



Cisco TelePresence 管理スイートプロビジョニング 拡張機能

導入ガイド

Cisco TMSPE 1.1
Cisco TMS 14.2
Cisco VCS X7.2

D14941 11

改訂：2013 年 9 月

【注意】 シスコ製品をご使用になる前に、安全上の注意 (www.cisco.com/jp/go/safety_warning/) をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

内容

概要	5
この導入ガイドについて	5
リリース ノート	5
前提条件と推奨事項	6
Cisco TMS およびサーバの要件	6
ハードウェア推奨事項	6
Cisco VCS の要件	7
SMTP サーバ要件	7
必要なセキュリティ権限	7
インストール	7
操作	7
MS SQL Server でのデータベースの手動作成	8
インストール中に必要な情報	8
Cisco TMS のユーザ名およびパスワード	8
データベース情報	8
データベースの場所	8
WebEx Enabled TelePresence 要件	9
ブラウザ要件	9
管理インターフェイス	9
ユーザ ポータル	9
導入のベスト プラクティス	9
エンドポイントの最新のソフトウェアへのアップグレード	9
AD/LDAP を使用したユーザ作成と管理の自動化	10
セキュア通信の使用	10
時刻の同期 : Cisco VCS と Cisco TMS	10
プロビジョニング用の Cisco VCS の設定	11
ネットワーク内でのプロビジョニング	11
Cisco VCS に対する DNS の設定	11
デバイス プロビジョニング オプション キーのインストール	12
SIP のイネーブル化	12
Cisco VCS による不明 IP アドレスへのコールの処理方法の設定	13
Cisco TMS への Cisco VCS の追加	13
Cisco VCS でのプロビジョニングのイネーブル化	15
クラスタ名を設定する方法	15
Cisco VCS でのプレゼンスのイネーブル化	15
VCS Control でのプレゼンス	15
Cisco VCS Expressway でのプレゼンス	16
デバイス認証の確認	17
Cisco TMSPE のインストール	18
冗長 Cisco TMS 設定での Cisco TMSPE のインストール	18
以前のバージョンからのアップグレード	18
新規インストールの実行	18
Cisco TMSPE のイネーブル化	19
Cisco TMS と Cisco VCS 間の通信の設定	20
プロビジョニングのための Cisco TMSPE の設定	22
グループの作成とユーザの追加	22
グループの設定	22
外部ディレクトリからのユーザのインポート	22
ユーザの手動追加	26
アドレス パターンの作成	26
アドレス パターン タイプ	26
パターンの追加	27

パターン例	28
プロビジョニングされたデバイスの設定を構成する方法	29
テンプレート スキーマの取得	29
スキーマのアップロード、アップロード先 : Cisco TMS	29
構成テンプレートの追加	30
グループへの構成テンプレートの割り当て	33
プロビジョニング電話帳	34
プロビジョニング電話帳ソースの作成および設定	34
グループへの電話帳の関連付け	35
アカウント情報の設定および送信	36
電子メールの設定	36
単一のユーザへの情報の送信	38
グループ内のすべてのユーザへのアカウント情報の送信	38
Smart Scheduler の導入	40
ベスト プラクティスと制限事項	40
予約の制限	41
Smart Scheduler へのユーザ アクセス	41
アクセス権と権限	41
タイム ゾーンを表示	42
WebEx の予約	42
Smart Scheduler の機能	42
FindMe の導入	43
FindMe の基礎	43
プロビジョニングを行わない FindMe の導入	43
発信者 ID パターンの定義	43
発信者 ID のインポートされたアカウントへの割り当て	43
FindMe のイネーブル化、対象 : Cisco TMSPE	45
手動で FindMe のアカウントとグループを追加する	45
FindMe ロケーションおよびデバイスの設定	46
推奨される最小設定	46
FindMe デバイス テンプレートの追加	47
FindMe ロケーション テンプレートの追加	48
デバイス テンプレートとロケーション テンプレートの関連付け	49
ロケーション テンプレートのグループへの割り当て	50
Cisco VCS の設定、対象 : FindMe	51
FindMe オプション キーのチェック	51
クラスタ名のセットアップ	52
FindMe 設定の有効化と設定	52
ISDN ゲートウェイを使用したコールの送信および返信	52
FindMe を使用した E.164 番号の FindMe ID への変換	53
ENUM を使用した E.164 番号の FindMe ID への変換	53
発信者 ID に ISDN ゲートウェイ プレフィックスを含める方法	53
FindMe ロケーションおよびデバイスの再作成	54
アカウントとグループ	54
ロケーション テンプレート	55
デバイス テンプレート	55
ユーザの FindMe ロケーションおよびデバイスの変更	55
その他の情報	56
FindMe ID で発信者 ID を上書きする方法の決定	56
Cisco VCS クラスタ内の FindMe	56
FindMe アカウント (ネットワーク内の別の Cisco VCS でホスト)	57
FindMe とプレゼンス	57
FindMe の個人タイプとグループ タイプ	57
SIP URI で許可される文字	57
FindMe の制限事項	58
FindMe デバイスとしての Microsoft Lync デバイス ID	58
Active Directory (AD) からの電話番号	58

ユーザとデバイスのメンテナンス	59
ユーザ データの同期化	59
LDAP および AD フィールドのマッピング	59
手動同期のテスト	59
手動同期の実行	60
ユーザおよびグループの移動	60
外部ソースからインポートされたユーザ アカウントの移動	60
クラスタ間でのグループの移動	60
ユーザ アカウントの検索	61
グループおよびユーザ アカウントの名前変更	61
プロビジョニングされたデバイスのソフトウェア アップグレード	62
構成のアップグレード	62
デバイスのアップグレード	62
Cisco TMS 接続詳細のアップデート	63
データベースの管理	64
データベースのバックアップ	64
バックアップからのデータベースの復元	64
データベースの移動	64
トラブルシューティング	65
Cisco TMSPE 診断の実行	65
ヘルス チェックの実行	65
システム ステータスの表示	66
Cisco VCS の通信履歴の表示	66
TMS プロビジョニング拡張機能 Windows サービスの再起動	66
プロビジョニング ログ	66
Cisco TMSPE および Cisco TMS ログ	66
Cisco VCS ログ	67
エンドポイント ログ	67
インストールに関するトラブルシューティング	67
インストール ログのチェック	67
「Java ランタイム中に SQL 接続を確立できませんでした... (Unable to establish SQL connection through Java runtime...)」	67
要求されたターゲットに有効な認証パスを見つけることができない	67
プロビジョニング問題のシナリオ	68
データベース接続が失敗する	68
Kerberos での AD のインポートが失敗する	68
電子メール送信の障害	69
Cisco VCS でデータ インポートの失敗がレポートされる	69
ユーザが「ライセンスが切れています (Out of licenses)」というメッセージを受信する	70
使用可能なテンプレートがない場合、サインインが失敗する	70
構成スキーマをアップロードしたときに表示される警告	71
電話帳を受信できない	71
Smart Scheduler と FindMe のトラブルシューティング	71
FindMe または Smart Scheduler にアクセスできない	71
Cisco TMSPE のアンインストール	72
Cisco VCS からのプロビジョニングの削除	72
マニュアルの変更履歴	73
資料のインベントリ	74
	75

概要

Cisco TMS プロビジョニング拡張機能(Cisco TMSPE) は、Cisco TelePresence Management Suite(Cisco TMS) と Cisco TelePresence Video Communication Server(Cisco VCS) のプロビジョニング アプリケーションです。

Cisco TMSPE を使用することで、ビデオ会議ネットワーク管理者は、大容量展開可能なビデオ会議ソリューションを作成および管理できるようになります。これは、次の機能を使用して実行されます。

- Active Directory のような外部ディレクトリから多数のユーザ アカウントをインポートし、その後スケジュールまたはオンデマンドで同期を行う。
- ユーザをグループ階層に振り分けて、使用可能な帯域幅、使用可能なエンドポイント デバイスのタイプ、または電話帳へのアクセス権などの設定要件の違いを許可する。
- グループ内のすべてのユーザに適用されるアドレス パターンおよび設定テンプレートの指定。
- プロビジョニングされた設定と電話帳を Cisco TelePresence Video Communication Server 経由でユーザに配布する。
- Cisco TMS サーバにエンド ユーザ FindMe ポータルが常駐した状態で FindMe™ を導入し AD ログインを使用してアクセス。この機能は、誰かが ID を呼び出すときにユーザがどのビデオおよびオーディオ デバイスが鳴るべきかを指定することができる。

この導入ガイドについて

このガイドは、Cisco TMSPE と Cisco TMS バージョン 14.1 の導入とメンテナンスについて説明します。

Cisco TMS の以前のバージョンのユーザは、このバージョンの導入ガイドを参照する必要があります。

このマニュアルでは、Cisco TMS サーバに Cisco TMSPE をインストールするためのベスト プラクティスと手順を提供します。

また、このマニュアルには、Cisco TMSPE 管理者のための一般的なメンテナンス作業、およびトラブルシューティングの項も含まれています。

プロビジョニングは、Cisco TMS および Cisco VCS の既存の機能を基盤に構築されているため、このマニュアルは、両方の製品についての知識があることを前提として書かれています。技術的に訓練を受けたユーザだけが、このマニュアルに記載された手順を実行することを推奨します。

リリースノート

初期インストールまたはアップグレードの詳細について、Cisco TMSPE、Cisco TMS、および Cisco VCS ソフトウェアのソフトウェア リリース ノートを読むことを推奨します。

前提条件と推奨事項

この項では、Cisco TMS および Cisco VCS とあわせて Cisco TMSPE をインストールして導入する場合の前提条件およびベスト プラクティスについて説明します。

Cisco TMS およびサーバの要件

Cisco TMSPE は、Cisco TMS と同じサーバにインストールする必要があります。

製品	バージョンと説明
Cisco TMS	<ul style="list-style-type: none"> バージョン 14.2。Cisco TMS の以前のバージョンのユーザは、このバージョンの導入ガイドを参照する必要があります。 次のハードウェアの推奨事項を参照してください。 すべての Cisco TMS の要件については、『Cisco TelePresence Management Suite Installation Guide』を参照してください。Cisco TMS トライアル バージョンでは、この拡張機能はアクティブ化できないため、注意してください。
SQL Server 接続	<ul style="list-style-type: none"> TCP/IP または名前付きパイプ プロトコルをイネーブルにする必要があります。TCP/IP は優先プロトコルです。次を参照してください。 SQL Server ブラウザが実行され、UDP ポート 1434 をリッスンできる必要があります。
Windows Server	<ul style="list-style-type: none"> Windows Updates が有効になっている必要があります。 SQL データベース接続に名前付きパイプ プロトコルを使用する場合、Windows Server には次のセキュリティ アップデートおよびホットフィックスが必要です。 <ul style="list-style-type: none"> Windows Server 2003 : http://support.microsoft.com/kb/958687 Windows Server 2008 R2 : http://support.microsoft.com/kb/2194664 および http://support.microsoft.com/kb/2194664 <p>デフォルトの接続プロトコルは、TCP/IP であることに注意してください。このプロトコルを使用すると、ホットフィックスは必要ではありません。</p>
Cisco TMS プロビジョニング拡張機能オプション キー	<ul style="list-style-type: none"> [Administrative Tools] > [General Settings] の下の [Licenses and Option Keys] ページで、Cisco TMS に追加されている必要があります。 ライセンスの消費状況は、利用状況、つまり同時にサインインしており、プロビジョニングされているデバイスの数に基づいています。同時に複数のデバイスにサインインしているユーザは、デバイスごとに 1 つのライセンスを消費します。
Java	<p>Cisco TMSPE は、Java 7 でテストされています(アップデート 40 と 17、32 ビットと 64 ビット バージョン)。</p> <p>(Windows Server 2003 の場合、32 ビット Java だけがサポートされています)。</p> <p>www.java.com からインストーラをダウンロードします。</p> <p>注意 : Cisco TMSPE の実行中に Java をアップグレードしないでください。アップグレード前に Windows サービスをディセーブルにします。サーバの自動 Java アップデートをディセーブルにすることを強く推奨します。</p>

ハードウェア推奨事項

最適なパフォーマンスを得るには、導入環境およびユーザ ベースのサイズに応じて、次のハードウェア仕様を推奨します。

- 小規模導入 : 4 GB RAM、2 GHz のデュアルコア プロセッサ
- 中規模導入 : 4 GB RAM、2 GHz クアッドコア プロセッサ
- 大規模導入 : 8 GB RAM、2 GHz クアッドコア プロセッサ

Cisco TelePresence Management Server

Cisco TMSPE は、現在製造中止された Cisco TelePresence Management Server にもインストールできます。ただし、システム リソースは 2 GB RAM に制限されており、パフォーマンスは低下するため、注意してください。サーバは小規模導入の場合のみ使用し、最終的には、より多くのリソースが使用できるハードウェアに移行することを推奨します。

複数のネットワークカードのサポートなし

Cisco TMS サーバでは、複数のネットワーク カードはサポートされていません。Cisco TMS のように、Cisco TMSPE はサーバ上で複数のネットワーク カードを使用できず、最初に使用可能なインターフェイスにバインドするのみです。

Cisco VCS の要件

Cisco VCS Control は、バージョン X7.2 以降でなければなりません。次のために、オプション キーが追加されている必要があります。

- Cisco VCS デバイス プロビジョニング。
- FindMe(該当する場合)。

SMTP サーバ要件

Cisco TMSPE からユーザにアカウント情報を送信するために、Cisco TMS サーバからの SMTP リレーを受け入れる有効な SMTP サーバが必要です。SMTP サーバが認証を必要とする場合、この情報が構成時に使用できることを確認します。

必要なセキュリティ権限

インストール

Cisco TMSPE のインストールには、次のセキュリティ権限が必要です。

アプリケーション	ユーザ権限
Cisco TMS Windows サーバ	管理者
MS SQL	<ul style="list-style-type: none"> ■ <i>sysadmin</i>: インストーラが MS SQL Server にデータベースを作成する場合 ■ <i>db_owner</i>: MS SQL Server 上の手動で作成されたデータベースを使用する場合。詳細については、「MS SQL Server でのデータベースの手動作成 [p. 8]」を参照してください。

操作

Cisco TMSPE の操作には、次のセキュリティ権限が必要です。

アプリケーション	ユーザ権限
Cisco TMS SQL サーバ インスタンス	<i>db_owner</i>
Cisco TMS	Cisco TMS のサイト管理者グループのメンバです。この目的のサービス アカウントは、ローカルまたは Active Directory に作成することを推奨します。冗長展開の場合、AD アカウントを使用します。

MS SQL Server でのデータベースの手動作成

Cisco TMS `tmsng` データベースが外部 SQL サーバ上にある場合は、データベース管理者は、インストール前に次の作業を行う必要があります。

- `tmsng` と同じインスタンスで、空のデータベース `tmspe` を作成します。
- 照合 `Latin1_General_CI_AS` を適用します。
- Cisco TMSPE のインストール中に使用するために、`db_owner` ロールのユーザを作成します。同じユーザを、操作でも使用できます。

インストール中に必要な情報

Cisco TMS のユーザ名およびパスワード

Cisco TMSPE インストーラでは、Cisco TMS のサイト管理者グループに属するサービス ユーザのユーザ名とパスワードの入力を求められます。

これらのクレデンシャルは、

- インストール後に [Administrative Tools] > [Configuration] > [Provisioning Extension Settings] 機能の設定にアクセスすることで表示したり、変更することができる、[Cisco TMS Connection] 設定の対応するフィールドに追加されます。
- Cisco TMSPE が Cisco TMS にデータを要求するために使用されます。
- Cisco TMS で Smart Scheduler ユーザの代わりに予約で使用されます。会議が予約または更新されるたびに、電子メール通知がこのユーザおよび会議のオーナーに送信されます。このサービス ユーザにこの電子メールを送信しない場合、使用可能な電子メール アドレスを指定せずにユーザが設定されている必要があります。

データベース情報

インストーラは Cisco TMS SQL データベース (`tmsng`) の場所を検出し、同じ場所およびインスタンスに、SQL db (`tmspe`) をインストールすることを推奨します。この場合、管理者は `tmsng` データベースについて、次のことを知っている必要があります。

- SQL サーバ名
- SQL サーバ インスタンス
- 十分な権限を持つ SQL サーバ クレデンシャル

データベースの場所

インストール中、インストーラによって別の場所とパラメータに `tmspe` データベースを保存する機会が提供されます。ただし、`tmsng` データベースと同じ場所に `tmspe` データベースを保存することを推奨します。データベース名は、必ず小文字の `tmspe` にしてください。

注意： 新しい、手動で作成されたデータベースでのインストールは、Cisco TMSPE 1.1 では作用しません。Cisco TMSPE インストーラによってデータベースが作成されるようにするか、手動作成が必要な場合は、Cisco TMSPE 1.0 を最初にインストールしてから、1.1 にアップグレードする必要があります。

必要に応じて、インストーラは、`tmspe` が動作するために、別の SQL のクレデンシャルを使用する機能を提供します。これらのクレデンシャルを変更するには、[TMS プロビジョニング拡張機能に別の SQL クレデンシャルを使用する (Provisioning Extension)] を選択します。適切な操作権限については、「[必要なセキュリティ権限 \[p. 7\]](#)」セクションを参照してください。

WebEx Enabled TelePresence 要件

WebEx が含まれる会議の予約に Cisco TMSPE を使用するには、Cisco TMS を設定する必要があります。

- WebEx Enabled TelePresence オプション キー
- 1 つ以上の WebEx サイト
- 各ユーザのシングル サインオンまたは指定 WebEx クレデンシヤル

WebEx Enabled TelePresence の設定のガイダンスについては、『WebEx Enabled TelePresence 2.0 Configuration Guide for Cisco TelePresence Management Suite』を参照してください。

ブラウザ要件

管理インターフェイス

管理者インターフェイスのクライアント要件は、Cisco TMS の要件と同じです。ご使用のバージョンの『Cisco TelePresence Management Suite Installation and Upgrade Guide』を参照してください。

ユーザ ポータル

Smart Scheduler および FindMe は、次のブラウザとバージョンでテストされています。

- Microsoft Internet Explorer 10、9、および 8
- Firefox 15 および 16
- Google Chrome 24
- Mac OS X 6.0.2 の Safari
- iPad 6.1.1 の Safari

その他のブラウザも動作する可能性はありますが、積極的にテストされていないため、サポートされていません。

導入のベスト プラクティス

エンドポイントの最新のソフトウェアへのアップグレード

Cisco TMSPE をインストールおよび展開する前に、すべてのエンドポイントを、使用可能な最新のソフトウェア バージョンにアップグレードすることを推奨します。

これにより、構成テンプレートのスキーマと Cisco TMSPE の互換性が確保でき、インストール後に維持管理するテンプレートとスキーマの数が制限されます。

Cisco TMSPE1.0 リリースの時点で、推奨されるエンドポイントのソフトウェア バージョンは次のとおりです。

ソフトウェア	バージョン
Cisco Jabber Video for TelePresence	4.2 以降
Cisco IP Video Phone E20	TE4.1.1 以降
Cisco TelePresence System EX と MX シリーズ	TC5.1 以降

AD/LDAP を使用したユーザ作成と管理の自動化

ユーザの作成および管理を自動化するために、Microsoft Active Directory または LDAP と、Cisco TMSPE のユーザを同期させることを推奨します。

Active Directory インポートが動作する要件は、次のとおりです。

- Active Directory と Cisco TMS は、同じドメイン内のメンバである必要があります。
- グローバル ディレクトリへの読み取りアクセスを持った、Active Directory 内の Cisco TMSPE の サービス アカウントが使用可能である必要があります。

セキュア通信の使用

Cisco TMSPE では、HTTPS での安全な接続が必要です。Cisco TMS をインストールまたはアップグレードすると、インストーラから、HTTPS 通信をイネーブルにするオプションが提示されます。HTTPS をイネーブルにし、有効な証明書を使用することを強く推奨します。これ以外の場合、Cisco TMS は自己署名証明書の作成を提示します。

Cisco VCS 通信を設定するときに、暗号設定が使用可能な証明書と一致していることを確認してください。詳細は、「[Cisco TMS と Cisco VCS 間の通信の設定 \[p.20\]](#)」を参照してください。

時刻の同期: Cisco VCS と Cisco TMS

Cisco TMS と Cisco VCS 間で、時刻の同期を維持します、同じ NTP (ネットワーク タイム プロトコル) サーバを使用するように、これらを設定することを推奨します。

- Cisco VCS で NTP サーバを設定するには、[System] > [Time] に移動します。
- Cisco TMS は、ホスト Windows Server のオペレーティング システムで NTP の設定を使用します。手順については、Microsoft 社のサポート技術情報『[Windows Server で権限のあるタイム サーバを構成する方法 \(How to configure an authoritative time server in Windows Server\)](#)』を参照してください。

プロビジョニング用の Cisco VCS の設定

初めてプロビジョニング機能を導入する場合、Cisco TMSPE をインストールしてアクティブにする前に、Cisco VCS をプロビジョニングのために設定する必要があります。

ネットワーク内でのプロビジョニング

2 種類の Cisco VCS があります。

- **Cisco VCS Control** : これは、企業のプライベート ネットワークにインストールして、企業内の、または VPN を通じて企業に接続する H.323 および SIP ベースのエンドポイントに登録およびルーティング機能を提供することを目的として設計されています。
- **Cisco VCS Expressway** : これは、企業の DMZ にインストールして、パブリックおよびホーム ベースの H.323 および SIP ベースのエンドポイントに登録およびルーティング機能を提供することを目的として設計されています。また、VCS Expressway は、内部の VCS Control および登録されているエンドポイントとの通信を可能にするため、ファイアウォール トラバーサル機能も提供しています。

Cisco VCS Expressway のみのネットワークでは、Cisco VCS Expressway でプロビジョニングをイネーブルにしてシステムを設定できますが、DMZ 内に設置されたアプライアンス上のユーザ データを保存するためのセキュリティを考慮する必要があります。

ユーザ アカウントは 1 つの Cisco VCS (または Cisco VCS クラスタ) だけに存在できます。つまり、ネットワークに Cisco VCS Expressway と Cisco VCS Control の組み合わせがある場合 (ソフト クライアントのようなエンドポイントが Control または Expressway に登録できる場合) は、Cisco VCS Control (または Control クラスタ) のみで設定してプロビジョニングをイネーブルにすることを推奨します。ソフト クライアントまたは他のエンドポイントが Cisco VCS Expressway に登録された場合、プロビジョニング要求は適切なトラバーサル ゾーンを経由して Expressway に関連付けられた Cisco VCS Control に (検索ルールを使用して) ルーティングされます。

階層的な Cisco VCS の導入では、1 つ以上の専用 Cisco VCS クラスタをプロビジョニング用に使用できます。その他のすべての Cisco VCS は、これらの専用プロビジョニング サーバにプロビジョニング要求をルーティングするように設定できます。ただし、各プロビジョニング Cisco VCS クラスタは、すべての Cisco VCS クラスタに適用される 10,000 ユーザのキャパシティ制限の対象となります。10,000 人を超えるユーザをプロビジョニングする必要がある場合、ご使用のネットワークには、適切に設計され、ダイヤル プランが設定された追加の Cisco VCS クラスタが必要になります。

プロビジョニングをイネーブルにする必要のない、任意の Cisco VCS (Control または Expressway) でプロビジョニングがイネーブルになっている場合、[「Cisco VCS からのプロビジョニングの削除 \[p. 72\]」](#) で指定されたプロセスを使用してディセーブルにする必要があります。

Cisco VCS に対する DNS の設定

Cisco VCS は DNS を使用し、DNS でアドレス指定可能でなければなりません。VCS の DNS サーバおよび DNS 設定を行うには、次の手順に従います。

1. [システム (System)] > [DNS] に移動します。
2. [Default DNS server Address 1] を、Cisco VCS が使用する DNS サーバの IP アドレスに設定します。
3. [Local host name] をこの Cisco VCS の DNS ホスト名に設定します (通常は [System] > [System] の [System name] と同じですが、スペースは除きます) 。
4. [Domain name] を、<Local host name>. <DNS domain name> がこの Cisco VCS で一意の FQDN になるように設定します。
5. [保存 (Save)] をクリックします。

デバイス プロビジョニング オプション キーのインストール

プロビジョニングは、デバイス プロビジョニング オプション キーを Cisco VCS にインストールすることによってアクティブになります。デバイス プロビジョニング オプション キーの取得方法については、シスコ 営業担当者にお問い合わせください。

Cisco VCS がクラスタ内にある場合は、オプションのキーは、各 VCS 上で手動で設定し、クラスタ内のすべての VCS で同じでなければなりません。

オプション キーを追加するには、次の手順に従います。

1. Cisco VCS で、[Maintenance] > [Option keys]に移動します。
2. キーがまだインストールされていないことを確認するため、画面の上部の既存のオプション キーのリストを確認します。[システム情報 (System information)]セクションには、ハードウェア シリアル番号およびインストールされているオプションの概要が示されます。
3. [ソフトウェア オプション (Software Options)]で、追加するオプション用にユーザに提供されている 20 文字のオプション キーを入力します。
4. [オプションの追加 (Add option)]をクリックします。

The screenshot shows the 'Maintenance' configuration page for Option keys. It includes a table of existing keys, system information, and a software option input field.

