デバイス クレデンシャルの管理

このセクションでは、次の点について説明します。

デバイス クレデンシャルの管理

Cisco Prime Collaboration Assurance を使用して管理するすべてのデバイスのデバイス クレデンシャルを設定する必要があります。デバイスを検出し、インベントリを更新するためにデバイス クレデンシャルが必要です。クレデンシャルがデバイスによって異なる場合は、別のクレデンシャル プロファイルを作成します。つまり、Cisco Prime Collaboration Assurance の 2 つの Cisco Unified Communications Manager を異なるクレデンシャルで管理する場合、2 つのクレデンシャル プロファイルを作成する必要があります。詳細については、[Credential Profiles] のフィールドの説明表を参照してください。

次は、クレデンシャル プロファイルを作成する際のいくつかの要件です。

- エンドポイントが Managed 状態になるまで、HTTP と SNMP にはクレデンシャルが必要です。
- **Cisco Prime Collaboration リリース 11.1 以前の場合**

  エンドポイントとネットワーク デバイスに関連するセッションをトラブルシュートするには、CLI クレデンシャルが必要です。
- **Cisco Prime Collaboration リリース 11.5 以降の場合**

  CLI クレデンシャルは、ビデオ テスト コールを管理し、SIP Call Flow Analyzer を介したコール シグナリングの分析に必要です。

- Unified CM の会議監視には、JTAPI クレデンシャルが必要です。このクレデンシャルは、エンドポイントでは必要ありません。
- Enterprise License Manager プロファイルを作成するには、Prime License Manager のデバイス タイプで Enterprise License Manager を選択します。
- Cisco Unified Intelligence Center（CUIC）、Cisco Voice Portal（CVP）、Cisco Finesse、Cisco SocialMiner、Cisco Unified Contact Center Enterprise（Unified CCE）、Cisco Unified Contact Center Express（Unified CCX）、Cisco MediaSense などの Unified Contact Center デバイスで、HTTP および SNMP のクレデンシャルを定義します。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  Cisco Unified Intelligence Center（CUIC）、Cisco Voice Portal（CVP）、Cisco Finesse、Cisco SocialMiner、Cisco Unified Contact Center Enterprise（Unified CCE）、Cisco Unified Contact Center Express（Unified CCX）、Cisco Virtualized Voice Browser などの Unified Contact Center デバイスで、HTTP および SNMP のクレデンシャルを定義します。
- Contact Center Enterprise の HTTP クレデンシャルを domain\administrator のフォーマットで入力します。たとえば、hcsdc2\administrator となります。
- *ServiceabilityAdministrationUserRole* 権限を持つ Cisco Unified Customer Voice Portal（CVP）の HTTP クレデンシャルを入力します。この権限は、デフォルトのユーザ名である *wsmadmin* に与えられています。
- クレデンシャルは、電話機、Cisco Cius、Cisco Jabber、TelePresence（Movi）エンドポイント用の Cisco Jabber Video には必要ありません。これらのエンドポイントは、登録されているコール プロセッサの検出を介して検出されます。
- [デバイス（Device）] タイプのドロップダウン リストから [VCS/EXPRESSWAY] を選択し、Cisco Expressway-Core、Cisco Expressway-Edge、Cisco Collaboration Edge または Core を備えた Cisco VCS のクレデンシャルを作成します。

（注）
- [クレデンシャル プロファイル（Credential Profile）] ページでクレデンシャル プロファイルを作成、または [デバイス検出（Device Discovery）] でデバイスを追加するときに、SNMP Community String、SNMPv3、HTTP、JTAPI、MSI の 8 文字のパスワードで * 記号を使用することはできません。
- [クレデンシャル プロファイル（Credential Profile）] ページでクレデンシャル プロファイルを作成、または [デバイス検出（Device Discovery）] でデバイスを追加するときに、CLI の 8 文字のパスワードで % 記号を使用することはできません。

デバイス クレデンシャル プロファイルの追加

クレデンシャル プロファイルを追加または複製するには、次の手順を実行します。

ステップ 1 **[Cisco Prime Collaboration Assurance]** ページ で、 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]** [ナビゲーションの切り替え（Toggle Navigation）] ペインから上記の順に選択します。

