

SDAおよび非SDAネットワークシナリオの両方で、有線およびワイヤレスデバイスのCisco Catalyst Centerからデバイスクレデンシャルを変更する

内容

[はじめに](#)

[背景説明](#)

[概要](#)

[ソリューション \(ベストプラクティス \)](#)

[要件](#)

[前提条件](#)

[Cisco Catalyst Centerからのクレデンシャルの変更手順](#)

[Cisco Catalyst CenterマネージドAAAを使用するサイト](#)

[ユーザのパスワード変更が必要 \(イネーブルパスワードの変更なし \)](#)

[ユーザのパスワードとイネーブルパスワードの変更が必要](#)

[Cisco Catalyst CenterアンマネージドAAAを使用するサイト](#)

[ユーザのパスワード変更が必要 \(イネーブルパスワードの変更なし \)](#)

[ユーザのパスワードとイネーブルパスワードの変更が必要](#)

はじめに

このドキュメントでは、ファブリックと非ファブリックの両方のネットワークシナリオで有線およびワイヤレスデバイス用にCisco Catalyst Center (旧称Cisco DNA Center) からクレデンシャルを変更する手順について説明します。

背景説明

このドキュメントは、ダイナミックネットワークアクセスコントロール(Dynamic Network Access Control)(Cisco Catalyst Center)の管理対象または管理対象外の認証、許可、アカウントティング(AAA)を使用するサイトにも適用されます。

概要

このドキュメントでは、自動化のためにCisco Catalyst Centerで使用されるクレデンシャルを更新するネットワーク要件がある状況について説明します。 管理対象デバイスは、ユーザ名とパスワードを使用してCisco Catalyst Centerによって検出され、同じクレデンシャルがCisco Catalyst Centerによって管理対象デバイスへのSSH接続 (自動化/インベントリ収集など) に使用されます。 このドキュメントでは、管理対象デバイスがCisco Catalyst Centerによって検出された後に、

そのパスワードを変更するベストプラクティスについて説明します。

ソリューション (ベストプラクティス)

要件

1. Cisco Catalyst CenterマネージドAAAを使用するサイト
 - ユーザのパスワードを変更する必要がある (イネーブルパスワードは変更しない) 。
 - ユーザのパスワードとイネーブルパスワードを変更する必要があります。
2. Cisco Catalyst CenterアンマネージドAAAを使用するサイト
 - ユーザのパスワードを変更する必要がある (イネーブルパスワードは変更しない) 。
 - ユーザのパスワードとイネーブルパスワードを変更する必要があります。

前提条件

- Cisco Catalyst Centerで、すべての非SDAサイトに対してAAAが設定されていないことを確認します。
- Pythonスクリプトを使用して、すべてのCatalyst 9kスイッチ (SDAまたは非SDA) がVTY回線へのSSHログインにRADIUSからISEを使用しているかどうかを検証します。ローカルクレデンシャルを使用しているデバイスを修正します。
- 拡張ノード用
 - 回線vty 0 ~ 4を更新するには、次の設定コマンドを使用します (これは拡張ノードにとって非常に最初のステップになる可能性があります) 。

