Cisco Hosted Collaboration Solution for Contact Center 構成ガイド、リリース 11.6(1)

初版：2017 年 8 月 24 日

最終更新：2018 年 6 月 5 日

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/

目 次

はじめに

変更履歴

次の表に、このガイドに加えられたすべての変更を一覧します。最新の変更が上部に表示されています。

変更	参照先	日付
Release 11.6(1) 用ドキュメントの最初のリリース		2017 年 8 月

変更	参照先	日付
HCS for CC では、11.5 以降の Active Directory からのみユーザーを作成できます。UCCE からユーザーを作成することはできません。	ユーザーの作成（211 ページ）	
HCS for CC では、11.6 から 500 エージェント導入モデルのサポートが削除されました。	ガイド全体	
Small Contact Center 導入モデル用に CUBE エンタープライズの構成手順が追加されました。	Small Contact Center 導入モデル用 CUBE エンタープライズの構成 （142 ページ）	
セッション ボーダー コントローラの統合が追加されました。	セッション ボーダー コントローラの統合 （202 ページ）	
VRF を使用した SCC 展開用ゲートウェイの構成手順が追加されました。	VRF を使用した SCC 展開のためのゲートウェイの構成（353 ページ）	
11.6 の基本構成パラメータを更新	基本構成パラメータ （550 ページ）	

このガイドについて

このドキュメントでは、Contact Center インスタンスの新しいHosted Collaboration Solution for Contact Center（HCS for CC）を必要なインプレース Hosted Collaboration Solution for Contact Centerインフラストラクチャに展開、構成、統合するために必要な情報を提供します。このソリューションを構成および統合するために実行する手順の一覧を示します。

このドキュメントでは、Hosted Collaboration Solution for Contact Center アプリケーションとインフラストラクチャが配置され、CC の展開と統合の HCS for CC 準備ができている必要があります。このドキュメントでは、CC ゴールデンテンプレートの HCS for CC が展開および統合用に作成されていることを前提としています。

対象者

このマニュアルは、シスコ Unified Contact Center Enterprise（Unified CCE）、製品、設計、要件、インストールおよび管理のメソッドと手順について認定された、または同等の経験があるシスコ認定テクノロジーパートナー（ATP）担当者を対象としています。

Hosted Collaboration Solution for Contact Center のサブセットとして、コンタクトセンターの HCS for CC の読者は、これらの必須およびオプションのアプリケーション、プラットフォーム、およびインフラストラクチャに対応する知識と経験を持つことが必要です。

関連資料

さまざまなコンポーネントとサブシステムを含む、Cisco HCS for Contact Center ソリューションの展開に関する設計上の考慮事項とガイドラインについては、「http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-implementation-design-guides-list.html」を参照してください。

Cisco HCS for Contact Center のインストール手順については、「http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html」を参照してください。

Hosted Collaboration Solution アプリケーションおよびインフラストラクチャの設計、インストール、および構成については、「https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html」を参照してください。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

フィールド通知

シスコでは、シスコ製品に関する重要な問題についてカスタマーとパートナーに通知するために、Field Notice を発行しています。通常それらの問題については、アップグレード、回避策、またはその他のユーザ アクションが必要になります。詳細については、https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html の「製品フィールド通知の概要」を参照してください。

次の通知で新しいアナウンスがリリースされた場合、シスコ製品、シリーズ、またはソフトウェアのカスタムサブスクリプションを作成して、電子メールアラートを受信したり、RSS フィードを利用できます。

- Cisco セキュリティ アドバイザリ
- Field Notice
- 販売終了またはサポートに関するアナウンス
- ソフトウェアアップデート
- 既知のバグの更新

カスタムサブスクリプションの作成の詳細については、https://cway.cisco.com/mynotifications の「マイ通知（*My Notifications*）」を参照してください。

マニュアルに関するフィードバック

このドキュメントに関するご意見は、contactcenterproducts_docfeedback@cisco.com まで電子メールでご共有ください。

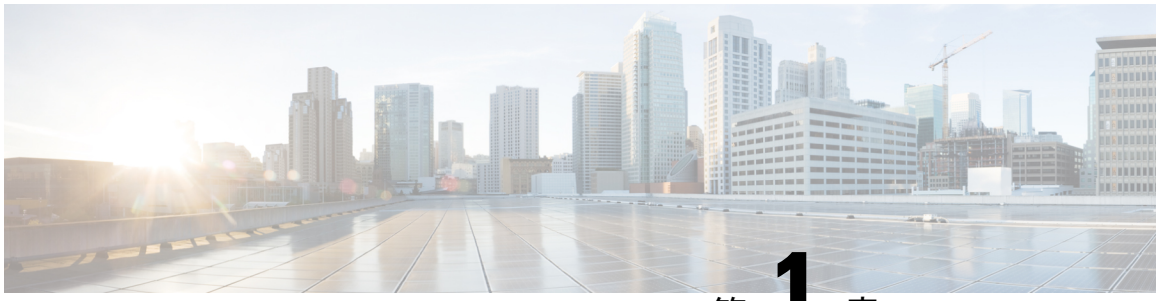
ご意見をお待ちしています。

表記法

このマニュアルでは、以下の表記法を使用しています。

表記法	説明
▿太字▵	太字は、ユーザエントリ、キー、ボタン、フォルダ名およびサブメニュー名などのコマンドを表すときに使用されます。 次に例を示します。 • **[編集（Edit）]** > **[検索（Find）]** の順に選択します。 • [完了（Finish）] をクリックします。
イタリック体	イタリック体は、次の内容を表すときに使用されます。 • 新しい用語の紹介。例：スキル グループとは、類似したスキルを持つエージェントの集合です。 • ユーザが置き換える必要のあるシンタックス値。例：IF (*condition, true-value, false-value*) • ドキュメントのタイトル。例： *Cisco Unified Contact Center Enterprise* インストールおよびアップグレード ガイドを参照してください。
ウィンドウ フォント	Courier などのウィンドウ フォントは、次の場合に使用されます。 • コード中のテキストや、ウィンドウに表示されるテキスト。例：`<html><title>Cisco Systems, Inc. </title></html>`
< >	山カッコは、次の場合に使用されます。 • コンテキストでイタリックが許可されない引数（ASCII 出力など）。 • ユーザが入力する文字列で、ウィンドウには表示されないもの（パスワードなど）。

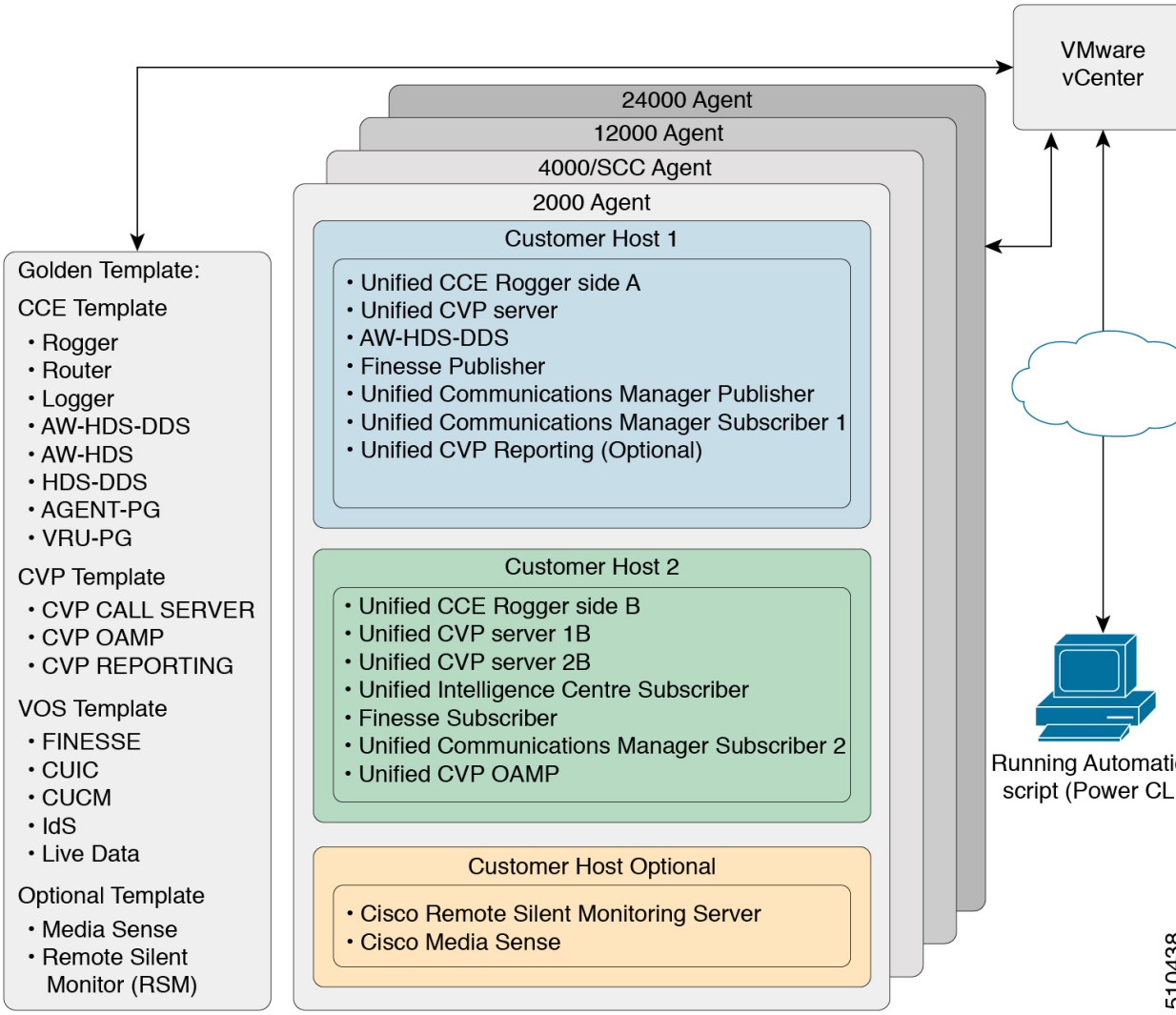
はじめに



第 1 章

クローンと OS のカスタマイズ

クローンと OS のカスタマイズプロセス



自動化クローニングと OS のカスタマイズ

次の自動化ソフトウェアおよびダウンロード情報については、http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html にある『*Cisco HCS for Contact Center* インストールおよびアップグレードガイド』の「自動化ソフトウェア」セクションを参照してください。

- GoldenTemplateTool
- PowerCLI
- OVF ツール

- WinImage

ゴールデンテンプレートを使用した自動化クローニングと OS のカスタマイズ

順序	タスク	完了
1	ゴールデンテンプレート自動化ツールのダウンロード （3 ページ）	
2	自動化スプレッドシートの入力 （4 ページ）	
3	自動化スクリプトの実行 （6 ページ）	
4	OS のカスタマイズプロセス （7 ページ）	

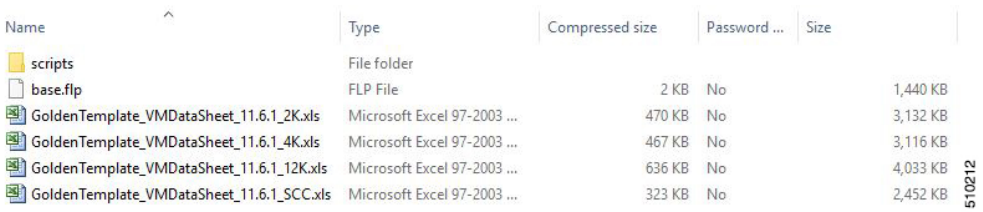
ゴールデンテンプレート自動化ツールのダウンロード

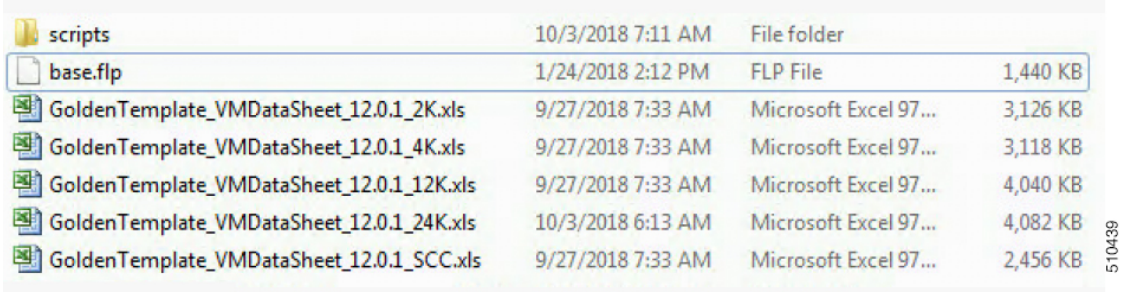
ゴールデンテンプレートツールは、ゴールデンテンプレートの自動複製と、カスタマイズされた仮想マシンのカスタマーインスタンスへの展開に必要です。ゴールデンテンプレートツールをダウンロードして、展開するには、システムの **C: ドライブ**のルーツへの 自動化クローニングと OS のカスタマイズ （2 ページ） を参照してください。VMware vSphere PowerCLI を使用して自動化スクリプトを参照できます。

抽出されたコンテンツには、次のものが含まれます。

- 自動化スプレッドシート、つまりスクリプトへのインターフェイス。
- 5 つのスクリプトを含むスクリプトフォルダ。deployVM.PS1 ファイルは、プライマリの自動化スクリプトで、残りの 4 つのスクリプトを呼び出します。
- エクスポート用の自動化スクリプトを実行するまで、*Archive*、*Log*、*OVF*、*PlatformConfigRepository* および *Report* フォルダは、空です。

図 *1* : 自動化ツールのダウンロード





スクリプトの初回実行後は：

- *Archive* には、日付とタイムスタンプとともに保存された自動化スプレッドシートの以前のバージョンが保持されます。
- *Log* には、保存されたすべてのログファイルが日付とタイムスタンプとともに保存されます。
- *OVF* では、ツールがエクスポート操作を実行すると、仮想マシンごとにサブフォルダが作成されます。フォルダは、スプレッドシートの GOLDEN_TEMPLATE_NAME セルから名前を取得します。これらのフォルダは、お客様の ESXi ホストに仮想マシンをインポートするために使用されます。
- *PlatformConfigRepository* には、ゴールデン テンプレート プロセスの一部として生成された XML ファイルを保持する 3 つのサブフォルダが入力されます。
- *Report*には、日時の記録とともに保存されたすべての自動化レポートが保持されます。

自動化スプレッドシートの入力

クローン作成プロセスの自動化スプレッドシートに記入するには、表に記載されている情報を入力します。VM 自動化スクリプトを展開では、仮想マシンをカスタマーインスタンスにクローンするためにこの情報が必要です。

次の表で、各仮想サーバーの値と関連するプロパティに関して説明します。

列	ドメインベースの VM	ワークグループベースの VM	VOS ベースの VM
CREATEVM	対応	対応	対応
カスタマイズ	対応	対応	対応
OPERATION			
SOURCE_HOST_IP	*10.10.0.10*	*10.10.0.10*	*10.10.0.10*
SOURCE_DATASTORE_NAME	*Datastore-A0*	*Datastore-A0*	*Datastore-A0*
SOURCE_VMNAME			
OVF_NETWORK1			
OVF_NETWORK2			

列	ドメインベースの VM	ワークグループベースの VM	VOS ベースの VM
GOLDEN_TEMPLATE_NAME	*GT-Rogger*	*GT-CVP-Server*	*GT-CUCM*
NEW_VM_NAME	*CCE-RGR-SIDE-A*	*CVP-SVR-SIDE-A*	*UCM-SUB-SIDE-A*
DEST_HOST_IP	*10.10.1.10*	*10.10.1.11*	*10.10.1.12*
DEST_DATASTORE_NAME	*Datastore-A1*	*Datastore-A3*	*Datastore-A6*
PRODUCT_VERSION			*10.0.1*
COMPUTER_NAME	*CCE-RGR-SIDE-A*	*CVP-SVR-SIDE-A*	*UCM-SUB-SIDE-A*
WORK_GROUP	いいえ	はい	
WORK_GROUP_NAME		*WORKGROUP*	
DOMAIN_NAME	*HCSCC.COM*		*HCSCC.COM* （オプション）
TIME_ZONE_LINUX_AREA			北米
TIMEZONE_LINUX_LOCATION			ロサンゼルス
TIME_ZONE_WINDOWS	*(GMT-08:00)*	*(GMT-08:00)*	
DOMAIN_USER	*HCSCC\administrator*		
DOMAIN_PASSWORD	••••••••		
PRODUCT_KEY	*XXXX-XXXX-XXXX-XXXX*	*XXXX-XXXX-XXXX-XXXX*	
OWNER_NAME	*HCS*	*HCS*	
ORGANIZATION_NAME	シスコ	シスコ	シスコ
ORGANIZATION_UNIT			*HCS*
ORGANIZATION_LOCATION			サンノゼ
ORGANIZATION_STATE			*CA*
ORGANIZATION_COUNTRY			米国
NTP_SERVER			*10.81.254.131*
NIC_NUM	*2*	*1*	*1*
IP_ADDRESS_NIC1	*10.10.10.10*	*10.10.10.20*	*10.10.10.30*
SUB_NET_MASK_NIC1	*255.255.255.0*	*255.255.255.0*	*255.255.255.0*
DEFAULT_GATEWAY_NIC1	*10.10.10.1*	*10.10.10.1*	*10.10.10.1*
DNS_IP_NIC1	*10.10.10.3*	*10.10.10.3*	*10.10.10.3*
DNS_ALTERNATE_NIC1			
IP_ADDRESS_NIC2	*192.168.10.10*		
SUB_NET_MASK_NIC2	*255.255.255.0*		

列	ドメインベースの VM	ワークグループベースの VM	VOS ベースの VM
DEFAULT_GATEWAY_NIC2	*192.168.10.1*		
DNS_IP_NIC2	*192.168.10.3*		
DNS_ALTERNATE_NIC2			
VM_NETWORK			

自動化スクリプトの実行

始める前に

クライアントコンピュータに VMware vSphere PowerCLI をダウンロードしてインストールします。

詳細については、を参照してください。 自動化クローニングと OS のカスタマイズ （2 ページ）

（注） WinImage（32 ビット）が C:\Program Files (x86)\WinImage にインストールされていることを確認します。

（注） 任意の VOS VM をインポートし、WinImage のライセンスされていないコピーがある場合は、各 VOS プラットフォームのポップアップが表示されます。**[OK]** をクリックしてインポートプロセスを続行します。

手順

ステップ 1 管理者としてサインインし、**VMware vSphere PowerCLI (32-bit)** アプリケーションを開きます。

ステップ 2 **get-executionPolicy** コマンドを入力し、制限付き実行ポリシーを決定します。

ステップ 3 ポリシーが制限されている場合は、**set-executionPolicy** コマンドを入力します。`[値を入力（Supply Values）]` プロンプトで、**`Unrestricted`** と入力したら、**`Y`** と入力します。

ローカルコンピュータで署名されていないスクリプトを実行し、他のユーザから署名されたスクリプトを実行するように実行ポリシーを変更します。

ステップ 4 **`CD < GoldenTemplate directory>`** コマンドを入力します。

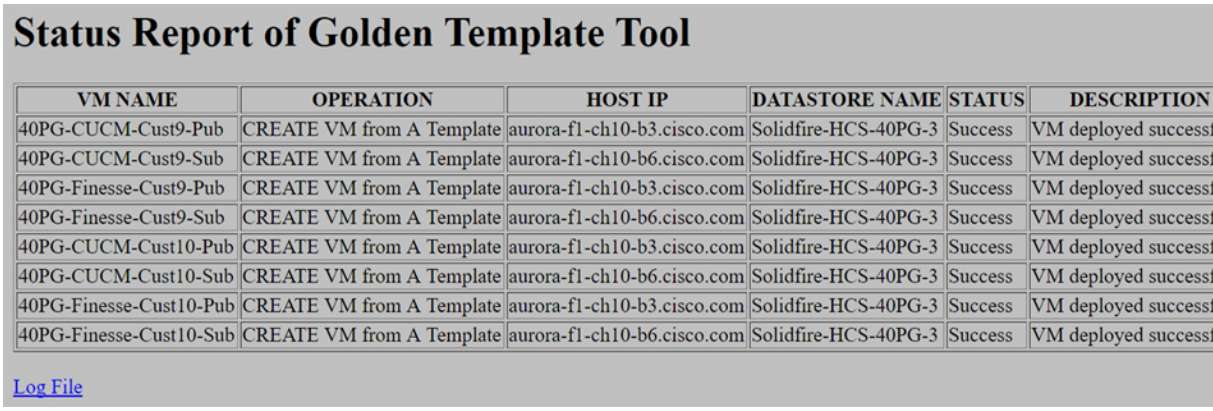
ステップ 5 次のシンタックスを使用して自動化スクリプトを実行します。

シンタックス：	例：
<Path to the script> <Path of the spreadsheet> <vCenter IP / Hostname> <vCenter User> <Password to connect to vCenter>	`.\scripts\DeployVM.PS1 C:\GoldenTemplate\GoldenTemplate_VMDataSheet.xls` **testvCenter testuser testpassword**

これにより、データを解析および検証するスクリプトが開始され、GoldenTemplate ディレクトリにエントリが作成されます。画面に完了率が表示され、[レポート（Report）] フォルダにステータスレポートが生成されます。

ステータスレポート内の [ログファイル（Log File）] リンクをクリックし、エラー状態をデバックし、シスコのサポートにお問い合わせください。

図 *2:* ゴールデ ンテンプレート ツールのステータスレポート



Status Report of Golden Template Tool

VM NAME	OPERATION	HOST IP	DATASTORE NAME	STATUS	DESCRIPTION
40PG-CUCM-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successf
40PG-CUCM-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successf
40PG-Finesse-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successf
40PG-Finesse-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successf
40PG-CUCM-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successf
40PG-CUCM-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successf
40PG-Finesse-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successf
40PG-Finesse-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successf

Log File

次のタスク

OS のカスタマイズプロセス （7 ページ）

OS のカスタマイズプロセス

順序	タスク	完了
Windows のカスタマイズプロセス		
1	ネットワークアダプタ設定と電源投入の検証 （8 ページ）	
2	レジストリ設定の編集および VM の再起動 （9 ページ）	
VOS のカスタマイズプロセス		

順序	タスク	完了
1	DNS サーバーの構成（140 ページ）	
2	DNS サーバーのホスト構成（141 ページ）	
3	ネットワークアダプタ設定と電源投入の検証 （8 ページ）	

ネットワークアダプタ設定と電源投入の検証

すべての Windows VM に対してこの手順を実行します。

手順

ステップ 1 vSphere クライアントで仮想マシンを選択します。[VM] を右クリックし、**[Edit Settings（設定の編集）]** を選択します。

ステップ 2 **[ハードウェア（Hardware）]** タブで各ネットワークアダプタを選択します。[デバイスの状態（Device Status）] グループの **[電源投入時に接続（Connect at power on）]** がオンになっていることを確認します。

ステップ 3 仮想マシンの電源をオンにします。

重要 Ctrl + Alt + Delete は押さないでください。電源投入後に Ctrl + Alt + Delete を押した場合、カスタマイズは反映されません。手動でカスタマイズを完了する必要があります。

ステップ 4 VM が再起動し、カスタマイズを適用するまで待ちます。この処理に 5 ～ 10 分かかることがあります。

電源投入時の *Ctrl+Alt+Del* の押下からの回復

[ネットワークアダプタ設定の検証（Validate Network Adapter Settings）] および [電源オン（Power On）] は、カスタマイズプロセスを初期化します。電源投入後に、**Ctrl-Alt-Delete** を押すことを要求されますが、これを押すとカスタマイゼーションが反映されなくなります。よって、**Ctrl-Alt-Del** は押さないでください。誤って **Ctrl-Alt-Del** を押した場合は、以下のオプションを使用してカスタマイゼーションを復元してください。

手順

ステップ 1 `C:/GoldenTemplateTool/Archive` から GoldenTemplate_VMDataSheet.xls を取得します。

ステップ 2 GoldenTemplate_VMDataSheet.xls コピーし、`C:/GoldenTemplateTool` に貼り付けます。

ステップ 3 GoldenTemplate_VMDataSheet.xls で、再展開が必要な行を除き、CREATEVM 列のすべての行で、**[いいえ（No）]** を選択します。

ステップ 4 もしくは、VM に対して手動でデータを入力します。

レジストリ設定の編集および VM の再起動

すべての Windows VM に対してこの手順を実行します。

手順

ステップ 1 **[スタート（Start）]** > **[すべてのプログラム（All Programs）]** > **[管理ツール（Administrative Tools）]** > **[コンピュータマネージャ（Computer Management）]** の順に選択します。

ステップ 2 左パネルで、**[コンピュータ管理（ローカル）（Computer Management (Local)）]** > **[システムツール（System Tools）]** > **[ローカルユーザーとグループ（Local Users and Groups）]** > **[ユーザー（Users）]** の順に選択します。

ステップ 3 右側のパネルで、[管理者（Administrator）] を右クリックし、**[パスワードの設定（Set Password）]** を選択します。

ステップ 4 警告メッセージで **[続行（Proceed）]** をクリックし、新規パスワードを入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 **[スタート（Start）]** > **[実行（Run）]** > **[Regedit]** の順に選択し、Registry Editor にアクセスします。

ステップ 7 **[HKEY_LOCAL_MACHINE]** > **[ソフトウェア（SOFTWARE）]** > **[Microsoft]** > **[Windows NT]** > **[現在のバージョン（Current Version）]** > **[Winlogon]** の順に選択します。

a) **[AutoAdminLogon]** を **0** に設定します。

b) **DefaultDomainName** と **DefaultUserName** のキーが存在する場合は、これらキーを削除します。

ステップ 8 マシンを再起動します。マシンがドメインに存在する場合は、ドメインにログインします。

ステップ 9 **NET TIME /DOMAIN:<domain>** コマンドを入力し、時間をドメインコントローラと同期します。

OVF を使用した自動化クローニングと OS のカスタマイズ

順序	タスク	完了
1	ゴールデンテンプレート自動化ツールのダウンロード （3 ページ）	

順序	タスク	完了
2	エクスポート用の自動化スプレッドシートの入力 （10 ページ）	
3	エクスポート用の自動化スクリプトの実行 （11 ページ）	
4	目的の場所への転送 （12 ページ）	
5	ロケーションの準備状況の確認 （13 ページ）	
6	インポート用のスプレッドシートの入力 （13 ページ）	
7	インポート用の自動化スクリプトの実行 （17 ページ）	
8	OS のカスタマイズプロセス （7 ページ）	

エクスポート用の自動化スプレッドシートの入力

前提条件：

エクスポートプロセスの前に、VM にエクスポートするネットワークアダプタが 1 つしかないことを確認します。

エクスポートする自動化スプレッドシートを入力したら、エクスポート自動化スクリプトが列のみを入力して、エクスポート自動化スクリプトが、 GoldenTemplate のサブフォルダである *OVF* にエクスポート *OVF* をエクスポートできるようにします。

表 *1:* エクスポート用の自動化スプレッドシートに必要な列

列	説明	例
CREATEVM	VM の作成を省略するには、**[いいえ（No）]** を選択します。	いいえ
OPERATION	**[ExportServer]** を選択してスクリプトで実行する操作をしていします。	ExportServer
SOURCE_HOST_IP	エクスポートする VM をホストする物理サーバーの IP アドレス。	xx.xx.xxx.xxx

列	説明	例
SOURCE_DATASTORE_NAME	VMware で定義されたデータストアの名前。	datastore1(3)
SOURCE_VMNAME	エクスポートする VM の名前には、スペースと特殊文字は使用できません。最大32文字です。	TemplateRoggerA
GOLDEN_TEMPLATE_NAME	エクスポートされた VM の新しい名前にはスペースや特殊文字は使用できません。最大32文字です。	CustomerRoggerA

その他すべての列は空白のままにします。

エクスポート用の自動化スクリプトの実行

エクスポートスクリプトは、エクスポートスプレッドシートのデータを処理し、必要なフィールドが正しい形式かどうかを検証します。

スクリプトにより、目的の場所に OVF をインポートできるフォルダが作成されます。

（注） `GoldenTemplate` ディレクトリからスクリプトを実行します。

始める前に

クライアントコンピュータに VMware vSphere PowerCLI をダウンロードしてインストールします。

詳細については、を参照してください。 自動化クローニングと OS のカスタマイズ （2 ページ）

手順

ステップ 1 **VMware vSphere PowerCLI（32 ビット）**を管理者として起動します。

ステップ 2 **`get-executionPolicy`** コマンドを入力して、制限付き実行ポリシーが有効にするか、無効にするかを決定します。

ステップ 3 ポリシーが制限されている場合は、**`set-executionPolicy`** コマンドを入力します。[値の入力（Supply Values）]プロンプトで、「**`Unrestricted`**」と入力します。次に、「**`Y`**」と入力します。これにより、実行ポリシーが変更され、ローカルコンピュータで作成した未署名のスクリプトと他のユーザーからの署名済みスクリプトを実行できるようになります。

ステップ 4 **`cd < GoldenTemplate directory>`** コマンドを入力します。

ステップ 5 次のシンタックスを使用して、自動化スクリプトを実行するコマンドを入力します。

シンタックス：	例：
<Path to the script> <Path of the spreadsheet> <vCenter IP / Hostname> <vCenter User> <Password to connect to vCenter>	`.\scripts\DeployVM.PS1 C:\GoldenTemplate\GoldenTemplate_VMDataSheet.xls` **testvCenter testuser testpassword**

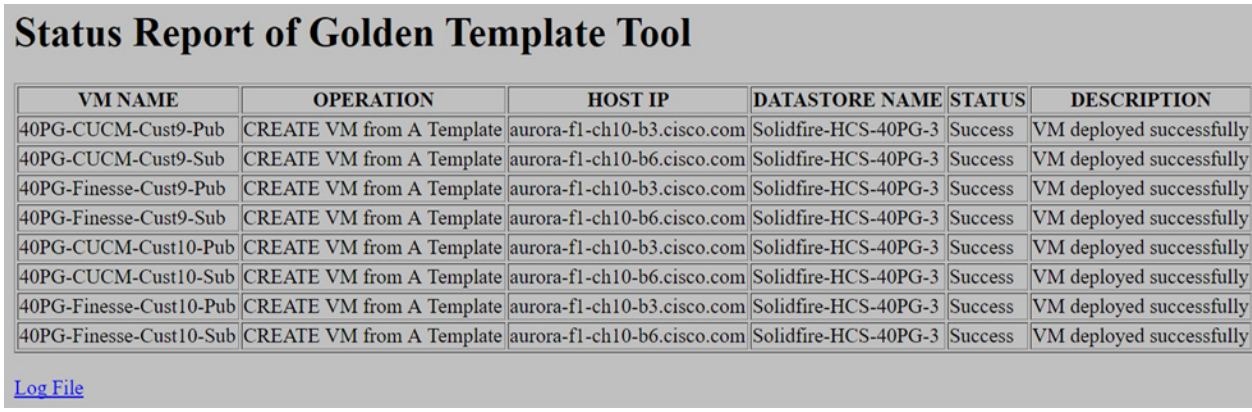
これにより、データを解析、検証し、GoldenTemplate ディレクトリの OVF フォルダにエントリを作成するスクリプトが開始されます。

エラーが発生してもスクリプトは実行されます。エラーが画面に表示され、ログファイルに保存されます。

このタスクが完了するまで、数時間かかります。

スクリプトが完了すると、Report フォルダにステータスレポートが生成されます。ステータスレポートには、ログファイルへのリンクがあります。このファイルを参照して、エラー状態をデバッグし、シスコのサポートにお問い合わせください。

図 *3:* ゴールデ ンテンプレート ツールのステータスレポート



Status Report of Golden Template Tool

VM NAME	OPERATION	HOST IP	DATASTORE NAME	STATUS	DESCRIPTION
40PG-CUCM-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully

Log File

目的の場所への転送

エクスポートプロセスが正常に完了したら、*OVF* ファイルを任意の場所に転送できます。

また、 GoldenTemplate ディレクトリを USB デバイスに転送することもできます。

（注） この場合は、インポートスプレッドシートに入力し、USB ドライブからインポートスクリプトを実行します。

ロケーションの準備状況の確認

インポートスプレッドシートを完成させ、インポートスクリプトを実行する前に、環境を次のように設定する必要があります。

- ESXihost または vCenter
- データストア

インポート用のスプレッドシートの入力

インポート用の自動化スプレッドシートに入力するには、次の表に示す情報を使用します。インポート自動化スクリプトでは、目的の ESXi ホストに仮想マシンをインポートするためにこの情報が必要です。

次の表で、各仮想サーバーの値と関連するプロパティに関して説明します。

表 *2:* インポート用自動化スプレッドシート列の入力

列	説明	例
CREATEVM	**[はい（Yes）]** をクリックすると、VM を作成します。 **[いいえ（No）]** をクリックすると、テンプレートを作成します。	はい
OPERATION	**ImportServer** を選択します。	ImportServer
カスタマイズ	**[はい（Yes）]** を選択すると、インポート済みサーバーにスプレッドシートの値を適用できます。 スプレッドシート入力時に値が無い場合は、**[いいえ（No）]** を選択します。 値がある場合で、**[いいえ（No）]** を選択すると、値は適用されません。	はい
SOURCE_HOST_IP	空欄のまま	空欄のまま
SOURCE_DATASTORE_NAME	空欄のまま	空欄のまま
SOURCE_VMNAME	ブランクのままにします。	ブランクのままにします。

列	説明	例
GOLDEN_TEMPLATE_NAME	*OVF* サブフォルダにあるエクスポートされたゴールデンテンプレートの名前を入力します。	GTCS-1A
NEW_VM_NAME	新しい VM の名前。スペースや特殊文字は使用できません。最大32文字です。	CustomerRoggerA
DEST_HOST_IP	新しい VM の ESXi ホストの IP アドレスまたは DNS 名。	xx.xx.xxx.xxx
DEST_DATASTORE_NAME	新しい VM のデータストアの名前。	datastore2(1)
PRODUCT_VERSION	現在、このフィールドは VOS 製品にのみ適用されます	11.x.x
COMPUTER_NAME	新しいコンピュータの NET BIOS 名。最大 15 文字。特殊文字は使用しないでください。	CUST-Rogger-A
WORK_GROUP	ドロップダウン： **YES** に設定すると VM にワークグループが追加され、WORK_GROUP_NAME が有効化されます。 **NO** に設定すると VM にドメインが追加され、DOMAIN_NAME、 DOMAIN_USER および DOMAIN_PASSWORD が有効化されます。	いいえ
WORK_GROUP_NAME	ワークグループ名を入力します。WORK_GROUP が、**YES** に設定されている場合のみ使用します。	該当なし
DOMAIN_NAME	ドメイン名を入力します。WORK_GROUP が **NO** に設定された場合にのみ使用されます。	xx.xx.xxx.xxx

列	説明	例
TIME_ZONE_LINUX_AREA	Unified CM に設定されるタイムゾーン地域のドロップダウン選択。米国の場合は、*[*米国（*America*）*]* を選択します。	北米
TIME_ZONE_LINUX_LOCATION	Unified CM、CUIC、または Finesse に設定されるタイムゾーンの場所のドロップダウン選択。	東部
TIME_ZONE_WINDOWS	Unified CVP および Unified CCE VM に設定するタイムゾーンのドロップダウンの選択肢。	（GMT-05:00）東部時間（米国およびカナダ）
DOMAIN_USER	新しいコンピュータをドメインに追加する権限を持つドメイン ユーザのユーザ名。WORK_GROUP が **NO** に設定された場合にのみ有効化されます。	DOMAIN\\Username （オプション）
DOMAIN_PASSWORD	package123 ドメインユーザーのパスワード。WORK_GROUP が **NO** に設定された場合にのみ有効化されます。	package123
PRODUCT_KEY	有効な Windows OS プロダクト キー。形式は xxxxx-xxxxx-xxxxx-xxxxx-xxxxx です。	ZZZM2-Y330L-HH123-99Y1B-GJ20B
OWNER_NAME	所有者の完全な名前。 *Administrator* や *Guest* という名前は使用できません。 これは、OS_TYPE が Windows 2016 の場合は必須フィールドです。	LabAdmin
ORGANIZATION_NAME	Unified CM、Cisco Unified Intelligence Center、MediaSense、またはFinesse に設定します。	MyName

列	説明	例
ORGANIZATION_UNIT	Unified CM、Cisco Unified Intelligence Center、MediaSense、またはFinesse に設定します。	MyUnit
ORGANIZATION_LOCATION	Unified CM、Cisco Unified Intelligence Center、MediaSense、またはFinesse に設定します。	MyCity
ORGANIZATION_STATE	Unified CM、Cisco Unified Intelligence Center、MediaSense、またはFinesse に設定します。	MyState
ORGANIZATION_COUNTRY	Unified CM、Cisco Unified Intelligence Center、MediaSense または Finesse に対して **[組織の国（Organization Country）]** ドロップダウンリストを設定します。	アメリカ合衆国
NTP_SERVER	NTP サーバの IP アドレス。	xx.xx.xxx.xxx
NIC_NUM	フィールドの値は VM_TYPE フィールドに基づいて事前に入力されており、保護されています。値は、「1」または「2」です。	2
IP_ADDRESS_NIC1	NIC1 の有効な IPv4 アドレス。 NIC_NUM フィールドの値が 1 の場合にのみ有効です。	xx.xx.xxx.xxx
SUB_NET_MASK_NIC1	NIC1 の有効なサブネットマスク（IPv4 アドレス）。	xx.xx.xxx.xxx
DEFAULT_GATEWAY_NIC1	NIC1 の有効なデフォルトゲートウェイ（IPv4 アドレス）。	xx.xx.xxx.xxx
DNS_IP_NIC1	NIC1 のプライマリ DNS の有効な IPv4 アドレス。	xx.xx.xxx.xxx

列	説明	例
IP_ADDRESS_NIC2	NIC2 の有効な IPv4 アドレス。 NIC_NUM フィールドの値が 2 の場合にのみ有効です。	xx.xx.xxx.xxx
SUB_NET_MASK_NIC2	NIC2 の有効なサブネットマスク（IPv4 アドレス）。Unified CCE VM のみ。	255.255.255.255
DNS_IP_NIC2	NIC2 のプライマリ DNS の有効な IPv4 アドレス。Unified CCE VM のみ。	xx.xx.xxx.xxx
DNS_ALTERNATE_NIC2	NIC2 の代替 DNS の有効な IPv4 アドレス。Unified CCE VM のみ。NIC2 のプライマリ DNS のアドレスとは異なっている必要があります。（オプション）	xx.xx.xxx.xxx
VM_NETWORK	有効なネットワークアダプタ設定	VLAN2

インポート用の自動化スクリプトの実行

スクリプトは、スプレッドシートの値を仮想マシンに適用できるように、OVF ファイルをインポートしてテンプレートに変換します。

（注） 任意の VOS VM をインポートし、WinImage の違法コピーがある場合は、各 VOS のプラットフォームにポップアップダイアログが表示されます。**[OK]** をクリックしてインポートプロセスを続行します。

手順

ステップ 1 **VMware vSphere PowerCLI（32 ビット）**を管理者として起動します。

ステップ 2 **`get-executionPolicy`** コマンドを入力して、制限付き実行ポリシーが有効にするか、無効にするかを決定します。

ステップ 3 ポリシーが制限されている場合は、**`set-executionPolicy`** コマンドを入力します。[値の入力（Supply Values）]プロンプトで、「**`Unrestricted`**」と入力します。次に、「**`Y`**」と入力します。これにより、実行ポリシーが変更され、ローカルコンピュータで作成した未署名のスクリプトと、他のユーザーからの署名済みスクリプトを実行できるようになります。

ステップ 4 **cd < GoldenTemplate directory>** コマンドを入力します。

ステップ 5 次のシンタックスを使用して、自動化スクリプトを実行するコマンドを入力します。

シンタックス：	例：
<Path to the script> <Path of the spreadsheet> <vCenter IP / Hostname> <vCenter User> <Password to connect to vCenter>	`.\scripts\DeployVM.PS1 C:\GoldenTemplate\GoldenTemplate_VMDataSheet.xls` **testvCenter testuser testpassword**

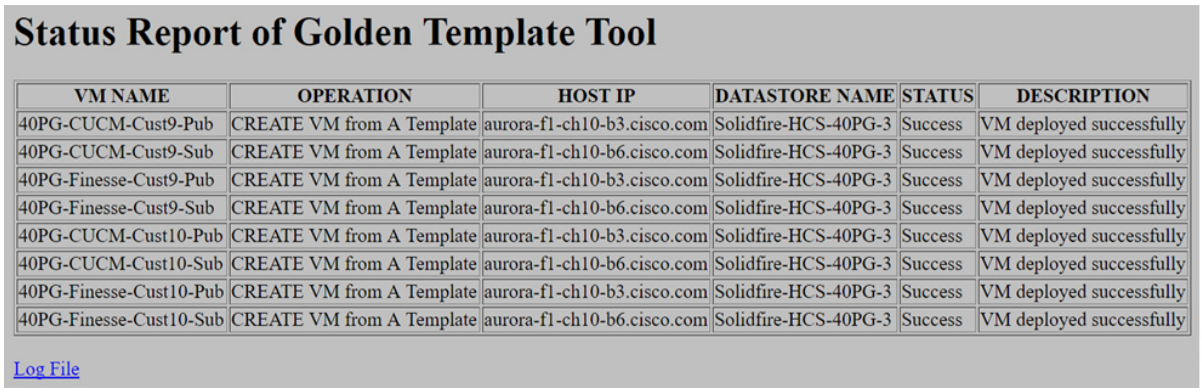
これにより、データを解析し、データを検証し、GoldenTemplate ディレクトリの OVF フォルダから OS レベルのカスタマイズを使用して仮想マシンを展開するスクリプトが開始されます。画面に完了率が表示されます。

エラーが発生してもスクリプトは実行されます。エラーが画面に表示され、ログファイルに保存されます。

このタスクが完了するまで、数時間かかります。

スクリプトが完了すると、Report フォルダにステータスレポートが生成されます。ステータスレポートには、ログファイルへのリンクがあります。このファイルを参照して、エラー状態をデバッグし、シスコのサポートにお問い合わせください。

図 *4:* ゴールデ ンテンプレート ツールのステータスレポート



Status Report of Golden Template Tool

VM NAME	OPERATION	HOST IP	DATASTORE NAME	STATUS	DESCRIPTION
40PG-CUCM-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust9-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust9-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-CUCM-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust10-Pub	CREATE VM from A Template	aurora-f1-ch10-b3.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully
40PG-Finesse-Cust10-Sub	CREATE VM from A Template	aurora-f1-ch10-b6.cisco.com	Solidfire-HCS-40PG-3	Success	VM deployed successfully

Log File

510047

手動クローニングと OS のカスタマイズ

Windows ベースのコンポーネントのカスタマイズファイルの作成

Windowsベースのコンポーネントのカスタマイズファイルを作成するには、以下の手順を実行します。

手順

ステップ 1 VMware vSphere クライアントで、[表示（View）] > [管理（Management）] > [カスタマイズ仕様マネージャ（Customization Specification Manager）] の順に選択します。

ステップ 2 [New] をクリックします。

ステップ 3 新しいカスタマイズ仕様ページで、新しいカスタマイズ仕様を入力します。

a) [対象仮想マシンOS（Target Virtual Machine OS）] メニューから [Windows] を選択します。

b) [カスタマイズ仕様情報（Customization Specification Information）]で、仕様の名前とオプションの説明を入力たら、**[次へ（Next）]** をクリックします。

ステップ 4 登録情報ページで、ゲストオペレーティングシステムのこのコピーの登録情報を指定します。仮想マシンの所有者名と組織を入力したら、**[次へ（Next）]** をクリックします。

ステップ 5 コンピュータ名ページで、ネットワーク上のこの仮想マシンを識別する最適なコンピュータ名オプションをクリックします。

ステップ 6 Windowsライセンスページで、次のゲストオペレーティングシステムの Windows ライセンス情報を指定します。

a) 製品のボリュームライセンスキーを入力します。

b) **[サーバーライセンス情報を含める（Include Server License information）]**（サーバー ゲスト オペレーティング システムをカスタマイズするために必要）をオンにします。

c) **[サーバーごと（Per server）]** をクリックして、サーバーライセンスモードを指定します。サーバーが受け入れる接続の最大数として 5 を入力します。**[次へ（Next）]** をクリックします。

ステップ 7 管理者パスワードページで、管理者アカウントのパスワードを入力し、パスワードを再入力して確認します。**[次へ（Next）]** をクリックします。

ステップ 8 タイムゾーンページで、仮想マシンのタイムゾーンを選択し、**[次へ（Next）]** をクリックします。

ステップ 9 一度実行ページで、**[次へ（Next）]** をクリックします。

ステップ 10 ネットワークページで、ゲスト オペレーティング システムに適用するネットワーク設定のタイプを選択し、**[次へ（Next）]** をクリックします。

a) 標準設定では、vCenter サーバーは DHCP サーバーからすべてのネットワーク インターフェイスを構成できます。

b) カスタム設定では、ネットワーク設定を手動で構成する必要があります

ステップ 11 ワークグループまたはドメインページで、[Windowsサーバードメイン（Windows Server Domain）] をクリックし、指定したドメインにコンピュータを追加する権限を持つユーザーアカウントの接続先ドメイン、ユーザー名、およびパスワードを入力します。

ステップ 12 オペレーティングシステムオプションページで、[新規セキュリティID（SID）の生成（Generate New Security ID（SID））] をオンにして新しいセキュリティ ID を生成し、**[次へ（Next）]** をクリックします。

ステップ 13 完了可能ページで、カスタマイズファイルのサマリーを見直したら、**[完了（Finish）]**をクリックします。

ゴールデンテンプレートから仮想マシンを展開

ゴールデンテンプレートから仮想マシンを展開するには、以下の手順を実行します。展開チェックリストを使用して、展開のホスト、IP アドレス、および SAN の場所を記録します。

手順

ステップ 1 テンプレートを右クリックし、このテンプレートで[仮想マシンの展開（Deploy Virtual Machine）] を選択します。

ステップ 2 仮想マシン名を入力し、場所を選択したら、**[次へ（Next）]** をクリックします。

ステップ 3 ホスト/クラスタページで、テンプレートを保存するホストを指定します。ホスト/クラスタが有効であることを確認します。[次へ（Next）] をクリックします。

ステップ 4 [詳細設定（Advanced）] をクリックします。展開する Contact Center コンポーネントの Cisco HCS for CC に準拠する仮想マシンに対して有効なデータストアを指定します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 インストールするコンポーネントのデータストア RAID レベルが、導入モデルの SAN 構成のテーブルで指定された条件に準拠していることを確認します。

ステップ 7 **[Thick provisioned Lazy Zeroed]** をクリックして、仮想ディスクに一定量のストレージスペースを割り当てます。[次へ（Next）] をクリックします。

ステップ 8 既存のカスタマイズ仕様を使用して**[カスタマイズ（Customize）]**をクリックし、**[次へ（Next）]** をクリックします。

ステップ 9 [テンプレート用カスタマイズファイル（Customization File for the Template）] で作成したカスタマイズファイルを選択します。

ステップ 10 新しい仮想マシンの設定を見直します。**[完了（Finish）]** をクリックします。

VOS 製品仮想マシンの応答ファイル生成

VOS 製品仮想マシンの応答ファイルを生成するには、以下の手順を実行します。

手順

ステップ 1 http://www.cisco.com/web/cuc_afg/index.html のリンクを開きます。

ステップ 2 以下のクラスタ全体パラメータを構成します。

a) [ハードウェア（Hardware）] で、[**プライマリノードのインストール先仮想マシン**（Virtual Machine for Primary Node Installed On）] を選択します。
b) [製品（Product）] で、製品名と製品バージョンを選択します。
c) [管理者のログイン情報（Administrator credentials）] で、管理者のユーザー名とパスワードを入力し、パスワードを確認します。
d) [セキュリティパスワード（Security Password）] で、パスワードを入力し、パスワードを確認します。
e) [アプリケーションユーザーログイン情報（Application user credentials）] で、アプリケーションユーザー名とパスワードを入力し、パスワードを確認します。

すべてのノードで、同じシステムアプリケーションまたは管理者ログイン情報を使用します。

f) [証明書情報（Certificate information）] で、Unified CM および Unified Intelligence Center の組織名、ユニット、場所、都道府県、国を入力します。
g) [SMTP] で、**[SMTPホストの構成（Configure SMTP host）]** ボックスをオンにし、SMTP の場所を入力します。

ステップ 3 次のプライマリ ノード パラメータを構成します。

a) [NICインターフェイス設定（NIC Interface Settings）] で、**[自動ネゴシエーションを使用する（Use Auto Negotiation）]** チェックボックスをオンにします。

（注） MTU 設定は変更しないでください。

b) [ネットワーク情報（Network Information）] で、IP アドレス、ホスト名、IP マスク、およびゲートウェイ情報を入力します。

[IPアドレス解決にDHCPを使用する（Use DHCP for IP Address Resolution）] オプションは選択しないでください。

c) [DNS] で、**[クライアントDNSの構成（Configure Client DNS）]** オプションを選択し、プライマリ DNS IP と DNS 名を入力します。
d) [タイムゾーン（Timezone）] で、**[プライマリタイムゾーン設定を使用する（Use Primary Time Zone Settings）]** オプションを選択します。
e) [ネットワークタイムプロトコル（Network Time Protocol）] で、**[ネットワークタイムプロトコルを使用する（Use Network Time Protocol）]** をオンにし、少なくとも 1 台の外部 NTP サーバーに対して IP アドレス、NTP サーバー名、またはNTP サーバープール名を入力します。

ステップ 4 次のセカンダリノードパラメータを構成します。

a) [NICインターフェイス設定（NIC Interface Settings）] で、**[自動ネゴシエーションを使用する（Use Auto Negotiation）]** チェックボックスをオンにします。

（注） MTU 設定は変更しないでください。

b) [ネットワーク情報（Network Information）] で、IP アドレス、ホスト名、IP マスク、およびゲートウェイ情報を入力します。

[IPアドレス解決にDHCPを使用する（Use DHCP for IP Address Resolution）] オプションは選択しないでください。

c) [DNS] で、**[クライアントDNSの構成（Configure Client DNS）]** オプションを選択し、プライマリ DNS IP と DNS 名を入力します。

d) [タイムゾーン（Timezone）] で、**[プライマリタイムゾーン設定を使用する（Use Primary Time Zone Settings）]** をオンにします。

e) [セカンダリノードの一覧（List of Secondary Nodes）]で、**[セカンダリノードの追加（Add Secondary Node）]** をクリックします。

ステップ 5 **[応答ファイルとライセンスMACの生成（Generate Answer files & License MAC）]** をクリックし、Publisher と 1 つ目の Subscriber に対して応用ファイルをダウンロードします。

（注） Unified CM の場合は、2 つ目の Subscriber に対する応答ファイルが必要な場合は、応答ファイルジェネレータ Web ページを閉じて開き、Publisher と 2 つ目の Subscriber の詳細を入力します。1 つ目の Subscriber と一緒に Publisher ファイルをすでにダウンロードしているので、2 つ目の Subscriber の応答ファイルのみをダウンロードします。

ステップ 6 VM に応答ファイルをマウントには、セクションに記載されている手順を実行します。

仮想マシンに応答ファイルをコピー

ゴールデンテンプレート自動化ツールは、無人インストール用の応答ファイルを生成します。各応答ファイルは、*C:\GoldenTemplateTool_lO\PlatformConfigRepository* ディレクトリにコピーされます。これらの応答ファイルはフロッピーディスクファイル形式に変換され、インストールプロセス中に VOS 製品 DVD に加えて使用されます。

始める前に

自動化スクリプトを実行するクライアントコンピュータにWinImage 8.5 をダウンロードし、インストールします。http://winimage.com/download.htm

手順

ステップ 1 生成された応答ファイルをフォルダにコピーし、その名前を platformConfig.xml に変更します。

例：

CUCM_PUB_SideA_platformConfig.xml を別のロケーションにコピーしたら、その名前を platformConfig.xml に変更します。

ステップ 2 WinImage を起動し、**[ファイル（File）]** > **[新規（New）]** > **[1.44 MB]** の順に選択し、**[OK]** をクリックします。

ステップ 3 *platformConfig.xml*をドラッグし、WinImage にドロップします。

ステップ 4 ファイルを挿入するように求められたら、**[はい（Yes）]** をクリックします。

ステップ 5 **[ファイル（File）]** > **[名前を付けて保存（Save as）]** の順に選択します。

ステップ 6 **[タイプとして保存（Save as type）]** リストから、**[仮想フロッピー画像（Virtual floppy image）]** を選択します。ファイルに *platformConfig.flp* という名前を付け、**[保存（Save）]** をクリックします。

ステップ 7 vSphere インフラストラクチャ クライアントを開き、vCenter に接続します。VM が展開されているお客様の ESXi ホストに移動します。

ステップ 8 [構成（Configuration）] タブに移動します。ストレージセクションにある [データストア（Datastore）] を右クリックし、**[データストアを参照（ Browse Datastore）]** を選んだら、<Product_Node> という名前のフォルダを作成します。

例：

CUCM_PUB。

ステップ 9 <Product_Node> というフォルダに *platformConfig.flp* を**アップロード**します。

例：

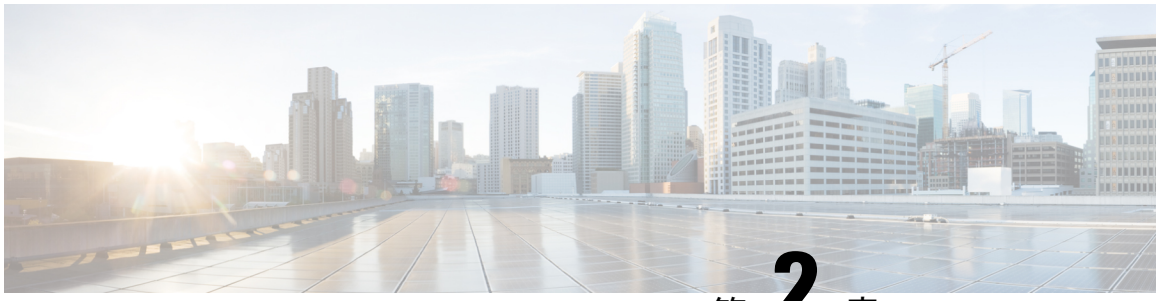
CUCM_PUB。

ステップ 10 <Product_Node> Virtual Machine（例：*CUCM_PUB_SideA*）に移動します。右クリックして、**[設定の編集（Edit Settings）]** を選択します。

ステップ 11 [ハードウェア（Hardware）] タブで、**[フロッピードライブ1（Floppy drive 1）]** をクリックし、**[データストアの既存のフロッピー画像を使用する（Use The Existing Floppy Image in Datastore）]** ラジオボタンを選択します。

ステップ 12 データストアで、<Product_Node> folder （例：*CUCM_PUB*） から **platformConfig.flp** をマウントし、**[OK]** をクリックします。

ステップ 13 ネットワークアダプタとフロッピードライブに対して、デバイスのステータスが、**[電源投入時に接続（Connect at Power On）]** になっていることを確認し、**[OK]** をクリックします。



第 2 章

カスタマー インスタンスの設定

2000 エージェント導入モデルのカスタマーインスタンスの構成

Contact Center 用 に Cisco HCS for CC に対して2000 エージェントを展開するカスタマーインスタンスを作成するには、次の一連のタスクに従います。

表 *3 : Contact Center* 用 *Cisco HCS for CC* に対する *2000* エージェント展開に対してカスタマーインスタンスを作成

順序	タスク	完了したか
1	VMware ツールのアップグレード （26 ページ）	
2	仮想マシンの起動とシャットダウンの設定 （26 ページ）	
3	ドメイン コントローラ サーバーの作成 （27 ページ）	
4	Cisco Unified CCE Rogger の構成 （30 ページ）	
5	Unified CCE AW-HDS-DDS の構成 （41 ページ）	
6	Unified CCE PG の構成 （47 ページ）	
7	Unified CVP の構成 （60 ページ）	
8	Cisco IOS Enterprise 音声ゲートウェイの構成 （81 ページ）	

順序	タスク	完了したか
9	Unified Communications Manager の構成 （87 ページ）	
10	Unified Intelligence Center Coresident 展開の構成 （93 ページ）	
11	Cisco Finesse の構成 （110 ページ）	

VMware ツールのアップグレード

手順

ステップ 1 VM を右クリックします。**[ゲスト（Guest）]** > **[VMwareツールのインストール/アップグレード（Install/Upgrade VMware tools）]** の順に選択します。

ステップ 2 ポップアップウィンドウが表示されるまで待ち（時間がかかる場合があります）、デフォルトの Automatic Tools Upgrade を許可します。

ステップ 3 [OK] をクリックします。

ステップ 4 プロンプトが表示された場合にのみ、再起動します。

（注） VMWare ツールは、すべての VM にインストールされ、最新の状態である必要があります。

仮想マシンの起動とシャットダウンの設定

手順

ステップ 1 **[VMware vSphereクライアント（VMware vSphere Client）]** ウィンドウで、**[ESXiサーバー（ESXi server）]** を選択します。

ステップ 2 [構成（Configuration）] タブをクリックします。

ステップ 3 **Virtual Machine Startup/Shutdown** リンクをクリックします。

ステップ 4 **[プロパティ（Properties）]**をクリックします。

ステップ 5 **[仮想マシンの起動とシャットダウン（Virtual Machine Startup and Shutdown）]** ダイアログボックスで、**[システムによる仮想マシンの自動起動と自動停止を許可（Allow Virtual machines to start and stop automatically with the system）]** チェックボックスをオンにします。

ステップ 6 **[上へ移動（Move Up）]** および **[下へ移動（Move Down）]** ボタンを使用して、**[自動起動（Automatic Startup）]** の下の仮想マシンを次の順序で並べ替えます。