Cisco Prime Collaboration リリース 11.5 以降の場合

[Cisco Prime Collaboration Assurance] ページ で、 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]** [ナビゲーションの切り替え（Toggle Navigation）] ペインから上記の順に選択します。

[Inventory Management] ページが表示されます。

ステップ 2 [クレデンシャルプロファイル（Credentials Profile）] ページで [追加（Add）] をクリックし、[Credential Profiles] のフィールドの説明 （3 ページ）の表で説明している必要な情報を入力します。

ステップ 3 **[保存（Save）]** をクリックします。

ネットワーク内で、すべてのデバイスに同じ SNMP クレデンシャルを設定している場合があります。このような場合は、まずプロファイルを新規に作成した後で、既存のプロファイルを複製してください。複製するには、[Credentials Profile] ページで既存のプロファイルを選択して [Clone] をクリックし、必要な更新をした後で [Add/Update] をクリックします。

[Credential Profiles] のフィールドの説明

デバイスの検出後、現在のインベントリ テーブルを確認し、Cisco Prime Collaboration Assurance データベースでクレデンシャルが更新されているかどうか確認できます。

次の表で [Credential Profiles] ページのフィールドについて説明します。

表 *1 : [Credential Profiles]* のフィールドの説明

フィールド名	説明
プロファイル名	クレデンシャル プロファイルの名前です。 次に例を示します。 • CUCM • router_switches

フィールド名	説明
デバイスタイプ	（任意）選択したデバイス タイプに基づき、クレデンシャル フィールド（SNMP、HTTP、CLI など）が表示されます。 再検出時間を短縮するため、クレデンシャル プロファイルを作成するときにデバイス タイプを選択することを推奨します。 クレデンシャル プロファイルを作成する際にデバイス タイプを選択しない場合、デフォルトのデバイス タイプは [任意（Any）] 「」になります。 デバイスタイプのリストについては、cisco.com を参照してください。 EX シリーズ、MXシリーズ、SXシリーズ、ベア コーデック デバイス、およびコーデックが指定されたすべてのプロファイルについては、デバイス タイプとして [TC_CE] を選択します。 共存型の PLM を管理している間は、CLI および HTTP クレデンシャルの両方を提供する必要があります。 • CLI クレデンシャルは、ライセンス情報にアクセスするために使用します。 • HTTP クレデンシャルは、Cisco Prime Collaboration Assurance で Prime License Manager を管理するために使用します。

フィールド名	説明
デバイス タイプ	

フィールド名	説明
	Cisco Prime Collaboration リリース 12.1 以降の場合 共存型の PLM を管理している間は、CLI および HTTP クレデンシャルの両方を提供する必要があります。 • CLI クレデンシャルは、ライセンス情報にアクセスするために使用します。 • HTTP クレデンシャルは、Cisco Prime Collaboration Assurance で Prime License Manager を管理するために使用します。 ルータが Cisco Unified Border Element（CUBE）として識別されるには、次の条件を満たす必要があります。 1. デバイス タイプ（ルータ）の CLI クレデンシャル情報（CLI ログイン ユーザ名および CLI ログイン パスワード）は必須です。 2. ルータの ポート 22 では SSH バージョン 2 以降を有効にする必要があります。 3. ルータで [パスワードの有効化（Enable Password）]が設定されている場合は、[CLI パスワード有効化（CLI Enable Password）] フィールドにパスワードを入力します。 **Cisco Prime Collaboration リリース 11.6 以降の場合** CE イメージ搭載の EX シリーズ、MX シリーズ、SX シリーズ、DX シリーズ、ベアなコーデック デバイス、コーデック付きのすべてのプロファイルでは、デバイス タイプとして [コーデック（コーデック）] を選択します。 MSEデバイスの場合は、デバイスタイプとして [Cisco MCU] を選択します。 **Cisco Prime Collaboration リリース 11.5 以降の場合** Virtualized Voice Browser デバイスの場合は、[Virtualized Voice Browser] デバイス タイプを選択します。

フィールド名	説明
	任意のクレデンシャル（SNMP、HTTP、CLI、MSI）を入力して、「[任意（Any）]」のクレデンシャル プロファイルを作成できます。自動検出（Ping スイープと CDP 検出）を実行するには、[任意（Any）]「」のクレデンシャル プロファイルを作成する必要があります。ただし、論理検出も実行できます。 ネットワークに複数のサブネットがある場合は、サブネットごとに [任意（Any）]「」のプロファイルを作成します。
IP バージョン	IP アドレスはバージョン 4 またはバージョン 6 です。

