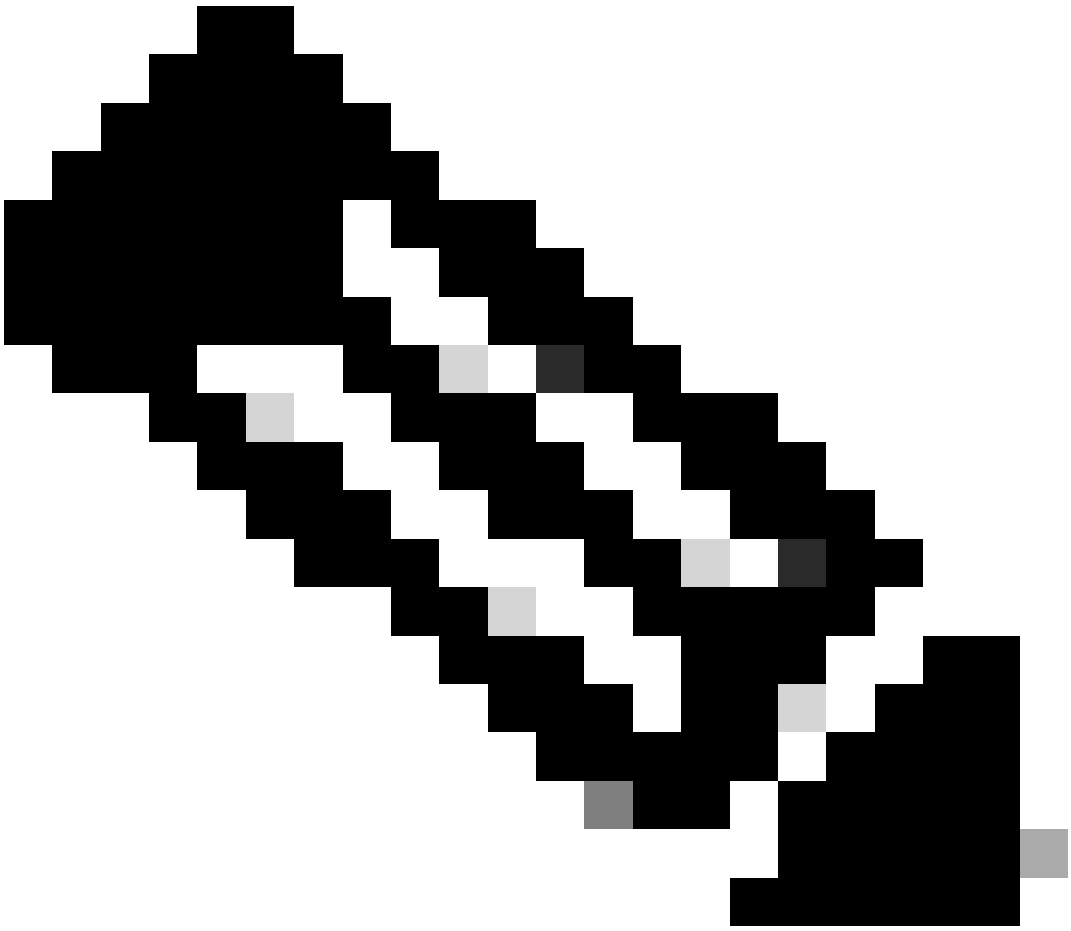
Remarque : lorsqu'un serveur AAA externe est configuré sur la page de conception de Cisco Catalyst Center pour un site, Cisco Catalyst Center n'effectue aucune action sur les périphériques gérés ou ISE lorsque vous modifiez les informations d'identification sur la page Informations d'identification globales.