- Cisco Unified CCE 中央コントローラサーバー

- Cisco Unified CCE 管理およびデータサーバー
- Cisco Unified CCE PG サーバー
- Cisco Unified CVP サーバー
- Cisco Finesse サーバー
- Cisco Unified Intelligence Center
- Cisco Unified Communication Manager
- Cisco Unified CVP レポーティングサーバー
- Cisco Unified CVP OAMP サーバー

ステップ 7 [OK] をクリックします。

ドメイン コントローラ サーバーの作成

ドメインコントローラの仮想マシンの作成

手順

ステップ 1 「仮想マシンの起動とシャットダウンの設定 （26 ページ）」を参照して、vCenter から新しい仮想マシンを作成します。

ステップ 2 **名前と場所**ページで、**ドメインコントローラ**の名前を指定します。

ステップ 3 **[ディスク形式（Disk format）]** フィールドで、**シックプロビジョニング**形式を選択します。

ステップ 4 仮想マシンの仕様を入力します。『*Cisco Hosted Collaboration Solution for Contact Center* 用ソリューション設計ガイド』の「*HCSCC* 用ドメインおよび *Active Directory* の考慮事項」の項を参照してください（http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html）。

ウイルス対策ソフトウェアのインストール

この手順は、ゴールデンテンプレートおよび直接インストールの両方のオプションに対して実行します。

Unified CCE コールサーバー、Unified CCE データサーバー、Unified CVP サーバー、Unified CVP OAMP サーバーおよび Unified Reporting サーバー用に以下のいずれかのウイルス対策ソフトウェア製品をインストールします。

- McAfee® VirusScan® Enterprise
- Symantec® Endpoint Protection
- Trend Micro Server Protect Version

Contact Center 用に HCS for CC がサポートしているウイルス対策ソフトウェアおよびバージョンについては、https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html の 「*CC* の互換性に関する *HCS* 用情報」を参照してください。

エンタープライズチャットおよびEメール（ECE）用に以下のいずれかのウイルス対策ソフトウェア製品をインストールします。

- McAfee® VirusScan® Enterprise
- Symantec® AntiVirus® Corporate Edition

重要 ウイルス対策ソフトウェアを手動で更新します。自動更新を有効にしないでください。

ヒント インストール プログラム ファイルまたはフォルダに対して必要なアクセスを許可するには、ウイルス対策製品のファイルおよびフォルダ保護ルールでファイルブロックの除外を実行します。McAfee VirusScan でこれを行うには、次の手順を実行します。

- VirusScan コンソールを起動します。
- **[アクセス保護（Access Protection）]** を右クリックし、**[プロパティ（Properties）]** を選択します。
- **[ウイルス対策標準保護（Anti-virus Standard Protection）]** カテゴリの **Block** 列で、[IRC通信不可（Prevent IRC communication）] チェックボックスがオフになっていることを確認します。

重要 Contact Center 用 HCS for CC は Symantec Endpoint Protection をサポートしています。

Symantec Endpoint Protection 12.1 のファイアウォールコンポーネント、ネットワーク驚異の防止機能は必ず無効にしてください。デフォルトでは有効になっていますが、有効な場合、デュプレックスルーターの両サイドがシンプレックスモードで稼働するため、ルーターの両サイド間の通信がブロックされます。このブロックは、すべての導入タイプに影響します。

デフォルト（有効の状態）をそのまま使用し、ルーターのサイド A およびサイド B でサービスを開始した場合、「クライアントは IP アドレス [サイド A 側のルーターアドレス] からのトラフィックを、今後 600 秒遮断します（The client will block traffic from IP address [side A router address] for the next 600 seconds(s)）」という Symantec メッセージがシステムトレイに表示されます。このメッセージは、クライアント管理セキュリティログにも表示されます。Symantec Network Threat Protectionトラフィックログには、「Block_all」と呼ばれるデフォルトのファイアウォール ルールが動的に有効化されたことが示されます。ルーターの両サイドの結果は、シンプレックスモードで表示されます。

この問題を回避するには、**Symantec** ファイアウォールを無効化にして、ルーターの両サイドを再起動する必要があります。これを実行するには、システムトレイの Symantec アイコンをダブルクリックし、**[設定の変更（Change Settings）]** を選択します。次に、ネットワーク脅威防止の設定を構成し、[ファイアウォール（Firewall）] タブの上部にある **[ファイアウォールを有効化（Enable Firewall）]** をオフにします。

ポートブロッキングの無効化

ポートをブロックするよう構成したアンチウィルスソフトウェアがあるコールサーバーやレポーティングサーバーなどの Unified CVP コンポーネントを実行するコンピュータでは、Unified CVP プロセスと `tomcat6.exe` は除外されます。また、コールサーバープロセスでは、VoiceBrowser.exe も除外する必要があります。

（注） McAfee Virus Scan 以外のウイルス対策ソフトウェアを使用している場合は、そのアンティウィルスソフトウェアのポート ブロッキング ルールで同等の除外を実行します。

手順

ステップ 1 **McAfee** を起動します。

ステップ 2 **VirusScanコンソール** で、**[アクセス保護（Access Protection）]** をダブルクリックし、**[ウイルス対策標準保護（Anti-Virus Standard Protection）]** を選択します。

ステップ 3 リストから **[IRC通信の防止（Prevent IRC communication）]** を選択し、**[編集（Edit）]** をクリックします。

ステップ 4 **[除外プロセス（Processes to Exclude）]** に `tomcat6.exe`、`tomcat5.exe`、`VoiceBrowser.exe` を追加し、**[OK]** をクリックします。

ステップ 5 [OK] をクリックします。

DNS サーバーの構成

DNS サーバーを構成するには、「DNS サーバーの構成 （140 ページ）」を参照してください。

ドメインコントローラの設定

ドメインコントローラを設定するには、以下の手順を実行します。

手順

ステップ 1 **[スタート（Start）]** > **[実行（Run）]** の順に選択し、**`dcpromo.exe`** と入力します。
ステップ 2 **[次へ（Next）]** をクリックし、Active Directory Domain Services Wizard を起動します。
ステップ 3 **[オペレーティングシステムの互換性]**ページで、**[次へ（Next）]** をクリックします。
ステップ 4 **展開構成を選択**ページで、**[新規フォレストで新規ドメインを作成する（Create a new domain in a new forest ）]** のラジオボタンを選択し、**[次へ（Next）]** をクリックします。
ステップ 5 **フォレストルートドメインに名前を付ける**ページで、完全修飾ドメイン名（FQDN）を入力し、**[次へ（Next）]** をクリックします。
ステップ 6 **フォレスト機能レベルの設定**ページのドロップダウンリストで **Windows Server 2008 R2** を選択し、**[次へ（Next）]**をクリックします。
ステップ 7 **追加ドメイン コントローラ オプション** ページで、**[DNSサーバー（DNS Server）]** を選択し、**[次へ（Next）]** をクリックします。
ステップ 8 **データベースのロケーション**、**ログファイル**、および**SYSVOL**ページで、デフォルトのフォルダを選択し、**[次へ（Next）]** をクリックします。
ステップ 9 **ディレクトリサービス復元モードの管理者パスワード**ページに記載されている基準を満たすパスワードを入力し、**[次へ（Next）]** をクリックします。
ステップ 10 **[次へ（Next）]** をクリックします。
ステップ 11 **[完了（Finish）]** をクリックし、Windows を再起動します。

双方向フォレストトラストの作成

Unified CCE および CCDM 間の双方向フォレストトラストを作成するには、「双方向フォレストトラストの確立 （158 ページ）」を参照してください。

Cisco Unified CCE Rogger の構成

このテーブルでは、Cisco Unified CCE Rogger を構成する際に実行すべき手順を説明します。

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ドメイン内マシンの検証 （33 ページ）	
3	ドメインマネージャの構成 （34 ページ）	
4	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	
5	CCE コンポーネント用 SQL Server の設定 （36 ページ）	
6	セカンダリドライブの構成 （36 ページ）	
7	Unified CCE Logger の構成 （37 ページ）	
8	Unified CCE ルーターの構成 （39 ページ）	
9	基本構成のロード （40 ページ）	
10	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
11	Cisco SNMP の設定 （56 ページ）	

ネットワークカードの構成

（注） 2 つのネットワークアダプタを持つすべての Unified CCE 仮想マシンに対してこれを実行します。

手順

ステップ 1 **[スタート（Start）]** > **[コントロールパネル（Control Panel）]** > **[ネットワークとインターネット（Network and Internet）]** > **[ネットワークと共有センター（Network and Sharing Center）]** の順に選択します。

ステップ 2 **[アダプタ設定の変更（Change adapter settings）]** をクリックして、ネットワーク接続ページを開きます。

ステップ 3 Visible IP アドレス構成のネットワークアダプタの名前を **Visible** に変更します。

ステップ 4 プライベート IP アドレス構成のネットワークアダプタの名前を **Private** に変更します。

ステップ 5 **ネットワーク接続**ページで、**Alt + N** を押し、[詳細（Advanced）] メニューを表示します。

ステップ 6 **[詳細（Advanced）]** メニューで、**[詳細設定（Advanced Settings）]** を選択します。

ステップ 7 **[アダプタとバインド（Adapters and Bindings）]** で、**visible** が一番上に表示されるよう、接続をソートします。

ステップ 8 [OK] をクリックします。

プライベート イーサネット カードの構成

手順

ステップ 1 **private** を右クリックし、**[プロパティ（Properties）]** を選択します。

ステップ 2 **[Microsoftネットワーク用クライアント（Client for Microsoft Networks）]** をオフにします。

ステップ 3 **[Microsoftネットワーク用ファイルおよびプリンタ共有（File and Printer Sharing for Microsoft Networks）]** をオフにします。

ステップ 4 **[インターネットプロトコルバージョン6（TCP/IPV6）（Internet Protocol Version 6 (TCP/IPV6)）]** をオフにします。

ステップ 5 **[インターネットプロトコルバージョン4（TCP/IPV4）（Internet Protocol Version 4 (TCP/IPV4)）]** をオンにして、**[プロパティ（Properties）]** をクリックします。

a) デフォルトゲートウェイの IP アドレスを削除します。
b) 優先 DNS サーバーの IP アドレスを削除します。
c) 代替 DNS サーバの IP アドレスを削除します。

ステップ 6 [詳細設定（Advanced）] ボタンをクリックします。[DNS] タブを開きます。**[DNS でこの接続のアドレスを登録（Register this connection's addresses in DNS）]** をオフにします。

ステップ 7 プライベート IP アドレスのエントリを追加します。

ステップ 8 オプション：プライベートハイ IP アドレスの別のエントリを追加します。

ステップ 9 **[OK]** を 2 回クリックします。そして、**[閉じる（Close）]** をクリックします。

プライベート イーサネット カードの構成

手順

ステップ 1 **Visible** を右クリックし、**[プロパティ（Properties）]** を選択します。

ステップ 2 **[Microsoftネットワーク用クライアント（Client for Microsoft Networks）]** をオンにします。

ステップ 3 **[Microsoftネットワーク用ファイルおよびプリンタ共有（File and Printer Sharing for Microsoft Networks）]** をオンにします。

ステップ 4 **[インターネットプロトコルバージョン6（TCP/IPV6）（Internet Protocol Version 6 (TCP/IPV6)）]** をオフにします。

ステップ 5 **[インターネットプロトコルバージョン4（TCP/IPV4）（Internet Protocol Version 4 (TCP/IPV4)）]** をオンにして、**[プロパティ（Properties）]** をクリックします。

ステップ 6 **パブリック IP アドレス**、**サブネットマスク**、**デフォルトゲートウェイ**、および**優先 DN サーバー**を確認し、**[詳細設定（Advanced）]** をクリックします。

ステップ 7 **[詳細設定（Advanced）]** タブで、上位のパブリックアドレスを入力します。

ステップ 8 [DNS] タブの [この接続のDNS接続（DNS connection for this connection）] フィールドに、サーバーのローカル DNS ゾーンの名前を入力し、**[DNSにこの接続アドレスを登録する（Register this connection's addresses in DNS）]** をオンにします。

ステップ 9 オプション：パブリックハイ IP アドレスの別のエントリを追加します。

ステップ 10 サーバーが別の信頼ドメインまたはDNSゾーンのリソースへのアクセスを必要とする場合は、**[これらのDNSサフィックスを順番に追加（Append these DNS Suffixs (in order)）]** を選択し、サーバーのローカル DNS ゾーンを最初に入力してから、信頼ドメインがある別のセカンダリゾーンを追加します。

ステップ 11 **[OK]**を 2 回クリックします。そして、**[閉じる（Close）]** をクリックします。

ローカル管理者パスワードの設定

手順

ステップ 1 **[コンピュータの管理（Computer Management）]** を開きます。

ステップ 2 左側のペインで、**[ローカルとユーザーグループ（Local and Users Groups）]** を展開し、**[ユーザー（Users）]** を選択します。

ステップ 3 右ペインで、**[管理者（Administrator）]** を右クリックし、**[パスワードの設定（Set Password）]** を選択します。
[管理者用パスワードの設定（Set Password for Administrator）] ダイアログボックスが表示されます。

ステップ 4 [続行（Proceed）] をクリックします。

ステップ 5 **[新しいパスワード（New Password）]** と **[確認用パスワード（Confirm Password）]** を入力します。

ドメイン内マシンの検証

Unified CCE ゴールデンテンプレートの場合、自動化ツールスクリプトは仮想マシンを複製し、接続先ドメインに自動的に展開します。仮想マシンが接続先ドメインに配置されているかどうかを確認するには、以下の手順を実行します。

Small Contact Center 導入モデルの場合、エージェント PG は、サービスプロバイダドメインではなくカスタマードメインに配置できます。

始める前に

ローカル管理者パスワードの設定 （33 ページ）

手順

ステップ 1 Unified CCE マシンにログインします。

ステップ 2 **[スタート（Start）]** > **[すべてのプログラム（All Programs）]** > **[管理ツール（Administrative Tools）]** > **[サーバーマネージャ（Server Manager）]** の順に選択し、仮想マシンが適切なドメインにマッピングされているか確認します。マシンがドメインにない場合は、以下の手順を実行します。

ステップ 3 右側のパネルで **[システムプロパティの変更（Change System Properties）]** をクリックして、[システムプロパティ（System Properties）] を開きます。

ステップ 4 [コンピュータ（Computer）] タブで、**[変更（Change）]** をクリックします。

ステップ 5 **[ドメイン（Domain）]** ラジオボタンを選択し、メンバーをワークグループからドメインに変更します。

ステップ 6 全修飾ドメイン名を入力し、**[OK]** をクリックします。

ステップ 7 [Windows のセキュリティ] ポップアップで、ドメインのログイン情報を確認して、**[OK]** をクリックします。

ステップ 8 認証が成功したら、**[OK]**をクリックします。

ステップ 9 サーバをリブートしたら、ドメインのログイン情報を使用してログインします。

ドメインマネージャの構成

この手順では、いずれかの Unified CCE コールサーバーから組織ユニット（Cisco_Unified CCE、ファシリティ、インスタンス）を作成します。

（注） ドメインマネージャの構成は、1 回のみです。サイド B のドメインマネージャを構成する必要はありません。

（注） Small Contact Center エージェント導入モデルの場合、以下の手順を実行して、Unified CCE ドメインと同様のサブカスタマードメインでエージェント PG の OU 構造を作成するか、Unified CCE ドメインにエージェント PG をインストールする場合は、以下の手順を省略します。

手順

ステップ 1 **Windows のスタート** アイコンをクリックして、下向きの矢印アイコンを選択して、すべてのアプリケーションを表示します。

ステップ 2 アプリケーションの一覧から **ドメイン マネージャ** アイコンを選択します。

ステップ 3 ドメインで組織ユニット（OU）を作成できる権限を持つユーザーとしてログインします。

ステップ 4 左側のセクションで、ドメインを展開します。

ステップ 5 Cisco_Unified CCE として Cisco Root を追加します。

a) [Ciscoルート（Cisco root）] の下の [追加（Add）] をクリックします。

b) Cisco ルート OU を作成する **OU** を選択し、[OK] をクリックします。

[ドメインマネージャ（Domain Manager）] ダイアログボックスに戻る際、ドメインルートまたは 選択した OU 配下で Cisco root OU が表示されます。これでファシリティを追加できます。

ステップ 6 ファシリティ組織単位（OU）を追加します。

a) ファシリティ OU を作成する Cisco Root OU を選択します。

b) 右側のセクションの [ファシリティ（Facility）] の下で、[追加（Add）] をクリックします。

c) **[ファシリティ（Facility）]** に名前を入力し、**[OK]** をクリックします。

ステップ 7 インスタンス OU を追加します。

a) インスタンス OU を作成するファシリティ OU に移動し、選択します。

b) 右側のセクションの [追加（Add）] をクリックします。

c) インスタンス名を入力し、[OK] をクリックします。

ステップ 8 [閉じる（Close）] をクリックします。

Unified CCE 暗号化ユーティリティの構成

手順

ステップ 1 **[すべてのプログラム（All Programs）]** > **[Cisco Unified CCE ツール（Cisco Unified CCE Tools）]** を起動します。

ステップ 2 **[SSL暗号化ユーティリティ（SSL Encryption Utility）]** を選択します。

ステップ 3 **[証明書の管理（Certificate Administration）]** タブをクリックします。

ステップ 4 [アンインストール（Uninstall）] をクリックします。[はい（Yes）] を選択します。

ステップ 5 アンインストールが完了したら、**[インストール（Install）]** を選択します。

「*SSL*証明書が正常にインストールされました（*SSL Certificate successfully installed*）」で終わる一連のメッセージが表示されます。

ステップ 6 [閉じる（Close）] をクリックします。

次のタスク

System CLI 証明書の作成とバインド （36 ページ）

System CLI 証明書の作成とバインド

システムの CLI 証明書の作成とバインドをするには、以下の手順を実行します。

手順

ステップ 1 コマンド プロンプトを開きます。
ステップ 2 **cd C:\icm\serviceability\diagnostics\bin** のコマンドを入力し、**Enter** キーを押します。
ステップ 3 **DiagFwCertMgr /task:CreateAndBindCert** のコマンドを入力し、**Enter** キーを押します。

CCE コンポーネント用 SQL Server の設定

手順

ステップ 1 **Windows のスタート** アイコンをクリックして、下向きの矢印アイコンを選択して、すべてのアプリケーションを表示します。
ステップ 2 **Microsoft SQL Server Management Studio** を開きます。
ステップ 3 ログインします。
ステップ 4 [セキュリティ（Security）] と [ログイン（Logins）] を順に展開します。
ステップ 5 BUILTIN \ Administrator グループが表示されていない場合:
a) [ログイン（Logins）] を右クリックし、[新しいログイン（New Login）] を選択します。
b) [検索（Search）] をクリックし、[場所（Locations）] を選択して、ドメイン ツリー内の BUILTIN の場所を見つけます。
c) **Administrators** と入力し、[名前の確認（Check Name）] をクリックし、[OK] をクリックします。
d) [BUILTIN\Administrators] をダブルクリックします。
e) [サーバ ロール（Server Roles）] を選択します。
f) **public** および **sysadmin** の両方のチェックがオンになっていることを確認します。

セカンダリドライブの構成

データをアーカイブするために追加のハードドライブが必要な仮想マシンに対してこれを実行します。

手順

ステップ 1 **[コンピュータの管理（Computer Management）]** を開きます。

ステップ 2 左ペインの **[ストレージ（Storage）]** を展開し、**[ディスク管理（Disk Management）]** をクリックします。

ステップ 3 **[ディスク 1（Disk 1）]** を右クリックし、**[オンライン（Online）]** を選択します。

ステップ 4 **[ディスク 1（Disk 1）]** を右クリックし、**[ディスクの初期化（Initialize Disk）]** を選択します。

ステップ 5 [ディスクの選択（Select Disks）] の下の [ディスクの初期化（Initialize Disk）] ポップアップ ウィンドウで、**[ディスク 1（Disk 1）]** をオンにし、**[選択したディスクに次のパーティションを使用する（Use the following partition style for the selected disks）]** ペインの **[MBR（マスター ブートレコード（MBR (Master Boot Record)）]** を選択します。[OK] をクリックします。

ステップ 6 初期化されたディスクを右クリックし、[新しいシンプル ボリューム（New Simple Volume）] を選択し、ウィザードを実行して、新しいディスクパーティションを作成します。

Unified CCE Logger の構成

サイド A とサイド B に対して Unified CCE Logger を構成します。

（注） ブラウザが有効になっていることを確認します。

手順

ステップ 1 **Unified CCE Web 設定** を起動します。

ステップ 2 ローカルの管理者権限を持つドメイン ユーザとしてサインインします。

ステップ 3 **[インスタンス管理（Instance Management）]** > **[追加（Add）]** の順に選択します。

ステップ 4 **[インスタンスの追加（Add Instance）]** ウィンドウのドロップダウンリストで、**[ファシリティ（Facility）]** と **[インスタンス（Instance）]** を選択します。

ステップ 5 **インスタンス数** フィールドで、**0** と入力して、**保存**をクリックします。

ステップ 6 以下の手順に従って、Logger データベースを設定します。

a) **ICMDBA** アプリケーションを開きます。

b) **サーバー** > **インスタンス**（Logger がインストールされている先）を選択します。

c) インスタンス名を右クリックして、**[作成（Create）]** を選択し、Logger データベースを作成します。

d) **コンポーネントの選択** ダイアログ ボックスで、作業中の Loggerを選択します（Logger A または Logger B）。[OK] をクリックします。

e) **Logger タイプの選択** ウィンドウで、ドロップダウンリストから **エンタープライズ** を選択します。[OK] をクリックします。

ステップ 7 **データベースの作成** ウィンドウで、以下の通り設定してログを作成します。

a) **DB タイプ** ドロップダウンリストで、**サイド A** または**サイド B** を選択します。

b) **リージョン**を選択します。

c) **ストレージ** ペインで、**追加**をクリックします。

ステップ 8 **デバイスの追加** ダイアログ ボックスで、以下の通り設定します。

a) **ログ** を選択します。
b) **C** ドライブを選択します。
c) [サイズ] フィールドでデフォルトを受け入れます。
d) [OK] をクリックします。

ステップ 9 **データベースの作成** ウィンドウの **ストレージ** セクションで、**追加** をクリックします。

ステップ 10 **デバイスの追加** ダイアログ ボックスで、以下の通り設定します。

a) **データ** を選択します。
b) セカンダリ ドライブ (通常は E) を選択します。
c) [サイズ] フィールドでデフォルトを受け入れます。
d) [OK] をクリックします。

ステップ 11 **データベースの作成** ウィンドウで、**作成** をクリックして、**起動**をクリックします。

正常に作成が完了したメッセージが表示されたら、 **OK** をクリックして、 **閉じる**をクリックします。

ステップ 12 Logger コンポーネントを以下の通り設定します。

a) [Unified CCE Web 設定（Unified CCE Web Setup）] に戻ります。再度ログインしなければならない場合があります。
b) **[コンポーネント管理（Component Management）]** > **[Loggers]** の順に選択します。
c) **追加**をクリックして、**インスタンス** を選択します。
d) **[フォールトトレランスモード（Fault Tolerance Mode）]** ドロップダウンリストで、**[デュプレックス（Duplexed）]** を選択し、**[次へ（Next）]** をクリックします。
e) **セントラル コントローラの接続** ウィンドウで、ルータ プライベート インターフェイスおよび Logger プライベート インターフェイスに、サイド A およびサイド B のホスト名を入力して、 **次へ**をクリックします。

ステップ 13 **その他のオプション** ウィンドウで、以下の通り設定します。

a) **履歴および詳細データ複製を有効にする** をオンにします。
b) **データベースの消去構成手順の表示** チェックボックスをオンにして、 **次へ**をクリックします。

ステップ 14 **データ保存期間** ウィンドウのデータ保持テーブルでは、デフォルト値を保持して**次へ**をクリックします。

ステップ 15 **データの消去** ページで、システム上で需要が低い曜日と時間の消去を設定します。[次へ（Next）] をクリックします。

次のタスク

データベースとログファイルのサイズの設定については、データベースとログファイルのサイズ （39 ページ）を参照してください。

データベースとログファイルのサイズ

データベースとログのサイズを増やすには、以下の手順を実行します。

始める前に

データベースとログファイルのサイズを計算するには、https://software.cisco.com/download/type.html?mdfid=268439622&catid=nullからデータベース サイズ推定ツールをダウンロードして使用します。

別の選択肢としては、以下の表の値を使用してデータベースとログのサイズを変更する方法があります。

手順

ステップ 1 **SQL サーバー管理スタジオ**を起動します。

ステップ 2 [接続（Connect）] をクリックします。左側のペインで、 **データベース**を展開します。

ステップ 3 Logger データベース [<Instance>_<Side>] を右クリックして、プロパティを選択します。

ステップ 4 左側のペインで、**ファイル**を選択します。データに対して **[自動拡張（Auto Growth）]** がされており、データに対して無効化されており、ログファイルに対して有効化されていることを確認します。ログファイルは、10% 刻みで自動的に拡張されます。

ステップ 5 データベースサイズ推定ツールまたは以下の表に従って、データファイルとログファイルの初期サイズを設定します。

表 *4:* データおよびログファイルのサイズ

データベース	データ サイズ（MB）	ログ サイズ（MB）	展開タイプ
サイド A、サイド B	409600	1024	12000 エージェント
サイド A、サイド B	122900	1024	CC 展開用その他 HCS for CC

Unified CCE ルーターの構成

手順

ステップ 1 Unified CCE Web Setup を起動します。

ステップ 2 ローカルの管理者権限を持つドメイン ユーザとしてサインインします。

ステップ 3 **[インスタンス管理（Instance Management）]** > **[追加（Add）]** の順に選択します。

ステップ 4 **[インスタンスの追加（Add Instance）]** ウィンドウのドロップダウンリストで、**[ファシリティ（Facility）]** と **[インスタンス（Instance）]** を選択します。

ステップ 5 **[インスタンス番号（Instance Number）]** フィールドに **0** と入力します。[保存（Save）] をクリックします。

ステップ 6 **コンポーネント管理** > **ルータ**を選択します。

ステップ 7 **追加** をクリックして、コール ルータを設定します。

ステップ 8 **[展開（Deployment）] ウィンドウ** で、適切な **サイド**を選択します。

ステップ 9 フォールト トレランス モードとして **デュプレックス** を選択します。[次へ（Next）] をクリックします。

ステップ 10 **ルータ接続** ウィンドウで、プライベートインターフェイスとパブリック（表示）インターフェイスを設定します。[次へ（Next）] をクリックします。

ステップ 11 **周辺機器ゲートウェイを有効にする** ダイアログ ボックスで、[周辺機器ゲートウェイを有効にする] フィールドに以下を入力します。[次へ（Next）] をクリックします。

- 2000 エージェント展開の場合は通常、**2 ～ 4**。
- 4000 エージェント展開の場合は通常、**2 ～ 4**。
- 12000 エージェント展開の場合は通常、**2 ～ 16**。

ステップ 12 **ルータのオプション** ウィンドウで、以下の通り設定します。

a) **[データベース ルーティングを有効化（Enable Database Routing）]** をオンにします。
b) **Quality of Service（QoS）を有効にする**をオンにします。（サイド A にのみに該当）。
c) [次へ（Next）] をクリックします。

ステップ 13 **[ルーターのサービス品質（Router Quality of Service）]** ウィンドウで、**次へ**をクリックします。（サイド A にのみに該当）。

ステップ 14 **[サマリー（Summary）]** ウィンドウで、ルーターのサマリーが正しいことを確認して、**[完了（Finish）]** をクリックします。

（注） • すべての Unified CCE コンポーネントがインストールされるまでサービスを起動しないでください。

次のタスク

Dnwildcard を有効にするには、[Registry > HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems > ICM > <instance> >RouterA > Router > CurrentVersion > Configurations > Global] を選択し、[DNWildcardEnabled] を選択して、**1**に設定します。

基本構成のロード

基本構成パラメータをインポートするには、以下の手順を実行します。基本構成パラメータの詳細については、「2000 エージェント展開の基本構成パラメータ （550 ページ）」を参照してください。

手順

ステップ 1 タイムゾーンに基づいて、HCS-CC_11.6.1-Day1_2000.zip または ファイルをダウンロードします。このファイルをローカルに保存して、解凍します。

ステップ 2 Domain_Update_Tool.zip ファイルをダウンロードします。このファイルをローカルに保存して、解凍します。

ステップ 3 構成フォルダをサイド A にある Unified CCE Rogger のローカルドライブにコピーします。

ステップ 4 サイド A の Unified CCE Rogger で ICMDBAZ ツールを開きます。

ステップ 5 Unified CCE Rogger を選択し、<instance name>_sideA にツリーを展開します。

ステップ 6 メニューバーの [データ（Data）] を選択し、**[インポート（Import）]** をクリックします。

ステップ 7 構成フォルダを参照して特定し、**[開く（Open）]** をクリックします。

ステップ 8 **[OK]** > **[インポート（Import）]** の順に選択します。

ステップ 9 **[スタート（Start）]** をクリックし、すべてのメッセージに対して **[OK]** をクリックします。

ステップ 10 Domain_Update_Tool フォルダに移動し、[UpdateDomain.PS1.] を右クリックしたら、 PowerShell で実行します。次のように入力します。

a) サーバー名として、サイド A の Unified CCE Rogger のコンピュータ名を入力します。
b) [データベース名（Database name）] に、<instance_sideA (Logger database)> と入力します。
c) ドメイン名として、カスタマーのドメイン名を入力します。

ステップ 11 ICMDBA ツールに戻ります。同期するサイドの Logger <instance name> を選択します。

ステップ 12 メニューバーの **[データ（Data）]** をクリックし、**[同期（Synchronize）]** を選択して、以下の手順を実行します。

a) **[同期（Synchronize）]** ウィンドウの **[ソール（Source）]** ペインで **[追加（Add）]** をクリックします。
b) **[サーバー名（Server Name）]** フィールドに送信元の Unified CCE Rogger のホスト名を入力し、**[OK]** をクリックします。
c) **[接続先（Destination）]** ペインで **[追加（Add）]** をクリックします。
d) **[サーバー名（Server Name）]** フィールドに接続先の Unified CCE Rogger のホスト名を入力し、**[OK]** をクリックします。
e) **[同期（Synchronize）]** をクリックします。

ステップ 13 **[スタート（Start）]** をクリックし、すべてのメッセージに対して **[OK]** をクリックします。

Unified CCE AW-HDS-DDS の構成

ここでは、サイド A およびサイド B の Unified CCE AW-HDS-DDS に対して実行する構成手順について説明します。

表 *5:* サイド *A* およびサイド *B* の *Unified CCE AW-HDS-DDS* の構成

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ネットワーク カードの検証 （61 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	
4	CCE コンポーネント用 SQL Server の設定 （36 ページ）	
5	セカンダリドライブの構成 （36 ページ）	
6	AW-HDS-DDS （42 ページ）	
7		
8	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
9	Cisco SNMP の設定 （56 ページ）	
10	HCS for CC 展開タイプの設定 （46 ページ）	

AW-HDS-DDS

インスタンスの作成

手順

ステップ 1 デスクトップで、Unified CCE Web 設定を起動し、ドメイン管理者のログイン情報を使用してログインし、インストールを完了します。

ステップ 2 **[インスタンス管理（Instance Management）]** > **[追加（Add）]** の順に選択します。

ステップ 3 [インスタンスの追加（Add Instance）] ウィンドウのドロップダウンリストで、**[ファシリティ（Facility）]** と **[インスタンス（Instance）]** を選択します。

ステップ 4 [インスタンス番号（Instance Number）] フィールドで、**0** と入力します。[保存（Save）] をクリックします。

HDS データベースの作成

手順

ステップ 1 HDS データベースを以下のように構成します。

a) **[スタート（Start）] > [プログラム（Programs）] > [Cisco Unified CCE ツール（Cisco Unified CCE Tools）] > [ICMdba]** の順に選択します。

b) **[サーバー（Server）] > [インスタンス（Instance）]** の順に選択します。

c) インスタンス名を右クリックし、**[作成（Create）]** を選択します。

ステップ 2 [コンポーネントの選択（Select Component）] ダイアログボックスのドロップダウンリストで、**[管理およびデータサーバー（Administration & Data Server）]** を選択します。[OK] をクリックします。

ステップ 3 「*SQL* サーバーが適切に構成されていません。今すぐ、構成しますか？」というプロンプトが表示されます。**[はい（Yes）]** をクリックします。

ステップ 4 構成ページの **[SQL サーバー構成（SQL Server Configurations）]** ペインで、**[メモリー（MB）（Memory (MB)）]** と **[回復間隔（Recovery Interval）]** をオンにします。[OK] をクリックします。

ステップ 5 サーバーの停止ページで、**[Yes（はい）]** をクリックし、サービスを停止します。

ステップ 6 **[AW タイプの選択（Select AW Type）]** ダイアログボックスのドロップダウンリストで、**[エンタープライズ（Enterprise）]** を選択します。[OK] をクリックします。

ステップ 7 **[データベースの作成（Create Database）]** ダイアログボックスで、以下のように構成します。

a) [DB タイプ（DB Type）] フィールドのドロップダウンで **[HDS]** を選択します。

b) [ストレージ（Storage）] ペインで、**[追加（Add）]** をクリックします。

ステップ 8 [デバイスの追加（Add Device）] ダイアログボックスで、次のように設定します。

a) **データ** を選択します。

b) セカンダリドライブを選択します（通常は **E** ドライブです）。

c) [サイズ] フィールドでデフォルトを受け入れます。

d) [OK] をクリックします。

ステップ 9 [データベースの作成（Create Database）] ダイアログボックスの [ストレージ（Storage）] で **[追加（Add）]** をクリックします。

ステップ 10 [デバイスの追加（Add Device）] ダイアログボックスで、次のように設定します。

a) **ログ** を選択します。

b) **C** ドライブを選択します。

c) [サイズ] フィールドでデフォルトを受け入れます。

d) [OK] をクリックします。

ステップ 11 [データベースの作成（Create Database）] ダイアログボックスで、以下のように構成します。

a) [作成（Create）] をクリックします。

b) [スタート（Start）] をクリックします。

c) [OK] をクリックします。

d) [閉じる（Close）] をクリックします。

AW-HDS-DDS の構成

Cisco Unified CCE 管理サーバー、リアルタイムデータサーバー、履歴データサーバーおよび詳細なデータサーバー（AW-HDS-DDS）をインストールするには、以下の手順を実行します。

始める前に

サービス アカウントのドメイン ユーザがすでに存在していない場合は、ドメイン ユーザを作成します。ドメインユーザの作成の詳細については、*Active Directory* でのユーザの作成を参照してください。

手順

ステップ 1 **コンポーネント管理 > 管理サーバとデータ サーバ**を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [展開] ウィンドウで、現在のインスタンスを選択します。

ステップ 4 管理サーバーとデータサーバの追加ウィンドウで、以下の通り設定します。

a) **エンタープライズ**をクリックします。
b) 展開サイズは、**小規模から中規模** をクリックします。
c) [次へ（Next）] をクリックします。

ステップ 5 [小規模から中規模の導入] ウィンドウのサーバの役割については、以下の通り設定します。

a) **管理サーバ リアルタイム データ サーバ**、**履歴データ サーバ**、および **詳細データ サーバ**（**AW-HDS-DDS**）のオプションを選択します。
b) [次へ（Next）] をクリックします。

ステップ 6 [管理サーバとデータ サーバの接続] ウィンドウで以下の通り設定します。

a) **管理サーバとデータ サーバ**を選択します。
b) [*セカンダリ管理サーバとデータ サーバ] フィールドに、該当サーバのホスト名を入力します。
c) プライマリおよびセカンダリ ペア（サイト）名 フィールドで、サイト名を入力します。

（注） サイト名が、**PG Explorer > エージェントの周辺機器 > エージェントの配置**で定義されているサイト名と一致していることを確認してください。

d) [次へ（Next）] をクリックします。

ステップ 7 [データベースとオプション] ページで、以下の通り設定します。

a) [データベースを作成するドライブ] フィールドで **E** を選択します。
b) **Configure Management Service（CMS）ノード**をオンにします。
c) **Internet Script Editor（ISE）サーバ**をオンにします。
d) **次へ**をクリックします。

ステップ 8 [セントラル コントローラの接続（Central Controller Connectivity）] ウィンドウで、以下の通り構成します。

a) ルータのサイド A の場合、ルータ A が存在するホスト名または IP アドレス マシンを入力します。
b) ルータのサイド B の場合、ルータ B が存在するホスト名または IP アドレス マシンを入力します。
c) Logger サイド A の場合は、Logger A が存在するホスト名または IP アドレス マシンを入力します。
d) Logger サイド B の場合は、Logger B が存在するホスト名または IP アドレス マシンを入力します。
e) **セントラル コントローラのドメイン名**を入力します。
f) **セントラル コントローラの優先サイド A**をクリックします。
g) [次へ（Next）] をクリックします。

データベースとログファイルのサイズ

データベースとログのサイズを増やすには、以下の手順を実行します。

始める前に

データベース サイズ推定ツール を使用して、データベースとログファイルのサイズを計算します。

別の選択肢としては、表 6 : データおよびログファイルのサイズ （46 ページ） の値を使用してデータベースとログのサイズを変更する方法があります。

手順

ステップ 1 **Microsoft SQL Server Management Studio** を開きます。
ステップ 2 Object Explore でデータベースを展開します。
ステップ 3 **HDS データベース**を選択します。[データベース]を右クリックして、**プロパティ** を選択します。
ステップ 4 **ファイル** をクリックして、データベース サイズおよびログ サイズを増やします。
ステップ 5 データに対して **[自動拡張（Auto Growth）]** が無効化されており、ログファイルに対して有効化されていることを確認します。ログファイルは、10% 刻みで自動的に拡張されます。
ステップ 6 データベースサイズ推定ツールまたは以下の表に従って、データファイルとログファイルの初期サイズを設定します。

表 *6:* データおよびログファイルのサイズ

データベース	データ サイズ（MB）	ログ サイズ
<instance>_hds	409600	1024

HCS for CC 展開タイプの設定

始める前に

- **CCE Web Administration** にログインするドメインユーザーが、すべての Unified CCEAW DB（リアルタイムディストリビュータ）マシンの `UcceConfig local` グループの一部であることを確認します。

手順

ステップ 1 **CCE Web Administration** を起動します。

ステップ 2 ユーザーのログイン情報でログインします。

ステップ 3 CC 展開タイプの HCS for CC を設定

a) **[システム（System）]** タブで **[展開（Deployment）]** をクリックします。

b) ドロップダウンリストで [展開タイプ（Deployment Type）] を選択します。

（注） Small Contact Center 用エージェント展開の場合は、**CC 4000エージェント用 HCS** として [展開タイプ（Deployment Type）] を選択します。

c) **[保存（Save）]** をクリック後、警告メッセージを確認して **[はい（Yes）]** をクリックします。

ステップ 4 展開タイプを表示します。

a) **[ホーム（Home）]** タブをクリックして、展開タイプを表示します。

ステップ 5 システム検証ルールの表示

a) **[システム（System）]** タブで **[情報（Information）]** をクリックします。

b) **[システム検証（System Validation）]** をクリックします。

ステップ 6 システム設定の制限の表示

a) **[システム（System）]** タブで **[情報（Information）]** をクリックします。

b) **[キャパシティ情報（Capacity Info）]** をクリックします。

Unified CCE PG の構成

次の表では、サイド A とサイド B の両方で Unified CCE PG を構成するために必要なタスクに関して説明します。

表 *7*:サイド *A* とサイド *B* の *Unified CCE Unified PG* の構成

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ネットワーク カードの検証 （61 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	
4	Cisco Unified Communications Manager 周辺機器ゲートウェイの構成 （47 ページ）	
5	VRU 周辺機器ゲートウェイの構成 （51 ページ）	
6	MR 周辺機器ゲートウェイの構成 （52 ページ）	
7	CTI サーバーの構成 （54 ページ）	
8	JTAPI のインストール （55 ページ）	
9	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
10	Cisco SNMP の設定 （56 ページ）	
11	Unified CCE サービスの起動 （60 ページ）	

Cisco Unified Communications Manager 周辺機器ゲートウェイの構成

以下のタスクを完了し、サイド A の PG サーバーの CUCM 周辺機器ゲートウェイを構成したら、サイド B にも同じ手順を繰り返します。

- Cisco Unified Communications Manager PG の構成 （48 ページ）
- PG の追加準備 （48 ページ）
- Cisco Unified Communications Manager PG の追加 （48 ページ）
- Cisco Unified Communications Manager PIM の追加 （49 ページ）
- PIM の作成後 （50 ページ）

Cisco Unified Communications Manager PG の構成

始める前に

ドメイン管理者または次のいずれかのグループに属している場合のみ Windows マシンにログイン後、**構成マネージャ**を起動できます。

- `UcceConfig Local` グループ
- `Local administrator` グループ

手順

ステップ 1 **[構成マネージャ（Configuration Manager）] > [PG Explorer]** の順に選択します。

ステップ 2 **[CUCMPG1ルーティングクライアントのエージェントレポーティングを有効にする（Enable Agent Reporting for CUCMPG1 Routing Client）]** オプションを選択します。

ステップ 3 Cisco Unified WIM および EIM 機能の **Unified Communications Manager PG** に、プライマリおよびセカンダリ CTI アドレスとポート情報を入力します。

ステップ 4 **[エージェントディストリビューション（Agent Distribution）]** タブの **[管理およびデータサーバー（Administration and Data Server）]** フィールドに拠点名を入力します。

PG の追加準備

手順

ステップ 1 **[周辺機器ゲートウェイ設定（Peripheral Gateway Setup）]** を開きます。

ステップ 2 **[ICMインスタンス（ICM Instances）]** ペインで、**[追加（Add）]** をクリックします。

ステップ 3 **[インスタンスの追加（Add Instance）]** ウィンドウのドロップダウンリストで、適切な **[ファシリティ（Facility）]** と **[インスタンス名（Instance Name）]** を選択します。

ステップ 4 **[インスタンス番号（Instance Number）]** フィールドに `0` と入力します。

ステップ 5 [保存（Save）] をクリックします。

Cisco Unified Communications Manager PG の追加

手順

ステップ 1 **[周辺機器ゲートウェイ設定（Peripheral Gateway Setup）]** を開きます。

ステップ 2 **[インスタンスコンポーネント（Instance Components）]** ペインで、**[追加（Add）]** をクリックします。

ステップ 3 **[ICM/CCE/CCHコンポーネントの選択（ICM/CCE/CCH Component Selection）]** ダイアログボックスで、**[周辺機器ゲートウェイ（Peripheral Gateway）]** を選択します。

ステップ 4 **[周辺機器ゲートウェイプロパティ（Peripheral Gateway Properties）]** ダイアログボックスで、以下の手順を実行します。

a) **[生産モード（Production mode）]** チェックボックスをオンにします。
b) **[システム起動自動開始（Auto start system startup）]** チェックボックスをオンにします。
c) **[デュプレックス周辺機器ゲートウェイ（Duplexed Peripheral Gateway）]** チェックボックスをオンにします。
d) **[PGノードプロパティID（PG Node Properties ID）]** ペインの **[ID]** ドロップダウンリストで適切な PG を選択します。
e) 適切なサイド（**サイド A** または**サイド B**）を選択します。
f) **[クライアントタイプの選択（Client Type Selection）]** ペインで、**選択したタイプ**に **CUCM** を追加します。
g) **[次へ（Next）]** をクリックします。

Cisco Unified Communications Manager PIM の追加

手順

ステップ 1 **周辺機器ゲートウェイコンポーネントのプロパティ** ウィンドウで、**追加**をクリックします。

ステップ 2 **[クライアントタイプ（Client Type）]** ドロップダウンで、**[CUCM]** を選択します。

ステップ 3 **[利用可能なPIMS（Available PIMS）]** リストで、**[PIM]** を選択したら、**[OK]** をクリックします。

ステップ 4 **[CUCM構成（CUCM Configuration）]** ダイアログボックスで、**[有効化（Enabled）]** チェックボックスをオンにします。

ステップ 5 **周辺機器名** フィールドに、周辺機器名を入力します。

ステップ 6 **周辺機器 ID** フィールドに、論理コントローラ ID を入力します。

ステップ 7 **[エージェントの内線番号の長さ（Agent Extension Length）]**フィールドに、この展開の内線番号の長さを入力します。

（注） SCC 導入モデルの場合、エージェントの内線番号の長さは 8 です。

ステップ 8 **[Cisco Unified Communications Managerパラメータ（CUCM Parameters）]** ペインで、以下のように構成します。

a) **[サービス（Service）]** フィールドで、適切な Unified Communications Manager Subscriber のホスト名を入力します。
b) **[ユーザーID（User ID）]** フィールドにユーザー ID を入力します。
c) **[ユーザーパスワード（User Password）]** フィールドに、Unified Communications Manager パスワードを入力します。
d) **[モバイルエージェントコーデック（Mobile Agent Codec）]** フィールドで、**G.711** または **G.729** を選択します。

e) [OK] をクリックします。

ステップ 9 残りの PIM を構成するには、これらの手順を繰り返します。

Unified Communication Domain Manager は、Unified Communication Manager の統合時に、デフォルトのパスワードを「pguser」に設定します。

PIM の作成後

手順

ステップ 1 **[ロジカルコントローラID（Logical Controller ID）]** フィールドに、PIM のロジカルコントローラ ID を入力します。

ステップ 2 **[CTI後処理データ遅延（CTI Wrapup Data Delay）]** フィールドに 0 と入力し、**[次へ（Next）]** をクリックします。

ステップ 3 **[デバイス管理プロトコルプロパティ（Device Management Protocol Properties）]** ウィンドウで、以下の手順を実行します。

a) 適切なサイド（**サイド A** または**サイド B**）を選択します。

b) **[サイドAプロパティ（Side A Properties）]** パネルで、**[コールバックルーター（Call Router）]** を選択します。

c) **[サイドBプロパティ（Side B Properties）]** パネルで、**[コールバックルーター（Call Router）]** を選択します。

d) **[使用可能な帯域幅（kbps）（Usable Bandwidth (kbps)）]** フィールドは、デフォルト値を保持します。

e) **[ハートビート間隔（100 ms）（Heartbeat Interval (100ms)）]** フィールドに **4** と入力し、**[次へ（Next）]** をクリックします。

ステップ 4 **[周辺機器ゲートウェイネットワークインターフェイス（Peripheral Gateway Network Interfaces）]** ウィンドウで、**[PG Private Interfaces]** および **[PG Visible (Public) Interfaces]** と入力します。

ステップ 5 サイド A のみで以下の手順を実行します。

a) **[プライベートインターフェイス（Private Interfaces）]** ペインで、**[QoS]** をクリックします。

b) **[PGプライベートリンクQoS設定（PG Private Link QoS Settings）]** ペインで、**[QoSの有効化（Enable QoS）]** チェックボックスをオンにし、**[OK]** をクリックします。

c) **[表示（パブリック）インターフェイス（Visible(Public) Interfaces）]** で、**[QoS]** をクリックします。

d) **[PGプライベートリンクQoS設定（PG Private Link QoS Settings）]** ペインで、**[QoSの有効化（Enable QoS）]** チェックボックスをオンにし、**[OK]** をクリックします。

（注） 12000 および SCC 展開で、6 つ以上のエージェント PG がある場合、QoS を無効化します。

ステップ 6 **[周辺機器ゲートウェイネットワークインターフェイス（Peripheral Gateway Network Interfaces）]** ウィンドウで、**[次へ（Next）]** をクリックします。

ステップ 7 **[設定情報の確認（Check Setup Information）]** ウィンドウで **[次へ（Next）]** をクリックします。

ステップ 8 **[設定完了（Setup Complete）]** ウィンドウで、**[完了（Finish）]** をクリックします。

（注） すべての Unified CCE コンポーネントがインストールされるまで、Unified CCE /CCNodeManager を起動しないでください。

VRU 周辺機器ゲートウェイの構成

- VRU PG の追加 （51 ページ）
- VRU PIM の追加 （52 ページ）
- PIM の作成後 （50 ページ）

VRU PG の追加

手順

ステップ 1 **[周辺機器ゲートウェイ設定（Peripheral Gateway Setup）]** を開きます。

ステップ 2 **[インスタンスコンポーネント（Instance Components）]** ペインで、**[追加（Add）]** をクリックします。

ステップ 3 **[コンポーネントの選択（Component Selection）]** ダイアログボックスで、**[周辺機器ゲートウェイ（Peripheral Gateway）]** を選択します。

ステップ 4 **[周辺機器ゲートウェイプロパティ（Peripheral Gateway Properties）]** ダイアログボックスで、以下の手順を実行します。

a) **[生産モード（Production mode）]** チェックボックスをオンにします。
b) **[システム起動自動開始（Auto start system startup）]** チェックボックスをオンにします。
c) **[デュプレックス周辺機器ゲートウェイ（Duplexed Peripheral Gateway）]** チェックボックスをオンにします。
d) **[PGノードプロパティID（PG Node Properties ID）]** ペインの **[ID]** ドロップダウンリストで、**[PG3]** を選択します。
e) 適切なサイド（**サイド A** または**サイド B**）を選択します。
f) **[クライアントタイプの選択（Client Type Selection）]** ペインで、**選択したタイプ**に **VRU** を追加します。
g) **[次へ（Next）]** をクリックします。

VRU PIM の追加

手順

ステップ 1 周辺機器ゲートウェイコンポーネントのプロパティ ウィンドウで、追加をクリックします。
ステップ 2 **[クライアントタイプ（Client Type）]** ドロップダウンで、**[VRU]** を選択します。
ステップ 3 **[利用可能なPIMS（Available PIMS）]** リストで、適切な PIM を選択したら、**[OK]** をクリックします。
ステップ 4 **[構成（Configuration）]** ダイアログ ボックスで、**有効化** チェックボックスをオンにします。
ステップ 5 **[周辺機器名（Peripheral Name）]** フィールドに、CVP サーバー名を入力します。
ステップ 6 **[周辺機器ID（Peripheral ID）]** フィールドに、CVP のロジカルコントローラ ID を入力します。
ステップ 7 **[VRUホスト名（VRU Hostname）]** フィールドに、CVP サーバーのホスト名を入力します。
ステップ 8 **[VRU接続ポート（VRU Connect port）]** フィールドに、`5000` と入力します。
ステップ 9 **[再接続間隔（秒）（Reconnect interval (sec)）]** フィールドに、`10`と入力します。
ステップ 10 **[ハートビート間隔（秒）（Heartbeat interval (sec)）]** フィールドに、`5`と入力します。
ステップ 11 **[DSCP]**ドロップダウンリストで、**CS3(24)** を選択します。
ステップ 12 [OK] をクリックします。
ステップ 13 残りの PIM を構成するには、これらの手順を繰り返します。

MR 周辺機器ゲートウェイの構成

- メディアルーティング PG の追加 （52 ページ）
- 2000 エージェント展開にマルチチャネル PIM を追加 （53 ページ）
- アウトバウンド PIM の追加 （54 ページ）
- PIM の作成後 （50 ページ）

メディアルーティング PG の追加

メディアルーティング PG を構成します。マルチチャネルとアウトバウンドは使用しません。この場合、メディアルーティング PG はアイドル状態または無効のままです。

手順

ステップ 1 **[周辺機器ゲートウェイ設定（Peripheral Gateway Setup）]** を開きます。
ステップ 2 **[インスタンスコンポーネント（Instance Components）]** ペインで、**[追加（Add）]** をクリックします。
ステップ 3 **[コンポーネントの選択（Component Selection）]** ダイアログボックスで、**[周辺機器ゲートウェイ（Peripheral Gateway）]** を選択します。

ステップ 4 **[周辺機器ゲートウェイプロパティ（Peripheral Gateway Properties）]** ダイアログボックスで、以下の手順を実行します。

a) **[生産モード（Production mode）]** チェックボックスをオンにします。
b) **[システム起動自動開始（Auto start system startup）]** チェックボックスをオンにします。
c) **[デュプレックス周辺機器ゲートウェイ（Duplexed Peripheral Gateway）]** チェックボックスをオンにします。
d) **[PGノードプロパティID（PG Node Properties ID）]** ペインの **[ID]** ドロップダウンリストで適切な PG を選択します。
e) 適切なサイド（**サイド A** または**サイド B**）を選択します。
f) **[クライアントタイプ（Client Type）]** ペインで、**選択したタイプ**に対して、**MediaRouting** を選択します。
g) **[次へ（Next）]** をクリックします。

2000 エージェント展開にマルチチャネル PIM を追加

手順

ステップ 1 **周辺機器ゲートウェイコンポーネントのプロパティ** ウィンドウで、**追加**をクリックします。

ステップ 2 **クライアント タイプ** ドロップダウンリストで、**メディア ルーティング**を選択します。

ステップ 3 **利用可能な PIMS** リストで、**MR PIM1**を選択し、**OK**をクリックします。

ステップ 4 **[構成（Configuration）]** ダイアログ ボックスで、**有効化** チェックボックスをオンにします。

ステップ 5 **周辺機器名** フィールドに、周辺機器名を入力します。

ステップ 6 **[周辺機器ID（Peripheral ID）]** フィールドで、追加する Unified CCE コンポーネントのロジカルコントローラ ID を入力します。以下は、データベースで表示される Unified CCE コンポーネントの名前です。

- ECE の名前は、*Multichannel* です。
- CCP の名前は、*Multichannel2* です。
- THIRD_PARTY_MULTICHANNEL の名前は、*MutliChannel3* です。

例：

ECE を追加する場合は、データベースで *Multichannel* という名前のコンポーネントを検索します。**[周辺機器ID（Peripheral ID）]** フィールドでコンポーネントのロジカルコントローラ ID を入力します。

ステップ 7 **[アプリケーションホスト名（1）（Application Hostname (1)）]** フィールドで、ECE サービス サーバーのホスト名または IP アドレスを入力します。

ステップ 8 **アプリケーション接続ポート (1)** フィールドに、ポート番号を入力します。

（注） アプリケーションとの通信に PIM が使用する ECE サービス サーバ上のポート番号を使用します。デフォルト ポートは 38001 です。

ステップ 9　**アプリケーション ホスト名 (2)** フィールドは空白のままにします。
ステップ 10　**アプリケーション 接続ポート (2)** フィールドは空白のままにします。
ステップ 11　**[ハートビート間隔（秒）（Heartbeat interval (sec)）]** フィールドに、**5**と入力します。
ステップ 12　**[再接続間隔（秒）（Reconnect interval (sec)）]** フィールドに、**10**と入力します。
ステップ 13　[OK] をクリックします。

アウトバウンド PIM の追加

手順

ステップ 1　**周辺機器ゲートウェイコンポーネントのプロパティ** ウィンドウで、**追加**をクリックします。
ステップ 2　**クライアント タイプ** ドロップダウンリストで、**メディア ルーティング**を選択します。
ステップ 3　**利用可能な PIMS** リストで、**MR PIM2**を選択し、**OK**をクリックします。
ステップ 4　**[構成（Configuration）]** ダイアログ ボックスで、**有効化** チェックボックスをオンにします。
ステップ 5　**周辺機器名** フィールドに、周辺機器名を入力します。
ステップ 6　**周辺機器 ID** フィールドに、論理コントローラ ID を入力します。
ステップ 7　**[アプリケーションホスト名（1）（Application Hostname(1)）]** フィールドに、サイド A のエージェント PG マシンの IP アドレスを入力します。
ステップ 8　**[アプリケーション接続ポート（1）（Application Connection port (1)）]** はデフォルト値のままにしておきます。
ステップ 9　**[アプリケーションホスト名（2）（Application Hostname(2)）]** フィールドに、サイド B のエージェント PG マシンの IP アドレスを入力します。
ステップ 10　**[アプリケーション接続ポート（2）（Application Connection port (2)）]** はデフォルト値のままにしておきます。
ステップ 11　**[ハートビート間隔（秒）（Heartbeat interval (sec)）]** フィールドに、**5**と入力します。
ステップ 12　**[再接続間隔（秒）（Reconnect interval (sec)）]** フィールドに、**10**と入力します。
ステップ 13　[OK] をクリックします。

CTI サーバーの構成

サイド A とサイド B に対して CTI サーバーを構成するには、以下の手順を実行します。

手順

ステップ 1　**[スタート（Start）] > [すべてのプログラム（All programs）] > [Cisco Unified CCE ツール（Cisco Unified CCE Tools）] > [周辺機器ゲートウェイの設定（Peripheral Gateway Setup）]** の順に選択します。

ステップ 2 [コンポーネントの設定（Components Setup）] ダイアログボックスの [インスタンスコンポーネント（Instance Components）] ペインで、**[追加（Add）]** をクリックします。

ステップ 3 [コンポーネントの選択（Component Selection）] ダイアログボックスで **[CTIサーバー（CTI Server）]** をクリックします。

a) **[生産モード（Production Mode）]** をオンにします。
b) **[システム起動自動開始（Auto start system startup）]** をオンにします。
c) **[デュプレックスCTIサーバー（Duplexed CTI Server）]** をオンにします。
d) エージェント PG1 には **CG1** を選択し、エージェント PG2 には **CG2** を選択します。
e) エージェント PG に対応するシステム ID 番号を入力します。
例：エージェント PG1 には 1 を、エージェント PG2 には 2 を入力します。
f) 適切なサイド（サイド A またはサイド B）をクリックします。
g) [次へ（Next）] をクリックします。

ステップ 4 [サーバーコンポーネントプロパティ（Server Component Properties）] ダイアログボックスで以下のように構成します。

a) サイド A には、[クライアント接続ポート番号（Client Connection Port Number）] フィールドに **42027** と入力します。
b) サイド B には、[クライアント接続ポート番号（Client Connection Port Number）] フィールドに **43027** と入力します。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [Network Interface Properties] ダイアログボックスで、プライベート インターフェイスを入力します。