Key	Description
<input type="checkbox"/> 110341000-1-07700001	Enhanced OCS Collaboration
<input type="checkbox"/> 110341000-1-07700002	H323-SIP Interworking Gateway
<input type="checkbox"/> 110341000-1-07700003	Dual Network Interfaces
<input type="checkbox"/> 110341000-1-07700004	Expressway
<input type="checkbox"/> 110341000-1-07700005	FindMe
<input type="checkbox"/> 110341000-1-07700006	50 Traversal Calls
<input type="checkbox"/> 110341000-1-07700007	25 Non-traversal Calls

System information:

Hardware serial number: 02410211

Active options: 25 Non Traversal Calls, 50 Traversal Calls, 2500 Registrations, 0 TURN Relays, Expressway, Encryption, Interworking, FindMe, Dual Network Interfaces, Enhanced OCS Collaboration.

Software option:

Add option key: * ⓘ

Add option

SIP のイネーブル化

SIP は、ネットワーク上の Cisco VCS (Control および Expressway) でイネーブルにする必要があります。

1. [SIP モード (SIP mode)]がオンになっていることを確認します ([VCS 設定 (VCS configuration)] > [プロトコル (Protocols)] > [SIP] > [設定 (Configuration)]) 。この設定はデフォルトで有効になっています。
2. 少なくとも 1 つの SIP ドメインが指定されていることを確認します ([VCS 設定 (VCS configuration)] > [プロトコル (Protocols)] > [SIP] > > [ドメイン (Domains)]) 。

Cisco VCS による不明 IP アドレスへのコールの処理方法の設定

[Calls to unknown IP addresses] 設定は、Cisco VCS またはそのネイバーに登録されていないシステムへのコールの試行方法を設定します。

これは、[ダイヤル プラン設定(Dial plan configuration)] のページ([VCS 設定(VCS configuration)] > [ダイヤル プラン(Dial plan)] > [設定(Configuration)]) で設定されます。

Cisco VCS Control

Cisco VCS Control は、[Calls to unknown IP addresses] で [Indirect] モードを使用するように設定します。

The screenshot shows the Cisco TelePresence Video Communication Server Control interface. The page title is 'Cisco TelePresence Video Communication Server Control'. The navigation menu includes 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. The current page is 'Dial plan configuration', with a breadcrumb trail: 'You are here: VCS configuration > Dial plan > Configuration'. The main configuration area is titled 'Configuration' and contains two fields: 'Calls to unknown IP addresses' with a dropdown menu set to 'Indirect' and an information icon, and 'Fallback alias' with an empty text input field and an information icon. A 'Save' button is located at the bottom left of the configuration area.

Cisco VCS Expressway

Cisco VCS Expressway を使用している場合は、[Calls to unknown IP addresses] で [Direct] モードを使用するように設定されている必要があります。

The screenshot shows the Cisco TelePresence Video Communication Server Expressway interface. The page title is 'Cisco TelePresence Video Communication Server Expressway'. The navigation menu includes 'Status', 'System', 'VCS configuration', 'Applications', and 'Maintenance'. The current page is 'Dial plan configuration', with a breadcrumb trail: 'You are here: VCS configuration > Dial plan > Configuration'. The main configuration area is titled 'Configuration' and contains two fields: 'Calls to unknown IP addresses' with a dropdown menu set to 'Direct' and an information icon, and 'Fallback alias' with an empty text input field and an information icon. A 'Save' button is located at the bottom left of the configuration area.

Cisco TMS への Cisco VCS の追加

この手順は、プロビジョニングが有効な Cisco VCS または Cisco VCS クラスタ(通常は Cisco VCS Control) では必須で、その他の Cisco VCS(Cisco VCS Expressway など) では任意です。

各 Cisco VCS で、次の手順を実行します。

1. Cisco TMS が Cisco VCS を検知し、追加できるようにする方法としては、SNMP をイネーブルにする方法が最善であるため、この方法を推奨します。
 - [システム(System)] > [SNMP] に移動して、[SNMP モード(SNMP mode)] が [v3 および TMS サポート(v3 plus TMS support)] に設定され、[SNMP コミュニティ名(SNMP community name)] が設定されていることを確認します。

- ネットワーク内で SNMP が許可されていない場合、SNMP を使用しないで Cisco TMS に Cisco VCS Control を追加できます。ただし、これは Cisco VCS を自動検出してモニタする Cisco TMS の機能に悪影響を及ぼします。
- [System]> [External manager] > [Address] で、Cisco TMS の IP アドレスまたは FQDN がインストールされていることを確認します。

The screenshot shows the 'External manager' configuration page in Cisco TMS. The 'Configuration' section includes the following fields:

- Address:** 10.44.9.141
- Path:** tms/public/external/management/SystemManagementService.asmx
- Protocol:** HTTP
- Certificate verification mode:** On

A 'Save' button is located at the bottom left of the configuration area.

Cisco TMS で、Cisco VCS を追加します。

- Cisco TMS で、[Systems]> [Navigator] に移動します。
- 左ペインで、Cisco VCS を追加するフォルダを選択します。
- Cisco VCS で、SNMP モードがオン になっている場合は、VCS の IP アドレスを入力し、[Next]をクリックします。Cisco TMS により、これと通信する方法がどの程度推奨されるかについての情報が VCS から収集されます。
 - ネットワークで SNMP がサポートされていない場合、別の方法を使用して Cisco TMS で VCS を検出できます。非 SNMP デバイスの検出については、『[Cisco TMS Management Suite Administrator Guide](#)』を参照してください。
- 右ペインで、[システムの追加 (Add Systems)]ボタンをクリックします。Cisco TMS の指示に従って、Cisco VCS を追加します。

The screenshot shows the 'Add Systems' dialog box in the Cisco TMS Navigator. The dialog box is titled 'Specify Systems by IP Addresses or DNS names' and contains the following sections:

- Specify Systems by IP Addresses or DNS names:** A text input field for entering IP addresses or DNS names, with a note: 'Enter the IP address, DNS name or IP range of the systems to add. Each entry must be separated by a comma. The following example will add two systems, and scan ten systems in range: user.tms.int, 10.0.0.1, 10.1.1.0 - 10.1.1.10'.
- Enter Location Settings:** Fields for ISDN Zone (Default), IP Zone (Default), and Time Zone ((GMT + 01:00) Amsterdam, Berlin, Bern, Oslo, Rome, Stockholm, Vienna).
- Advanced Settings:**
 - Set authentication settings (if systems requires authentication to be added):** Fields for Username, Password, and Admin Password.
 - Persistent Settings:** A dropdown menu for Persistent Template (No Template).
 - Discovery Options:** A text input field for SNMP community names (public, Public, RVGET2, RVGK) and checkboxes for 'Discover Non-SNMP Systems' and 'Add unsupported systems'.
 - Other:** A dropdown menu for Usage Type (Meeting Room).

Buttons for 'Next' and 'Cancel' are located at the bottom of the dialog box.

- Cisco TMS のホスト名が、Cisco VCS で設定されていることを確認してください。
 - [システム (Systems)]> [ナビゲータ (Navigator)] に移動します。
 - [VCS] を選択します。
 - [接続 (Connection)]タブを選択します。

6. [Host Name]を、たとえば `example vcs1.example.com` のような、Cisco VCS の FQDN に設定します。
7. [保存/試行 (Save/Try)]をクリックします。

Cisco VCS でのプロビジョニングのイネーブル化

Cisco VCS クラスタの設定とプロビジョニングのイネーブル化は個別のプロセスであり、同時に試行されることはありません。Cisco VCS クラスタを設定する場合は、最初にクラスタ名を設定し、プロビジョニングの設定を次の手順で実行します。その後、『[Cisco VCS Cluster Creation and Maintenance Deployment Guide](#)』で説明されているように、クラスタを設定します。

クラスタ名を設定する方法

FindMe を使用するときには、クラスタの一部であるかどうかに関係なく、クラスタ名で Cisco VCS をセットアップする必要があります。クラスタ名は次のような条件を満たす必要があります。

- 当該の Cisco VCS によって管理されるその他の Cisco VCS または Cisco TMS クラスタと比較して一意。

クラスタ名を設定または変更するには以下を行います。

1. [VCS 設定 (VCS configuration)] > [クラスタリング (Clustering)]に移動します。
2. クラスタ名を入力します。
 - Cisco VCS がクラスタの一部である場合は、クラスタのアドレスを指定する SRV レコードで使用されている完全修飾ドメイン名に指定します (「cluster1.example.com」 など) 。
 - Cisco VCS がクラスタの一部ではない場合は、Cisco VCS のアドレスを指定する SRV レコードで使用されている完全修飾ドメイン名に指定します (「vcs1.example.com」 など) 。
3. [保存 (Save)]をクリックします。

Cisco VCS でのプレゼンスのイネーブル化

Jabber Video などのエンドポイントは、Cisco VCS をプレゼンス サーバとして使用し、他のユーザとプレゼンス情報 (オフライン、オンライン、不在または通話中など) を共有できます。

- 導入環境の SIP ドメインごとに、単一の Cisco VCS または Cisco VCS クラスタのプレゼンスのみをイネーブルにする必要があります。
- プレゼンスのイネーブル化はオプションです。

VCS Control でのプレゼンス

1. Cisco VCS Control の [Applications] > [Presence]で、[SIP SIMPLE Presence Server]を [On]にします。
2. Cisco VCS Control が、登録されている自身のプレゼンスを公開していないエンドポイント (つまり、Jabber Video 以外のエンドポイント) を公開しないエンドポイントに代わってプレゼンスを公開する場合、[SIP SIMPLE Presence User Agent]も [On]にする必要があります。



Status System VCS configuration **Applications** Maintenance [? Help](#) [Logout](#)

Presence You are here: [Applications](#) > Presence

PUA

SIP SIMPLE Presence User Agent [i](#)

Default published status for registered endpoints [i](#)

Presence Server

SIP SIMPLE Presence Server [i](#)

Status

Presence User Agent	Active
Presence Server	Active

Cisco VCS Expressway でのプレゼンス

1. Cisco VCS Expressway の [Applications]> [Presence] で、[SIP SIMPLE Presence Server]を [Off]にします。
 プレゼンス サーバは Cisco VCS Expressway で有効にはいけません。Cisco VCS Expressway はプレゼンス情報をローカルで保持するのではなく Cisco VCS Control のプレゼンス サーバに渡します。
2. Cisco VCS Expressway が、登録されている自身のプレゼンスを公開していないエンドポイント(つまり、Jabber Video 以外のエンドポイント)を公開しないエンドポイントに代わってプレゼンスを公開する場合、[SIP SIMPLE Presence User Agent]を [On]にする必要があります。



Status System VCS configuration **Applications** Maintenance [? Help](#) [Logout](#)

Presence You are here: [Applications](#) > Presence

PUA

SIP SIMPLE Presence User Agent [i](#)

Default published status for registered endpoints [i](#)

Presence Server

SIP SIMPLE Presence Server [i](#)

Status

Presence User Agent	Active
Presence Server	Inactive

デバイス認証の確認

Cisco VCS のプロビジョニング サーバでは、受信するプロビジョニング要求または電話帳要求は、Cisco VCS へのゾーンまたはサブゾーン エントリ ポイントにおいて、すでに認証されている必要があります。プロビジョニング サーバは、自分自身で認証チャレンジを行うことはありません。未認証のメッセージはすべて拒否されます。

次に示す各ゾーンまたはサブゾーンで、[認証ポリシー (Authentication policy)] が [クレデンシャルを確認する (Check credentials)] または [認証済みとして扱う (Treat as authenticated)] に設定されていることを確認します。

- デフォルト ゾーン。確認するには、次の手順に従います。
 - Cisco VCS X7.1 を使用している場合は、[VCS configuration]> [Zones] に移動し、[Default Zone] を選択します。
 - Cisco VCS X7.2 を使用している場合は、[VCS configuration]> [Zones] > [Zones] に移動し、[Default Zone] を選択します。
- すべてのトラバーサル クライアント ゾーン。
 - Cisco VCS X7.1 を使用している場合は、[VCS configuration]> [Zones] に移動し、[Traversal client] タイプの各ゾーンを選択します。
 - Cisco VCS X7.2 を使用している場合は、[VCS configuration]> [Zones] > [Zones] に移動し、[Traversal client] タイプの各ゾーンを選択します。
- デフォルト サブゾーン。この設定は、[VCS 設定 (VCS configuration)] > [ローカル ゾーン (Local Zone)] > [デフォルト サブゾーン (Default Subzone)] にあります。
- その他の設定済みサブゾーン。[VCS 設定 (VCS configuration)] > [ローカル ゾーン (Local Zone)] > [サブゾーン (Subzones)] に移動し、各サブゾーンを選択してその設定を確認します。

デバイス認証の設定の詳細については、『[Cisco TelePresence Device Authentication on Cisco VCS Deployment Guide](#)』を参照してください。

Cisco TMSPE のインストール

ここでは、Cisco TMSPE をインストールするプロセスを説明します。

冗長 Cisco TMS 設定での Cisco TMSPE のインストール

Network Load Balancer を使用して、冗長 Cisco TMS 導入環境に Cisco TMSPE をインストールする場合は、拡張機能をすべてのサーバにインストールする必要があります。一部の例外を除いて、一般的なインストール手順が適用されます。

全体的なプロセスは次のとおりです。

1. クリーン インストールの手順に従って、1 つの Cisco TMS サーバに Cisco TMSPE をインストールします。「[新規インストールの実行 \[p. 18\]](#)」を参照してください。
2. クリーン インストールの同じ手順に従って、残りのサーバに Cisco TMSPE をインストールします。プロンプトが表示されたら、インストーラで見つかった既存のデータベースを再利用することを選択します。
3. 上記の手順が完了した後に、すべてのサーバのプロビジョニング モードを変更します。「[Cisco TMSPE のイネーブル化 \[p. 19\]](#)」を参照してください。

また、サービスが応答することを確認するために、`/tmsagent/tmsportal` をプローブすることを推奨します。

冗長性の参考資料として、『*Cisco TelePresence Management Suite*』の「Redundant deployments」を参照してください。

以前のバージョンからのアップグレード

Cisco TMSPE1.0 からアップグレードする場合:

1. サーバに重要な Windows Update がすべてインストールされていることを確認します。
2. 開いているすべてのアプリケーションを閉じ、ウイルス スキャン ソフトウェアをディセーブルにします。
3. zip アーカイブから、Cisco TMSPE インストーラを Cisco TMS サーバに解凍します。
4. Cisco TMSPE インストーラを実行します。
5. インストーラの指示に従います。

アップグレード時に既存のプロビジョニングと FindMe の設定が維持されます。

使用するために新しい Smart Scheduler を設定するには、「[Smart Scheduler の導入 \[p. 40\]](#)」を参照してください。

新規インストールの実行

インストールするには、次の手順に従います。

1. サーバに重要な Windows Update がすべてインストールされていることを確認します。
2. 開いているすべてのアプリケーションを閉じ、ウイルス スキャン ソフトウェアをディセーブルにします。
3. zip アーカイブから、Cisco TMSPE インストーラを Cisco TMS サーバに解凍します。
4. Cisco TMSPE インストーラを実行します。
5. 設定の手順に従います。
 - a. [次へ(Next)]をクリックして、設定を開始します。
 - b. 使用許諾契約書の条項に同意し、[次へ(Next)]をクリックします。

- c. Cisco TMSPE が Cisco TMS に接続するために使用する、サービス ユーザの**ユーザ名** と**パスワード** を入力します。このユーザは、Cisco TMS のサイト管理者グループのメンバーである必要があります。
[次へ(Next)]をクリックします。
 - d. インストーラは、TMS SQL データベース(**tmsng**) がインストールされている場所を検出します。Cisco TMSPE SQL データベース(**tmspe**) を同じ場所およびインスタンスにインストールすることを推奨します。
 - i. 適切な **SQL サーバ名**と**インスタンス名**を確認するか、または入力します。冗長設定で展開する場合、両方のインストールが同じデータベースの場所を指していることを確認します。
 - ii. 必要なクレデンシャルを入力します。
 - iii. [次へ(Next)]をクリックします。
 - e. [インストール(Install)]をクリックして、インストールを開始します。[戻る(Back)]をクリックして、インストール設定の確認または変更を行います。
 - f. インストールが完了したら、[Finish]をクリックして [Setup] ウィンドウを閉じます。
6. ウィルス スキャン ソフトウェアを再びイネーブルにします。

Cisco TMSPE のイネーブル化

インストールを完了したら、次の手順に従います。

1. Cisco TMS で、[Administrative Tools]> [Configuration] > [General Settings] に移動し、[Provisioning Mode]フィールドを [Provisioning Extension]に設定して、[Save]をクリックします。この選択後、ブラウザ ウィンドウをリフレッシュするか、ブラウザのキャッシュを空にする必要がある場合があります。

The screenshot shows the 'General Settings' configuration page in Cisco TMSPE. The 'Provisioning Mode' is set to 'Provisioning Extension'. Other visible settings include 'Default Time Zone' (GMT + 01:00), 'Default ISDN Zone' (example), and 'Default IP Zone' (example). The 'Provisioning Mode' dropdown is expanded, showing 'Provisioning Extension' as the selected option, with 'Off' and 'TMS Agent Legacy' as other options. An 'Edit Login Banner' button is visible on the right side of the page.

2. [管理ツール(Administrative Tools)]> [活動状況(Activity)] に移動し、切り替えが完了したことを確認します。
3. Cisco TMSPE 機能が現在使用でき、機能していることを確認します。
 - a. Cisco TMS の次のページをブラウズします。
 - [システム(Systems)]> [プロビジョニング(Provisioning)]> [ユーザ(Users)]。このページに、ユーザ リポジトリへの接続の問題が報告されていると、データベース接続は動作していません。「[インストールに関するトラブルシューティング \[p. 67\]](#)」を参照してください。
 - [システム(Systems)]> [プロビジョニング(Provisioning)]> [FindMe]
 - [システム(Systems)]> [プロビジョニング(Provisioning)]> [デバイス(Devices)]
 - [管理ツール(Administrative Tools)]> [構成(Configuration)]> [プロビジョニング拡張機能の設定(Provisioning Extension Settings)]
 - b. [管理ツール(Administrative Tools)]> [プロビジョニング拡張機能の診断(Provisioning Extension Diagnostics)] に移動し、発生しているアラームがないか確認して、[ヘルス チェック

クを実行 (Run Health Check)] をクリックします。アラームが発生している場合は、それをクリックして詳細を参照し、記載されている対処方法を実行します。詳細については、「[インストールに関するトラブルシューティング \[p. 67\]](#)」を参照してください。

4. 上記のすべての Cisco TMSPE ページが正常にブラウズでき、[Provisioning Extension Diagnostics] でアラームが報告されていない場合は、「[Cisco TMS と Cisco VCS 間の通信の設定 \[p. 20\]](#)」に進みます。

Cisco TMS と Cisco VCS 間の通信の設定

Cisco VCS または VCS クラスタが Cisco TMSPE と通信できるようにするには、次の手順を実行します。Cisco VCS がクラスタ化されている場合は、クラスタ内の 1 つの Cisco VCS だけを設定します。

- Cisco VCS は、ユーザ設定、FindMe 設定、電話帳、およびライセンス情報を Cisco TMSPE からインポートします。
- Cisco TMSPE は、プロビジョニングされたデバイスに関する情報を Cisco VCS から受信します。

次の手順に従ってください。

1. Cisco TMS で [Systems] > [Navigator] に移動し、Cisco VCS を選択します。これはクラスタの任意の Cisco VCS で構いません。
2. [プロビジョニング (Provisioning)] をクリックします。
3. ページの下部にある、[デフォルト接続設定 (Set Default Connection Settings)] ボタンをクリックします。
[Cisco TMS Connection Settings] ペインは、推奨値が入力されています。
4. テレプレゼンス インフラストラクチャに従って接続設定を調整します。

Configuration	
VCS Provisioning Mode:	Provisioning Extension
TMS Connection Settings	
Server Address:	10.47.28.131
Encryption:	Off
Certificate Verification Enabled:	No
Certificate Hostname Checking Enabled:	No
Username:	exch2k3\teo
Password:
Base Group:	Unknown (d9b263d8-2168-4c55-9d76-feb12125d0f3)

- デフォルト値および推奨される暗号化設定は、TLS です。「[セキュア通信の使用 \[p. 10\]](#)」を参照してください。セキュアな通信を使用しないことを選択している場合は、必ずこの設定を [オフ (Off)] に変更してください。こうしないと、接続が拒否されます。暗号化をイネーブルにしている場合は、有効な証明書および証明書のホスト名をチェックするかどうかを選択します。
 - ユーザ名とパスワードは、Cisco TMS のサイト管理者グループのメンバにする必要があります。
 - 大規模な展開では、[Base Group] が Cisco VCS ごとに root レベルではなく、グループ レベルに設定されていることを確認します。
5. [Services] ペインまでスクロールし、リストされている各サービス (該当する場合は FindMe も含め) の [Enable Service] をオンにします。
 6. [保存 (Save)] をクリックします。
 7. イネーブルにした各サービスの [ステータス (Status)] フィールドを確認します。エラーがサービスのいずれかに表示された場合、対応する警告アイコンをクリックし、表示された手順に従います。その後、[強制的に更新 (Force Refresh)] をクリックします。

Service	Enable Service	Polling Interval (seconds)	Status
Users	<input checked="" type="checkbox"/>	2 minutes	✓ OK (click for details)
FindMe	<input checked="" type="checkbox"/>	2 minutes	✓ OK (click for details)
Phone Books	<input checked="" type="checkbox"/>	3 hours	✓ OK (click for details)
Devices	<input checked="" type="checkbox"/>	root	✓ OK (click for details)

- すべてのサービスで緑色のチェック マークが表示されたら、ページ上部の [VCS プロビジョニング モード (VCS Provisioning Mode)] にスクロールし、[プロビジョニングの拡張機能の診断 (Provisioning Extension)] を選択します。[保存 (Save)] をクリックします。

「[プロビジョニングのための Cisco TMSPE の設定 \[p. 22\]](#)」に進みます。

プロビジョニングのための Cisco TMSPE の設定

ここでは、プロビジョニングのための Cisco TMSPE を設定するために必要な手順について説明します。

グループの作成とユーザの追加

ユーザは、外部ディレクトリからインポートして Cisco TMSPE に追加するか、または手動で個別に追加できます。ユーザを追加する前に、グループ階層を設定する必要があります。

ルート グループにユーザを直接インポートしたり、追加したりしないでください。こうすると、Cisco VCS クラスタの拡張性が失われ、ユーザの一括削除が必要になった場合に、操作が複雑になります。

グループの設定

お客様の組織の Cisco VCS の組織と一致するように、ユーザを地理的な場所に従ってグループ化することを推奨します。Cisco VCS で許容できる最大ユーザ数は 10,000 ユーザであるため、各グループはこのユーザ数を超えてはいけません。

ユーザを手動で追加したり、外部ソースから特定のグループにユーザをインポートすると、ユーザはその都度、グループに割り当てられているユーザ、FindMe、電話帳およびデバイス設定を継承します。グループ レベルで割り当てられていないすべての設定は、親グループから継承されます。

グループを追加するには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ(Users and Groups)] コンテナで、追加するグループの親をクリックします。
3. エクスプローラ ビューの上で、[グループを追加(Add Group)] をクリックします。
[グループを追加(Add Group)] ダイアログボックスが表示されます。
4. [表示名(Display Name)] フィールドにグループ名を入力します。
5. [保存(Save)] をクリックします。

これで、外部ディレクトリからグループにユーザをインポートしたり、手動でユーザを追加したりできるようになります。

外部ディレクトリからのユーザのインポート

次の外部ソースからのユーザ アカウント データをインポートして同期できます。

- Active Directory
- Kerberos を使用した Active Directory
- Lightweight Directory Access Protocol(LDAP)

Active Directory 以外の LDAP 実装では、インポートと同期に対して次の内容がサポートされている必要があることに注意してください。

- [RFC 4530](#) に定義されている **entryUUID** フィールド。
- [RFC 2696](#) に定義されている簡単なページング。

インポートはグループごとに設定されます。インポートを設定する前に、ユーザをインポートするグループを 1 つ以上追加したことを確認します。これは、ユーザを直接ルート グループの下に追加してはいけないためです。

インポートの設定

ユーザ アカウントを外部ディレクトリからインポートするには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ (Users and Groups)]コンテナで、ユーザ アカウントをインポートするグループをクリックします。
選択したグループに関する情報が複数のペインに表示されます。

example_group

Rename Group... Delete Send Account Information Move Group Toggle Details

User Settings

Name	Pattern	Origin
Video Address Pattern	{first_name}.{last_name}@example.com	example_group
Caller ID Pattern	{mobile_phone}	example_group
Device Address Pattern	{username}. {device.model}@example.com	example_group
Image URL Pattern		root

Edit Reload

User Import

No user import has been configured for this group.