フィールド名	説明
IP アドレス パターン	

フィールド名	説明
	クレデンシャルを指定するデバイスの IP アドレスです。次の作業が必要です。 • 複数の IP アドレスはパイプ文字（|）で区切ります。 • 0.0.0.0 および 255.255.255.255 は使用しないでください。 • 疑問符（?）は使用しないでください。 次のことを行うことを推奨します。 • Cisco Unified CM、Cisco TMS に IP アドレスを正確に入力します。 • CTS またはネットワーク デバイスのいずれかの IP アドレスを正確に入力します。 • アドレス パターンではワイルドカード式を多数使用しないでください。 次に例を示します。 • 100.5.10.*|100.5.11.*|100.5.20.*|100.5.21.* • 200.5.1*.*|200.5.2*.*|200.5.3*.* • 172.23.223.14 • 150.5.*.* 150.*.*.* や 192.78.22.1? などのパターンの使用は避けます。150.5.*.*/24. デバイスの共通パターンが見つからない場合は、*.*.*.* と入力します。 クレデンシャルプロファイルで IP アドレスのパターンを定義するときには、できるだけワイルドカード文字（*）の使用を避けます。 **Cisco Prime Collaboration リリース 11.5 以降の場合** **[インベントリ（Inventory）] > [インベントリ管理（Inventory management）] > [クレデンシャルの管理（Manage Credentials）]** ワイルドカード文字を使用すると、検出時間が長くなる可能性があります。 パターンの使用方法については、SNMPv2C を

フィールド名	説明
	参照してください。
一般的な SNMP オプション	[SNMP Timeout]：デフォルトは 10 秒です。
	[SNMP Retries]：デフォルトは 2 です。
	[SNMP Version]：SNMP バージョンを選択する必要があります。
SNMPv2C デバイスの検出と管理に使用されます。	SNMP Read Community String SNMPv2C または SNMPv3 のいずれかのクレデンシャルを指定できます。Cisco TelePresence システムとネットワーク デバイスには異なる SNMP クレデンシャルを使用することを推奨します。 Cisco Prime Collaboration Assurance は、IP アドレスのパターンに基づきクレデンシャル プロファイルを検索します。次に、Cisco Prime Collaboration Assurance は SNMP クレデンシャルに一致するプロファイルを選択します。一致する複数のプロファイル（つまり、同じ SNMP クレデンシャルを持つプロファイル）が存在することがあります。この場合、Cisco Prime Collaboration Assurance は最初に一致するプロファイルを選択します。 **Cisco Prime Collaboration リリース 11.1 以前の場合** （注） 複数のプロファイルで同じ SNMP クレデンシャルを使用し、CLI クレデンシャルが異なる場合、Cisco Prime Collaboration Assurance はデバイスで正しい SNMP クレデンシャルを選択しますが、間違った CLI クレデンシャルを選択する場合があります。この場合、トラブルシューティング ワークフローが機能しないことがあります。
	SNMP Write Community String

フィールド名	説明
SNMPv3 デバイスの検出と管理に使用されます。	[SNMP Security Name]：セキュリティ名を入力します。
	[SNMP Authentication Protocol]：MD5 または SHA を選択できます。
	[SNMP Authentication Passphrase]：パスフレーズを入力します。
	SNMP Privacy Protocol：AES、AES128、または DESMD5 を選択できます。 **Cisco Prime Collaboration リリース 11.5 以降の場合** SNMP Privacy Protocol：AES128 または DES を選択できます。