ステップ 7 パブリック（表示）インターフェイスと CG 表示インターフェイスを入力し、**[次へ（Next）]** をクリックします。

ステップ 8 設定情報の確認ページで、すべての設定を確認し、**[次へ（Next）]** をクリックします。

ステップ 9 [設定完了（Setup Complete）] ダイアログボックスで、**[完了（Finish）]** をクリックします。

ステップ 10 **[設定を終了（Exit Setup）]** をクリックします。

（注） すべての Unified CCE コンポーネントがインストールされるまで Unified CCE/CC Node Manager を起動しないでください。

JTAPI のインストール

（注） この手順は、Unified Communications Manager PIM を備えた PG を使用する Unified Contact Center Enterprise マシンに必要です。 ただし、この作業は Unified Communications Manager の構成 （87 ページ） 後まで延期する必要があります。ただし、Unified Communications Manager を構成するまで、このタスクを延期する必要があります。

サイド A およびサイド B で Unified Communications Manager PIM を備えた PG を使用する Unified Contact Center Enterprise マシンに JTAPI をインストールするには、以下の手順を実行します。

手順

ステップ 1 ブラウザ（https://{callmanager-hostname}）で、Unified Communications Manager を起動し、ログインします。

ステップ 2 **[アプリケーション（Application）]**>**[プラグイン（Plugins）]** の順に選択します。[検索（Find）] をクリックします。

ステップ 3 ダウンロードしたファイルをインストールし、すべてのデフォルト設定を受け入れます。

ステップ 4 プロンプトで、Unified Communications Manager TFTP サーバーの IP アドレスを入力し、**[次へ（Next）]** をクリックします。

ステップ 5 **[完了（Finish）]** をクリックします。

Cisco Diagnostic Framework Portico の検証

これは、Unified CCE マシンに対して実行します。

手順

ステップ 1 コマンドプロンプトを開き、**cd C:** と入力します。

ステップ 2 **cd icm\serviceability\diagnostics\bin** と入力し、**Enter** キーを押します。

ステップ 3 **DiagFwCertMgr /task:CreateAndBindCert /port:7890** と入力し、**Enter** キーを押します。

ステップ 4 **[スタート（Start）]**>**[実行（Run）]** の順に選択し、**services.msc** と入力して、サービスツールを開きます。Cisco Diagnostic Framework サービスが実行されていることを確認します。実行されていない場合は起動します。

ステップ 5 **[スタート（Start）]** > **[プログラム（Programs）]** > **[Cisco Unified CCEツール（Cisco Unified CCE Tools）]** > **[診断フレームワークPortico（Diagnostic Framework Portico）]** の順に選択し、診断フレームワーク Portico を開きます。ドメインユーザのログイン情報を使用して Diagnostic Framework Portico にログインできることを確認します。

Cisco SNMP の設定

Cisco SNMP を設定するには、以下の手順を実行します。

- Cisco SNMP エージェント管理スナップインの追加 （57 ページ）
- Cisco SNMP エージェント管理スナップイン ビューの保存 （57 ページ）
- SNMP V1 and V2c のコミュニティ名の設定 （58 ページ）
- SNMP V3 用の SNMP ユーザー名の設定 （58 ページ）

• SNMP トラップの接続先設定 （59 ページ）
• SNMP Syslog の接続先設定 （60 ページ）

Cisco SNMP エージェント管理スナップインの追加

Cisco SNMP エージェント管理の設定は、Windows 管理コンソールのスナップインを使用して設定することができます。

スナップインを追加して、Cisco SNMP 管理の設定を変更するには、以下の手順を実行します。

手順

ステップ 1 [スタート] メニューで、**mmc.exe/32**と入力します。
ステップ 2 コンソールから、 **ファイル** > **スナップインの追加または削除**を選択します。
ステップ 3 [スナップインの追加または削除] ダイアログ ボックスで、利用可能なスナップイン一覧から **Cisco SNMP エージェント管理** を選択します。[追加（Add）] をクリックします。
ステップ 4 選択されたスナップインのペインで、 **Cisco SNMP エージェント管理**をダブルクリックします。
ステップ 5 Cisco SNMP エージェント管理拡張機能のダイアログ ボックスで、**常に使用可能なすべての拡張機能を有効にする**を選択します。[OK] をクリックします。
ステップ 6 [スナップインの追加および削除] ウィンドウで、 **OK**をクリックします。これで、Cisco SNMP Agent Management スナップインがコンソールに読み込まれました。

Cisco SNMP エージェント管理スナップイン ビューの保存

[Cisco SNMP エージェント管理] MMC スナップインをロードした後、コンソール ビューを「.MSC」のファイル拡張子が付いたファイルに保存することができます。[管理ツール] からこのファイルを直接起動することができます。

Cisco SNMP エージェント管理スナップイン ビューを保存するには、以下の手順を実行します。

手順

ステップ 1 **ファイル** > **保存**を選択します。
ステップ 2 [ファイル名] フィールドに、 **Cisco SNMP エージェント管理**と入力します。
ステップ 3 [名前を付けて保存] の [ファイルの種類] フィールドで、**Microsoft 管理コンソール ファイル（*.msc）等の管理ツールにマップするファイル名を選択します。**
ステップ 4 [保存（Save）] をクリックします。

SNMP V1 and V2c のコミュニティ名の設定

SNMP v1 あるいは v2c を使用する場合は、ネットワーク管理システム（NMS）がサーバから提供されるデータにアクセスできるように、コミュニティ名を設定する必要があります。SNMP コミュニティ名を使用して、SNMP 情報のデータ交換を認証します。NMS は、同じコミュニティ名を使用するサーバに対してのみ SNMP 情報をやり取りすることができます。

SNMP v1 および v2c のコミュニティ名を設定するには、以下の手順を実行します。

始める前に

手順 Cisco SNMP エージェント管理スナップインの追加 （57 ページ）および Cisco SNMP エージェント管理スナップイン ビューの保存 （57ページ） を使用して、Cisco SNMP が追加され、保存されたことを確認します。

手順

ステップ 1 **スタート** > **すべてのプログラム** > **管理ツール** > **Cisco SNMP エージェント管理**を選択します。

ステップ 2 **Cisco SNMP エージェント管理** を右クリックして、**管理者として実行する**を選択します。

ステップ 3 [Cisco SNMP エージェント管理] 画面に、トラップおよびシステムログに SNMP を必要とする設定の一部が表示されます。

ステップ 4 **コミュニティ名（SNMP v1 または v2c）** を右クリックして、 **プロパティ**を選択します。

ステップ 5 [コミュニティ名（SNMP v1 または v2c）のプロパティ] ダイアログ ボックスで、**新規コミュニティの追加**をクリックします。

ステップ 6 [コミュニティ名] フィールドに、コミュニティ名を入力します。

ステップ 7 [ホストのアドレス一覧] フィールドに、ホストの IP アドレスを入力します。

ステップ 8 **適用する** をクリックして、**OK**をクリックします。

SNMP V3 用の SNMP ユーザー名の設定

SNMP v3 を使用する場合は、NMS がサーバから提供されるデータにアクセスできるように、ユーザ名を設定する必要があります。

SNMP のユーザ名を設定するには、以下の手順を実行します。

始める前に

手順 Cisco SNMP エージェント管理スナップインの追加 （57 ページ）および Cisco SNMP エージェント管理スナップイン ビューの保存 （57ページ） を使用して、Cisco SNMP が追加され、保存されたことを確認します。

手順

ステップ 1 コンソール ルートで、**Cisco SNMP エージェント管理** > **ユーザ名（SNMP v3）** > **プロパティ**を選択します。

ステップ 2 [新規ユーザを追加（Add New User）] をクリックします。

ステップ 3 [ユーザ名（User Name）] フィールドに、ユーザ名を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ダイアログ ボックスの上部にある [設定済ユーザ] ペインにユーザ名が表示されます。

ステップ 6 **適用する** をクリックして、**OK**をクリックします。

SNMP トラップの接続先設定

SNMP v1、SNMP v2c、および SNMP v3 の SNMP トラップの接続先を設定することができます。トラップは、SNMP エージェントが特定のイベントを NMS に伝達するために使用する通知です。

トラップの接続先を設定するには、以下の手順を実行します。

始める前に

手順 Cisco SNMP エージェント管理スナップインの追加 （57 ページ）および Cisco SNMP エージェント管理スナップイン ビューの保存 （57 ページ） を使用して、Cisco SNMP が追加され、保存されたことを確認します。

手順

ステップ 1 コンソール ルートで、**Cisco SNMP エージェント管理** > **トラップの接続先** > **プロパティ**を選択します。

ステップ 2 **トラップ エンティティの追加**をクリックします。

ステップ 3 NMS が使用する SNMP のバージョンをクリックします。

ステップ 4 [トラップ エンティティ名] フィールドに、トラップ エンティティの名前を入力します。

ステップ 5 このトラップと関連付けるユーザ名またはコミュニティ名を選択します。この一覧には、設定された既存のユーザまたはコミュニティ名が自動的に提示されます。

ステップ 6 IP アドレス入力フィールドに、1 つあるいは複数の IP アドレスを入力します。**挿入** をクリックして、トラップの接続先を定義します。

ステップ 7 **適用する** をクリックして、**保存** をクリックして、新しいトラップの接続先を保存します。

ダイアログ ボックス上部の [トラップ エンティティ] セクションに、トラップ エンティティ名が表示されます。

ステップ 8 [OK] をクリックします。

SNMP Syslog の接続先設定

Cisco SNMP エージェント管理スナップインで、SNMP の Syslog の接続先を設定することができます。

Syslog の接続先を設定するには、以下の手順を実行します。

手順

ステップ 1 コンソール ルートで、**Cisco SNMP エージェント管理** > **Syslog の接続先** > **プロパティ**を選択します。
ステップ 2 リスト ボックスでインスタンスを選択します。
ステップ 3 **フィードを有効にする**をオンにします。
ステップ 4 [コレクタ アドレス] フィールドにコレクタの IP アドレスを入力します。
ステップ 5 **[保存（Save）]** をクリックします。
ステップ 6 **OK** をクリックして、Logger を再起動します。

Unified CCE サービスの起動

Unified CCE コンポーネントは、ホストコンピュータの Windows サービスとして実行されます。これらサービスは、デスクトップの **Unified CCE サービスコントロールツール**で起動、停止、サイクルできます。

（注） この手順は、Unified CCE サービスを有効化するために必要です。ただし、このタスクは、導入モデルに含まれるすべての仮想マシンに Unified CCE コンポーネントをインストールするまで、保留にしなければなりません。

手順

ステップ 1 各 Unified CCE サーバーマシンで、**Unified CCE サービスコントロール**を開きます。
ステップ 2 **Unified CCE コンポーネント**サービスを起動します。

Unified CVP の構成

このセクションでは、Unified CVP の構成手順に関して説明します。

順序	タスク	完了したか
1	Unified CVP サーバーの構成 （61 ページ）	

順序	タスク	完了したか
2	Unified CVP レポーティングサーバーの構成（64 ページ）	
3	Cisco Unified CVP オペレーションコンソールの構成 （70 ページ）	

Unified CVP サーバーの構成

このセクションでは、Unified CVP サーバーの構成方法を説明します。

順序	タスク	完了したか
1	ネットワーク カードの検証 （61 ページ）	
2	Unified CVP メディアサーバー IISの設定 （61 ページ）	
3	FTP サーバーの設定 （63 ページ）	

ネットワーク カードの検証

手順

ステップ 1 **[スタート（Start）]** を選択したら、**[ネットワーク（Network）]** を右クリックします。

ステップ 2 [プロパティ（Properties）] を選択します。**[アダプタ設定の変更（Change Adapter Settings）]** を選択します。

ステップ 3 **[ローカルエリア接続（Local Area Connection）]** を右クリックし、**[プロパティ（Properties）]** を選択します。

ステップ 4 **[インターネットプロトコルバージョン6（TCP/IPV6）（Internet Protocol Version 6 (TCP/IPV6)）]** をオフにします。

ステップ 5 **[インターネットプロトコルバージョン4（Internet Protocol Version 4 ）]** チェックボックスをオンにし、**[プロパティ（Properties）]** を選択します。

ステップ 6 表示 IP アドレス、サブネットマスク、デフォルトゲートウェイ、優先 DNS サーバー、および代替 DNS サーバーのデータを確認します。

ステップ 7 [OK] をクリックします。

Unified CVP メディアサーバー IISの設定

手順

ステップ 1 **スタート** > **管理ツール**に移動します。

ステップ 2 **サーバ マネージャ** オプションを選択して、**管理** > **役割と機能の追加**に移動します。

ステップ 3 **インストール タイプ** タブに移動して、**役割ベースまたは機能ベースのインストール** オプション タブで、**[次へ（Next）]** を選択します。

ステップ 4 **サーバの選択**ウィンドウで、リストからサーバを選択して、**[次へ（Next）]** をクリックします。

ステップ 5 **[ウェブ サーバ (iis)] チェックボックスをオンにして iis を有効にし、[次へ（Next）] をクリックします。**

ステップ 6 ウェブアダプタをインストールするために追加の機能は必要ありません。**[次へ（Next）]** をクリックします。
ウェブ サーバの役割（IIS） タブを表示します。

ステップ 7 [次へ（Next）] をクリックします。
役割サービスの選択 タブを表示します。

ステップ 8 以下の一覧の ウェブ サーバ コンポーネントが有効になっていることを確認します。

- Web サーバー
  - HTTP 共通機能
    - デフォルトのドキュメント
    - 静的コンテンツ
  - セキュリティ
    - フィルタ処理機能の要求
    - 基本認証
    - Windows Authentication
  - アプリケーション開発
    - .NET 機能拡張 4.5
    - ASP.NET 4.5
    - ISAPI Extensions
    - ISAPI フィルタ
- 管理ツール
  - IIS 管理コンソール
  - IIS 管理互換性
    - IIS6 メタベース互換性
  - IIS 管理スクリプトとツール
  - 管理サービス

ステップ 9 [次へ（Next）] をクリックします。
ステップ 10 設定値が正しいことを確認して、**[インストール（Install ）]**をクリックします。
ステップ 11 インストール後に **[閉じる（Close）]**をクリックします。

FTP サーバーの設定

- FTP サーバーのインストール （63 ページ）
- FTP サーバーの有効化 （63 ページ）
- 基本的な FTP プロキシ設定 （64 ページ）

FTP サーバーのインストール

手順

ステップ 1 **スタート** > **管理ツール**を選択します。
ステップ 2 **サーバ マネージャ**を選択して、**[管理（Manage）]** をクリックします。
ステップ 3 **[ロールおよび機能の追加（Add Roles and Features）]** を選択して、**[次へ（Next）]**をクリックします。
ステップ 4 **インストールタイプの設定**タブで、**ロール ベースまたは機能ベースのインストール**を選択し、**[次へ（Next）]** をクリックします。
ステップ 5 リストから必要なサーバを選択して、**[次へ（Next）]** をクリックします。
ステップ 6 ウェブアダプタをインストールするために追加の機能は必要ありません。**[次へ（Next）]**をクリックします。
ステップ 7 **サーバーの役割**ページで、**[Webサーバー（IIS）（Web Server (IIS)）]** を展開します。
ステップ 8 **[FTPサーバー（FTP Server）]** をオンにし、**[次へ（Next）]** をクリックします。
ステップ 9 **機能**ページで、**[次へ（Next）]** をクリックします。
ステップ 10 **構成**ページで、**[インストール（Install）]** をクリックします。

FTP サーバーの有効化

手順

ステップ 1 **スタート** > **管理ツール**に移動します。
ステップ 2 **サーバ マネージャ** を選択して、**IIS**をクリックします。
ステップ 3 FTPサーバを有効にするサーバを右クリックして、サブメニューから **インターネット インフォメーション サービス （IIS）マネージャ** オプションを選択します。
ステップ 4 **接続** パネルに移動します。

a) FTP サイトを追加する CVP サーバを展開します。
b) **サイト**を右クリックして、**FTP サイトの追加**オプションをサブメニューから選択します。

ステップ 5 **FTP サイト名**を入力します。
ステップ 6 **物理パス** フィールドで、`C:\Inetpub\wwwroot` を参照して、**次へ**をクリックします。
ステップ 7 ドロップダウンリストで CVP の **IP アドレス** を選択します。
ステップ 8 **ポート**番号を入力します。
ステップ 9 **SSL なし** チェックボックスをオンにして、**次へ**をクリックします。
ステップ 10 **認証** パネルで **匿名** および **基本** チェックボックスをオンにします。
ステップ 11 **許可する** ドロップダウンリストで **すべてのユーザ** を選択します。
ステップ 12 **読み取り** および **書き込み** チェックボックスをオンにして、**完了**をクリックします。

基本的な *FTP* プロキシ設定

手順

ステップ 1 **接続** タブで作成した**FTP サーバ** に移動します。
ステップ 2 **アクション** タブに移動して、**基本設定**をクリックします。
ステップ 3 **接続**をクリックします。
ステップ 4 **アプリケーションユーザ（パススルー認証）**オプションを選択して、**OK**をクリックします。
ステップ 5 **サイトの編集** ウィンドウで **OK** をクリックします。

Unified CVP レポーティングサーバーの構成

（注）
- 2000 エージェント展開用 Unified CVP レポーティングサーバーはひとつです。
- 別のエージェント展開用 Unified CVP レポーティングサーバーは 2 台あります。

次の表に、Unified CVP レポーティングサーバーの構成方法を説明します。

順序	タスク	完了したか
1	ネットワーク カードの検証 （61 ページ）	?
2	セカンダリドライブの構成 （36 ページ）	?
3	Unified CVP レポーティングユーザー （65 ページ）	?
4	Cisco Unified CVP レポートデータのデータソースの作成 （67 ページ）	?

Unified CVP レポーティングユーザー

レポートユーザーの作成

Unified CVP レポーティングユーザーが Unified Intelligence Center にサインインできるのは、そのユーザーが管理コンソールにスーパーユーザとして存在するか、またはそのユーザーのドメインの Unified Intelligence Center 管理コンソールに Active Directory（AD）が設定されている場合のみです。

- 後から追加したスーパーユーザは、IP Multimedia Subsystem（IMS）ユーザであると見なされます。
- Active Directory で認証されたユーザーは、Lightweight Directory Access Protocol（LDAP）ユーザーであると見なされます。

IMS ユーザと LDAP ユーザの両方が、Unified Intelligence Center レポーティングにログインできます。ただし、Unified Intelligence Center レポーティング セキュリティ管理者が追加のロールを付与し、アクティブユーザであることを示すフラグを設定するまで、ログインユーザロールに制限されます。

Unified Intelligence Center ユーザーリストページでユーザーを作成できても、このユーザーリスト上にエントリがあるのみでは、そのユーザーは Unified Intelligence Center にサインインできません。このユーザ リスト ページでユーザを作成する 1 つの理由として、Active Directory ドメインを設定する前に、ユーザの権限を迅速に付与できることを挙げることができます。

スーパーユーザの作成

手順

ステップ 1 Cisco Unified Intelligence Center 管理コンソール（`https://<HOST ADDRESS>/oamp`）にログインします。

ステップ 2 **[管理者ユーザー管理（Admin User Management）] > [管理者ユーザー管理（Admin User Management）]** の順に選択し、ユーザーページを開きます。

ステップ 3 **[新規追加（Add New）]** をクリックし、新規ユーザーを追加、構成するか既存のユーザー名をクリックし、そのユーザーの構成を編集します。

このページには、[一般（General）]、[ログイン情報（Credentials）]、および[ポリシー（Policy）] の 3 つのタブがあります。これらのタブの入力方法については、「https://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html」の または、管理コンソールオンラインヘルプを参照してください。

ステップ 4 [保存（Save）] をクリックします。

LDAP ユーザー用 Active Directory サーバーの設定

Cisco Unified Intelligence Center 管理コンソールの [Active Directory] タブを構成すると、Unified CVP レポーティングユーザーは、ドメインで定義したユーザー名とパスワードを使用して Unified Intelligence Center レポーティングアプリケーションにログインできるようになります。

手順

ステップ 1 Cisco Unified Intelligence Center 管理アプリケーションで、**[クラスタ構成（Cluster Configuration）] > [レポーティング構成（Reporting Configuration）]** の順に選択し、[Active Directory] タブを選択します。

ステップ 2 このページにあるすべてのフィールドを入力します。ガイダンスについては、オンラインヘルプを参照してください。

ステップ 3 [テスト接続（Test Connection）] をクリックします。

ステップ 4 接続の確認ができたら、**[保存（Save）]** をクリックします。

Cisco Unified Intelligence Center レポーティング インターフェイスにサインイン

Unified Intelligence Center レポーティング インターフェイスにサインインできるユーザ：

- 初期状態では、デフォルトのスーパーユーザであるシステム アプリケーション ユーザ。
- その後、管理コンソールに IMS スーパーユーザーまたは LDAP ユーザーとして作成された Unified CVP ユーザー。

以下の手順を実行して、Unified Intelligence Center レポーティングインターフェイスにサインインしてください。

手順

ステップ 1 Cisco Unified Intelligence Center 管理コンソールにサインインします（*https://<HOST ADDRESS>/oamp*）。

ステップ 2 **[コントロールセンター（Control Center）] > [デバイスコントロール（Device Control）]** の順に選択します。

ステップ 3 アクセスするメンバーノードの名前をクリックします。これにより、そのメンバの [Cisco Unified Intelligence Center] ログイン ページが開きます。

ステップ 4 ユーザー ID とパスワードを入力します。[概要（Overview）] ページが表示されます。

ステップ 5

レポートテンプレートの作成

順序	タスク	完了したか
1	Cisco Unified CVP レポートデータのデータ ソースの作成 （67 ページ）	
2	Cisco Unified CVP レポートテンプレートの取得（68 ページ）	

順序	タスク	完了したか
3	Unified CVP レポートテンプレートのインポートおよびデータ ソースの設定 （69 ページ）	

Cisco Unified CVP レポートデータのデータ ソースの作成

手順

ステップ 1 `https://<hostname of CUIC Publisher>:8444/cuic` で Unified Intelligence Center にログインします。

ステップ 2 ナビゲーションウィンドウで、**[構成（Configure）] > [データ ソース（Data Sources）]** の順に選択します。
Unified Intelligence Center レガシーインターフェイスにリダイレクトします。

ステップ 3 [データ ソース（Data Sources）] タブで、[作成（Create）] をクリックします。

ステップ 4 このページの各フィールドに以下の通り値を指定します。

フィールド	値
名前	このデータ ソースの名前を入力します。 レポートデザイナおよびレポート定義作成者は、[データ ソース（Data Sources）]ページにアクセスできませんが、カスタム レポートを作成するときにデータ ソースのリストを参照できます。それらのユーザにわかりやすいように、新しいデータ ソースにわかりやすい名前を付けます。
説明	このデータ ソースの説明を入力します。
タイプ	[Informix] を選択します。 （注） 編集モードでは、[タイプ（type）]はディセーブルになります。
データベースホスト	Unified CVP レポーティングサーバーの IP アドレスまたはドメインネームシステム（DNS）を入力します。
ポート	ポート番号を入力します。通常、ポートは 1526 です。
データベース名	データベース名は、`cvp_data` または `callback` です。
インスタンス	目的のデータベースのインスタンス名を指定します。デフォルトは、`cvp` です。

フィールド	値
タイムゾーン	データベースに格納されているデータに正しいタイム ゾーンを選択します。[標準時間（Standard Time）] から [サマータイム（Daylight Savings Time）] への変更がある場所では、このタイム ゾーンが自動的に更新されます。
データベースユーザー ID	Operations Console に設定されているレポーティング ユーザのユーザ ID を入力して、Unified CVP レポーティング データベースにアクセスします。 （cvp_dbuser アカウントは、Unified CVP レポーティング サーバーのインストール中に自動的に作成されます）。
Password および Confirm Password	データベース ユーザのパスワードを入力し、確認します。
文字セット	[UTF-8] を選択します。
デフォルトの許可	[自分のグループ] および [すべてのユーザ] グループについて、このデータ ソースに対する権限を表示または編集します。

ステップ 5 [テスト接続（Test Connection）] をクリックします。

ステータスがオンラインでない場合、エラー メッセージを確認して原因を究明し、それに応じてデータ ソースを編集します。

ステップ 6 [保存（Save）] をクリックして、[データ ソースの追加（Add Data Source）]ウィンドウを閉じます。

（注） CVP コールバック レポートを標準データ ソース（cvp_data）にインポートする必要がある場合は、「インポートを完了できません。選択したデータ ソースのクエリ検証に失敗しました。（*Import could not be completed: Query validation failed against the selected data source.*）」というメッセージが表示され、インポートが失敗します。

この問題を修正するには、cvp_data データベースではなく、コールバック データベースを指す別個のデータ ソースを作成します。

新しいデータ ソースが、[データ ソース（Data Sources）]リストに表示されます。

Cisco Unified CVP レポートテンプレートの取得

インポート Unified CVP レポート テンプレートを取得可能なユーザー：組織内のすべてのユーザー。

Unified CVP レポーティング テンプレート XML ファイルは、Unified CVP とともにインストールされます。ファイルの保存先に移動し、ファイルを Cisco Unified Intelligence Center クライアント ワークステーションにコピーします。

インポート Unified CVP レポート テンプレートを取得するには、以下の手順を実行します。

手順

ステップ 1 Unified CVP サーバーで、Unified CVP テンプレート ファイルを検索します。これらは、%CVP_HOME%\CVP_Reporting_Templates のレポーティングサーバーにある XML ファイルです。また、\Downloads and Samples\Reporting Templates のインストールディレクトリでも見つけることができます。

ステップ 2 ファイルを選択し、Unified Intelligence Center Reporting Web アプリケーションを起動できるクライアントコンピュータにコピーします。

Unified CVP レポートテンプレートのインポートおよびデータソースの設定

手順

ステップ 1 `URL http://<HOST ADDRESS>:8444/cuic` を使用して Unified Intelligence Center Web アプリケーションを起動します。

ステップ 2 [ユーザー名（User Name）] と [パスワード（Password）] を入力します。

ステップ 3 左側のナビゲーションウィンドウで、**[レポート（Reports）]** をクリックします。

ステップ 4 **[レポート（Reports）]** ツールバーで、**[新規フォルダ（New Folder）]** をクリックします。

ステップ 5 Unified CVP レポートのコンテナとして新規フォルダに名前を付けます。[保存（Save）] をクリックします。

ステップ 6 **[レポート（Reports）]** ツールバーで **[新規（New）] > [インポート（Import）]** の順に選択します。Unified Intelligence Center レガシーインターフェイスの概要ページにリダイレクトされます。

ステップ 7 **[レポート（Reports）]** ドロワーをクリックし、Unified CVP レポートをインポートするために作成したフォルダを選択します。

ステップ 8 ツールバーで、**[レポートをインポート（Import Report）]** をクリックします。

ステップ 9 手順 5 で作成した Unified CVP フォルダに**保存**します。

ステップ 10 [インポート（Import）] をクリックします。

ステップ 11 サービス コールバックテンプレートにこれを繰り返します。

Cisco Unified CVP オペレーションコンソールの構成

順序	タスク	完了したか
1	ネットワーク カードの検証 （61 ページ）	
2	Unified CVP オペレーションコンソールの有効化 （70 ページ）	
3	Unified CVP コール サーバー コンポーネントの構成 （71 ページ）	
4	Unified CVP サーバー コンポーネントの構成 （72 ページ）	
5	Unified CVP レポーティングサーバーの構成 （73 ページ）	
6	Unified CVP メディアサーバーの構成 （74 ページ）	
7	Unified CVP ライセンスのインストール （74 ページ）	
8	ゲートウェイの構成 （75 ページ）	
9	Unified CCE デバイスの追加 （76 ページ）	
10	Unified Communications Manager デバイスの追加 （77 ページ）	
11	Unified Intelligence Center デバイスの追加 （77 ページ）	
12	スクリプトおよびメディアファイルの転送 （75 ページ）	
13	SNMP の構成 （76 ページ）	
14	SIP サーバーグループの構成 （78 ページ）	
15	ダイヤル番号パターンの構成 （79 ページ）	

Unified CVP オペレーションコンソールの有効化

Cisco Unified CVP オペレーションコンソールを有効化するには、CVP OAMP サーバーで、以下の手順を実行します。

手順

ステップ 1 **[スタート（Start）] > [実行（Run）]** の順に選択し、**services.msc** と入力します。

ステップ 2 Cisco CVP OPSConsoleServer サービスが実行中であることを確認します。実行中でない場合は、そのサービスを右クリックし、**[スタート（Start）]** をクリックします。

ステップ 3 **[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Unified Customer Voice Portal] > [オペレーションコンソール（Operation Console）]** の順に選択し、Unified CVP

OPSConsole ページを開きます。 Microsoft Internet Explorer を使用している場合は、自己署名証明書を受け入れる必要があります。

Unified CVP コール サーバー コンポーネントの構成

（注）
- 500 エージェント展開では、サイド A とサイド B に Unified CVP サーバーが 1 台ずつあります。
- 1000 エージェント展開では、サイド A とサイド B に Unified CVP サーバーが 2 台ずつあります。
- 4000 エージェント展開では、サイド A とサイド B に Unified CVP サーバーが 8 台ずつあります。

手順

ステップ 1 Unified CVP OAMP サーバーで、**[スタート（Start）]**>**[すべてのプログラム（All Programs）]**>**[Cisco Unified Customer Voice Portal]** の順に選択します。

ステップ 2 **[オペレーションコンソール（Operations Console）]** をクリックして、ログインします。

ステップ 3 **[デバイス管理（Device Management）]** > **[Unified CVPコールサーバー（Unified CVP Call Server）]** の順に選択します。

ステップ 4 [新規追加（Add New）] をクリックします。

ステップ 5 [一般（General）] タブで、Cisco Unified CVP サーバー のIP アドレスとホスト名を入力します。**[ICM]**、**[IVR]** および **[SIP]** にチェックを入れます。**[次へ（Next）]** をクリックします。

ステップ 6 **[ICM]** タブをクリックします。各 Cisco Unified CVP コールサーバーで、VRU 接続ポートのデフォルトポートを 5000 のままにします。

ステップ 7 **[SIP]** タブをクリックします。

a) [アウトバウンドプロキシを有効にする（Enable outbound proxy）] フィールドで、**[いいえ（No）]** を選択します。

b) [DNS SRVタイプクエリの使用（Use DNS SRV type query）] フィールドで、**[はい（Yes）]** を選択します。

c) **[SRVレコードをローカルに解決（Resolve SRV records locally）]** をオンにします。

ステップ 8 **[デバイスプール（Device Pool）]** タブをクリックします。デフォルトのデバイス プールが選択されていることを確認してください。

ステップ 9 （オプション）**[インフラストラクチャ（Infrastructure）]** タブをクリックします。[Syslog設定の構成（Configuration Syslog Settings）] ペインで、これらのフィールドを次のように構成します。

a) syslog サーバの IP アドレスまたはホスト名を入力します。

例：

プライムサーバー

b) syslog サーバーのポート番号に **514** と入力します。

c) Reporting Server がログ メッセージを書き込むバックアップサーバーの名前を入力します。

d) [バックアップサーバーポート番号（Backup server port number）] フィールドに、バックアップ syslog サーバーのポート番号を入力します。

ステップ 10 [保存して展開（Save & Deploy）] をクリックします。

ステップ 11 残りの Unified CVP サーバーに対してこの手順を繰り返します。

Unified CVP サーバー コンポーネントの構成

Cisco Unified CVP サーバーの VXML サーバー コンポーネントを構成するには、以下の手順を実行します。

（注）

- 2000 エージェント展開では、サイド A とサイド B に Unified CVP サーバーが 1 台ずつあります。
- 4000 エージェント展開および Small Contact Center エージェント展開では、サイド A とサイド B には Unified CVP サーバーが 8 台ずつあります。
- 12000 エージェント展開では、サイド A とサイド B に Unified CVP サーバーが 24 台ずつあります。

手順

ステップ 1 Unified CVP オペレーションコンソールで、**[デバイス管理（Device Management）]** > **[Unified CVP VXMLサーバー（Unified CVP VXML Server）]** に移動します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [一般（General）] タブで、Cisco Unified CVP サーバーの IP アドレスとホスト名を入力します。

ステップ 4 プライマリおよびバックアップ CVP コールサーバーを構成します。

ステップ 5 [構成（Configuration）] タブをクリックします。**[CVP VXMLサーバーに対してレポーティングを有効化する（Enable reporting for this CVP VXML Server）]** フィールドで、**[はい（Yes）]** をクリックし、任意でレポーティングを有効化します。レポーティングを有効化しない場合は、**[いいえ（No）]** を選択します。

ステップ 6 **[デバイスプール（Device Pool）]** タブをクリックします。デフォルトのデバイス プールが選択されていることを確認してください。プライマリおよびセカンダリ コールサーバーを再起動するように求められたら、[いいえ、今は再起動しないでください。（No. Do not restart at this time.）] をクリックします。

ステップ 7 [保存して展開（Save & Deploy）] をクリックします。

ステップ 8 すべての CVP サーバーに対して、この手順を繰り返します。

Unified CVP レポーティングサーバーの構成

オペレーションコンソールで Unified CVP レポーティング サーバーコンポーネントを構成するには、以下の手順を実行します。

（注） CVP レポーティングサーバーへの負荷バランスを取るため、各サイドには、2 つの CVP レポーティングサーバーが展開されています。お客様が、2 つのレポーティングサーバーを保持している場合は CVP レポーティング サーバー サイド A を構成し、すべての サイド A CVP コールサーバーを関連付けます。サイド B レポーティングサーバーでは、サイド B に属しているすべての CVP コールサーバーを関連付けます。これは、各 CVP コールサーバーと各 VXML サーバーは、1 つのレポーティングサーバーにしか関連付けることができないからです。レポートは、複数の Informix データベース間で作成できません。サイド A のコールサーバーは、サイド A のレポーティングサーバーにのみレポートし、サイド B のコールサーバーは、サイド B のレポーティングサーバーにのみレポートします。

お客様が保持する CVP レポーティングサーバーが 1 台の場合は、1 台のレポーティングサーバーにすべてのコールサーバーを関連付けます。一時的なデータベースの停止中は、メッセージがファイルにバッファリングされ、データベースがオンラインに戻った後にデータベースに挿入されます。メッセージをバッファできる時間は、システムによって異なります。

手順

ステップ 1 オペレーションコンソールで、**[デバイス管理（Device Management）]** > **[Unified CVP レポーティングサーバー（Unified CVP Reporting Server）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[一般（General）]** タブで、以下項目を構成します。

a) IP アドレスを入力します。
b) ホスト名を入力します。
c) 使用可能なすべての関連する Unified CVP コールサーバーを選択します。

ステップ 4 **[インフラストラクチャ（Infrastructure）]** タブで次を構成します。

a) [最大スレッド（Maximum Threads）]、[統計集約間隔（Statistics Aggregation Interval）]、[ログファイルプロパティ（Log File Properties）] の設定はデフォルトのままにしておきます。
b) レポーティングサーバーが、syslog イベントを送信する Syslog サーバーの IP アドレスまたはホスト名を入力します。

例：

プライムサーバー

c) サーバーポート番号に **514** と入力します。

d) レポーティングサーバーが、syslogイベントを送信するオプションのバックアップサーバーの IP アドレスまたはホスト名を入力します。
e) オプションのバックアップサーバーのポート番号を入力します。

ステップ 5 [保存して展開（Save & Deploy）] をクリックします。

ステップ 6 すべての CVP レポーティングサーバーに対して手順 1 ～ 5 を繰り返します。

Unified CVP メディアサーバーの構成

手順

ステップ 1 CVP オペレーションコンソールで、**[デバイス管理（Device Management）] > [メディアサーバー（Media Server）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 **[一般（General）]** タブで、以下項目を構成します。
a) Unified CVP サーバーの IP アドレスとホスト名を入力します。
b) **[FTPの有効化（FTP Enabled）]** をオンにします。
c) **[匿名アクセス（Anonymous Access）]** をオンにするか、ログイン情報を入力します。
d) **[サインインのテスト（Test SignIn）]** をクリックして、FTP アクセスを検証します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 すべてのメディアサーバーに対して手順 1 ～ 4 を繰り返します。

ステップ 6 すべてのメディアサーバーを構成したら、**[展開（Deploy）]** をクリックします。

ステップ 7 [展開ステータス（Deployment Status）] をクリックして、構成が適用されていることを確認します。

ステップ 8 CVP オペレーションコンソールで、**[デバイス管理（Device Management）] > [メディアサーバー（Media Server）]** の順に選択します。

ステップ 9 [デフォルトメディアサーバー（Default Media Server）] を **[なし（None）]** からいずれかの Unified CVP サーバーに変更します。**[設定（Set）]** をクリックします。

ステップ 10 [展開（Deploy）] をクリックします。

Unified CVP ライセンスのインストール

手順

ステップ 1 **CVP オペレーションコンソール** にサインインします。

ステップ 2 **[一括管理（Bulk Administration）] > [ファイル転送（File Transfer）] > [ライセンス（Licenses）]** の順に選択します。

ステップ 3 [デバイスタイプの選択（Select device type）] フィールドで、**[すべてのUnified CVPデバイス（All Unified CVP devices）]** を選択します。

ステップ 4 ライセンスファイルを参照して選択します。

ステップ 5 [転送（Transfer）] をクリックします。

ステップ 6 [ファイル転送ステータス（File Transfer Status）] をクリックして転送の進捗状況をモニタします。

ゲートウェイの構成

手順

ステップ 1 Unified CVP Operations Console で、**[デバイス管理（Device Management）]** > **[ゲートウェイ（Gateway）]** に移動します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [一般（General）] タブで、以下の通り設定します。

a) IP アドレスを入力します。
b) ホスト名を入力します。
c) デバイス タイプを選択します。
d) [ユーザ名とパスワード（Username and Passwords）] ペインに、ユーザ名とパスワードを入力し、パスワードを有効にします。

ステップ 4 [サインインのテスト（Test Sign-in）] をクリックして、ゲートウェイとの接続を確立でき、ログイン情報が正しいことを確認します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 すべてのゲートウェイに対して繰り返し行ってください。

スクリプトおよびメディアファイルの転送

通知先を作成し、すべての Unified CVP デバイスに展開します。

手順

ステップ 1 Unified CVP オペレーションコンソールで、**[一括管理（Bulk Administration）]** > **[ファイル転送（File Transfer）]** > **[スクリプト&メディア（Scripts & Media）]** の順に選択します。

ステップ 2 [デバイスタイプの選択（Select device type）] フィールドで、**ゲートウェイ**を選択します。

ステップ 3 すべてのゲートウェイを [選択済み（Selected）] に移動します。

ステップ 4 **[デフォルトゲートウェイファイル（Default Gateway files）]** をクリックします。

ステップ 5 **[転送（Transfer]** をクリックし、ポップアップウィンドウで **[OK]** を選択します。

ステップ 6 [ファイル転送ステータス（File Transfer Status）] をクリックして転送の進捗状況をモニタします。

SNMP の構成

手順

ステップ 1 Unified CVP Operations Consoleで、**SNMP** > **V1/V2c** > **コミュニティ文字列** に移動します。

ステップ 2 [新規追加（Add New）] をクリックします。

a) **一般** タブで、コミュニティ文字列の名前を指定します。
b) **デバイス** タブで、使用可能なデバイスのリストから必要なデバイスを選択します。
c) [保存して展開（Save and Deploy）] をクリックします。

ステップ 3 通知先を作成し、すべての Unified CVP デバイスに展開します。

a) **[SNMP]** > **[V1/V2c]** > **[通知の送信先（Notification Destination）]** の順に選択します。
b) [新規追加（Add New）] をクリックします。
c) 各フィールドに値を指定します。
d) [デバイス（Devices）] タブを選択し、SNMP 通知先をデバイスに割り当てます。
e) [保存して展開（Save and Deploy）] をクリックします。

Unified CCE デバイスの追加

手順

ステップ 1 **Unified CVP オペレーションコンソール**にログインします。

ステップ 2 **[デバイス管理（Device Management）]** > **[Unified ICM]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 [一般（General）] タブで、以下の通り設定します。

a) IP アドレスを入力します。
b) ホスト名を入力します。
c) [有用性の有効化（Enable Serviceability）] を選択します。
d) ユーザ名を入力します。
e) パスワードを入力します。
f) パスワードを確認します。
g) デフォルト ポートを受け入れます。

（注） Small Contact Center 展開では、エージェント PG の NAT IP アドレスを追加します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 すべての Unified CCE マシンに対して手順 1 ー 5 を繰り返します。

Unified Communications Manager デバイスの追加

手順

ステップ 1 **CVP オペレーションコンソール**にログインします。
ステップ 2 **[デバイス管理（Device Management）] > [Unified CM]** の順に選択します。
ステップ 3 [新規追加（Add New）] をクリックします。
ステップ 4 [一般（General）] タブで、以下の通り設定します。

a) IP アドレスを入力します。
b) ホスト名を入力します。
c) [同期の有効化（Enable Synchronization）] をオンにします。
d) ユーザ名を入力します。
e) パスワードを入力します。
f) パスワードを確認します。
g) デフォルト ポートを受け入れます。

（注） Small Contact Center 展開では、Unified CM の NAT IP アドレスを追加します。

ステップ 5 [保存（Save）] をクリックします。
ステップ 6 すべての Unified Communications Manager デバイスに対して手順 1 ー 5 を繰り返します。

Unified Intelligence Center デバイスの追加

手順

ステップ 1 **CVP オペレーションコンソール**にログインします。
ステップ 2 Cisco Unified Intelligence Center デバイスに移動します。**[デバイス管理（Device Management）] > [Unified IC]** の順に選択します。
ステップ 3 [新規追加（Add New）] をクリックします。
ステップ 4 [一般（General）] タブで、以下の通り設定します。

a) IP アドレスを入力します。
b) ホスト名を入力します。
c) [有用性の有効化（Enable Serviceability）] を選択します。
d) ユーザ名を入力します。
e) パスワードを入力します。
f) パスワードを確認します。
g) デフォルト ポートを受け入れます。

h) 既存のすべての CVP レポーティングサーバーを関連付けます。

ステップ 5 [保存（Save）] をクリックします。

SIP サーバーグループの構成

SIP サーバーグループは、Cisco Unified Communications Manager およびゲートウェイで必要となります。

手順

ステップ 1 Unified CVP オペレーションコンソールで、**[システム（System）]**>**[SIPサーバーグループ（SIP Server Group）]** の順に選択します。

ステップ 2 Cisco Unified Communications Manager デバイス用のサーバーグループを作成します。

a) [一般（General）] タブで、**[新規追加（Add New）]** をクリックします。

b) **[SRVドメイン名FQDN（SRV Domain Name FQDN）]** フィールドに、Communications Manager の エンタープライズパラメータの Cluster FQDN 設定でも使用する値を入力します。たとえば、cucm.cisco.com のようになります。

c) **[IPアドレス/ホスト名（IP Address/Hostname）]** フィールドに、Unified Communications Manager ノードの IP アドレスまたはホスト名を入力します。

d) [追加（Add）] をクリックします。

e) Unified Communications Manager サブスクライバごとに手順 c と d を繰り返します。[保存（Save）] をクリックします。

（注） サーバーグループに Publisher ノードを置かないでください。

Communications Manager 用の SIP サーバーグループは SCC 展開に対して必要ありません。これは、Communications Manager から SCC モデルの CVP に作成された直接 SIP トランクが存在しないからです。

ステップ 3 ゲートウェイ デバイス用にサーバーグループを作成します。

a) [一般（General）] タブで、**[新規追加（Add New）]** をクリックします。

b) **[SRVドメイン名FQDN（SRV Domain Name FQDN）]** フィールドに、SRV ドメイン名 FQDN を入力します。たとえば、vxmlgw.cisco.com のように入力します。

c) **[IPアドレス/ホスト名（IP Address/Hostname）]** フィールドに、各ゲートウェイの IP アドレスまたはホスト名を入力します。

d) [追加（Add）] をクリックします。

e) ゲートウェイごとに手順 c と d を繰り返します。[保存（Save）] をクリックします。

展開と分岐に適切な VXML ゲートウェイをすべて追加します。すべての VXML ゲートウェイをサーバーグループに追加すると、すべてのメンバー サーバー グループ ゲートウェイに対してコールのロードバランスが行われます。

ステップ 4 これらサーバーグループをすべての Unified CVP コールサーバーに関連付けます。

a) **[コールサーバー展開（Call Server Deployment）]** タブで、すべての Unified CVP コールサーバーを **[利用可能（Available）]** リストから **[選択済み（Selected）]** リストに移動します。
b) [保存して展開（Save and Deploy）] をクリックします。

（注）
- Small Contact Center エージェント展開の場合、CUBE(SP) は FQDN 構成に対応していないため、各サブカスタマーに対して CUBE(SP) を指す SIP サーバーグループを作成できません。
- 12000 エージェント導入モデルでは、各 CUCM クラスタにサブスクライバノードを持つ 1 つの SIP サーバーグループが必要です。

ダイヤル番号パターンの構成

ダイヤル番号パターンは、次の場合に必要です。

- エージェント デバイス
- ネットワーク VRU
- 呼出音
- エラー

手順

ステップ 1 Unified CVP Operations Console で、**[システム（System）]** > **[ダイヤル番号パターン（Dialed Number Pattern）]** に移動します。

ステップ 2 以下の表のダイヤル番号パターンごとに、以下の手順を実行します。

a) [新規追加（Add New）] をクリックします。
b) [ダイヤル番号パターン（Dialed Number Pattern）] フィールドに、ダイヤル番号パターンを入力します。
c) [説明（Description）] フィールドに、ダイヤル番号パターンの説明を入力します。
d) [ダイヤル番号パターンのタイプ（Dialed Number Pattern Types）] ペインで、指定したダイヤル番号パターンのタイプを確認します。
e) **[保存（Save）]**をクリックします。

ステップ 3 すべてのダイヤル番号パターンを設定した後、[展開（Deploy）] をクリックします。

ステップ 4 [展開ステータス（Deployment Status）] をクリックして、構成が適用されていることを確認します。

ダイヤル番号パターン	説明	ダイヤル番号パターンのタイプ
91*	呼出音	[ローカル スタティック ルートを有効にする（Enable Local Static Route）] をオンにします。 SIP サーバーグループ、および IP アドレス/ホスト名/サーバーグループ名へのルートは、いずれも VXML ゲートウェイです（たとえば、vxmlgw.Cisco.com）。 [発信元へのコールの送信を有効にする（Enable Send Calls to Originator）] をオンにします。
92*	エラー	[ローカル スタティック ルートを有効にする（Enable Local Static Route）] をオンにします。 SIP サーバーグループ、および IP アドレス/ホスト名/サーバーグループ名へのルートは、いずれも VXML ゲートウェイです（たとえば、vxmlgw.Cisco.com）。 [発信元へのコールの送信を有効にする（Enable Send Calls to Originator）] をオンにします。
エージェント拡張パターン。たとえば、エージェント内線の範囲が 5001 ～ 500999 の場合は 500* と入力します。	エージェント デバイス。	[ローカル スタティック ルートを有効にする（Enable Local Static Route）] をオンにします。 SIP サーバーグループ、および IP アドレス/ホスト名/サーバーグループ名へのルートは、いずれも Unified Communications Manager ゲートウェイです。 [発信コールのRNA タイムアウトを有効にする（Enable RNA Timeout for Outbound Calls）] をオンにします。デフォルトのタイムアウト値は60秒です。
777*	ネットワーク VRU ラベル	[ローカル スタティック ルートを有効にする（Enable Local Static Route）] をオンにします。 SIP サーバーグループ、および IP アドレス/ホスト名/サーバーグループ名へのルートは、いずれも VXML ゲートウェイです（たとえば、vxmlgw.Cisco.com）。 [発信元へのコールの送信を有効にする（Enable Send Calls to Originator）] をオンにします。

ダイヤル番号パターン	説明	ダイヤル番号パターンのタイプ
SCC モデルのサブカスタマーに対するエージェントの内線パターン。たとえば、エージェント内線の範囲が 5001 ～ 500999 の場合は 500* と入力します。	SCC モデルのサブ カスタマーに対するエージェント デバイス ラベル。	[ローカル スタティック ルートを有効にする（Enable Local Static Route）] をオンにします。 [IPアドレス/ホスト名/サーバーグループ（IP Address/Hostname/Server Group）] フィールドに、CUBE(SP) での CVP 隣接関係のシグナリング IP アドレスとポートを、<IP アドレス>:<ポート番号> の形式で入力します。 各サブ カスタマーごとに一意のポートを設定する必要があります。 [発信コールのRNA タイムアウトを有効にする（Enable RNA Timeout for Outbound Calls）] をオンにします。タイムアウトは 15 秒です。

（注） 12000 エージェント導入モデルでは、各 CUCM クラスタに、エージェントの内線の範囲が設定された個別のダイヤル番号パターンが必要です。

ステップ 5 Unified CVP コール サーバのコンポーネントを再起動します。

Cisco IOS Enterprise 音声ゲートウェイの構成

Cisco IOS 音声ゲートウェイを設定するには、次の手順を実行します。特に明記されていない限り、手順は TDM および Cisco UBE 音声ゲートウェイの両方に適用されます。

（注） すべての構成手順を **enable** > **configuration terminal** モードで実行します。

```
logging buffered 2000000 debugging
no logging console
service timestamps debug datetime msec localtime
ip routing
ip cef
ip source-route
interface GigabitEthernet0/0
     ip route-cache same-interface
     duplex auto
     speed auto
     no keepalive
     no cdp enable

voice service voip
     no ip address trusted authenticate
     ip address trusted list
          ipv4 0.0.0.0 0.0.0.0 # OR an explicit Source IP Address Trust List
     allow-connections sip to sip
     signaling forward unconditional
```

イングレスゲートウェイの構成

手順

ステップ 1 グローバル設定を次のように構成します。

```
voice service voip
 no ip address trusted authenticate
 allow-connections sip to sip
 signaling forward unconditional
 # If this gateway is being licensed as a Cisco UBE the following lines are also required

 mode border-element
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0               # Or an explicit Source IP Address Trust List
sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru
```

ステップ 2 音声コーデック プリファレンスを次のように設定します。

```
voice class codec 1
     codec preference 1 g711ulaw
     codec preference 2 g729r8
```

ステップ 3 デフォルトのサービスを次のように設定します。

```
#Default Services
application
     service survivability flash:survivability.tcl
```

ステップ 4 ゲートウェイおよび sip-ua タイマーを次のように設定します。

```
gateway
 media-inactivity-criteria all
 timer receive-rtp 1200

sip-ua
 retry invite 2
 retry bye 1
 timers expires 60000
 timers connect 1000
 reason-header override
```

ステップ 5 POTS ダイヤルピアを次のように設定します。

```
# Configure Unified CVP survivability
dial-peer voice 1 pots
     description CVP TDM dial-peer
     service survivability
     incoming called-number .T
     direct-inward-dial
```

ステップ 6 スイッチ レッグを次のように設定します。

```
#Configure the Switch leg where
# preference is used to distinguish between sides.
# max-conn is used prevent overloading of Unifed CVP
# options-keepalive is used to handle failover
```

```
# Note: the example below is for gateways located on the A-side of a geographically
#distributed deployment
# Note: Ensure that you configure switch dial-peers for each Unified CVP server.

dial-peer voice 70021 voip
     description Used for Switch leg SIP Direct
     preference 1
     max-conn 225
     destination-pattern xxxx..... #Customer specific destination pattern
     session protocol sipv2
     session target ipv4:###.###.###.###     #IP Address for Unified CVP1, SideA
     session transport tcp
     voice-class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad



dial-peer voice 70023 voip
     description Used for Switch leg SIP Direct
     preference 2
     max-conn 225
     destination-pattern xxxx..... #Customer specific destination pattern
     session protocol sipv2
     session target ipv4:###.###.###.###    #IP Address for Unified CVP1, SideB
     session transport tcp
     voice-class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad
```

ステップ 7 ハードウェア リソース（トランスコーダ、会議ブリッジ、および MTP）を次のように設定します。

（注） この構成セクションは、仮想 CUBE あるいは CSR 1000v ゲートウェイには必要ありません。上記には、物理 DSP リソースがありません。

```
#For gateways with physical DSP resources, configure Hardware resources using
#Unified Communications Domain Manager.

# Configure the voice-cards share the DSP resources located in Slot0
voice-card 0
     dspfarm
     dsp services dspfarm
voice-card 1
     dspfarm
     dsp services dspfarm
voice-card 2
     dspfarm
     dsp services dspfarm
voice-card 3
     dspfarm
     dsp services dspfarm
voice-card 4
     dspfarm
     dsp services dspfarm

# Point to the contact center call manager
sccp local GigabitEthernet0/0
     sccp ccm ###.###.###.### identifier 1 priority 1 version 7.0 # Cisco Unified CM sub
 1
```

```
     sccp ccm ###.###.###.### identifier 2 priority 1 version 7.0 # Cisco Unifed CM sub
 2

# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
     associate ccm 1 priority 1
     associate profile 2 register <gw70mtp>
     associate profile 1 register <gw70conf>
     associate profile 3 register <gw70xcode>

# Configure DSPFarms for Conference, MTP and Transcoder

dspfarm profile 1 conference
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions 24
     associate application SCCP

dspfarm profile 2 mtp
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions software 500
     associate application SCCP

dspfarm profile 3 transcode universal
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions 52
     associate application SCCP

# Note: Universal transcoder is only needed for cases where you engage the G.729 caller
 to
G.729 only agent with IVR in middle and performs any supplementary services or use
features
like whisper announcement or agent greeting.
```

ステップ 8 （任意）SIP トランキングを設定します。

```
# Configure the resources to be monitored
voice class resource-group 1
     resource cpu 1-min-avg threshold high 80 low 60
     resource ds0
     resource dsp
     resource mem total-mem
     periodic-report interval 30

# Configure one rai target for each CVP Server
sip-ua
     rai target ipv4:###.###.###.### resource-group1 # CVP1A
     rai target ipv4:###.###.###.### resource-group1 # CVP2A
     rai target ipv4:###.###.###.### resource-group1 # CVP1B
     rai target ipv4:###.###.###.### resource-group1 # CVP2B
     permit hostname dns:%Requires manual replacement - ServerGroup Name defined in
CVP.System.SIP Server Groups%
```

ステップ 9 着信 PSTN SIP トランク ダイヤルピアを設定します。

```
dial-peer voice 70000 voip
     description Incoming Call From PSTN SIP Trunk
     service survivability
     incoming called-number xxxx……    # Customer specific incoming called-number pattern
```

```
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     session protocol sipv2
     voice class codec 1
     no vad
```

VXML ゲートウェイの構成

始める前に

（注） VVB を構成している場合は、VXML ゲートウェイを構成する必要はありません。VVB または VXML ゲートウェイのいずれか、または両方を構成できます。

手順

ステップ 1 グローバル設定を次のように構成します。

```
voice service voip
sip
     rel1xx disable
     header-passing
     options-ping 60
     midcall-signaling passthru
```

ステップ 2 デフォルトの Unified CVP サービスを次のように設定します。

```
#Default CVP Services
application
     service new-call flash:bootstrap.vxml
     service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
     service ringtone flash:ringtone.tcl
     service cvperror flash:cvperror.tcl
     service bootstrap flash:bootstrap.tcl
```

ステップ 3 ダイヤルピアを次のように設定します。

（注） VXML ゲートウェイの構成時には、音声クラス コーデックは使用しないでください。ダイヤルピアには一般に G711ulaw を使用できますが、実装によってはその他のコーデックを使用することがあります。

```
# Configure Unified CVP Ringtone
dial-peer voice 919191 voip
     description CVP SIP ringtone dial-peer
     service ringtone
     incoming called-number 9191T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad

# Configure Unified CVP Error
```

```
dial-peer voice 929292 voip
     description CVP SIP error dial-peer
     service cvperror
     incoming called-number 9292T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad
```

ステップ 4 デフォルトの Unified CVP HTTP、ivr、rtsp、mrcp および vxml 設定を構成します。

```
http client cache memory pool 15000
http client cache memory file 1000
http client cache refresh 864000
no http client connection persistent
http client connection timeout 60
http client connection idle timeout 10
http client response timeout 30
ivr prompt memory 15000
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
rtsp client timeout connect 10
rtsp client timeout message 10
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
vxml tree memory 500
vxml audioerror
vxml version 2.0
```

ステップ 5 プライマリおよびセカンダリ メディア サーバを次のように設定します。

```
#Configure the media servers where
# the primary matches the default media server defined in OAMP.
# the secondary is located on the opposite side of the primary.

ip host mediaserver ###.###.###.###          # IP Address for primary media server.
ip host mediaserver-backup ###.###.###.###   # IP Address for secondary media server.
```

ステップ 6 着信コール番号がネットワーク VRU ラベルと一致する VXML レッグを設定します。

```
dial-peer voice 7777 voip
     description Used for VRU leg
     service bootstrap
     incoming called-number 777T
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad
```

ステップ 7 ASR TTS を次のように設定します。

```
#Configure primary server
ip host asr-en-us <ASR server ip>
ip host tts-en-us <TTS server hostname>
voice class uri TTS sip
pattern tts@<TTS server ip>
voice class uri ASR sip
pattern asr@<ASR server hostname>
ivr asr-server sip:asr@<ASR server hostname*>
ivr tts-server sip:tts@<TTS server hostname*>

dial-peer voice 5 voip
     description FOR ASR calls
     preference1
```

```
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     session target ipv4:<ASR server IP>
     destination uri ASR
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad

dial-peer voice 6 voip
     description FOR TTS calls
     preference1
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     session target ipv4:<TTS server IP>
     destination uri TTS
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad

#Configure backup server
dial-peer voice 7 voip
     destination uri ASR
     session target ipv4:<ASR backup server IP>
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry
     2dtmf-relay rtp-nte
     codec g711ulaw
     preference 2
     no vad

dial-peer voice 8 voip
     destination uri TTS
     session target ipv4:<TTS backup server IP>
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry
     2dtmf-relay rtp-nte
     codec g711ulaw
     preference 2
     no vad
```