Configure

3. [ユーザ インポート (User Import)]ペインで、[構成 (Configure)]をクリックします。
4. 開始点として親グループからユーザのインポート設定をコピーする場合は、[親からコピー (Copy from parent)]をクリックします。
5. [タイプ (Type)]フィールドで、ユーザ データのインポート元の外部ディレクトリのタイプを選択します。インポート元として選択した外部ディレクトリのタイプに基づいて、[構成 (Configuration)]フィールドが表示されます。次のスクリーンショットは、セキュア AD で使用可能なフィールドを示します。

User Import

Type: Active Directory with Kerberos (Secure AD) ▼

Hostname: fqdn.example.com

Port: 3268

Username:

Password:

Base dn:

Relative search dn:

Search filter:

Distribution center:

Distribution center timeout:

Realm:

Copy from parent Save Cancel

6. 表示されるフィールドに、Cisco TMSPE が外部ディレクトリに接続するために必要な情報を指定しま

す。次の表に従ってフィールドを設定します。

フィールド	Active Directory (AD)	Kerberos を使用した Active Directory (セキュア AD)	Lightweight Directory Access Protocol (LDAP)	説明
ホストネーム (Hostname)	Yes	Yes	Yes	外部ディレクトリをホストしているサーバ。完全修飾ドメイン名 (FQDN) を入力します。
ポート (Port)	Yes	Yes	Yes	外部ディレクトリにアクセスするために使用されるサーバのポート。 Kerberos のインポートにはグローバル カタログ ポート 3268 を使用します。
ユーザー名 (Username)	Yes	Yes	Yes	外部ディレクトリへのログイン時に Cisco TMSPE が使用するユーザー名。パスワードも参照してください。
パスワード (Password)	Yes	Yes	Yes	外部ディレクトリへのログイン時に Cisco TMSPE が使用するパスワード。ユーザー名も参照してください。
ベース dn (Base dn)	Yes	Yes	Yes	LDAP 識別名。詳細については、MSDN ライブラリの記事『 Distinguished Names 』を参照してください。
相対検索 dn (Relative search dn)	Yes	Yes	Yes	ベース DN から見た LDAP の相対識別名 (ベース DN も参照)。相対 DN は、ベース DN から親フォルダを見たときの相対ファイル名です。たとえば、DN が <code>C:\-example\folder\myfile.txt</code> の場合、相対 DN は <code>myfile.txt</code> です。詳細については、MSDN ライブラリの記事『 Distinguished Names 』を参照してください
サーチ フィルタ (Search filter)	Yes	Yes	Yes	インポートするアカウントを指定した検索フィルタ。これらのフィルタの詳細および構成方法の詳細については、RFC4515 : 『 Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters 』を参照してください。
配布センター (Distribution center)	No	Yes	No	Kerberos キー配布センターのサーバのアドレス、つまりご使用の Active Directory (AD) のアドレスです。この値は、完全修飾ドメイン名 (FQDN) または、AD サーバが存在するドメインになります。ドメインの場合は、DNS SRV が実行されて、FQDN が特定されます。

フィールド	Active Directory (AD)	Kerberos を使用した Active Directory (セキュア AD)	Lightweight Directory Access Protocol (LDAP)	説明
配布センターのタイムアウト (Distribution center timeout)	No	Yes	No	キー配布センターからの応答を待機する時間の最大ミリ秒。
レルム (Realm)	No	Yes	No	Kerberos 認証用の AD で設定されているレルム。
接続タイプ (Connection type)	No	No	Yes	接続タイプを選択します。次のオプションを使用できます。 <ul style="list-style-type: none"> • 非セキュア (Unsecured) • StartTLS • SSL : この接続タイプでは、証明書処理がサポートされていないことに注意してください。
証明書エラーを無視 (Ignore certification errors)	No	No	Yes	[はい (Yes)]または [いいえ (No)]を選択します。

7. [Save]をクリックします。

Active Directory および LDAP のフィールドの Cisco TMSPE 属性へのマッピング、手動同期の実行手順の詳細については、「[ユーザ データの同期化 \[p. 59\]](#)」を参照してください。

Active Directory 接続設定の確認

接続設定をチェックし、フィルタ テンプレートがインポートする対象に対して適切であることを確認します。

1. [Administrative Tools] > [Configuration] > [Provisioning Extension Settings]に移動します。
2. [Active Directory Connection]設定にスクロールします。

Active Directory Connection

Connection Timeout * (milliseconds)

Filter Template *

Follow Referrals * Yes No

3. 必要に応じて設定を変更します。
 - [Connection Timeout]はミリ秒単位
 - [Filter Template]は、すべてのグループ インポートに適用されます。テンプレートの %s 変数は、グループ インポートの [Search Filter] セットに置き換えられます。
4. [保存 (Save)]をクリックします。

ユーザの手動追加

外部ディレクトリからユーザ アカウントをインポートする代わりに、ユーザ アカウントを手動で追加することができます。

ユーザ アカウントを追加する前に、アカウントが所属するグループがグループ階層にすでに存在していることを確認します。「[ユーザの手動追加 \[p. 26\]](#)」を参照してください。

手動で作成したユーザ名が次のいずれかと一致しない限り、手動で追加されたユーザが FindMe ユーザポータルにサインインできないことに注意してください。

- 存在する場合は、Active Directory ユーザ名。
- ユーザに Active Directory アカウントがない場合は、Cisco TMS/Cisco TMSPE サーバのローカル Windows ユーザ名。このようなアカウントを作成している場合は、必要なクレデンシャルを必ずユーザに提供して、ポータルにサインインできるようにします。

ユーザ アカウントを追加するには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ(Users and Groups)] コンテナのヘッダーの下にある検索フィールドを使用し、ユーザ アカウントがすでに存在していないことを確認します。
3. [ユーザとグループ(Users and Groups)] コンテナで、所属するグループをクリックします。
4. [ユーザとグループ(Users and Groups)] コンテナで、[ユーザの追加(Add user)] をクリックします。
[ユーザの追加(Add user)] ダイアログボックスが開きます。
5. 提供されたフィールドにユーザに関する情報を指定します。
6. [保存(Save)] をクリックします。

アドレス パターンの作成

アドレス パターンタイプ

Cisco TMSPE には、2 種類の主なアドレス パターンのタイプがあります。

- デバイス アドレス パターンは、Cisco TMSPE がプロビジョニング済みデバイスのアドレスを作成するときに使用するテンプレートです。Cisco TMSPE がユーザをデバイスに接続できるようにするために、デバイス アドレス パターンを割り当てる必要があります。
- ビデオ アドレス パターンは、FindMe ID(FindMe が使用されている場合) およびプロビジョニング電話帳ソース内のユーザ用メイン アドレスの両方として動作する、ビデオ アドレスを生成するために使用されます。ビデオ アドレスは、SIP URI、H. 323 ID、または E. 164 番号になります。

さらに、次のパターンがあります。

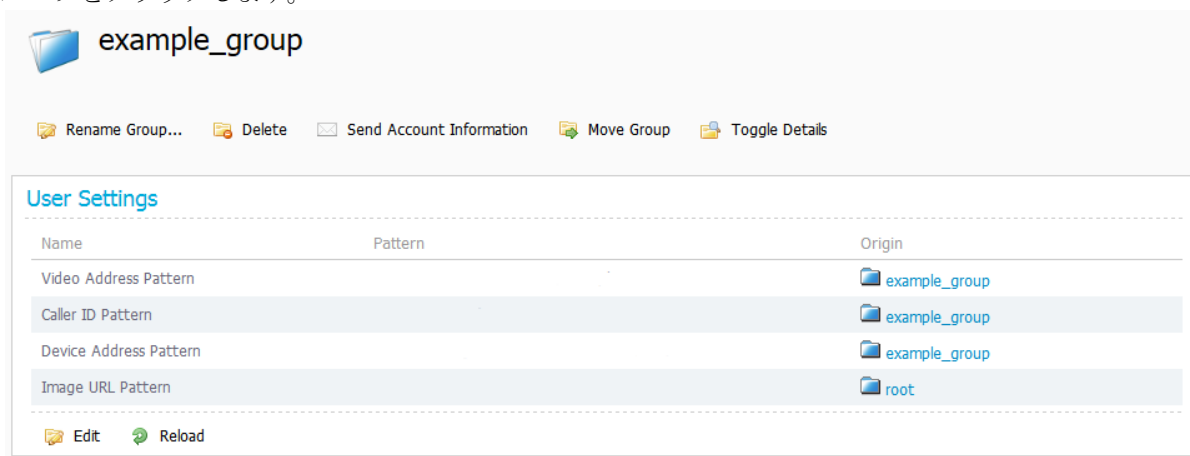
- **発信者 ID パターン**：ISDN ゲートウェイを経由してルーティングされるコールの発信者 ID を生成するために、FindMe によって使用されます。「[発信者 ID パターンの定義 \[p. 43\]](#)」は、このマニュアルの「[FindMe の導入 \[p. 43\]](#)」セクションで説明されています。
- **イメージ URL パターン**：ユーザ イメージを持つサーバが使用可能な場合、ユーザ グループを設定するときに、オプションで追加できます。イメージは、Cisco TMSPE および FindMe のユーザ インターフェイス、および互換性のあるデバイスの電話帳で使用されます。

グループに割り当てられているすべてのパターンは、グループ内のすべてのユーザ、すべてのサブグループ、およびサブグループ内のすべてのユーザに継承されることに注意してください。

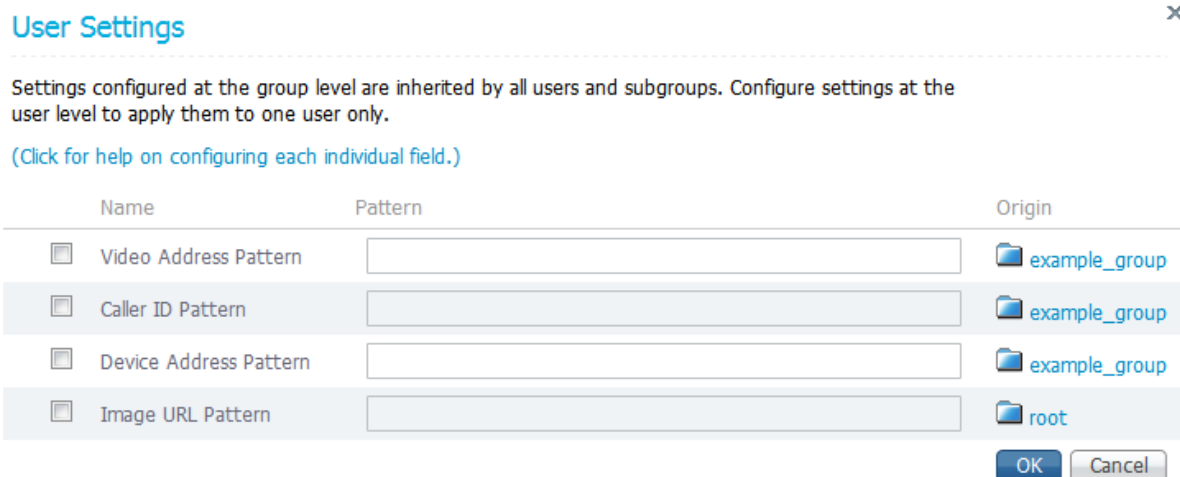
パターンの追加

デバイス アドレス パターン、ビデオ アドレス パターンおよび任意でイメージ URL パターンを作成するには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ (Users and Groups)]コンテナで、デバイス アドレス パターンを割り当てるグループをクリックします。



3. [ユーザ設定 (User Settings)]ペインで [編集 (Edit)]をクリックします。[ユーザ設定 (User Settings)]ダイアログボックスが開きます。



4. [Video Address Pattern]フィールドで、選択したグループ内のユーザの FindMe ID を定義する際に、Cisco TMSPE が使用するパターンを指定するか、選択したユーザに対する明示的 FindMe ID を指定します。
パターンでは、次のユーザ属性を任意に使用できます。
 - {username}
 - {display_name}
 - {first_name}
 - {last_name}
 - {email}
 - {office_phone}
 - {mobile_phone}
5. [Device Address Pattern]フィールドで、プロビジョニング済みデバイスの名前を作成する際に、Cisco TMSPE が使用するパターンを指定します。

パターンでは、上記に示すいずれのユーザ属性も使用できます。また、このパターンでは、次のデバイス属性を任意に使用できます。

- {device.model}
これは、デバイス モデルに解決します(例: e20、movi、ex90)。
- {device.connectivity}
これは、デバイスが Cisco VCS Control に登録されている場合は *internal* に、デバイスが Cisco VCS Expressway に登録されている場合は *external* に解決されます。

User Settings

Settings configured at the group level are inherited by all users and subgroups. Configure settings at the user level to apply them to one user only.

(Click for help on configuring each individual field.)

Name	Pattern	Origin
<input checked="" type="checkbox"/> Video Address Pattern	<input type="text" value="{first_name}.{last_name}@example.com"/>	example_group
<input type="checkbox"/> Caller ID Pattern	<input type="text"/>	example_group
<input checked="" type="checkbox"/> Device Address Pattern	<input type="text" value="{username}.{device.model}@example.com"/>	example_group
<input type="checkbox"/> Image URL Pattern	<input type="text"/>	root

6. オプションで、[イメージ URL パターン(Image URL Pattern)] フィールドで、ユーザのイメージを収集する際に使用するパターンを指定します。サポートされている形式は、.jpg、.jpeg、.png です。パターンでは、次のユーザ属性を任意に使用できます。

- {username}
- {display_name}
- {first_name}
- {last_name}
- {email}
- {office_phone}
- {mobile_phone}

7. [OK]をクリックします。

パターン例

ビデオアドレス

- {username}@example.com
- {email}

デバイスアドレス

- {username}.{device.model}@example.com
- {username}.{device.model}.{device.connectivity}@example.com

次に、パターンでどのように regex 置換を使用できるかについての例を示します。

- {username [' '='']}.{device.model}@example.com
この置換により、パターンからスペースが削除されます。
- {user-
name}.
{device.model}.{device.connectivity['internal']='office','external']='home']}@example.com

この方法では「internal」から「office」に、「external」から「home」に接続が変わります。

イメージ URL

`http://yourimageserver/users/{username}.png`

プロビジョニングされたデバイスの設定を構成する方法

目的の一連の設定を持つデバイスをプロビジョニングするには、Cisco TMSPE にテンプレートを作成し、ユーザ グループに割り当てる必要があります。各テンプレートには、有効なスキーマ (XML ファイルのデバイス固有モデルおよびバージョンでサポートされるすべての可能な設定) に基づく必要があります。

構成を設定するには、構成テンプレートを追加してグループに割り当てる前に、導入環境で使用されているエンドポイントの各タイプについて、テンプレート スキーマを取得およびアップロードする必要があります。

テンプレートスキーマの取得

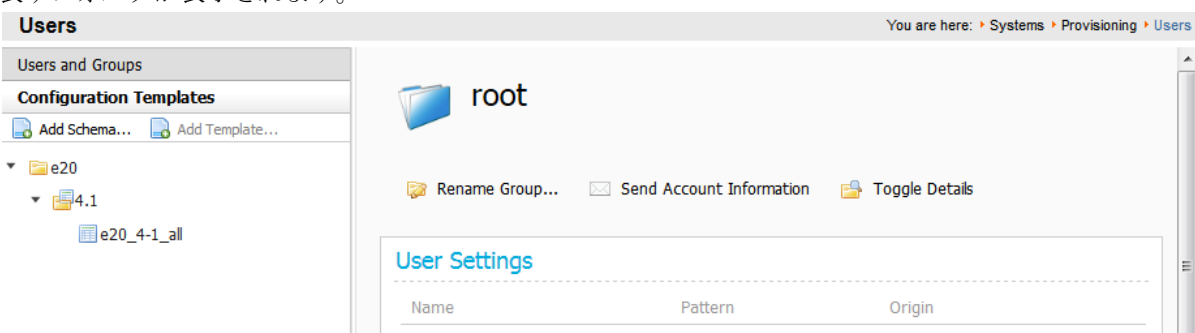
ネットワークで使用できるエンドポイントの各モデルおよびバージョンについては、関連するスキーマを取得し、Cisco TMSPE にアップロードする必要があります。テンプレート スキーマは通常、デバイスのソフトウェア リリース内の、ソフトウェア バンドル内、またはリリース ノートが利用可能な場合は同じページに含まれます。スキーマがソフトウェア バンドルに含まれていない場合は、<http://cisco.com> の検索機能を使用し、テンプレート スキーマを検索してローカル サーバにダウンロードします。

互換性のあるテンプレート スキーマをダウンロードし、Cisco TMSPE を追加するには、以下の手順に従います。

1. 検索文字列として「Configuration Templates for TMS」と入力します。
2. 検索結果のリストをスクロールして、必要なスキーマが含まれる .zip ファイルを見つけます。

スキーマのアップロード、アップロード先: Cisco TMS

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザ (Users)] ページで、[構成テンプレート (Configuration Templates)] コンテナをクリックします。テンプレート スキーマがすでにアップロードされたデバイスのモデルおよびバージョンを表すフォルダが表示されます。



3. [構成テンプレート (Configuration Templates)] のコンテナで、[スキーマを追加 (Add schema)] をクリックします。[テンプレート スキーマのアップロード (Upload Template Schema)] ダイアログ ボックスが開きます。

Upload Template Schema

Please select a valid Cisco Configuration Template Schema:

- [ブラウズ(Browse)]ボタンをクリックし、スキーマをダウンロードしたローカル サーバ上のフォルダに移動し、[OK]をクリックします。テンプレート スキーマはデバイスに関連するモデルおよびバージョンに関連するフォルダに追加されます。

Name	Type	Connectivity	Map To Key	Editable
Bandwidth Prober Auto Scheduling	Literal	Internal	Configuration/BandwidthProberAutoScheduln	true
Bandwidth Prober Time	Integer	Internal	Configuration/BandwidthProberTime	true
ClearPath	Literal	Internal	Services/ClearPath	true
Cloud Services (xmpp)	Literal	Internal	Services/Xmpp/Enable	true
Default Mediatype Candidate	Literal	Internal	Services/Sip/DefaultMediaCandidateType	true
Detect Media Mangling	Literal	Internal	Services/Sip/DetectMediaMangling	true
Display Name	String	Internal	Configuration/DisplayName	false
Encryption Policy	Literal	Internal	Services/Encryption	true
Far End Camera Control	Literal	Internal	Services/Sip/EnableH224	true
FindMe URI	String	Internal	Configuration/FindMeUri	false
Help URL	String	Internal	Configuration/HelpUrl	true
ICE	Literal	Internal	Services/Sip/EnableIce	true
IP Version	Literal	Internal	Services/Sip/IpVersion	true
Inviter Contact URI	String	Internal	Configuration/InviterContact	true
MNS Mode	Literal	Internal	Services/Sip/EnableMnsMode	true
Maximum In Bandwidth	Integer	Internal	Configuration/MaxInBandwidth	true
Maximum Out Bandwidth	Integer	Internal	Configuration/MaxOutBandwidth	true

構成テンプレートの追加

構成テンプレートは、ユーザ グループに割り当てることを選択する設定の集まりを指定します。選択する構成は関連するテンプレートのスキーマに定義されます(「[テンプレート スキーマの取得 \[p. 29\]](#)」を参照)。