フィールド名	説明
CLI トラブルシューティングの目的でメディア パスを検出するために、CLI を介してデバイスにアクセスするために使用されます。	[CLI Login Username] と [Password] CLI クレデンシャルは、トラブルシューティング ワークフロー中に使用されます。クレデンシャルが入力されていない場合、または入力されたクレデンシャルが正しくない場合、トラブルシューティング ワークフローは機能しないことがあります。 **Cisco Prime Collaboration リリース 11.5 以降の場合** CLI クレデンシャルは、ビデオ テスト コールを管理し、SIP Call Flow Analyzer を介したコール シグナリングの分析に使用します。 **Cisco Prime Collaboration リリース 12.1 以降の場合** ルータが Cisco Unified Border Element（CUBE）として識別されるには、次の条件を満たす必要があります。 **1.** デバイス タイプ（ルータ）の CLI クレデンシャル情報（CLI ログイン ユーザ名および CLI ログイン パスワード）は必須です。 **2.** ルータの ポート 22 では SSH バージョン 2 以降を有効にする必要があります。 **3.** ルータで [パスワードの有効化（Enable Password）] が設定されている場合は、[CLI パスワード有効化（CLI Enable Password）] フィールドにパスワードを入力します。
HTTP システム ステータスと会議情報をポーリングするために HTTP を介してデバイスにアクセスするために使用されます。	[HTTP Username] と [Password] Cisco Prime Collaboration Assurance は、最初に HTTP用のアクセスを確認します。アクセス試行に失敗した場合、Cisco Prime Collaboration Assurance は HTTPS 用のアクセスをチェックします。 <domain/username> の形式で Cisco TMS にログインした場合、[HTTPS Username] フィールドに同じ <domain/username> 値を追加してください。

フィールド名	説明
JTAPI Cisco Unified CM からセッション ステータス情報を取得する際に使用します。	（オプション）JTAPIユーザ名とパスワード。 （注） パスワードにはセミコロン（;）または等号（=）を使用しないでください。

フィールド名	説明

フィールド名	説明
	Cisco Prime Collaboration リリース 11.5 以降の場合 Cisco Unified CM からセッション ステータス情報を取得する際に使用します。 **Cisco Prime Collaboration リリース 12.1 SP1 の場合** 安全な JTAPI（TLS v1.2）接続を確立するため、JTAPI 固有の新しいパラメータ セットが導入されました。 （注） 1. CTI、JTAPI、および TAPI アプリケーションを保護する方法の詳細や、Certificate Authority Proxy Function の詳細については、『Cisco Unified Communications Manager のセキュリティ ガイド』の「CTI、JTAPI、TAPI の認証と暗号化のセットアップ」および「Certificate Authority Proxy Function」の各章を参照してください。 2. CUCM が [Mixed} モードであることを確認します。 JTAPI 固有のパラメータ セットは、次のとおりです。 1. **[セキュア接続（Secure Connection）]** チェックボックス 1. **チェックボックスをオンにする**：このオプションをオンにすると、Cisco Unified Communications Manager へのセキュアな TLS 接続が有効になります。 「この JTAPI ユーザには、その他の必要なロールとともに、[Standard CTI Secure Connection] ロールが関連付けられていることを確認します」という警告メッセージが表示されます。[OK] をクリックして、Cisco Prime Collaboration Assurance に戻ります。

フィールド名	説明
	2. **チェックボックスをオフにする**：このチェックボックスをオフにすると、JTAPI はセキュアな接続を確立できません。 「この JTAPI ユーザに関連付けられた [Standard CTI Secure Connection] ロールが削除されていることを確認します」という警告メッセージが表示されます。[Monitor Conferences] へと続行するには、必要な役割が設定されていることを確認します。[OK] をクリックして、Cisco Prime Collaboration Assurance に戻ります。 詳細については、「Cisco Prime Collaboration Assurance 用のデバイスをセットアップ」を参照してください。 チェックボックスを使用すると、新しい Secure JTAPI フィールドにパラメータを入力できます（有効または無効）。

フィールド名	説明

フィールド名	説明
	２．**TFTP サーバ IP アドレス**：TFTP サーバの IP アドレスを指定します。 （注） この値は、CUCM クラスタのいずれかのノードである必要があります。そのノードで、TFTP サービスが実行されていることを確認します。 **3. TFTP サーバ ポート**：TFTP サーバ ポートのデフォルト値は 69 です。 （注） システム管理者に推奨されない限り、デフォルト値は変更しないようにします。 **4. CAPF サーバ IP アドレス**：CAPF サーバの IP アドレスを指定します。 （注） 1. 証明書の認証プロキシ機能の詳細については、『Cisco Unified Communications Manager 用のセキュリティ ガイド』の「証明書の認証プロキシ機能」の章を参照してください。 2. CUCM で CAPF プロファイルを作成するときは、**[キーの順序（Key Order）]** ドロップダウンリストから **[RSA のみ（RSA Only）]** を選択してください。 3. CUCM Publisher IP アドレスは、常に指定する必要があります。 **5. CAPF サーバ ポート**：CAPF サーバ ポート番号のデフォルト値は 3804 です。 （注） 入力した値が、Cisco Unified Communication Manager で設定された値と一致していることを確認します。 **7. パブリッシャ用のインスタンス ID**：このフィールドには、アプリケーションの CAPF 設定、または Cisco Unified Communication Manager クラスタのエンド ユーザ CAPF のプ