Unified Communications Manager の構成

Unified Communications Manager を構成するには、以下の手順を実行します。

順序	タスク	完了したか
1	Unified Communications Manager Publisher の構成 （88 ページ）	
2	Unified Communications Manager Subscriber の構成 （89 ページ）	
3	Windows 用 VMware ツールのインストール （394 ページ）	

順序	タスク	完了したか
4	Unified Communications Manager ライセンス （90 ページ）	
5	サービスのアクティブ化 （91 ページ）	
6	クラスタ全体のドメイン構成の検証 （92 ページ）	
7	Unified CCE サーバー に JTAPI をインストール （93 ページ）	
8	SNMP の構成 （120 ページ）	

Unified Communications Manager Publisher の構成

Subscriber をカスタマイズする前に、Unified Communications Manager Publisher をカスタマイズしてください。

始める前に

ネットワークアダプタおよびフロッピードライブに対して、仮想マシンデバイスのステータスが、**[電源投入時に接続（Connect at Power On）]** になっていることを確認します。

手順

ステップ 1 パブリッシャの電源を入れます。これにより、.flp ファイルの情報に基づいてインストールが始まります。インストールは通知なしで自動で実行開始されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 2 VM の **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、Publisher マシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 3 VM を右クリックし、**[設定の編集（Edit settings）]** を選択し、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

（注） Publisher/プライマリをカスタマイズすると、ユーザー名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

- OS 管理者のデフォルトパスワード：**c1sco@123**
- アプリケーションユーザー名：**Administrator**
- アプリケーションユーザーのデフォルトパスワード：**c1sco@123**
- Sftp パスワード：**c1sco@123**
- IPSec パスワード：**c1sco@123**

Unified Communications Manager Subscriber の構成

Subscriber を追加するために Unified Communications Manager Publisher を起動

サブスクライバを追加するには、パブリッシャ ノードを起動する必要があります。

手順

ステップ 1 http://<IP Addr of CUCM Publisher>/ccmadmin のブラウザで、Unified Communications Manager Publisher を起動します。

ステップ 2 ユーザー名とパスワードを入力して、Unified Communications Manager にログインします。

ステップ 3 **[システム（System）]** > **[サーバー（Server）]** > **[新規追加（Add New）]** の順に選択します。

ステップ 4 サーバーの追加ページで、サーバータイプに対して、**[Cisco Unified Communications Manager 音声/ビデオ（CUCM Voice/Video）]** を選択します。[次へ（Next）] をクリックします。

ステップ 5 サーバー情報ページで、1 つ目の Subscriber の IP アドレスを入力します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 2 つ目の Subscriber に対して手順 3 ～ 6 を繰り返します。

Subscriber の構成

始める前に

ネットワークアダプタおよびフロッピードライブに対して、仮想マシンデバイスのステータスが、**[電源投入時に接続（Connect at Power On）]** になっていることを確認します。

手順

ステップ 1 Subscriber の電源をオンにします。
.flp ファイルの情報に基づいてインストールが始まります。インストールが自動的に始まり、ユーザの操作なしで実行されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 2 VM の **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、Cisco Unified Communications Manager セカンダリマシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 3 VM を右クリックし、**[設定の編集（Edit settings）]** を選択し、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

（注） サブスクライバノードのカスタマイズ中、ユーザー名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

- OS 管理者のデフォルトパスワード：**c1sco@123**
- アプリケーションユーザー名：**Administrator**
- アプリケーションユーザーのデフォルトパスワード：**c1sco@123**
- Sftp パスワード：**c1sco@123**
- IPSec パスワード：**c1sco@123**

Unified Communications Manager ライセンス

Unified Communications Manager ライセンスを設定するには、最初に製品インスタンスを追加します。その後、ライセンスの生成と登録を行い、最後にそのライセンスをインストールします。

Unified Communications Manager ライセンスのアップグレード

手順

ステップ 1 電子メール メッセージからライセンス ファイルを解凍します。

ステップ 2 ブラウザ（`https://<IP Address of CUCM Publisher>`）で Unified Communications Manager を起動します。

ステップ 3 **Cisco Prime License Manager** をクリックし、**[ライセンス（License）]** > **[履行（Fulfillment）]** の順に選択します。

ステップ 4 [その他の履行オプション（Other Fulfillment Options）] で、[ライセンスをファイルから履行（Fulfill Licenses from File）] を選択します。

ステップ 5 [参照（Browse）] をクリックしてライセンス ファイルを検索します。

ステップ 6 [インストール（Install）] をクリックし、ポップアップ ウィンドウを閉じます。

ステップ 7 [製品インスタンス（Product Instances）] に移動します。古いインスタンスを削除します。次に、[追加（Add）] をクリックします。

ステップ 8 Cisco Unified Communications Manager パブリッシャの名前、ホスト名/IP アドレス、ユーザ名、およびパスワードを入力します。

ステップ 9 Unified CM の製品タイプを選択します。

ステップ 10 [OK] をクリックします。

ステップ 11 [今すぐ同期（Synchronize Now）] をクリックします。

ライセンスの生成と登録

手順

ステップ 1 [ライセンス管理（License Management）] -> [ライセンス（Licenses）] に移動します。[他の履行（Other Fulfillment）] オプションの下で、[ライセンス要求の生成（Generate License Request）] をクリックします。

ステップ 2 **[ライセンス要求と次の手順（License Request and Next Steps）]** ウィンドウが開いたら、指示に従ってテキスト（PAK ID）をコピーし、テキスト エディタに保存します。

ステップ 3 [シスコ ライセンス登録（Cisco License Registration）] サイトをクリックし、そのサイトで手順を続行します。必要になるので、PAK を近くに置いておきます。

ステップ 4 プロンプトが表示されたら、PAK を入力します。

ライセンス ファイルが電子メール メッセージで届きます。

ライセンスのインストール

ライセンスをインストールするには、以下の手順を実行します。

手順

ステップ 1 電子メール メッセージからライセンス ファイルを解凍します。

ステップ 2 **[ライセンス管理（License Management）] > [ライセンス（Licenses）]** の順に選択します。

ステップ 3 [その他の履行オプション（Other Fulfillment Options）] で、**[ライセンスをファイルから履行（Fulfill Licenses from File）]** を選択します。

ステップ 4 ライセンスファイルを参照し、**[インストール（Install）]** をクリックします。

ステップ 5 **[監視（Monitoring）] をクリックして、ライセンスの利用**ページに移動し、インストールが正常に完了したことを確認します。

サービスのアクティブ化

サービスをアクティブ化するには、次の手順を実行します。

手順

ステップ 1 ブラウザで Unified Communications Manager を起動します（http://<IP Address of CUCM Node>）。

ステップ 2 Cisco Unified Serviceability で、**[ツール（Tools）] > [サービスのアクティブ化（Service Activation）]** の順に選択します。

ステップ 3 [サーバー（Server）] ドロップダウンリストで、サービスを有効化するサーバーを選択し、**[移動（Go）]** をクリックします。

ウィンドウには、サービスのサービス名とアクティベーション ステータスが表示されます。

ステップ 4 有効化するには、次のサービスを確認します。

a) パブリッシャ:

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco AXL Web Service
- Cisco Bulk Provisioning サービス
- Cisco Serviceability Reporter
- Cisco CTL Provider
- Cisco Certificate Authority Proxy Function

b) Subscriber：

- 通話処理サブスクライバ
  - Cisco CallManager
  - Cisco IP Voice Media Streaming App
  - Cisco CTIManager
  - Cisco CTL Provider
  - Cisco AXL Web Service
- 保留中の TFTP のサブスクライバ

（注） 専用 TFTP および MoH サーバーを持たない HCS for CC 展開の Publisherノードで TFTP サービスを有効にします。

  - Cisco TFTP
  - Cisco IP Voice Media Streaming App

ステップ 5 [保存（Save）] をクリックします。

（注） Cisco CallManager を有効化すると、CTIManager と Cisco Dialed Number Analyzer サーバーが自動的に有効化されます。プロンプトが表示されたら [OK] をクリックします。

クラスタ全体のドメイン構成の検証

コールを実行するには、この検証が必要です。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 2 **[クラスタ全体のドメイン構成（Clusterwide Domain Configuration）]** までスクロールダウンします。

クラスタ完全修飾ドメイン名は、Unified CVP SIP サーバーグループのサーバーグループ名と一致する必要があります（SIP サーバーグループの構成 （78 ページ））。

Unified CCE サーバー に JTAPI をインストール

これで、Unified Communications Manager を構成したので、JTAPI のインストール （55 ページ）をすることができます。

Unified Intelligence Center Coresident 展開の構成

順序	タスク	完了したか
1	Unified Intelligence Center Publisher の構成 （94 ページ）	
2	Unified Intelligence Center Subscriber の構成 （94 ページ）	
3	システムインベントリに共存（ライブデータおよびIdS がある Cisco Unified Intelligence Center ）マシンタイプを追加 （96 ページ）	
4	Windows 用 VMware ツールのインストール （394 ページ）	
5	Unified Intelligence Center レポーティングの構成 （97 ページ）	
6	Unified Intelligence Center Administration の設定 （101 ページ）	
7	SNMP の構成 （120 ページ）	
8	ライブデータ AW アクセスの構成 （104 ページ）	
9	Live Data Unified Intelligence データソースの構成 （106 ページ）	
10	ライブデータレポーティング間隔の構成 （107ページ）	
11	Transport Layer Security の設定 （108 ページ）	

順序	タスク	完了したか
12	ライブデータ レポートのインポート （108 ページ）	
13	HTTPS ガジェットの証明書の追加 （108 ページ）	

Unified Intelligence Center Publisher の構成

Cisco Unified Intelligence Center パブリッシャをカスタマイズするには、先にサブスクライバをカスタマイズしておく必要があります。

始める前に

ネットワークアダプタおよびフロッピードライブに対して、仮想マシンデバイスのステータスが、**[電源投入時に接続（Connect at Power On）]** になっていることを確認します。

手順

ステップ 1 パブリッシャの電源を入れます。
.flp ファイルの情報に基づいてインストールが始まります。インストールが自動的に始まり、ユーザの操作なしで実行されます。1時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 2 VM の **[コンソール（Console）]** タブをクリックします。管理ユーザーのログイン情報を使用して、CUIC プライマリマシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 3 VM を右クリックし、**[設定の編集（Edit settings）]** を選択し、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

（注） Publisher/プライマリをカスタマイズすると、ユーザー名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

- OS 管理者のデフォルトパスワード：**c1sco@123**
- アプリケーションユーザー名：**Administrator**
- アプリケーションユーザーのデフォルトパスワード：**c1sco@123**
- Sftp パスワード：**c1sco@123**
- IPSec パスワード：**c1sco@123**

Unified Intelligence Center Subscriber の構成

ライブデータを使用する Cisco Unified Intelligence Center とライブデータのスタンドアロン展開の両方について、以下の手順を実行します。

（注） サブスクライバノードを追加する前に、ライセンスが更新されていることを確認します。

Publisher を起動して Subscriber を追加

手順

ステップ 1 `http://<HOST ADDRESS>/oamp` の URL をブラウザに入力します。*HOST ADDRESS* は Cisco Unified Intelligence Center Publisher の IP アドレスまたはホスト名で置き換えます。

ステップ 2 インストール時に定義したシステム アプリケーションのユーザ ID とパスワードを使用してサインインします。

ステップ 3 左側のパネルで、**[デバイス管理（Device Management）]** > **[デバイス構成（Device Configuaration）]** の順に選択します。

ステップ 4 [メンバーの追加（Add Member）] をクリックします。

ステップ 5 **[名前（Name）]** フィールドに、ホスト名または IP アドレスを入力します。

ステップ 6 デバイスの**説明**を入力します。

ステップ 7 [保存（Save）] をクリックします。

Subscriber の構成

始める前に

ネットワークアダプタおよびフロッピードライブに対して、仮想マシンデバイスのステータスが、**[電源投入時に接続（Connect at Power On）]** になっていることを確認します。

手順

ステップ 1 Subscriber の電源をオンにします。
.flp ファイルの情報に基づいてインストールが始まります。インストールが自動的に始まり、ユーザの操作なしで実行されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 2 VM の **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、Cisco Unified Intelligence Center セカンダリマシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 3 VM を右クリックし、**[設定の編集（Edit settings）]** を選択し、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

（注） サブスクライバノードのカスタマイズ中、ユーザー名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

- OS 管理者のデフォルトパスワード：**c1sco@123**
- アプリケーションユーザー名：**Administrator**
- アプリケーションユーザーのデフォルトパスワード：**c1sco@123**
- Sftp パスワード：**c1sco@123**
- IPSec パスワード：**c1sco@123**

システムインベントリに共存（ライブデータおよび IdS がある Cisco Unified Intelligence Center ）マシンタイプを追加

手順

ステップ 1 Unified CCE Administration で、**[システム（System）]** > **[展開（Deployment）]** の順に選択します。

ステップ 2 システムインベントリに新規マシンを追加するには、以下の手順を実行します。

a) [追加（Add）] をクリックします。

[マシンの追加（Add Machine）] ポップアップウィンドウが開きます。

b) ドロップダウンメニューで、以下のマシンタイプを選択します。

CUIC_LD_IdS Publisher（2000 エージェント参照デザインで共存可能な Unified Intelligence Center、ライブデータ, およびアイデンティティ サービスマシン）。

c) **[ホスト名（Hostname）]** Finesse で、マシンの FQDN、ホスト名または IP アドレスを入力します。

システムは、入力する値を FQDN に変換しようとします。

d) マシンの管理者用ログイン情報を入力します。

e) [保存（Save）] をクリックします。

マシンとそれに関連する Subscriber またはセカンダリマシンはシステムインベントリに追加されます。

次のタスク

展開からコンポーネントを削除する場合は、システムインベントリからコンポーネントを削除します。コンポーネントを再度追加するには、該当するコンポーネントをシステムインベントリに追加します。

VOS 用 VMware ツールのインストール

VOS を使用して VMware ツールをインストールまたはアップグレードするには、以下の手順を実行します。

手順

ステップ 1 仮想マシンの電源がオンになっていることを確認します。

ステップ 2 [VM] メニューを右クリックします。**[ゲスト（Guest）]**>**[VMwareツールのインストール/アップグレード（Install/Upgrade VMware tools）]** の順に選択します。

ステップ 3 ツールのインタラクティブ更新を選択し、**[OK]** をクリックします。

ステップ 4 コンソールを開き、コマンド プロンプトでログインします。

ステップ 5 **utils vmtools refresh** コマンドを入力して確認します。
サーバが自動的に 2 回再起動します。

ステップ 6 再起動後に、VM の [サマリー（Summary）] タブを調べ、VMware ツールのバージョンが最新であることを確認します。最新でない場合は、VM を再起動し、バージョンを再度確認します。

このプロセスには数分かかります。このプロセスが完了すると、vSphere の VM の [サマリー（Summary）] タブで、ツールが [実行中（最新）（Running (Current)）] と表示されます。

Unified Intelligence Center レポーティングの構成

Unified Intelligence Centerレポーティングを構成するには、以下の手順を実行します。

SQL ユーザーアカウントの構成

Unified CCE 履歴データベースサーバーと Unified CCE リアルタイム データベース サーバーの両サイドで以下の手順を実行して、SQL 認証を許可し、TCP/IP プロトコルとリモートネットワーク接続を有効にします。

手順

ステップ 1 導入環境の Unified CCE 履歴およびリアルタイム データベース サーバーにログインします。

ステップ 2 **SQL サーバー管理スタジオ**を起動します。

ステップ 3 デフォルトのログイン情報を使いログインします。

ステップ 4 **[セキュリティ（Security）]** タブを展開します。**[ログイン（Logins）]** を右クリックし、**[新規ログイン（New Login）]** を選択します。

ステップ 5 **一般**ページで、以下の値を入力します。

a) **ログイン名**を入力します。

例：

ユーザ

b) **SQL サーバー認証**を選択します。
c) **パスワード**を入力し、確認用パスワードを入力します。
d) **[パスワードポリシーの適用（Enforce password policy）]** チェックボックスをオフにします。

ステップ 6 **サーバーの役割**ページで、次のチェックボックスをオンにします：

- **public**
- **securityadmin**
- **server-admin**
- **setupadmin**
- **sysadmin**

ステップ 7 **ユーザーマッピング**ページで、以下の値を入力します。

a) **[リアルタイムデータベース（Real-time database）]** および **[履歴データベース（Historical database）]** チェックボックスをオンにします。
b) **[データベースロールメンバーシップ（Database role memberships）]** ペインで、以下のチェックボックスをオンにします。

- **db_datareader**
- **db_datawriter**
- **db_ddladmin**
- **db_owner**
- **db_securityadmin**
- **public**

ステップ 8 [OK] をクリックします。

Unified Intelligence Center データ ソースの構成

Unified Intelligence Center が Unified CCE 履歴データ ソースおよび Unified CCE リアルタイム データ ソースを構成するには、以下の手順を実行します。

（注） コマンド ライン インターフェイスや従来の名前解決を使用することにより、レポート負荷をいくつかの Unified CCE AW_HDS データベースに分散させることができます。特定のメンバー ノードをデータ ソース インターフェイスで構成されたデータベースホスト以外のデータベースホストにダイレクトする必要がある場合は、「set cuic-properties host-to-ip」というコマンドを使用すると、各ノードごとに異なる方法でデータ ソース名を解決できます。

手順

ステップ 1 管理者として Unified Intelligence Center ポータル（http://{hostname}）にログインします。

ステップ 2 ナビゲーションウィンドウで、**[構成（Configure）] > [データソース（Data Sources）]** の順に選択します。
Unified Intelligence Center レガシーインターフェイスにリダイレクトします。

ステップ 3 **Unified CCE 履歴** データソースを選択します。省略記号の **[編集（Edit）]** をクリックし、データソースページを開きます。[プライマリ（Primary）] タブで、次の値を入力します。

a) [データソースホスト（Datasource Host）] フィールドに、プライマリ履歴データベースサーバー（**AW-HDS-A1**）のホスト名/IP アドレスを入力します。
b) **[ポート（Port）]** フィールドに、SQL サーバーデータベースに使用するポート番号 1433 を入力します。
c) **[データベース名（Database Name）]** フィールドに、プライマリの履歴データベース名を入力します。
d) **[インスタンス（Instance）]** フィールドは、SQL サーバーのオプションであるため、空白のままにします。
e) **[タイムゾーン（Timezone）]** フィールドで、データベースに格納するデータのタイムゾーンを選択します。
f) **[データベースユーザーID（Database User ID）]** フィールドに、Cisco Unified Intelligence Center またはデータベースへのアクセス用に作成された SQL ユーザーアカウントを入力します。
g) **[パスワード（Password）]** と **[パスワードの確認（Confirm Password）]** フィールドに SQL ユーザーアカウントのパスワードを入力します。
h) **[文字セット（Charset）]** ドロップダウンフィールドで、**ISO-8859-1**（ラテン 1 エンコーディング）を選択します。
i) **[権限（Permissions）]** ペインは、デフォルト値のままにしておきます。

ステップ 4 **[セカンダリ（Secondary）]** タブをクリックし、次の値を入力します。

a) **[フェールオーバーの有効化（Failover Enabled）]** をオンにします。
b) [データソースホスト（Datasource Host）] フィールドで、セカンダリ履歴データベースサーバー（**AW-HDS-B1**）のホスト名/IP アドレスを入力します。
c) **[ポート（Port）]** フィールドに、SQL サーバーデータベースに使用するポート番号 1433 を入力します。
d) **[データベース名（Database Name）]** フィールドでセカンダリ履歴データベース名を入力します。
e) **[インスタンス（Instance）]** フィールドは、SQL サーバーのオプションであるため、空白のままにします。
f) **[タイムゾーン（Timezone）]** フィールドで、データベースに格納するデータのタイムゾーンを選択します。
g) **[データベースユーザーID（Database User ID）]** フィールドに、Cisco Unified Intelligence Center またはデータベースへのアクセス用に作成された SQL ユーザーアカウントを入力します。

h) **[パスワード（Password）]** と **[パスワードの確認（Confirm Password）]** フィールドに SQL ユーザーアカウントのパスワードを入力します。

i) **[文字セット（Charset）]** ドロップダウンフィールドで、**ISO-8859-1**（ラテン 1 エンコーディング）を選択します。

j) **[権限（Permissions）]** ペインは、デフォルト値のままにしておきます。

ステップ 5 **[テスト接続（Test Connection）]** をクリックし、データソースがオンラインになっているか確認したら、**[保存（Save）]** をクリックします。

ステップ 6 **Unified CCE リアルタイム**データソースを選択します。**[編集（Edit）]** > **[データ ソース（Data Source）]** の順に選択し、**編集**ページを開きます。[プライマリ（Primary）]タブで、次の値を入力します。

a) [データソースホスト（Datasource Host）] フィールドに、プライマリ リアルタイム データベース サーバー（**AW-HDS-A2**）のホスト名/IP アドレスを入力します。

b) **[ポート（Port）]** フィールドに、SQL サーバーデータベースに使用するポート番号 1433 を入力します。

c) [データベース名（Database Name）] フィールドに、プライマリのリアルタイムデータベース名を入力します。

d) **[インスタンス（Instance）]** フィールドは、SQL サーバーのオプションであるため、空白のままにします。

e) **[タイムゾーン（Timezone）]** フィールドで、データベースに格納するデータのタイムゾーンを選択します。

f) **[データベースユーザーID（Database User ID）]** フィールドに、Cisco Unified Intelligence Center またはデータベースへのアクセス用に作成された SQL ユーザーアカウントを入力します。

g) **[パスワード（Password）]** と **[パスワードの確認（Confirm Password）]** フィールドに SQL ユーザーアカウントのパスワードを入力します。

h) **[文字セット（Charset）]** ドロップダウンフィールドで、**ISO-8859-1**（ラテン 1 エンコーディング）を選択します。

i) **[権限（Permissions）]** ペインは、デフォルト値のままにしておきます。

ステップ 7 **[セカンダリ（Secondary）]** タブをクリックし、次の値を入力します。

a) **[フェールオーバーの有効化（Failover Enabled）]** をオンにします。

b) [データソースホスト（Datasource Host）] フィールドに、セカンダリ リアルタイム データベース サーバー（**AW-HDS-B2**）のホスト名/IP アドレスを入力します。

c) **[ポート（Port）]** フィールドに、SQL サーバーデータベースに使用するポート番号 1433 を入力します。

d) [データベース名（Database Name）] フィールドに、セカンダリのリアルタイムデータベース名を入力します。

e) **[インスタンス（Instance）]** フィールドは、SQL サーバーのオプションであるため、空白のままにします。

f) **[タイムゾーン（Timezone）]** フィールドで、データベースに格納するデータのタイムゾーンを選択します。

g) **[データベースユーザーID（Database User ID）]** フィールドに、Cisco Unified Intelligence Center またはデータベースへのアクセス用に作成された SQL ユーザーアカウントを入力します。

h) **[パスワード（Password）]** と **[パスワードの確認（Confirm Password）]** フィールドに SQL ユーザーアカウントのパスワードを入力します。

i) **[文字セット（Charset）]** ドロップダウンフィールドで、**ISO-8859-1**（ラテン 1 エンコーディング）を選択します。

j) **[権限（Permissions）]** ペインは、デフォルト値のままにしておきます。

ステップ 8 **[テスト接続（Test Connection）]** をクリックし、データソースがオンラインになっているか確認したら、**[保存（Save）]** をクリックします。

次のタスク

Unified Intelligence Center の構成後、インポート機能を使用するとストックテンプレートをインポートし、要件に基づいてストックレポートをカスタマイズすることができます。ストックテンプレートは、Unified CCE /CC データを表示するように設計されています。『Cisco Unified Intelligence Center レポーティング アプリケーション ユーザーガイド』に移動します。**「レポート」**章の**「ストック レポート テンプレート」**項を参照して、Unified CCE レポートテンプレートをインポートします。

Unified Intelligence Center Administration の設定

Unified Intelligence Center Administration を設定するには、以下の手順を実行します。

手順

ステップ 1 **Cisco Unified Intelligence Center 管理コンソール**（`https://<ホスト名>:8443/oamp`）にログインします。

ステップ 2 **[クラスタ管理（Cluster Configuration）] > [レポーティング構成（Reporting Configuration）]** の順に選択し、[アクティブディレクトリ（Active Directory）] タブ を構成します。

a) プライマリ Active Directory サーバのホスト アドレスとして、ドメイン コントローラの IP アドレスを入力します。

b) [ポート（Port）] に、ドメイン コントローラ用のポート番号を入力します。

c) **[マネージャの識別名（Manager Distinguished Name）]** フィールドにお客様に必要な情報を入力します。

d) マネージャがドメイン コントローラにアクセスするときに使用するパスワードを入力し、確認します。

e) [ユーザ検索ベース] で、ユーザおよびドメイン名およびサブドメイン名 を指定します。

f) [ユーザ ID の属性] で、必要なオプションを選択します。

（注） Windowsドメイン名とNETBIOS名が異なる場合は、以下の手順を実行します。**[CiscoUnified Intelligence Center管理コンソール（CiscoUnified Intelligence Center Administration Console）]** の、**[アクティブディレクトリ設定（Active Directory Settings）]** にある **[ユーザーIDの属性（Attribute for User ID）]** フィールドで、*[sAMAccountName]* を選択し、*NETBIOS* 値をデフォルト値として設定します。

g) UserName ID に対して少なくとも 1 つのドメインを追加します。ドメイン名の前に @ 記号を入力しないでください。
h) ドメインをデフォルトとして設定します。
i) [テスト接続（Test Connection）] をクリックします。
j) [保存（Save）] をクリックします。

（注） 詳細については、オンライン ヘルプを参照してください。

ステップ 3 すべてのデバイスのための syslog を設定します。

a) **[デバイス管理（Device Management）] > [ログおよびトレースの設定（Log and Trace Settings）]** の順に選択します。
b) ホスト アドレスごとに、次を実行します。
   - 関連するサーバを選択し、矢印をクリックして展開します。
   - サーバ名を選択します。
   - **[有用性設定の編集（Edit Serviceability Settings）]** 画面の **[Syslogの設定（Syslog Settings）]** ペインで、プライマリホストとバックアップホストを設定します。[保存（Save）] をクリックします。

ステップ 4 使用する場合は、すべてのデバイスの SNMP を設定します。

a) **[ネットワーク管理（Network Management）] > [SNMP]** の順に選択します。
b) SNMP への移動、および各サーバに対して、次の内容を追加します。
   - V1/V2c コミュニティ文字列
   - 通知先

Unified Intelligence Center のライセンスおよびサインイン

管理コンソールにサインイン

管理コンソールにサインインできるユーザー：デフォルトのスーパーユーザーであるシステム アプリケーション ユーザー。

ライセンスをアップロードするには、Unified Intelligence Center 管理コンソールにサインインする必要があります。これは、Unified Intelligence Center 用の OAMP インターフェイスです。Administration アプリケーションに初めてサインインするユーザは、インストール中にシステ

ムアプリケーションユーザに対して定義されたユーザ ID とパスワードを使用してサインインする必要があります。このユーザは、Unified Intelligence Center Administration の初期スーパーユーザです。

手順

ステップ 1 `http://<HOST ADDRESS>/oamp` の URL を入力します。ここでは、HOST ADDRESS をコントローラノードの IP アドレスまたはホスト名で置き換えます。

ステップ 2 インストール時に定義したシステム アプリケーション ユーザ ID とパスワードを入力します。

'ライセンスのアップロード'

ライセンスをアップロードできるユーザー：デフォルトのスーパーユーザーであるシステム アプリケーション ユーザー。

システム アプリケーション ユーザーがサインインしたらすぐに、ユーザーはライセンスファイルをアップロードする必要があります。このファイルは、数分以内にコントローラ パブリッシャノードにアップロードされ、クラスタ内のすべてのノードに自動的に複製されます。

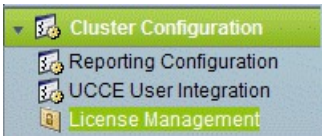
パートナーは一意のライセンスを取得して、カスタマー サイトのインポートされた Unified Intelligence Center サーバーに適用する必要があります。

手順

ステップ 1 Cisco Unified Intelligent Center Administration で、**[クラスタ管理（Cluster Configuration）]** > **[ライセンス管理（License Management）]** の順に選択します。

ライセンスファイル管理ページを開きます。

図 *5:* ライセンスファイル管理



ステップ 2 **[参照（Browse）]**をクリックします。

ステップ 3 *.lic ファイルを保存した場所に移動します。

ステップ 4 **[ライセンスの適用（Apply License）]** をクリックし、ライセンスをロードします。

ライセンスファイルが正常にアップロードされ、およそ 1 分後に、クラスタ内の（ある場合は）別のノードに配布されることを伝えるメッセージが表示されます。

（注） 1 分に 1 回、変更があるかどうかを確認するために、データベースに対するポーリングが実行されます。ライセンスの複製は即時ではありませんが、1 分以内に行われます。

次のタスク

レポートユーザーの作成 （65 ページ）

ライブデータ AW アクセスの構成

Live Data AW DB access コマンドを使用すると、Unified CCE ライブデータ製品展開選択に対して、Unified CCE AW DB（リアルタイムディストリビュータ）アクセスを構成および表示できます。接続テストを実行することもできます。

手順

ステップ 1 **Cisco Unified Intelligence Center ライブデータコンソール** にログインし、以下のコマンドを実行します。

set live-data aw-access primary *addr port db user pwd* [*test*]

set live-data aw-access secondary *addr port db user pwd* [*test*]

表 *8:* コマンドの説明

コマンド	説明	例
addr	プライマリまたはセカンダリ Unified CCE AW のホスト名または IP アドレスを指定します（最大 255 文字）。	10.10.10.10 または AWmachinename.domain.com
port	データベースサーバーのリスニングポートを指定します。範囲は、1 ～ 65535 です。	1433 db
db	データベース名を指定します（最大 128 文字）。	inst_awdb
user	ログインユーザーを指定します（最大 128 文字） ユーザー作成に関する詳細は、「SQL ユーザーアカウントの構成 （97 ページ）」を参照してください。	ユーザ
pwd	ログイン パスワードを指定します（最大 128 文字）。	password

コマンド	説明	例
テスト	このパラメータはオプションです。 プライマリまたはセカンダリ AW DB への接続をテストします。AW DB ユーザーが構成済みユーザーにあくせすできるかどうか、そしてその結果を確認します。	

ステップ 2 以下のコマンドを実行して、プライマリおよびセカンダリ Unified CCE AW DB アクセス情報を表示します。オプションで、ライブデータから各 AW DB への接続をテストし、各ノードの構成済みユーザーが、適切な AW DB アクセスを保持しているか確認します。

show live-data aw-access primary *addr port db user pwd* [*test*]

show live-data aw-access secondary *addr port db user pwd* [*test*]

ライブ データ マシン サービスの構成

手順

ステップ 1 **Cisco Unified Intelligence Center Live Data Console** にログインします。

ステップ 2 以下のコマンドを実行して、マシンサービステーブルのライブデータから最新情報を構成します。

```
set live-data machine-services awdb-user awdb-pwd
```

（注） このコマンドは、共存展開では有効ではありません。共存展開の場合は、Unified CCE 管理ツールのシステムインベントリを使用します。

表 *9:* コマンドの説明

コマンド	説明	例
awdb-user	書き込みアクセス権限を持つ AW データベース ドメイン ユーザーを指定します。	administrator@domain.com
awdb-pwd	AW データベースのユーザ パスワードを指定します。	password

ステップ 3 **マシンサービス**テーブルのライブデータエントリを表示するには、以下のコマンドを実行します。

```
show live-data machine-services awdb-user awdb-pwd
```

（注） FQDNホスト名を正しい形式で入力します。マシン（ホスト）名は、英数字文字列で始め、最大 32 文字まで使用できます。マシン名には、ピリオド（.）、下線（_）、ダッシュ（-）、英数字などの文字のみを使用できます。ホスト名に無効な文字が含まれている場合、または名前が 32 文字を超える場合は、エラーメッセージが表示されます。

ステップ 4 ライブデータサーバーのホスト名を更新した後、次のコマンドを再実行して、ライブデータマシンサービスを新しいホスト名で更新する必要があります。

```
set live-data machine-services awdb-user awdb-pwd

set live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd
```

Live Data Unified Intelligence データ ソースの構成

始める前に

- AW ディストリビュータおよび Cisco Unified Intelligence Center Publisher をサービスに含める必要があります。
- ライブデータ Cisco Unified Intelligence Center データソースを構成する同じノードで AW DB 接続情報が更新されていることを確認します。
- **マシンサービス** テーブルでライブデータエンドポイントを構成

手順

ステップ 1 以下のコマンドを実行して、Cisco Unified Intelligence Center のライブデータのデータ ソースを構成します。

```
set live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd
```

表 *10* : コマンドの説明

コマンド	説明	例
cuic-addr	Cisco Unified Intelligence Center Publisher ノードの完全修飾ドメイン名（FQDN）を指定します。	10.10.10.10 または CUIC + LiveDatamachinename.domain.com **重要** 指定されたノードは起動中です。
cuic-port	Cisco Unified Intelligence Center REST API ポートを指定します。通常、このポートは8444 です。	

コマンド	説明	例
cuic-user	Cisco Unified Intelligence Center での認証に使用するユーザ名を指定します。デフォルトでは、Cisco Unified Intelligence Center にはユーザー名を含むドメインとして **Cisco Unified Intelligence Center** が必要です。	`CUIC\administrator`
cuic-pwd	Cisco Unified Intelligence Center での認証に使用するパスワードを指定します。	password

ステップ 2 次のコマンドを実行して、データソースを表示します。

```
show live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd
```

ライブデータレポーティング間隔の構成

手順

ステップ 1 **Cisco Unified Intelligence Center Live Data Console** にログインします。

ステップ 2 次のコマンドを実行して、ライブデータレポーティング間隔を分形式で設定します。

```
set live-data reporting-interval reporting-interval-in-minutes
```

表 *11* : コマンドの説明

コマンド	説明	例
reporting-interval-in-minutes	レポーティング間隔を分単位で指定します。 有効値は5、10、15、30、および60 分です。	5

ステップ 3 ライブデータレポーティング間隔を設定したら、次のコマンドを実行して、パブリッシャノードとサブスクライバノードを再起動します（最初に非アクティブノードを再起動し、次にアクティブノードを再起動します）。

```
utils system restart
```

ステップ 4 ライブデータレポーティング間隔を表示するには、次のコマンドを実行します。

```
show live-data reporting-interval
```

Transport Layer Security の設定

TLS サーバーおよび TLS クライアントの最小バージョンを設定する手順に従います。

ライブデータ レポートのインポート

インポートするレポート定義で使用するデータソースが、Unified Intelligence Center で構成されていることを確認します。また、レポート定義に値リストが定義されている場合は、値リストで使用されているデータ ソースが Unified Intelligence Center で定義されていることを確認します。

以下の手順を実行し、既存の Unified Intelligence Center の在庫レポートとレポート定義をインポートします。

手順

ステップ 1 左側のナビゲーションウィンドウで、**[レポート（Reports）]** をクリックします。

ステップ 2 **[レポート（Reports）]** ツールバーで **[新規（New）] > [インポート（Import）]** の順に選択します。
Unified Intelligence Center レガシーインターフェイスにリダイレクトします。

ステップ 3 **[レポート（Reports）]** ドロワーをクリックします。

ステップ 4 ツールバーで、**[レポートをインポート（Import Report）]** をクリックします。

ステップ 5 **[ファイル名 (XML ファイル)（File Name (XML File)）]** フィールドで、**[参照（Browse）]** をクリックして XML ファイルを選択します。

ステップ 6 レポート XML zip ファイルを参照し、**[開く（Open）]** をクリックします。

ステップ 7 **[保存先（Save To）]** フィールドで、インポートしたレポート定義を保存するフォルダを参照します。

矢印キーを使用してフォルダを展開します。

ステップ 8 [インポート（Import）] をクリックします。

ステップ 9 ドロップダウンログインで、**[レポート定義のデータ ソース（Data Source for ReportDefinition）]** を選択します。

ステップ 10 ドロップダウンログインで、レポート定義で定義された **[値リストのデータ ソース（Data Source for ValueList）]** を選択します。

ステップ 11 オプションで、**[保存先（Save To）]** フィールドで、インポートしたレポート定義を保存するフォルダを参照します。

ステップ 12 [インポート（Import）] をクリックします。

HTTPS ガジェットの証明書の追加

セキュア HTTP （HTTPS）ガジェットに対する証明書を追加すると、Finesse デスクトップにガジェットをロードし、Finesse サーバーへの HTTPS 要求を正常に実行することができます。

このプロセスでは、Finesse ガジェットのコンテナとサードパーティガジェットのサイト間の HTTPS 通信を可能にし、ガジェットをロードして、ガジェットがサードパーティ製サーバーに対して行う API コールを実行できます。

（注） HTTPS を使用するガジェットは、そのガジェットが存在しているアプリケーションサーバーとガジェットの間の HTTP 通信も使用できます。すべてのトラフィックが安全である必要がある場合、ガジェットの開発者はアプリケーションサーバーへの API コールを発信するために HTTPS を使用する必要があります。

証明書には共通名で署名する必要があります。デスクトップレイアウトのガジェット URL に、（IP アドレスを使用するか、完全修飾ドメイン名を使用するかに関係なく）証明書に署名した名前と同じ名前を使用する必要があります。証明書の名前とガジェット URL の名前が一致しない場合、接続が信頼できず、ガジェットはロードされません。

始める前に

Finesse、Cisco Unified Intelligence Center およびライブデータサーバーからサーバーへの通信に対してセキュリティ証明書を設定します。次の表に示すように、証明書をサーバーにインポートします。

サーバ	証明書のインポート
Finesse	ライブデータおよび Cisco Unified Intelligence Center
Cisco Unified Intelligence Center	ライブデータ

手順

ステップ 1 サードパーティガジェットのホストから tomcat-trust.pem 証明書をダウンロードします。

a) サードパーティガジェット ホスト（`http://host or IP address/cmplatform`）で Cisco Unified Operating System Administration にサインインします。ここでは、`host` または `IP address` をホスト名またはサードパーティ ガジェット ホストのホスト名で置き換えます。
b) **[Security（セキュリティ）] > [Certificate Management（証明書管理）]** を選択します。
c) [検索（Find）] をクリックします。
d) 必要な Tomcat 信頼の **[共通名（Common Name）]** ハイパーリンクをクリックします。
e) **[Download.PEM ファイル（Download.PEM File）]** をクリックします。

ステップ 2 Finesse Publisher サーバーに証明書をアップロードします。

a) Finesse Publisher サーバーの Cisco Unified Operating System Administration（`http://host or IP address/cmplatform`）にサインインします。ここでは、`host` or `IP address` Finesse サーバーのホスト名または IP アドレスに置き換えます）。

b) **[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。
c) **[証明書のアップロード]**をクリックします。
d) **[証明書の用途（Certificate Purpose）]** ドロップダウンリストで **[Tomcat信頼（Tomcat Trust）]** 選択します。
e) 必要な Tomcat 信頼の **[共通名（Common Name）]** ハイパーリンクをクリックします。
f) **[参照（Browse）]** をクリックして、ダウンロードした tomcat-trust.pem ファイルを選択します。
g) [ファイルのアップロード（Upload File）] をクリックします。

ステップ 3 Finesse Publisher サーバーで、**Cisco Tomcat** と **Cisco Finesse Tomcat** を再起動します。

ステップ 4 Finesse Subscriber サーバーで証明書が同期されていることを確認します。

ステップ 5 Finesse Subscriber サーバーで、**Cisco Tomcat** および **Cisco Finesse Tomcat サービス**を再起動します。

Cisco Finesse の構成

次の表に、Cisco Finesse の構成手順を示します。

順序	タスク	完了したか
1	Cisco Finesse プライマリノードの構成 （110 ページ）	
2	-	
3	Cisco Finesse セカンダリノードの構成 （114 ページ）	
4	Windows 用 VMware ツールのインストール （394 ページ）	
5	Cisco Finesse 管理の構成 （115 ページ）	
6	SNMP の構成 （120 ページ）	

Cisco Finesse プライマリノードの構成

（注） まず Cisco Finesse プライマリノードを構成してから、セカンダリノードをカスタマイズする必要があります。

始める前に

ネットワークアダプタおよびフロッピードライブに対して、仮想マシンデバイスのステータスが、**[電源投入時に接続（Connect at Power On）]** になっていることを確認します。

手順

ステップ 1 プライマリ ノードの電源をオンにします。.flp ファイルの情報に基づいてインストールが始まります。
インストールが自動的に始まり、ユーザの操作なしで実行されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 2 VM の **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、Finesse プライマリマシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 3 VM を右クリックし、**[設定の編集（Edit settings）]** を選択し、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

（注） プライマリをカスタマイズすると、ユーザ名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

- OS 管理者のデフォルトパスワード：**c1sco@123**
- アプリケーションユーザー名：**Administrator**
- アプリケーションユーザーのデフォルトパスワード：**c1sco@123**
- Sftp パスワード：**c1sco@123**
- IPSec パスワード：**c1sco@123**

リブート後、VM のインストールが完了し、VM のスプレッドシートにすべてのパラメータが記載されます。

CTI サーバーおよび管理とデータサーバーの構成

- Cisco Finesse プライマリ ノードでの CTI サーバーの構成 （111 ページ）
- Unified Contact Center Enterprise 管理およびデータサーバーの構成 （113 ページ）
- Cisco Tomcat サービスの再起動 （114 ページ）

Cisco Finesse プライマリ ノードでの CTI サーバーの構成

手順

ステップ 1 以下の URL を実行します。 `http://<HOST ADDRESS>/cfadmin`。*Host Address* は、使用するプライマリ Cisco Finesse サーバのホスト名あるいは IP アドレスです。

ステップ 2 **ホーム > Contact Center Enterprise CTI サーバの設定**に移動します。

ステップ 3 **Contact Center Enterprise CTI サーバの設定**で、以下を更新します。

a) #unique_178 unique_178_Connect_42_table_974D78FE37B941D1B6D38A462FB80090 を参照にして、サイド A のホストまたは IP アドレスを入力します。

b) サイド A のポート（サイド A の CTI サーバ ポート）に、**42027**を入力します。

c) #unique_178 unique_178_Connect_42_table_974D78FE37B941D1B6D38A462FB80090 を参照して、（CallManager の PIM の) 周辺機器 ID を入力します。

d) #unique_178 unique_178_Connect_42_table_974D78FE37B941D1B6D38A462FB80090 を参照にして、サイド B のホストまたは IP アドレスを入力します。

e) サイド B ポート（サイド B の CTI サーバー ポート）に、**43027** を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

表 *12 : Cisco Finesse* の構成

	2000 エージェント	4000 エージェント	小規模のコンタクト センター	12,000 エージェント
A サイドのホストまたは IP アドレス	FINESSE1：CCE エージェント PG 1A	FINESSE1：CCE エージェント PG 1A FINESSE2：CCE エージェント PG 2A	FINESSEX：CCE エージェント PG XA。*X* は 補助顧客番号です。	FINESSE1：CCE エージェント PG 1A FINESSE2：CCE エージェント PG 2A FINESSE3: CCE エージェント PG 3A FINESSE4：CCE エージェント PG 4A FINESSE5：CCE エージェント PG 5A FINESSE6：CCE エージェント PG 6A
サイド A ポート	42027	42027	42027	42027

	2000 エージェント	4000 エージェント	小規模のコンタクト センター	12,000 エージェント
周辺機器 ID	5000	FINESSE1：5000 FINESSE2：5001	**PG Explorer** を確認して、補助顧客の周辺機器 ID を入力します。	FINESSE1：5000 FINESSE2：5001 FINESSE3：5002 FINESSE4：5003 FINESSE5：5004 FINESSE6：5005
B サイドのホストまたは IP アドレス	FINESSE1：CCE エージェント PG 1B	FINESSE1：エージェント PG 1B FINESSE2：エージェント PG 2B	FINESSEX：CCE エージェント PG XB。*X* は 補助顧客番号です。	FINESSE1：CCE エージェント PG 1B FINESSE2：CCE エージェント PG 2B FINESSE3：CCE エージェント PG 3B FINESSE4：CCE エージェント PG 4B FINESSE5：CCE エージェント PG 5B FINESSE6：CCE エージェント PG 6B
サイド B ポート	43027	43027	43027	43027

Unified Contact Center Enterprise 管理およびデータサーバーの構成

手順

ステップ 1 **ホーム** > **Contact Center Enterprise 管理サーバとデータ サーバの設定**を選択します。（このメニュー構造は、デフォルト設定を前提とします）。

ステップ 2 **Contact Center Enterprise 管理サーバとデータ サーバの設定**で、以下を更新します。

a) （サイド A の AW サーバの）プライマリ ホスト/IP アドレス

b) データベース ポート：1433
c) （サイド B の AW サーバの）バックアップ ホスト/IP アドレス
d) ドメイン（必須フィールド）：Finesse が接続する Unified CCE の名前。
e) AW データベース名：<ucceinstance_awdb>
f) ユーザ名：データベースへのサインインに必要なドメインユーザ名。SQL ユーザは指定できません。
g) パスワード：データベースへのサインインに必要なパスワード。

ステップ 3 [保存（Save）] をクリックします。

Cisco Tomcat サービスの再起動

Unified CCE 管理サーバー設定の任意の値を変更、保存したら、Cisco Finesse サーバー上の Cisco Tomcat Service を再起動します。

手順

ステップ 1 Cisco Tomcat サービスを停止するには、**utils service stop Cisco Tomcat** コマンドを入力します。
ステップ 2 Cisco Tomcat サービスを開始するには、**utils service start Cisco Tomcat** コマンドを入力します。

次のタスク

ゴールデン テンプレートの場合、セカンダリ ノードを設定します。

直接インストールの場合、レプリケーション ステータスを確認します。

Cisco Finesse セカンダリノードの構成

Finesse 管理コンソールを起動して Secondary Finesse を構成

セカンダリノードを追加するには、プライマリノードを起動し、クラスタにセカンダリノードを追加します。

手順

ステップ 1 ブラウザ（`http://Primary Node FQDN/cfadmin`）で Cisco Finesse プライマリノードを起動します。ここでは、自分のホストのプライマリノードまたは IP アドレスに置き換えます。
ステップ 2 **[設定（Settings）] > [クラスタ設定（Cluster Settings）]** の順に選択します。。（クラスタ設定は、デフォルト設定に基づいており、クラスタ設定ツールのページを変更していないことを前提としています）。
ステップ 3 Cisco Finesse セカンダリ ノードの IP アドレスを追加します。
ステップ 4 **[保存（Save）]**をクリックします。

ステップ 5 次のように Cisco Tomcat を再起動します。

a) Cisco Tomcat Service を停止するには、CLI コマンド **utils service stop Cisco Tomcat** を入力します。

b) Cisco Tomcat Service を開始するには、CLI コマンド **utils service start Cisco Tomcat** を入力します。

セカンダリノードに Cisco Finesse をインストール

始める前に

ネットワークアダプタおよびフロッピードライブの仮想マシンの **[電源投入時に接続（Connect at Power On）]** チェックボックスをオンにします。

手順

ステップ 1 セカンダリノードの電源をオンにして、.flp ファイルの情報に基づいてインストールを開始します。
インストールが自動的に始まり、ユーザの操作なしで実行されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 2 仮想マシンの **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、Cisco Finesse セカンダリマシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 3 仮想マシンを右クリックし、**[設定の編集（Edit settings）]** を選択したら、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

（注） セカンダリノードをカスタマイズすると、ユーザー名とパスワードが次のように変更されます。パスワードは変更可能です。

- OS 管理者のデフォルトパスワード：**c1sco@123**
- アプリケーションユーザー名：**Administrator**
- アプリケーションユーザーのデフォルトパスワード：**c1sco@123**
- Sftp パスワード：**c1sco@123**
- IPSec パスワード：**c1sco@123**

Cisco Finesse 管理の構成

- CA 証明書の取得およびアップロード （116 ページ）
- Cisco Finesse 用 自己署名証明書の信頼 （117 ページ）
- Internet Explorer のブラウザ設定 （119 ページ）

CA 証明書の取得およびアップロード

（注） この手順は、HTTPS を使用している場合にのみ適用されます。

この手順は任意です。HTTPS を使用している場合、CA 証明書を取得してアップロードするか、Cisco Finesse で提供される自己署名証明書を使用するかを選択できます。

ログイン毎にブラウザにセキュリティ警告が表示されないようにするには、認証局（CA）によって署名されたアプリケーション証明書およびルート証明書を取得します。Cisco Unified オペレーティング システムの管理から証明書管理ユーティリティを使用します。

Cisco Unified オペレーティング システムの管理を開くには、以下の URL をブラウザに入力します。`https://FQDN of primary Finesse server:8443/cmplatform`。

Cisco Finesse のインストール時に作成されたアプリケーション ユーザ アカウントのユーザ名とパスワードを使用してログインします。

手順

ステップ 1 以下の通り CSR を生成します。

a) **セキュリティ > 証明書管理 > CSRの生成**を選択します。
b) [証明書名] ドロップダウンリストで、**tomcat**を選択します。
c) [CSR の生成（Generate CSR）] をクリックします。

ステップ 2 CSR をダウンロードします。

a) **[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [CSRのダウンロード（Download CSR）]** の順に選択します。
b) [証明書名] ドロップダウンリストで、**tomcat**を選択します。
c) [CSR のダウンロード（Download CSR）] をクリックします。

ステップ 3 CSR を使用して、認証局から署名付きのアプリケーション証明書と CA ルート証明書を取得します。

ステップ 4 証明書を受け取ったら、**セキュリティ > 証明書管理 > 証明書のアップロード**を選択します。

ステップ 5 ルート証明書をアップロードします。

a) **証明書名** ドロップダウンリストで、**tomcat-trust** を選択します。
b) **ファイルのアップロード** フィールドで、**参照** をクリックして、ルート証明書ファイルをアップロードします。
c) [ファイルのアップロード（Upload File）] をクリックします。

ステップ 6 アプリケーション証明書をアップロードします。

a) **証明書名** ドロップダウンリストで、**tomcat** を選択します。
b) **ルート証明書** フィールドで、CA ルート証明書名を入力します。
c) **ファイルのアップロード** フィールドで、**参照** をクリックして、ルート証明書ファイルをアップロードします。

d) [ファイルのアップロード（Upload File）] をクリックします。

ステップ 7 アップロードが完了したら、Cisco Finesse からログオフします。

ステップ 8 プライマリ Cisco Finesse サーバで CLI にアクセスします。

ステップ 9 **utils service restart Cisco Finesse Notification Service** コマンドを入力して、Cisco Finesse Notification サービスを再起動します。

ステップ 10 **utils service restart Cisco Tomcat** コマンドを入力して、Cisco Tomcat サービスを再起動します。

ステップ 11 セカンダリ Cisco Finesse サーバにルート証明書およびアプリケーション証明書をアップロードします。

（注） セカンダリサーバーの **Cisco Unified オペレーティングシステム管理** を開くには、以下の URL をブラウザに入力します。`https://FQDN of secondary Finesse server:8433/cmplatform`

ステップ 12 セカンダリ Cisco Finesse サーバの CLI にアクセスし、Cisco Finesse Notification サービスと Cisco Tomcat サービスを再起動します。

Cisco Finesse 用 自己署名証明書の信頼

構成設定を定義したら、サービスを再起動します。権限を持つエージェントは、Cisco Finess エージェントデスクトップにログインすることができます。

Cisco Finesse を再起動すると、すべてのサーバ関連のサービスの再起動に約 6 分かかります。そのため、6 分待ってからエージェントデスクトップへのログインを試みてください。

手順

ステップ 1 ブラウザに `https://FQDN of Finesse server:8443/cmplatform` の URL を入力します。

ステップ 2 HTTPS を使用してエージェントデスクトップに最初にアクセスする際、Cisco Finesse に付属の自己署名証明書を信頼するように促されます。サポートされる各ブラウザでの手順を下記の表で説明します。

（注） HTTP を使用している場合、または CA 証明書をインストールしている場合は、自己署名付き証明書を信頼するように求められることはありません。エージェント ID、パスワード、および内線番号を入力して **[サインイン（Sign In）]** をクリックします。

ブラウザ	説明
Internet Explorer	**1.** Web サイトのセキュリティ証明書に問題があることを示すページが表示されます。**このサイトの閲覧を続行する（推奨されません）** をクリックします。このアクションでは、Agent Desktop のサインインページが開きます。 証明書エラーはブラウザのアドレスバーに表示されます。

ブラウザ	説明
	2. [証明書エラー（Certificate Error）] をクリックし、[証明書の表示（View Certificates）] をクリックすると、[証明書（Certificate）] ダイアログボックスが開きます。 **3.** [証明書] ダイアログボックスで、**証明書のインストール**をクリックして [証明書インポートウィザード] を開きます。 **4.** [次へ（Next）] をクリックします。 **5.** [すべての証明書を次のストアに配置（Place all certificates in the following store）] を選択し、[参照（Browse）] をクリックします。 **6.** [信頼されたルート証明書機関（Trusted Root Certification Authorities）] を選択し、[OK] をクリックします。 **7.** [次へ（Next）] をクリックします。 **8.** [完了（Finish）] をクリックします。 **9.** 証明書をインストールするかどうかを尋ねる [セキュリティ警告] ダイアログ ボックスが表示されたら、**はい**をクリックします。 インストール後、正常にインストールされたというメッセージが表示されます。 **10.** [OK] をクリックします。 **11.** エージェント ID、パスワード、および内線番号を入力して **ログイン** をクリックします。
Mozilla Firefox	**1.** この接続が信頼できないことを示すページが表示されます。 **2. [リスクを理解します（I Understand the Risks）]** をクリックし、**[例外の追加]（Add Exception）]** をクリックします。 **3. セキュリティ例外の追加** ダイアログ ボックスで、**例外を恒久的に保存する** チェックボックスがオンになっていることを確認します。 **4.** [セキュリティ例外の確認（Confirm Security Exception）] をクリックします。 この接続が信頼できないことを示すページが自動的に閉じられ、エージェントデスクトップが開きます。 **5.** エージェント ID、パスワード、および内線番号を入力して**ログイン**をクリックします。

Internet Explorer のブラウザ設定

次のプライバシーと詳細設定を設定します。

始める前に

Internet Explorer を使用して Cisco Finesse デスクトップにアクセスする場合、Cisco Finesse のすべての機能が正しく動作するためにブラウザで以下の設定を行う必要があります。

- ポップアップ ブロッカを無効にします。
- デスクトップが互換性表示で実行されていないことを確認します。Cisco Finesse では、互換性表示はサポートされていません。

手順

ステップ 1 ブラウザのメニュー バーで、**ツール** > **インターネット オプション**を選択します。
ステップ 2 **プライバシー** タブをクリックして、**サイト**をクリックします。
ステップ 3 **アドレス** フィールドで、Cisco Finesse サーバのサイド A のドメイン名を入力します。
ステップ 4 [許可（Allowed）] をクリックします。
ステップ 5 **アドレス** フィールドで、Cisco Finesse サーバのサイド B のドメイン名を入力します。
ステップ 6 **許可** をクリックして **OK**をクリックします。
ステップ 7 インターネット オプションのダイアログ ボックスの **詳細設定** タブをクリックします。
ステップ 8 **セキュリティ** ペインで、 **証明書アドレスの不一致について警告する** チェックボックスをオフにします。
ステップ 9 [OK] をクリックします。

次のタスク

ユーザがサインインできるようにするには、次のセキュリティ設定を有効にします。

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked as safe for scripting
- Active scripting

設定を有効にするには、以下の手順を実行します。

1. ブラウザのメニュー バーで、**ツール** > **インターネット オプション**を選択します。
2. **セキュリティ** タブを選択し、**カスタム レベル**をクリックします。
3. **ActiveX コントロールおよびプラグイン**で、**ActiveX コントロールとプラグインを実行する**および**スクリプトを実行しても安全とマークされた ActiveX コントロールのスクリプト**を有効にします。
4. **スクリプト** で **アクティブ スクリプト**を有効にします。

SNMP の構成

手順

ステップ 1 管理者のログイン情報を使用して、Cisco Unified Serviceability（*https://hostname of primary server/ccmservice*）にログインします。

ステップ 2 **[SNMP]** > **[V1/V2c]** > **[コミュニティ文字列（Community String）]** の順に選択します。

ステップ 3 **サーバ** ドロップダウンリストで、コミュニティ文字列を設定するサーバを選択して、**検索**をクリックします。

ステップ 4 **新規追加** をクリックして、新しいコミュニティ文字列を追加します。

a) **コミュニティ文字列**を入力します。

例：

public を使用してデバイスへのアクセスを試みます。

b) **ホスト IP アドレス情報** フィールドで、**任意のホストからの SNMP パケットを受け入れる** を選択します。

c) **アクセス権限** ドロップダウンリストで、**ReadWriteNotify** オプションを選択します。

d) **すべてのノードに適用** チェックボックスをオンにして、クラスタのすべてのノードにコミュニティ文字列を適用します。

情報メッセージが表示されます。

e) [OK] をクリックします。

f) [保存（Save）] をクリックします。

SNMP プライマリエージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP プライマリエージェントを再起動せずに構成を続行するには、**[キャンセル（Cancel）]** をクリックします。SNMP プライマリ エージェント サービスを再起動するには、**[OK]** をクリックします。

g) [OK] をクリックします。

ステップ 5 **[SNMP]** > **[V1/V2c]** > **[通知先（Notification Destination）]** の順に選択します。

ステップ 6 **サーバ** ドロップダウンリストで、通知先を設定するサーバを選択して、**検索**をクリックします。

ステップ 7 新しい SNMP 通知先を追加するには、**[新規追加（Add New）]** ボタンをクリックします。

a) **[ホスト IP アドレス]** ドロップダウンリストで、**[新規追加（Add New）]** を選択します。

b) **ホスト IP アドレス** フィールドに、Prime Collaboration サーバの IP アドレスを入力します。

c) **ポート番号** フィールドで、通知を受信するポート番号を入力します。

（注） デフォルトのポート番号は、162 です。

d) **SNMP バージョン情報** フィールドで、SNMP バージョン、V2C を選択します。

e) **通知タイプ情報** フィールドで、**通知タイプ** ドロップダウンリストから **トラップ**を選択します。

f) **[コミュニティ文字列情報（Community String Information）]** フィールドの **[コミュニティ文字列（Community String）]** ドロップダウンリストで、ステップ 4 で作成したコミュニティ文字列を選択します。

g) **すべてのノードに適用** チェックボックスをオンにして、すべてのノードにコミュニティ文字列を適用します。

情報メッセージが表示されます。

h) [OK] をクリックします。

i) [挿入（Insert）] をクリックします。

SNMP プライマリエージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP プライマリエージェントを再起動せずに構成を続行するには、**[キャンセル（Cancel）]** をクリックします。SNMP プライマリ エージェント サービスを再起動するには、**[OK]** をクリックします。

j) [OK] をクリックします。

4000 エージェント導入モデル用カスタマーインスタンスの作成

Cisco HCS for CC 用 4000 エージェントを展開するカスタマーインスタンスを作成するには、以下の一連のタスクに従います。各タスクの後で、このページに戻ってそのタスクを「「完了」」としてマークしたら、次の手順に進みます。