Vous devez modifier le mot de passe de l'utilisateur et le mot de passe enable

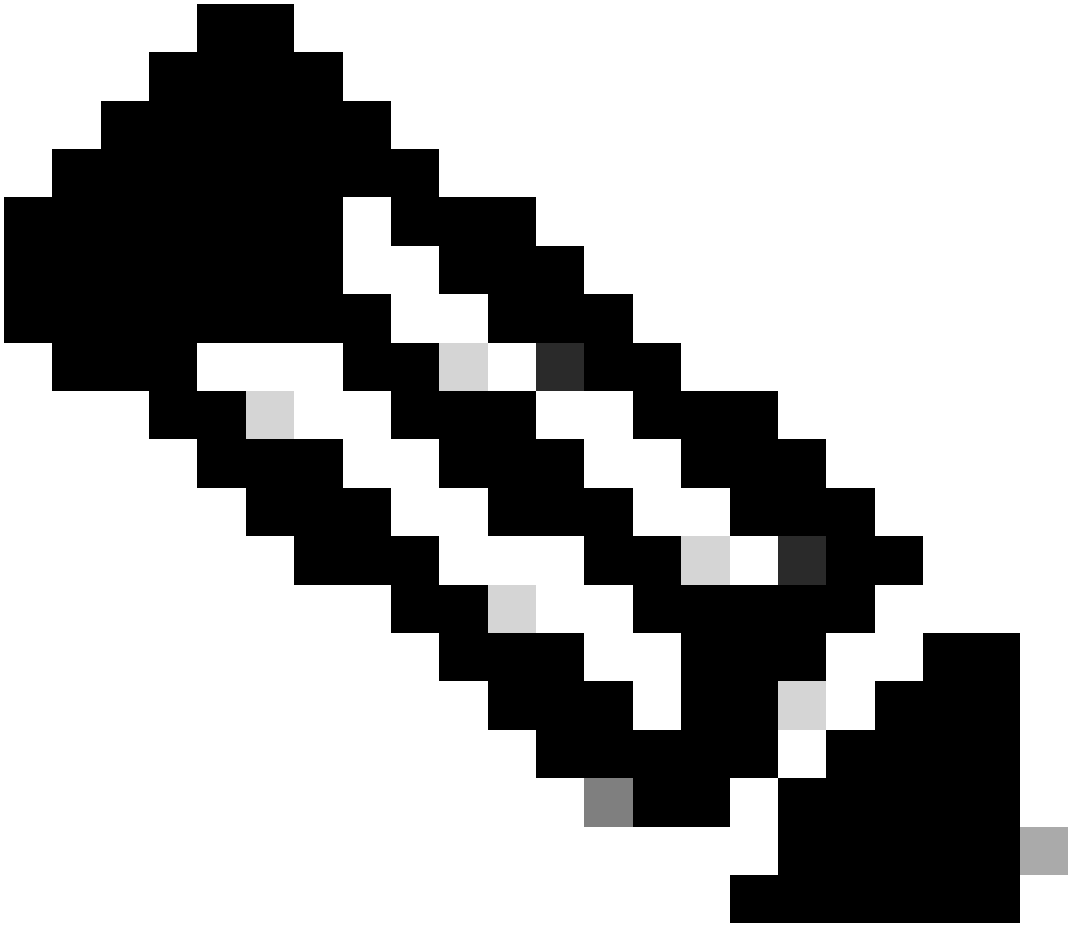
1. Mettez d'abord à jour les informations d'identification (mot de passe pour le nom d'utilisateur approprié) dans ISE. Cela entraînera un échec de collecte d'inventaire et les états d'inventaire des périphériques gérés passeront à Inaccessible, Échec de collecte partielle ou Informations d'identification incorrectes.
2. Sur la page Provisionner > Inventaire, sélectionnez un ou plusieurs périphériques et sélectionnez Actions > Inventaire > Modifier le périphérique > onglet Informations d'identification. Ensuite, mettez à jour les informations d'identification « Add device specific credential » avec le nouveau nom d'utilisateur et/ou mot de passe ainsi que le mot de passe enable. À ce stade, Cisco Catalyst Center sera en mesure de se connecter aux

périphériques avec les informations d'identification mises à jour et les états d'inventaire des périphériques reviendront à Géré.

3. La dernière étape consiste à mettre à jour ces mêmes informations d'identification sur la page Informations d'identification et de connexion globales. Cela permet de s'assurer que les périphériques récemment découverts ou ajoutés à l'aide de LAN Automation utilisent les informations d'identification mises à jour de la page Conception > Paramètres réseau > Informations d'identification des périphériques > Informations d'identification de l'interface de ligne de commande > modifier le nom d'utilisateur > mettre à jour le mot de passe de l'utilisateur et le mot de passe actif.



Remarque : lorsque le serveur AAA externe est accessible, le nom d'utilisateur et le mot de passe sont authentifiés par le serveur AAA externe et le mot de passe actif est authentifié localement par le périphérique géré.