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

Cisco Catalyst Centerからのクレデンシャルの変更手順

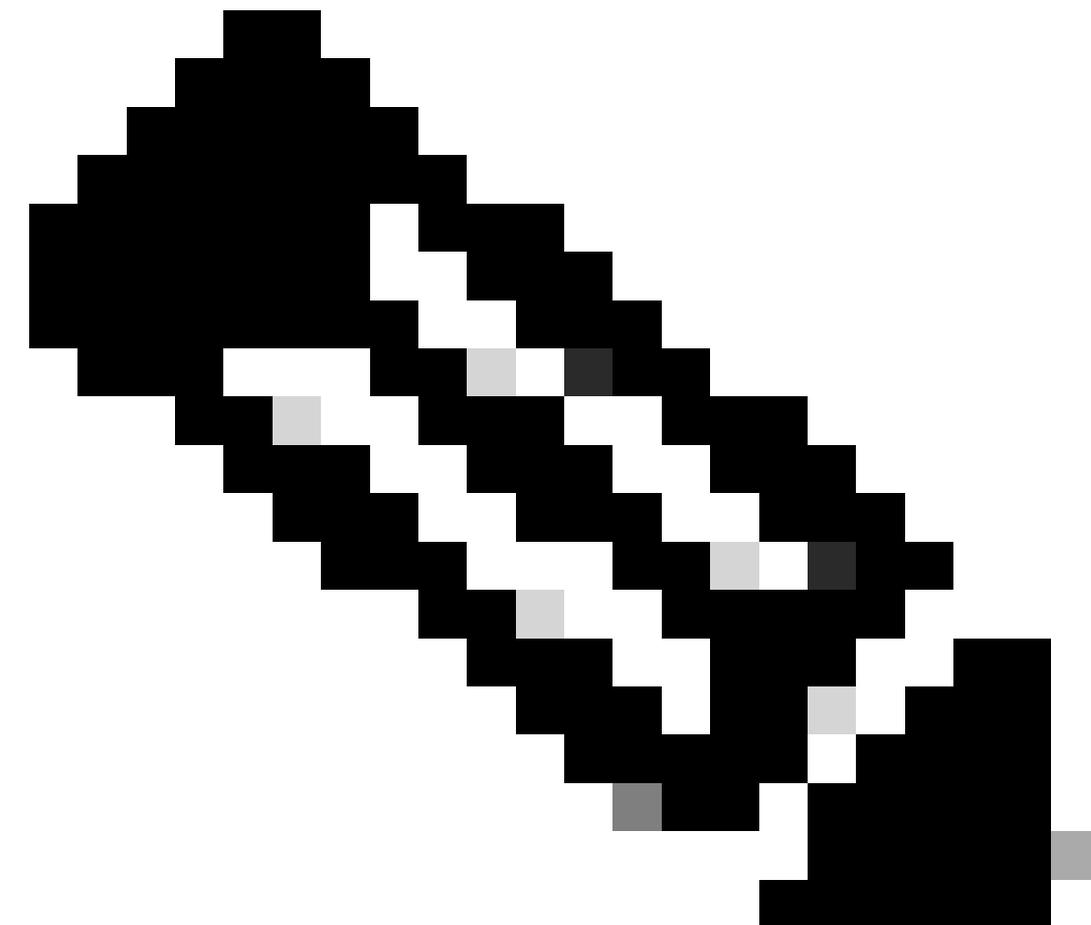
Cisco Catalyst CenterマネージドAAAを使用するサイト

ユーザのパスワード変更が必要 (イネーブルパスワードの変更なし)

1. まず、ISEでクレデンシャル (関連するユーザ名のパスワード) を更新します。これにより、インベントリ収集が失敗し、管理対象デバイスのインベントリ状態が到達不能、部分的な収集の失敗、または間違ったクレデンシャルに変わります。
2. Provision > Inventoryページで、1つ以上のデバイスを選択し、Actions > Inventory > Edit Device > Credentialsタブを選択します。次に、「デバイス固有の認証情報の追加」を新しいユーザ名またはパスワードで更新します (イネーブルパスワードは変更しないでください) 。この時点で、Cisco Catalyst Centerは更新されたクレデンシャルを使用してデバイスに

ログインでき、デバイスインベントリの状態は管理対象に戻ります。

- 外部AAAサーバに到達できないときにCisco Catalyst Centerがデバイスにログインできるように、デバイスのローカルクレデンシャルをフォールバックとして更新できます。ローカルクレデンシャルは、Cisco Catalyst Centerのテンプレートエディタ、カスタムPythonスクリプトを使用して更新するか、手動で更新することができます。
 - 最後の手順では、「グローバル認証情報」ページで同じ認証情報を更新します。これにより、LANオートメーションを使用して追加された新しく検出されたデバイスまたはデバイスは、Designページ> Network Settings > Device Credentials > CLI Credentials > ユーザ名の編集 > enable passwordを変更することなく、更新されたクレデンシャルを使用します。
-



