CHAPTER 11

クレデンシャルの管理

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 1.2 Quick Start Guide*』の「Setting Up the Network」の項を参照してください。

次のデバイスについて、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。

エンドポイント	
Cisco IP Phone（89xx、99xx）	Cisco IP Video Phone E20
Cisco Cius	Cisco Codec EX60 および EX90 Cisco Codec C20、C40、C60、および C90
Cisco TelePresence System 500 Cisco TelePresence System 1100 Cisco TelePresence System 1300 Cisco TelePresence System 1400 Cisco TelePresence System 3000 Cisco TelePresence System 3010 Cisco TelePresence System 3200 Cisco TelePresence System 3210	Cisco TelePresence System 1000 MXP Cisco TelePresence 1700 MXP Cisco TelePresence 1500 MXP Cisco TelePresence 150 MXP Cisco TelePresence 3000 MXP Codec Cisco TelePresence 6000 MXP Codec
Cisco TelePresence TX9000 シリーズ	Cisco Telepresence MX 200、MX 300
Cisco TelePresence Integrator および Quick Set C シリーズ	Cisco TelePresence Movi
Cisco Profile 42 C20 および C60 Cisco Profile 52 および Cisco Profile 52 デュアル（C40 と C60） Cisco Profile 65 および Cisco Profile 65 デュアル（C60 と C90）	Polycom VSX Polycom HDX 4000 Polycom HDX 7000 Polycom HDX 8000 Polycom HDX 9000
Cisco TelePresence SX20 クイック セット	—
インフラストラクチャ デバイス	
サードパーティ デバイス	Cisco TelePresence Multipoint Switch
Cisco TelePresence Supervisor MSE 8050	Cisco ルータ

Cisco TelePresence MCU 4500 シリーズ Cisco MCU MSE 8510	Cisco スイッチ
Cisco TelePresence Management Suite（Cisco TMS）	Cisco Telepresence Conductor
CTS-Manager	Cisco Telepresence Server 7010 Cisco Telepresence Server MSE 8710
Cisco Unified CM	Cisco TelePresence Video Communication Server（Control と Expressway）
不明	無線（アクセス ポイント）

（注） Prime CM は、管理性が MIB-II サポートによって異なるサードパーティ デバイスをサポートします。

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、Prime CM で別のクレデンシャルを使用して 2 つの Cisco Unified CMs 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する必要があります。

トラブルシューティング ワークフローを開始するには、CLI クレデンシャルは必須です。トラブルシューティング ワークフローを開始する前に、すべてのエンドポイントとネットワーク デバイスについて CLI クレデンシャルを入力する必要があります。CLI クレデンシャルを入力しなかった場合、クレデンシャルを入力してデバイスを検出します。

（注） Cisco Unified IP Phone 8900 および 9900 シリーズ、Cisco Cius、および Cisco TelePresence Movi の各エンドポイントにはクレデンシャルは必要ありません。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 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。	
IP Address Pattern	クレデンシャルを指定するデバイスの IP アドレス。次の作業が必要です。 • 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.11-6）を参照してください。 **（注）** Prime CM は IPv4 が設定されたエンドポイントのみをサポートします。IPv6 が設定されたエンドポイントはサポートしません。また、Prime CM はデュアル スタック（IPv4 と IPv6 が設定された）エンドポイントはサポートしません。	• 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。 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、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、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、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] と [CLI Login 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] と [HTTP Password]	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、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] **（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。	—

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

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、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。

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]）。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、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。 **（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。

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、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.14-3）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

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 プロファイルを削除するには、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。

クラスタの管理

Prime CM は、CTS-Manager および Cisco TMS のクラスタまたは複数のサーバを管理して、CTS-Manager または Cisco TMS 設定にフェールオーバーがある場合にセッションの継続的なモニタリングを行えます。プライマリ設定とセカンダリ設定がサーバに対してセットアップされるため、あるインスタンスがダウンすると、別のインスタンスが選択されます。

プライマリ、セカンダリ、ホット スタンバイ、およびロード バランサーの各設定は手動で設定する必要があります。Prime CM は複数の CTS-Manager または Cisco TMS を管理しますが、セッションのインポートは [Manage Clusters] ページの設定ごとにプライマリ CTS-Manager または Cisco TMS からのみ行われます。

Prime CM はアプリケーション サーバのみをモニタします。データベース インスタンスはモニタしません。クラスタ内のすべての CTS-Manager または Cisco TMS アプリケーション サーバに対して健全性ポーリングが実行されます。

クラスタを管理するには、次のようにします。

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

[Device Inventory] ページが表示されます。

ステップ 2　[Manage Clusters] をクリックします。

[Manage Clusters] ウィンドウが表示されます。

ステップ 3　[Cluster Name] に入力し、ドロップダウン メニューからクラスタ タイプを選択します。

ステップ 4　プライマリ、セカンダリ、ホット スタンバイ、およびロード バランサーの各サーバの IP アドレスを入力します。

プライマリ サーバの IP アドレスは必須です。

ステップ 5　[Add] をクリックします。

新しいクラスタが追加されます。

既存のクラスタ設定を変更する必要がある場合は、[Update] をクリックします。

クラスタ設定をリセットするには、[Manage Clusters] ページの上部にある [Add] をクリックします。