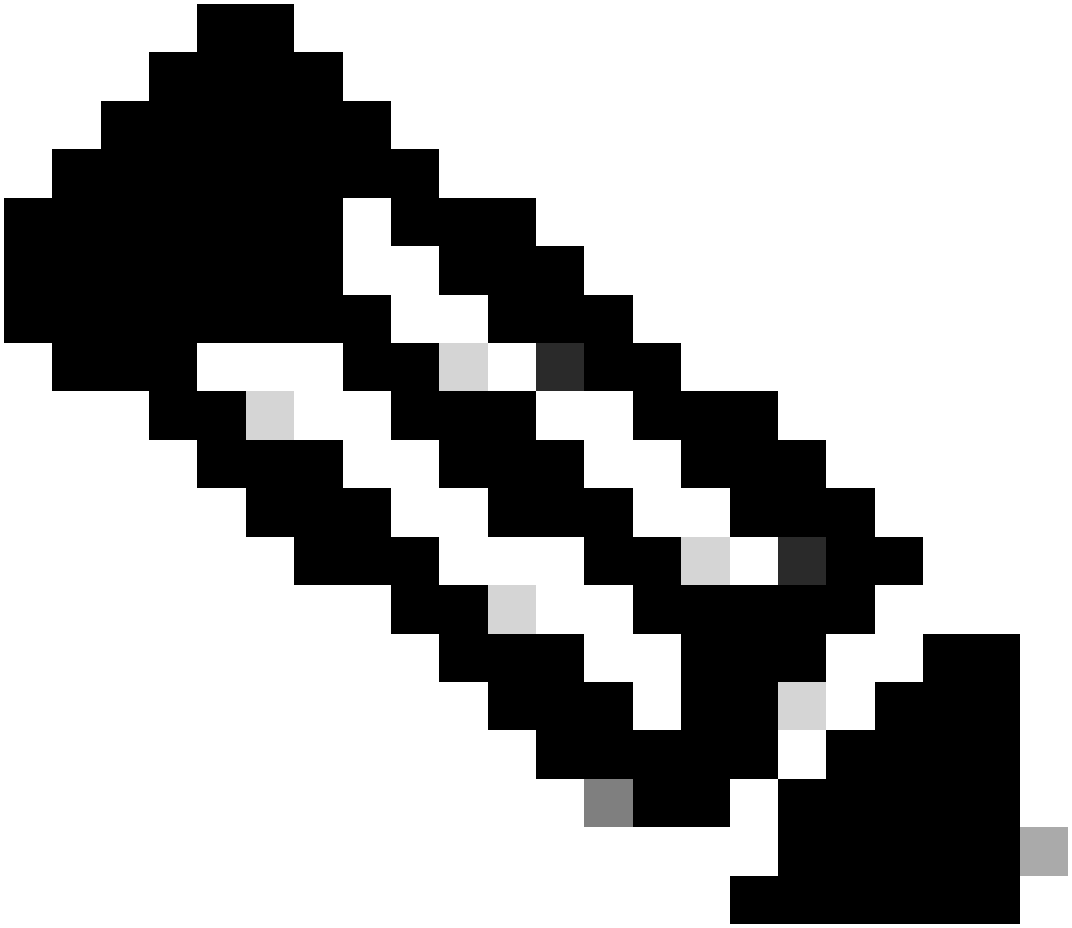
Remarque : lorsqu'un serveur AAA externe est configuré sur la page de conception de Cisco Catalyst Center pour un site, Cisco Catalyst Center n'effectue aucune action sur les périphériques ou ISE lorsque vous modifiez les informations d'identification sur la page Informations d'identification globales.

Sites avec Cisco Catalyst Center AAA non géré

Il est obligatoire de modifier le mot de passe de l'utilisateur (pas de modification du mot de passe actif)

1. Mettez à jour les informations d'identification sur la page Global Credentials de Design > Network Settings > Device Credentials > CLI Credentials > edit the username > update the user’s password sans modifier le mot de passe enable.
2. Une fois les informations d'identification modifiées sur la page Informations d'identification globales, les périphériques gérés sur les sites où Cisco Catalyst Center ne gère pas le système AAA peuvent être reconfigurés avec les informations d'identification mises à jour.

Cisco Catalyst Center peut diffuser un script EEM temporaire pour valider les informations d'identification. Si la connexion réussit, la configuration peut être conservée.