ネットワークのエンドポイント デバイスのタイプおよび使用中のサービスに応じて、通常次の設定が最も重要です。

- SIP サーバ アドレス
- 電話帳 URI
- プレゼンス URI

使用可能な設定の詳細および各エンドポイント タイプの制限値の詳細については、管理者ドキュメントを参照してください。

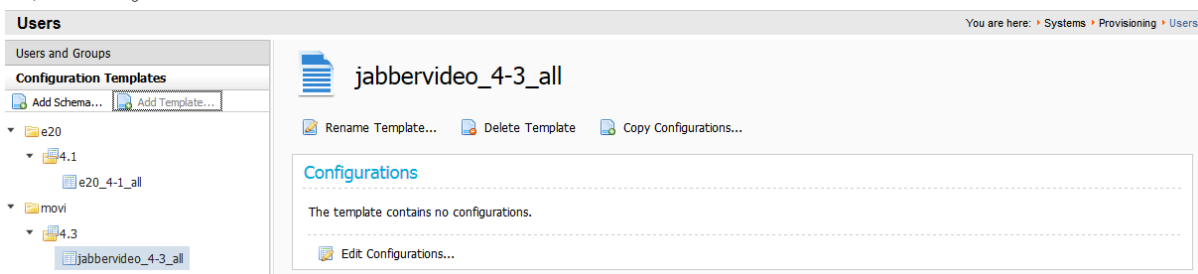
構成テンプレートを作成するには、次の手順に従います。

- [ユーザ(Users)]ページで、[構成テンプレート(Configuration Templates)]コンテナをクリックします。
- [構成テンプレート(Configuration Templates)]コンテナで、デバイスに関連するモデルおよびバージョンのフォルダに移動し、[テンプレートの追加(Add template)]をクリックします。[テンプレートの追加(Add template)]ダイアログボックスが開きます。

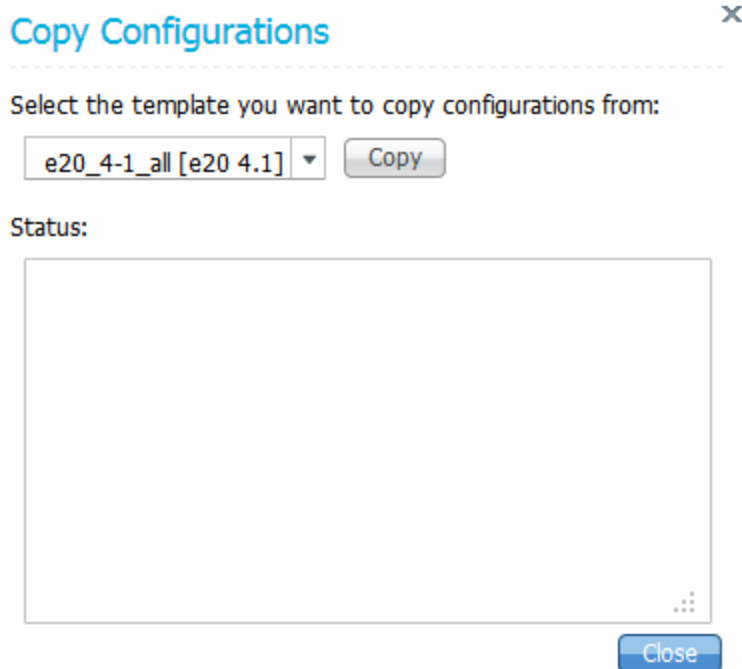
Add Template ×

Display Name:

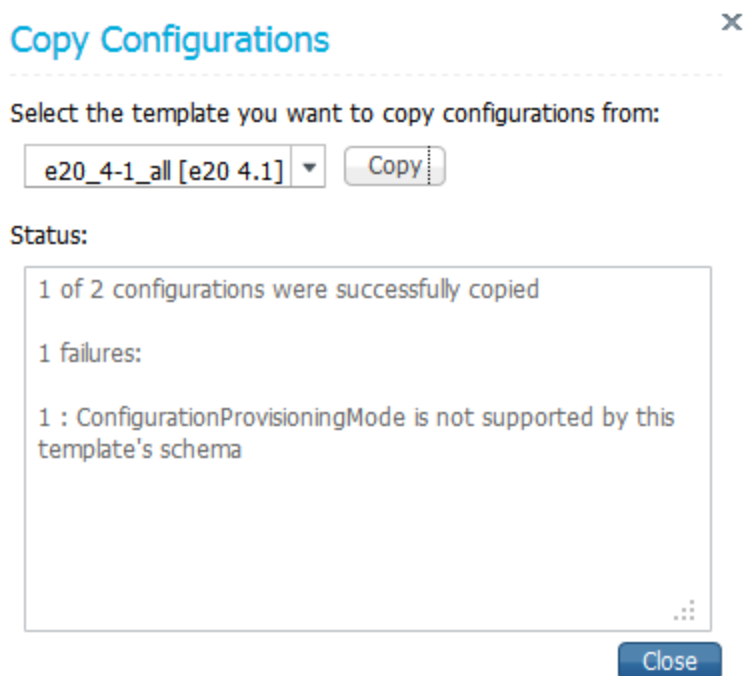
3. テンプレートに適切な表示名を入力し、[OK]をクリックします。テンプレートは、[構成テンプレート (Configuration Templates)] コンテナに追加されます。この時点で、テンプレートには設定は含まれません。



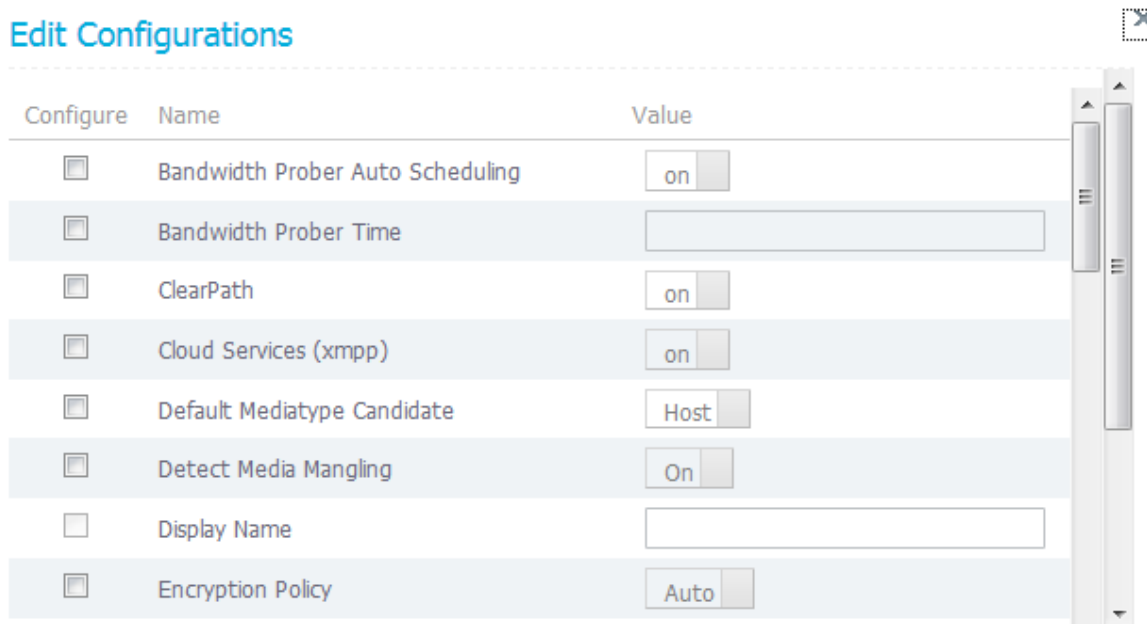
4. 次のいずれか方法で、設定を追加します。
 - 既存のテンプレートから、設定をコピーします。
 - i. [構成 (Configuration)] ペインの上部で、[構成のコピー (Copy Configurations)] をクリックします。[構成のコピー (Copy Configurations)] ダイアログボックスが開きます。



- ii. すべての設定のコピー元を選択し、[コピー (Copy)] をクリックします。[ステータス (Status)] フィールドには、コピーの結果が報告されます。正常にコピーされた設定の数、失敗したコピー (たとえば、ターゲット テンプレートのスキーマで、元のテンプレートのスキーマと同じキーがサポートされていないなどの原因によるもの) の数が表示されます。



- iii. [閉じる (Close)]をクリックします。
- 個別設定を追加します。
 - i. [構成 (Configuration)]ペインで、[構成の編集 (Edit Configurations)]をクリックします。 [構成の編集 (Edit Configurations)]ダイアログボックスが開きます。



- ii. テンプレートに追加する各設定について、[構成 (Configure)]チェックボックスを選択し、[値 (Value)]フィールドで値を入力するか、選択します。
- iii. [保存 (Save)]をクリックして設定を保存します。 [構成 (Configuration)]ペインに表示され

る追加した設定。

The screenshot shows the 'Users' page in Cisco TMSPE. On the left, a tree view shows the hierarchy: Users and Groups > Configuration Templates > e20 > 4.1 > e20_4-1_all > movi > 4.3 > jabbervideo_4-3_all. The main area displays the configuration for 'jabbervideo_4-3_all'. It includes options to 'Rename Template...', 'Delete Template', and 'Copy Configurations...'. Below is a 'Configurations' table with the following data:

Name	Value
Help URL	https://intra.example.com/jabbervideo/default.htm
Phone Book Server URI	phonebook@example.com
Presence Server URI	presence@example.com
SIP Server Address	192.0.2.0

There is also an 'Edit Configurations...' button at the bottom.

ユーザの 1 つ以上のグループに構成テンプレートを割り当てることができます。

グループへの構成テンプレートの割り当て

グループに割り当てるテンプレートは、グループ内のすべてのユーザ、すべてのサブグループ、およびサブグループ内のすべてのユーザが継承します。テンプレートを個別のユーザに直接割り当てることはできません。特定のモデルおよびバージョンに複数の構成テンプレートが存在する場合、グループに割り当てることができるのは 1 つだけです。

構成テンプレートをグループに割り当てるには、次の手順に従います。

1. [ユーザ(Users)] ページで、[ユーザとグループ(Users and Groups)] コンテナをクリックし、その後、目的のグループをクリックします。[構成テンプレート(Configuration Templates)] ペインまでスクロールします。

Configuration Templates

Name	Model	Version	Origin
e20_4-1_all	e20	4.1	root

Assign Templates

2. [テンプレートの割り当て(Assign templates)] をクリックします。[テンプレートの割り当て(Assign templates)] ダイアログボックスが開きます。

Assign Templates

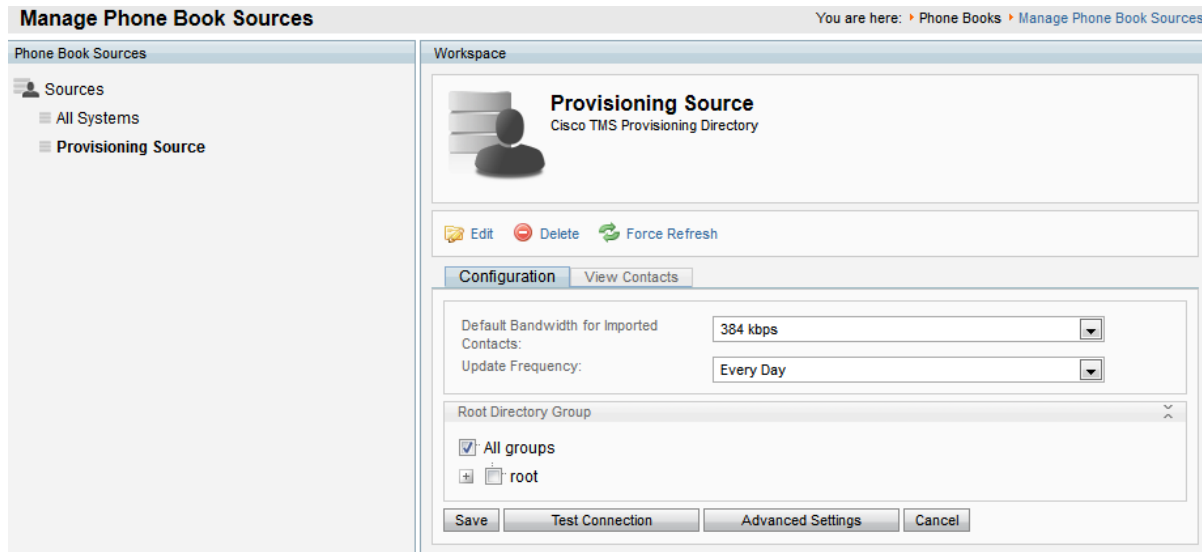
Assign	Name	Model	Version	Origin
<input type="checkbox"/>	e20_4-1_all	e20	4.1	root
<input type="checkbox"/>	jabbervideo_4-3_all	movi	4.3	

3. グループに割り当てる各構成テンプレートのチェックボックスをオンにします。
4. [保存(Save)] をクリックします。

プロビジョニング電話帳

プロビジョニングされたエンドポイントと、Cisco TMS に登録されたエンドポイントとでは、電話帳の設定方法が異なります。ユーザを、そのユーザがアクセス権を持つ 1 つ以上の電話帳を使用するようにプロビジョニングするには、グループに設定した電話帳 URI (`phonebook@example.com`) が使用されます。

プロビジョニング電話帳ソースの作成および設定



より限定された電話帳へのグループ アクセスを提供できるように、ユーザ ディレクトリのルート フォルダから 1 つのプロビジョニング ソースを作成するか、または異なるディレクトリで複数のプロビジョニング ソースを作成できます。

電話帳とソースがどのように動作するかについての詳細は、『[Cisco TelePresence Management Suite Administrator Guide](#)』または組み込み Web ヘルプを参照してください。

プロビジョニング ソースを作成するには、次の手順に従います。

1. Cisco TMS で、[Phone Books]> [Manage Phone Book Sources] に移動します。
2. 右側のペインで、[新規 (New)] をクリックします。
3. [名前 (Name)] フィールドに、新しいソースの識別に役立つ名前を入力します。
4. [タイプ (Type)] ドロップダウン メニューから、[Cisco TMS プロビジョニング ディレクトリ (Cisco TMS Provisioning Directory)] を選択します。
5. [保存 (Save)] をクリックします。
ルート ディレクトリを含め、新しいプロビジョニング ソースの設定を変更するには、次の手順を実行します。

既存のプロビジョニング ソースの設定を変更するには、次の手順に従います。

1. [電話帳 (Phone Books)] > [電話帳ソースの管理 (Manage Phone Book Sources)] > [プロビジョニング ソース (Provisioning Source)] に移動します。
2. [詳細設定 (Advanced Settings)] ボタンをクリックし、ソースに含まれるものを構成する設定を開きます。
 - [プロビジョニングされたデバイス (Provisioned Devices)] をチェックして、ユーザがログインしてデバイスがプロビジョニングされたときにソースにデバイス アドレスが追加されるようにします。

- [オフィスの電話 (Office Phone)] および [携帯電話 (Mobile Phone)] をチェックして、インポートされたか、または手動で作成されたプロビジョニング ユーザについてこれらのフィールドが含まれるようにします。
3. [ルート ディレクトリ (Root Directory)] ペインで、このプロビジョニング ソースのベースとするグループをチェックします。
 4. [保存 (Save)] をクリックします。

追加プロビジョニング電話帳の作成

電話帳として使用するには、プロビジョニング ソースを Cisco TMS の新規または既存の電話帳に接続する必要があります。

新しい電話帳を作成するには、次の手順に従います。

1. [電話帳 (Phone Books)] > [電話帳の管理 (Manage Phone Books)] に移動します。
 2. [新規 (New)] をクリックします。
 3. 電話帳の表示名を入力し、[保存 (Save)] をクリックします。
- 1 つ以上のプロビジョニング ソースを既存の電話帳に接続するには、次の手順に従います。
1. [電話帳 (Phone Books)] > [電話帳の管理 (Manage Phone Books)] に移動します。
 2. 左ペインで、目的の電話帳をクリックします。
 3. 右側のペインで、[接続 (Connect)] ボタンをクリックします。
 4. 接続するプロビジョニング ソースをチェックします。
 5. [OK] をクリックします。

電話帳ソースの活動状況

Cisco TMS の [Phone Books] > [Phone Book Sources Activity Status] で、活動状況をモニタします。

Phone Book Sources Activity Status You are here: Phone Books > Phone Book Sources Activity Status

Information

Get an overview of activity status on events. See which events has been run and if they failed or succeeded. Click on "View" link on the right to see more detailed log.

Start Date: 3/29/2012 End Date: 3/29/2012 Show only mine

Start Time	Scheduled by	Description	Progress	Recurrence	Status
3/29/2012 10:08:47 AM	User, System	Phone Book Source update All Systems	100% Event successful	Every 5th minute	✓

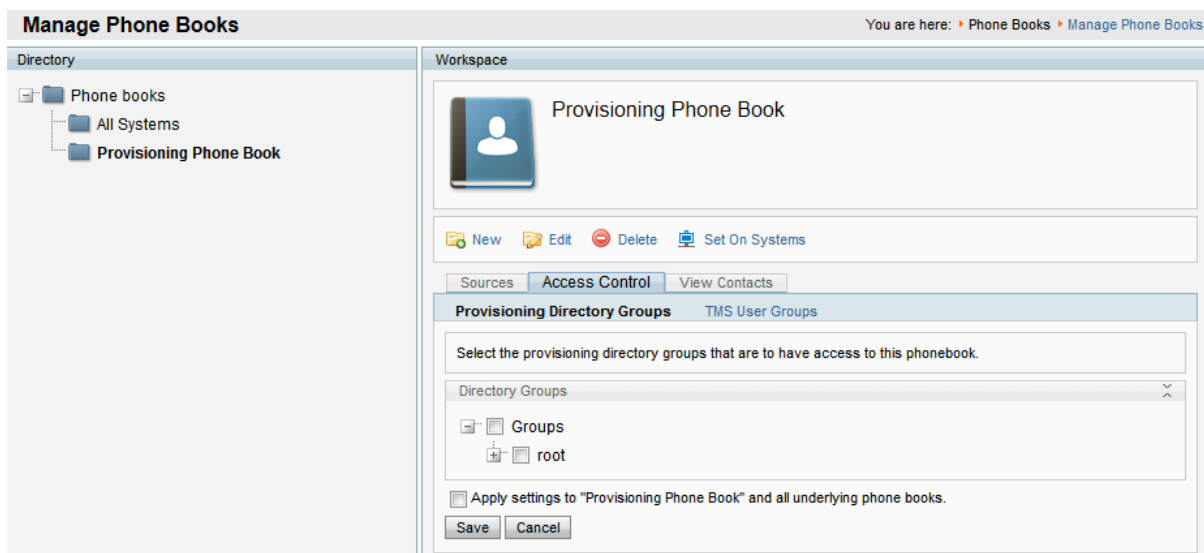
1 Records per Page 20 Displaying page 1 of 1

グループへの電話帳の関連付け

各ユーザ グループで 1 つ以上の電話帳を利用可能にします。

グループに電話帳アクセスを関連付けるには、次の手順に従います。

1. Cisco TMS で [Phone Books] > [Manage Phone Books] に移動し、[Directory] ペインで、目的の電話帳をクリックします。
指定されたプロビジョニング電話帳に関する情報は [ワークスペース (Workspace)] ペインに表示されます。
2. [ワークスペース (Workspace)] ペインで、[アクセス制御 (Access Control)] タブをクリックします。



3. [プロビジョニング ディレクトリ グループ (Provisioning Directory Groups)]をクリックし、選択された電話帳へのアクセス権を持つことになるユーザをクリックします。ルート グループを展開してサブグループを表示します。
4. すべての基盤となるの電話帳へのアクセスも許可する場合は、[<phone_book> および基盤となるすべての電話帳に設定を適用します (Apply settings to <phone_book> and all underlying phone books)]を選択します。
5. [保存 (Save)]をクリックします。

[<phone_book> および基盤となるすべての電話帳に設定を適用します (Apply settings to <phone_book> and all underlying phone books)]を使用するとアクセス権は継承されますが、これは既存の電話帳のみ適用されるものであり、この手順を実行した後に作成された電話帳には適用されません。したがって新しい電話帳を作成するときは、アクセス コントロールは常に指定されている必要があります。

電話帳の要求処理

プロビジョニングされたデバイスからの電話帳の要求は、そのデバイスをプロビジョニングしたものと同一 Cisco VCS またはクラスターで処理される必要があります。電話帳の要求が、異なるプロビジョニング対応 VCS に送信された場合、その要求は失敗し、そのデバイスで電話帳を使用可能にできません。

アカウント情報の設定および送信

ユーザへのアカウント情報の配信を簡素化するために、Cisco TMSPE では、設定可能な電子メール テンプレートを使用した電子メール機能を提供します。この機能は、FindMe などの機能で使用するためのプロビジョニング アカウント設定およびアカウント詳細を、個々のユーザまたはグループに通知するために使用できます。

電子メールの設定

電子メールを設定するには、次の手順に従います。

1. Cisco TMS で、[Administrative Tools]> [Configuration] > [Provisioning Extension Settings] に移動します。

Account Information Email

Sender Address *

Subject *

Body *

```
{display_name}:
Below is your provisioning account information:

Username: {username}
Password: {password}
```

SMTP Hostname *

SMTP Port *

SMTP Username

SMTP Password

Save Cancel Restore Default

- [アカウント情報電子メール(Account Information Email)]ペインで、次のようにフィールドを設定します。

差出人アドレス (Sender Address)	電子メール通知を送信するときの送信者の電子メール アドレスとして Cisco TMSPE が使用する電子メール アドレス。アドレスは、受信者の電子メール クライアントの [差出人 (From)]フィールドに表示されます
件名 (Subject)	電子メール通知の件名。件名は、受信者の電子メール クライアントの [件名 (Subject)]行に表示されます。
本文 (Body)	ユーザに送信される電子メールの本文を決めるテンプレート。例については、上記のスクリーンショットを参照してください。 FindMe を使用する場合は、次の追加情報を追加することを推奨します。 You can be contacted via your FindMe ID: {video_address}
SMTP ホスト名 (SMTP Hostname)	SMTP (メール) サーバの IP アドレスまたはホスト名。
SMTP ポート (SMTP Port)	SMTP (メール) サーバによって使用されるポート番号。
SMTP ユーザ名 (SMTP Username)	メール サーバにアクセスするために必要になったら使用するユーザ名
SMTP パスワード (SMTP Password)	メール サーバにアクセスするために必要になったら使用するパスワード名。

- [User Repository]の下で、[Enable automatic email sending to imported users]を選択するかどうかを決めます。
デフォルトでは、[No]に設定されています。

4. [保存 (Save)]をクリックします。

Active Directory からユーザをインポートし、自動電子メールの送信を有効にする場合は、次の手順に従う必要はありません。

単一のユーザへの情報の送信

大きなユーザ グループにアカウント情報を送信する前に、単一のユーザ(たとえば自分のアカウント)にアカウント情報を送信することを推奨します。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ (Users and Groups)]コンテナで、自分のユーザ名およびその他の適切なテストメールの受信者をクリックします。選択したユーザに関する情報が複数のペインに表示されます。

Name	Pattern	Origin
Video Address	firstname.lastname@example.com	example_group
Caller ID		root
Device Address	firstname.lastname.{device.model}@example.com	example_group
Image URL		root

3. [ユーザ設定 (User Settings)]ペインの上の領域で、[アカウント情報の送信 (Send Account Information)]をクリックします。
電子メールの送信がスケジュールされたことを確認するメッセージが表示されます。
電子メール サーバの設定によっては、スケジュールされた電子メールは数分内に指定した受信者の受信トレイに到着します。電子メールが配信されなかったら、[診断 (Diagnostics)]ページの [アラーム (Alarms)]ペインを確認してください。「[Cisco TMSPE 診断の実行 \[p. 65\]](#)」を参照してください。

グループ内のすべてのユーザへのアカウント情報の送信

グループに通知することを選択した場合、Cisco TMSPE は、そのグループのユーザだけでなく、サブグループのすべてのユーザにも通知します。

アカウント情報をグループに送信するには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ (Users and Groups)]コンテナで、目的のグループをクリックします。選択したグループに関する情報が複数のペインに表示されます。

example_group

Rename Group... Delete Send Account Information Move Group Toggle Details

User Settings

Name	Pattern	Origin
Video Address Pattern	{first_name}.{last_name}@example.com	example_group
Caller ID Pattern	{mobile_phone}	example_group
Device Address Pattern	{username}.{device.model}@example.com	example_group
Image URL Pattern		root

Edit Reload

3. [ユーザ設定 (User Settings)] ペインの上の領域で、[アカウント情報の送信 (Send Account Information)] をクリックします。確認用のプロンプトが表示されます。

Send account information email to all users in this group and its subgroups?