表 *13 : Contact Center* 用 *Cisco HCS for CC* に対する *4000* エージェント展開に対してカスタマーインスタンスを作成

順序	タスク	完了したか
1	VMware ツールのアップグレード （26 ページ）	
2	仮想マシンの起動とシャットダウンの設定 （26 ページ）	
3	ドメイン コントローラ サーバーの作成 （27 ページ）	
4	Cisco Unified CCE Rogger の構成 （122 ページ）	
5	Unified CCE AW-HDS-DDS の構成 （41 ページ）	
6	Unified CCE PG の構成 （47 ページ）	
7	Unified CVP の構成 （60 ページ）	
8	Cisco IOS Enterprise 音声ゲートウェイの構成 （81 ページ）	
9	Unified Communications Manager の構成 （87 ページ）	
10	Unified Intelligence Center の構成 （123 ページ）	

順序	タスク	完了したか
11	ライブ データ レポーティング システムの構成 （134 ページ）	
12	Cisco Finesse の構成 （110 ページ）	
13	Cisco Identity Service の構成 （124 ページ）	

Cisco Unified CCE Rogger の構成

このテーブルでは、Cisco Unified CCE Rogger を構成する際に実行すべき手順を説明します。

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ドメイン内マシンの検証 （33 ページ）	
3	ドメインマネージャの構成 （34 ページ）	
4	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	
5	CCE コンポーネント用 SQL Server の設定 （36 ページ）	
6	セカンダリドライブの構成 （36 ページ）	
7	Unified CCE Logger の構成 （37 ページ）	
8	Unified CCE ルーターの構成 （39 ページ）	
9	基本構成のロード （122 ページ）	
10	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
11	Cisco SNMP の設定 （56 ページ）	

基本構成のロード

基本構成パラメータをインポートするには、以下の手順を実行します。基本構成パラメータの詳細については、「4000 エージェント展開の基本構成パラメータ （558 ページ） 」を参照してください。

手順

ステップ 1 タイムゾーンに基づいて、HCS-CC_11.6.1-Day1_4000.zip または ファイルをダウンロードします。このファイルをローカルに保存して、解凍します。

ステップ 2 Domain_Update_Tool.zip ファイルをダウンロードします。このファイルをローカルに保存して、解凍します。

ステップ 3 構成フォルダをサイド A にある Unified CCE Rogger のローカルドライブにコピーします。

ステップ 4 サイド A の Unified CCE Rogger で ICMDBAZ ツールを開きます。

ステップ 5 Unified CCE Rogger を選択し、<instance name>_sideA にツリーを展開します。

ステップ 6 メニューバーの [データ（Data）] を選択し、**[インポート（Import）]** をクリックします。

ステップ 7 構成フォルダを参照して特定し、**[開く（Open）]** をクリックします。

ステップ 8 **[OK]** > **[インポート（Import）]** の順に選択します。

ステップ 9 [スタート（Start）] をクリックし、すべてのメッセージに対して **[OK]** をクリックします。

ステップ 10 Domain_Update_Tool フォルダに移動し、[UpdateDomain.PS1.] を右クリックしたら、 PowerShell で実行します。次のように入力します。

a) サーバー名として、サイド A の Unified CCE Rogger のコンピュータ名を入力します。
b) [データベース名（Database name）] に、<instance_sideA (Logger database)> と入力します。
c) ドメイン名として、カスタマーのドメイン名を入力します。

ステップ 11 ICMDBA ツールに戻ります。同期するサイドの Logger <instance name> を選択します。

ステップ 12 メニューバーの **[データ（Data）]** をクリックし、**[同期（Synchronize）]** を選択して、以下の手順を実行します。

a) **[同期（Synchronize）]** ウィンドウの **[ソール（Source）]** ペインで **[追加（Add）]** をクリックします。
b) **[サーバー名（Server Name）]** フィールドに送信元の Unified CCEE Rogger のホスト名を入力し、**[OK]** をクリックします。
c) **[接続先（Destination）]** ペインで **[追加（Add）]** をクリックします。
d) **[サーバー名（Server Name）]** フィールドに接続先の Unified CCE Rogger のホスト名を入力し、**[OK]** をクリックします。
e) **[同期（Synchronize）]** をクリックします。

ステップ 13 [スタート（Start）] をクリックします。同期後、**[OK]** をクリックします。

Unified Intelligence Center の構成

Unified Intelligence Center を構成するには、以下のタスクを実行します。

順序	タスク	完了したか
1	Unified Intelligence Center Publisher の構成 （94 ページ）	

順序	タスク	完了したか
2	Unified Intelligence Center Subscriber の構成 （94 ページ）	
3	Windows 用 VMware ツールのインストール （394 ページ）	
4	Unified Intelligence Center レポーティングの構成 （97 ページ）	
5	Unified Intelligence Center Administration の設定 （101 ページ）	
6	SNMP の構成 （120 ページ）	

ライブ データ レポーティング システムの構成

順序	タスク	完了したか
1	ライブデータ AW アクセスの構成 （104 ページ）	
2	ライブデータ マシン サービスの構成 （105 ページ）	
3	Live Data Unified Intelligence データソースの構成 （106 ページ）	
4	ライブデータ レポーティング間隔の構成 （107 ページ）	
5	Transport Layer Security の設定 （108 ページ）	
6	ライブデータ レポートのインポート （108 ページ）	
7	HTTPS ガジェットの証明書の追加 （108 ページ）	

Cisco Identity Service の構成

順序	タスク	完了したか
1	Ids Publisher の構成 （125 ページ）	
2	IDS サブスクライバ ノードの設定 （125 ページ）	

順序	タスク	完了したか
3	Ids Subscriber の構成 （126 ページ）	

Ids Publisher の構成

Subscriber をカスタマイズする前に、Cisco Identity Service Publisher をカスタマイズしておく必要があります。

始める前に

ネットワークアダプタおよびフロッピードライブに対して、仮想マシンデバイスのステータスが、**[電源投入時に接続（Connect at Power On）]** になっていることを確認します。

手順

ステップ 1 パブリッシャの電源を入れます。これにより、.flp ファイルの情報に基づいてインストールが始まります。インストールは通知なしで自動で実行開始されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 2 VM の **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、Publisher マシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 3 VM を右クリックし、**[設定の編集（Edit settings）]** を選択し、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

IDS サブスクライバ ノードの設定

パブリッシャーのノードに、サブスクライバーノードのアドレスを提供する必要があります。これは、**set id サブスクライバー**コマンドを使用して行います。

手順

ステップ 1 パブリッシャー Id ノードにログインします。

ステップ 2 次のコマンドを実行してサブスクライバ ノードを設定します：

set ids subscriber *name*
name

Id サブスクライバーノード アドレスのホスト名または ip アドレスを指定します。

次のタスク

これらのCisco IdS CLI コマンドは、Id スタンドアロン展開でのみ使用できます。パブリッシャノードでこれらのコマンドを実行します。

必要な最低限の権限レベル: 通常

このコマンドを使用して、[サブスクライバーノード (Id)] ノードの情報を表示します。

show ids subscriber

必須のパラメータはありません。

必須最小権限レベル： 高度

このコマンドを使用して、IdS subscriber ノード構成を解除します。

unset ids subscriber

必須のパラメータはありません。

Ids Subscriber の構成

始める前に

ネットワークアダプタおよびフロッピードライブに対して、仮想マシンデバイスのステータスが、**[電源投入時に接続（Connect at Power On）]** になっていることを確認します。

手順

ステップ 1 Subscriber の電源をオンにします。
.flp ファイルの情報に基づいてインストールが始まります。インストールが自動的に始まり、ユーザの操作なしで実行されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 2 VM の **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、Cisco Unified Communications Manager セカンダリマシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 3 VM を右クリックし、**[設定の編集（Edit settings）]** を選択し、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

12000エージェント導入モデルのカスタマーインスタンスの作成

Cisco HCS for CC 用 4000 エージェントを展開するカスタマーインスタンスを作成するには、以下の一連のタスクに従います。各タスクの後で、このページに戻ってそのタスクを「完了」としてマークしたら、次の手順に進みます。

表 *14 : Cisco HCS for CC* 用 *12000* エージェント展開に対するカスタマーインスタンスの作成

順序	タスク	完了したか
1	VMware ツールのアップグレード （26 ページ）	
2	仮想マシンの起動とシャットダウンの設定 （26 ページ）	
3	ドメイン コントローラ サーバーの作成 （27 ページ）	
4	Unified CCE Logger の構成 （127 ページ）	
5	Unified CCE ルーターの構成 （129 ページ）	
6	Unified CCE AW-HDS の構成 （129 ページ）	
7	Unified CCE HDS-DDS の構成 （131 ページ）	
8	Unified CCE PG の構成 （47 ページ）	
9	Unified CVP の構成 （60 ページ）	
10	Cisco IOS Enterprise 音声ゲートウェイの構成 （81 ページ）	
11	Unified Communications Manager の構成 （87 ページ）	
12	Unified Intelligence Center の構成 （123 ページ）	
13	ライブ データ レポーティング システムの構成 （134 ページ）	
14	Cisco Finesse の構成 （110 ページ）	
15	シングルサインオン管理 （313 ページ）	
16	Cisco Identity Service の構成 （124 ページ）	

Unified CCE Logger の構成

このセクションでは、Unified CCE Logger に対して実行する構成手順んを説明します。

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ドメイン内マシンの検証 （33 ページ）	
3	ドメインマネージャの構成 （34 ページ）	
4	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	

順序	タスク	完了したか
5	CCE コンポーネント用 SQL Server の設定 （36 ページ）	
6	セカンダリ ドライブの構成 （36 ページ）	
7	Unified CCE Logger の構成 （37 ページ）	
8	基本構成のロード （128 ページ）	
9	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
10	Cisco SNMP の設定 （56 ページ）	

基本構成のロード

基本構成パラメータをインポートするには、以下の手順を実行します。基本構成パラメータの詳細については、「12000 エージェント展開の基本構成パラメータ （565 ページ）」を参照してください。

手順

ステップ 1 タイムゾーンに基づいて、HCS-CC_11.6.1-Day1_12000.zip またはファイルをダウンロードします。このファイルをローカルに保存して、解凍します。

ステップ 2 Domain_Update_Tool.zip ファイルをダウンロードします。このファイルをローカルに保存して、解凍します。

ステップ 3 サイド A の Unified CCE Logger のローカルドライブに構成フォルダをコピーします。

ステップ 4 サイド A の Unified CCE Logger で ICMDBA ツールを開きます。

ステップ 5 Unified CCE Logger を選択し、<instance name>_sideA のツリーを展開します。

ステップ 6 メニューバーの [データ（Data）] を選択し、**[インポート（Import）]** をクリックします。

ステップ 7 構成フォルダを参照して特定し、**[開く（Open）]** をクリックします。

ステップ 8 **[OK]** > **[インポート（Import）]** の順に選択します。

ステップ 9 [スタート（Start）] をクリックし、すべてのメッセージに対して **[OK]** をクリックします。

ステップ 10 Domain_Update_Tool フォルダに移動し、[UpdateDomain.PS1.] を右クリックしたら、 PowerShell で実行します。次のように入力します。

a) サーバー名については、Unified CCE Logger サイド A のコンピュータ名を入力します。

b) [データベース名（Database name）] に、<instance_sideA (Logger database)> と入力します。

c) ドメイン名として、カスタマーのドメイン名を入力します。

ステップ 11 ICMDBA ツールに戻ります。同期するサイドの Logger <instance name> を選択します。

ステップ 12 メニューバーの **[データ（Data）]** をクリックし、**[同期（Synchronize）]** を選択して、以下の手順を実行します。

a) **[同期（Synchronize）]** ウィンドウの **[ソール（Source）]** ペインで **[追加（Add）]** をクリックします。
b) **[サーバー名（Server Name]** フィールドに送信元の Unified CCE Logger のホスト名を入力し、**[OK]** をクリックします。
c) **[接続先（Destination）]** ペインで **[追加（Add）]** をクリックします。
d) **[サーバー名（Server Name）]** フィールドに接続先の Unified CCE Logger のホスト名を入力し、**[OK]** をクリックします。
e) **[同期（Synchronize）]** をクリックします。

ステップ 13 **[スタート（Start）]** をクリックし、すべてのメッセージに対して **[OK]** をクリックします。

Unified CCE ルーターの構成

このセクションでは、Unified CCE ルーターに対して実行する構成手順を説明します。

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ネットワーク カードの検証 （61 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	
4	Unified CCE ルーターの構成 （39 ページ）	
5	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
6	Cisco SNMP の設定 （56 ページ）	

Unified CCE AW-HDS の構成

このセクションでは、サイド A および B で Unified CCE AW-HDS に対して実行する構成手順について説明します。

表 *15*：サイド *A* および サイド *B* で *Unified CCE AW-HDS* を構成

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ドメイン内マシンの検証 （33 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	
4	CCE コンポーネント用 SQL Server の設定 （36 ページ）	

順序	タスク	完了したか
5	セカンダリドライブの構成 （36 ページ）	
6	AW-HDS （130 ページ）	
7	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
8	Cisco SNMP の設定 （56 ページ）	
9	HCS for CC 展開タイプの設定 （46 ページ）	

AW-HDS

- インスタンスの作成 （42 ページ）
- HDS データベースの作成 （43 ページ）
- AW-HDS の構成 （130 ページ）
- データベースとログファイルのサイズ （45 ページ）

AW-HDS の構成

Unified CCE 管理サーバーおよびリアルタイム、履歴データサーバー（AW-HDS）をインストールするには、以下の手順を実行します。

手順

ステップ 1 **コンポーネント管理** > **管理サーバとデータ サーバ**を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 **[展開（Deployment）]** ウィンドウで、現在のインスタンスを選択します。

ステップ 4 **管理サーバとデータ サーバの追加** ウィンドウで、以下の通り設定します。

a) **エンタープライズ**をクリックします。
b) 展開サイズは **大** をクリックします。
c) [次へ（Next）] をクリックします。

ステップ 5 **大規模導入でのサーバの役割** ウィンドウで、以下の通り設定します。

a) **管理サーバ、リアルタイムおよび履歴データ サーバ（AW-HDS）** のオプションを選択します。
b) [次へ（Next）] をクリックします。

ステップ 6 **管理サーバとデータ サーバの接続** ウィンドウで、以下の通り設定します。

a) **管理サーバとデータ サーバ**を選択します。
b) **セカンダリ管理サーバとデータ サーバ** フィールドに、セカンダリ AW-HDS のホスト名を入力します。
c) **プライマリおよびセカンダリ ペア（サイト）名** フィールドで、サイト名を入力します。

（注） サイト名が、**PG Explorer** > **エージェントの周辺機器** > **エージェントの配置**で定義されているサイト名と一致していることを確認してください。

d) [次へ（Next）] をクリックします。

ステップ 7 **[データベースとオプション（Database and Options）]** ウィンドウで、以下の通り構成します。

a) **ドライブ上のデータベースの作成** フィールドで、セカンダリ ドライブ（通常は **D** または **E**）を選択します。

b) **構成管理サービス（CMS）ノード** をオンにします。

c) **Internet Script Editor（ISE）サーバ**をオンにします。

d) [次へ（Next）] をクリックします。

ステップ 8 **セントラルコントローラの接続**ページで、以下の通り設定します。

a) ルータのサイド A の場合、ルータ A が存在するホスト名または IP アドレス マシンを入力します。

b) ルータのサイド B の場合、ルータ B が存在するホスト名または IP アドレス マシンを入力します。

c) Logger サイド A の場合は、Logger A が存在するホスト名または IP アドレス マシンを入力します。

d) Logger サイド B の場合は、Logger B が存在するホスト名または IP アドレス マシンを入力します。

e) **セントラル コントローラのドメイン名**を入力します。

f) **セントラル コントローラの優先サイド A**をクリックします。

g) **次へ** をクリックします。

ステップ 9 **サマリー** ウィンドウで確認して、**終了**をクリックします。

（注） すべての Unified CCE のインストールが完了するまで、サービスを起動しないでください。

Unified CCE HDS-DDS の構成

ここでは、サイド A およびサイド B の Unified CCE HDS-DDS に対して実行する構成手順について説明します。

表 *16*：サイド *A* およびサイド *B* の *Unified CCE HDS-DDS* の構成

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ネットワーク カードの検証 （61 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	
4	CCE コンポーネント用 SQL Server の設定 （36 ページ）	

順序	タスク	完了したか
5	セカンダリドライブの構成 （36 ページ）	
6	HDS-DDS （132 ページ）	
7	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
8	Cisco SNMP の設定 （56 ページ）	

HDS-DDS

- インスタンスの作成 （42 ページ）
- HDS データベースの作成 （43 ページ）
- HDS-DDS の構成 （132 ページ）
- データベースとログファイルのサイズ （45 ページ）

HDS-DDS の構成

以下の手順に従って、Cisco Unified CCE 管理サーバー、リアルタイム、履歴データサーバー（AW-HDS）をインストールします。

手順

ステップ 1 **コンポーネント管理** > **管理サーバとデータ サーバ**を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 **[展開（Deployment）]** ウィンドウで、現在のインスタンスを選択します。

ステップ 4 **管理サーバとデータ サーバの追加** ウィンドウで、以下の通り設定します。

a) **エンタープライズ**をクリックします。
b) 展開サイズは **大** をクリックします。
c) [次へ（Next）] をクリックします。

ステップ 5 **大規模導入でのサーバの役割** ウィンドウで、以下の通り設定します。

a) **履歴データ サーバと詳細データサーバ（HDS-DDS）**オプションを選択します。
b) [次へ（Next）] をクリックします。

ステップ 6 **管理サーバとデータ サーバの接続** ウィンドウで、以下の通り設定します。

a) **管理サーバとデータ サーバ**を選択します。
b) **セカンダリ管理サーバとデータ サーバ**フィールドに、セカンダリ HDS-DDS のホスト名を入力します。
c) **プライマリおよびセカンダリ ペア（サイト）名** フィールドで、サイト名を入力します。

（注） サイト名が、**PG Explorer** > **エージェントの周辺機器** > **エージェントの配置**で定義されているサイト名と一致していることを確認してください。

d) [次へ（Next）] をクリックします。

ステップ 7 **データベースとオプション** ウィンドウで、**データベースを作成** する **ドライブ** フィールドで、セカンダリ ドライブを選択します（通常は **D** または **E**）。

ステップ 8 **セントラルコントローラの接続**ページで、以下の通り設定します。

a) ルータのサイド A の場合、ルータ A が存在するホスト名または IP アドレス マシンを入力します。

b) ルータのサイド B の場合、ルータ B が存在するホスト名または IP アドレス マシンを入力します。

c) Logger サイド A の場合は、Logger A が存在するホスト名または IP アドレス マシンを入力します。

d) Logger サイド B の場合は、Logger B が存在するホスト名または IP アドレス マシンを入力します。

e) **セントラル コントローラのドメイン名**を入力します。

f) **セントラル コントローラの優先サイド A**をクリックします。

g) **次へ** をクリックします。

ステップ 9 **サマリー** ウィンドウで確認して、**終了**をクリックします。

（注） すべての Unified CCE コンポーネントがインストールされるまで起動しないでください。

Unified Intelligence Center の構成

Unified Intelligence Center を構成するには、以下のタスクを実行します。

順序	タスク	完了したか
1	Unified Intelligence Center Publisher の構成 （94 ページ）	
2	Unified Intelligence Center Subscriber の構成 （94 ページ）	
3	Windows 用 VMware ツールのインストール （394 ページ）	
4	Unified Intelligence Center レポーティングの構成 （97 ページ）	
5	Unified Intelligence Center Administration の設定 （101 ページ）	
6	SNMP の構成 （120 ページ）	

ライブ データ レポーティング システムの構成

順序	タスク	完了したか
1	ライブデータ AW アクセスの構成 （104 ページ）	
2	ライブデータ マシン サービスの構成 （105 ページ）	
3	Live Data Unified Intelligence データ ソースの構成 （106 ページ）	
4	ライブデータ レポーティング間隔の構成 （107 ページ）	
6	HTTPS ガジェットの証明書の追加 （108 ページ）	

SmallContactCenterエージェント導入モデルのカスタマーインスタンスの作成

Contact Center 用 に Cisco HCS for CC に対して小規模エージェントを展開するためにカスタマーインスタンスを作成するには、次の一連のタスクに従います。各タスクの後で、このページに戻ってそのタスクを「完了」としてマークしたら、次の手順に進みます。

表 *17*：コアコンポーネントのカスタマーインスタンスの作成

順序	タスク	完了
1	VMware ツールのアップグレード （26 ページ）	
2	仮想マシンの起動とシャットダウンの設定 （26 ページ）	
3	Small Contact Center 展開の Finesse 用 DNS サーバーの作成 （139 ページ）	
4	Small Contact Center エージェント展開用 Unified CCE Rogger の構成 （136 ページ）	
5	Unified CCE AW-HDS-DDS の構成 （41 ページ）	
6	VRU 周辺機器ゲートウェイの構成 （51 ページ）	
7	Unified CVP の構成 （60 ページ）	
8	Small Contact Center 導入モデル用 CUBE エンタープライズの構成 （142 ページ）	

順序	タスク	完了
9	Unified Intelligence Center の構成 （123 ページ）	
10	ライブ データ レポーティング システムの構成 （124 ページ）	

表 *18* : 専用コンポーネント サブ カスタマー オプションの構成

順序	タスク	完了
1	仮想マシンの起動とシャットダウンの設定 （26 ページ）	
2	Unified CCE PG の構成 （47 ページ）	
3	Unified Communications Manager の構成 （87 ページ）	
4	SW MTP および SW 会議リソースの増加 （312 ページ）	
5	Cisco Finesse の構成 （110 ページ）	
6	Cisco Identity Service の構成 （124 ページ）	

表 *19* : 共有コンポーネント サブ カスタマー オプションの構成

順序	タスク	完了
1	仮想マシンの起動とシャットダウンの設定 （26 ページ）	
2	Unified CCE PG の構成 （47 ページ）	
3	Shared Unified Communications Manager の構成 （138 ページ）	
4	Cisco Finesse の構成 （110 ページ）	
5	Cisco Identity Service の構成 （124 ページ）	

Small Contact Center エージェント展開用に共有コアコンポーネントとサブ カスタマー コンポーネントのカスタマーインスタンスを作成した後、Internet Script Editor と統合するように Unified CCDM を構成します。「Partition Internet Script Editor 用 Small Contact Center エージェント展開を CCDM に統合 （177 ページ）」を参照してください。

Small Contact Center エージェント展開用に、共有コアコンポーネントとサブ カスタマー コンポーネントのカスタマーインスタンスを作成した後、以下の手順を実行します。

- Internet Script Editor と統合するように unified CCDM を構成します。Partition Internet Script Editor 用 Small Contact Center エージェント展開を CCDM に統合 （177 ページ）を参照してください。
-

Small Contact Center エージェント展開用 Unified CCE Rogger の構成

ここでは、Unified CCE Rogger に対して実行する構成手順に関して説明します。

順序	タスク	完了したか
1	ネットワークカードの構成 （31 ページ）	
2	ドメイン内マシンの検証 （33 ページ）	
3	ドメインマネージャの構成 （34 ページ）	
4	Unified CCE 暗号化ユーティリティの構成 （35 ページ）	
5	CCE コンポーネント用 SQL Server の設定 （36 ページ）	
6	セカンダリドライブの構成 （36 ページ）	
7	Unified CCE Logger の構成 （37 ページ）	
8	Small Contact Center 向け Unified CCE ルーターの構成 （137 ページ）	
9	基本構成のロード （136 ページ）	
10	Cisco Diagnostic Framework Portico の検証 （56 ページ）	
11	Cisco SNMP の設定 （56 ページ）	

基本構成のロード

基本構成パラメータをインポートするには、以下の手順を実行します。基本構成パラメータの詳細については、「Small Contact Center エージェント展開用基本構成パラメータ （574 ページ）」を参照してください。

手順

ステップ 1 HCS-CC_11.6.1-Day1_SCC.zip または ファイルをダウンロードします。このファイルをローカルに保存して、解凍します。

ステップ 2 Domain_Update_Tool.zip ファイルをダウンロードします。このファイルをローカルに保存して、解凍します。

ステップ 3 構成フォルダをサイド A にある Unified CCE Rogger のローカルドライブにコピーします。

ステップ 4 サイド A の Unified CCE Rogger で ICMDBA ツールを開きます。

ステップ 5 Unified CCE Rogger を選択し、<instance name>_sideA にツリーを展開します。

ステップ 6 メニューバーの [データ（Data）] を選択し、**[インポート（Import）]** をクリックします。

ステップ 7 構成フォルダを参照して特定し、**[開く（Open）]** をクリックします。

ステップ 8 **[OK]** > **[インポート（Import）]** の順に選択します。

ステップ 9 [スタート（Start）] をクリックし、すべてのメッセージに対して **[OK]** をクリックします。

ステップ 10 Domain_Update_Tool フォルダに移動し、[UpdateDomain.PS1.] を右クリックしたら、 PowerShell で実行します。次のように入力します。

a) サーバー名として、サイド A の Unified CCE Rogger のコンピュータ名を入力します。
b) [データベース名（Database name）] に、<instance_sideA (Logger database)> と入力します。
c) ドメイン名として、カスタマーのドメイン名を入力します。

ステップ 11 ICMDBA ツールに戻ります。同期するサイドの Logger <instance name> を選択します。

ステップ 12 メニューバーの **[データ（Data）]** をクリックし、**[同期（Synchronize）]** を選択して、以下の手順を実行します。

a) **[同期（Synchronize）]** ウィンドウの **[ソール（Source）]** ペインで **[追加（Add）]** をクリックします。
b) **[サーバー名（Server Name）]** フィールドに送信元の Unified CCE Rogger のホスト名を入力し、**[OK]** をクリックします。
c) **[接続先（Destination）]** ペインで **[追加（Add）]** をクリックします。
d) **[サーバー名（Server Name）]** フィールドに接続先の Unified CCE Rogger のホスト名を入力し、**[OK]** をクリックします。
e) **[同期（Synchronize）]** をクリックします。

ステップ 13 **[スタート（Start）]** をクリックし、すべてのメッセージに対して **[OK]** をクリックします。

Small Contact Center 向け Unified CCE ルーターの構成

以下の手順を実行し、Unified CCE ルーターを構成します。

手順

ステップ 1 Unified CCE Web Setup を起動します。

ステップ 2 ローカルの管理者権限を持つドメイン ユーザとしてサインインします。

ステップ 3 **[コンポーネント管理（Component Management）]** > **[ルーター（Routers）]** の順に選択します。

ステップ 4 **追加** をクリックして、コール ルータを設定します。

ステップ 5 [展開（Deployment）] ウィンドウで、適切な **[サイド（Side）]** を選択します。

ステップ 6 **[デュプレックス（Duplexed）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 7 **ルータ接続** ウィンドウで、プライベートインターフェイスとパブリック（表示）インターフェイスを設定します。[次へ（Next）] をクリックします。

ステップ 8 **周辺機器ゲートウェイを有効にする** フィールドで、PG に割り当てられた番号を入力して有効にします。

ハイフンを使用して、範囲を指定し、コンマで値を区切ります。たとえば、「2～4、6、79～80」では、PG2、PG3、PG4、PG6、PG79、およびPG80が有効となります。スペースは無視されます。

（注） システムに存在するPGのIDのみを入力します。未使用のPG IDを追加すると、誤ったルーターフェールオーバー処理が発生する場合があります。

ステップ 9 PG 81ー150の場合は、**[詳細設定（Advanced）]**をクリックして展開し、使用するPG番号を入力します。

ステップ 10 **[ルーターのオプション（Router Options）]**ウィンドウで、以下の通り構成し、**[次へ（Next）]**をクリックします。

a) **[データベース ルーティングを有効化（Enable Database Routing）]**をオンにします。

b) **Quality of Service（QoS）を有効にする**をオンにします。（サイドAにのみに該当）。

ステップ 11 **[ルーターのサービス品質（Router Quality of Service）]**ウィンドウで、**[次へ（Next）]**をクリックします。

ステップ 12 **[サマリー（Summary）]**ウィンドウで、ルーターのサマリーが正しいことを確認して、**[完了（Finish）]**をクリックします。

（注） Unified CCE コンポーネントのインストールが完了するまで、サービスを起動しないでください。

Shared Unified Communications Manager の構成

この一連のタスクに従って、共有 Cisco Unified Communications Manager を構成します。

順序	タスク	完了したか
1	Unified Communications Manager Publisher の構成 （88 ページ）	
2	Unified Communications Manager Subscriber の構成 （89 ページ）	
3	Windows 用 VMware ツールのインストール （394 ページ）	
4	Unified Communications Manager ライセンス （90 ページ）	
5	サービスのアクティブ化 （91 ページ）	
6	クラスタ全体のドメイン構成の検証 （92 ページ）	
7	Unified CCE サーバー に JTAPI をインストール （93 ページ）	

順序	タスク	完了したか
8	SNMP の構成 （120 ページ）	
9	パーティションの設定 （533 ページ）	
10	コーリングサーチスペースの設定 （533 ページ）	
11	CSSおよびパーティションと電話および回線の関連付け （534 ページ）	
12	CSS とトランクの関連付け （534 ページ）	

Small Contact Center 展開の Finesse 用 DNS サーバーの作成

一部の VOS マシン（Finesseなど）では、VOS を正常にインストールするために、同じネットワーク内でローカルに使用可能な DNS サーバー解像度が必要です。Small Contact Center 展開のサブカスタマーネットワークに DNS をインストールします。

DNS サーバーを作成するには、以下の手順を実行します。

- DNS サーバーの有効化 （139 ページ）
- DNS サーバーの構成 （140 ページ）

DNS サーバーの有効化

手順

ステップ 1 サブカスタマーネットワークのサーバーマシンにログインします。

ステップ 2 **[管理ツール（Administrative Tools）]** > **[サービス（Services）]** の順に選択します。

ステップ 3 左側のペインで、**[ロール（Roles）]** をクリックします。

ステップ 4 [ロール（Roles）] ウィンドウで、**[ロールの追加（Add Roles）]** をクリックします。

ステップ 5 [ロールの追加（Add Roles）] ウィザードで **[次へ（Next）]** をクリックします。

ステップ 6 [サーバーの役割の選択（Select Server Roles）] ウィンドウで、**[DNSサーバー（DNS Server）]** をオンにします。[次へ（Next）] をクリックします。

ステップ 7 [DNSサーバー（DNS Server）] ウィンドウで、**[次へ（Next）]** をクリックします。

ステップ 8 [インストールの選択の確認（Confirm Installation Selections）] で、**[インストール（Install）]** をクリックし、インストールが完了したら、[閉じる（Close）] ウィザードをクリックします。

DNS サーバーの構成

手順

ステップ 1 **[スタート（Start）]** > **[管理ツール（Administrative Tools）]** > **[DNS]** の順に選択します。

ステップ 2 [左側のサーバー（Server on Left）] ペインを展開します。

ステップ 3 [正引きルックアップゾーン（Forward Lookup Zones）]を右クリックし、**[新規ゾーン（New Zone）]** をクリックします。

ステップ 4 [新規ゾーン（New Zone）] ウィザードで、**[次へ（Next）]** をクリックします。

ステップ 5 [ゾーンタイプ（Zone type）] ウィンドウで、**[プライマリゾーン（Primary zone）]** を選択します。[次へ（Next）] をクリックします。

ステップ 6 [ゾーン名（Zone Name）]ウィンドウで、完全修飾 *DNS* 名を入力します。[次へ（Next）] をクリックします。

ステップ 7 [ゾーンファイル（Zone File）] ウィンドウで、**[このファイル名で新規ファイルを作成（Create a new file with this file name）]** を選択します。[次へ（Next）] をクリックします。

ステップ 8 [動的更新（Dynamic Update）] ウィンドウで、**[動的更新を許可しない（Do not allow dynamic updates）]** を選択します。[次へ（Next）] をクリックします。

ステップ 9 [完了（Finish）] をクリックします。

ステップ 10 [逆ルックアップゾーン（Reverse Lookup Zones）] を右クリックし、**[新規ゾーン（New zone）]** をクリックします。

ステップ 11 [新規ゾーン（New zone）] ウィザードで、**[次へ（Next）]** をクリックします。

ステップ 12 [ゾーンタイプ（Zone type）] ウィンドウで、**[プライマリゾーン（Primary zone）]** を選択します。[次へ（Next）] をクリックします。

ステップ 13 [逆引きルックアップゾーン名（Reverse Lookup Zone Name）]で、**[IPv4リリースルックアップゾーン（IPv4 Reverse Lookup Zone）]** を選択します。[次へ（Next）] をクリックします。

ステップ 14 **[ネットワーク（Network）]**フィールドに*IP*アドレスの最初の*3*オクテットを入力します。[次へ（Next）] をクリックします。

（注） Small Contact Center 導入モデルの場合、Finesse インストール時に共有 DNS を使用した場合のみ、お客様が、共有 IP と内部 IP の両方の逆引きルックアップゾーンを追加する必要があります。

例：

10.10.10.X（共有 IP）と 20.20.20.X（内部 IP）に対して逆引きルックアップゾーンを作成します。

ステップ 15 [ゾーンファイル（Zone File）] ウィンドウで、**[このファイル名で新規ファイルを作成（Create a new file with this file name）]** を選択します。[次へ（Next）] をクリックします。

ステップ 16 [動的更新（Dynamic Update）] ウィンドウで、**[動的更新を許可しない（Do not allow dynamic updates）]** を選択します。[次へ（Next）] をクリックします。

ステップ 17 **[完了（Finish）]** をクリックします。

DNS サーバーのホスト構成

手順

ステップ 1 **[DNSマネージャ（DNS Manager）]** に移動します。

ステップ 2 **[転送ドメインゾーン（Forward domain zone）]** を右クリックします。**[新規ホスト（A または AAAA）（New Host (A or AAAA)）]** を選択します。

ステップ 3 ホスト名を入力します。

ステップ 4 ホストの IP アドレスを入力します。

ステップ 5 **[関連付けられたポインタ（PTR）レコードの作成（Create Associated Pointer（PTR）Record）]** チェックボックスをオンにします。**[ホストの追加（Add host）]** をクリックします。

ステップ 6 [OK] をクリックします。**[完了（Done）]** をクリックします。

（注） Small Contact Center 導入モデルでは、お客様が Finesse のインストールに共有 DNS を使用している場合は、以下の手順を実行します。

1. 共有 DNS の正引きルックアップゾーンと逆引きルックアップゾーンの両方に、Finesse 内部 IP（nated IP ではない）を追加します。
2. IP アドレスを同じにすることができる DNS サーバーに一意の Finesse ホスト名を追加します。
3. Finesse プライマリおよびセカンダリを正常にインストールしたら、ホストエントリを Finesse 内部 IP の逆ルックアップゾーンから削除します。
4. DNS サーバーに Finesse ホスト名の natted IP を追加します。これにより SSO がサポートされます。

   （注） ライブデータは、専用サブカスタマーオプションの共有 DNS 構成ではサポートされません。

5. すべてのサブカスタマーの Finesse サーバーの OS カスタマイズは、並行してではなく、順次に行う必要があります。

Small Contact Center 導入モデル用 CUBE エンタープライズの構成

VRF の構成

マルチ VRF 機能を使用すると、同じ CUBE デバイス内のルーティングおよび転送テーブルの 1 つ以上のインスタンスを構成および維持でき、VRF に基づいて音声トラフィックを区別できます。

サブカスタマー 1 に VRF を構成する：

```
ip vrf SUB-Customer1
rd 20.20.20.10:1
```

ルート識別子を指定して VRF テーブルを作成します。AS 番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。

サブカスタマー 2 に VRF を構成する：

```
ip vrf SUB-Customer2
rd 20.20.20.10:2
```

VRF にインターフェイスを割り当て

VRF にインターフェイスを割り当てるには、以下の手順を実行します。

```
interface GigabitEthernet2
 ip vrf forwarding Customer1
```

VRF をインターフェイスに関連付けます。インターフェイスに関連付けられている IP アドレスがある場合、その IP アドレスはクリアされ、IP アドレスを再度割り当てるように求められます。

```
 ip address 10.10.10.5 255.255.255.0
```

グローバル設定の構成

```
 voice service voip
 no ip address trusted authenticate
 address-hiding
 mode border-element
```

コーデックリストの構成

```
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
codec preference 3 g729br8
codec preference 5 g711alaw
```

デフォルトサービスの構成

```
Default Services
application
service survivability flash:survivability.tcl
```

VRF 固有の RTP ポート範囲の構成

VoIP RTP 接続の場合、各 VRF が音声サービス VoIP で独自の RTP ポート範囲を持つように構成できます。最大 10 個の VRF ポート範囲に対応しています。異なる VRF でも、重複する RTP ポート範囲を指定できます。

VRF ベースの RTP ポート範囲の制限（最小および最大ポート番号を含む）は、グローバル RTP ポート範囲と同じです。グローバル、メディアアドレス、および VRF ベースの 3 つのポート範囲はすべて、CUBE で共存できます。RTP ポート割り当ての優先順位は次のとおりです。

- VRF ベースのポート範囲
- メディアアドレスベースのポート範囲
- グローバル RTP ポート範囲

```
media-address voice-vrf SUB-Customer1 port-range 25000 28000
media-address voice-vrf SUB-Customer2 port-range 25000 28000
```

IP ルートの構成

```
ip route vrf SUB-Customer1 0.0.0.0 0.0.0.0 20.20.20.1
ip route vrf SUB-Customer2 0.0.0.0 0.0.0.0 20.20.20.1
```

ダイヤルピアの構成

ダイヤルピアのコントロールとメディアは、同じ VRF にバインドする必要があります。そうしないと、CLI 解析がエラーを表示します。

CVP の着信ダイヤルピアの構成

```
dial-peer voice 23991 voip
 description Incoming dial-peer for CVP
 service survivability
 session protocol sipv2
 session transport udp
 incoming called-number .T
 voice-class codec 1
 voice-class sip rel1xx disable
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
 dtmf-relay rtp-nte
```

CVP の発信ダイヤルピアの構成

```
 dial-peer voice 1001 voip
 description outgoing dial-peer for CVP
 translation-profile outgoing strip-digit
 destination-pattern .T
 session protocol sipv2
 session target ipv4:10.10.10.10
 session transport udp
 voice-class codec 1
 voice-class sip rel1xx disable
 voice-class sip bind control source-interface GigabitEthernet1
```

```
voice-class sip bind media source-interface GigabitEthernet1
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Sub-customer1 VRF1 の着信ダイヤルピアの構成

```
dial-peer voice 21991 voip
description "Incoming Dial-peer for VRF1"
service survivability
session protocol sipv2
session transport udp
incoming called-number [12][03][27].......
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.100
voice-class sip bind media source-interface GigabitEthernet2.100
dtmf-relay rtp-nte
```

Sub-customer2 VRF2 の着信ダイヤルピア

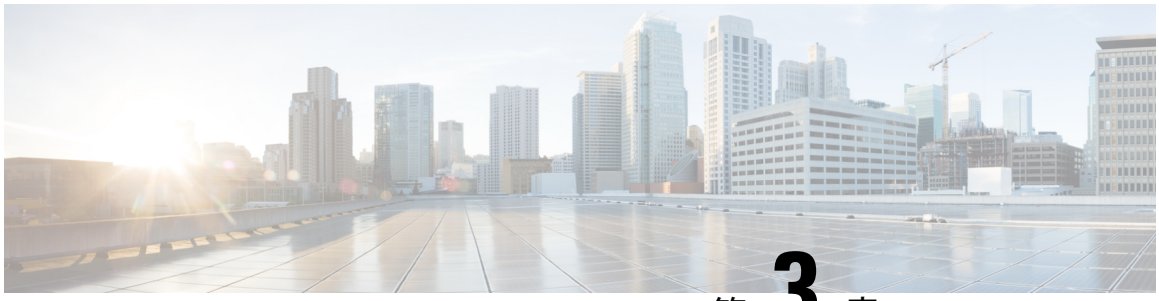
```
dial-peer voice 22991 voip
description "Incoming dial-peer for VRF2"
service survivability
session protocol sipv2
session transport udp
incoming called-number 1[03][16].......
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet3
voice-class sip bind media source-interface GigabitEthernet3
dtmf-relay rtp-nte
```

Sub-customer1 VRF1 のダイヤルピアの構成

```
dial-peer voice 21001 voip
description from CVP towards VRF1 to CUCM Sub-Customer1
destination-pattern 101....
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.100
voice-class sip bind media source-interface GigabitEthernet2.100
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Sub-customer2 VRF2 のダイヤルピアの構成

```
dial-peer voice 22001 voip
description from CVP towards VRF2 to CUCM Sub-Customer2
destination-pattern 201....
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.200
voice-class sip bind media source-interface GigabitEthernet2.200
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```



第 3 章

カスタマーインスタンスと共有管理の統合

シングルサインオン統合

Cisco IdS に対する信頼関係の確立

アプリケーションを有効にし、シングルサインオンにシスコアイデンティティサービス（Cisco IdS）を使用するには、Cisco IdS とホストされたアイデンティティプロバイダ（IdP）間でメタデータの交換を実施します。

- SAML SP メタデータファイルである `sp.xml` を Cisco IdS publisher プライマリノードにダウンロードします。

  1. 次のいずれかを実行して、アイデンティティサービス管理を開きます。
     - [アイデンティティサービス管理（Identity Service Management）] ウィンドウを開きます（`https://<Unified CCX server address>:8553/idsadmin`）。
     - Administration で **[システム（System）]** > **[シングルサインオン（Single Sign-On）]** の順に選択し、**[アイデンティティサービス管理（Identity Service Management）]** をクリックします。
  2. **[設定（Settings）]** > **[IdS トラスト（IdS Trust）]** タブで、`sp.xml` という SAML SP メタデータファイルをダウンロードします。

- IdP から、federationmetadata.xml というアイデンティティ プロバイダ メタデータ ファイルをダウンロードします。次の例を参考にしてください。

1. AD FS の場合は、次の場所にある IdP からアイデンティティ プロバイダ メタデータ ファイルをダウンロードします。

   `https://<ADFSServer FQDN>/federationmetadata/2007-06/federationmetadata.xml`.

2. **アイデンティティサービス管理**ページを開き、前に手順でダウンロードした、アイデンティティ プロバイダ メタデータ ファイルをアップロードします。

SAML SSO は信頼認証証明書を使用して、IdP（AD FSなど）と Cisco IdS の間で認証および承認の詳細を交換します。これにより、サーバー間の通信が保護されます。

（注）
- Cisco IdS は SAML 認証のための自己署名証明書に対応しています。
- IdP 証明書が管理者によって自動的にロールオーバー、手動で更新、またはアップデートされた場合は、IdS と IdP 間の信頼関係が再確立されます。

共有 ADFS にカスタマーインスタンスを統合

Cisco IdS を共有管理 ADFS に統合

手順

ステップ 1 AD FS では、デフォルトの認証タイプが [フォーム] に設定されていることを確認します。（Cisco Identity Service では、フォーム ベースの認証を提供するために ID プロバイダが必要です。）詳細については、Microsoft AD FS のドキュメントを参照してください。

ステップ 2 AD FS サーバで、**AD FS 管理を開きます**。

ステップ 3 **AD FS -> 信頼関係 -> 信頼当事者証明を右クリックします**。

ステップ 4 メニューで、**信頼当事者証明の追加** を選択して、**信頼当事者証明の追加ウィザード**を起動します。

ステップ 5 **データ ソースの選択** 手順で、**信頼当事者についてのデータをファイルからインポートする**オプションを選択します。

ステップ 6 Cisco Identity Server からダウンロードした `sp.xml` ファイルに**移動して**、インポートを完了し、信頼当事者証明を確立します。

ステップ 7 **表示名の指定**手順を選択し、信頼当事者証明を識別するために使用できる有意の名前を追加します。

ステップ 8 Windows サーバーの AD FS の場合、**[Configure Multi-factor Authentication Now（今すぐ多要素認証を構成する）]** 手順で、**[この時点では信頼当事者の多要素認証設定を構成しない（I do not want to configure multi-factor authentication settings for the relying party at this time）]** オプションを選択します。

この手順は AD FS 2.0 または 2.1 では表示されません。以下の手順に進んでください。

ステップ 9 発行認証ルールの選択手順で、**[すべてのユーザに対してこの信頼当事者へのアクセスを許可する（Permit all users to access this relying party）]** オプションを選択して、**[次へ（Next）]**をクリックします。

ステップ 10 **次へ** をもう一度クリックして、信頼当事者の追加を完了します。

ステップ 11 **信頼当事者証明**を右クリックして、**プロパティ**をクリックします。**識別子** タブを選択します。

ステップ 12 [識別子] タブで、**表示名** を信頼当事者証明の作成時に指定した名前に設定して、**信頼当事者識別子** を `sp.xml` をダウンロードした Cisco Identity Server の **完全修飾ホスト名** に設定します。

ステップ 13 さらに **プロパティ**で、**詳細設定** タブを選択します。

ステップ 14 **セキュア ハッシュ アルゴリズム** に **SHA-1** を選択して、**OK**をクリックします。

（注） 以下の手順では、2 つの要求ルールを設定して、AD FS から Cisco Identity Service に送信される要求を、正常な SAML アサーションの一部として指定します。

- アサーションには、次のカスタムクレームを含む要求ルールが属性ステートメントとして含まれています。
  - **uid**：アプリケーションに送信されるクレーム内の認証済みのユーザを識別します。
  - **user_principal**：Cisco Identity Serviceに送信されたアサーション内のユーザーの認証レルムを識別します。
- 2 番目の要求ルールは、AD FS サーバと Cisco ID サーバの完全修飾ドメイン名を指定する NameID カスタム要求ルールです。

QoS を設定する手順は、以下の通りです。

ステップ 15 **信頼当事者証明**で、作成した信頼当事者証明を右クリックして、**要求ルールの編集**をクリックします。

ステップ 16 この手順に従って、**LDAP 属性を要求として送信する** で要求ルール テンプレートとしてルールを追加します。

a) **発行変換ルール** タブで、**ルールの追加**をクリックします。

b) **ルール タイプの選択** 手順で、**LDAP 属性をクレームとして送信する** の要求ルールテンプレートを選択して、**次へ**をクリックします。

c) **要求ルールの設定** 手順で、**要求ルール名** フィールドで、**NameID**を入力します。

d) **属性ストア** ドロップダウンを **Active Directory**に設定します。

e) **LDAP属性の発信要求タイプへのマッピング** テーブルを適切な **LDAP属性** に、使用するユーザ識別子タイプに応じた **発信要求タイプ** を設定します。

- 識別子が **SAM-Account-Name** 属性として保存される場合：
  1. **SAM-Account-Name**の **LDAP 属性**を選択し、対応する **発信要求タイプ** を **uid**（小文字）に設定します。

2. **User-Principal-Name** の 2 つ目の **LDAP 属性** を選択して、対応する **発信要求タイプ** を **user_principal**（小文字）に設定します。

- 識別子が UPN の場合：

1. **User-Principal-Name**の **LDAP 属性**を選択し、対応する **発信要求タイプ** を **uid**（小文字）に設定します。
2. **User-Principal-Name** の 2 つ目の **LDAP 属性**を選択して、対応する **発信要求タイプ** を **user_principal**（小文字）に設定します。

（注） SAM-Account-Name または UPN の選択は、AW で設定したユーザ ID に基づきます。

ステップ 17 この手順に従って、**カスタム要求ルール**テンプレートで 2 つ目のルールを追加します。

a) **要求ルールの編集** ウィンドウで、**ルールの追加** を選択します。
b) **カスタム ルールを使用して要求を送信する**を選択します。
c) ルール名を Cisco Identity Server のパブリッシャ（プライマリ）ノードの **完全修飾ドメイン名（FQDN）** に設定します。
d) 以下のルール テキストを追加します。

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>
 issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",

 Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
 Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 =
 "http://<AD FS Server FQDN>/adfs/services/trust",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
 "<fully qualified domain name of Cisco IdS>");
```

e) スクリプトを以下の通りに編集します。

- **<ADFS Server FQDN>** を置き換えて、ADFS サーバの FQDN（完全修飾ドメイン名）と（大文字小文字の区別も含めて）完全に一致させます。
- **<Cisco IdS server FQDN>** を置き換えて、（大文字小文字の区別も含めて）Cisco Identity サーバの FQDN と完全に一致させます。

ステップ 18 フェデレーションシ ナリオに以下のルールを追加します。

a) 名前 ID のルールを追加します。

- **発行変換ルール** タブで、**追加**をクリックします。

- 要求規則テンプレートを **受信要求をパス スルーあるいはフィルタ処理する**として選択します。
- **要求ルールの設定** 手順で、{2}要求ルール名{2} フィールドで、{3}NameID{3}を入力します。
- **名前 ID**に **着信要求タイプ** を選択します。
- [一時的な識別子] に [受信 name_ID] の形式を選択し、**終了**をクリックします。

b) Uid のルールを追加します。

- **発行変換ルール** タブで、**追加**をクリックします。
- 要求規則テンプレートを **受信要求をパス スルーあるいはフィルタ処理する**として選択します。
- **要求ルールの設定** 手順で、{2}要求ルール名{2} フィールドで、{3}NameID{3}を入力します。
- **受信要求タイプ** フィールドで、**uid**を入力して、**終了**をクリックします。

c) user_principal のルールを追加します。

- **発行変換ルール** タブで、**追加**をクリックします。
- 要求規則テンプレートを **受信要求をパス スルーあるいはフィルタ処理する**として選択します。
- **要求ルールの設定** 手順で、{2}要求ルール名{2} フィールドで、{3}NameID{3}を入力します。
- **受信要求タイプ** フィールドで、**user_principal**を入力して、**終了**をクリックします。

ステップ 19 [OK] をクリックします。

共有管理 ADFS にカスタマー ADFS をフェデレーション

カスタマー ADFS に要求説明を追加

手順

ステップ 1 **AD FS Management Console** を開き、**[サービス（Service）]** > **[要求（Claim Descriptions）]** の順に選択します。

ステップ 2 **[要求（Claim Descriptions）]** を右クリックし、**[要求説明の追加（Add Claim Descriptions）]** を選択します。

ステップ 3 uid 要求の説明を作成します。

a) 表示名を **uid** として入力します。

b) クレーム ID を **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uid** として入力します。

c) **[フェデレーションサービスを受け入れられる要求タイプとしてフェデレーションメタデータにこの要求説明を発行する（Publish this claim description in federation metadata as a claim type that this Federation Service can accept）]** チェックボックスをオンにします。

d) **[このフェデレーションサービスが送信できる要求タイプとしてフェデレーションメタデータにこの要求説明を発行する（Publish this claim description in federation metadata as a claim type that this Federation Service can send）]** チェックボックスをオンにしたら、**[OK]** をクリックします。

ステップ 4 user_principal 要求説明を作成します。

a) 表示名を **user_principal** として入力します。

b) クレーム ID を **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/user_principal** として入力します。

c) **[フェデレーションサービスを受け入れられる要求タイプとしてフェデレーションメタデータにこの要求説明を発行する（Publish this claim description in federation metadata as a claim type that this Federation Service can accept）]** チェックボックスをオンにします。

d) **[このフェデレーションサービスが送信できる要求タイプとしてフェデレーションメタデータにこの要求説明を発行する（Publish this claim description in federation metadata as a claim type that this Federation Service can send）]** チェックボックスをオンにしたら、**[OK]** をクリックします。

重要 要求説明の作成後、Hosted AD FS の要求プロバイダトラストのフェデレーションメタデータを更新します。

カスタマー ADFS に信頼当事者証明の要求規則を追加

次の手順を使用して、カスタマー ADFS に信頼当事者証明の要求規則を追加します。

手順

ステップ 1 **AD FS 管理コンソール** を開きます。

ステップ 2 **[信頼関係（Trust Relationships）]** > **[信頼当事者証明（Relying Party Trusts）]** の順に選択します。

ステップ 3 適切な信頼当事者証明を選択して右クリックし、**[要求規則の編集（Edit Claim Rules）]** を選択します。

ステップ 4 **Send LDAP Attributes as Claims** という規則を要求規則テンプレートとして追加します。

a) **発行変換ルール** タブで、**ルールの追加**をクリックします。**Send LDAP Attributes as Claims** という要求規則テンプレートを選択します。

b) **[要求規則構成（Configure Claim Rule）]** で、規則名を **NameID** として構成します。
c) **Active Directory** として **[属性ストア（Attribute store）]** 選択します。
d) LDAP 属性である **User-Principal-Name** を **user_principal**（小文字）の **Outgoing Claim Type** にマッピングします。
e) アプリケーションユーザーを識別する LDAP 属性の 1 つを選択し、**uid**（小文字）にマッピングします。

（注） 作成するルールは、複数の LDAP 属性のいずれかを使用してユーザーを識別できます。正確なマッピングは、ルールが使用する属性によって異なります。

- 識別子が **SAMAccountName** 属性として保存される場合：
  - 発信要求タイプである **uid** はLDAP 属性である**SAM-Account-Name** にマッピングされます。
  - 発信要求タイプである **user_principal** はLDAP 属性である**User-Principal-Name** にマッピングされます。

- 識別子が UPN の場合：
  - 発信要求タイプである **uid** は、LDAP 属性である **User-Principal-Name** にマッピングされます。
  - 発信要求タイプである **user_principal** はLDAP 属性である**User-Principal-Name** にマッピングされます

ステップ 5 **カスタム要求規則**テンプレートを使用して別の規則を追加します。

a) **要求ルールの編集** ウィンドウで、**ルールの追加** を選択します。
b) **カスタム ルールを使用して要求を送信する**を選択します。
c) ルール名を Cisco Identity Server のパブリッシャ（プライマリ）ノードの **完全修飾ドメイン名（FQDN）** に設定します。
d) 以下のルール テキストを追加します。

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>
 issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",

 Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
 Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 =
 "http://<AD FS Server FQDN>/adfs/services/trust",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
 "<fully qualified domain name of Cisco IdS>");
```

- **<AD FS Server FQDN>** を大文字小文字を含め AD FS FQDN と完全に一致するように設定します。
- **<fully qualified domain name of Cisco IdS>** を大文字小文字を含め Cisco Identity Server FQDN と完全に一致するように設定します。

ステップ 6 [OK] をクリックします。

共有管理 ADFS に要求プロバイダ信頼の要求規則を追加

（注） ホステッド（共有管理）ADFS（Cisco IDS が登録されている ADFS）に要求プロバイダの信頼の要求規則を追加します。

手順

ステップ 1 **AD FS 管理コンソール**を開きます。

ステップ 2 **[信頼関係（Trust Relationships）]** > **[要求プロバイダの信頼（Claim Provider Trusts）]** の順に選択します。

ステップ 3 適切な要求プロバイダ信頼を右クリックしたら、**[要求規則の編集（Edit Claim Rules）]** を選択します。

ステップ 4 **[承諾変換規則（Acceptance Transform Rules）]** タブで、**[追加（Add）]** をクリックします。

ステップ 5 名前 ID のルールを追加します。

a) 要求規則テンプレートを **受信要求をパス スルーあるいはフィルタ処理する**として選択します。
b) **要求ルールの設定** 手順で、{2}要求ルール名{2} フィールドで、{3}NameID{3}を入力します。
c) **名前 ID**に **着信要求タイプ** を選択します。
d) [一時的な識別子] に [受信 name_ID] の形式を選択し、**終了**をクリックします。

ステップ 6 Uid のルールを追加します。

a) **[受信要求の変換（Transform an Incoming Claim）]** として、要求規則テンプレートを選択します。
b) **要求ルールの設定** 手順で、{2}要求ルール名{2} フィールドで、{3}NameID{3}を入力します。
c) **[受信要求の種類（Incoming Claim type）]** を **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/uid** に選択します。
d) **[発信要求の種類（Outgoing Claim type）]** を **uid** に選択したら、**[完了（Finish）]** をクリックします。

ステップ 7 user_principal のルールを追加します。

a) **[受信要求の変換（Transform an Incoming Claim）]** として、要求規則テンプレートを選択します。
b) **要求ルールの設定** 手順で、{2}要求ルール名{2} フィールドで、{3}NameID{3}を入力します。
c) **[受信要求の種類（Incoming Claim type）]** を **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/user_principal** に選択します。
d) **[発信要求の種類（Outgoing Claim type）]** を **`user_principal`** に選択したら、**[完了（Finish）]** をクリックします。

Windows サーバーの ADFS サインインページをカスタマイズしてフェデレーテッド ドメイン リストを非表示にする（オプション）

手順に従って、エンドユーザーを組織に自動的にリダイレクトします。これは、コンタクトセンター ソリューションにパートナーとのマルチドメインフェデレーションがあり、フェデレーション対象の IdP のリストを表示しない場合に必要です。

手順

ステップ 1 Hosted AD FS の **Windows Powershell** を開きます。

ステップ 2 **`Set-ADFSClaimsProviderTrust -TargetName "<adfsCPName>" -OrganizationalAccountSuffix @("<mydomain>")`** コマンドを入力します。

上記のコマンドでは、**<adfsCPName>** represents **AD FS Claim Provider Trust Name** および **<mydomain>** は **組織のドメイン名** を示します。

署名済み SAML アサーションの有効化

信頼当事者証明（Cisco Identity Service）の SAML アサーションの署名を有効化します。

手順

ステップ 1 **スタート** をクリックして、**powershell** を [検索] フィールドに入力して、Windows Powershell アイコンを表示します。

ステップ 2 Windows Powershell プログラム アイコンを右クリックして、**管理者として実行する**を選択します。

（注） このプロシージャ内のすべての PowerShell コマンドは、管理者モードで実行する必要があります。

ステップ 3 **Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Display Name> -SamlResponseSignature "MessageAndAssertion"** コマンドを実行します。

（注） <信頼当事者証明表示名> を、信頼当事者証明プロパティの識別子タブと（大文字と小文字を含めて）完全に一致させます。

次に例を示します。

