CHAPTER 11

クレデンシャルの管理

Cisco Prime CM でデバイスを管理するために必要なデバイス クレデンシャルについては、『*Cisco Prime Collaboration Manager Quick Start Guide 1.1*』の「Setting Up the Network」の項を参照してください。

次のものについて、すべての必須クレデンシャルで別個のクレデンシャル プロファイルを作成することを推奨します。

- CTS-Manager
- Cisco TMS
- Cisco Unified CM
- Cisco VCS
- CTMS
- Cisco TS
- MCU および MSE
- CTS
- Cisco TelePresence EX シリーズ、Cisco Telepresence System Integrator C シリーズ、および Cisco TelePresence System Quick Set C シリーズ
- ルータ
- スイッチ

クレデンシャルがデバイスによって異なる場合は、別個のクレデンシャル プロファイルを作成してください。つまり、Cisco Prime CM で別のクレデンシャルを使用して 2 つの Cisco Unified CM を管理する場合は、2 つの別個のクレデンシャル プロファイルを作成します。

デバイス クレデンシャル プロファイルの追加およびコピー

ネットワーク内の各デバイスに対して、設定されている SNMP クレデンシャルはすべて同じであっても、CLI クレデンシャルはそれぞれ異なることがあります。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。

新しいクレデンシャル プロファイルを追加する手順は次のとおりです。

ステップ 1 [Inventory] > [Device Inventory] を選択します。

[Inventory] ページが表示されます。

ステップ 2 [Manage Credentials] をクリックします。

[Credentials Profiles] ウィンドウが表示されます。デフォルトでは、リストに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　[Add] をクリックして、新しいプロファイルを作成し、次の詳細情報を入力します。

フィールド名	説明	例
Profile Name	クレデンシャル プロファイルの名前。	• CTS_MAN • CUCM • router_switches
Device Type	デバイス クレデンシャルを管理するデバイスのタイプ。 選択したデバイス タイプに基づいて、クレデンシャルのフィールド（SNMP.CLI など）が表示されます。 デバイス タイプの値は、インスール後初めて検出を実行する場合には使用されません。それ以降の検出の際にはこの値が使用されます。それにより、再検出の所要時間が短縮されます。 再検出の所要時間を短縮するためにも、クレデンシャルを作成する際には適切なデバイス タイプを選択することを推奨します。 MSE および Cisco Ex シリーズのデバイスに対しては、デバイス タイプとしてそれぞれ MCU および C_Codec を選択します。	
Pattern	クレデンシャルを指定するデバイスの IP アドレス。You must • 有効な IPv4 アドレスだけを入力します。 • 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。 • CTS-Manager、Cisco Unified CM、および CTMS の 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。 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。 パターンの使用方法を理解するには、「[SNMPv2C]」（P.11-3）を参照してください。	• 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? などのパターンは使用しないでください。

ステップ 4　デバイスに接続するための次の詳細を入力します。

フィールド名		デフォルト値 / 追加情報
General SNMP Options	SNMP Timeout	SNMP タイムアウトはデフォルトで 10 秒に設定されます。
	SNMP Retries	再試行値はデフォルトでは 2 です。
	SNMP Version	—
[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 SMNP クレデンシャルを使用することを推奨します。 Cisco Prime CM は、IP アドレス パターンに基づいてクレデンシャル プロファイルを検索します。その後、Cisco Prime CM は、SNMP クレデンシャルが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。そのような場合は、Cisco Prime CM は、最初に一致するプロファイルを選択します。 **（注）**　場合によっては、SNMP クレデンシャルが同じでも、CLI クレデンシャルが異なる複数のプロファイルが存在することがあります。これによって、Cisco Prime CM は、正しい SNMP クレデンシャルを含んでいても、デバイスの CLI クレデンシャルが正しくないプロファイルを選択します。この場合、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。
	SNMP Write Community String	—
SNMPv3 デバイスの検出と管理に使用されます。	SNMP Security Name	—
	SNMP Authentication Protocol	MD5 と SHA のいずれかを選択できます。
	SNMP Authentication Passphrase	—
	SNMP Privacy Protocol	—
	SNMP Privacy Passphrase	—
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 and 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。

フィールド名		デフォルト値 / 追加情報
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 and Password	Cisco Prime CM では最初に HTTP アクセスのチェックが行われます。アクセスの試行に失敗すると、Cisco Prime CM では HTTPS アクセスのチェックが行われます。
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。	[JTAPI Username] と [JTAPI Password]	—