Yes No

4. グループ内のすべてのユーザがアカウント情報を送信するかどうかを確認します。電子メールの送信がスケジュールされたことを確認するメッセージが表示されます。電子メールが配信されなかったら、[診断 (Diagnostics)] ページの [アラーム (Alarms)] ペインを確認してください。「[Cisco TMSPE 診断の実行 \[p. 65\]](#)」を参照してください。

後日追加されたユーザにアカウント情報を送信するには、インポートされたユーザへの電子メールの自動送信がイネーブルになっていない場合は、「[単一のユーザへの情報の送信 \[p. 38\]](#)」

Smart Scheduler の導入

Smart Scheduler は Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA) を使用した Cisco TMS の予約にスマートでクリーンなインターフェイスです。これは、FindMe ユーザ ポータルと同じポータル フレームワークを使用します。

レイアウトは拡張可能で、タッチ スクリーンが使いやすくなっています。

Smart Scheduler は、WebEx Enabled TelePresence ソリューションの一部であり、ユーザは WebEx の有無にかかわらずテレプレゼンス会議を設定できます。

ユーザは次の内容を予約できます。

- テレプレゼンス会議室
Cisco TMS の予約可能なシステムを直接スケジューリングできます。
- コールインの参加者
Cisco TMS 予約でサポートされていないシステムをコールインの参加者 (Cisco TMSPE としてプロビジョニングされたデバイスを含む) としてスケジューリングできます。

ベスト プラクティスと制限事項

Cisco TMS で作成された予約を Smart Scheduler を使用して変更しないことを強く推奨します。このインターフェイスは Cisco TMS の会議に選択されている可能性があるすべての機能とオプションをサポートしないからです。

具体的には次のとおりです。

- 一連の定例会議の例外は Smart Scheduler でサポートされません。変更は、すべてのインスタンスに適用されます。
- Smart Scheduler は Cisco TMS から追加されたコールインの参加者の名前を変更します。

予約の制限

Cisco TelePresence Management Suite Extension Booking API を介した予約には、次の制限があります。

- Cisco TMS の設定およびティアダウン バッファの使用は、サポートされていません。
- 参加者人数が最初の MCU の容量を超えたときの追加の MCU へのカスケードは、サポートされていません。
このようなシナリオをサポートするには、Cisco TMS のデフォルトの MCU として Cisco TelePresence Conductor を設定します。
- サービス ユーザがすべての予約を実行する場合、予約の権限はすべてのユーザで同じです。個々の権利および制限は無視されます。
- 過去から将来に会議を移動できません。

進行中の会議の変更

現在進行中の 1 つの会議を更新することはできますが、いつも失敗しないとは限りません。

次に例を示します。

- 開始時間を変更すると、会議が中断することがあります。
- 会議が WebEx をサポートしない MCU を使用している場合に、WebEx を追加できないことがあります。機能させるためには、会議を切断し、再ルーティングする必要があります。

インスタンスの進行中に、一連の定例会議を変更する場合：

- 開始時間を変更すると、一連の会議全体に適用され、進行中の会議が中断する可能性があります。
- その他の変更は次のインスタンスにのみ適用され、進行中の会議は例外としてマークされます。

Smart Scheduler へのユーザ アクセス

必要な証明書を持つユーザは Smart Scheduler にすぐに到達できます。

`http://<Cisco TMS server address>/tmsagent/tmsportal/#scheduler`

Cisco TMS をすでに使用しているユーザは、右上隅のポータル アイコンをクリックして、Smart Scheduler および FindMe に進むこともできます。



アクセス権と権限

Smart Scheduler へのアクセスは、Cisco TMS へのアクセスと同じように作用します。ユーザは次のいずれかを持っている必要があります。

- Cisco TMS Windows Server のローカル アカウント
- サーバが Active Directory を介して信頼するドメイン アカウント。サーバをドメインのメンバーにすることによって、すべての信頼ドメインのユーザは、既存の Windows クレデンシャルを自動的に使用できます。

すでに存在しない場合は、サイトにアクセスするときに、Cisco TMS ユーザが作成されます。

実際の予約は個々のユーザによって直接作成されませんが、インストール時に追加された Cisco TMSPE サービス ユーザが変わって作成されることに注意してください。このため、予約の権限はすべてのユーザで同じです。

Smart Scheduler にログインし、予約を作成するのに、このサービス ユーザを使用しないでください。

タイムゾーンの表示

予約は、ユーザのコンピュータで検出されたタイムゾーンを使用して作成されます。これらのタイムゾーンを表示するために、ユーザは Smart Scheduler の日時に移動できます。検出はタイムゾーンのルールセットに作用しますが、名前には作用しないことに注意してください。ユーザのタイムゾーンに表示される名前は正しく表示されない場合があります。

ここでは、ユーザは日時に対する好みの表示形式を設定できます。これは、ブラウザのクッキーに保存されます。

ユーザがタイムゾーンとは異なるコンピュータの時間を設定する場合、予約は設定されたコンピュータ時間ではなく、タイムゾーン情報に基づいて作成されることに注意してください。

WebEx の予約

Smart Scheduler を使用すると、ユーザは次の内容を予約できます。

- WebEx Enabled TelePresence 会議：WebEx とのテレプレゼンス。
- TelePresence のみの会議。

会議に WebEx を含めるオプションは、Smart Scheduler が WebEx Enabled TelePresence とともに設定されている場合、Cisco TMS 予約形式で使用できます(「[WebEx Enabled TelePresence 要件 \[p. 9\]](#)」を参照)。

ユーザを容易に追加したり、管理したりできるように、Cisco TMS および WebEx にシングル サインオンを導入することを強く推奨します。

非 SSO シナリオでは、WebEx で予約される各 Cisco TMS/Smart Scheduler ユーザに、WebEx ユーザ名とパスワードを手動で追加する必要があります。管理者はこれを Cisco TMS に追加できます。または、ユーザは Smart Scheduler 設定を介してクレデンシャル自体を追加できます。

Smart Scheduler の機能

1. ドメイン ユーザが Smart Scheduler にサインインし、会議を予約するときに、要求が Cisco TMS に渡されます。
2. この通信は、Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA) を通過します。
3. Cisco TMSPE のインストール中に入力された Cisco TMS ユーザは、Smart Scheduler のサービス ユーザです。このユーザは、Cisco TMS ユーザに代わりに、Cisco TMSPE の予約を作成します。Cisco TMSPE ユーザが Cisco TMS にすでに存在しない場合は、予約時に作成されます。
4. 予約が完了すると、Cisco TMS は会議を予約したユーザに確認メールを送信します。ルート、スケジューリングされたシステム、WebEx 情報などの会議の詳細を含むメッセージがその後、他の会議参加者に転送される可能性があります。
予約が作成または更新されると、Cisco TMS も Smart Scheduler のサービス ユーザに電子メールを送信します。サービス ユーザおよび電子メールを受信しないように設定する方法の詳細については、「[Cisco TMS のユーザ名およびパスワード \[p. 8\]](#)」を参照してください。

FindMe の導入

FindMe は Cisco TMSPE に統合されていますが、オプションの部分です。プロビジョニングおよび FindMe は別々または同時に導入できます。FindMe も、いつでも Cisco TMSPE の導入に追加できます。

FindMe の基礎

FindMe は、誰かがユーザの FindMe ID をコールしたときにどのエンドポイント（ビデオおよびオーディオのみ）を呼び出すかを指定する機能を提供します。FindMe はまた、いずれかのプライマリ デバイスがビジー状態の場合にコールされるフォールバック デバイスを指定したり、すべてのプライマリ デバイスが応答されない場合にコールされるフォールバック デバイスを指定したりできるようにします。

FindMe の重要な機能は、管理者が、着信側のエンドポイントに表示される発信者 ID を、発信者のエンドポイントの ID ではなく、発信者の FindMe ID に設定できることです。つまり、そのコールが戻されるときには FindMe ID に戻され、元のコールを行った時のエンドポイントだけが呼び出されるのではなく、そのユーザのアクティブな FindMe ロケーションのすべての電話が呼び出されます。

プロビジョニングを行わない FindMe の導入

Cisco TMSPE では、プロビジョニングを行わない FindMe 機能も使用できます。本章で説明する手順を開始する前に、次の設定手順を実行しておくことが推奨されます。

1. グループを作成し、外部ソースからユーザをインポートするか、または手動で追加します。「[グループの作成とユーザの追加 \[p. 22\]](#)」を参照してください。これらのグループは、ビデオ アドレス パターンが設定され（次のステップを参照）、FindMe がイネーブルにされたときに FindMe に自動的に追加されます。
2. ビデオ アドレス パターンをこれらのグループに割り当てます。「[アドレス パターンの作成 \[p. 26\]](#)」を参照してください。このパターンは、各ユーザの FindMe ID を生成するために使用されます。これは、ユーザがあらゆるデバイスでコールを受信することができるようにするためのビデオ アドレスです。FindMe ID は、SIP URI、H.323 ID、または E.164 番号になります。

FindMe アカウントおよびグループは手動で追加できますが、このようなユーザは FindMe にアクセスできないため注意してください。そのため、手動アカウントは、ポータルへのアクセスを必要としないグループ アカウントおよびその他のユーザにのみ使用することを推奨します。個人およびグループの FindMe アカウントの詳細については、「[FindMe の個人タイプとグループ タイプ \[p. 57\]](#)」を参照してください。

発信者 ID パターンの定義

発信者 ID パターンは、各ユーザのコールバック番号を生成するために使用されます。このコールバック番号は、FindMe コールが ISDN ゲートウェイを介してルーティングされている場合に使用されます。これにより、発信者がテレプレゼンス エンドポイントを使用している場合でも、電話に着信を受けたユーザは、ビデオ アドレスではなくコールバック番号を確認できます。

発信者 ID のインポートされたアカウントへの割り当て

この手順は、[Users] ページからインポートされた FindMe アカウントに対してのみ適用されます。手動で作成された FindMe アカウントについては、アカウントの作成中または編集時に、FindMe ID と発信者 ID を定義します。「[手動で FindMe のアカウントとグループを追加する \[p. 45\]](#)」を参照してください。

発信者 ID パターンを割り当てるには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ(Users and Groups)]コンテナで、ビデオ アドレス パターンを割り当てるグループまたはユーザをクリックします。選択したグループまたはユーザに関する情報が、ペインの数の下に表示されます。
3. [ユーザ設定(User Settings)]ペインで [編集(Edit)]をクリックします。[ユーザ設定(User Settings)]ダイアログボックスが開きます。

User Settings ✕

Settings configured at the group level are inherited by all users and subgroups. Configure settings at the user level to apply them to one user only.

(Click for help on configuring each individual field.)

Name	Pattern	Origin
<input checked="" type="checkbox"/> Video Address Pattern	<input type="text" value="{first_name}.{last_name}@example.com"/>	example_group
<input type="checkbox"/> Caller ID Pattern	<input type="text"/>	example_group
<input checked="" type="checkbox"/> Device Address Pattern	<input type="text" value="{username}.{device.model}@example.com"/>	example_group
<input type="checkbox"/> Image URL Pattern	<input type="text"/>	root

4. [Caller ID Pattern]フィールドで、選択したグループ内のユーザのコールバック番号を定義する際に、Cisco TMSPE が使用するパターンを指定するか、選択したユーザに対するコールバック番号を指定します。
パターンでは、次のユーザ属性を任意に使用できます。
 - {office_phone}
 - {mobile_phone}
5. [OK]をクリックします。

example_group

Rename Group...
 Delete
 Send Account Information
 Move Group
 Toggle Details

User Settings

Name	Pattern	Origin
Video Address Pattern	{first_name}.{last_name}@example.com	example_group
Caller ID Pattern	{mobile_phone}	example_group
Device Address Pattern	{username}.{device.model}@example.com	example_group
Image URL Pattern		root

Edit
 Reload

発信者 ID パターンの例

- {office_phone}

次に、パターンでどのように regex 置換を使用できるかについての例を示します。

- {office_phone ['-'=' ', '¥+'=' ', ' '=']}
この置換により、不要な文字が削除されます。

FindMe のイネーブル化、対象: Cisco TMSPE

Cisco TMSPE で FindMe をイネーブルにすると、プロビジョニング ユーザは FindMe のアカウント ビューにインポートされます。FindMe をイネーブルにする前に、FindMe に含めるすべてのグループおよびユーザのビデオ アドレス パターンを定義してください。

- グループは、ビデオ アドレス パターンを定義していなければ追加されません。
- ビデオ アドレスを持たないユーザは、手動で設定したのもでも、グループのビデオ アドレス パターンをベースにしたものでも、追加されません。

ビデオ アドレス パターンに関する詳細については「[アドレス パターンの作成 \[p. 26\]](#)」を参照してください。

FindMe をイネーブルにするには:

1. Cisco TMS で、[Administrative Tools]> [Configuration] > [Provisioning Extension Settings] に移動し、[FindMe] ペインにスクロール ダウンします。

FindMe

2. [Enable SSO] を [Yes] に設定します。
3. [プロビジョニング済みデバイス (Provisioned Devices)] フィールドで、使用できるオプションの中から、目的のプロビジョニング済みデバイスの処理方法を 1 つ選択します。

ユーザのアクティブなロケーションのデフォルト デバイスとして設定する (Set as default device for user's active location)	デバイスがプロビジョニングされたら、それをプロビジョニング済みユーザの FindMe アカウントのデバイス リストに追加し、現在アクティブなロケーションの初期デバイスとして呼び出すように設定します。
ユーザのデバイス リストに追加 (Add to user's device list)	デバイスがプロビジョニングされたら、それをプロビジョニング済みユーザの FindMe アカウントのデバイス リストに追加します。
含めない (Do not include)	デバイスはプロビジョニング済みのため、プロビジョニング済みユーザの FindMe アカウントには追加しません。

4. [保存 (Save)] をクリックします。
5. 「[TMS プロビジョニング拡張機能 Windows サービスの再起動 \[p. 66\]](#)」の説明に従って、TMS プロビジョニング拡張機能 Windows サービスを再起動します。これは、FindMe をイネーブルまたはディセーブルするときに実行する必要があります。

FindMe をイネーブルにすると、Cisco TMS Web インターフェイスの右上隅にある、各ユーザの FindMe ポータルにリンクするアイコンがアクティブになります。

FindMe ポータルの URL は、ご使用の Cisco TMS インストール環境の URL に、`/tmsagent/portal/` を追加したものです。

手動で FindMe のアカウントとグループを追加する

FindMe アカウントおよびグループは手動で追加できますが、このようなユーザは FindMe にアクセスできないため注意してください。そのため、手動アカウントは、ポータルへのアクセスを必要としないグループ アカウントおよびその他のユーザにのみ使用することを推奨します。個人およびグループの FindMe アカウントの詳細については、「[FindMe の個人タイプとグループ タイプ \[p. 57\]](#)」を参照してください。

FindMe グループを追加するには、次の手順を実行します。

1. Cisco TMS で、[Systems] > [Provisioning] > [FindMe]に移動します。
2. [アカウントとグループ(Accounts and Groups)]コンテナで、作成するグループの親をクリックします。
3. エクスプローラ ビューの上で、[グループを追加(Add Group)]をクリックします。
[グループを追加(Add Group)]ダイアログボックスが表示されます。
4. [表示名(Display Name)]フィールドにグループ名を入力します。
5. [保存(Save)]をクリックします。

FindMe アカウントを追加するには、次の手順を実行します。

1. Cisco TMS で、[Systems] > [Provisioning] > [FindMe]に移動します。
2. [アカウントとグループ(Accounts and Groups)]コンテナで、アカウントを追加するグループに移動します。
3. エクスプローラ ビューの上で、[アカウントを追加(Add Account)]をクリックします。
[アカウントを追加(Add Account)]ダイアログボックスが表示されます。
4. 次のようにフィールドを設定します。

表示名(Display Name)	アカウントの表示名。
ユーザ名(Username)	アカウントのユーザ名。
FindMe アドレス(FindMe Address)	アカウントの FindMe ID。
発信者 ID(Caller ID)	FindMe コールが ISDN ゲートウェイを通じてルーティングされるときに使用されるコールバック番号
アカウントの種類(Account Type)	[個人(Individual)]または[グループ(Group)]を選択します。

FindMe ロケーションおよびデバイスの設定

FindMe ユーザが FindMe User Portal にアクセスしたときに、ロケーションおよびデバイスをそのユーザに提供するには、FindMe のロケーションおよびデバイス テンプレートを作成します。提供した情報は、構成済み VCS に渡されて使用されます。

FindMe のロケーションおよびデバイスを設定するには、次の作業を実行します。

1. [FindMe デバイス テンプレートの追加 \[p. 47\]](#)
2. [FindMe ロケーション テンプレートの追加 \[p. 48\]](#)
3. [デバイス テンプレートとロケーション テンプレートの関連付け \[p. 49\]](#)
4. [ロケーション テンプレートのグループへの割り当て \[p. 50\]](#)
5. [FindMe ロケーションおよびデバイスの再作成 \[p. 54\]](#)

推奨される最小設定

FindMe の最小設定では、次の方法を実行することを推奨します。

1. [プロビジョニング済みデバイスを含める(Include Provisioned Devices)]フィールドを [ユーザのアクティブなロケーションのデフォルト デバイスとして設定する(Set as default device for user's active location)]に設定した状態で、FindMe をイネーブルにします。このオプションによって、ユーザがログインしてデバイスをプロビジョニングすると、関連するアカウントの FindMe ポータルにデバイスが追加されるようになります。また、初期デバイスはアクティブなロケーションで呼び出し音を鳴らすように設定されます。[「FindMe のイネーブル化、対象: Cisco TMSPE \[p. 45\]」](#)を参照してください。

- たとえば **Office** のような名前の 1 つのロケーション テンプレートを定義し、デフォルトの呼び出し時間の 5 秒を受け入れます。「[FindMe ロケーション テンプレートの追加 \[p. 48\]](#)」を参照してください。
- グループ階層の最上位にあるグループにロケーションのテンプレートを割り当てます。「[ロケーション テンプレートのグループへの割り当て \[p. 50\]](#)」を参照してください。

FindMe デバイス テンプレートの追加

FindMe ユーザへの接続に使用される、各エンドポイント タイプのデバイス テンプレートを追加します。

FindMe デバイス テンプレートを追加するには、次の手順に従います。

- Cisco TMS で [Systems]> [Provisioning] > [FindMe] に移動し、[Device Templates] コンテナをクリックします。1 つ以上のデバイス テンプレートがすでに追加されている場合は、エクスプローラ ビューに表示されます。テンプレートが存在しない場合は、次が表示されます。



[Click to add a template](#)

- エクスプローラ ビュー上で、[デバイス テンプレートを追加 (Add Device Template)] をクリックします。[デバイス テンプレートを追加 (Add Device Template)] ダイアログボックスが表示されます。

Add Device Template ✕

Display Name:

Device Type:

Device Address Pattern:

3. 次のようにフィールドを設定します。

表示名 (Display Name)	FindMe デバイス名 (例 : E20) 。
デバイスの種類 (Device Type)	表示される画像。次の中から選択します。 <ul style="list-style-type: none"> ビデオ エンドポイント (Video Endpoint) 電話機 (Telephone) 携帯電話 (Mobile Phone) ラップトップ (Laptop) 人 (Person) ボイス メール (Voice Mail) <p>メッセージが正しいボイス ボックスに録音されるようにするには、ボイスメールシステムではこのデバイス タイプを選択する必要があります。この設定により、Diversion ヘッダーに元の着信側に関する情報が含まれるようになります。</p> <ul style="list-style-type: none"> ビデオ メール (Video Mail) グループ (Group)
デバイス アドレス パターン (Device Address Pattern)	デバイスのアドレスまたは番号を作成するために使用するパターン (例 : {username} .e20@example.com) 。

4. [保存 (Save)]をクリックします。

FindMe ロケーション テンプレートの追加

FindMe ユーザが使用可能なエンドポイント デバイスは、現在のロケーションによって異なる場合があります。この違いを表すようにロケーション テンプレートを追加できます。

たとえば、「自宅」または「オフィス」などの異なる物理的ロケーションを表すだけでなく、「休暇中」または「会議中」などの異なる状況を表すことができます。

FindMe ロケーション テンプレートを追加するには、次の手順に従います。

1. Cisco TMS で [Systems] > [Provisioning] > [FindMe] に移動し、[Location Templates] コンテナをクリックします。1 つ以上のロケーション テンプレートがすでに追加されている場合は、エクスプローラ ビューに表示されます。テンプレートが存在しない場合は、次が表示されます。



[Click to add a template](#)

2. エクスプローラ ビュー上で、[ロケーション テンプレートを追加 (Add Location Template)]をクリックします。[ロケーション テンプレートを追加 (Add Location Template)]ダイアログボックスが表示されます。

Add Location Template
×

Display Name:

Ring Duration: ▼

3. 次のようにフィールドを設定します。

表示名 (Display Name)	FindMe ロケーション名 (例 : 自宅、ホーム オフィス、出張中) ユーザが FindMe を設定したときに、これが FindMe ロケーションとして表示されます。
呼び出し時間 (Ring Duration)	この設定は、現在のロケーションにあるデバイスが着信したときの呼び出し時間の長さ (秒単位) を設定します。この時間を過ぎると、コールは代替宛先に転送されるか (通話中または応答なしの場合 (設定されている場合))、またはクリアされます。

4. [保存 (Save)]をクリックします。

デバイス テンプレートとロケーション テンプレートの関連付け

追加する各ロケーション テンプレートについて、ユーザの FindMe アドレスに対して接続が行われたときに、必ずデフォルトでダイヤルされるデバイスを、少なくとも 1 台指定する必要があります。

また、次の場合にダイヤルするデバイスも指定できます。

- 指定されたデフォルトのデバイスが通話中の場合。
- 設定されたロケーションの呼び出し時間内に応答がない場合。

デバイスとロケーションを関連付けるには、次の手順に従います。

1. Cisco TMS で [Systems] > [Provisioning] > [FindMe] に移動し、[Location Templates] コンテナをクリックしてから、エクスプローラ ビューでデバイス テンプレートを割り当てるロケーション テンプレートをクリックします。

2. [デバイス テンプレート (Device Templates)]ペインで、[テンプレートの割り当て (Assign Templates)]をクリックします。[デバイス テンプレートの構成 (Configure Device Templates)]ダイアログボックスが開きます。

Configure Device Templates



Name	Default Device	Busy Device	No Answer Device
Cisco IP Video Phone E20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Jabber Video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mobile	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 該当するチェックボックスを次から 1 つ以上選択して、デバイスを登録します。
 - [デフォルト (Default)] : このロケーションがアクティブな場合に最初に呼び出されるデバイス。
 - [ビジー (Busy)] : デフォルトのデバイスが通話中の場合に呼び出すデバイス。
 - [応答なし (No Answer)] : デフォルトのデバイスが応答しない場合に呼び出すデバイス。
 通話中、応答なしは、相互に転送されないことに注意してください。デフォルトのデバイスが通話中または応答なしの場合のみ、自動的に転送されます。
- [保存 (Save)] をクリックします。

The screenshot shows the 'Office' location template configuration in the FindMe console. The 'Device Templates' section is expanded, showing a table with the following data:

Name	Default Device	Busy Device	No Answer Device
Cisco IP Video Phone E20	✓		
Jabber Video		✓	
Mobile			✓

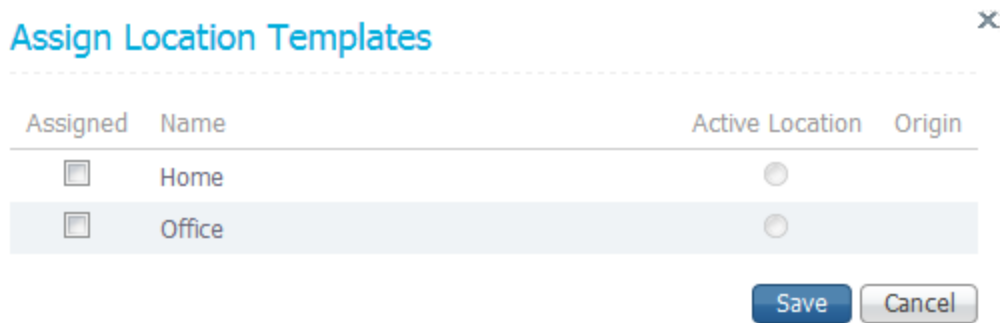
Below the table, there is an 'Assign Templates...' button. The 'Assigned Groups' section shows a message: 'This location template is not in use by any groups. Assign it to a group in the groups pane.'