フィールド名	説明
	ロファイル設定ページで設定した、アプリケーション インスタンスの識別子を指定します。 **8. セキュア認証文字列**：アプリケーションの CAPF 設定セクション、または各 Communication Manager Publisher のエンドユーザ CAPF のプロファイル設定ページで設定した認証文字列を入力します。 （注） 「セキュアな JTAPI 接続のトラブルシューティング」セクションには、考えられるエラーに対するトラブルシューティングの詳細や、Conference Diagnostics が捉えることのできない CUCM for Secure JTAPI and Sessions のセットアップで推奨されるアクションが一覧表示されます。

Cisco Prime Collaboration リリース 11.5 以降の場合

[クレデンシャル プロファイル（Credential Profiles）] ページでは、次のデバイスの名前が変更されています。

- CISCO INTERACTION MANAGER から WEB/EMAIL INTERACTION MANAGER に名前変更
- CUIC から INTELLIGENCE CENTER に名前変更
- CTS から CTS/IX ENDPOINT に名前変更
- CISCO UNIFIED COMMUNICATIONS MANAGER から COMMUNICATIONS MANAGER に名前変更
- C_SERIES CODEC から TC/CE ENDPOINT に名前変更
- E20 から E20 ENDPOINT に名前変更
- ISDN から ISDN GATEWAY に名前変更
- MCU から MULTIPOINT CONTROLLER に名前変更
- MXP から MXP ENDPOINT に名前変更
- ROUTER から ROUTER/VOICEGATEWAY に名前変更
- TPS から TELEPRESENCE SERVER に名前変更
- TELEPRESENCE CONDUCTOR から TELEPRESENCE CONDUCTOR に名前変更

（注） Cisco デバイス、、Cisco Unified Communications Manager Express（Cisco Unified CME）、UC500 シリーズ デバイスでは、[クレデンシャル プロファイル（Credential Profiles）] ページにクレデンシャルを追加する必要はありません。

デバイス ディスカバリの SSL 証明書認証

Cisco Prime Collaboration リリース 11.1 以前の場合

Cisco Prime Collaboration Assurance では、デバイスが追加されると、HTTPS を使用して保護されたリソースにアクセスすることによって、クレデンシャル検証用の SSL 証明書が交換されます。SSL 証明書は交換中に Cisco Prime Collaboration Assurance の信頼ストアに保存されないため、その後のそのデバイスとの通信は失敗します。このデバイスにアクセスするには、SSL 証明書を手動で Cisco Prime Collaboration Assurance の信頼ストアにインポートすることをお勧めします。

Cisco Prime Collaboration Assurance では、HTTPS でのデバイスまたはアプリケーションとの通信中に SSL 証明書の信頼性を確認することができます。ただし、この場合でも証明書を認証せずにデバイスの検出を続行するため、これは必須ではありません。

デフォルトでは、Cisco Prime Collaboration Assurance は通信するデバイスまたはアプリケーションからの証明書を検証しません。

SSL 証明書認証を有効にするには:

ステップ 1 選択 **[システム管理（System Administration）]** > **[証明書管理（Certificate Management）]**。
[証明書の管理（Certificate Management）] ページが表示されます。

ステップ 2 [デバイス証明書の管理（Device Certificate Management）] タブで、[デバイス検出のための SSL 証明書認証を有効にする（Enable SSL certificate authentication for device discovery）] チェックボックスをオンにします。

ステップ 3 [Import Certificates] ボタンをクリックします。

ステップ 4 Cisco Prime Collaboration Assurance を再起動し、信頼マネージャ内の変更を有効にします。

```
cm/admin# application stop cpcm
cm/admin# show application status cpcm
cm/admin# application start cpcm
```