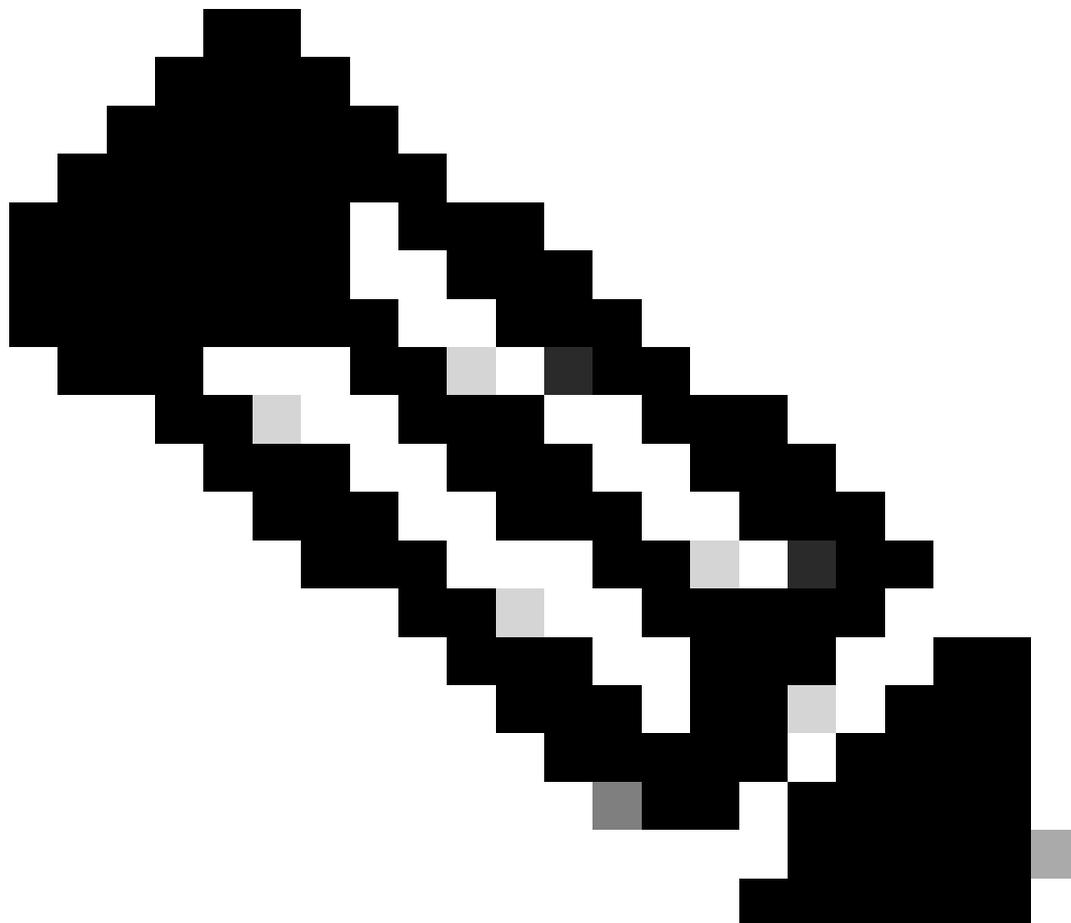
注:SSH/Telnetログインは、外部AAAサーバによって認証されます。ローカルデバイスのクレデンシャルは更新されません。

注：外部AAAサーバがCisco Catalyst Centerのサイトの設計ページで設定されている場合、Cisco Catalyst Centerでは、Global Credentialsページでクレデンシャルを変更する際に、管理対象デバイスやISEに対するアクションは実行されません。

ユーザのパスワードとイネーブルパスワードの変更が必要

1. まず、ISEでクレデンシャル（関連するユーザ名のパスワード）を更新します。これにより、インベントリ収集が失敗し、管理対象デバイスのインベントリ状態が到達不能、部分的な収集の失敗、または間違ったクレデンシャルに変わります。
2. Provision > Inventoryページで、1つ以上のデバイスを選択し、Actions > Inventory > Edit Device > Credentialsタブを選択します。次に、「デバイス固有の認証情報の追加」を新しいユーザ名とパスワード、またはイネーブルパスワードで更新します。この時点で、Cisco Catalyst Centerは更新されたクレデンシャルを使用してデバイスにログインでき、デバイスインベントリの状態は管理対象に戻ります。
3. 最後の手順では、「グローバル認証情報」ページで同じ認証情報を更新します。これにより、LANオートメーションを使用して追加された新しく検出されたデバイスまたはデバイス

は、Designページ> Network Settings > Device Credentials > CLI Credentials >ユーザ名の編集>ユーザのパスワードとイネーブルパスワードの更新から、更新されたクレデンシャルを使用します。