```
Set-ADFSRelyingPartyTrust -TargetName CUICPub.PCCERCDN.cisco.com
-SamlResponseSignature "MessageAndAssertion".
```

ステップ 4 [シスコアイデンティティサービス管理（Cisco Identity Service Management）] に戻ります。

ステップ 5 [設定（Settings）] をクリックします。
デフォルトでは、**[IdS トラスト（IdS Trust）]** タブが表示されます。

ステップ 6 [SAML SPメタデータのダウンロード（Download SAML SP Metadata）]ウィンドウと [IdPメタデータのアップロード（Upload IdP Metadata）]ウィンドウで、IdP と IdS の間に信頼関係がすでに確立されているため、[次へ（Next）]をクリックします。

ステップ 7 [AD FS 認証（AD FS authentication）] ウィンドウで、ログイン情報を入力します。

ステップ 8 SSO が正常に設定されると、「SSO 構成のテストが正常に終了しました（SSO Configuration is test successfully）」というメッセージが表示されます。

（注） 「エラーが発生しました（An error occurred）」というエラーメッセージが表示された場合は、AD FS で作成した要求が有効になっていることを確認します。

「IdP 構成エラー：SAML 処理に失敗（IdP configuration error: SAML processing failed）」というエラーメッセージが表示された場合は、ルールの ID と AD FS の名前が正しいことを確認します。

Unified CCDM の統合

Unified CCDM は通常、複数のカスタマーインスタンス間で共有管理レベルでホストされます。この章では、共有 Unified CCDM から複数のカスタマーインスタンスを構成する方法について説明します。

このセクションでは以下の手順について説明します。

Unified CCDM クラスタでの Unified CCE サーバーの構成

Unified CCDM がプロビジョニング用に接続する前に、Unified CCE コンポーネントを構成する必要があります。Unified CCDM 接続用 Unified CCE を構成するには、以下の手順を実行します。

- Unified CCE 前提条件 （155 ページ）
- 双方向フォレストトラストの確立 （158 ページ）
- Unified CCDM クラスタでの Unified CCE サーバーの設定 （161 ページ）
- 機器マッピングの作成 （163 ページ）

Unified CCE 前提条件

Unified CCE を Unified CCDM と統合する前に、SQL エージェントと CMS サーバーを設定する必要があります。前提条件の構成については、以下の手順を実行します。

- Unified CCDM に対して Unified CCE AW データベース（AWDB）を構成 （155 ページ）
- プロビジョニング用 Unified CCE のAWの構成 （156 ページ）

Unified CCDM に対して Unified CCE AW データベース（AWDB）を構成

次の場合は、AWDB を構成する前に、フォレスト間に双方向の信頼関係を作成してください。

- CCDM および Unified CCE ドメインが別のフォレストにある
- カスタマードメインおよび Unified CCE ドメインが別のフォレストにある
- カスタマードメインと CCDM ドメインが別々のフォレストにある

詳細については、双方向フォレストトラストの確立 （158 ページ）を参照してください。

SQL サーバー認証を使用して Unified CCDM を Unified CCE に接続する場合、

Unified CCE

管理ワークステーションデータベース（AWDB）の構成は必要ありません。SQL 認証を使用していない場合は、AWDB を構成して、Unified CCDM を Unified CCE に接続します。

AWDB を構成するには、以下の手順を実行します。

手順

ステップ 1 Unified CCE Admin Workstation サーバーにローカル管理者権限でログインします。

ステップ 2 **SQL Server Management Studio** を開き、**[接続（Connect）]** をクリックして、サーバーに接続を確立します。

ステップ 3 **Security** フォルダを展開し、**[ログイン（Logins）]** を選択します。

ステップ 4 [ログイン（Logins）] を右クリックし、**[新規ログイン（New Logins）]** を選択します。

ステップ 5 サイド A とサイド B の両方の Unified CCDM サーバーに SQL ログインを追加します（これには、両サイドの Web サーバー、CCDM ドメイン管理者、およびデータベースサーバーが含まれます）。

一般ページを次のように構成します。

1. [ログイン名（Login Name）] フィールドに、<DOMAIN>\<Unified CCDM-HOSTNAME>$ の形式でマシンの名前を入力します。
2. 別のドメインのサーバーに接続する場合を除き、[Windows 認証（Windows Authentication）] を選択します。
3. デフォルト言語を**英語**にします。

ユーザーマッピングページで以下のように構成します。

1. [このログインにマッピングされたユーザー（Users mapped to this login）] フィールドで、hcs_awdb データベースを確認します。
2. [データベースロールメンバーシップ（Database role membership for）] フィールドで、AWDB ログインできるように **public** と **db_datareader** のロールを付与します。

ステップ 6 [OK] をクリックします。

ステップ 7 Unified CCE AW サーバーに 2 つのサイドがある場合、サイド B に手順 1 を繰り返します。

プロビジョニング用 Unified CCE のAWの構成

Unified CCDM Resource Management が接続する各 Unified CCE インスタンスは、次の条件を満たす必要があります。

-
- Unified CCDM が Unified CCE に接続する Unified CCE ディストリビュータマシン（AW）でアプリケーション インスタンスを構成します。アプリケーションタイプを **Cisco Voice** としてアプリケーション インスタンスを構成します。

> **注** CCDM のアプリケーション インスタンスは、ロードベース構成の一部として提供されます。詳細については、「基本構成のロード （40 ページ） からのアプリケーション インスタンス リスト」を参照してください。アプリケーション インスタンスのデフォルト名は、ロードベース構成に基づき、**CCDM** です。

- AW がデュアルサイドの場合、各 Unified CCE AW は Unified CCDM データサーバーの異なる RMI レジストリポートに接続する必要があります。

各 Unified CCE インスタンスには、Unified CCDM resource management に接続する個別のプライマリ ディストリビュータ AW が必要です。

Unified CCE で *CMS* サーバーを設定

新しいアプリケーション接続は、各データベースサーバーの構成した Unified CCE

インスタンスで定義する必要があります。これにより、デュアルサイドシステムでは、代替サイドもフェールオーバーシナリオで Unified CCE に接続できます。

各 Unified CCE の Configuration Management Service（CMS）サーバーを設定するには、以下の手順を実行します。

始める前に

Unified CCDM サーバークラスタを構成する前に、Unified CCDM データベースサーバーごとに Unified CCE で CMS サーバーが正しく設定されていることを確認します。まず、Admin Workstation の構成時に [CMS ノード（CMS Node）] オプションが選択されていることを確認します。Unified CCE で実行されている cmsnode プロセスと cms_jserver プロセスを調べることで、これが該当するかどうかを判断できます。

手順

ステップ 1 Unified CCE Admin Workstation サーバーサイド A で、**CMS 制御**アプリケーションを開きます。

ステップ 2 **[アプリケーション（Application）]** タブで **[追加（Add）]** をクリックし、**アプリケーション接続詳細**ページで以下を構成します。

a) **管理およびデータサーバーリンク** ー Unified CCDM データベースサーバーの名前を入力します。これは、CCDMDBServer などのように、すべて大文字で指定し、最後に Server と付け加えます。

b) **管理およびデータサーバー RMI レジストリポート** ーUnified CCDM サービスに対して Unified CCE AW ポート番号を入力し、接続します。通常は 2099 です。Unified CCDM プロビジョニングサービスが複数の Unified CCE インスタンスに接続する場合、各インスタンスで異なるポートを使用する必要があります。

サイド B の Unified CCE で CMS サーバーを構成する場合は、別の RMI レジストリポートを使用します。

c) **アプリケーションリンク** ー Unified CCDM データベースサーバーの名前を入力します。これは、CCDMDBClient などのように、すべて大文字で指定し、最後に Client と付け加えます。

d) **アプリケーション RMI レジストリポート** ー Unified CCE AW が接続する Unified CCDM データベースサーバーのポート番号を入力します。

これは、管理およびデータサーバー RMI レジストリポートと同じである必要があります。各 Unified CCE AW は、Unified CCDM データベースサーバーの異なるポートに接続する必要があります。将来の使用に備えて、この情報を記録する必要があります。

e) **アプリケーションホスト名** ー Unified CCDM などのサーバー名を入力します。

f) **[OK]** をクリックして変更を保存し、**[アプリケーション接続の詳細（Application Connection Details）]** を閉じます。

ステップ 3 **[OK]** をクリックして変更を保存し、**CMS Control Console** を閉じます。

ステップ 4 手順 1 ー 3 を繰り返して、Cisco Unified CCE Admin Workstation サーバー（サイド A）で Unified CCDM データベースサーバーサイド B の CMS サーバーを設定します。

[アプリケーション接続の詳細（Application Connection Details）] で、サイド A の Unified CCDM データベースサーバーに使用したものと同じポートを使用することを確認します。

（注） CMS JServer プロセスが Unified CCDM に接続できない場合は、Unified CCE エンタープライズ ディストリビュータ サービスを再起動します。

双方向フォレストトラストの確立

ドメインが別のフォレストにある場合は、Unified CCDMのカスタマーインスタンスごとに、サービスプロバイダとカスタマードメインコントローラ間に双方向の信頼を作成します。双方向のフォレストの信頼を作成する前に、サービスプロバイダのドメインコントローラとカスタマーのドメインコントローラで。

カスタマードメインの条件付きフォワーダの作成

条件付きフォワーダを作成するには、以下の手順を実行します。

始める前に

（注） この手順は、Contact Center 版 Cisco Hosted Collaboration Solution 展開のみに必要です。

手順

ステップ 1 [DNSマネージャ（DNS Manager）] に移動します。

ステップ 2 **[条件付きフォワーダ（Conditional Forwarder）]** をクリックします。

ステップ 3 **[新規条件付きフォワーダ（New Conditional Forwarder）]** を右クリックして選択します。

ステップ 4 DNS ドメイン名を入力します。

ステップ 5 [IPアドレス（IP address）]フィールドで、サービスプロバイダドメインの NAT IP アドレスをクリックして入力します。

ステップ 6 [OK] をクリックします。

カスタマードメイン用フォワーダの作成

フォルダを作成するには、以下の手順を実行します。

始める前に

（注） この手順は、Contact Center 版 Cisco Hosted Collaboration Solution 展開のみに必要です。

手順

ステップ 1 [DNSマネージャ（DNS Manager）] に移動します。
ステップ 2 [ドメイン名（Domain Name）] を右クリックします。
ステップ 3 **[プロパティ（Properties）]**をクリックします。
ステップ 4 **[フォワーダ（Forwarders）]** タブをクリックし、**[編集（Edit）]** をクリックします。
ステップ 5 [IPアドレス（IP address）]フィールドで、サービスプロバイダドメインの NAT IP アドレスをクリックして入力します。
ステップ 6 **[OK]** を押して、フォワーダを作成したら、**[適用（Apply）]** > **[OK]** の順に選択します。

サービスプロバイダドメインの条件付きフォワーダの作成

条件付きフォワーダを作成するには、以下の手順を実行します。

手順

ステップ 1 [DNSマネージャ（DNS Manager）] に移動します。
ステップ 2 **[条件付きフォワーダ（Conditional Forwarder）]** をクリックします。
ステップ 3 **[新規条件付きフォワーダ（New Conditional Forwarder）]** を右クリックして選択します。
ステップ 4 DNS ドメイン名を入力します。
ステップ 5 [IP アドレス（IP address）] フィールドで、カスタマードメインの NAT IP をクリックして入力します。
ステップ 6 [OK] をクリックします。

サービスプロバイダドメインのフォワーダの作成

手順

ステップ 1 [DNSマネージャ（DNS Manager）] に移動します。

ステップ 2 **[ドメイン名（Domain Name）]** を右クリックします。

ステップ 3 **[プロパティ（Properties）]**をクリックします。

ステップ 4 **[フォワーダ（Forwarders）]** タブをクリックし、**[編集（Edit）]** をクリックします。

ステップ 5 [IP アドレス（IP address）] フィールドで、カスタマードメインの NAT IP をクリックして入力します。

ステップ 6 **[OK]** を押して、フォワーダを作成したら、**[適用（Apply）]** > **[OK]** の順に選択します。

双方向フォレストトラストの作成

双方向のフォレストの信頼を作成するには、カスタマー ドメイン コントローラから以下の手順を実行します。

手順

ステップ 1 **[アクティブディレクトリドメインとトラスト（Active Directory Domains and Trusts）]** のドメインを右クリックします。

ステップ 2 **[プロパティ（Properties）]**をクリックします。

ステップ 3 **[トラスト（Trust）]** タブをクリックし、**[新規トラスト（New Trust）]** をクリックします。

ステップ 4 **[次へ（Next）]** をクリックします。

ステップ 5 サービスプロバイダのドメイン名を入力し、**[次へ（Next）]** をクリックします。

ステップ 6 **[フォレストトラスト（Forest Trust）]** オプションを選択し、**[次へ（Next）]** をクリックします。

ステップ 7 **[双方向トラスト（Two-way Trust）]** オプションを選択し、**[次へ（Next）]** をクリックします。

ステップ 8 **[このドメインと指定ドメインの両方（Both this domain and specified domain）]** オプションを選択し、**[次へ（Next）]** をクリックします。

ステップ 9 カスタマーの認証ユーザー名と指定したドメインのパスワードを入力し、**[次へ（Next）]**をクリックします。

トラストを作成するには、管理者権限が必要です。

ステップ 10 **[フォレスト全体の認証（Forest-wide authentication）]** オプションを選択し、[送信信頼の確認（Confirm Outgoing Trust）] が表示されるまで **[次へ（Next）]** をクリックします。

ステップ 11 **[はい、送信信頼を確認します（Yesconfirm the outgoing trust）]** オプションを選択し、**[次へ（Next）]** をクリックします。

ステップ 12 **[はい、受信信頼を確認します（Yes, confirm the incoming trust）]** オプションを選択し、**[次へ（Next）]** をクリックします。

ステップ 13 **[完了（Finish）]** をクリックします。

統合構成環境の起動

Unified CCDM データサーバーで Integrated Configuration Environment（ICE）を起動するには、以下の手順を実行します。

手順

ステップ 1 **Integrated Configuration Environment** アプリケーションを開きます。

ステップ 2 **データベース接続**ページで、次のように入力します。

a) **[サーバー名（Server Name）]** フィールドのデフォルト値は **current machine** です。

b) **[データベース名（Database Name）]** フィールドは、デフォルト値（Portal）のままにします。

c) **[認証（Authentication）]** フィールドは、デフォルト値のままにします。

ステップ 3 **[テスト（Test）]** をクリックして、最初のデータベースサーバー接続テストを実施します。テストが不合格の場合、**データベース接続**設定を確認します。

ステップ 4 **[OK]** をクリックして ICE を開きます。

ICE を起動すると、クラスタ構成ツールがデフォルトのツールになります。ツールバーの **[ツール（Tool）]** ドロップダウンリストを使用して、他の ICE ツールに切り替えることができます。

Unified CCDM クラスタでの Unified CCE サーバーの設定

Unified CCDM の Unified CCE を構成するには、以下の手順を実行します。

手順

ステップ 1 Unified CCDM データベースサーバーサイド A で、**統合構成完了** を起動します。「統合構成環境の起動 （161 ページ）」を参照してください。

ステップ 2 [ICEクラスタ構成（ICE Cluster Configuration）] ツールの **[ツール（Tool）]** ドロップダウンリストで **[クラスタ構成（Cluster Configuration）]** を選択します。

ステップ 3 **[Configure Cisco Unified Contact Enterpriseサーバー（Configure Cisco Unified Contact Enterprise Servers）]** をクリックします。

ステップ 4 **[タスクの選択（Select Task）]** ドロップダウンリストで **[新しいインスタンスの追加（Add a New Instance）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 5 **[リソース名の指定（Specify Resource Name）]** で、構成するインスタンスの名前を指定します。[次へ（Next）] をクリックします。

ステップ 6 **[必要なコンポーネントの選択（Select Required Components）]** で、展開に必要なコンポーネントを選択し、**[次へ（Next）]** をクリックします。

- **Admin Workstation**：これはすべての構成において必要なコンポーネントです。

- **Provision Components (ConAPI/Unified config)**：リソース管理が必要な場合のこのオプションを選択します。

ステップ 7 **[冗長性の構成（Configure Redundancy）]** で、片面設定または両面設定のどちらを構成するかを選択します。

ステップ 8 **[AWサーバーの構成（Configure AW Server）]** で、プライマリサーバーの名前と IP アドレスを入力します。

（注） Unified CCE が両面設定の場合、セカンダリサーバーの名前と IP アドレスを入力します。

ステップ 9 **[接続詳細の構成（Configure Connection Details）]** で、認証詳細を入力して、Admin Workstation データベースに接続します。

a) **Windows Authentication**：これは、デフォルトの認証モードです。
b) **SQL Authentication**：SQL サーバーユーザー名と対応するパスワードを指定してデータベースに接続します。

ステップ 10 **[Unified CCEインスタンスの選択（Select Unified CCE Instance）]** で、展開用の AW インスタンスを選択したら、**[次へ（Next）]** をクリックします。

ステップ 11 **[Cisco Unified Contact Center Enterpriseサーバー（Configure Cisco Unified Contact Center Enterprise Server）]** ウィンドウで以下のように **Unified Config Webサーバー**を構成します。

- **プライマリ Unified Config Web サービスの構成**ページでプライマリ Unified CCE Admin workstation サーバーのドメインユーザー名とパスワードを入力し、**[次へ（Next）]** をクリックします。
- **Secondary Unified Config Web サーバーの構成**ページで、Unified CCE が両面設定の場合、セカンダリ Unified CCE Admin Workstation サーバーのドメインユーザー名とパスワードを入力し、**[次へ（Next）]** をクリックします。

（注） ドメインアカウントのログイン情報を使用してログインします。ユーザー名の形式は、*username@domain.com* です。

ステップ 12 手順 4 で、ConAPI Server (Provisioning) オプションを選択した場合、以下の詳細を入力します。

- **Local Registry Port**：Unified CCDM Provisioning サービスに対して Unified CCE のポート番号を入力し、接続します。デフォルトポートは 2099 です。Unified CCE で CMS サーバーを設定 （157 ページ） の Application RMI レジストリポートに構成されている Unfied CCDM Database サーバーポート番号と同じ番号を入力してください。
- **Remote Registry Port**：Unified CCE に対する Unified CCDM Database サーバーのポート番号を入力して接続します。デフォルトポートは 2099 です。Unified CCE で CMS サーバーを設定 （157 ページ） の Administration & Data Server RMI Registry Port に構成されている Unified CCE AW ポート番号と同じ番号を入力してください。
- **Local Port** ：Unified CCE と Unified CCDM サーバー間のライブ プロビジョニング トラフィック指定ポートとしてこれを選択します。各 Unified CCE に対して一意のポートを割り当てます。Unified CCE および Unified CCDM サーバー間のファイアウォールを構成し、このポートで双方向トラフィックを許可します。

（注） Unified CCE が両面設定の場合、Unified CCE の 設定 CMS のサイド B に対して構成したポート詳細と同じ詳細を入力します。

ステップ 13 **[ConAPIアプリケーションインスタンスの構成（Configure ConAPI Application Instance）]** ダイアログボックスで、以下の詳細を入力したら、**[次へ（Next）]** をクリックします。

- **Application Name**：Unified CCDM からの Unified CCE プロビジョニングに使用するアプリケーション名。**CCDM** として値を入力します（負荷ベースの構成の一環として事前構成済み）。
- **Application Key**：上記で指定したアプリケーションのパスワードを使用します。

ステップ 14 Cisco Unified WIM および EIM アプリケーション インスタンスを使用して音声以外のやり取りをサポートするには、**[マルチメディアサポート（Multi Media Support）]** ダイアログボックスで、**[はい（Yes）]** を選択します。デフォルト値は **[いいえ（No）]** です。

ステップ 15 Unified CCDM から削除する際に Unified CCE から自動で項目を消去するには、**[削除時に消去（Purge On Delete）]** ダイアログボックスで、**[はい（Yes）]** を選択します。デフォルト値は **[はい（Yes）]** です。

ステップ 16 既存のアクティブ ディレクトリ ユーザー アカウントを Unified CCE スーパーバイザに関連付けるサポートをするには、[スーパーバイザアクティブディレクトリ統合（Supervisor Active Directory Integration）] ダイアログボックスで、**[はい（Yes）]** を選択します。デフォルト値は **[いいえ（No）]** です。**[はい（Yes）]** を選択した場合は、以下を入力します。

1. **[アクティブディレクトリ接続の構成（Configure Active Directory Connections）]** で、プライマリ ドメイン コントローラとセカンダリ ドメイン コントローラの両方のアドレスを入力し、必要なセキュリティ設定を構成して接続します。[次へ（Next）]をクリックします。
2. **[スーパーバイザアクティブディレクトリロケーションの選択（Select Supervisor Active Directory Location）]** で、必要なアクティブディレクトリを選択したら、**[次へ（Next）]** をクリックします。

ステップ 17 サマリーページの詳細を見直したら、**[次へ（Next）]** をクリックしてモデルに変更を適用します。

ステップ 18 Unified CCE が正常に構成されたら、**[終了（Exit）]** をクリックして、ウィザードを閉じ、**[保存（Save）]** をクリックして、データベースへの変更を保持します。

機器マッピングの作成

テナントおよび Unified CCE 機器間の機器マッピングを作成するには、以下の手順を実行します。

（注） SCC 展開用機器マッピングの作成については、「展開固有の構成（169ページ）」を参照してください。

手順

ステップ 1 Unified CCDM データベースサーバーサイド A で、**統合構成完了** を起動します。「統合構成環境の起動 （161 ページ）」を参照してください。

ステップ 2 **[ツール（Tool）]** ドロップダウンリストで、**[クラスタ構成（Cluster Configuration）]** を選択します。**[機器マッピング（Equipment Mapping）]** タブを選択します。

ステップ 3 フォルダツリーで、ルートフォルダを右クリックし、**[テナントの追加（Add Tenant）]** を選択します。

ステップ 4 新規テナントに名前を指定します。

ステップ 5 すべてのカスタマー用テナントを作成します。

例：

Cust1CCE

ステップ 6 新しく追加したカスタマーテナントを選択し、隣接するペインで、選択したテナントを関連付ける [Unified Contact Center機器（Unified Contact Center equipment）] チェックボックスをオンにします。

ステップ 7 右側のペインで、**[デフォルトのインポートロケーション（Default Import Location）]** を選択します。

デフォルトのインポートロケーションを使用して、Unified CCDM で選択したテナントにインポートされたすべてのリソース。

ステップ 8 [保存（Save）] をクリックします。

Unified CCDM クラスタでの Unified CVP サーバーの構成

Unified CCDM クラスタで Unified CVP サーバーを設定

[Cisco Unified CVP サーバーの構成（Configure Cisco Unified CVP Servers）] ウィザードは、Cisco Unified CVP サーバークラスタを構成します。Cisco Unified CVP サーバークラスタは、Unified CVP オペレーションコンソールと、オプションで 1 台以上のコールサーバーで構成されます。Cisco Unified CVP サーバークラスタを構成するには、以下の手順を実行します。

手順

ステップ 1 Unified CCDM データベースサーバーサイド A で、**統合構成完了** を起動します。「統合構成環境の起動 （161 ページ）」を参照してください。

ステップ 2 ICE クラスタ構成ツールで、**[設定（Setup）]** タブを選択し、**[Cisco Unified CVP サーバーの構成（Configure Cisco Unified CVP Servers）]** をクリックしてウィザードを開始します。

ステップ 3 **[新規インスタンスの追加（Add a New Instance）]** を選択して、**[次へ（Next）]** をクリックします。

ステップ 4 **[Unified CVPオペレーションコンソールリソース名（Unified CVP Operations Console Resource Name）]** ダイアログボックスで、Unified CVP オペレーションコンソールの名前を指定し、**[次へ（Next）]** をクリックします。

ステップ 5 **[バージョンの選択（Select Version）]** ダイアログボックスで、構成する CVP クラスタで実行されている Unified CVP のバージョンを指定し、**[次へ（Next）]** をクリックします

ステップ 6 **[Unified CVPオペレーションコンソールの構成（Configure Unified CVP Operations Console）]** ダイアログボックスで、次のように入力します。

- **プライマリサーバー**：
  - **サーバー名**：これは、Cisco Unified CVP オペレーションコンソールが展開されている非ドメイン修飾マシン名です。
  - **サーバーアドレス**：サーバー名のデフォルトです。これは、サーバーの IP アドレスまたはドメイン修飾名に変更できます。
- **セカンダリサーバー**：このオプションは常に無効化されています。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 **[プライマリUnified Config Webサービスの構成（Configure Primary Unified Config Web Service）]** ダイアログボックス（選択した Unified CVP バージョンが 10.0 以降の場合にのみ表示）で、以下の詳細を入力します。

- **URL**：これは、Unified CVP クラスタ上のプライマリ統合構成 Web サービスの自動生成された URL です。
- **ユーザー名**：これは、Web サービスが実行されている Unified CVP への適切なアクセス権を持つユーザー名です。
- **パスワード**：これはユーザーのパスワードです。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 **[コールサーバー数の選択（Select Number of Call Servers）]** ダイアログボックスで、CVP クラスタ内の CVP コールサーバー数を指定し、**[次へ（Next）]** をクリックします。

（注） すべての CVP コールサーバーは Unified CVP オペレーションコンソールと同じ Unified CCE にある必要があります。

ステップ 11 少なくとも 1 つのコールサーバーを指定した場合：

1. **[Unified CVP コールサーバー 1 リソース名（Unified CVP Call Server 1 Resource Name）]** ダイアログボックスで、コールサーバーの名前を入力します。
2. **[Unified CVP コールサーバー 1 の構成（Configure Unified CVP Call Server 1）]** ダイアログボックスで、以下のように入力します。
   - **プライマリサーバー**：

- **サーバー名**：これは、Cisco Unified CVP コールサーバーが存在する非ドメイン修飾マシン名です。
- **サーバーアドレス**：サーバー名のデフォルトです。これは、サーバーのIPアドレスまたはドメイン修飾名に変更できます。

- **セカンダリサーバー**：このオプションは常に無効化されています。

3. [次へ（Next）] をクリックします。

（注） 複数のコールサーバーを構成するには、以下の手順を実行します。

ステップ 12 オプションで、[**サーバー**のUnified CCE**構成**（Configure Server）] ダイアログボックスで、構成済みの Unified CVP インスタンスにリンクされている Unified CCE サーバーを選択します。

ステップ 13 **[サマリー（Summary）]** ダイアログボックスには、構成されている Unified CVP クラスタの概要と選択した設定が表示されます。

ステップ 14 詳細を確認し、**[次へ（Next）]** をクリックします。

ステップ 15 ウィザードが正常に完了したことを示す確認メッセージが表示されます。**[終了（Exit）]** をクリックし、ウィザードを閉じます。

ステップ 16 [Save] アイコンをクリックします。

CCDM を使用した CVP の機器マッピング

CVP が統合後の Small Contact Center 導入モデルの場合、CVP はデフォルトで 未割当フォルダにインポートされます。

手順

ステップ 1 **統合済み構成環境** アプリケーションを開き、**[クラスタ構成（Cluster Configuration）]** > **[機器マッピング（Equipment Mapping）]** タブの順に選択します。

ステップ 2 フォルダツリーで、**[ルート（Root）]** を右クリックし、**[テナントの追加（Add Tenant）]** をクリックして、テナント名を指定します。

（注） 既存のUnified CCE カスタマーテナントを使用しても、Unified CVP をマッピングできます。

ステップ 3 すべての CVP カスタマーインスタンスのテナントを作成します。

例：

Cust1CVP

ステップ 4 新しく追加されたテナントを選択し、隣接するペインで、選択したテナントに関連付ける Unified CVP の各項目の横にあるチェックボックスをオンにします。

ステップ 5 右側のペインで、**[デフォルトのインポート場所（Default Import Location）]** を選択して、Unified CCDM で選択したテナントにすべてのリソースをインポートします。

ステップ 6 [保存（Save）] をクリックします。

Active Directory のユーザーの作成

CCDM からテナントまたは下位顧客を作成するには、ユーザを Active Directory で作成する必要があります。

手順

ステップ 1 **Active Directory ドメイン**にログインします。
ステップ 2 **Active Directory ユーザとコンピュータ** を開き、**ユーザ**をクリックします。
ステップ 3 **ユーザ** を右クリックして、**新規** > **ユーザ**を選択します。
ステップ 4 ユーザの **名前**、**姓**、**ログイン名** を入力して、**次へ**をクリックします。
ステップ 5 **パスワード** を入力し、**パスワードの確認** フィールドに再入力します。
ステップ 6 **ユーザのパスワード変更不可** チェックボックスをオンにします。
ステップ 7 **パスワードを無期限にする** チェックボックスをオンにして、**次へ**をクリックします。
ステップ 8 **[完了（Finish）]** をクリックします。

Partitioned Internet Script Editor に対して Unified CCE を構成

シスコの Internet Script Editor（ISE）は、Unified CCDM と統合できます。これにより、Unified CCDM セキュリティを使用して、ルーティングスクリプトとこれらルーティングスクリプト内のリソースを分割できます。ISE ユーザーは、Unified CCDM セキュリティモデルに従って、アクセスが許可されているスクリプトおよびスクリプト内のリソースのみを表示できます。たとえば、ダイヤル番号にルーティングするルーティングスクリプト要素を作成すると、ISE ユーザーには、対応する Unified CCDM ユーザーがアクセスを許可されているダイヤル番号だけが表示されます。同様に、使用可能なルーティングスクリプトを表示すると、ISE ユーザーには、対応する Unified CCDM ユーザーが使用可能なスクリプトのみが表示されます。

ISE と Unified CCDM の統合では、Unified CCDM Analytical Data Web サービスを使用して安全なパーティショニングを実装します。また、正しく動作するためには、Unified CCE と Unified CCDM の両方で特定の構成が必要です。

（注）

- Unified CCDM を使用した安全なパーティショニングは、現在 Cisco Internet Script Editor（ISE）でのみサポートされています。Unified CCE AW の標準 Script Editor を使用しても、関連付けられた Unified CCE インスタンスのすべてのリソースを確認することができます。
- Small contact Center 導入モデルについては、「Partition Internet Script Editor 用 Small Contact Center エージェント展開を CCDM に統合 （177 ページ）」を参照してください。

• Internet Script Editor の Unified CCE Admin Workstation を構成 （168 ページ）
• ユーザーの作成 （211 ページ）
• ロールをユーザーに割り当てる （213 ページ）
• Internet Script Editor のインストール （169 ページ）
• Internet Script Editor を使用したルーティングスクリプトのプロビジョニング （283 ページ）

Internet Script Editor の Unified CCE Admin Workstation を構成

次の手順を実行して、Internet Script Editor を Unified CCDM に統合するための Unified CCE Admin Workstation を構成します

手順

ステップ 1 Unified CCE にログインし、**[コンポーネント管理（Component Management）]** > **[管理とデータサーバー（Administration & Data server）]** の順に選択し、**[管理とデータサーバー（Administrator & Data server）]** チェックボックスをオンにして、**[編集（Edit）]** をクリックします。

ステップ 2 [データベースとオプション（Database and Options）] タブが表示されるまで **[次へ（Next）]** をクリックし、[データベースとオプション（Database and Options）] タブで次のオプションを選択します。

a) **[Internet Script Editor（ISE）サーバー（Internet Script Editor (ISE) Server）]** を選択します。
b) **[承認サーバー（Authorization Server）]** を選択します。
c) 承認サーバーの名前を入力します。

これは、Unified CCDM セキュリティを適用してリソースデータを分割するために使用される Unified CCDM アプリ/Web サーバーです。

d) Unified CCDM Analytical Data Services Web サービスがホストされているポートを入力します。

デフォルトポートは 8087 です。これをインストール時に変更した場合、インストールで使用する値を入力します。

e) **[次へ（Next）]** をクリックします。

ステップ 3 [中央コントローラ接続（Central Controller Connectivity）] タブで、次の詳細を入力します。

a) **[中央コントローラ接続（Central Controller Connectivity）]** セクションで、ルーターサイドA、ルーターサイドB、Logger サイドA、Logger サイドB の IP アドレスを入力します。
b) **[中央コントローラドメイン（Central Controller Domain）]** でドメイン名を入力します。
c) **[中央コントローラの優先サイド（Central Controller Preferred Side）]** の **[中央コントローラのサイドAを優先（Central Controller Side A Preferred）]** のラジオボタンを選択し、**[次へ（Next）]** をクリックします。

ステップ 4 [Summary]タブで、[Finish]をクリックします。

ステップ 5 Unified CCE AW が実行されているサーバーで、ファイアウォールが適切なポートで ISE からのインバウンドトラフィックを許可するように構成されていることを確認します。

ステップ 6 着信 HTTPS トラフィックを許可するように、Unified CCDM 承認サーバーの指定された承認サーバーポートがファイアウォールで構成されていることを確認します。

Internet Script Editor のインストール

手順

ステップ 1 AW マシン（`https://localhost/install/iScriptEditor.htm`）から Internet Script Editor をダウンロードします。

ステップ 2 特定のカスタマーまたはサブカスタマー用の共有場所に、`iscripteditor.exe` を保存します。

ステップ 3 `iscripteditor.exe` ファイルをダブルクリックします。
[Cisco ICM Internet Script Editor設定（Cisco ICM Internet Script Editor Setup）] ウィンドウが表示されます。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 ファイルをインストールするフォルダを選択して、 **次へ**をクリックします。

ステップ 6 インストール後、**[完了（Finish）]** をクリックします。

展開固有の構成

UCCE の Small Contact Center エージェント展開を CCDM に統合

カスタマー定義の作成

手順

ステップ 1 AW マシンにログインし、**[構成マネージャ（Configuration Manager）]**を開きます。

ステップ 2 **[エクスプローラツール（Explorer Tools）]** > **ICM Instace Explorer]** の順に選択します。

ステップ 3 **[取得（Retrieve）]** をクリックし、[SCC展開用のICMインスタンス（ICM Instance for SCC Deployment）]を選択します。

ステップ 4 **[カスタマー定義の追加（Add Customer Definition）]** をクリックします。

ステップ 5 **[名前（Name）]** フィールドで、サブカスタマー定義の名前を入力します。

例：

SubCust1

ステップ 6 **[ネットワークVRU（Network VRU）]** ドロップダウンリストで、**CVP_Network_VRU** のオプションを選択します。

ステップ 7 [保存（Save）] をクリックします。

（注） すべてのサブカスタマーに対して同じ手順を繰り返します。

Small Contact Center 展開用機器マッピング

Small Contact Center のテナントまたはフォルダと Unified CCE 機器の間の機器マッピングを作成するには、以下の手順を実行します。

始める前に

AW を CCDM と統合します。AW の統合方法の詳細については「Unified CCDM クラスタでの Unified CCE サーバーの設定 （161 ページ）」を参照してください。

手順

ステップ 1 ICE クラスタ構成ツールで、**[機器マッピング（Equipment Mapping）]** タブを選択します。

ステップ 2 フォルダツリーで、ルートを右クリックし、**[テナントの追加（Add Tenant）]** をクリックして、テナントの名前を入力します。

すべてのサブカスタマーのテナントを作成します。

例：

SubCust1

ステップ 3 新しく作成したサブカスタマーテナントを選択し、隣接するペインで、選択したテナントに関連付ける Unified CCE の各項目の横にあるチェックボックスをオンにします。

ステップ 4 右側のペインで、**[カスタマーリソースマッピング（Customer Resource Mapping）]** を選択し、**[+]** アイコンをクリックします。

ステップ 5 **[タイプ（Type）]**ドロップダウンリストで、**[リモートテナント（Remote Tenant）]** オプションを選択します。

ステップ 6 **[リソース（Resource）]**ドロップダウンリストで、サブカスタマー用に作成したカスタマー定義を選択します。

ステップ 7 **[Active Directory構成（Active Directory Configuration）]** タブをクリックし、次のように構成します。

a) **[Active Directory設定の構成（Configure Active Directory Settings）]** チェックボックスをオンにします。

b) **[プライマリドメインコントローラ（Primary Domain Controller）]** フィールドに、サブ カスタマー ドメイン コントローラの IP アドレスを入力します。

c) **[次へ（Next）]** をクリックし、ドメインコントローラ名が正しいことを確認します。

d) [更新（Update）] をクリックします。

ステップ 8 **[Small Contact Center設定（Small Contact Center Settings）]** タブを選択し、次のように構成します。

a) **[Small Contact Centerの有効化（Enable Small Contact Center）]** チェックボックスをオンにします。

b) **[部署名（Department Name）]** フィールドに、サブカスタマードメインの部署名を入力します。

c) **[部署の作成（Create Department）]** をクリックします。

ステップ 9 [OK] をクリックします。

ステップ 10 すべてのサブカスタマーに対して上記手順を繰り返します。

ステップ 11 未割り当てフォルダをクリックし、統合済みの Unified CCE フォルダを選択します。隣接するペインで、選択したテナントに関連付ける Unified CCE 機器チェックボックスの各項目をオンにし、**[デフォルトインポート（Default Import）]** チェックボックスをオンにします。

（注） デフォルトでは、Unified CCE配下のすべての構成が、**未割り当て** フォルダにインポートされます。

ステップ 12 [保存（Save）] をクリックします。

Small Contact Center エージェント展開用リソース割り当て

- サブカスタマーテナントにリソースを移動 （175 ページ）
- ネットワーク VRU タイプにラベルをマッピング （175 ページ）

* サブカスタマーユーザーによる構成

** 未割り当てフォルダにインポートされるロードベース構成で提供される構成

*** 構成は未割り当てフォルダからサブカスタマードメインに移動され、構成はサービスプロバイダによって行われます

パラメータ	サブカスタマーによる構成	サービスプロバイダによる構成	注意事項
周辺機器とルーティングクライアント		** & ***	周辺機器、Cisco Unified Communications Manager のルーティングクライアントおよび MR はサブカスタマーテナントの配下に移動されます。
論理インターフェイスコントローラ		** & ***	Cisco Unified Communications Manager のロジカルインターフェイスコントローラおよび MR 周辺機器は、サブカスタマーテナントの配下に移動されます。
物理インターフェイスコントローラ		** & ***	Cisco Unified Communications Manager の 物理インターフェイスコントローラおよび MR 周辺機器はサブカスタマーテナントの配下に移動されます。
ネットワーク VRU		**	Type10 および Type2 のネットワーク VRU は、Day1 構成で指定されます。デフォルトでは、未割り当てフォルダで使用できます。
ECC 変数	*	**	ECC 変数は Day1 構成で指定します。デフォルトでは、未割り当てフォルダで使用できます。配列サイズも制限内に収まる必要があります

パラメータ	サブカスタマーによる構成	サービスプロバイダによる構成	注意事項
ネットワーク VRU スクリプト	*	** & ***	Day1 構成で指定されたネットワーク VRU スクリプト。デフォルトでは、未割り当てフォルダで使用できます。 （注） これは、Day1 構成のカスタマー定義である「HCS for CC」にマッピングされるため、カスタマー定義が HCS for CC のサブカスタマーによって使用されます。サブカスタマーは、自分のテナントのサブカスタマー固有のネットワーク VRU スクリプトを作成します。
アプリケーションインスタンス		** & ***	この項目はテナント/フォルダの配下には移動できませんが、サービスプロバイダは AW のカスタマー要求に基づいて作成できます
メディアクラス		**	

パラメータ	サブカスタマーによる構成	サービスプロバイダによる構成	注意事項
メディアルーティングドメイン		**	Day1 構成で指定されたデフォルトの MRD。デフォルトでは、未割り当てフォルダで使用できます。
エージェント	*		
エージェント チーム	*		
エージェントデスクトップ	*		
コールタイプ	*		
部門	*		
ダイヤル番号	*		
エンタープライズスキル グループ	*		
ラベル	*		Day1 構成で指定されたラベルは、未割り当てフォルダの配下にインポートされます。サービスプロバイダは、カスタマー要求に基づいてラベルを AW のネットワーク VRU タイプにマッピングします。ラベルをネットワーク VRU タイプにマッピングする方法については、「ネットワーク VRU タイプにラベルをマッピング（175 ページ）」を参照してください。
Person	*		
プレシジョン属性	*		
プレシジョンキュー	*		
スキル グループ	*		
ユーザー変数	*		

パラメータ	サブカスタマーによる構成	サービスプロバイダによる構成	注意事項
アウトバウンド		***	すべてのアウトバウンド構成はサービスプロバイダによってAWで行われ、それらの構成はサブカスタマーテナントに移動されます。

サブカスタマーテナントにリソースを移動

手順

ステップ 1 テナント管理者のログイン情報で CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[リソースマネージャ（Resource Manager）]** > **[未割当て（Unallocated）]** > **[SCCテナントフォルダ（SCC Tenant Folder）]** の順に選択します。

ステップ 3 ツリー構造をクリックし、サブカスタマーテナントに移動するパラメータを選択します。

例：

サブカスタマー固有のルーティングクライアントを選択します。

ステップ 4 **[移動（Move）]** をクリックし、**[サブカスタマーテナント（Sub Customer Tenant）]** を選択します。

ステップ 5 **[保存（Save）]** > **[OK]** の順に選択します。

[サブカスタマーテナント（Sub Customer Tenant）] に移動するすべてのパラメータにこの手順を繰り返します。

ネットワーク *VRU* タイプにラベルをマッピング

（注） このアクションは、サブカスタマーの要求に基づいてサービスプロバイダによって実行されます。

手順

ステップ 1 AW マシンにログインします。

ステップ 2 **[構成マネージャ（Configuration Manager）]** > **[エクスプローラツール（Explore Tools）]** > **[Network VRU Explorer]** の順に選択します。

ステップ 3 **[取得（Retrieve）]** をクリックして、**未割り当て**ツリー構造を展開します。

ステップ 4 ネットワーク VRU Type10 にマッピングするラベルを右クリックします。

ステップ 5 **[切り取り（Cut）]** オプションをクリックします。

ステップ 6 ラベルをマッピングする Network VRU Type 10 を選択し、右クリックします。

ステップ 7 **[貼り付け（Paste）]** > **[保存（Save）]** の順に選択します。

エージェントと部署の関連付け

手順

ステップ 1 CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックします。

ステップ 3 **[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 4 **[テナント（Tenant）]** > **[エージェント（Agent）]** の順に選択します。

ステップ 5 部署に関連付けるテナントをクリックします。

ステップ 6 [Advanced] タブをクリックします。

ステップ 7 **[部署（Department）]** ドロップダウンリストで必要な部署を選択します。

ステップ 8 [保存（Save）] をクリックします。

Small Contact Center エージェント導入モデルのリソース用命名規則

次の表に、Small Contact Center エージェント導入モデルでリソースが従うべき命名規則の例を示します。

パラメータ	Sub Customer1	Sub Customer2
ダイヤル番号	エンタープライズ名：9220000001<RoutingClient> , Dialed Number String: 9220000001 またはエンタープライズ名：PlayAgentGreeting<RoutingClient> Dialed Number String: PlayAgentGreeting	エンタープライズ名：9330000001<RoutingClient> , Dialed Number String: 9330000001 またはエンタープライズ名：PlayAgentGreeting<RoutingClient> Dialed Number String: PlayAgentGreeting
コールタイプ	エンタープライズ名：CT1Cust1	エンタープライズ名：CT1Cust2
エージェント	エンタープライズ名：10101010 ログイン名：10101010 エージェント ID：6001	エンタープライズ名：20202020 ログイン名：20202020 エージェント ID：6001
スキル グループ	エンタープライズ名：Skg1Cust1 周辺機器番号：7001	エンタープライズ名：Skg1Cust2 周辺機器番号：7001

パラメータ	Sub Customer1	Sub Customer2
ネットワーク VRU スクリプト	エンタープライズ名：AgentGreetingCust1 VRU スクリプト名：PM,-a,,Cust1	エンタープライズ名：AgentGreetingCust2 VRU スクリプト名：PM,-a,,Cust2
ネットワーク VRU ラベル	名前：9999500001 ラベル：9999500001<RoutingClient>	名前：9999500001 ラベル：9999500001<RoutingClient>
ルーティングスクリプト	名前：Script1	名前：Script1

Partition Internet Script Editor 用 Small Contact Center エージェント展開を CCDM に統合

CCDM をInternet Script Editor と統合するように構成するには、以下の手順を実行します。

（注） これらの手順は、サブカスタマーごとに繰り返す必要があります。

- Internet Script Editor の Unified CCE Admin Workstation を構成 （168 ページ）
- ユーザーの作成 （211 ページ）
- サブカスタマーテナントおよびユーザーへの権限割り当て （213 ページ）
- Internet Script Editor のインストール （169 ページ）
- Internet Script Editor を使用したルーティングスクリプトのプロビジョニング （283 ページ）

IDP の構成

- IDP へのメタデータ交換の構成 （177 ページ）
- Hosted AD FS にアイデンティティサーバーを追加 （178 ページ）
- 要求規則の追加 （179 ページ）
- フェデレーションシナリオの AD FS の構成 （182 ページ）

IDP へのメタデータ交換の構成

手順

ステップ 1 ICE ツールを開きます。

ステップ 2 **[ツール（Tool）]** ドロップダウンリストで、**[システムプロパティ（System Properties）]** を選択します。

ステップ 3 **[グローバルプロパティ（Global Properties）]** > **[ログイン認証構成（Login Authentication Configuration）]** を選択します。

ステップ 4 **[AD FSメタデータURL（AD FS Metadata URL）]** フィールドに、AD FS サーバーのメタデータ URL を入力します。

https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml

ステップ 5 **[ログインタイプの有効化（Enabled Login Types）]** で、**[ADFSログイン（adfs）（ADFS Logins (adfs)）]** チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 コマンドプロンプトを開き、すべての CCDM サーバーで `iisreset` を実行します。

Hosted AD FS にアイデンティティサーバーを追加

手順に従って、Unified CCDM アイデンティティサーバーを手動で追加します。

手順

ステップ 1 **AD FS 管理コンソール** を開きます。

ステップ 2 **[信頼関係（Trust Relationships）]** > **[信頼当事者証明（Relying Party Trusts）]** の順に選択します。

ステップ 3 **[信頼当事者証明の追加（Add Relying Party Trusts）]** を追加したら、**[スタート（Start）]** をクリックします。

ステップ 4 **[信頼当事者に関するデータの手動入力（Enter data about the relying party manually）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 5 適切な表示名を入力し、**[次へ（Next）]** をクリックします。

例：

Unified CCDM アイデンティティサーバー

ステップ 6 **[AD FSプロファイル（AD FS profile）]** を選択して、**[次へ（Next）]** をクリックします。

ステップ 7 **[証明書の構成（Configure Certificate）]** 手順で、**[次へ（Next）]** をクリックします。

（注） Unified CCDM は、オプションのトークン暗号化証明書をサポートしていません。

ステップ 8 **[WS-Federationパッシブプロトコルのサポートを有効にする（Enable support for the WS-Federation Passive protocol）]** チェックボックスをオンにします。

ステップ 9 **[Relying Party WS-Federationパッシブプロトコル URL（Relying Party WS-Federation Passive Protocol URL）]** フィールドに、アイデンティティサーバー AD FS エンドポイントの次の URL を入力します。

```
https://<CCDM web server fqdn name>/identity/adfs
```

（注） URL は、AD FS の信頼できる SSL 証明書を使用する必要があります。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 **[信頼当事者証明識別子（Relying party trust identifier）]** ペインで、アイデンティティサーバーの次の URL を入力します。

```
https://<CCDM web server fqdn name>/identity
```

ステップ 12 **[追加（Add）]** > **[次へ（Next）]** の順に選択します。

ステップ 13 信頼当事者証明に対してマルチファクター認証設定を構成せずに、**[次へ（Next）]** をクリックします。

ステップ 14 **[この信頼当事者へのアクセスをすべてのユーザーに許可（Permit all user to access this relying trust party）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 15 設定を確認し、**[次へ（Next）]** をクリックし、信頼当事者証明を AD FS 構成データベースに追加します。

（注） 要求規則をすぐに編集するには、**[ウィザードを閉じる際にこの信頼当事者証明の要求規則の編集ダイアログボックスを開く（Open the Edit Claim Rules dialog for this relying party trust when the wizard closes）]** チェックボックスをオンにします。

ステップ 16 [閉じる（Close）] をクリックします。

ステップ 17 アイデンティティサーバーごとに手順を繰り返します。

要求規則の追加

Hosted AD FS の手順に従って、Unified CCDM の要求規則を以下のように追加します。

手順

ステップ 1 **[Unified CCDM トラスト（Unified CCDM trust）]** を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ 2 **発行変換ルール** タブで、**ルールの追加**をクリックします。

ステップ 3 **[要求規則テンプレート（Claim Rule Template）]** ドロップダウンリストで、**[要求としてLDAP属性を送信（Send LDAP Attributes as Claims）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 必要な要求を個別に追加します。

要求規則名（Claim Rule Name）	店舗	LDAP 属性	出力方向の要求の種類 （Outgoing Claim Type)	必須
AD：SID（NameID として）	Active Directory	objectSid（直接入力）	[名前ID（Name ID））]	はい
AD：名前としての UPN	Active Directory	User-Principal-Name	名前	○
AD：名	Active Directory	Given-Name	名	オプション
AD：姓	Active Directory	姓	姓	オプション
AD：E メール	Active Directory	E-Mail-Addresses	E-Mail-Address	オプション

重要　各要求規則の名前IDは一意である必要があります。したがって、常に名前IDとしてSIDを使用します。

ステップ5 [完了（Finish）] をクリックします。

ステップ6 **[規則の追加（Add Rule）]** をクリックし、**[着信要求の変換（Transform an Incoming Claim）]** を選択したら、[変換要求の追加（Add Transform Claim）] ウィザードを閉じます。

要求規則名 （Claim Rule Name）	着信要求タイプ	出力方向の要求の種類（Outgoing Claim Type)	必須
TFN：名前としてのWindowsアカウント名	Windowsアカウント名	名前	○

ステップ7 要求規則を追加後、**[完了（Finish）]** をクリックします。

自動ユーザープロビジョニング

これは、ユーザーをプロビジョニングするための代替手順です。

手順

ステップ1 **[Unified CCDMトラスト（Unified CCDM trust）]** を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ2 **発行変換ルール** タブで、**ルールの追加**をクリックします。

ステップ3 要求規則テンプレートとして **[要求としてグループメンバーシップを送信（Send Group Membership as a Claim）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ4 以下の要求規則を追加します。

要求規則名 （Claim Rule Name）	ユーザーのグループ	出力方向の要求の種類（Outgoing Claim Type)	出力方向の要求の値
AD：ロール＝スーパーバイザ	<windows group>	ロール	スーパーバイザ
AD：ロール＝上級	<windows group>	ロール	Advanced

ステップ5 要求規則を追加後、**[完了（Finish）]** をクリックします。

AD FS の設定

手順

ステップ 1 **AD FS 管理コンソール** を開きます。

ステップ 2 **[信頼関係（Trust Relationships）]** > **[要求プロバイダの信頼（Claim Provider Trusts）]** の順に選択します。

ステップ 3 **[Active Directory]** > **[要求規則の編集（Edit Claim Rules）]** の順に選択します。

ステップ 4 **[Active Directoryの要求規則を編集（Edit Claim Rules for Active Directory）]** ダイアログボックスで、**[規則の追加（Add Rule）]** をクリックします。

ステップ 5 **[要求規則テンプレート（Claim Rule Template）]** ドロップダウンリストで、**[要求としてLDAP属性を送信（Send LDAP Attributes as Claims）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 6 **[要求規則名（Claim Rule Name）]** フィールドに、Pass-thru DN と入力します。

ステップ 7 **[属性ストア（Attribute Store）]** ドロップダウンリストで、**[Active Directory]** を選択します。

ステップ 8 LDAP 属性を進行中の要求タイプにマッピングします。

LDAP Attribute (Select or type or add more) 列に、**`distinguishedname`** と入力します。**Ongoing Claim Type (Select or type or add more)** 列に **`http://temp.org/claims/DistinguishedName`** と入力します。

ステップ 9 **[完了（Finsh）]** > **[OK]** の順に選択し、サーバーを再起動します。

AD FS にテナントをマッピング

手順

ステップ 1 **[Unified CCDMトラスト（Unified CCDM trust）]** を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ 2 **発行変換ルール** タブで、**ルールの追加**をクリックします。

ステップ 3 **[変換要求規則ウィザードの追加（Add Transform Claim Rule Wizard）]** ウィンドウで、**[カスタム規則を使用して要求を送信（Send Claims Using a Custom Rule）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 要求規則名を入力します。

要求規則名の形式：`AD: Tenant(<TenantPath>)`

ステップ 5 次のカスタム規則テキストを入力します。

```
c:[Type == "http://temp.org/claims/DistinguishedName", Value =~ "^.*()$"]
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "/");
```

例：

```
c:[Type == "http://temp.org/claims/DistinguishedName", Value =~ "^.*()$"]
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "qacce");
```

ステップ 6 **[完了（Finish）]** をクリックします。

フェデレーションシナリオの AD FS の構成

（注） Hosted AD FS と Customer AD FS の間にフェデレーション信頼を作成します。

信頼当事者証明に対する要求規則の追加

（注） Customer AD FS にの頼当事者証明の要求規則を追加します。

手順

ステップ 1 Customer AD FS で信頼当事者証明を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ 2 **発行変換ルール** タブで、**ルールの追加**をクリックします。

ステップ 3 **[要求規則テンプレート（Claim Rule Template）]** ドロップダウンリストで、**[要求としてLDAP属性を送信（Send LDAP Attributes as Claims）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 必要な要求を個別に追加します。

要求規則名（Claim Rule Name）	店舗	LDAP 属性	出力方向の要求の種類 （Outgoing Claim Type)	必須
AD：プライマリ SID としての SID	Active Directory	objectSid（直接入力）	プライマリ SID	はい
AD：名前としての UPN	Active Directory	User-Principal-Name	名前	○
AD：名	Active Directory	Given-Name	名	オプション
AD：姓	Active Directory	姓	姓	オプション
AD：E メール	Active Directory	E-Mail-Addresses	E-Mail-Address	オプション

重要 各要求規則の名前 ID は一意である必要があります。したがって、常に名前 ID として SID を使用します。

ステップ 5 [完了（Finish）] をクリックします。

ステップ 6 **[要求規則テンプレート（Claim Rule Template）]** ドロップダウンリストで別の規則を追加し、**[パススルーまたは着信要求のフィルタ処理（Pass Through or Filter an Incoming Claim）]** > **[次へ（Next）]** の順に選択します。

要求規則名 （Claim Rule Name）	着信要求タイプ	すべての要求値をパススルー	必須
AD：Windows アカウント名	Windows アカウント名	はい	はい

ステップ 7 要求規則を追加後、**[完了（Finish）]** をクリックします。

自動ユーザープロビジョニング

これは、ユーザーをプロビジョニングするための代替手順です。

手順

ステップ 1 Customer AD FS で信頼当事者証明を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ 2 **発行変換ルール** タブで、**ルールの追加**をクリックします。

ステップ 3 要求規則テンプレートとして **[要求としてグループメンバーシップを送信（Send Group Membership as a Claim）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 以下の要求規則を追加します。

要求規則名 （Claim Rule Name）	ユーザーのグループ	出力方向の要求の種類（Outgoing Claim Type）	出力方向の要求の値
AD：ロール = スーパーバイザ	<windows group>	ロール	スーパーバイザ
AD：ロール = 上級	<windows group>	ロール	Advanced

ステップ 5 要求規則を追加後、**[完了（Finish）]** をクリックします。

要求プロバイダ信頼の要求規則の追加

（注） Hosted AD FS の要求プロバイダ信頼の要求規則を追加します。

手順

ステップ 1 Hosted AD FS で [要求プロバイダトラスト（Claims provider trust）] を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ 2 **[承諾変換規則（Acceptance Transform Rules）]** タブで、**[規則の追加（Add Rule）]** をクリックします。

ステップ 3 **[トランスフォーム要求規則の追加ウィザード（Add Transform Claim Rule Wizard）]** ウィンドウで、**[パススルーまたは着信要求のフィルタ処理（Pass Through or Filter an Incoming Claim）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 必要な要求規則を個別に追加します。

要求規則名 （**Claim Rule Name**）	着信要求タイプ	すべての要求値をパススルー	必須
SID	プライマリSID	はい	はい
名前	名前	はい	はい
名	名	はい	オプション
姓	姓	はい	オプション
EmailAddress	E-Mail-Address	はい	オプション
Windowsアカウント名	Windowsアカウント名	はい	オプション
[名前ID（Name ID）]	[名前ID（Name ID）]	はい	オプション

重要
- 各要求規則の名前IDは一意である必要があります。したがって、常に名前IDとしてSIDを使用します。
- Windowsアカウント名要求の場合は、**[特定の値で始まる要求値のみをパススルーする（Pass through only Claim values from start with a specific value）]** を選択します。

ステップ 5 要求を設定したら、**[完了（Finish）]** をクリックします。

自動ユーザープロビジョニング

これは、ユーザーをプロビジョニングするための代替手順です。

手順

ステップ 1 Hosted AD FS で [要求プロバイダトラスト（Claims provider trust）] を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ 2 **[承諾変換規則（Acceptance Transform Rules）]** タブで、**[規則の追加（Add Rule）]** をクリックします。

ステップ 3 **[トランスフォーム要求規則の追加ウィザード（Add Transform Claim Rule Wizard）]** ウィンドウで、**[パススルーまたは着信要求のフィルタ処理（Pass Through or Filter an Incoming Claim）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 以下の要求規則を追加します。

要求規則名 （**Claim Rule Name**）	着信要求タイプ	特定の要求値のみをパススルーの選択	受信要求値
Role = 上級	ロール	はい	詳細
ロール= スーパーバイザ	ロール	はい	スーパーバイザ

ステップ 5 カスタム規則を作成するには、要求規則テンプレートとして、**[カスタム規則を使用して要求を送信（Send Claims Using a Custom Rule）]** を選択し、**[次へ（Next）]** をクリックします。

- 要求規則名を入力します。
- 以下の形式でカスタム規則を入力します。