デバイス クレデンシャルの変更

Cisco Prime Collaboration Assurance アプリケーションで現在管理しているデバイス クレデンシャルを変更した場合は、Cisco Prime Collaboration Assurance データベースで、関連するクレデンシャル プロファイルを変更する必要があります。

ログイン情報に誤りがある場合、デバイスにアクセスできないという重大イベントが Cisco Prime Collaboration Assurance からトリガーされます**[モニタ（Monitor）] > [アラームおよびイベント（Alarms & Events）] > [イベント（Events）]**。

クレデンシャル プロファイルを編集するには：

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）] > [インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**

ステップ 2 [インベントリ管理（Inventory Management）] ページでデバイスを選択し、**[クレデンシャルの変更（Modify Credentials）]**をクリックし ます。

ステップ 3 [Credential Profiles] のフィールドの説明 （3 ページ） の表の説明に従って、クレデンシャルを更新します。

ステップ 4 **[再検出（Rediscover）]** をクリックします。

Cisco Prime Collaboration Assurance では、変更したクレデンシャルでデータベースが更新されるのに数分かかります。クレデンシャルの更新後に、情報イベントの Device is accessible from Collaboration Manager がトリガーされます。Cisco Prime Collaboration Assurance では、次のポーリング ジョブで更新されたクレデンシャルが使用されます。

デバイス クレデンシャルの確認

Cisco Prime Collaboration リリース 11.5 以降の場合

クレデンシャルの誤りが原因でデバイス検出が失敗した場合は、失敗したデバイスのクレデンシャルをテストしてそのデバイスを再検出できます。選択 **[Device Inventory（デバイスインベントリ）] > [インベントリ管理（Inventory Management）] > [検出ジョブ（Auto Jobs）]** を選択すると、検出されなかったデバイスが一覧表示されます。

（注） 検出ジョブの実行中にこの作業を実行しないでください。

デバイス クレデンシャルを確認するには、以下を実施します。

ステップ 1 **Cisco Prime Collaboration リリース 11.5 以降の場合**

移行方法 **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**。

[Inventory Management] ページが表示されます。

ステップ 2 [Credential Profiles] ページから、クレデンシャルのテストに使用するプロファイル名を選択し、[Verify] をクリックします。

ステップ 3 クレデンシャルをテストするために有効なデバイスの IP アドレスを入力します。検証できるのは一度に 1 つのデバイスだけです。*.*.*.* や 192.2.*.* などの式は入力できません。

ステップ 4 [Test] をクリックします。タスクが完了するまで、テスト ボタンの横に処理中アイコンが表示されます。テスト結果は、[Test Credential Result] ペインの下に表示されます。

検証に失敗した場合は、「クレデンシャル検証のエラー メッセージ」に記載される、可能性のある理由を確認してください。

（注） クラスタ内のすべてのノードがすべてのプロトコルを実行するとは限りません。たとえば、JTAPI がすべてのノードでは実行されないこともあります。その結果、クレデンシャル検証テストが一部のノードで不合格となることがあります。クレデンシャルの問題点を解消したら、デバイス クレデンシャルを再度検証し、そのデバイスの検出を実行します。デバイスが検出されたら、[現在のインベントリ（Current Inventory）] テーブル内の Cisco Prime Collaboration Assurance データベースでアクセス情報が更新されたかどうかを確認できます。

クレデンシャル検証のエラー メッセージ

クレデンシャル検証のエラー メッセージを次の表に示します。

表 *2:* クレデンシャル検証のエラー メッセージ

エラー メッセージ	条件	解決策
SNMPv2		
SNMP Request: Received no response from *IP Address*.	次のいずれかの原因により失敗。 • デバイスの応答が遅い。 • デバイスが到達不能である。 • クレデンシャル プロファイルに入力されたコミュニティ ストリングが正しくない	• デバイスの接続性を検証する。 • 正しいコミュニティ ストリングを指定してクレデンシャル プロファイルを更新する
SNMP timeout.	デバイスの応答が遅いか、またはデバイスが到達不能である。	• デバイスの接続性を検証する。 • クレデンシャル プロファイルで [SNMP Timeout] および [SNMP Retries] の値を大きくする。