ロケーション テンプレートのグループへの割り当て

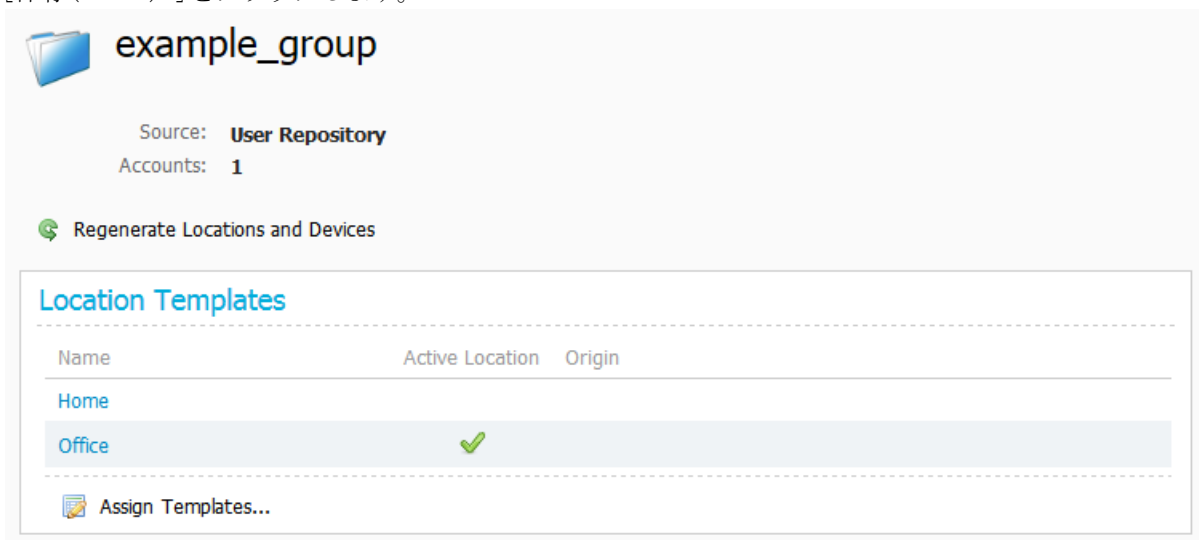
ロケーション テンプレートをグループに割り当て、グループのロケーションとデバイスを再作成することでそのテンプレートを適用した場合、情報は設定済みの VCS に渡され、使用されます。ロケーション テンプレートは、グループ内のすべてのユーザが次回ユーザ ポータルにアクセスしたときに、グループ内のすべてのユーザに対して表示されます。ロケーションは、サブグループのすべてのユーザに継承されます。

ロケーションをグループに割り当てるには、次の手順に従います。

- Cisco TMS で [Systems] > [Provisioning] > [FindMe] に移動し、[Accounts and Groups] コンテナをクリックします。
- エクスプローラ ビューで、ロケーションを割り当てるグループをクリックします。
- [ロケーション テンプレート (Location Templates)] ペインで、[テンプレートの割り当て (Assign Templates)] をクリックします。[ロケーション テンプレートの割り当て (Assign Location Templates)] ダイアログボックスが表示されます。



4. [割り当て済み (Assigned)]カラムで、グループに割り当てる各ロケーションをチェックします。
5. [アクティブなロケーション (Active Location)]カラムで、オプション ボタンを使用してグループのユーザのデフォルトのアクティブなロケーションを示します。
6. [保存 (Save)]をクリックします。



7. [ロケーションおよびデバイスを再作成... (Regenerate Locations and Devices...)] をクリックして、現在のグループのすべてのアカウントおよびサブグループにテンプレートを割り当てます。詳細については、「[FindMe ロケーションおよびデバイスの再作成 \[p. 54\]](#)」を参照してください。

単一のユーザまたはアカウントにテンプレートを直接割り当てることができない場合は、そのユーザまたはアカウントの代理として FindMe ポータルにアクセスし、ロケーションおよびデバイスを変更できます。「[ユーザの FindMe ロケーションおよびデバイスの変更 \[p. 55\]](#)」を参照してください。

Cisco VCS の設定、対象: FindMe

ユーザの FindMe ID と関連付けられたデバイスにコールをルーティングできるように、Cisco VCS で FindMe 機能が有効になっている必要があります。

FindMe オプション キーのチェック

Cisco VCS に FindMe のオプション キーがインストールされていることを確認します ([Maintenance] > [Option keys])。インストールされていない場合は、リセラーに問い合わせてキーを取得してください。

クラスタ名のセットアップ

FindMe を使用するときには、クラスタの一部であるかどうかに関係なく、クラスタ名で Cisco VCS をセットアップする必要があります。

クラスタ名を設定または変更するには以下を行います。

1. [VCS 設定(VCS configuration)] > [クラスタリング(Clustering)]に移動します。
2. クラスタ名を入力します。
 - Cisco VCS がクラスタの一部である場合は、クラスタのアドレスを指定する SRV レコードで使用されている完全修飾ドメイン名に指定します(「cluster1.example.com」など)。
 - Cisco VCS がクラスタの一部ではない場合は、Cisco VCS のアドレスを指定する SRV レコードで使用されている完全修飾ドメイン名に指定します(「vcs1.example.com」など)。
3. [保存(Save)]をクリックします。

FindMe 設定の有効化と設定

FindMe を Cisco VCS 上で有効にし、設定するには以下を行います。

1. [FindMe configuration]ページ([Applications] >[FindMe] > [Configuration]) に移動します。
2. [FindMe mode]をオンに設定します。
3. [Caller ID]を FindMe IDに設定することを推奨します。次のオプションがあります。
 - [FindMeID] : この Cisco VCS 経由で作成されているコールの発信者 ID は、関連する FindMe ID に置き換えられます。
 - [IncomingID]] : 発信者 ID は変わりません。着信側エンドポイントに提供された発信者 ID が、発信したエンドポイントの ID です。
 発信者 ID と FindMe ID の使用の詳細については、[「FindMe ID で発信者 ID を上書きする方法の決定 \[p. 56\]」](#)を参照してください。
4. [Save]をクリックします。

The screenshot shows the 'FindMe configuration' page in the Cisco VCS web interface. The breadcrumb trail is 'You are here: Applications > FindMe > Configuration'. The configuration table is as follows:

Configuration	
FindMe mode	On
Caller ID	FindMe ID
Cluster name (FQDN for Provisioning)	my.fqdn.example.com

A 'Save' button is located at the bottom left of the configuration area.

ISDN ゲートウェイを使用したコールの送信および返信

ここでは、FindMe で ISDN ゲートウェイ経由でルーティングされたコールを処理する方法について説明します(たとえば、携帯電話またはその他の ISDN でアクセス可能な宛先を呼び出すとき)。

Cisco VCS で、発信者ID([Applications] > [FindMe] >[Configuration]) がFindMe ID を使用するように設定されている場合、表示される発信者 ID はユーザの E. 164 電話番号になります。E. 164 電話番号は、ユーザ アカウントが作成されたときに手動で入力されたものであるか、または Cisco TMS により AD プロビジョニング済みユーザのアカウントが作成された場合は、AD により(オフィスの電話番号から) 指定されたものです。

着信側がコールを返す(および、E. 164 番号をビデオ ネットワークの ISDN ゲートウェイにネットワークによってルーティングする) 場合、コールは ISDN ゲートウェイで受信され、E. 164 電話番号を着信番号として Cisco VCS に転送されます。

Cisco VCS はこのため、ユーザのエンドポイントをコールできるように、このコールを関連する FindMe ID にルーティングするように設定される必要があります。これは、別の FindMe エントリを使用するか、または ENUM を設定することによって実行できます。

FindMe を使用した E.164 番号の FindMe ID への変換

この方法では、E.164 着信番号を URI にリダイレクトするために、追加の FindMe アカウントを使用します。

URI 形式または H.323 ID の FindMe ID と、関連する E.164 電話番号の両方を持つ各ユーザについて、次の内容で第 2 のユーザ アカウントを設定します。

- [ユーザ名 (Username)] (例: **123456-name.surname**)
- ユーザの E.164 電話番号に設定された [FindMe ID]
- メイン アカウントの FindMe ID に設定された [プリンシパル デバイス アドレス (Principal device address)]

これはスタティック マッピングのため、ユーザはこの第 2 の (E.164) アカウントにログインする必要はありません。そのユーザに関連付けられたデバイスの変更は、メイン アカウントから行うことができます。

ENUM を使用した E.164 番号の FindMe ID への変換

ENUM を使用することで、着信 E.164 番号を ENUM サーバで検索し、その番号に関連付けられた URI にコールを転送できます。

ENUM 変換を使用するためには、FindMe の各アカウントについて DNS サーバの ENUM アドレスとして電話番号を設定し、そのアドレスをそのアカウントの FindMe ID にマッピングする必要があります。

ENUM の設定と実装の詳細については、『*ENUM dialing on Cisco VCS Deployment Guide*』で説明されています。

発信者 ID に ISDN ゲートウェイプレフィックスを含める方法

発信者 ID に ISDN ゲートウェイプレフィックスを含めるように Cisco VCS を設定すると、ISDN ゲートウェイ経由で受信された PSTN/ISDN コールを返すことが簡単になります。

ゲートウェイ発信者 ID を Cisco VCS で設定するには

1. [H.323] ページ ([VCS 設定 (VCS configuration)] > [プロトコル (Protocols)] > [H.323]) に移動します。
2. 必要に応じて、[ゲートウェイ発信者 ID (Gateway caller ID)] を設定します。次のオプションがあります。
 - [プレフィックスを含める (Include prefix)] : 受信側の電話に表示される発信者 ID が、ISDN ゲートウェイのプレフィックスが、発信者の電話番号の先頭にプレフィックスとして追加された番号になります。これにより、受信者は番号を選択し、返信コールを押すことでこのコールに直接折り返すことができます (ただし、このプレフィックスを持つコールが、ISDN ゲートウェイにルーティングされるように、適切な検索ルールが設定されていることが条件です)。これは推奨オプションです。
 - [プレフィックスを除外する (Exclude prefix)] : 受信側の電話に表示される発信者 ID は、発信者の電話番号だけです。コールに折り返すには、この番号をリダイヤルするか、番号を編集してゲートウェイプレフィックスをこの番号のプレフィックスとして追加し、コールが電話回線網のゲートウェイにルーティングされるようにする必要があります。

Cisco VCS が E164 H.323 コールと相互作用する場合、その相互作用を行った VCS の IP アドレスに設定されたドメインで、発信者 ID を作成します。これらのコールのルーティングを処理するために適切な検索ルールが作成されているか、または **number@IPofVCS** を **number@LocalSipDomain** に変換するトランスフォームが実装されている必要があります。

FindMe ロケーションおよびデバイスの再作成

ロケーションおよびデバイス テンプレートを作成しても、[Regenerate Locations and Devices...] をクリックしてコマンドを発行するまで、変更内容は、影響を受ける FindMe には伝播しません。

次のように、いくつかのレベルでこのコマンドを発行できます。

レベル	説明
アカウント	ロケーションおよびデバイスは、そのアカウントで利用可能なテンプレートに基づいて、選択されたアカウントに対してのみ、再作成されます。 このオプションは、たとえばグループ レベルで再作成する前に、FindMe のロケーションおよびデバイス テンプレートに加えた変更の影響をテストする場合に役に立ちます。
グループ	ロケーションおよびデバイスは、選択したグループとサブグループのすべてのアカウントについて再帰的に再作成されます。 このオプションは、たとえばロケーションおよびデバイス テンプレートに加えた変更が、いくつかの特定のグループだけに影響がある場合に役立ちます。
ロケーションのテンプレート	ロケーションおよびデバイスは、ロケーション テンプレートが割り当てられているすべてのグループについて再帰的に再作成されます。再作成中に、ロケーション テンプレートに関連付けられたすべてのデバイス テンプレートも適用されます。 このオプションは、たとえば多数のグループに関連付けられたロケーション テンプレートに変更を加えた場合に役立ちます。
デバイス テンプレート	デバイスは、影響を受けるすべてのグループについて再帰的に再作成されます。変更は、既存のデバイスのテンプレートだけで考慮されます。新しいデバイス テンプレートは考慮されません。 このオプションは、たとえば多数のロケーション テンプレートにリンクした特定のデバイス テンプレートに変更を加え、多数のグループが影響を受ける場合に役立ちます。

注： FindMe のロケーションおよびデバイスの再作成は、バックグラウンドで実行されるプロセスであり、非常に大規模なユーザ ベースで実行する場合は最大 30 分かかります。そのため、最適な結果は [再作成 (Regenerate)] ボタンを一度だけクリックし、プロセスが完了するまで待つことで得られます。[再作成 (Regenerate)] ボタンを繰り返しクリックすると、複数のバックグラウンド プロセス要求が不必要に発行され、パフォーマンスに悪影響を及ぼす可能性があります。

アカウントとグループ

FindMe のロケーションおよびデバイスを、特定のアカウントに対して、またはグループとサブグループのすべてのアカウントに対して再帰的に再作成するには、次の手順に従います。

1. Cisco TMS で [Systems] > [Provisioning] > [FindMe] に移動します。
2. [アカウントとグループ (Accounts and Groups)] コンテナのエキスプローラ ビューで、目的のアカウント グループに移動します。
3. [場所 (Locations)] ペイン上部の詳細の領域で、[ロケーションおよびデバイスの再作成... (Regenerate Locations and Devices...)] をクリックします。
4. 次のいずれかをクリックして、ユーザがロケーションおよびデバイスに対しておこなった変更を、再作成の際に上書きするかどうかを選択します。
 - [はい (Yes)] : テンプレートを適用するときに、すべての既存のロケーションおよびデバイスが上書きされます。
 - [いいえ (No)] : ユーザの編集内容を削除または変更しないでテンプレートを適用します。

ロケーション テンプレート

テンプレートに関連付けられているすべてのアカウントについて、FindMe ロケーションを再帰的に再生するには、次の手順に従います。

1. Cisco TMS で [Systems]> [Provisioning] > [FindMe] に移動します。
2. [ロケーション テンプレート (Location Templates)] ペインをクリックしてから、エクスプローラ ビューで必要なロケーション テンプレートをクリックします。
3. [デバイス テンプレート (Device Templates)] ペイン上部の詳細の領域で、[ロケーションおよびデバイスの再作成... (Regenerate Locations and Devices...)] をクリックします。
4. 次のいずれかをクリックして、ユーザがロケーションおよびデバイスに対しておこなった変更を、再作成の際に上書きするかどうかを選択します。
 - [はい (Yes)] : テンプレートを適用するときに、すべての既存のロケーションおよびデバイスが上書きされます。
 - [いいえ (No)] : ユーザの編集内容を削除または変更しないでテンプレートを適用します。

デバイス テンプレート

テンプレートに関連付けられているすべてのアカウントについて、FindMe デバイスを再帰的に再生するには、次の手順に従います。

1. Cisco TMS で [Systems]> [Provisioning] > [FindMe] に移動します。
2. [デバイス テンプレート (Device Templates)] ペインをクリックしてから、エクスプローラ ビューで必要なデバイス テンプレートをクリックします。
3. [ロケーション テンプレート (Location Templates)] ペイン上部の詳細の領域で、[ロケーションおよびデバイスの再作成... (Regenerate Locations and Devices...)] をクリックします。
4. 次のいずれかをクリックして、ユーザがデバイスに対しておこなった変更を、再作成の際に上書きするかどうかを選択します。
 - [はい (Yes)] : テンプレートを適用するときに、既存のデバイスおよびユーザがおこなったアップデートが上書きされます。
 - [いいえ (No)] : ユーザの編集内容を削除または変更しないでテンプレートを適用します。

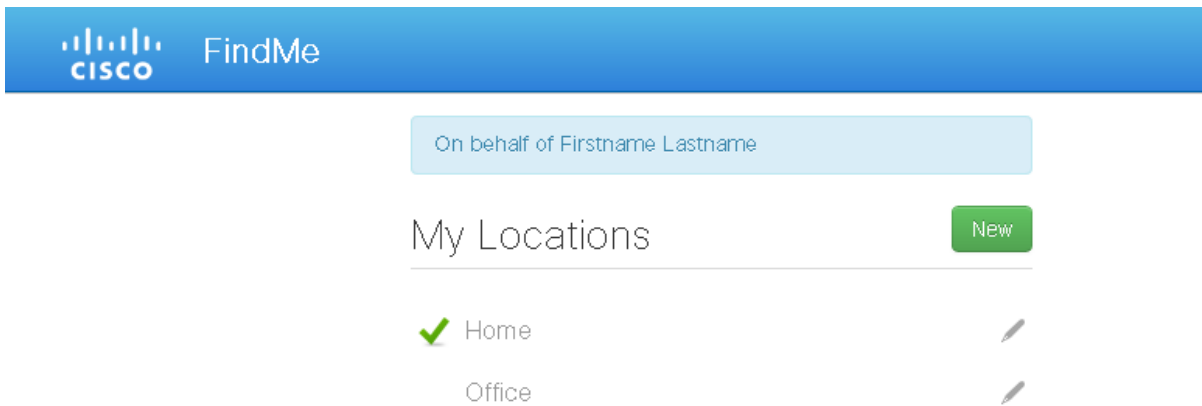
ユーザの FindMe ロケーションおよびデバイスの変更

単一のユーザまたはアカウントに、ロケーション/テンプレートを直接割り当てることはできません。ただし、ユーザが助けを求めている場合、または特別な設定を必要としている場合は、ユーザに代わって管理者が FindMe ポータルにアクセスし、ロケーションおよびデバイスを変更できます。

FindMe アカウントが手動で作成されたユーザは、FindMe ポータルにアクセスできません。ロケーションおよびデバイスは、この手順でしか変更できません。

ユーザの FindMe ロケーションおよびデバイスを変更するには、次の手順に従います。

1. [Systems]> [Provisioning] > [FindMe] に移動します。
2. [Accounts and Groups] コンテナを開き、変更する FindMe アカウントに移動します。
3. [FindMe ユーザ ポータルでの変更 (Edit in FindMe User Portal)] をクリックします。別のブラウザ タブまたはウィンドウで、ユーザ ポータルが開きます。



4. 必要に応じてロケーションを追加したり、その他の変更を行います。
5. 更新内容を保存し、ブラウザ タブを閉じます。ユーザではなく、管理者としてサインインしたままになるため、注意してください。

その他の情報

FindMe ID で発信者 ID を上書きする方法の決定

Cisco VCS は次の場合にのみ発信者 ID を FindMe ID で上書きすることができます。

- コール シグナリングが、FindMe アカウントをホストする Cisco VCS (または Cisco VCS クラスタ) を通過する場合。
- Cisco VCS が、エンドポイントの発信者 ID のオーナーとして FindMe を識別できる場合。これは、着信コールで提供された発信者 ID が次のいずれかに一致する場合に可能です。
 - FindMe の 1 つのアカウントだけで見つかる FindMe デバイス
 - 単一のプリンシパル FindMe デバイス (同じデバイス アドレスが FindMe の複数のロケーションに関連付けられている場合)

いずれかの条件が満たされていない場合、着信コールの発信者 ID は未変更で渡されます。

Cisco VCS クラスタ内の FindMe

FindMe を Cisco VCS クラスタで使用する場合、FindMe オプション キーがクラスタ内のすべての Cisco VCS ピアで有効になっている必要があります。FindMe データベースは、コールが経由するすべてのピア上で FindMe 機能が実行できるように、クラスタ内のすべてのピアに渡って複製されます。

Cisco VCS クラスタの詳細については、『*Cisco VCS Cluster Creation and Maintenance Deployment Guide*』を参照してください。

Microsoft Lync および Cisco VCS B2BUA

FindMe が、「Lync ゲートウェイ」Cisco VCS と一緒に使用される場合、クラスタ内の各ピアが FindMe ユーザの一部を Microsoft Lync に登録して、コール ロードがクラスタ ピア間で共有されるようにします (Lync から Cisco VCS へのコールは、ユーザを登録した Cisco VCS に Lync によって送信されます)。

詳細については、『*Microsoft Lync 2010 and Cisco VCS Deployment Guide*』を参照してください。

FindMe アカウント(ネットワーク内の別の Cisco VCS でホスト)

FindMe アカウントは複数の Cisco VCS(または Cisco VCS クラスタ) に渡って分散できますが、個々のアカウントは 1 つの Cisco VCS(または Cisco VCS クラスタ) でのみホストできます。

FindMe が発信者の FindMe ID で発信者 ID を上書きするには、コール シグナリングが、関連するアカウントをホストする Cisco VCS(または Cisco VCS クラスタ) を通過する必要があります。

したがって、発信者 ID を常に上書きすることができるように、システム トポロジの設計に注意する必要があります。

たとえば、2 人のユーザが Cisco VCS Control にアカウントを持っているが、両方のユーザが(Cisco VCS Control にトラバーサル ゾーンを持つ) Cisco VCS Expressway に登録されているエンドポイントで自宅勤務している場合があります。

- 1 人のユーザが他のユーザの FindMe ID を呼び出すと、それらのユーザの発信者 ID がそれらのユーザの FindMe ID で上書きされます。これは、コール シグナリングが、ユーザ アカウントがホストされている Cisco VCS Control を通過するためです。
- 1 人の発信者が他のユーザのエンドポイント URI を直接コールすると、コール シグナリングは Cisco VCS Control ではなく Cisco VCS Expressway を通過します。このシナリオでは、発信者 ID は FindMe ID で上書きされません。これは、シグナリングが Cisco VCS Control を通過しないためです(ユーザが個々のデバイス URI ではなく FindMe ID をコールすることが推奨されます)。