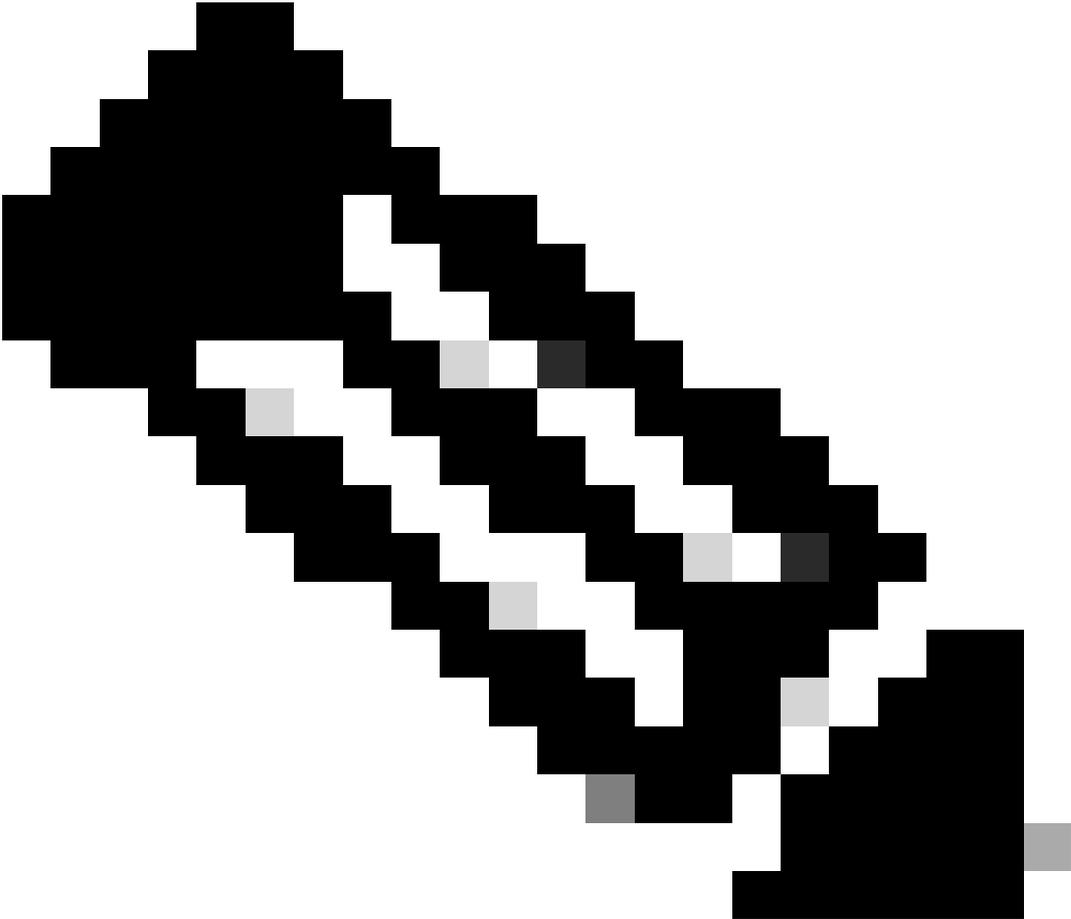
注：外部AAAサーバが到達可能である場合、ユーザ名とパスワードは外部AAAサーバによって認証され、イネーブルパスワードは管理対象デバイスによってローカルで認証されます。

注：外部AAAサーバがサイトのCisco Catalyst Centerの設計ページで設定されている場合、グローバルクレデンシャルページでクレデンシャルを変更しても、Cisco Catalyst CenterはデバイスまたはISEに対するアクションを実行しません。

Cisco Catalyst CenterアンマネージドAAAを使用するサイト

ユーザのパスワード変更が必要（イネーブルパスワードの変更なし）

1. Design > Network Settings > Device Credentials > CLI Credentials > edit the username > update the user's password without changing the enable passwordで、Global Credentialsページのクレデンシャルを更新します。
2. Global Credentialsページでクレデンシャルを変更すると、Cisco Catalyst CenterがAAAを管理していないサイトの管理対象デバイスを、更新されたクレデンシャルで再設定できます。Cisco Catalyst Centerは、一時的なEEMスクリプトをプッシュしてクレデンシャルを検証できます。ログインが成功した場合は、設定を保存できます。



注：Cisco Catalyst CenterがAAA設定を管理しないサイトにある管理対象デバイスについては、管理対象デバイスが外部AAAサーバを使用して手動で設定されているのか、管理対象デバイスがローカルのクレデンシャルのみを使用しているのかについてはCisco Catalyst Centerでは認識されないため、影響を受ける管理対象デバイスでパスワードが設定されている場合は、外部AAAサーバでパスワードが更新されてから、次の手順に進みます。

ユーザのパスワードとイネーブルパスワードの変更が必要

1. Design > Network Settings > Device Credentials > CLI Credentials > edit the username > update the user's passwordで、Global Credentialsページのクレデンシャルを更新します。
2. Global Credentialsページでクレデンシャルを変更すると、Cisco Catalyst CenterがAAAを管理していないサイトの管理対象デバイスを、更新されたクレデンシャルで再設定できます。Cisco Catalyst Centerは、一時的なEEMスクリプトをプッシュしてクレデンシャルを検証できます。ログインが成功した場合は、設定を保存できます。



注：Cisco Catalyst CenterがAAA設定を管理しないサイトにある管理対象デバイスについては、管理対象デバイスが外部AAAサーバを使用して手動で設定されているのか、管理対象デバイスがローカルのクレデンシャルのみを使用しているのかについてはCisco Catalyst Centerでは認識されないため、影響を受ける管理対象デバイスでパスワードが設定されている場合は、外部AAAサーバでパスワードが更新されてから、次の手順に進みます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。