```
=> issue(Type = "http://egain.net/claims/identity/tenant", Value = "/<tenantname>",
 Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"]
 = "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified");
```

ステップ 6 要求規則を追加後、**[完了（Finish）]** をクリックします。

要求を通過するパスの追加

（注） Hosted AD FS の信頼当事者証明の要求規則を追加します。

手順

ステップ 1 [Hosted AD FS] で [信頼当事者証明（Relying party trust）] を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ 2 **発行変換ルール** タブで、**ルールの追加**をクリックします。

ステップ 3 **[変換要求規則の追加ウィザード（Add Transform Claim Rule Wizard）]** ウィンドウで、**[着信要求の変換（Transform an Incoming Claim）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 必要な要求規則を個別に追加します。

要求規則名 （Claim Rule Name）	着信要求タイプ	出力方向の要求の種類（Outgoing Claim Type)	必須
フェデレーション：名前 ID としてプライマリ SID を変換	プライマリSID	[名前ID（Name ID））]	はい

ステップ 5 **[トランスフォーム要求規則の追加ウィザード（Add Transform Claim Rule Wizard）]** ウィンドウで、**[パススルーまたは着信要求のフィルタ処理（Pass Through or Filter an Incoming Claim）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 6 必要な要求規則を個別に追加します。

要求規則名 （Claim Rule Name）	着信要求タイプ	すべての要求値をパススルー	必須
名前	名前	はい	はい
名	名	はい	オプション
姓	姓	はい	オプション
EmailAddress	E-Mail-Address	はい	オプション
Windows アカウント名	Windows アカウント名	はい	オプション
[名前ID（Name ID））]	[名前ID（Name ID））]	はい	オプション

重要
- 各要求規則の名前 ID は一意である必要があります。したがって、常に名前 ID として SID を使用します。
- Windows アカウント名要求の場合は、**[特定の値で始まる要求値のみをパススルーする（Pass through only Claim values from start with a specific value）]** を選択します。

ステップ 7 要求を設定したら、**[完了（Finish）]** をクリックします。

自動ユーザープロビジョニング

これは、ユーザーをプロビジョニングするための代替手順です。

手順

ステップ 1 [Hosted AD FS] で [信頼当事者証明（Relying party trust）] を選択し、**[要求規則の編集（Edit Claim Rules）]** をクリックします。

ステップ 2 **発行変換ルール** タブで、**ルールの追加**をクリックします。

ステップ 3 **[トランスフォーム要求規則の追加ウィザード（Add Transform Claim Rule Wizard）]** ウィンドウで、**[パススルーまたは着信要求のフィルタ処理（Pass Through or Filter an Incoming Claim）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 以下の要求規則を追加します。

要求規則名 （Claim Rule Name）	着信要求タイプ	特定の要求値をパススルーする	受信要求値
Role = 上級	ロール	はい	詳細
ロール = スーパーバイザ	ロール	はい	スーパーバイザ

ステップ 5 カスタム規則を作成するには、要求規則テンプレートとして、**[カスタム規則を使用して要求を送信（Send Claims Using a Custom Rule）]** を選択し、**[次へ（Next）]** をクリックします。

- 要求規則名を入力します。
- 以下の形式でカスタム規則を入力します。

```
c:[Type == "http://egain.net/claims/identity/tenant"]=> issue(claim = c);
```

ステップ 6 要求規則を追加後、**[完了（Finish）]** をクリックします。

Cisco UCDM 統合

Unified Communication Domain Manager の基本構成

顧客の追加

手順

ステップ 1 プロバイダまたはリセラー管理者として Cisco Unified Communications Domain Manager にログインします。

ステップ 2 階層パスが適切なレベルに設定されていることを確認します。

（注） プロバイダとリセラーの両方にカスタマーを追加できます。プロバイダの配下にカスタマーを追加するには、プロバイダとしてログインします。リセラーの配下にカスタマーを追加するには、プロバイダまたはリセラーとしてログインします。

ステップ 3 **[カスタマー管理（Customer Management）]** > **[カスタマー（Customer）]** の順に選択します。

ステップ 4 必要な詳細を以下に入力します。

a) **名前**を入力します。
b) **説明**を入力します。
c) **ドメイン名**を入力します。
d) **[ローカル管理者を作成（Create Local Admin）]** チェックボックスをオンにします。
e) **[Adminロールのクローン（Clone Admin role）]** および **[デフォルトのAdminロール（Default Admin Role）]** はデフォルト値のままにします。
f) **デフォルトの管理者パスワード**を入力して、**[パスワードの確認（Confirm Password）]** テキストボックスで確認します。

ステップ 5 [保存（Save）] をクリックします。

（注） カスタマーを削除し、Unified Communication Manager の構成を保持する場合は、「UCDM から Unified Communication Manager の関連付けを解除 （309 ページ）」を参照してください。

Cisco Unified Communication Manager サーバーの設定

手順

ステップ 1 プロバイダ、リセラーまたはカスタマー管理者として Cisco Unified Communications Domain Manager にログインします。

ステップ 2 階層パスが適切なレベルに設定されていることを確認します。

（注） 共有インスタンスはプロバイダまたはリセラーレベルで作成し、専用インスタンスはカスタマーレベルで作成する必要があります。

ステップ 3 **[デバイス管理（Device Management）]** > **[CUCM]** > **[サーバー（Server）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **Cisco Unified Communications Manager サーバー名** を入力します。

ステップ 6 パブリッシャノードを構成するには、**[パブリッシャ（Publisher）]** チェックボックスをオンにします。

ステップ 7 **[クラスタ名（Cluster Name）]** を入力します。

（注） **[パブリッシャ（Publisher）]** チェックボックスをオフにし、ドロップダウンリストで **[クラスタ名（Cluster Name）]** を選択してサブスクライバノードを統合します。

ステップ 8 **[ネットワークアドレス（Network Address）]** タブで、以下の手順を実行します。

a) **[アドレス空間（Address Space）]** ドロップダウンリストで**[Service_Provider_Space]** を選択します。

b) **[IPV4アドレス（IPV4 Address）]** フィールドに Cisco Unified Communications Manager の IP アドレスを入力します。

c) **ホスト名** を入力します。デフォルトのホスト名は、Cisco Unified Communications Manager サーバー名です。

d) **ドメイン**を入力します。

e) **説明**を入力します。

ステップ 9 **[ログイン情報（Credentials）]** タブで以下の手順を実行します。

a) **[ログイン情報タイプ（Credential Type）]** ドロップダウンリストで、**Admin** を選択します。

b) **[ユーザーID（User ID）]** テキストボックスに Cisco Unified Communications Manager ユーザー ID を入力します。

c) **[パスワード（Password）]** テキストボックスに、Cisco Unified Communications Manager のパスワードを入力します。

d) **[アクセスタイプ（Access Type）]** ドロップダウンリストで適切なアクセスタイプを選択します。

e) **説明**を入力します。

ステップ 10 [保存（Save）] をクリックします。

ネットワークデバイスリストの構成

手順

ステップ 1 プロバイダまたはリセラー管理者として Cisco Unified Communications Domain Manager にログインします。

ステップ 2 **[カスタマー管理（Customer Management）]** > **[ネットワークデバイスリスト（Network Device Lists）]** の順に選択します。階層ツリーから特定のカスタマーを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **ネットワークデバイスリスト名**を入力します。

ステップ 5 ネットワークデバイスリストの**説明**を入力します。

ステップ 6 デフォルトでは、HCM-F の IP アドレスは、**[Cisco HCM-F]** ドロップダウンリストで選択されます。

ステップ 7 **[Cisco Unified CM]** タブを展開し、ドロップダウンリストで **[cisco unified communication manager]** インスタンスを選択します。

ステップ 8 [保存（Save）] をクリックします。

サイトの追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communications Domain Manager にログインします。

ステップ 2 階層パスが適切なレベルに設定されていることを確認します。

ステップ 3 **[拠点管理（Site Management）]** > **[拠点（Sites）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 必要な詳細を以下に入力します。

a) **拠点名**を入力します。
b) **説明**を入力します。
c) **[ローカル管理者を作成（Create Local Admin）]** チェックボックスをオンにします。
d) **デフォルトの管理者パスワード**を入力して、**[パスワードの確認（Confirm Password）]** テキストボックスで確認します。
e) ドロップダウンリストで **[国（Country）]** を選択します。
f) ドロップダウンリストで、**[ネットワークデバイスリスト（Network Device List）]** を選択します。

ステップ 6 [保存（Save）] をクリックします。

（注） Small Contact Centers 専用オプションでは、サブカスタマーに対して、UCDM で 1 人のお客様とお客様ごとに 1 つの拠点が作成されますSmall Contact Center の共有オプションでは、UCDM の 1人のお客様と 1 つの拠点が複数のサブカスタマーで共有されます。

カスタマーダイヤルプランの追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なカスタマーレベルに設定されていることを確認します。

ステップ 3 **[ダイヤルプラン管理（Dial Plan Management）]** > **[カスタマー（Customer）]** > **[ダイヤルプラン（Dial Plan）]** の順に選択します。

ステップ 4 **[追加（Add）]** をクリックします。

ステップ 5 [保存（Save）] をクリックします。

（注）
- カスタマー ID はカスタマーに割り当てられた、固有で、自動生成され、読み取り専用の数字です。
- 拠点のロケーションコードが指定されていない場合、ダイヤルプランタイプはデフォルトで Type_4 に設定されます

サイトダイヤルプランの追加

始める前に

カスタマーダイヤルプランが作成されていることを確認します。「カスタマーダイヤルプランの追加 （191 ページ）」を参照してください。

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なサイトに設定されていることを確認します。

ステップ 3 **[ダイヤルプラン管理（Dial Plan Management）]** > **[拠点（Site）]** > **[管理（Management）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **[内線番号の長さ（Extension Length）]** 値は、1 ～ 11 です。

ステップ 6 [保存（Save）] をクリックします。

拠点情報は、Cisco Unified Communications Manager にロードされ、カスタマー ID、拠点 ID のプレフィックスを使用して識別できます。

（注）　拠点ダイヤルプランをプロビジョニングするには、数分かかります。

ASA 統合

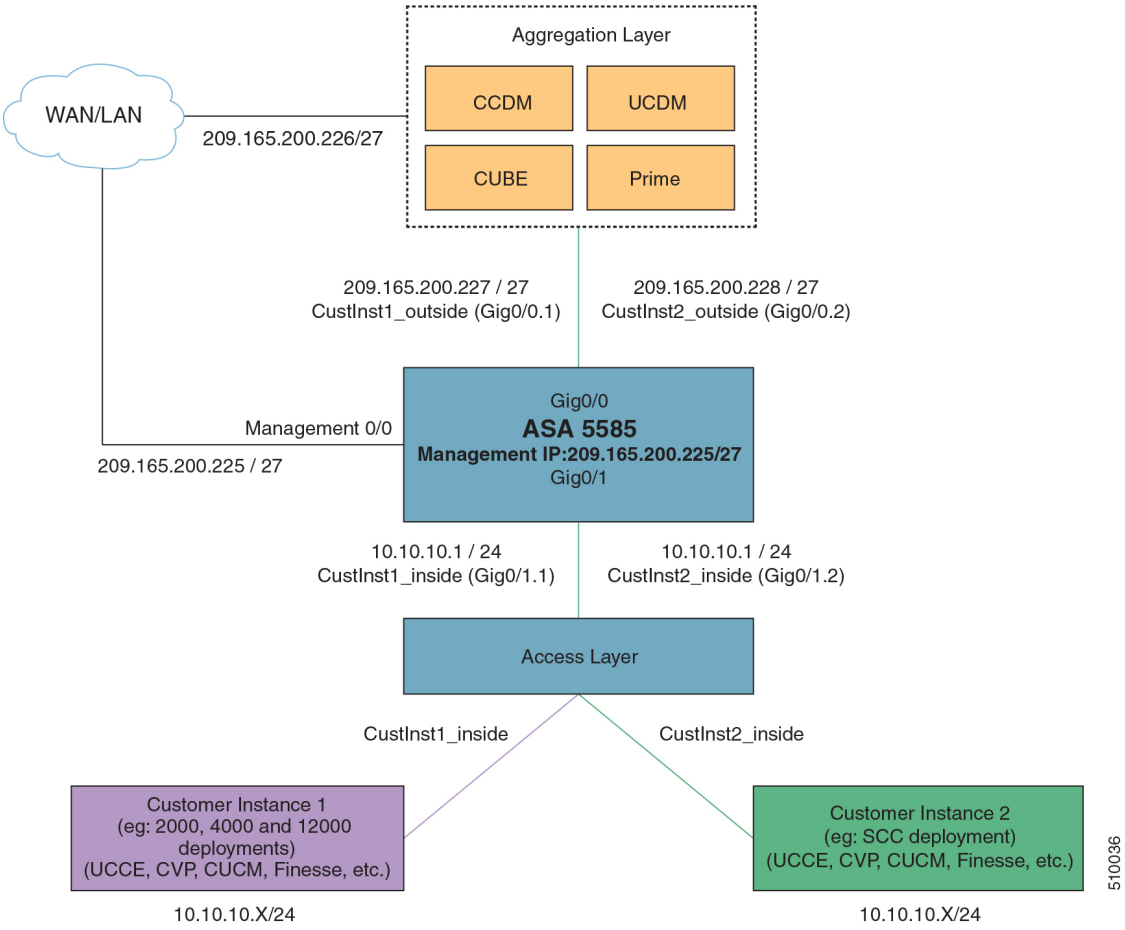
この項では、すべてのタイプの HCS for CC 展開用カスタマーインスタンスを統合するために Cisco ASA で必要な構成手順について説明します。

• HCS for CC 導入モデルの ASA の統合 （192 ページ）
• Small Contact Center 導入モデル用 ASA の統合 （198 ページ）

HCS for CC 導入モデルの ASA の統合

2000、4000、および12000エージェント導入モデルの場合、カスタマーインスタンス コンポーネントと共有コンポーネントを統合するために Cisco ASA で以下の構成が必要です。次の図は、単一 ASA でのさまざまなタイプの展開を示しています。

図 *6* : 共有コンポーネントと統合された *2* つの異なる展開タイプのカスタマーインスタンス



カスタマーインスタンスごとに ASA を統合するには、以下の手順を繰り返します。各カスタマーインスタンスに必要な VLAN ID とサブインターフェイス ID は異なります。したがって、IP アドレスはこれらの展開に再利用できます。

- System Execution Space でインターフェイスを構成 （194 ページ）
- セキュリティコンテキストの構成 （195 ページ）
- カスタマー インスタンス コンテキストでインターフェイスを構成 （195 ページ）
- カスタマー インスタンス コンテキストでアクセスリストを構成 （196 ページ）
- カスタマー インスタンス コンテキストで NAT を構成 （196 ページ）

System Execution Space でインターフェイスを構成

手順

ステップ 1 グローバル構成モードに移動します。

```
hostname/context_name#changeto system
hostname#configure terminal
hostname(config)#
```

ステップ 2 GigabitEthernet 0/1 のインターフェイスに移動し、以下のコマンドを入力します。

```
hostname(config)#interface gigabitethernet 0/1
hostname(config-if)#no shut
```

ステップ 3 サブインターフェイスに移動し、次のコマンドを入力して、customer_instance 内の customer_instance コンテキストと vlan ID にサブインターフェイスを割り当てます。

```
hostname(config-if)#interface GigabitEthernet0/1.X
hostname(config-if)#vlan x
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.X
hostname(config-if)#vlan x
hostname(config-if)#no shut
```

ステップ 4 上記の手順を繰り返して、各 カスタマーインスタンスにサブインターフェイスを割り当てます。

例：

2000 エージェント カスタマー インスタンスの場合：

```
hostname(config)#interface  Gigabit Ethernet 0/1
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/1.1
hostname(config-if)#vlan 2
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.1
hostname(config-if)#vlan 340
hostname(config-if)#no shut
```

4000 エージェント カスタマー インスタンスの場合：

```
hostname(config-if)#interface GigabitEthernet0/1.2
hostname(config-if)#vlan 4
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.2
hostname(config-if)#vlan 341
hostname(config-if)#no shut
```

セキュリティコンテキストの構成

手順

ステップ 1 システム実行スペースで customer_instance コンテキストを作成します。

```
hostname(config)#context customer_instance
```

ステップ 2 customer_instance コンテキスト定義を構成します。

```
hostname(config-ctx)#description customer_instance context (optional)
hostname(config-ctx)#allocate-interface GigabitEthernet0/1.1 cust_inside invisible
hostname(config-ctx)#allocate-interface GigabitEthernet0/0.1 cust_outside invisible
hostname(config-ctx)#config-url disk0:/ customer_instance.cfg
```

カスタマー インスタンス コンテキストでインターフェイスを構成

手順

ステップ 1 customer_instance コンテキスト構成モードに移動します。

```
hostname#changeto context customer_instance
hostname/customer_instance#configure  terminal
hostname/customer_instance(config)#
```

ステップ 2 カスタマーインスタンスのインターフェイスを構成します。

a) cust_inside のインターフェイスに移動します。

```
hostname/customer_instance(config)#interface gigabitethernet0/1.1
```

b) customer_instance コンテキストの内部インターフェイスに名前を付けます

```
hostname/customer_instance(config-if)#nameif inside_if_name
```

c) 内部インターフェイスの customer_instance の IP アドレスを入力します

```
hostname/customer_instance(config-if)#ip address ip_address subnet_mask
```

d) cust_outside のインターフェイスに移動します。

```
hostname/customer_instance(config-if)#interface gigabitethernet0/0.1
```

e) customer_instance コンテキストの外部インターフェイスに名前を付けます。

```
hostname/customer_instance(config-if)#nameif outside_if_name
```

f) 外部インターフェイスの customer_instance の IP アドレスを入力します

```
hostname/customer_instance(config-if)#ip address ip_address subnet_mask
```

例：

```
hostname#changeto context 2000deployment
hostname/2000deployment#configure terminal
hostname/2000deployment(config)#interface gigabitethernet0/1.1
```

```
hostname/2000deployment(config-if)#nameif inside
hostname/2000deployment(config-if)#ip address 10.10.10.1 255.255.255.0
hostname/2000deployment(config-if)#interface gigabitethernet0/0.1
hostname/2000deployment(config-if)#nameif outside
hostname/2000deployment(config-if)#ip address 209.165.200.227 255.255.255.224
hostname/2000deployment(config-if)#exit
hostname/2000deployment(config)#exit
hostname/2000deployment#changeto context 4000deployment
hostname/4000deployment#configure terminal
hostname/4000deployment(config)#interface gigabitethernet0/1.2
hostname/4000deployment(config-if)#nameif inside
hostname/4000deployment(config-if)#ip address 10.10.10.1 255.255.255.0
hostname/4000deployment(config-if)#interface gigabitethernet0/0.2
hostname/4000deployment(config-if)#nameif outside
hostname/4000deployment(config-if)#ip address 209.165.200.228 255.255.255.224
```

カスタマー インスタンス コンテキストでアクセスリストを構成

IP トラフィックを許可するようにアクセスリストを構成します。access-list は外部インターフェイスおよび内部インターフェイスの両方に適用されます。

手順

ステップ 1 外部および内部 IP トラフィック用のアクセスリストを作成します。

```
hostname/customer_instance(config)#access-list access_list_name_outside extended permit
 ip any any
hostname/customer_instance(config)#access-list access_list_name_inside extended permit
ip any any
```

ステップ 2 外部および内部 IP トラフィックの両方にアクセスリストを適用します。

```
hostname/customer_instance(config)#access-group access_list_name_outside in interface
outside_if_name
hostname/customer_instance(config)#access-group access_list_name_inside in interface
inside_if_name
```

（注） ネットワークの要件に応じて、access-list の IP アドレスを許可または拒否します。

カスタマー インスタンス コンテキストで NAT を構成

手順

ステップ 1 内部ホストのインターネット接続を有効にするように NAT を構成します。

a) カスタマーインスタンスの内部ネットワーク用のネットワークオブジェクトを作成します。

```
hostname/customer_instance(config)#object network inside_network_name
```

b) サブネットマスクがある内部ネットワークに **network id** を入力します。

```
hostname/customer_instance(config-network-object)#subnet network-id subnet-mask
```

c) 内部ネットワークのダイナミック NAT をイネーブルにします。

```
hostname/customer_instance(config-network-object)#nat (inside,outside) dynamic
interface
```

例：

```
hostname/customer_instance(config)#object network my-inside-net
hostname/customer_instance(config-network-object)#subnet 10.10.10.0 255.255.255.0
hostname/customer_instance(config-network-object)#nat (inside, outside) dynamic interface
```

ステップ 2 AW A と B で動作するように、CCDM の customer_instance の静的アドレス変換を構成します。

a) AW-A サーバーアドレスのネットワークオブジェクトを作成します。

```
hostname/customer_instance(config)#object network DATASERVER-A
```

b) AW-A サーバーアドレスを定義して、アイデンティティ ポート変換がある静的 NAT を構成します。

```
hostname/customer_instance(config-network-object)#host 10.10.10.21
```

c) AW-A の SQL ポートを開きます。

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.230 service tcp 1433 1433
```

d) AW-A の ConAPI ポートを開きます。

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.230 service tcp 2094 2094
```

e) AW-A の HTTPS ポートを開きます。

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.230
service tcp 443 443
```

f) AW-B の SQL ポートを開きます。

```
hostname/customer_instance(config)#object network DATASERVER-B
hostname/customer_instance(config-network-object)#host 10.10.10.22
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.231 service tcp 1433 1433
```

g) AW-B の ConAPI ポートを開きます。

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.231 service tcp 2095 2095
```

h) AW-B の HTTPS ポートを開きます。

```
hostname/customer_instance(config-network-object)#nat (inside,outside) static
209.165.200.231 service tcp 443 443 hostname/customer_instance (config)#route outside
 0.0.0.0 0.0.0.0 209.165.200.240
```

（注） AW A および B の ConAPI ポートは、CCDM クラスタで構成されたポートと一致する必要があります。

ポートの詳細については、『*Hosted Collaboration Solution for Contact Center* 用 ソリューション設計 http://www.cisco.com/c/en/us/support/unified-communications/

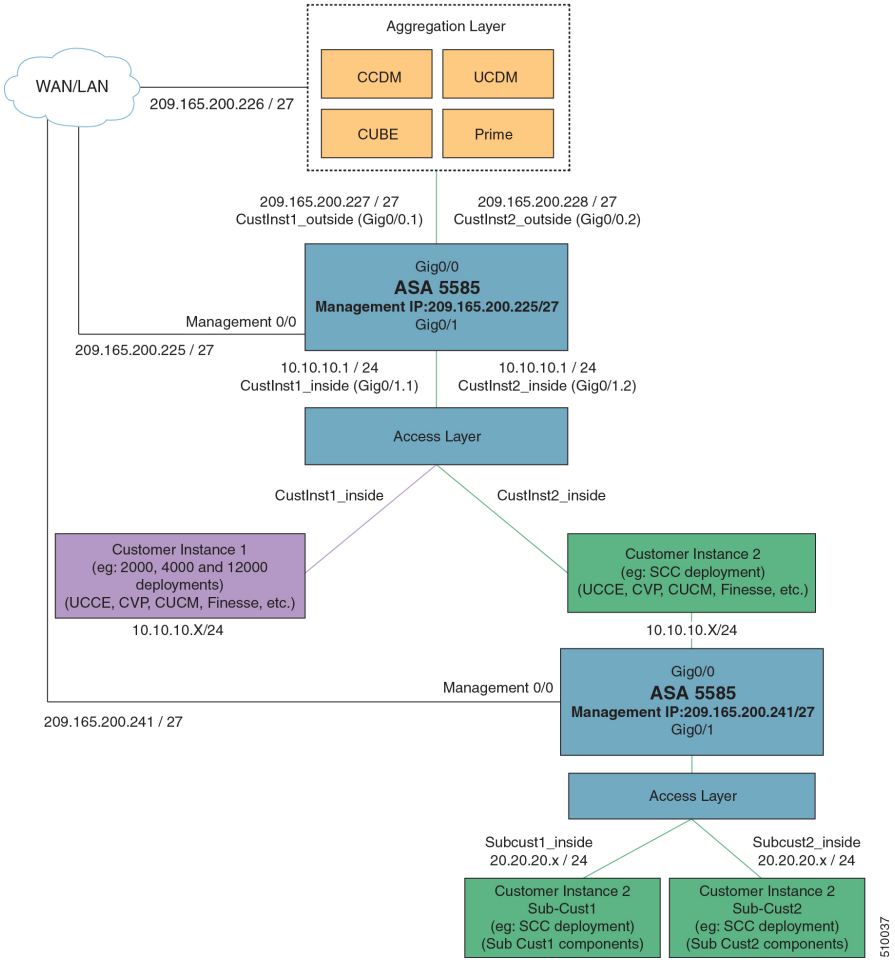
hosted-collaboration-solution-contact-center/products-installation-guides-list.html』の「ホストベースのファイアウォール」セクションを参照してください。NAT を実行し、それぞれのコンテキストの特定のポートを構成します。

Small Contact Center 導入モデル用 ASA の統合

Small Contact Center 導入モデルには、Small Contact Center カスタマーインスタンスを共有コンポーネントに統合する ASA と、サブカスタマーインスタンスを Small Contact Center インスタンスに統合する ASA の 2 つの ASA が必要です。

次の図は、2 つの Cisco ASA を使用した 2000、4000、12000 エージェントと Small Contact Center インスタンスの展開に関して示しています。

図 *7*: 共有コンポーネントと統合された *Small Contact Center* モデル用の *2* つのカスタマーインスタンス



Small Contact Center 用 ASA を共有コンポーネントに統合し、Small Contact Center カスタマーインスタンス用 ASA をサブカスタマーインスタンスに統合します。ASA のインストールおよび

構成に関する詳細は、http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html の『*Cisco Hosted Collaboration Solution for Contact Center* 用インストールおよびアップグレードガイド』の「*ASA* ファイアウォールおよび *NAT* のインストールおよび構成」項を参照してください。

ASA のインストール後、サブカスタマーインスタンスごとに次の手順を繰り返します。サブカスタマーインスタンスに必要な VLAN ID とサブインターフェイス ID は異なります。したがって、IP アドレスはこれらの展開に再利用できます。

- System Execution Space でインターフェイスを構成 （199 ページ）
- 各サブカスタマーコンテキストのセキュリティコンテキストの構成 （200 ページ）
- 各サブカスタマー インスタンス コンテキストでインターフェイスを構成 （200 ページ）
- サブカスタマー インスタンス コンテキストでアクセスリストを構成 （201 ページ）
- サブカスタマー インスタンス コンテキストで静的 NAT を構成 （202 ページ）

System Execution Space でインターフェイスを構成

手順

ステップ 1 グローバル構成モードに移動します。

```
hostname/context_name# changeto system
hostname# configure terminal
hostname(config)#
```

ステップ 2 GigabitEthernet 0/1 のインターフェイスに移動し、以下のコマンドを入力します。

```
hostname(config)#interface gigabitethernet 0/1
hostname(config-if)#no shut
```

ステップ 3 sub-interface に移動し、以下のコマンドを入力し、sub-interface を sub-customer_instance 配下の sub-customer_instance と vlan ID に割り当てます。

```
hostname(config-if)#interface GigabitEthernet0/1.X
hostname(config-if)#vlan x
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.X
hostname(config-if)#vlan x
hostname(config-if)#no shut
```

ステップ 4 上記の手順を繰り返して、各サブカスタマーインスタンスにサブインターフェイスを割り当てます。

例：

sub-cust1 の場合

```
hostname(config)#interface  gigabitethernet0/1
hostname(config-if)#No shut
```

```
hostname(config-if)#interface gigabitethernet0/1.1
hostname(config-if)#vlan 10
hostname(config-if)#no shut

hostname(config-if)#interface GigabitEthernet0/0.1
hostname(config-if)#vlan 11
hostname(config-if)#no shut
```

sub-cust2 の場合

```
hostname(config-if)#interface gigabitethernet0/1.2
hostname(config-if)#vlan 20
hostname(config-if)#no shut

hostname(config-if)#interface gigabitethernet0/0.2
hostname(config-if)#vlan 21
hostname(config-if)#no shut
```

各サブカスタマーコンテキストのセキュリティコンテキストの構成

手順

ステップ 1 システム実行スペースで sub-customer_instance コンテキストを作成します。

```
hostname(config)#context sub-customer_instance
```

ステップ 2 customer_instance コンテキスト定義を構成します。

```
hostname(config-ctx)#description sub-customer_instance context (optional)
hostname(config-ctx)#allocate-interface GigabitEthernet0/1.1 subcustX_inside invisible
hostname(config-ctx)#allocate-interface GigabitEthernet0/0.1 subcustX_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-customer_instance.cfg
```

例：

```
hostname/admin#changeto system
hostname#configure terminal
hostname(config)#context sub-cust1
hostname(config-ctx)#description sub-customer_1 context
hostname(config-ctx)#allocate-interface gigabitethernet0/1.1 sub-cust1_inside invisible
hostname(config-ctx)#allocate-interface gigabitethernet0/0.1 sub-cust1_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-cust1.cfg
hostname(config-ctx)#context sub-cust2
hostname(config-ctx)#description sub-customer_2 context
hostname(config-ctx)#allocate-interface gigabitethernet0/1.2 sub-cust2_inside invisible
hostname(config-ctx)#allocate-interface gigabitethernet0/0.2 sub-cust2_outside invisible
hostname(config-ctx)#config-url disk0:/ sub-cust2.cfg
```

各サブカスタマー インスタンス コンテキストでインターフェイスを構成

手順

ステップ 1 sub-customer_instance コンテキスト構成モードに移動します。

```
hostname#changeto context sub_customer_instance_name
hostname/sub_customer_instance#configure  terminal
hostname/sub_customer_instance (config)#
```

ステップ 2 sub-customer インスタンスのインターフェイスを構成します。

a) sub-cust_inside のインターフェイスに移動します。

```
hostname/sub_customer_instance (config)#interface gigabitethernet0/1.1
```

b) sub-customer_instance コンテキストの内部インターフェイスに名前を指定します。

```
hostname/sub_customer_instance (config-if)#nameif inside_if_name
```

c) 内部インターフェイスの sub-customer_instance の IP アドレスを入力します

```
hostname/sub_customer_instance (config-if)#ip address ip_address subnet_mask
```

d) sub-cust_outside のインターフェイスに移動します。

```
hostname/sub_customer_instance (config-if)#interface gigabitethernet0/0.1
```

e) sub-customer_instance コンテキストの外部インターフェイスに名前を指定します。

```
hostname/sub_customer_instance (config-if)#nameif outside_if_name
```

f) 外部インターフェイスの sub-customer_instance の IP アドレスを入力します。

```
hostname/sub_customer_instance (config-if)#ip address ip_address subnet_mask
```

例：

```
hostname#changeto context sub-cust1
hostname/sub-cust1#configure terminal
hostname/sub_cust1(config)#interface sub-cust1_inside
hostname/sub_cust1(config-if)#nameif inside
hostname/sub_cust1(config-if)#ip address 20.20.20.1 255.255.255.0
hostname/sub_cust1(config-if)#interface sub-cust1_outside
hostname/sub_cust1(config-if)#nameif outside
hostname/sub_cust1(config-if)#ip address 10.10.10.254 255.255.255.0
hostname/sub_cust1(config)#interface sub-cust2_inside
hostname/sub_cust1(config-if)#nameif inside
hostname/sub_cust1(config-if)#ip address 20.20.20.1 255.255.255.0
hostname/sub_cust1(config-if)#interface sub-cust2_outside
hostname/sub_cust1(config-if)#nameif outside
hostname/sub_cust1(config-if)#ip address 10.10.10.254 255.255.255.0
```

サブカスタマー インスタンス コンテキストでアクセスリストを構成

IP トラフィックを許可するようにアクセスリストを構成します。access-list は外部インターフェイスおよび内部インターフェイスの両方に適用されます。

手順

ステップ 1 外部および内部 IP トラフィック用のアクセスリストを作成します。

```
hostname/sub_customer_instance(config)#access-list access_list_name_outside extended
permit ip any any
```

```
hostname/sub_customer_instance(config)#access-list access_list_name_inside extended
permit ip any any
```

ステップ 2 外部および内部 IP トラフィックの両方にアクセスリストを適用します。

```
hostname/sub_customer_instance(config)#access-group access_list_name_outside in interface
 outside_if_name
hostname/sub_customer_instance(config)#access-group access_list_name_inside in interface
 inside_if_name
```

（注） ネットワークの要件に応じて、access-list の IP アドレスを許可または拒否します。

サブカスタマー インスタンス コンテキストで静的 NAT を構成

サブカスタマーインスタンスとカスタマーインスタンスを統合するための静的 NAT を構成するには、以下の手順を実行します。

手順

ステップ 1 sub_cust1 サイド A のネットワークオブジェクトを作成します。

```
hostname/sub_customer_instance(config)#object network sub_cust_host
```

ステップ 2 ホスト IP アドレスを定義し、静的 NAT を構成します。

```
hostname/sub_customer_instance(config-network-object)#host X.X.X.X
```

ステップ 3 外部 IP アドレスを定義します。

```
hostname/customer_instance(config-network-object)#nat (inside_if_name, outside_if_name)
 static X.X.X.X
```

例：