FindMe とプレゼンス

Cisco VCS は、ユーザの現在アクティブな FindMe ロケーションに関連付けられた各デバイスのプレゼンスを集約します。しかし、集約できるのは、関連する FindMe アカウントをホストする同じ Cisco VCS(または Cisco VCS クラスタ) に置かれた Presence サーバによって管理されているデバイスに対してだけです。

そのため、FindMe アカウントの管理に使用するのと同じ Cisco VCS(または Cisco VCS クラスタ) 上で Presence サーバを有効にすることを推奨します。

FindMe の個人タイプとグループタイプ

FindMe の各プロファイルは、個人またはグループに設定されます。

個別

個人モードでは、個々のユーザが一度に 1 台のデバイスでのみコールを受信できると想定します。

- 現在アクティブなロケーションにあるデバイスがビジー状態の場合、この FindMe ID へのコールは、すぐにオンビジー デバイスに転送されます。
- 現在アクティブなロケーションにあるどのデバイスもビジー状態でない場合、指定された呼び出し時間の後、コールは未応答デバイスにルーティングされます。

Group

グループモードでは、複数のユーザがこの FindMe にコールを受信できると想定します。

- 現在アクティブなロケーションにあるデバイスがビジー状態でない場合、ノンビジー デバイスが呼び出されます。現在アクティブなロケーションにあるすべてのデバイスがビジー状態の場合にのみ、コールはすぐにオンビジー デバイスに転送されます。
- 現在アクティブなロケーションにあるデバイスがビジー状態でない場合、指定された呼び出し期間の後、FindMe はコールを以下にルーティングします。
 - 現在アクティブなロケーションのデバイスがビジー状態の場合はオンビジー デバイス
 - 現在アクティブなロケーションのデバイスのすべてがビジー状態でない場合は未応答デバイス

SIP URI で許可される文字

次の文字セットが SIP URI で使用できます(詳細については、RFC 3261 で参照できます)。

a-z、A-Z、0-9、「-」、「_」、「.」、「!」、「~」、「*」、「'」、「(」、「)」、「&」、「=」、「+」、「\$」、「,」、「;」、「?」、「/」

その他の文字が必要な場合は、必須の文字の ASCII 値を表す 2 桁の 16 進数の前に「%」を使用して「エスケープ」する必要があります。

たとえば、「alice smith@example.com」は「alice%20smith@example.com」としてエンコードする必要があります（「%20」は空白文字を表します）。

FindMe の制限事項

FindMe デバイスとしての Microsoft Lync デバイス ID

コールを行うときにデバイスの独自のエンドポイント ID ではなく FindMe ID が発信者 ID として示されるように、発信者ID([Applications] > [FindMe] >[Configuration]) が FindMe ID を使用するよう設定されている場合、Lync デバイス ID をその FindMe のデバイスとして含めることはできません (Lync は、Cisco VCS が発信者 ID を FindMe ID として示す設定方法である、応答メッセージでの宛先名や送信者名の変更をサポートしません) 。

ビデオ エンドポイントと Lync デバイスを関連付けるには、Cisco VCS の B2BUA for OCS/Lync デバイスを有効にし、FindMe ID を Lync URI と同じにする必要があります。

Cisco VCS と Lync の設定の詳細については、『*Microsoft Lync 2010 and Cisco VCS Deployment Guide*』を参照してください。

Active Directory(AD)からの電話番号

Cisco TMS のユーザ アカウントが AD から作成された場合、[電話番号(Phone number)]は、AD のオフィスの電話番号を元に作成されます。

電話番号を ISDN ゲートウェイに対して有効にする場合(ISDN ゲートウェイがその電話番号を発信者 ID として使用する場合) 、ISDN ゲートウェイで、AD オフィス電話番号が受け入れ可能である必要があります。

これは通常、AD のオフィスの電話番号が次の条件を満たす必要があることを意味します。

- カッコ、スペース、ハイフンまたは他の数字以外の文字が含まれていない数値ストリング
- ネットワークによって ISDN ゲートウェイで終端するように設定された電話番号
- ISDN ネットワークの正しい形式であること。たとえば次のようなものです。
 - 国コードを含む完全な番号(例: 441189123456)
 - 市内番号(例: 123456)
 - 内線番号(例: 3456)

ISDN のサブライヤに受け入れ可能な形式を確認します。

ユーザとデバイスのメンテナンス

ここでは、プロビジョニング用に Cisco TMSPE を設定した後に実行することが必要になる可能性があるメンテナンス作業について説明します。

ユーザデータの同期化

外部ソースからのユーザ アカウントのインポートを設定した場合（「[グループの作成とユーザの追加 \[p. 22\]](#)」を参照）Cisco TMSPE は、ユーザが指定した情報を使用して同期スケジュールを設定します。同期は 1 日 1 回実行されます。スケジュールは変更できませんが、手動同期はいつでも実行できます。（「[手動同期の実行 \[p. 60\]](#)」を参照）。

Active Directory 以外の LDAP 実装では、インポートと同期に対して次の内容がサポートされている必要があることに注意してください。

- [RFC 4530](#) に定義されている **entryUUID** フィールド。
- [RFC 2696](#) に定義されている簡単なページング。

LDAP および AD フィールドのマッピング

次の表に、ユーザ データをインポートし、同期したときに、外部 Active Directory または LDAP ソースからのユーザ属性が、Cisco TMSPE にどのようにマップされるかを示します。Active Directory および LDAP パスワードを含め、他のフィールドはインポートまたは同期されません。

Cisco TMSPE ユーザ属性の列には、外部ディレクトリの属性がマッピングされるユーザ属性の名前が表示されます。テンプレート パターンにこれらのユーザ属性を含めることができます。次に、ビデオ アドレス パターンに **username** 属性を含める例を示します。

```
{username}@example.com
```

一部のユーザ属性とは、特定のパターンを定義するためだけに使用できます。たとえば、発信者 ID パターンにユーザ名属性を含めることはできません。詳細については、Cisco TMSPE オンライン ヘルプを参照してください。

Active Directory から	LDAP から	Cisco TMSPE へ	Cisco TMSPE ユーザ属性
objectGUID	entryUUID	external_id	
sAMAccountName	cn	ユーザ名 (Username)	username
mail	mail	Email	email
title	title	タイトル(Title)	
givenName	givenName	名 (First Name)	first_name
sn	sn	姓 (Last Name)	last_name
company	company	会社名 (Company)	
department	department	部署名 (Department)	
telephoneNumber	telephoneNumber	オフィスの電話 (Office Phone)	office_phone
mobile	mobile	携帯電話 (Mobile Phone)	mobile_phone
displayName	displayName	表示名 (Display Name)	display_name

手動同期のテスト

手動同期を実行した結果をプレビューし、検証するには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ(Users and Groups)]コンテナで、テストするグループをクリックします。選択したグループに関する情報が複数のペインに表示されます。
3. [ユーザ インポート(User Import)]ペインで、[インポートをテスト(Test import)]をクリックします。
情報は [ユーザ インポート(User Import)]ペインに表示され、テストが進行中であることが示されます。テストの実行が終了したら、情報はテストが正常に完了したかどうかを確認します。処理されたレコードの合計数と、または手動同期によって作成、更新、移動、または削除されるレコード数が表示されます。

手動同期の実行

手動同期を実行するには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ(Users and Groups)]コンテナで、同期するグループをクリックします。選択したグループに関する情報が複数のペインに表示されます。
3. [ユーザ インポート(User Import)]ペインで、[インポートを開始(Start import)]をクリックします。

ユーザおよびグループの移動

グループおよび手動で作成したアカウントを移動するには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ(Users and Groups)]コンテナで、移動するグループまたはユーザをクリックします。選択したグループに関する情報が複数のペインに表示されます。
3. [ユーザ設定(User Settings)]ペインの上部で、[ユーザの移動(Move User)]または [グループの移動(Move Group)]をクリックします。
4. [移動(Move)]ダイアログボックスで、ターゲット ユーザまたはグループに移動してクリックし、[移動(Move)]をクリックします。

外部ソースからインポートされたユーザアカウントの移動

外部ソースからインポートされたユーザを移動するには、現在ユーザがインポートされているグループ、およびユーザをインポートする先のターゲット グループのインポート フィルタを変更する必要があります。現在のグループのフィルタは、ユーザが除外されるように変更し、ターゲット グループには、ユーザが含まれるようなフィルタを適用します。

クラスタ間でのグループの移動

グループを移動することで、ユーザおよび FindMe アカウントが 2 つの Cisco VCS クラスタ間を移動することになる場合は、サービスをクリーンアップし、クラスタの完全同期を行って、VCS でユーザおよびアカウントが正しく表示されるようにする必要があります。

1. Cisco TMS で、[Administrative Tools]> [Provisioning Extension Diagnostics] に移動します。
2. ユーザ設定および FindMe で、[Cleanup]を実行します。
3. [システム(Systems)] > [ナビゲータ(Navigator)]に移動し、同期するクラスタに移動します。
4. [プロビジョニング(Provisioning)]タブに移動します。
5. タブの下部までスクロールし、[完全同期の実行(Perform Full Synchronization)]をクリックします。

関連するすべてのクラスタでこの手順を繰り返します。

ユーザアカウントの検索

ユーザ アカウントを検索するには、次の手順に従います。

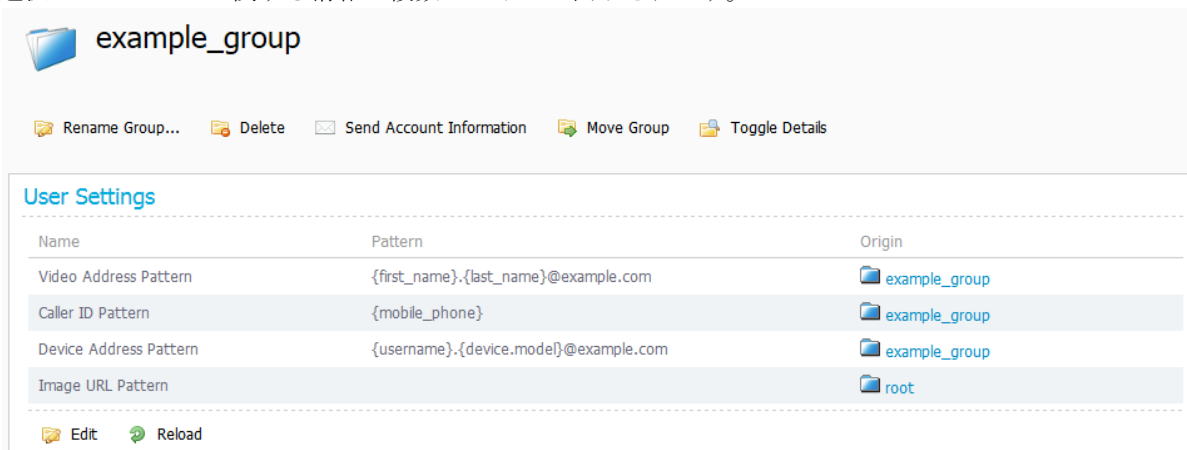
1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ(Users and Groups)]コンテナの見出しの下の検索フィールドに、検索するユーザ アカウントの表示名を入力します。
部分的な検索文字列を入力できます。検索文字列に一致するユーザ アカウントが、[ユーザとグループ(Users and Groups)]コンテナに表示されます。
3. 一致するユーザ アカウントの詳細を表示するには、そのアカウントをクリックします。
4. そのアカウントが属するグループを識別するには、[ユーザ設定(User Settings)]の上にある [グループへ移動(Go to group)]をクリックします。

グループおよびユーザアカウントの名前変更

グループおよび手動で作成されたユーザの表示名を変更できます。外部ディレクトリからインポートされたユーザの表示名は変更できないため注意してください。

ユーザおよびグループの表示名を変更するには、次の手順に従います。

1. Cisco TMS で、[Systems]> [Provisioning] > [Users] に移動します。
2. [ユーザとグループ(Users and Groups)]コンテナで、表示名を変更するグループまたはユーザをクリックします。
選択したグループに関する情報が複数のペインに表示されます。

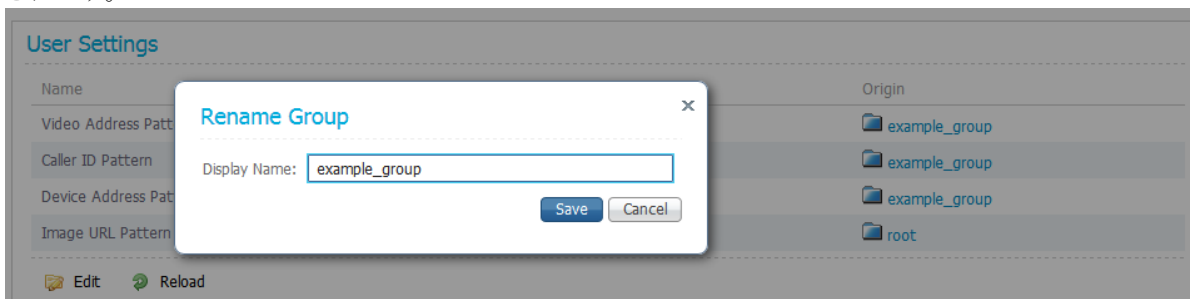


The screenshot shows the 'example_group' configuration page. At the top, there are icons for 'Rename Group...', 'Delete', 'Send Account Information', 'Move Group', and 'Toggle Details'. Below this is the 'User Settings' section, which contains a table with the following data:

Name	Pattern	Origin
Video Address Pattern	{first_name}.{last_name}@example.com	example_group
Caller ID Pattern	{mobile_phone}	example_group
Device Address Pattern	{username}.{device.model}@example.com	example_group
Image URL Pattern		root

At the bottom of the 'User Settings' section, there are 'Edit' and 'Reload' buttons.

3. [ユーザ設定(User Settings)]ペインの上部で、[ユーザを編集...(Edit User...)]または [グループの名前を変更...(Rename Group...)]をクリックします。対応するダイアログボックスが表示されます。



The screenshot shows the 'Rename Group' dialog box overlaid on the 'User Settings' section. The dialog box has a title bar 'Rename Group' and a close button 'x'. It contains a text input field labeled 'Display Name:' with the value 'example_group'. Below the input field are 'Save' and 'Cancel' buttons.

4. [ユーザを編集(Edit User)]または [グループの名前を変更(Rename Group)]ダイアログボックスで新しい名前を入力し、[保存(Save)]をクリックします。

プロビジョニングされたデバイスのソフトウェア アップグレード

このプロセスは、Jabber Video ではなくハードウェア エンドポイントのみに適用されます。Windows および Mac OS X への Jabber Video の導入およびアップグレードについては、『Cisco Jabber Video for TelePresence Administrator Guide』を参照してください。

構成のアップグレード

ソフトウェア アップグレードには通常、新しい設定、既存の設定への変更などが含まれた新しいスキーマが伴います。プロビジョニングされたデバイスのソフトウェアをアップグレードする前に、新しいスキーマをアップロードし、設定をアップグレードします。

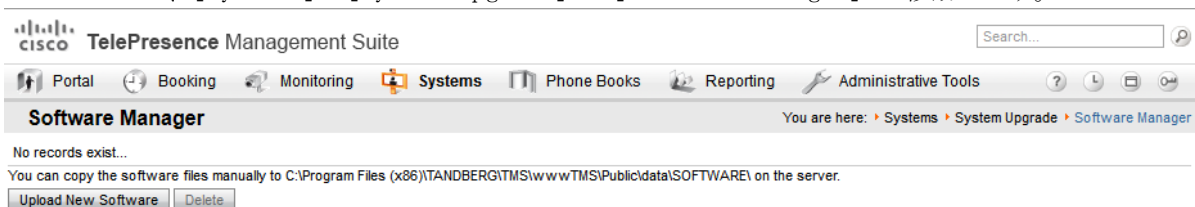
設定をアップグレードするには、次の手順に従います。

1. 新しいスキーマをダウンロードし、追加します。「[テンプレート スキーマの取得 \[p. 29\]](#)」を参照してください。
2. 新しいスキーマに基づいて新しい構成テンプレートを追加します。
 - a. 古いテンプレートから構成をコピーします。「[構成テンプレートの追加 \[p. 30\]](#)」を参照してください。
 - b. 導入環境によっては、必要に応じて、スキーマの以前のバージョンでは使用できなかった新しい構成を追加します。使用可能な設定については、エンドポイントの管理者のマニュアルで提供されます。
3. グループに新しい構成テンプレートまたはテンプレートを割り当てます。「[グループへの構成テンプレートの割り当て \[p. 33\]](#)」を参照してください。

デバイスのアップグレード

ハード エンドポイントをアップグレードするには、次の手順に従います。

1. Cisco TMS サーバのソフトウェア ディレクトリに、必要な新しいエンドポイントのソフトウェア バージョンをアップロードします。
 - a. Cisco TMS で、[Systems]> [System Upgrade] > [Software Manager] に移動します。



- b. [新しいソフトウェアをアップロード (Upload New Software)] ボタンを使用するか、TMS サーバにソフトウェア ファイルを手動でコピーします。このタスクの詳細については、オンライン ヘルプを参照してください。
2. Cisco TMS で、[Systems]> [System Upgrade] > [System Upgrade] に移動します。
 3. [システムの選択 (Select systems)] ペインで、[プロビジョニング拡張機能によって管理されているシステム (Systems managed by the Provisioning Extension)] オプション ボタンをクリックします。情報は、プロビジョニングされたシステムのソフトウェア バージョンについて表示されます。

System Upgrade You are here: > Systems > System Upgrade > System Upgrade

Select systems: TMS systems Systems managed by the Provisioning Extension

Systems	
Order by Software Version	
<input type="checkbox"/> Software Version	Number of Systems
<input type="checkbox"/> TE4.1.1	200

Information

System upgrade enables you to upgrade the software on systems in your network. Before you can upgrade systems you first have to use the Software Manager to upload the software files to TMS.

1. Choose which systems to upgrade software on from the list on the left
2. Click the 'Next' button to select software versions and enter release keys.
3. After selecting sw versions and entering release keys, clicking the 'Upgrade' button will upgrade the selected systems. The task is scheduled as a background activity job.

4. アップグレードするシステムで使用可能なオプションを使用し、[次へ(Next)]をクリックします。使用可能なオプションの詳細については、オンライン ヘルプを参照してください。
5. [リリース キー(Release Key)]カラムには、各システムのリリース キーを入力します。
6. [ソフトウェア(Software)]カラムから、各システムの目的のソフトウェア パッケージを選択します。
7. 表示されるフィールドに、アップグレード プロセスを開始する日時を選択し、[アップグレード(Upgrade)]をクリックします。

選択したエンドポイントは、次回ユーザがそのデバイスでサインインし、プロビジョニングされた時点でアップデートされます。上記で指定したソフトウェア パッケージのバージョンおよびパスは保存され、ユーザレベルの設定として、関連するすべてのユーザがこれを表示できます。[システム(Systems)] > [プロビジョニング(Provisioning)] > [ユーザ(Users)]に移動し、影響を受ける各ユーザの [ユーザ設定(User configurations)]セクションを確認します。

Cisco TMS 接続詳細のアップデート

Cisco TMS の接続の詳細をアップデートするには、次の手順に従います。

1. [管理ツール(Administrative Tools)] > [構成(Configuration)] > [プロビジョニング拡張機能の設定(Provisioning Extension Settings)]に移動します。
2. [Cisco TMS Connection]セクションまでスクロールします。

Cisco TMS Connection

	HTTPS *	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Connection Timeout *	<input type="text" value="10"/>	(seconds)	
Receive Timeout *	<input type="text" value="60"/>	(seconds)	
Username *	<input type="text" value="administrator"/>		
Password *	<input type="password" value="....."/>		

3. 設定を必要に応じて変更します。
4. [保存(Save)]をクリックします。
5. プロビジョニング拡張機能サービスを再起動します。 [「TMS プロビジョニング拡張機能 Windows サービスの再起動 \[p. 66\]」](#) を参照してください。

データベースの管理

データベースのバックアップ

Cisco TMSPE データベースを定期的にバックアップすることを推奨します。

バックアップからのデータベースの復元

バックアップからデータベースを復元する場合は、Cisco VCS クラスタとの完全同期を実行する必要があります。

1. [システム(Systems)] > [ナビゲータ(Navigator)]に移動し、Cisco VCS を開きます。
2. [プロビジョニング(Provisioning)]タブを開きます。
3. タブの下部までスクロールし、[完全同期の実行(Perform Full Synchronization)]をクリックします。

データベースの移動

データベースを移動した後で、Cisco TMSTools でデータベース設定を更新する必要があります。

1. Cisco TMS サーバで、[Start] > [Cisco TelePresence Management Suite] > [Cisco TMSTools] に移動します。
2. [構成(Configuration)] > [プロビジョニング拡張機能 DB 設定(Change Provisioning Extension DB Settings)]に移動します。
3. 新しいロケーションで、[データベース サーバ¥インスタンス(Database Server¥Instance)]をアップデートします。
4. [Database Name]がまだ [tmspe]であることを確認します。
データベース名を変更することはできません。このインストールが停止します。
5. [ユーザ名(Username)]を確認します。
6. 上記のユーザの [パスワード(Password)]を入力します。
7. [OK]をクリックします。

冗長 Cisco TMS 導入の場合、上記の手順を両方のサーバに対して実行します。

データベース インスタンスを更新した後、Windows サービスを再起動して接続設定の変更を有効にします。詳細については、「[TMS プロビジョニング拡張機能 Windows サービスの再起動 \[p. 66\]](#)」を参照してください。

トラブルシューティング

ここでは、Cisco TMSPE の組み込み診断ツールについて、およびトラブルシューティングのシナリオと解決方法について説明します。

Cisco TMSPE 診断の実行

Cisco TMSPE は、定期的なヘルス チェックを 30 分ごとに実行し、見つかった問題を、Cisco TMS の [Administrative Tools] > [Provisioning Extension Diagnostics] でアラームのリストとして表示します。ヘルス チェックは、すべてのサービス（たとえば、ユーザ リポジトリ、ユーザ設定および電話帳）、およびデータベース接続および内部メッセージング通信などの、基盤となるリソースをモニタします。

追加のシステム モニタリングは 10 分ごとに実行され、ディスク容量の不足、高いシステム メモリ使用率などの問題が報告されます。

ヘルス チェック中またはシステム モニタリングの結果として検出された診断問題は、[アラーム (Alarms)] ペインに表示されます。

[プロビジョニング拡張機能の診断 (Provisioning Extension Diagnostics)] ページに表示される情報は自動的に更新されません。情報を更新するには、ページをリロードします。

Provisioning Extension Diagnostics You are here: Administrative Tools > Provisioning Extension Diagnostics

Run Health Check

Alarms

No alarms have been raised.