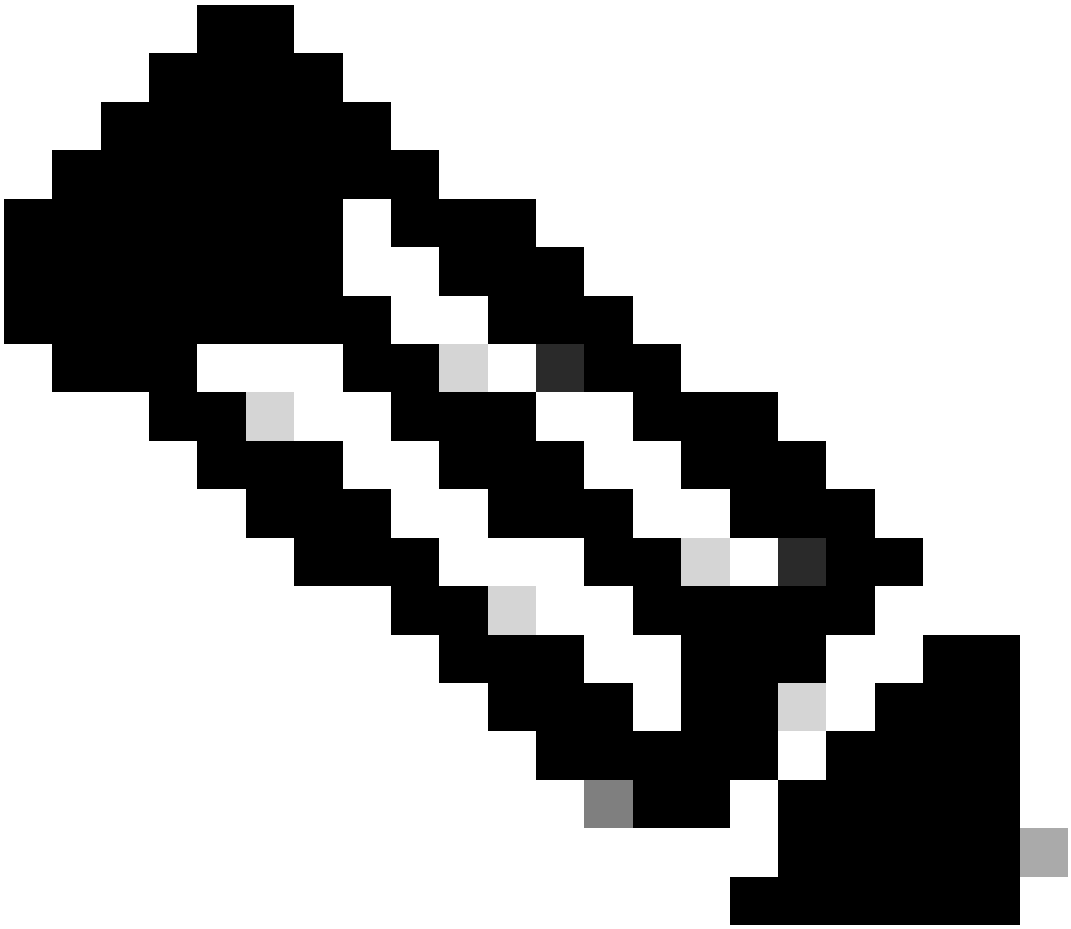


Remarque : pour les périphériques gérés sur les sites où Cisco Catalyst Center ne gère pas la configuration AAA, Cisco Catalyst Center ne sait pas si les périphériques gérés sont configurés manuellement avec le serveur AAA externe ou si les périphériques gérés utilisent uniquement des informations d'identification locales. Assurez-vous donc que le mot de passe est mis à jour sur le serveur AAA externe s'il est configuré sur les périphériques gérés concernés avant de poursuivre ces étapes.

Vous devez modifier le mot de passe de l'utilisateur et le mot de passe enable

1. Mettez à jour les informations d'identification sur la page Global Credentials de Design > Network Settings > Device Credentials > CLI Credentials > edit the username > update the user's password with the enable password.
2. Une fois les informations d'identification modifiées sur la page Informations d'identification globales, les périphériques gérés sur les sites où Cisco Catalyst Center ne gère pas le

système AAA peuvent être reconfigurés avec les informations d'identification mises à jour. Cisco Catalyst Center peut diffuser un script EEM temporaire pour valider les informations d'identification. Si la connexion réussit, la configuration peut être conservée.



Remarque : pour les périphériques gérés sur les sites où Cisco Catalyst Center ne gère pas la configuration AAA, Cisco Catalyst Center ne sait pas si les périphériques gérés sont configurés manuellement avec le serveur AAA externe ou si les périphériques gérés utilisent uniquement des informations d'identification locales. Assurez-vous donc que le mot de passe est mis à jour sur le serveur AAA externe s'il est configuré sur les périphériques gérés concernés avant de poursuivre ces étapes.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.