エラー メッセージ	条件	解決策
Failed to fetch table due to: Request timed out.	デバイスの応答が遅いか、またはデバイスが到達不能である。	クレデンシャル プロファイルで [SNMP Timeout] および [SNMP Retries] の値を大きくする。
SNMPv3		
The configured SNMPv3 security level is not supported on the device.	設定された SNMPv3 セキュリティ レベルがデバイスでサポートされていない。	クレデンシャル プロファイルで、SNMPv3 セキュリティ レベルを、サポートされているセキュリティ レベルに変更する。
The SNMPv3 response was not received within the stipulated time.	デバイスの応答が遅いか、またはデバイスが到達不能である。	デバイスの接続性を検証する。
SNMPv3 Engine ID is wrong.	クレデンシャル プロファイルに入力されたエンジン ID が正しくない。	クレデンシャル プロファイルで、正しい SNMPv3 エンジン ID を入力する。
SNMPv3 message digest is wrong.	次のいずれかの原因により失敗。 • SNMPv3 認証アルゴリズムまたはデバイス パスワードが正しくない • ネットワーク エラー	• クレデンシャル プロファイルに正しい SNMPv3 認証アルゴリズムおよびデバイス パスワードが設定されていることを確認する • ネットワーク エラーがないかどうかを確認する
SNMPv3 message decryption error.	SNMPv3 メッセージを復号化できない。	クレデンシャル プロファイルに正しい SNMPv3 認証アルゴリズムが入力されていることを確認する。
Unknown SNMPv3 Context.	クレデンシャル プロファイルに設定されている SNMPv3 コンテキストがデバイスに存在しない。	クレデンシャル プロファイルに設定されている SNMPv3 コンテキストが正しいことを確認する。
Unknown SNMPv3 security name.	クレデンシャル プロファイルに設定された SNMPv3 ユーザ名が正しくない、またはデバイスで SNMPv3 ユーザ名が設定されていない。	クレデンシャル プロファイルおよびデバイスで正しい SNMPv3 ユーザ名が設定されていることを確認する。

エラー メッセージ	条件	解決策
CLI		
Login authentication failed.	クレデンシャル プロファイルに入力されたクレデンシャルが正しくない。	クレデンシャル プロファイルで、デバイスの CLI クレデンシャルを確認し再入力する。
Connection refused.	デバイス上で SSH サービスまたは Telnet サービスが実行されていない可能性がある。	1. サポートされている CLI（ポート）についてデバイスの接続性を検証する。 2. デバイス上で SSH サービスまたは Telnet サービスが実行されているかどうかを確認する
HTTP		
Server returned HTTP response code: 401 for URL.	HTTP サービスが実行されていない、または URL が無効である。	• デバイス上で HTTP サービスまたは HTTPS サービスが実行されているかどうかを確認する • サーバで URL が有効かどうかを確認する
Connection refused.	HTTP サービスまたは HTTPS サービスが実行されていない。	デバイス上で HTTP サービスまたは HTTPS サービスが実行されているかどうかを確認する
HTTP check failed.	クレデンシャル プロファイルに入力された HTTP クレデンシャルが正しくない。	クレデンシャル プロファイルで、デバイスの HTTP クレデンシャルを確認し再入力する。
Cisco Prime Collaboration リリース 11.1 以前の場合 MSI		
Failed to access MSI.	クレデンシャル プロファイルに入力された MSI クレデンシャルが正しくない。	デバイスの MSI クレデンシャルを確認し、クレデンシャル プロファイルに再入力する。

デバイス クレデンシャル プロファイルの削除

未使用のクレデンシャル プロファイルのみを削除できます。Cisco Prime Collaboration Assurance アプリケーションで管理されているデバイスのクレデンシャルプロファイルを削除しないことを推奨します。

クレデンシャル プロファイルを削除するには、次の手順を実行します。

ステップ 1 選択 **[デバイスインベントリ（Device Inventory）]** > **[インベントリ管理（Inventory Management）]**。

Cisco Prime Collaboration リリース 11.5 以降の場合

移行方法 **[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**

ステップ 2 [Inventory Management] ページで、[Manage Credentials] をクリックします。デフォルトでは、リスト上で最初に表示されるデバイスのクレデンシャルが表示されます。

ステップ 3 プロファイル名を選択し、[削除（Delete）] をクリックします。