System Status

Service	Status	User Import	Device Import	Cleanup	Actions
User Repository	●			●	Cleanup
Device Repository	●			●	Cleanup
User Preference	●	●		●	Cleanup User Import
Phone Book	●			●	Cleanup
FindMe	●	●	●	●	Cleanup User Import Device Import
Diagnostics	●			●	Cleanup

Cisco VCS Communication

VCS IP Address	Cluster Name	Last Request	Request URI
10.10.10.10	Cluster1	2023-03-20 13:20:03 (GMT+02:00)	/dr/groups/id/ea32a8f5-d9a2-41d9-9209-7a5c9ec90006

ヘルス チェックの実行

ヘルス チェックを随時トリガーするには、次の手順に従います。

1. Cisco TMS で、[Administrative Tools] > [Provisioning Extension Diagnostics] に移動します。
2. [アラーム (Alarms)] ペインの上部で、[ヘルス チェックを実行 (Run Health Check)] をクリックします。
ヘルス チェックが完了すると、メッセージが表示されます。新しいアラームは [アラーム (Alarms)] ペインに表示されます。
3. [アラームの詳細 (Alarm Detail)] ダイアログボックスに問題の説明および推奨される対処方法を表示するには、[詳細 (Details)] 列内のアイコンをクリックします。
4. 次のいずれかの操作を実行します。
 - [承認 (Acknowledge)] をクリックして問題を承認し、[アラーム (Alarms)] ペインから削除します。
 - [キャンセル (Cancel)] をクリックして [アラーム (Alarms)] ペインに残したままにします。

システム ステータスの表示

プロビジョニング拡張機能ソリューションに役立つサービスは、現在のステータスを判別するために定期的にモニタされます。

システム ステータスを表示し、是正措置を取るには次の手順に従います。

1. [プロビジョニング拡張機能の診断(Provisioning Extension Diagnostics)]ページで、[システムの状態(System Status)]ペインまでスクロールします。
2. 色分けされたステータスの円を表示します。赤色の円はエラーまたは警告を示します。
3. 問題を解決するには、対応するボタンをクリックします。
 - システムの状態：[クリーンアップ(Cleanup)]をクリックします。
この動作は、ユーザおよびグループの更新など、データの変更に関する情報を格納するデータベースのデルタ テーブルをクリーンアップします。デルタ テーブルに変更が累積されていくことで、データベースが経時的に大きくなる場合があります。
 - ユーザ インポートの状態：[ユーザ インポート(User Import)]をクリックします。
この動作は、ユーザ リポジトリからターゲット サービスへの完全なインポートを開始します。
 - デバイス インポートの状態：[デバイス インポート(Device Import)]をクリックします。
この動作は、デバイス リポジトリからターゲット サービスへの完全なインポートを開始します。
4. クリーンアップのステータスの円を表示して、問題が解決したことを確認します。
一般的に、プロセスの待機中はステータスがオレンジに変わり、タスクが進行中の場合は歯車のアイコンになり、ステータスが OK になると、緑色の円に変わります。

Cisco VCS の通信履歴の表示

[Provisioning Extension Diagnostics]ページでは、Cisco VCS から Cisco TMSPE におこなったデータのポーリング試行についての、最近の履歴を確認できます。

現在アクティブなすべての Cisco VCS は、[Cisco VCS Communication]ペインに表示されます。最新のポーリングのタイムスタンプは、[最終コール時刻(Last Call)]列に表示されます。

最新のポーリング試行がどれくらい前に行われたかを確認することで、問題の根本原因の特定に役立つ場合があります。

TMS プロビジョニング拡張機能 Windows サービスの再起動

一部のエラー状態では、Cisco TMSPE が問題を解決するために、Windows サービスの再起動が必要な場合があります。特定のシナリオでは、これは [TMS プロビジョニング拡張機能の診断(TMS Provisioning Extension Diagnostics)]ページの [修正処置(Corrective action)] としても表示されます。

サービスを再起動するには、次の手順に従います。

1. Server Manager を開きます。
2. [構成(Configuration)]> [サービス(Services)] に移動します。
3. TMS プロビジョニング拡張機能サービスを見つけ、[再起動(Restart)]をクリックします。

サービスの初期化には 2 ~ 3 分かかる場合があります。この間、Cisco TMS の Cisco TMSPE パーツは使用できなくなってしまうため、注意してください。

プロビジョニング ログ

Cisco TMSPE および Cisco TMS ログ

Cisco TMSPE および Cisco TMS の使用可能なすべてのログのスナップショットを取得するには、次の手順に従います。

1. [Administrative Tools]> [TMS Server Maintenance] に移動します。
2. [Download Log Files]をクリックします。

Cisco VCS ログ

- [Status] > [Logs] > [Network Log]に移動して、登録済み、登録失敗、およびその他のネットワークを確認します。
- すべてのイベントについては、[Status] > [Logs] > [Event Log]に移動します。
- [Status] > [Logs] > [Configuration Log]に移動して、Cisco VCS の構成変更の概要を確認します。

エンドポイント ログ

ハード エンドポイントについては、その IP アドレスをブラウザして、ログを表示またはダウンロードします。

インストレーションに関するトラブルシューティング

インストール ログのチェック

問題が Cisco TMS サーバへの Cisco TMSPE のインストール中に発生した場合は、Cisco TMSPE のインストール ログを参照してください。Cisco TMSPE インストール ログは、次の場所にあります。

C:\Program Files\TANDBERG\TMS\TMSProvisioningExtension\app\logs

このログには、[管理ツール(Administrative Tools)]> [TMS サーバ メンテナンス(TMS Server Maintenance)] に移動し、[ログ ファイルのダウンロード(Download Log Files)]をクリックすることで提供される、ログのアーカイブにも含まれています。

「Java ランタイム中に SQL 接続を確立できませんでした...(Unable to establish SQL connection through Java runtime...)」

Cisco TMSPE インストーラの実行中にこのエラーが表示される場合は、SQL Server Browser が動作状態でないか確認します。SQL クライアントは、名前付きインスタンスおよびポート番号の解決に SQL Server Browser を使用します。

SQL Server Browser を表示し、必要に応じて起動するには、次の手順に従います。

1. SQL Server で次のいずれかを開きます。
 - SQL のコンフィギュレーション マネージャに移動し、SQL Server サービスを開きます。
 - [コンピュータの管理(Computer Management)]> [サービスとアプリケーション(Services and Applications)] > [サービス(Services)] に移動します。
2. SQL Server Browser サービスを検索し、実行されていない場合は起動します。

サービスを起動しない場合は、Cisco TMSPE インストーラでポート番号を指定する必要があります。ポート番号の入力でサポートされている唯一の形式は、<SERVER NAME>:<port number> です。

ただし、名前付きインスタンスがデフォルトでダイナミック TCP ポートを使用する場合は、データベース サーバのリポート時に接続が切断されるため、注意してください。したがって、SQL Server Browser が動作している状態を維持することを強く推奨します。

要求されたターゲットに有効な認証パスを見つけることができない

プロビジョニング拡張機能の診断で、電話帳サービスに赤い円が表示されている場合は、次の手順に従います。

1. [クリーンアップ(Cleanup)]をクリックします。
2. 数分後に、ヘルス チェックを実行して表示される情報を更新します。
3. それでも円が赤い場合は、ログを確認します。 `tmsprovisioningextension.log` ファイルに次の行が含まれる場合は、次の手順に移動します。


```
Caused by: javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target]
```

 - a. Cisco TMS サーバの任意の場所に証明書ファイルを置きます。
 - b. 次のコマンドを使用して、サーバの `JRE_HOME\bin` から JRE キーストアをアップデートします。


```
keytool -import -alias myprivateroot -keystore ..\lib\security\cacerts -
file c:\hello.cer
```
 - c. プロンプトが表示されたら、キーストアのパスワードを入力します。 デフォルトのパスワードは `changeit` です。

プロビジョニング問題のシナリオ

データベース接続が失敗する

Cisco TMSPE からのデータベースへの接続が失敗する場合、[Users] ページにアクセスすると右下隅にエラー メッセージが表示されます。診断ではアラームは発行されませんが、赤のインジケータにより、サービスが機能していないことが示されます。

「指定されたネットワーク名は使用できません(The specified network name is no longer available) 」

名前付きパイプ プロトコルを使用する Microsoft SQL Server Data Engine を使用して Cisco TMS を設定している場合で、データベースへの接続が失敗し「指定されたネットワーク名は使用できません(The specified network name is no longer available) 」というエラー メッセージが表示されるようになった場合は、Windows Server に必要なホットフィックスが適用されていません。

「[Cisco TMS およびサーバの要件 \[p. 6\]](#)」参照してください。

Kerberos での AD のインポートが失敗する

Kerberos 認証を使用した Active Directory からユーザ インポートを構成しており、それが `tmsprovisioningextension.txt` ログの次に示すようなエラーで失敗する場合、サポートされていないバージョンの Java を実行している可能性が高いです。

問題を解決するには、次の手順に従います。

1. プロビジョニング拡張機能 Windows サービスを停止します。
2. Java 6 をアンインストールします。
3. Java 7 アップデート 17(32 ビットまたは 64 ビット) をインストールします。
32 ビットから 64 ビットの Java バージョンに変更する場合は、Cisco TMSPE も再インストールする必要があります。
4. Windows サービスを再起動します。

ログの抜粋

ログで次のようなメッセージを検索します。

```
2012-10-25 15:02:24,951 [common] [JettyThread-24] ERROR U:administrator
c.c.ts.mgmt.lib.api.i18n.Localizer - key Lock prevents new connection, parallel connections not
supported due to underlying os operations. is not localized
```

```
2012-10-25 15:02:24,951 [common] [JettyThread-24] ERROR U:administrator
c.c.t.m.l.a.i18n.ExceptionLocalizer - Key not localized:
```

```
com.cisco.ts.mgmt.ur.service.userimport.settings.UserImportCommunicationException
com.cisco.ts.mgmt.ur.service.userimport.settings.UserImportCommunicationException: null
```

また、メッセージに次のようなステートメントが含まれていないか検索します。

```
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) ~[na:1.6.0_34]
```

```
at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source) ~[na:1.6.0_34]
```

```
at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source) ~[na:1.6.0_34]
```

```
at java.lang.reflect.Method.invoke(Unknown Source) ~[na:1.6.0_34]
```

電子メール送信の障害

アカウント情報の電子メールが受信者に到達しない場合は、次の手順に従います。

- 「[電子メールの設定 \[p. 36\]](#)」で、SMTP サーバ、ポート、ユーザ名、およびパスワードが正しく設定されていることを確認します。
- アンチウイルス ソフトウェアにより電子メールの送信が妨げられていないか確認します。一部のアンチウイルス アプリケーションでは、すべての電子メールの大量送信がブロックされます。

Cisco VCS でデータ インポートの失敗がレポートされる

Cisco VCS で、「TMS プロビジョニング拡張機能サービスのデータ インポート失敗 (TMS Provisioning Extension services data import failure)」というアラームが発生し Cisco TMS チケットが発行される場合、Cisco TMSPE から受信したデータ形式またはエントリ数に問題があります。

「VCS が内部テーブル制限を超過するおそれがあります (Would cause the VCS to exceed internal table limits)」

すべてのサイズの Cisco VCS クラスタで、次のインポートがサポートされています。

- 10,000 人のプロビジョニングするユーザ
- 10,000 個の FindMe アカウント
- 200,000 の電話帳エントリ

上記のアラームが発生した場合、ユーザ、FindMe アカウント、電話帳エントリのいずれかが最大数を超過しています。

修正処置： 最初に、報告されたエントリ数が正しいことを確認します。

1. Cisco TMS で、[Administrative Tools]> [Provisioning Extension Diagnostics] に移動します。
2. 該当するサービス (ユーザ、電話帳、または FindMe) の横で、[Cleanup] をクリックします。
3. [システム (Systems)] > [ナビゲータ (Navigator)] に移動し、Cisco VCS を開きます。
4. [プロビジョニング (Provisioning)] タブを開きます。
5. タブの下部までスクロールし、[完全同期の実行 (Perform Full Synchronization)] をクリックします。

アラームの原因が Cisco TMSPE でのデータの重複である場合、これで同期が正常に完了します。

それでもまだ Cisco VCS 制限を超過している場合、Cisco VCS イベント ログを表示して詳細を確認してください。

- ユーザおよび FindMe が制限を超過している場合は、使用可能なキャパシティを持つクラスタにグループを移動します。
- Cisco TMS の電話帳の合計エントリ数が 200,000 を超過している場合は、減らします。

「識別できないデータ形式です(Unrecognized data format)」

チケットから「TMS プロビジョニング拡張機能サービスからインポートされた 1 つ以上のレコードが、認識されないデータ形式であったためドロップされました (One or more records imported from the TMS Provisioning Extension services have been dropped due to unrecognized data format)」というレポートが発行された場合、問題は次のいずれかです。

- レコードが、認識可能な形式でない
- FindMe URI などの必須フィールドが空であるか、欠落している
- フィールドに誤ったタイプのデータまたは無効な値が含まれている

修正処置:

1. 詳細については、Cisco VCS イベント ログを参照してください。
2. イベント ログに基づいてエラーを修正します。

ユーザが「ライセンスが切れています(Out of licenses)」というメッセージを受信する

ユーザが Cisco Jabber Video for TelePresence にサインインしたときに、「ライセンスが切れています(Out of licenses)」というメッセージを受信する場合、通常は最大同時ユーザ数を越えたことを意味します。ただし、これが Cisco TMSPE を設定した直後に発生した場合、このメッセージは構成ミスが原因である可能性があります。

これをチェックするには、次の手順を実行します。

1. [システム(Systems)] > [ナビゲータ(Navigator)] に移動します。
2. クライアントがサインインを試行している Cisco VCS を選択し、[Provisioning] > [Devices] ペインに移動します。
3. [デバイス(Devices)] ペインで、[サービスのイネーブル化(Enable Service)] が選択されていることを確認します。

手順の詳細については、「[Configuring Cisco VCS via Cisco TMS](#)」を参照してください。

使用可能なテンプレートがない場合、サインインが失敗する

デバイスは、デバイスのタイプ用のテンプレートが存在しない場合、サインインしてプロビジョニングすることはできません。該当のバージョンに対してテンプレートが存在しない場合、Cisco TMSPE は、以前のバージョンで使用可能な最新のテンプレートにフォールバックします。そのデバイスの特定バージョンまたはそれよりも前のバージョンに対するテンプレートが存在しない場合、Cisco TMSPE は、それよりも新しいテンプレートにフォールバックできないため、注意してください。

特定のデバイス タイプでサインインが失敗する場合は、次の手順に従います。

1. Cisco VCS で、[Status] > [Logs] > [Event Log] に移動します。
2. ログに次のようなエラー メッセージがある場合は、Cisco TMSPE でデバイスのテンプレートが設定されていません。
`provisioning: Level="ERROR" Detail="Failed to provision user" User-URI="[user's SIP URI]" Reason="No provisioning template document found" Device-model="[device]" Device-version="[software version]". (プロビジョニング: レベル = "エラー" 詳細 = "ユーザのプロビジョニングに失敗しました" ユーザ URL = "[ユーザの SIP URI]" 理由 = "プロビジョニング テンプレート ドキュメントが存在しません" デバイスモデル "[デバイス]" デバイスバージョン = "[ソフトウェア バージョン]".)`

テンプレートを追加する手順については、「[プロビジョニングされたデバイスの設定を構成する方法](#) [p. 29]」を参照してください。

構成スキーマをアップロードしたときに表示される警告

スキーマをアップロードすると、警告が Cisco TMSPE 管理インターフェイスに表示される場合、HTTP PUT 要求が IIS により停止される Web サーバの構成の問題が原因である可能性があります。

1. Cisco TMSPE サーバで IIS Manager を開きます。
2. Cisco TMSPE Web アプリケーションを選択します(`<machinename>/Sites/Default Web Site/tmsagent`)。
3. 中央のペインで、[要求のフィルタリング(Request Filtering)]をダブルクリックします。
4. 同じペインで、[HTTP 動詞(HTTP Verbs)]タブを選択します。
5. PUT が **Allowed=True** に設定されていることを確認します。

Web アプリケーションの中で PUT がすでに有効になっている場合、サーバ全体の設定により個々の Web アプリケーションの設定が上書きされていないか確認します。

この問題は、[WebDAV パブリッシュ(WebDAV Publishing)] が [IIS ロール サービス(IIS Role Service)] である場合のみ発生するため、注意してください。

電話帳が受信できない

一人以上のプロビジョニング ユーザがデバイスで電話帳を受信しない場合は、次の手順に従います。

- そのユーザのアクセス コントロールが正しく設定されていることを確認します。「[グループへの電話帳の関連付け \[p. 35\]](#)」(p. 1) を参照してください。
- プロビジョニングされたデバイスからの電話帳の要求が、そのデバイスをプロビジョニングしたものと同一 Cisco VCS またはクラスタで処理されていることを確認します。電話帳の要求が、異なるプロビジョニング対応 VCS に送信された場合、その要求は失敗し、そのデバイスで電話帳を使用可能にできません。

Smart Scheduler と FindMe のトラブルシューティング

FindMe または Smart Scheduler にアクセスできない

- エラー メッセージ: アクセスが拒否される。サーバに重要な Windows Update がすべてインストールされていることを確認します。
- フレームワークに空白ページが表示される場合、ユーザが手動で URL を入力し、後続のスラッシュを忘れた可能性があります。

検索履歴を使用した、FindMe 問題の診断

FindMe 関連の問題の診断を開始するのに最良な場所は、通常、検索履歴(関連するユーザ アカウントをホストする、Cisco VCS または Cisco VCS クラスタの検索履歴) です。

検索履歴には、FindMe ID の検索と、ユーザ ポリシーが現在アクティブな場所にあるすべてのデバイスを確認するためにコールをどのように分岐するかが示されます。各デバイスの検索の結果も表示されます。

Cisco TMSPE のアンインストール

Cisco TMSPE をアンインストールする方法は 2 通りあります。動作は、次に説明されているように、システム設定とアンインストールの方法に応じて、異なる場所でログに記録されます。Cisco TMSPE をアンインストールすることで、ログ データが削除されることはありません。

インストーラの使用

1. インストーラを実行します。
2. 画面上の指示に従ってアンインストールします。

アンインストール ログは、次の場所で作成されます。

C:\Program Files\TANDBERG\TMS\www\TMS\Data\Logs\Install

アンインストール プロセスを開始すると Windows サービスが停止しますが、アンインストールをキャンセルしてもサービスは再起動されないため、注意してください。詳細については、「[TMS プロビジョニング拡張機能 Windows サービスの再起動 \[p. 66\]](#)」を参照してください。

コントロール パネルの使用

1. Microsoft サポートの記事『[Windows インストーラのログの記録を有効にする方法 \(How to enable Windows Installer logging\)](#)』の手順に従って、動作がログに記録されることを確認します。
2. Windows コントロール パネルの [プログラムの追加と削除 (Add/Remove Programs)] リストを開きます。
3. リストで TMS プロビジョニング拡張機能を見つけ、[削除 (Remove)] をクリックします。

アンインストール ログは、サーバの Temp フォルダに作成されます。ログにアクセスするには、次の手順に従います。

1. Windows の [スタート (Start)] > [ファイル名を指定して実行 (Run)] に移動します。
2. **%Temp%** と入力し、[OK] をクリックしてフォルダを開きます。
3. **MSI** で始まる、拡張子が **.LOG** のファイル名を見つけます。

再インストール時の既存の SQL データベースの再利用または置換

Cisco TMSPE は、アンインストールしても SQL データベースの **tmspe** が自動的に削除されることはありません。インストーラにより、既存の Cisco TMSPE の SQL データベースである **tmspe** が検出されます。また、このデータベースを再利用するかどうか尋ねられます。

SQL Server Management Studio を使用して、**tmspe** を削除します。[SQL Server Management Studio](#) は Microsoft SQL Server 2005 以降のバージョンに含まれています。

Cisco VCS からのプロビジョニングの削除

プロビジョニングがなくなったり、またはプロビジョニングが Cisco VCS Expressway で誤ってイネーブルにされた場合は、次の手順に従います。

Cisco VCS で、次の手順を実行します。

1. [メンテナンス (Maintenance)] > [オプション キー (Option keys)] に移動します。
2. [デバイス プロビジョニング (Device Provisioning)] オプション キーを選択します。
3. [削除 (Delete)] をクリックします。

マニュアルの変更履歴

日付	リビジョン	説明
2013年9月	11	<p>以前は FindMe ユーザ ガイドにしかなかったブラウザ要件を追加し、更新しました。</p> <p>Cisco TMSPE が Java 7 アップデート 40 でテストされたことを反映するために、Java 要件を更新しました。</p> <p>データベース メンテナンスの項を明確化しました。データベース名の変更は、サポートされていません。</p>
2013-06-17	10	<p>Cisco TMS 14.2.2 のリリースを反映するように更新されました。現在は、Smart Scheduler を使用した導入の要件になります。詳細については、『Cisco TelePresence Management Suite Release Notes』（14.2.2）を参照してください。</p>
2013-05-15	09	<p>未解決の問題 CSCu74973 に関する注意事項を追加しました。Cisco TMSPE 1.1 では、空白の手動で作成したデータベースのインストールは実行できません。Cisco TMSPE} 1.1.回避策については、『データベースの場所 [p.8]』を参照してください。</p>
2013-04-24	08	<p>Cisco TMSPE 1.1 のリリース。</p>
2012-12-17	07	<p>Cisco TMS 14.1 の導入を扱うために、ドキュメントを更新しました。Cisco TMS} 14.1.移行は現在サポートされていません。Cisco TMS 13.2 を使用して実行する必要があります。</p>
2012-10-30	06	<p>Java 6 の要件を明確化し、関連のトラブルシューティング項目を追加しました。Cisco TMS の要件に、IIS リダイレクト制限を追加しました。Cisco Jabber Video for TelePresence 4.2 を含むように、エンドポイントの推奨事項を変更しました。Cisco Jabber Video for TelePresence} 4.2.データベース名では、大文字と小文字が区別されることを指定しました。FindMe URL のディセーブル化に関する情報が追加されました。</p>
2012-09-13	05	<p>要件セクションの SQL の前提条件を明確化しました。電話帳とテンプレートのアップロードのトラブルシューティング シナリオを追加しました。</p>
2012-08-07	04	<p>Cisco VCS X7.2 のサポートが追加されました。</p>
2012-07-06	03	<p>テンプレートが使用できない場合の証明書の検証エラー、およびサインイン失敗のトラブルシューティング シナリオを追加しました。</p>
2012-05-10	02	<p>動作しない SQL Server Browser のトラブルシューティング項目を追加しました。</p> <p>デフォルトのデータベース インスタンス向けの不要なインストールの回避策を削除しました。</p>
2012-04-27	01	<p>Cisco TMSPE 1.0 のリリース。</p>

資料のインベントリ

Cisco TMSPE の最新バージョンのすべての資料は、http://www.cisco.com/en/US/products/ps11472/tsd_products_support_series_home.html から入手できます。

Title	参照先	Link
<i>Cisco TMSPE Release Notes</i>	D14940	http://cisco.com
<i>Cisco TelePresence FindMe User Guide</i>	D14958	http://cisco.com
<i>Cisco VCS Administrator Guide</i>	D14049	http://cisco.com
<i>Cisco TelePresence Video Communication Server Cluster Creation and Maintenance Deployment Guide</i>	D14367	http://cisco.com
<i>Cisco TMS Installation and Getting Started Guide</i>	D14389	http://cisco.com
<i>Cisco TMS Administrator Guide</i>	D13741	http://cisco.com
<i>Cisco TelePresence Video Communication Server FindMe Deployment Guide (X6)</i>	D14525	http://cisco.com
<i>ENUM dialing on Cisco VCS Deployment Guide</i>	D14465	http://cisco.com
Windows インストーラーのログの記録を有効にする方法 (How to enable Windows Installer logging)	-	http://support.microsoft.com/kb/223300
<i>Distinguished Names</i>	-	http://msdn.microsoft.com
「Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters」	RFC4515	http://tools.ietf.org/html/rfc4515

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. その他の商標はそれぞれの権利者の財産です。The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2013 Cisco Systems, Inc. All rights reserved.

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>