ステップ 5　[Add/Update] をクリックします。

[Credentials Profiles] ページが、新しいプロファイル詳細で更新されます。

既存のプロファイルをコピーする場合は、[Credentials Profiles] ウィンドウでいずれかのプロファイルを選択し、[Clone] をクリックします。プロファイルの新しい名前を入力すると、いずれかの既存フィールドを更新することができます。プロファイルを保存する場合は、[Add/Update] をクリックする必要があります。

デバイス クレデンシャルの更新

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

クレデンシャルが正しくない場合は、主要イベントである `Device is not accessible from Collaboration Manager` がトリガーされます（[Monitoring] > [Events]）。

クレデンシャル プロファイルを更新するには、次のようにします。

ステップ 1　[Inventory] > [Device Inventory] を選択します。

[Inventory] ページが表示されます。

ステップ 2　[Manage Credentials] をクリックします。

[Credentials Profiles] ウィンドウが表示されます。

ステップ 3　プロファイル名を選択します。

前に入力したクレデンシャル詳細が表示されます。

ステップ 4　クレデンシャルを更新して、[Add/Update] をクリックします。

Cisco Prime CM では、更新したクレデンシャルでデータベースを更新す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 `Device is accessible from Collaboration Manager` がトリガーされます（[Monitoring] > [Events]）。Cisco Prime CM は、次のポーリング ジョブで更新されたクレデンシャルを使用します。

クレデンシャルの検証

デバイス クレデンシャルが正しく入力されていないと、そのデバイスは検出されません。検出の実行後、Cisco Prime CM では、検出されなかったデバイスが、ジョブ結果としてリスト表示されます（[Inventory] > [Device Inventory] > [List Discovery Jobs]）。クレデンシャルが正しくないために検出されなかったデバイスについては、そのクレデンシャルを検証したうえで再度検出を実行することができます。

（注） 検出ジョブの実行中はクレデンシャルの検証を行わないでください。[Inventory] > [Device Inventory] > [List Discovery Jobs] を使用すると、検出のステータスをチェックできます。

デバイス クレデンシャルを検証する手順は次のとおりです。

ステップ 1　[Inventory] > [Device Inventory] を選択します。

[Inventory] ページが表示されます。

ステップ 2　[Manage Credentials] をクリックします。

[Credentials Profiles] ウィンドウが表示されます。

ステップ 3　クレデンシャルの検証時に使用するプロファイル名を選択します。

前に入力したクレデンシャル詳細が表示されます。

ステップ 4　[Verify] をクリックします。

ステップ 5　クレデンシャルを検証するデバイスの IP アドレスを入力します。一度に検証できるデバイスは 1 つだけです。

..*.* や 192.2.*.* などの表記は使用できません。有効な IP アドレスを入力する必要があります。

ステップ 6　[Test] をクリックします。

[Test Credential Result] ペインに検証結果が表示されます。

検証は、以下のような原因により失敗する場合があります。

表 11-1　クレデンシャルに関するエラー メッセージ

エラー メッセージ		状況	対処方法
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 または • 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し、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。
	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。

表 11-1　クレデンシャルに関するエラー メッセージ（続き）

エラー メッセージ		状況	対処方法
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 を再入力する。
	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。
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。	• 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 および • 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

表 11-1　クレデンシャルに関するエラー メッセージ（続き）

エラー メッセージ		状況	対処方法
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。
JTAPI	Failed to access JTAPI.	クレデンシャル プロファイルに入力された JTAPI 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 JTAPI クレデンシャルを確認し再入力する。

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。デバイスの検出に関する詳細については、「デバイスの追加」（P.12-7）を参照してください。

デバイスが検出されたら、Cisco Prime CM データベースのアクセス情報が更新されたかどうかを、[Current Inventory] テーブル（「アクセス情報」（P.13-3）を参照）で確認することができます。

デバイス クレデンシャルの削除

Cisco Prime CM アプリケーションで管理されているデバイスのプロファイルは削除できません。未使用のプロファイルだけを削除できます。プロファイルが使用されているかどうかを確認する場合は、[Inventory] ページに移動して、デバイスを選択します。デバイスのプロファイル詳細は、[Access Information] ペインに表示されます。

クレデンシャル プロファイルを更新するには、次のようにします。

ステップ 1　[Inventory] > [Device Inventory] を選択します。

[Inventory] ページが表示されます。

ステップ 2　[Manage Credentials] をクリックします。

[Credentials Profiles] ウィンドウが表示されます。デフォルトでは、リストに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ます。

前に入力したクレデンシャル詳細が表示されます。

ステップ 4　[Delete] をクリックします。