```
hostname/sub-cust1(config)# object network sub-cust1APGA
hostname/sub-cust1(config-network-object)# host 20.20.20.21
hostname/sub-cust1 (config-network-object)# nat(inside,outside) static 10.10.10.121
```

ポートの詳細については、『*Hosted Collaboration Solution for Contact Center* 用ソリューション設計 http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html』の「ホストベースのファイアウォール」セクションを参照してください。NAT を実行し、それぞれのコンテキストの特定のポートを構成します。

セッション ボーダー コントローラの統合

アグリゲーションレイヤで CUBE Enterprise を SBC として統合する方法については、「http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/hcs/11_5/White_Papers/CUBE_E_deployment_for_Cisco_HCS.PDF」を参照してください。

アグリゲーションレイヤでのサードパーティ製セッション ボーダー コントローラの統合については、「http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html」を参照してください。

Small Contact Center 導入モデル用 Cisco Prime Collaboration Assurance の統合

Prime Collaboration Assurance 用カスタマー管理

手順

ステップ 1 *https://<IP_address_of_Prime_Collaboration_application/* の URL を使用して Prime にログインします。

ステップ 2 **[管理（Administration）][カスタマー管理（Customer Management）]** の順に選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **[一般情報（General Info）]** タブで、**[カスタマー名（Customer Name）]** を入力します。

ステップ 5 **[次へ（Next）]** > **[保存（Save）]** の順に選択します。

クラスタの追加

手順

ステップ 1 管理者のログイン情報を使用して、HCM-F にログインします。

ステップ 2 **[クラスタ管理（Cluster Management）]**>**[クラスタ（Cluster）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

ステップ 3 クラスタ名を入力します。

ステップ 4 ドロップダウンリストでカスタマーを選択します。

ステップ 5 ドロップダウンリストで、**CC** のクラスタタイプを選択します。

ステップ 6 ドロップダウンリストで、クラスタ アプリケーション バージョンを選択します。

ステップ 7 [クラスタを監視するアプリケーション（Application Monitoring the Cluster）] ドロップダウンリストで、ホスト名として [PCA] を選択します。

ステップ 8 [保存（Save）] をクリックします。

コンタクト センター コンポーネントの追加

カスタマーコンタクトコンポーネントには、AW-HDS、エージェント周辺機器ゲートウェイ、VRU 周辺機器ゲートウェイ、CVP、CVP OAMP、CVP RSA が含まれます。

手順

ステップ 1 管理者のログイン情報を使用して、HCM-F にログインします。

ステップ 2 **[アプリケーション管理（Application Management）]** > **[クラスタアプリケーション（Cluster Application）]** の順に選択します。

ステップ 3 **[一般情報（General Information）]** セクションで以下を構成します。

a) [新規追加（Add New）] をクリックします。

b) **[アプリケーションタイプ（Application Type）]** ドロップダウンログインで、**[UCCE]** を選択します。

CVP、CVP OAMP、CVP RSA に対しては、**[CVP]** を選択し、Rogger、AW-HDS、エージェント周辺機器ゲートウェイ、VRU 周辺機器ゲートウェイに対しては、**[UCCE]** を選択します。

c) CC コンポーネントのホスト名を入力します。

d) ドロップダウンログインでクラスタを選択します。

e) [保存（Save）] をクリックします。

ステップ 4 **[ログイン情報（Credentials）]** セクションで以下を構成します。

a) [新規追加（Add New）] をクリックします。

b) **[ログイン情報タイプ（Credential Type）]** ドロップダウンリストで、**SNMP _V2** を選択します。

c) CC コンポーネントで構成した**コミュニティ文字列**を入力します。

d) アクセスタイプに対して、**[読み取り専用（Read Only）]** オプションを選択します。

e) [保存（Save）] をクリックします。

f) **[新規追加（Add New）]** をクリックします。

g) **[ログイン情報タイプ（Credential Type）]** ドロップダウンリストで、**ADMIN** を選択します。

h) 管理者のログイン情報を入力します。

CVP、CVP OAMP については、CVP RSA は OAMP Web UI に対して構成した **wsmadmin** のユーザー ID とパスワードを使用します。

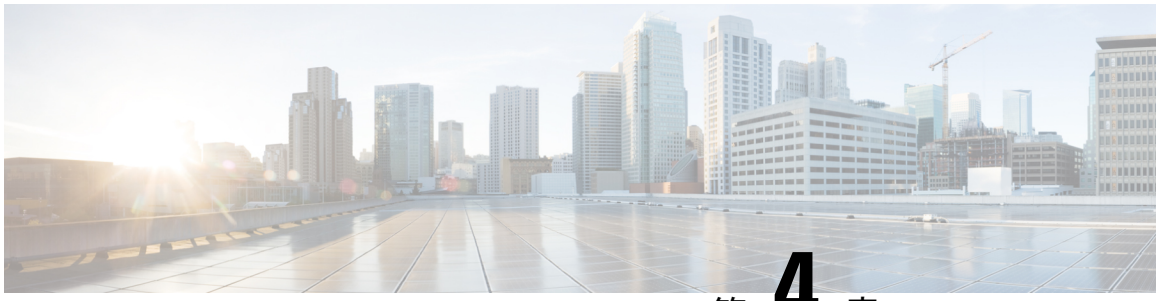
i) アクセスタイプに対して、**[読み取り専用（Read Only）]** オプションを選択します。

j) [保存（Save）] をクリックします。

ステップ 5 **[ネットワークアドレス（Network Addresses）]** セクションで、以下を構成します。

a) [新規追加（Add New）] をクリックします。
b) **[ネットワークスペース（Network Space）]** ドロップダウンリストで **[アプリケーションスペース（Application Space）]** を選択します。
c) IPV4 アドレスとホスト名を入力します。
d) [保存（Save）] をクリックします。
e) **[新規追加（Add New）]** をクリックします。
f) **[ネットワークスペース（Network Space）]** ドロップダウンリストで **[サービスプロバイダスペース（Service Provider Space）]** を選択します。
g) NAT IPV4 アドレスとホスト名を入力します。
h) [保存（Save）] をクリックします。

（注） 同じ手順に従って、AW-HDS、エージェント周辺機器ゲートウェイ、VRU 周辺機器ゲートウェイ、CVP、CVP OAMP、および CVP RSA を追加します。Cisco Unified IC はサポートされていません。



第 4 章

管理（Administration）

Unified CCE 管理（Administration）

Unified CCDM を使用した Unified CCE のプロビジョニング

Unified Contact Center Domain Manager（Unified CCDM）を使用して Unified CCE をプロビジョニングするには、以下の手順を実行します。

Unified CCDM オブジェクトの CRUD 操作

次の表に、Unified CCDM オブジェクトの作成、読み取り、更新、および削除（CRUD）操作を示します。

（注） 一括アップロードは、作成操作のみをサポートします。Unified CCDM を使用した一括操作 （251 ページ）を参照してください。

CCDM ポータルのデフォルトリソースは編集できません。

オブジェクト	作成	[読み取り（Read）]	更新	削除	一括アップロード
バケット間隔については、「コールタイプの構成 （222ページ）」を参照してください。		x			

オブジェクト	作成	[読み取り（Read）]	更新	削除	一括アップロード
ECC 変数については、「拡張コール変数の構成（233 ページ）」を参照してください。	x	x	x	x	
ネットワーク VRU スクリプトについては、「ネットワーク VRU スクリプトの構成 （228 ページ）」を参照してください。	x	x	x	x	x
コールタイプについては、「コールタイプの作成（222 ページ）」を参照してください。	x	x	x	x	x
ダイヤル番号については、「ダイヤル番号の構成（230 ページ）」を参照してください。	x	x	x	x	x
スキルグループについては、「スキルグループの構成（244 ページ）」を参照してください。	x	x	x	x	x
フォルダについては、「フォルダの構成 （235 ページ）」を参照してください。	x	x	x	x	x
グループについては、「グループの構成 （236 ページ）」を参照してください。	x	x	x	x	
エージェントについては、「エージェントの構成（216 ページ）」を参照してください。	x	x	x	x	x

オブジェクト	作成	[読み取り（Read）]	更新	削除	一括アップロード
エージェントデスクトップについては、「エージェントデスクトップの構成（219ページ）」を参照してください。	x	x	x	x	x
エージェントチームについては、「エージェントチームの構成（220ページ）」を参照してください。	x	x	x	x	x
個人については、「個人の構成（240ページ）」を参照してください。	x	x	x	x	x
ユーザーについては、「ユーザーの構成（211ページ）」を参照してください。	x	x	x	x	x
ユーザー変数については、「ユーザー変数の構成（250ページ）」を参照してください。	x	x	x	x	x
エンタープライズ スキル グループについては、「エンタープライズ スキル グループの構成（232ページ）」を参照してください。	x	x	x	x	x
ラベルについては、「ラベルの構成（238 ページ）」を参照してください。	x	x	x	x	x
属性については、「プレシジョン属性の構成（224ページ）」を参照してください。	x	x	x	x	x

オブジェクト	作成	[読み取り（Read）]	更新	削除	一括アップロード
プレシジョンキューについては、「プレシジョンキューの構成 （226 ページ）」を参照してください。	x	x	x	x	x
サービスについては、「サービスの構成 （242 ページ）」を参照してください。	x	x	x	x	

ユーザーの構成

ユーザーを構成するには、以下の手順を実行します。

- Active Directory のユーザーの作成 （167 ページ）
- ユーザーの作成 （211 ページ）
- ロールをユーザーに割り当てる （213 ページ）
- サブカスタマーテナントおよびユーザーへの権限割り当て （213 ページ）
- ユーザーの編集 （214 ページ）
- ユーザーの削除 （214 ページ）

ユーザーの作成

（注） 管理者としてログインして、テナントまたは下位顧客のユーザを作成します。

手順

ステップ 1 Unified CCDM ポータルで、左上隅にあるハンバーガー アイコンをクリックして、**セキュリティ** > **ユーザ**を選択します。

ステップ 2 ユーザを作成するテナントを選択して、 **新規**をクリックします。

ステップ 3 **ログイン名**を入力します。

ステップ 4 ユーザの **名**、**姓**、そして **説明**を入力します。

ステップ 5 **カルチャー** ドロップダウンリストで、**英語（日本）** オプションを選択します。

ステップ 6 次のチェックボックスをオンにします。

Advanced モード

- 有効なアカウント
- パスワードを無期限にする（**Password Never Expires**）
- ユーザによるパスワード変更を無効にする（**User Cannot Change Password**）
- 有効な **Internet Script Editor** （ISE ユーザの場合）

ステップ 7 **ユーザのホーム フォルダ** フィールドで選択されたパスが正しいことを確認します。

このユーザの新規フォルダを作成する チェックボックスがオフになっていることを確認します。

ステップ 8 **パスワード** と **パスワードの確認** にパスワードを入力します。

ステップ 9 **[保存（Save）]** をクリックします。

インポートした Unified CCE ユーザーの構成

Unified CCE と Unified CCDM の統合後、Unified CCDM は、既存の Unified CCE ユーザーをインポートします。インポートされたすべてのユーザは、デフォルトのインポート場所に保管されています。インポートしたユーザを適切なテナントまたはフォルダに移動します。

以下の手順で、インポートしたユーザを設定します。

手順

ステップ 1 Unified CCDM で、インポートした Unified CCE ユーザーを見つけます。Unified CCDM のユーザ名の編集手順：

<*username*>@<*domainname*>の形式にします。ユーザ名 は、Windows ユーザ名、 *domainname* は、Windows ドメインの完全修飾名です。

例：

iseuser1@testdomain.local

ステップ 2 ユーザを選択して詳細を表示します。

ステップ 3 [**詳細** タブを選択して、以下のチェックボックスをオンにします。

- 有効なアカウント
- **Advanced モード**
- **Internet Script Editor** （ISE ユーザの場合）

ステップ 4 **保存** をクリックして、リンクした Unified CCDM ユーザの詳細を更新します。

（注） SSO が無効になっている場合は、ISE にログインする前に、インポートした Unified CCE ユーザーとして Unified CCDM ポータルにログインする必要があります。対応する Windows Active Directory ユーザの **パスワード** フィールドに入力します。

ロールをユーザーに割り当てる

対応するロールをユーザーに割り当てるには、以下の手順を実行します。

手順

ステップ 1 Unified CCDM ポータルで、左上隅にあるハンバーガー アイコンをクリックして、**セキュリティ** > **ユーザ**を選択します。

ステップ 2 リストから新しく作成したユーザーを選択します。

ステップ 3 **[グループ（Group）]** タブを選択し、**[グループに追加（Add to Group）]** をクリックします。

ステップ 4 ロールを割り当てるユーザーが含まれるテナント/フォルダを選択します。

ステップ 5 **[基本ユーザー（Basic Users）]** チェックボックスをオンにして、テナントに基本的な権限を付与します。

ステップ 6 テナント/ISE ユーザーの **[上級ユーザー（Advanced Users）]** チェックボックスをオンにし、**[OK]** をクリックします。

デフォルトで、上級ユーザーには、**Browse Dimension** 権限が付与されています。

ステップ 7 スーパーバイザの **[スーパーバイザ（Supervisors）]** チェックボックスをオンにしたら、**[OK]** をクリックします。

ステップ 8 [保存（Save）] をクリックします。

サブカスタマーテナントおよびユーザーへの権限割り当て

手順

ステップ 1 CCDM Web ポータルにログインします。

ステップ 2 バーガーアイコンをクリックします。

ステップ 3 **[セキュリティ（Security）** > **[権限（Permissions）** の順に選択します。

ステップ 4 サブカスタマーテナントを選択し、**[権限（Permission）]** タブをクリックし、**[権限の継承元/ルート（Inherit Permissions from /Root）]** をオフにして、**[OK]** をクリックします。

[未割当て（Unallocated）] > **SCCTenantフォルダ（SCCTenant Folder）** の順に選択し、この手順を繰り返します。

ステップ 5 新しく追加したユーザーを選択し、**[グループ（Group）]** タブをクリックします。

ステップ 6 **[グループを追加（Add to Groups）]** をクリックします。

ステップ 7 **[未割当て（Unallocated）]** > **[SCCTenantフォルダ（SCCTenant Folder）]** の順に選択し、**[基本ユーザー権限（Basic Users Permission）]** を有効化します。

ステップ 8 サブカスタマーテナントをクリックし、**Advanced Users** 権限を割り当て、**[OK]** をクリックします。

デフォルトでは、**Advanced User** は、**Browse Dimension** 権限が割り当てられています。

ステップ 9 [保存（Save）] をクリックします。

ユーザーの編集

ユーザーを編集するには、以下の手順を実行します。

手順

ステップ 1 Unified CCDM ポータルで、左上隅にあるハンバーガー アイコンをクリックして、**セキュリティ** > **ユーザ**を選択します。

ステップ 2 フォルダツリーから、編集するユーザーを含むフォルダを選択します。

ステップ 3 編集するユーザーを選択します。

ステップ 4 **[詳細（Details）]** タブをクリックします。

ステップ 5 必要情報を編集します。

ステップ 6 **[グループ（Groups）]** タブをクリックして、グループを追加または削除します。

ステップ 7 [保存（Save）] をクリックします。

ユーザーの削除

ユーザーを削除するには、次の手順に従います。

手順

ステップ 1 Unified CCDM ポータルで、左上隅にあるハンバーガー アイコンをクリックして、**セキュリティ** > **ユーザ**を選択します。

ステップ 2 左側のフォルダツリーから、削除するユーザーを含むフォルダを選択します。

ステップ 3 削除するユーザーを選択します。

ステップ 4 **[削除（Delete ）]** > **[はい（Yes）]** の順に選択します。

部署の構成

部門を設定するには、以下の手順を実行します。

部署の作成

手順

ステップ 1 テナント管理者として、CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 テナントから必要なフォルダを選択します。**[リソース（Resource）]** をクリックし、**[部署（Department）]** を選択します。
ステップ 4 部署名を入力し、必須フィールドを入力します。
ステップ 5 [保存（Save）] をクリックします。

部署の編集

手順

ステップ 1 テナント管理者として、CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 テナントから必要なフォルダを展開します。**[部署（Department）]** をクリックします。
ステップ 4 編集する部署を選択し、必須フィールドを変更します。
ステップ 5 [保存（Save）] をクリックします。

部署の移動

手順

ステップ 1 テナント管理者として、CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 テナントから必要なフォルダを展開します。**[部署（Department）]** をクリックします。
ステップ 4 **[部署（Department）]** タブで、移動する部署を選択し、**[移動（Move）]** をクリックします。

ステップ 5 部署を移動する接続先フォルダを参照し、**[保存（Save）]** > **[OK]** の順に選択します。

部署の削除

手順

ステップ 1 テナント管理者として、CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 テナントから必要なフォルダを展開します。**[部署（Department）]** をクリックします。

ステップ 4 **[部署（Department）]** タブで、削除する部署を選択します。

ステップ 5 **[削除（Delete）]** > **[OK]** の順に選択します。

エージェントの構成

エージェントを構成するには、以下の手順を実行します。

- エージェントの作成 （216 ページ）
- エージェントの編集 （218 ページ）
- エージェントの削除 （218 ページ）

エージェントの作成

エージェントを作成するには、以下の手順を実行します。

手順

ステップ 1 テナント、サブカスタマーユーザーまたはスーパーバイザとして、CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** を選択します。

ステップ 3 エージェントを作成します。

- テナントまたはサブカスタマーユーザーとしてログインした場合は、**[リソースマネージャ（Resource Manager）]** を選択し、エージェントを作成するフォルダを選択します。**[リソース（Resource）]** > **[エージェント（Agent）]** の順に選択します。
- スーパーバイザユーザーの場合は、**[エージェントチームマネージャ（Agent Team Manager）]** を選択し、**[新しい個人（New Person）]** をクリックします。

ステップ 4 **[詳細（Details）]** タブをクリックし、以下のように構成します。

a) エージェントの名前を入力します。
b) エージェントの説明を入力します。
c) エージェントを作成する周辺機器を選択します。
d) 個人をエージェントに関連付けます。

エージェントを既存の人物に関連付けるか、そのエージェントに新規人物を作成するかを選択できます。

- **既存の個人を選択**：ドロップダウンリストで既存の個人を選択します。検索ボックスで個人の名前の一部を入力すると、特定の個人を検索できます。新規エージェントは、個人の周辺機器ログインボックスで指定された詳細を使用して、エージェントデスク設定にログインします。
- **個人の新規作成**：個人の名および姓を入力し、周辺機器へのログインに使用する詳細を入力します。個人が自動的に作成され、エージェントに関連付けられます。

e) Unified CCE がハイブリッドモードの場合、**[SSO]** チェックボックスをオンにして、エージェントを SSO エージェントにします。

ステップ 5 エージェントをスーパーバイザにするには、**[スーパーバイザ（Supervisor）]** タブをクリックし、**[スーパーバイザ（Supervisor）]** チェックボックスをオンにします。スーパーバイザが非 SSO エージェントの場合は、以下の手順を実行します。

a) ドメインアカウント（コンタクト センター ネットワークのコンピュータにログインする際にエージェントが使用するアカウント）にエージェントを関連付けます。

（注） 通常、Unified CCDM からドメインアカウントを設定することはできません。これは、セキュリティルールによって防止されるためです。使用するドメインアカウントがわからない場合は、管理者にお尋ねください。

b) アカウント名を入力し、**[検索（Find）]** をクリックし、正しいアカウントを選択します。

ステップ 6 **[エージェントチーム（Agent Teams）]** タブをクリックし、以下のように構成します。

a) エージェントが属するエージェントチームを選択します。エージェントがメンバーになれるチームは1つだけですが、スーパーバイザは複数のチームを監督できます。[選択済みパス（Selected Path）] ドロップダウンリストを使用して別のフォルダにあるエージェントチームを参照します。
b) [追加（Add）] をクリックして、チームをこのエージェントに関連付けます。
c) **[メンバー（Member）]** チェックボックスをオンにして、エージェントをチームメンバーにします。

スーパーバイザは、メンバーになることなくチームを監督できます。

d) エージェントがスーパーバイザの場合は、監督するチームのプライマリまたはセカンダリ スーパーバイザ ロールを選択します。

スーパーバイザは、このチームのメンバーであっても、メンバーでなくてもかまいません。

ステップ 7 **[スキルグループ（Skill Groups）]** タブをクリックし、以下のように構成します。

a) エージェントが所属するスキル グループを選択します。フォルダを変更するには、[選択されたパス（Selected Path）] ドロップダウンを使用します。
b) [追加（Add）] をクリックして、選択したスキル グループにエージェントを追加します。

ステップ 8 [保存（Save）] をクリックします。

エージェントの編集

エージェントを表示または編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 **Resource Manager** 内のフォルダツリーパネルで、エージェントを編集するフォルダを選択します。
ステップ 4 **[項目（Items）]** パネルで、リストからエージェントを選択します。
ステップ 5 エージェントの詳細を編集します。

スーパーバイザやエージェントチームなど別のタブをクリックすると、別のフィード一式が表示されます。必要に応じて、前のタブに戻ることができます。

ステップ 6 [保存（Save）] をクリックします。

エージェントの削除

エージェントを削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 の**[リソースマネージャ（Resource Manager）]** で、削除するエージェントを含むフォルダに移動し、、[項目（Items）]パネルのリストビューを使用してそのフォルダのエージェントを表示します。
ステップ 4 [項目（Items）]パネルで、削除する必要なエージェントのチェックボックスをオンにします。
ステップ 5 [削除（Delete）] をクリックします。
ステップ 6 > **[はい（Yes）]** の順に選択し、エージェントを削除します。

エージェントデスクトップの構成

エージェントデスクトップを構成するには、以下の手順を実行します。

エージェントデスクトップの作成

エージェントデスクトップを作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとしてUnified CCDM ポータルにログインし、**[リソースマネージャ（Resource Manager）]** を選択します。

ステップ 2 リソースマネージャの [フォルダ ツリー（Folder Tree）] パネルで、エージェントデスクトップを作成するフォルダを選択します。

ステップ 3 **[リソース（Resource）]** > **[エージェントデスクトップ（Agent Desktop）]** の順に選択します。

ステップ 4 必要なフィールドに入力します。

ステップ 5 [保存（Save）] をクリックします。

エージェントデスクトップの編集

エージェントデスクトップを編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 編集するエージェントデスクトップを含むフォルダを選択し、[項目（Items）] パネルリストビューを使用して、そのフォルダのエージェントデスクトップを表示します。

ステップ 4 **[項目（Items）]** パネルで、編集するエージェントデスクトップをクリックします。

エージェントデスクトップの詳細が [詳細（Details）] パネルに表示されます。

ステップ 5 **[詳細（Details）]** タブで該当するタブをクリックし、目的に合わせて変更を行います。

ステップ 6 [保存（Save）] をクリックします。

エージェントデスクトップの削除

エージェントデスクトップを削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 削除するエージェントデスクトップを含むフォルダを選択し、[項目（Items）] パネルリストビューを使用して、そのフォルダのエージェントデスクトップを表示します。

ステップ 4 [項目（Items）] パネルで、削除する 1 つ以上のエージェントデスクトップのチェックボックスをオンにします。

ステップ 5 **[削除（Delete ）]** > > **[はい（Yes）]** の順に選択します。

（注） エージェントデスクトップを削除すると、関連するエージェントデスクトップが自動的に削除されます。

エージェントチームの構成

エージェントチームを構成するには、以下の手順を実行します。

- エージェントチームの作成 （220 ページ）
- エージェントチームの編集 （221 ページ）
- エージェントチームの削除 （221 ページ）

エージェントチームの作成

エージェントチームを作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 フォルダツリーパネルで、エージェントチームを作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** > **[エージェントチーム（Agent Team）]** の順に選択します。

ステップ 5 チームの一意の名前を入力します。

ステップ 6 エージェントチームを作成するために必要なすべてのフィールドに入力します。

ステップ 7 エージェントをチームに割り当てるには、[エージェント（Agents）] タブで 1 つ以上のエージェントのチェックボックスをオンにし、**[追加（Add）]** をクリックします。

ステップ 8 エージェントをチームに追加したら、そのエージェントの[メンバー（Member）]チェックボックスもオンにして、チームのメンバーにする必要があります。

これは、スーパーバイザであれば、メンバーにならなくともチームに参加することが可能であるためです。

エージェントがスーパーバイザである場合、右側のカラムにドロップダウンリストが表示されます。

ステップ 9 この特定のチームでエージェントにスーパーバイザロールを割り当てるか指定します。

ステップ 10 [保存（Save）] をクリックします。

エージェントチームの編集

エージェントチームを編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 編集するエージェントチームを含むフォルダを選択し、[項目（Items）]パネルリストビューを使用して、そのフォルダのエージェントチームを表示します。

ステップ 4 **[項目（Items）]** パネルで、編集するエージェントチームをクリックします。

[詳細（Details）] パネルにエージェントチームの詳細が表示されます。

ステップ 5 それぞれのタブをクリックし、変更するフィールドを編集します。

ステップ 6 チームからエージェントを削除するには、**[エージェント（Agents）]** タブをクリックし、チームから削除するエージェントのチェックボックスをオンにし、**[削除（Remove）]** をクリックします。

ステップ 7 [保存（Save）] をクリックします。

エージェントチームの削除

エージェントチームを削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 削除するエージェントチームを含むフォルダを選択し、[項目（Items）]パネルリストビューを使用して、そのフォルダのエージェントチームを表示します。

ステップ 4 **[項目（Items）]** パネルで、削除する 1 つ以上のエージェントチームのチェックボックスをオンにします。

ステップ 5 [Delete（削除）] をクリックします。

[エージェントチームの削除（Delete Agent Teams）]確認ダイアログボックスが表示されます。

ステップ 6 > **[はい（Yes）]** の順に選択し、エージェントチームを削除します。

コールタイプの構成

コールタイプの作成

コールタイプを作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 [フォルダ ツリー（Folder Tree）] パネルで、コールタイプを作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** > **[コールタイプ（Call Type）]** の順に選択します。

ステップ 5 次の詳細を入力します。

a) **[名前（Name）]** フィールドに一意の名前を入力します。

b) ドロップダウンリストで、**[バケット間隔（Bucket Interval）]** を選択します。

（注） バケット間隔とは、コールタイプの間隔として使用される応答呼または放棄呼の数です。デフォルト値はシステムのデフォルトです。

c) ドロップダウンリストで、**[サービスレベルしきい値（Service Level Threshold）]** を選択します。

d) ドロップダウンリストで、**[サービスレベルタイプ（Service Level Type）]** を選択します。

ステップ 6 [保存（Save）] をクリックします。

コールタイプの編集

コールタイプを編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 削除するコールタイプを含むフォルダを選択し、[項目（Items）]パネルリストビューを使用してフォルダのコールタイプを表示します。
ステップ 4 **[項目（Items）]** パネルで、編集するコールタイプを選択します。
ステップ 5 それぞれのタブをクリックし、変更するフィールドを編集します。
ステップ 6 [保存（Save）] をクリックします。

コールタイプの削除

コールタイプを削除するには、以下の手順を実行します。

（注） デフォルトのコール タイプは削除できません。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 削除するコールタイプを含むフォルダを選択し、[項目（Items）] パネルリストビューの [サマリー（Summary）] で **[コールタイプ（Call Type）]** をクリックします。
ステップ 4 **[項目（Items）]** パネルで、削除するコールタイプを選択します。
ステップ 5 **[削除（Delete ）]** > **[はい（Yes）]** の順に選択します。

プレシジョンルーティングの構成

プレシジョンルーティングを構成するには、以下の手順を実行します。

- プレシジョン属性の構成 （224 ページ）
- エージェントにプレシジョン属性を割り当てる （225 ページ）
- プレシジョンキューの構成 （226 ページ）

- ルーティングスクリプトの作成 （227 ページ）

プレシジョン属性の構成

プレシジョン属性を構成するには、以下の手順を実行します。

- プレシジョン属性の作成 （224 ページ）
- プレシジョン属性の編集 （224 ページ）
- プレシジョン属性の削除 （225 ページ）

プレシジョン属性の作成

プレシジョン属性を作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 プレシジョン属性を作成するために必要なテナントを選択します。
ステップ 4 **[リソース（Resource）]** をクリックし、**[プレシジョン属性（Precision Attribute）]** をクリックします。
ステップ 5 プレシジョン属性の名前を指定します。たとえば、**ENGLISH** です。
ステップ 6 プレシジョン属性の説明を入力します。
ステップ 7 プレシジョン属性のデータ型を選択します。たとえば、**Proficiency** です。
ステップ 8 ドロップダウンリストで、**[デフォルト値（Default Value）]** を選択します。
ステップ 9 [保存（Save）] をクリックします。

プレシジョン属性の編集

プレシジョン属性を編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 **リソースマネージャ**で、編集するプレシジョン属性を含むフォルダに移動し、[項目（Items）] パネルのリストビューを使用してそのフォルダのプレシジョン属性を表示します。
ステップ 4 [項目（Items）] パネルで、編集するプレシジョン属性をクリックします。

このプレシジョン属性の詳細が [詳細（Details）] パネルに表示されます。

ステップ 5 [詳細（Details）] パネルで該当するタブをクリックし、目的に合わせて変更を行います。

ステップ 6 [保存（Save）] をクリックします。

（注） データ型のプレシジョン属性は、一度割り当てられると変更できません。ただし、データ型のデフォルト値は変更できます。

プレシジョン属性の削除

プレシジョン属性を削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 **リソースマネージャ**で、削除するプレシジョン属性を含むフォルダに移動し、[項目（Items）] パネルのリストビューを使用してそのフォルダのプレシジョン属性を表示します。

ステップ 4 **[項目（Items）]** パネルで、削除する 1 つ以上のプレシジョン属性のチェックボックスをオンにします。

ステップ 5 [削除（Delete）] をクリックします。

（注） プレシジョンキューで参照されているプレシジョン属性は削除できません。プレシジョン属性を削除するには、参照を削除します。

ステップ 6 **[はい（Yes）]** をクリックします。

エージェントにプレシジョン属性を割り当てる

次の手順を実行して、エージェントにプレシジョン属性を割り当てます。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 **[リソースマネージャ（Resource Manager）]**で、プレシジョン属性を割り当てるエージェントを含んでいるフォルダに移動し、**[項目（Items）]** パネルのリストビューを使用してそのフォルダのエージェントを表示します。

ステップ 4 [項目（Items）] パネルで、プレシジョン属性を割り当てるエージェントをクリックします。

[詳細（Details）] パネルにエージェントの詳細が表示されます。

ステップ 5 [詳細（Details）] パネルで、**[プレシジョン属性（Precision Attribute）]** をクリックします。[プレシジョン属性（Precision Attribute）] タブのチェックボックスをオンにし、**[追加（Add）]** をクリックします。

ステップ 6 [保存（Save）] をクリックします。

（注） スーパーバイザエージェントにプレシジョン属性を割り当てるには、そのスーパーバイザ エージェントをドメイン アカウントに関連付ける必要があります。

プレシジョンキューの構成

プレシジョンキューを構成するには、以下の手順を実行します。

- プレシジョンキューの作成 （226 ページ）
- プレシジョンキューの編集 （227 ページ）
- プレシジョンキューの削除 （227 ページ）

プレシジョンキューの作成

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 プレシジョンキューを作成するために必要なテナントを選択します。

ステップ 4 **[リソース（Resource）]** > **[プレシジョンキュー（Precision Queue）]** の順に選択します。

新しいページが表示されます。

ステップ 5 必要なフィールドに入力する

ステップ 6 **[手順（Steps）]** タブで、**Step1** をクリックします。新しいページが表示されます。

ステップ 7 [Expression1] フィールドに属性名を入力し、ドロップダウンリストで操作を選択し、ドロップダウンリストで [熟練度（Proficiency level）] を選択します。たとえば、属性 = **ENGLISH**、操作 >、熟練度 **6** などです。

（注） 要件に基づいて、属性、式、および手順を追加できます。

ステップ 8 [OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

プレシジョンキューの編集

プレシジョンキューを編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 **リソースマネージャ**で、編集するプレシジョンキューを含むフォルダを選択し、**[項目（Items）]** パネルのリストビューを使用してそのフォルダのプレシジョンキューを表示します。

ステップ 4 [項目（Items）] パネルで、編集するプレシジョンキューをクリックします。

このプレシジョンキューの詳細が [詳細（Details）] パネルに表示されます。

ステップ 5 [詳細（Details）] パネルで該当するタブをクリックし、目的に合わせて変更を行います。

ステップ 6 [保存（Save）] をクリックします。

プレシジョンキューの削除

プレシジョンキューを削除するには、以下の手順を実行します。

（注） ルーティングスクリプトで参照されているプレシジョンキューは削除できません。プレシジョンキューを削除するには、参照を削除します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 **リソースマネージャ**で、削除するプレシジョンキューを含むフォルダに移動し、**[項目（Items）]** パネルのリストビューを使用してそのフォルダのプレシジョンキューを表示します。

ステップ 4 [項目（Items）]パネルで、削除する 1 つ以上のプレシジョンキューのチェックインをオンにします。

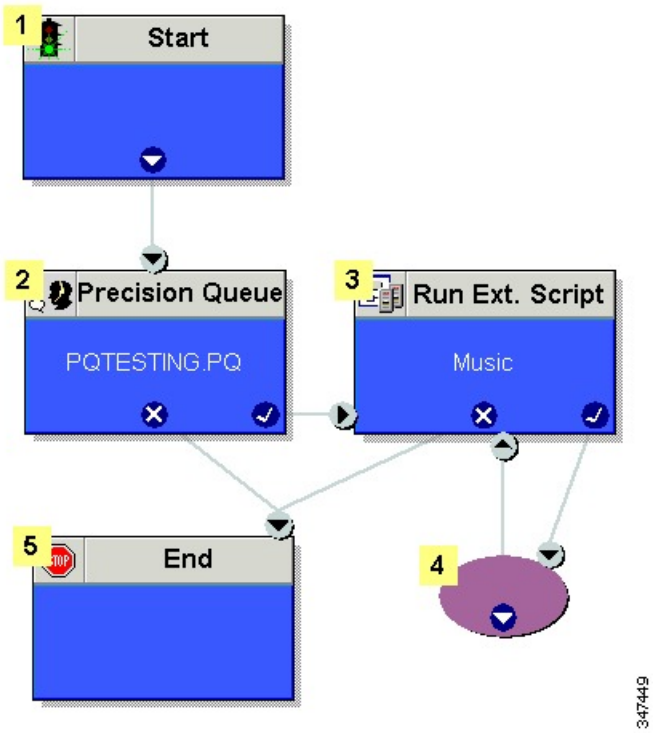
ステップ 5 **[Delete（削除）]** をクリックします。

ステップ 6 **[はい（Yes）]** をクリックします。

ルーティングスクリプトの作成

ルーティングスクリプトを作成するには、次の図を参照してください。

図 *8:* ルーティングスクリプトの作成



ネットワーク VRU スクリプトの構成

ネットワーク VRU スクリプトの作成

ネットワーク VRU スクリプトを設定するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 ネットワーク VRU スクリプトを作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** を選択して、**[ネットワークVRUスクリプト（Network Vru Script）]** をクリックします。

ステップ 5 次のようにフィールドに入力します。

a) Name* （必須）ー スクリプトを識別する一意の名前を入力します。

例：

Play_Welcome

b) Network VRU*（必須）ー ドロップダウンリストでネットワーク VRU を選択します。
c) VRU Script Name*（必須）ー Unified CVP で認識されているスクリプト名を入力します。
d) Configuration Parameter（オプション）ーIVR サービスを追加パラメータに渡すために Unified CVP が使用する文字列。文字列の内容は、アクセスされるマイクロアプリケーションによって異なります。
e) Timeout*（必須）ー スクリプトを実行するように指示した後に、システムがルーティングクライアントからの応答を待機する秒数を示す数字を入力します。
f) Interruptible（オプション）ーたとえば、エージェントが電話対応できるようになった時などにスクリプトを中断できるかどうかを示すチェックボックスです。

（注）
- **[詳細（Advance）]** タブで、デフォルトのエンタープライズ名が生成されます。
- ネットワーク VRU スクリプトの初回作成時は、オーディオファイルをアップロードできません。

ステップ 6 [保存（Save）] をクリックします。

ネットワーク VRU スクリプトの編集

ネットワーク VRU の詳細を編集し、オーディオファイルを VRU スクリプトに関連付けるには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 編集する**ネットワーク VRU スクリプト** を含むフォルダを選択します。
ステップ 4 **[項目（Items）]** パネルで、編集する**ネットワーク VRU スクリプト**をクリックします。
ステップ 5 **[オーディオ（Audio）]** タブをクリックします。
ステップ 6 **[参照（Browse）]** をクリックし、ハードドライブからオーディオファイルを選択します。
ステップ 7 [アップロード（Upload）] をクリックします。
ステップ 8 ファイルをアップロードしたら、**[保存（Save）]** をクリックします。

ネットワーク VRU スクリプトの削除

（注） スクリプトで参照されているダイヤル番号は削除できません。ダイヤル番号を削除するには、この参照を削除する必要があります。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 削除する**ネットワーク VRU スクリプト**を含むフォルダを選択します。
ステップ 4 **[項目（Items）]** パネルで、削除する**ネットワーク VRU スクリプト**をクリックします。
ステップ 5 **[削除（Delete）]** オプションを選択します。
ステップ 6 > **[はい（Yes）]** の順に選択し、ネットワーク VRU スクリプトを削除します。

ダイヤル番号の構成

ダイヤル番号を構成するには、以下の手順を実行します。

- ダイヤル番号の作成 （230 ページ）
- ダイヤル番号の編集 （231 ページ）
- ダイヤル番号の削除 （231 ページ）

ダイヤル番号の作成

1 つ以上のダイヤル番号を作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 ダイヤル番号を作成するフォルダを選択します。
ステップ 4 **[リソース（Resource）]** > **[ダイヤル番号（Dialed Number）]** の順に選択します。
ステップ 5 ダイヤル番号について最大 32 文字の一意の名前を入力します。

この名前は英数字、ピリオド、および下線だけで構成する必要があります。

ワイルドカードのダイヤル番号は、以下のパターンに従います。

例：

7xx

ステップ 6 [ダイヤル番号（Dialed Number）] フィールドと同様にフィールドに入力します。

ステップ 7 [追加（Add）] をクリックして、このダイヤル番号に関連付けるコール タイプとその他のダイヤル情報を指定します。

ステップ 8 [保存（Save）] をクリックします。

ダイヤル番号の編集

ダイヤル番号を編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 編集するフォルダを選択し、**[項目（Items）]** パネルリストビューを使用して、そのフォルダ内のダイヤル番号を表示します。

ステップ 4 **[項目（Items）]** パネルで、編集するダイヤル番号をクリックします。

ステップ 5 変更後、**[保存（Save）]** をクリックします。

ダイヤル番号の削除

1 つ以上のダイヤル番号を削除するには、以下の手順を実行します。

（注） スクリプトで参照されているダイヤル番号を削除することはできません。ダイヤル番号を削除するには、参照を削除してください。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 削除するダイヤル番号を含むフォルダを選択し、[項目（Item）]パネルリストビューを使用してフォルダ内のダイヤル番号を表示します。

ステップ 4 **[項目（Items）]** パネルで、削除するダイヤル番号を選択します。

ステップ 5 **[Delete（削除）]** をクリックします。

ステップ 6 **[はい（Yes）]** をクリックします。

エンタープライズ スキル グループの構成

エンタープライズ スキル グループを構成するには、以下の手順を実行します。

- エンタープライズ スキル グループの作成 （232 ページ）
- エンタープライズ スキル グループ構成の編集 （232 ページ）
- エンタープライズ スキル グループの削除 （233 ページ）

エンタープライズ スキル グループの作成

エンタープライズ スキル グループを作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 エンタープライズ スキル グループを作成するフォルダを選択します。
ステップ 4 **[リソース（Resource）]** > **[エンタープライズスキルグループ（Enterprise Skill Group）]** の順に選択します。
ステップ 5 グループの一意の名前を入力します。
ステップ 6 エンタープライズスキル グループを作成するために必要なすべてのフィールドに入力します。
ステップ 7 スキルグループをグループに割り当てるには、**[追加（Add）]** をクリックし、1 つ以上のスキルグループを選択します。
ステップ 8 [保存（Save）] をクリックします。

エンタープライズ スキル グループ構成の編集

エンタープライズ スキル グループを編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 フォルダツリーパネルで、編集するフォルダを選択し、**[項目（Items）]** パネルリストビューを使用して、そのフォルダ内のエンタープライズ スキル グループを表示します。

ステップ 4 **[項目（Items）]** パネルで、編集するグループを選択します。

ステップ 5 変更後、**[保存（Save）]** をクリックします。

エンタープライズ スキル グループの削除

エンタープライズ スキル グループを削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 削除するエンタープライズ スキル グループが含まれるフォルダに移動し、[項目（Items）] パネルのリストビューを使用して、そのフォルダ内のエンタープライズ スキル グループを表示します。

ステップ 4 **[項目（Items）]** パネルで、削除する 1 つ以上のエンタープライズ スキル グループのチェックボックスをオンにします。

ステップ 5 [削除（Delete）] をクリックします。

ステップ 6 > **[はい（Yes）]** の順に選択します。

拡張コール変数の構成

拡張コール変数を構成するには、以下の手順を実行します。

- 拡張コール変数の作成 （233 ページ）
- 拡張コール変数の編集 （234 ページ）
- 拡張コール変数の削除 （234 ページ）

拡張コール変数の作成

拡張コール変数を作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 拡張コール変数を作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** > **[拡張コール変数（Expanded Call Variable）]** の順に選択します。

ステップ 5 次のフィールドに必要な情報を入力します。

a) **[名前（Name）]** フィールドに一意の名前を入力します。
b) **[説明（Description）]** フィールドに、説明を入力します。
c) **[最大長（Maximum Length）]** フィールドに、コール変数の最大長を入力します。
d) オプションで、**[永続（Persistent）]** をオンにします。
e) オプションで、**[有効化（Enabled）]** チェックボックスをオンにします。
f) オプションで、**[ECCアレイ（ECC Array）]** チェックボックスをオンにします。

ステップ 6 **[詳細（Advanced）]** タブで、コール変数の終了日を設定します。

（注） 終了日を設定するには、**[永久（Forever）]** チェックボックスをオフにします。

ステップ 7 [保存（Save）] をクリックします。

拡張コール変数の編集

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 拡張コール変数を変更するフォルダを選択します。
ステップ 4 [項目（Items）] パネルの **[拡張コール変数（Expanded Call Variable）]** をクリックします。
ステップ 5 変更する拡張コール変数を選択します。
ステップ 6 必要に応じて、[詳細（項目）] タブのフィールドを変更します。
ステップ 7 [保存（Save）] をクリックします。

拡張コール変数の削除

拡張コール変数を削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 削除する拡張コール変数を含むフォルダを選択し、拡張コール変数を表示します。
ステップ 4 **[項目（Items）]** パネルで、削除する拡張コール変数を選択します。
ステップ 5 [削除（Delete）] をクリックします。

ステップ 6 > **[はい（Yes）]** の順に選択します。

フォルダの構成

フォルダ構成に対して以下の手順を実行します。

- フォルダの作成 （235 ページ）
- フォルダ名の変更 （235 ページ）
- フォルダの移動 （236 ページ）
- フォルダの削除 （236 ページ）

フォルダの作成

フォルダを作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 新しいフォルダを作成するフォルダ/テナントを選択します。
ステップ 4 **[システム（System）]** > **[フォルダ（Folder）]** の順に選択します。
ステップ 5 [名前（Name）] フィールドに、新しいフォルダの名前を入力します。
ステップ 6 オプションで、[説明（Description）] フィールドに、フォルダの説明を入力します。
ステップ 7 必要に応じて、**[権限の継承（Inherit Permissions）]** チェックボックスをオフにして、このフォルダをポリシー ルートにします。ポリシー ルートは、セキュリティ権限をその親フォルダから継承しません。
ステップ 8 ツリー構造で同じ地点にさらにフォルダを作成する場合は、**[続けて作成（Create Another）]** チェックボックスをオンにします。
ステップ 9 [保存（Save）] をクリックして、新しいフォルダをツリーに保存します。

フォルダ名の変更

手順

[リソースマネージャ（Resource Manager）] のフォルダツリーパネルにあるフォルダを右クリックし、**[フォルダの名前変更（Rename Folder）]** を選択し、必要な名前を入力します。

フォルダの移動

フォルダを移動するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 [項目（Items）] パネルで **[フォルダ（Folders）]** をクリックします。
ステップ 4 移動するフォルダのチェックボックスをオンにします。
ステップ 5 [移動（Move）] をクリックします。
ステップ 6 フォルダツリーで、フォルダの移動先のロケーションを選択します。
ステップ 7 [保存（Save）] をクリックします。

ドラッグ アンド ドロップ オプションを使用してもフォルダを移動することができます。

フォルダの削除

フォルダを削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 [項目（Items）] パネルで **[フォルダ（Folders）]** をクリックします。
ステップ 4 削除するフォルダのチェックボックスをオンにします。
ステップ 5 [削除（Delete）] をクリックします。
ステップ 6 [フォルダの削除（Delete folder）] ダイアログで、> **[はい（Yes）]** の順に選択します。

グループの構成

以下の手順を完了して、グループを構成します。

- グループの作成 （237 ページ）
- グループの編集 （237 ページ）
- グループの移動 （238 ページ）
- グループの削除 （238 ページ）

グループの作成

グループを作成するには、以下の手順を実行します。

手順

ステップ 1 管理者/テナント/サブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 新しいフォルダを作成するフォルダまたはテナントを選択します。

ステップ 4 **[システム（System）]** > **[グループ（Group）]** の順に選択します。

ステップ 5 次の詳細を入力します。

a) [名前（Name）] フィールドに、新規グループの名前を入力します。

フォルダが異なればグループに同じ名前を使用できます。

b) [説明（Description）] フィールドに、その権限の概要や、対象ユーザのカテゴリなど、グループの説明を入力します。

c) 複数のグループを作成する場合、[続けて作成（Create Another）] チェックボックスをオンにすると、このグループを作成した後でも引き続き [グループの新規作成（Create a new group）] ページが表示されます。

d) [保存（Save）] をクリックします。

グループの編集

グループの詳細を編集または表示するには、以下の手順を実行します。

手順

ステップ 1 管理者/テナント/サブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 編集するグループを含むフォルダを選択し、[項目（Items）] パネルリストビューを使用してフォルダのグループを表示します。

ステップ 4 **[項目（Items）]** パネルで、編集するグループを選択します。

ステップ 5 必要に応じて、グループの詳細を編集します。

ステップ 6 **[メンバー（Members）]** タブをクリックして、グループのメンバーを追加または削除します。

ステップ 7 **[グループ（Groups）]** タブをクリックして、他のグループからグループを追加または削除します。

ステップ 8 [保存（Save）] をクリックします。

グループの移動

グループを移動するには、以下の手順を実行します。

手順

ステップ 1 管理者/テナント/サブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioing）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 移動するグループを含むフォルダを選択し、[項目（Items）] パネルリストビューを使用してフォルダのグループを表示します。
ステップ 4 **[項目（Items）]** パネルで、移動するグループを選択します。
ステップ 5 [移動（Move）] をクリックします。
ステップ 6 グループを移動するテナントまたはフォルダに移動します。
ステップ 7 [保存（Save）] をクリックします。

グループの削除

グループを削除するには、以下の手順を実行します。

手順

ステップ 1 管理者/テナント/サブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 削除するグループを含むフォルダを選択し、[項目（Items）] パネルリストビューを使用してフォルダのグループを表示します。
ステップ 4 **[項目（Items）]** パネルで、削除するグループを選択します。
ステップ 5 **[削除（Delete）]** オプションをクリックし、プロンプトが表示されたら削除の確認をします。

ラベルの構成

ラベルを構成するには、以下の手順を実行します。

- ラベルの作成 （239 ページ）
- ラベルの編集 （239 ページ）
- ラベルの削除 （239 ページ）

ラベルの作成

ラベルを作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 ラベルを作成するフォルダを選択します。
ステップ 4 **[リソース（Resource）]** > **[ラベル（Label）]** の順に選択します。
ステップ 5 ラベルのすべてのフィールドに入力します。
ステップ 6 [保存（Save）] をクリックします。

ラベルの編集

ラベルを編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 編集するラベルを含むフォルダを選択し、**[項目（Items）]** パネルリストビューを使用して、そのフォルダのラベルを表示します。
ステップ 4 **[項目（Items）]** パネルで、編集するラベルをクリックします。
ステップ 5 変更後、**[保存（Save）]** をクリックします。

ラベルの削除

ラベルを削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。
ステップ 3 削除するラベルを含むフォルダを選択し、[項目（Items）]パネルリストビューを使用して、そのフォルダのラベルを表示します。

ステップ 4 [項目（Items）] パネルで、削除する 1 つ以上のラベルのチェックボックスをオンにします。

ステップ 5 [削除（Delete）] をクリックします。

ステップ 6 [ラベルの削除（Delete Labels）] ダイアログボックスで、> **[はい（Yes）]** の順に選択します。

個人の構成

個人を構成するには、以下の手順を実行します。

- 個人の作成 （240 ページ）
- 個人の編集 （241 ページ）
- 個人の削除 （241 ページ）

個人の作成

個人を作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーまたはスーパーバイザユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** を選択します。

ステップ 3 個人を作成します。

- テナントまたはサブカスタマーユーザーとしてログインした場合は、**[リソースマネージャ（Resource Manager）]** を選択し、エージェントを作成するフォルダを選択します。**[リソース（Resource）]** > **[個人（Person）]** の順に選択します。
- スーパーバイザユーザーの場合は、**[エージェントチームマネージャ（Agent Team Manager）]** を選択し、**[新しい個人（New Person）]** をクリックします。

ステップ 4 個人の必須フィールドに値を入力します。

ステップ 5 **[機器（Equipment）]** タブで [Unified Contact Center Enterprise] を選択します。

ステップ 6 **[詳細設定（Advanced）]** タブで、有効開始日と有効終了日を設定します。

ステップ 7 [保存（Save）] をクリックします。

（注） 個人を作成した後は、その個人の Unified CCDM アカウントの詳細を別の個人から編集することはできません。Unified CCDM アカウントの詳細を直接編集する必要があります。

個人は既存の Unified CCDM ユーザーアカウントとリンクできません。

個人の編集

個人を編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 編集する個人を含むフォルダを選択し、**[項目（Items）]** パネルリストビューを使用して、そのフォルダの個人を表示します。

ステップ 4 **[項目（Items）]** パネルで、編集する個人をクリックします。

ステップ 5 オプションで、次のようにパスワードをリセットします。

a) **[詳細（Details）]** タブを選択します。

b) **[パスワードのリセット（Reset Password）]** チェックボックスをオンにします。

c) 新しいパスワードを入力し、確認します。

ステップ 6 変更後、**[保存（Save）]** をクリックします。

個人の削除

個人を削除するには、以下の手順を実行します。

（注） 個人に関連付けられているすべてのエージェントを削除します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 削除する個人を含むフォルダを選択し、[項目（Items）]パネルリストビューを使用して、そのフォルダの個人を削除します。

ステップ 4 [項目（Items）] パネルで、削除する個人のチェックボックスをオンにします（複数可）。

ステップ 5 [削除（Delete）] をクリックします。

ステップ 6 > **[はい（Yes）]** の順に選択します。

スーパーバイザの構成

スーパーバイザを構成するには、以下の手順を実行します。

始める前に

これは、スーパーバイザがドメインアカウントに関連付ける必要がある Small Contact Center 展開のサブカスタマーユーザーに適用されます。

1. **[セキュリティ（Security）]**>**[サブカスタマーテナント（Sub-customer Tenant）]**の順に選択します。
2. **[ユーザータブ（User Tab）]** > **[ユーザー（User）]** の順に選択し、**[権限の変更（Change Permission）]** をクリックします。
3. サブカスタマーテナントに対して、**[完全な権限（Full Permission）]** チェックボックスをオンにし、**[OK]** をクリックします。
4. このサブカスタマーテナントを **[詳細なグループ（Advanced Group）]** に追加します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして CCDM ポータルにログインし、**[リソースマネージャ（Resource Manager）]**を選択します。

ステップ 2 **[リソースマネージャ（Resource Manager）]**でスーパーバイザにするエージェントを含むフォルダを選択するか、スーパーバイザとして構成する新規エージェントを作成します。詳細については、「エージェントの作成 （216 ページ）」を参照してください。

ステップ 3 **[スーパーバイザ（Supervisor）]**タブをクリックし、**[スーパーバイザ（Supervisor）]**チェックボックスをオンにします。スーパーバイザが非 SSO エージェントの場合は、以下の手順を実行します。

a) ドメインアカウント（コンタクト センター ネットワークのコンピュータにログインする際にエージェントが使用するアカウント）にエージェントを関連付けます。

（注） 通常、Unified CCDM からドメインアカウントを設定することはできません。これは、セキュリティルールによって防止されるためです。使用するドメインアカウントがわからない場合は、管理者にお問い合わせください。

b) アカウント名を入力し、**[検索（Find）]** をクリックし、正しいアカウントを選択します。

ステップ 4 [保存（Save）] をクリックします。

サービスの構成

（注） サービスを構成するには、以下の手順を実行します。

- サービスの作成 （243 ページ）
- サービスの編集 （243 ページ）
- サービスの削除 （243 ページ）

サービスの作成

サービスを作成するには、以下の手順を実行します。

手順

ステップ 1 Unified CCDM ポータルにテナントとしてログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 左側のパネルから、サービスを作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** ドロップダウンリストで **[サービス（Service）]** を選択します。

ステップ 5 必要なフィールドに入力します。

ステップ 6 **[詳細（Advanced）]** タブにある **[メディアルーティングドメイン（Media Routing Domain）]** ドロップダウンリストで **Cisco_Voice** を選択します。

ステップ 7 **[スキルグループ（Skillgroups）]** タブに移動し、追加するスキルグループをオンにして、**[追加（Add）]** をクリックします。

ステップ 8 [保存（Save）] をクリックします。

サービスの編集

手順

ステップ 1 Unified CCDM ポータルにテナントとしてログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 左側のパネルから、編集またはサービスを表示するフォルダに移動します。
[項目（Item）] パネルにすべてのサービスのリストが表示されます。

ステップ 4 編集するサービスをクリックします。

ステップ 5 編集後、**[保存（Save）]** をクリックします。

サービスの削除

手順

ステップ 1 Unified CCDM ポータルにテナントとしてログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 左側のパネルから、サービスを削除するフォルダを選択します。

ステップ 4 削除するリストでサービスをオンにします。

ステップ 5 **[削除（Delete ）]** > > **[はい（Yes）]** の順に選択します。

スキルグループの構成

スキルグループを構成するには、以下の手順を実行します。

- スキルグループの作成 （244 ページ）
- スキルグループの編集 （244 ページ）
- スキルグループの削除 （245 ページ）

スキルグループの作成

スキルグループを作成するには、以下の手順を実行します。

（注） スキルグループを作成すると、デフォルトルートが作成されます。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 [フォルダツリー（Folder Tree）] パネルで、スキル グループを作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** > **[スキルグループ（Skill Group）]** の順に選択します。

ステップ 5 グループの一意の名前を入力します。

ステップ 6 **[エージェント（Agents）]** タブを選択し、エージェントのチェックボックスをオンにしたら、**[追加（Add）]** をクリックします。

ステップ 7 [保存（Save）] をクリックします。

スキルグループの編集

スキルグループを編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 編集するスキルグループを含むフォルダを選択し、[項目（Items）]パネルのリストビューを使用して、そのフォルダ内のスキルグループを表示します。

ステップ 4 [項目（Items）] パネルで、編集するスキルグループをクリックします。

[詳細（Details）] パネルにこのスキルグループの詳細が表示されます。

ステップ 5 タブをクリックし、変更するフィールドを編集します。

ステップ 6 オプションで、スキルグループからエージェントを削除するには、**[エージェント（Agents）]** タブを選択し、チームから削除するエージェントを選択します。

ステップ 7 [Remove] をクリックします。

ステップ 8 オプションで、スキルグループからルートの関連付けを削除するには、**[ルート（Route）]** タブを選択し、削除するルートの **[削除（Delete）]** をクリックします。

ステップ 9 オプションで、スキルグループに関連付けられている既存ルートの詳細を編集するには、**[ルート（Route）]** タブを選択し、削除するルートの **[編集（Edit）]** をクリックします。[更新（Update）] をクリックします。

ステップ 10 [保存（Save）] をクリックします。

スキルグループの削除

スキルグループを削除するには、以下の手順を実行します。

（注） スクリプトで参照されているスキルグループを削除することはできません。スキルグループを削除するには、参照を削除します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 削除するスキルグループを含むフォルダを選択し、[項目（Items）]パネルのリストビューを使用して、そのフォルダ内のスキルグループを表示します。

ステップ 4 [項目（Items）] パネルで、削除するスキルグループを選択します。

（注） スキルグループがどのサービスにもマッピングされていないことを確認します。

ステップ 5 [削除（Delete）] をクリックします。

スキルグループの削除ページが表示されます。

ステップ 6 > **[はい（Yes）]** の順に選択します。

スキルグループが削除されます。

ルートの構成

ルートを構成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 [フォルダツリー（Folder Tree）] パネルで、ルートを作成するフォルダを選択します。

ステップ 4 [フォルダツリー（Folder Tree）] パネルで、**[スキルグループ（Skill Group）]** をクリックします。

ステップ 5 ルートを作成するスキルグループを選択します。

ステップ 6 **[ルート（Routes）]** タブを選択します。

ステップ 7 **[ルート名（Route Name）]** フィールドでスクリプトを識別する一意の名前を入力します。

ステップ 8 **[追加（Add）]** をクリックします。

ステップ 9 [保存（Save）] をクリックします。

エージェントの再スキルとエージェント チーム マネージャ

スーパーバイザロールを持つユーザーとしてログインすると、エージェントの再スキル化とエージェントチームマネージャを実行できます。

これらのタスクを実行する前に、ユーザーが作成されていることを確認します。ユーザーを作成するには、「ユーザーの作成（211 ページ）」を参照し、スーパーバイザロールを割り当てるには、「ロールをユーザーに割り当てる（213 ページ）」を参照してください。

CCDM でのエージェントの再スキルおよびエージェント チーム マネージャのスーパーバイザ構成

手順

ステップ 1 管理者として、CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 リソースをクリックし、**[エージェント（Agent）]** リソースを選択します。

ステップ 4 スーパーバイザに対してエージェントを選択します。

ステップ 5 **[スーパーバイザ（Supervisor）]** タブで、[スーパーバイザ（Supervisor）] チェックボックスをオンにし、**[保存（Save）]** をクリックします。

ステップ 6 **[個人（Person）]** タブで、**goto person** アイコンを選択します。

ステップ 7 **[ポータル（Portal）]** タブで、ポータルアカウントをクリックし、既存のユーザーをクリックします。

ステップ 8 テナントを選択したら、ユーザの一覧からスーパーバイザを選択します。

ステップ 9 次へのアイコンをクリックします。
[ユーザーのグループ（User's Group）] ダイアログボックスを表示します。

ステップ 10 スーパーバイザグループがユーザーに追加されていることを確認し、**[保存（Save）]** をクリックします。

ステップ 11 [保存（Save）] をクリックします。

スーパーバイザエージェントとエージェントチームの関連付け

手順

ステップ 1 管理者として、Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 [リソース（Resource）] をクリックし、**[エージェント（Agent）]** をクリックします。

ステップ 4 スーパーバイザエージェントを選択します。

ステップ 5 [エージェントチーム（Agent Team）] タブで、追加するエージェントチームを選択し、**[追加（Add）]** をクリックします。

ステップ 6 **Supervisory Role** 列で、ドロップダウンリストで **[プライマリ（Primary）]** を選択し、**[保存（Save）]** をクリックします。

スキルグループの表示

スキルグループを表示するには、以下の手順を実行します。

手順

ステップ 1 スーパーバイザとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[エージェントの再スキル（Agent Re-Skilling）]** の順に選択します。

ステップ 3 **[スキルグループ（Skill Group）]** ドロップダウンリストで、表示するスキルグループを選択します。
選択したスキルグループのエージェントのリストを表示します。

ステップ 4 エージェントの詳細を変更するには、**[エージェントに移動（Goto Agent）]** アイコンをクリックします。

スキルグループにエージェントを追加

スキルグループにエージェントを追加するには、以下の手順を実行します。

手順

ステップ 1 スーパーバイザとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[エージェントの再スキル（Agent Re-Skilling）]** の順に選択します。

ステップ 3 ドロップダウンリストで、**[スキルグループ（Skill Group）]** を選択します。
選択したスキルグループのエージェントのリストを表示します。

ステップ 4 **[周辺機器上のエージェント（My Agents on Peripheral）]** リストで、スキルグループに追加するE メールを選択したら、**[追加（Add）]** をクリックします。

（注） エージェント名の一部を検索バーに入力すると、エージェントを検索できます。

ステップ 5 [保存（Save）] をクリックします。

スキルグループからエージェントを削除

スキルグループからエージェントを削除するには、以下の手順を実行します。

手順

ステップ 1 スーパーバイザとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[エージェントの再スキル（Agent Re-Skilling）]** の順に選択します。

ステップ 3 スキルグループを選択し、1 人以上のエージェントを削除します。

ステップ 4 トップ リストでチェックボックスを使用し、スキル グループから削除するエージェントを選択します。

ステップ 5 エージェント名の一部を検索ボックスに入力し、**[検索（Search）]** をクリックすると、指定した検索文字列でエージェントリストがフィルタ処理されます。

ステップ 6 [削除（Remove）] をクリックして、エージェントをこのスキル グループから削除します。

ステップ 7 [保存（Save）] をクリックして変更を保存するか、[キャンセル（Cancel）] をクリックして詳細を開始前の状態に戻します。

エージェントチームの表示

スーパーバイザユーザとしてログインし、次の手順を実行してエージェントチームを表示します。

手順

ステップ 1 スーパーバイザとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[エージェントチームマネージャ（Agent Team Manager）]** の順に選択します。

ステップ 3 **[エージェントチーム（Agent Team）]** ドロップダウンリストを選択し、表示するエージェントチームを選択します。
選択したエージェントチームのエージェントのリストを表示します。

エージェントチームの変更

エージェントのチームを変更するには、以下の手順を実行します。

手順

ステップ 1 スーパーバイザとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[エージェントチームマネージャ（Agent Team Manager）]** の順に選択します。

ステップ 3 **[マイエージェントチーム（My Agent Team）]** ドロップダウンリストで、エージェントが属するエージェントチームを選択します。

ステップ 4 エージェントの詳細を変更するには、**[エージェントに移動（Goto Agent）]** アイコンをクリックします。

ステップ 5 **[エージェントチーム（Agent Team）]** タブを選択します。
エージェントチームのエージェントの現在のメンバーシップを表示します。

ステップ 6 オプションで、削除するエージェントチームのチェックボックスをオンにし、**[削除（Remove）]** をクリックします。

ステップ 7 オプションで、リストから追加するエージェントチームを選択し、**[追加（Add）]** をクリックします。

（注） そのチームのメンバーとしてエージェントを追加するには、**[メンバー（Member）]** チェックボックスをオンにします。メンバーではなくスーパーバイザエージェントの場合は、プライマリまたはセカンダリスーパーバイザとしてエージェントを追加することもできます。

ステップ 8 [保存（Save）] をクリックします。

ユーザー変数の構成

ユーザー変数を構成するには、以下の手順を実行します。

- ユーザー変数の作成 （250 ページ）
- ユーザー変数の編集 （250 ページ）
- ユーザー変数の削除 （250 ページ）

ユーザー変数の作成

ユーザー変数を作成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 [フォルダツリー（Folder Tree）] パネルで、ユーザー変数を作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** > **[ユーザー変数（User Variable）]** の順に選択します。

ステップ 5 ユーザー変数に必要なフィールドに値を入力します。

ステップ 6 **[詳細設定（Advanced）]** タブで、有効開始日と有効終了日を設定します。

ステップ 7 [保存（Save）] をクリックします。

ユーザー変数の編集

ユーザー変数を編集するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 編集するユーザー変数を含むフォルダを選択して、**[項目（Items）]** パネルリストビューを使用してそのフォルダのユーザー変数を表示します。

ステップ 4 **[項目（Items）]** パネルで、編集するユーザー変数をクリックします。

ステップ 5 変更後、**[保存（Save）]** をクリックします。

ユーザー変数の削除

ユーザ変数を削除するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 削除するユーザー変数を含むフォルダを選択して、[項目（Items）]パネルリストビューを使用してそのフォルダのユーザー変数を表示します。

ステップ 4 [項目（Items）] パネルで、削除するユーザー変数のチェックボックスをオンにします。

ステップ 5 [削除（Delete）] をクリックします。

ステップ 6 [ユーザー変数の削除（Delete User Variables）] ダイアログボックスで、 > **[はい（Yes）]** の順に選択します。

ユーザー変数が削除されます。

Unified CCDM バージョンの表示

Unified CCDM バージョンを表示するには、以下の手順を実行します。

手順

ステップ 1 設定ページで、**[設定（Settings）]** をクリックします。

ステップ 2 **[About]** をクリックします。

システムにインストールされている Unified CCDM バージョンを表示します。

Unified CCDM を使用した一括操作

一括アップロードツールは、多数のリソース項目を Unified CCDM にインポートする際に使用します。これは、標準の CSV 形式を使用してリソースの属性を入力し、エージェントやスキル グループなどのリソースを生成するために使用します。すべての CSV ファイルには、各値の入力先を示すヘッダーが必要です。これらヘッダーは、Unified CCDM の適切な一括アップロードページからダウンロードしたテンプレートが提供します。次のリソースを一括アップロードできます。

- エージェント
- エージェントデスクトップ
- エージェントチーム
- コールタイプ
- 部署
- ダイヤル番号

- エンタープライズ スキル グループ
- スキルグループ
- ユーザー変数
- フォルダ
- ネットワーク VRU スクリプト
- ラベル
- 個人
- ユーザー
- プレシジョン属性
- プレシジョンキュー

Unified CCDM の一括アップロード

Unified CCDM を一括アップロードするには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーとして Unified CCDM ポータルにログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioing）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 必要なフォルダをクリックします。

ステップ 4 [フォルダツリー（Folder Tree）] パネルで **[アップロード（Upload）]** をクリックし、ドロップダウンリストで一括アップロードする項目タイプを選択します。

一括アップロード制御ページが表示されます。

ステップ 5 選択したリソースのテンプレートを選択します。ページの上部近くにある水平のツールバーには、テンプレートのリンクがあります。選択するとダウンロードボックスが表示され、マシンに CSV ファイルを保存できます。に移動します。

ステップ 6 必要なエディタ（メモ帳など）でテンプレートを開き、データの入力を開始するか、または別のソースからデータをペーストします。

一括アップロードテンプレートの詳細については、『Cisco Unified Contact Center ドメインマネージャ用ユーザーガイド』を参照してください。

ステップ 7 [一括アップロード制御（Bulk Upload Control）] ページに戻り、パスが正しく設定されていることを確認します。

（注） このパスは、CSV ファイルの Path 列を削除した時のみ使用されます。このオプションは、フォルダ、ダッシュボード レイアウト、またはダッシュボード スタイルには使用できません。

ステップ 8 データを入力した CSV ファイルを参照します。

ステップ 9 [アップロード（Upload）] をクリックします。

画面下の進捗バーに、アップロードの進捗が表示されます。

（注）　*1* つの *CSV* ファイルにつき、*500* 項目を超えてアップロードしないでください。

CSV ファイル作成テンプレート

データ型

CSV ファイルの作成には、以下のデータタイプが使用されます。

- 標準命名規則（SNC）。これは、感嘆符やハイフンを含まない英数字データですが、下線は使用できます。
- BOOLEAN 値は以下のいずれかの値です。
  - TRUE。
  - FALSE。
  - 空のフィールド。このフィールドを空にすると、フィールドはデフォルトで FALSE に設定されます。
- Y/N は Boolean に似ていますが、指定できるのは Y または N の値だけです。
- 日付形式は、<Year>-<Month>-<Day> の汎用日付形式です。たとえば、2006-08-30 です。
- ハイフン（-）のマークが付いているデータ型は、フィールドへの入力に制限がないことを意味します（ネイティブ CSV 形式によって課される制限を除く）。
- カラムで値のリストがサポートされる場合（たとえば、エージェントが複数のスキル グループに属している場合）、各スキル グループをセミコロン（;）で区切ります。たとえば、Skillgroup1; Skillgroup2; Skillgroup3 です。

グローバル テンプレート カラム

明記されている場合を除き、これらの列は、すべてのテンプレートファイルで共通です。**Required?** 列は、列を完全に削除できるかどうかを示します。

カラム名	データ タイプ	必須かどうか	説明
パス	パス	なし	リソースを作成できるツリーの場所を示します。一括アップロード画面でパスを指定する場合、このカラムを削除する必要があります。 （注） 列をそのままにして、値を設定しない場合、ルートディレクトリにアップロードが試行されます。これは、フォルダなどの項目には有効ですが、エージェントやスキルグループなどのリソースには使用できません。この列を完全に削除すると、一括アップロードを開始したときに作業中のフォルダにリソースをアップロードします。
名前	SNC	可能	Unified CCDM システムのリソース名。これは一意名でなければなりません。ほとんどの場合、これはプロビジョニングされません。
説明	—	はい	作成された寸法を示します。これはプロビジョニングされません。
EnterpriseName	SNC	×	作成されるリソースの名前です。このフィールドはプロビジョニングされます。空白のままにすると、エンタープライズ名が生成されます。
EffectiveFrom	日付	なし	リソースがアクティブになる日付です。デフォルトは現在の日付です。 （注） この日付はローカライズされず、UTC 日付として扱われます。
EffectiveTo	日付	なし	リソースが非アクティブになる日付です。デフォルトは forever です。 （注） この日付はローカライズされず、UTC 日付として扱われます。

部署テンプレート

カラム名	データ タイプ	必須かどうか	説明
EnterpriseName	SNC	×	作成する部署名。このフィールドはプロビジョニングされます。空白のままにすると、エンタープライズ名が生成されます。
名前	SNC	可能	Unified CCDM システムの部署名。これは一意名でなければなりません。ほとんどの場合、これはプロビジョニングされません。
EffectiveFrom	日付	なし	リソースがアクティブになる日付です。デフォルトは現在の日付です。注意：この日付はローカライズされず、UTC 日付として扱われます。
EffectiveTo	日付	なし	リソースが非アクティブになる日付です。デフォルトは forever です。注：この日付はローカライズされず、UTC 日付として扱われます。

個人テンプレート

カラム名	データ タイプ	必須かどうか	説明
EquipmentName	SNC	非対応	Unified CCE のインスタンス名またはこの個人を追加する Unified CM。この名前は、Unified CCDM クラスタ構成ユーティリティの構成時に指定した機器インスタンス名に直接該当します。
FirstName	SNC	可能	個人の名です。
LastName	SNC	可能	個人の姓です。
LoginName	SNC	可能	個人の周辺機器ログイン名です。

PassPhrase	パスワード	はい	個人の周辺機器ログイン パスワードです。
DepartmentMember	エンタープライズ名	×	この個人を表す部署。

エージェント テンプレート

カラム名	データ タイプ	必須かどうか	説明
PeripheralNumber	数値	×	周辺機器で認識されるサービス番号です。
PeripheralName	SNC	なし	関連付けられている周辺機器のエージェントを識別する名前。
スーパーバイザ（Supervisor）	ブール	なし	エージェントがスーパーバイザかどうかを示します。スーパーバイザカラム名は、Unified CCDM システム ユーザーを作成しませんが、このエージェントをドメインログイン名にバインドできます。
AgentStateTrace	Y/N	なし	ソフトウェアがエージェントのエージェント状態のトレース データを収集するかどうかを示します。
DomainLogin	NETBIOS ログイン名	エージェントがスーパーバイザの場合	このエージェントが関連付けられているドメイン ユーザのログイン名です。ログイン名によく使用される形式は、<domain>\<username> です。
DomainUserName	NETBIOS ユーザ名	エージェントがスーパーバイザの場合	エージェントが関連付けられているドメイン ユーザのユーザー名です。

カラム名	データ タイプ	必須かどうか	説明
PeripheralMember	エンタープライズ名 - PG 名	はい	このエージェントを割り当てる周辺機器です。
AgentDesktopMember	エンタープライズ名（Enterprise Name）	なし	このエージェントが使用するデスクトップです。
PersonMember	エンタープライズ名（Enterprise Name）	可能	このエージェントを表す個人です。
AgentTeamMember	エンタープライズ名（Enterprise Name）	なし	このエージェントが属するチームです。チームは同じ周辺機器にる必要があります。そうでないとプロビジョニングが失敗します。また、このカラムにはキャパシティの制限がある場合があります。たとえば、1つのチームに多数のエージェントが許可されているために、チームのキャパシティに達していることもあります。
SkillGroupMember	エンタープライズ名（Enterprise Name）	なし	このエージェントが属する 1 つまたは複数のスキル グループ。スキルグループは同じ周辺機器にる必要があります。そうでないとプロビジョニングが失敗します。複数のスキル グループを指定するには、各スキル グループをセミコロン（;）文字で区切ります。
DepartmentMember	エンタープライズ名（Enterprise Name）	×	エージェントを表す部署。

カラム名	データ タイプ	必須かどうか	説明
PrecisionAttributeMember	エンタープライズ名と値	いいえ	このエージェントが持つ属性、および各値。「=」を使用して値を割り当て、複数の属性をセミコロン（;）で区切ります。 例：Spanish = 5、MortgageTraining = True
DefaultSkillGroup	エンタープライズ名（Enterprise Name）	なし	

エージェント デスクトップ テンプレート

カラム名	データ タイプ	必須かどうか	説明
WrapupDataIncomingMode	数値	×	着信コールの後に、エージェントが後処理データを入力できるかまたはその必要があるかどうかを示します。 **0**：必須 **1**：オプション **2**：許可しない **3**：後処理データで必須値が空白の場合、デフォルト値である 1 が割り当てられます。
WrapupDataOutgoingMode	数値	×	発信コールの後に、エージェントが後処理データを入力できるかまたはその必要があるかどうかを示します。 **0**：必須 **1**：オプション **2**：許可しない **3**：後処理データで必須値が空白の場合、デフォルト値である 1 が割り当てられます。

WorkModeTimer	数値	×	コールを後処理するためにエージェントに割り当てられた秒単位の時間（1 ～ 7200）です。 デフォルト値は 7200 です。
RemoteAgentType	数値	×	モバイル エージェントが処理される方法を示します。 **0**：リモートアクセスなし **1**：コールルーティングごとのコールを使用 **2**固定接続を使用 **3**：ログイン時にエージェントがルーティングを選択 **4**：後処理で必須。値が空欄の場合は、デフォルト値である 1 を割り当て。
DepartmentMember	英数字	×	このエージェントデスクトップが表す部門

エージェント チーム テンプレート

カラム名	データ タイプ	必須かどうか	説明
PeripheralMember	エンタープライズ名 - PG 名	はい	このエージェントチームを割り当てる周辺機器です。
DialedNumberMember	エンタープライズ名（Enterprise Name）	なし	このエージェントチームに使用するダイヤル番号です。
DepartmentMember	エンタープライズ名（Enterprise Name）	×	エージェントチームを表す部署。

コールタイプテンプレート

カラム名	データ タイプ	必須かどうか	説明
ServiceLevelType	数値	なし	システム ソフトウェアがスキル グループのサービスレベルを計算する方法を示します。このフィールドの値が 0 の場合、Unified CCE は関連する周辺機器と MRD のペアに対してデフォルトの値を使用します。指定可能な値は次の通りです。0 または、空欄=デフォルトを使用。1 = 放棄呼を無視。2 = 放棄呼をマイナスの影響として処理。3 = 放棄呼をプラスの影響として処理。
ServiceLevelThreshold	数値	なし	サービスレベルに対する秒単位でのサービスレベルのしきい値です。このフィールドが負の値の場合、周辺機器表のサービスレベルしきい値フィールドの値が使用されます。
DepartmentMember	エンタープライズ名（Enterprise Name）	なし	エージェントチームを表す部署。

ダイヤル番号テンプレート

カラム名	データ タイプ	必須かどうか	説明
ダイヤル番号	SNC	可能	エージェント/IVR コントローラがこのダイヤル番号を識別する文字列の値。

カラム名	データ タイプ	必須かどうか	説明
RoutingClient Member	SNC	可能	ルーティング要求を Unified CCE に送信するためにこの番号が使用する NIC または PG などのルーティングクライアントの名前。
MediaRouting DomainMember	SNC	可能	メディア ルーティング ドメインの名前。
DepartmentMember	エンタープライズ名（Enterprise Name）	なし	エージェントチームを表す部署。

スキル グループ テンプレート

カラム名	データ タイプ	必須かどうか	説明
PeripheralNumber	数値	×	周辺機器で認識されるサービス番号です。
PeripheralName	SNC	非対応	サイトで認識される周辺機器の名前です。
AvailableHoldoffDelay	数値	なし	この周辺機器に関連付けられている値を使用しないこのスキルグループの値。
優先順位	数値	なし	スキルのルーティング優先順位です。これは 0 に設定してください。
Extension	数値	なし	サービスの内線番号。
IPTA	Y/N	なし	Unified CCE がエージェントを選択するかどうかを示します。
ServiceLevelThreshold	数値	なし	サービスレベルに対する秒単位でのサービスレベルのしきい値です。このフィールドが負の値の場合、周辺機器表の[サービスレベルしきい値（Service Level Threshold）] フィールドの値が使用されます。

ServiceLevelType	数値	なし	システム ソフトウェアがスキル グループのサービスレベルを計算する方法を示します。このフィールドの値が 0 の場合、Unified CCE は関連する周辺機器と MRD のペアに対してデフォルトの値を使用します。次の値が使用できます。 0 = デフォルトを使用 1 = 放棄呼を無視する 2 = 放棄呼をマイナスの影響として処理 3 = 放棄呼をプラスの影響として処理
DefaultEntry	数値	なし	通常のエントリは 0（ゼロ）です。0 より大きい値を持つすべてのレコードは、構成目的のためデフォルトのスキルグループと見なされます。Unified CCE はデフォルトのターゲットスキルグループとして 1 の値があるレコードを使用します。
PeripheralMember	エンタープライズ名（Enterprise Name）	可能	このスキル グループを割り当てる周辺機器です。
MediaRoutingDomainMember	数値	可能	スキルグループのアップロード後は、このカラム名を変更することはできません。
DepartmentMember	エンタープライズ名（Enterprise Name）	可能	このスキルグループが表す部署。
RouteMember	SNC	なし	このスキル グループに関連付けられたルートです。ルートのリストを指定するには、リスト内のルートをセミコロン（;）で区切ります。 （注） 指定する 1 つ以上のルートがすでに存在してはいけません。これらは、スキル グループの一括アップロードの一部として作成されます。

エンタープライズ スキル グループ テンプレート

カラム名	データ タイプ	必須かどうか	説明
DepartmentMember	エンタープライズ名（Enterprise Name）	なし	この項目が属する部署です。このフィールドは、テナントをUnified CCE バージョン 10.0 以降で実行されているUnified CCE インスタンスに関連付ける場合のみ有効です。それ以外の場合、このフィールドが存在するとエラーが報告されます。
SkillGroupMember	エンタープライズ名（Enterprise Name）	なし	このエンタープライズ スキル グループに関連付けられる 1 つまたは複数のスキル グループです。スキル グループは、同じ周辺機器にある必要があります。そうでないと、プロビジョニングは失敗します。複数のスキル グループを指定するには、各スキル グループをセミコロン（;）文字で区切ります。

ユーザー変数テンプレート

カラム名	データ タイプ	必須かどうか	説明
ObjectType	数値	可能	変数を関連付けるオブジェクトのタイプを示す数字です。ユーザー変数をオブジェクトに関連付けない場合は、31（ユーザー変数）を選択します。有効な番号は次のとおりです。 **1**：サービス **2**：スキルグループ **7**：コールタイプ **8**：エンタープライズ サービス **9**：エンタープライズ スキル グループ **11**：ダイヤル番号 **14**：周辺機器 **16**：トランクグループ **17**：ルート **20**：マスタースクリプト **21**：スクリプトテーブル **29**：アプリケーション ゲートウェイ **31**：ユーザー変数

ラベルテンプレート

カラム名	データ タイプ	必須かどうか	説明
RoutingClientMember	SNC	可能	ルーティングクライアント名（NIC または PG）。この番号は、ルーティング要求を Unified CCE に送信する際に使用します。

カラム名	データ タイプ	必須かどうか	説明
LableType	数値	False	ラベルのタイプ： • 0：標準 • 1：DNIS オーバーライド • 2：ビジー • 3：リング • 4：ポストクエリ • 5：リソース
ラベル	SNC	False	ルーティング クライアントでラベルを識別するために使用される文字列値

ネットワーク *VRU* スクリプトテンプレート

カラム名	データ タイプ	必須かどうか	説明
NetworkVruMember	SNC	可能	このネットワーク VRU スクリプトに関連付けるネットワーク VRU。
VruScriptName	SNC	可能	VRU スクリプト名の表現
DepartmentMember	エンタープライズ	いいえ	ネットワーク VRU を表す部署。
タイムアウト	数値	可能	スクリプトの実行を開始した後に、応答を待機する秒数。

フォルダテンプレート

（注） フォルダには、エンタープライズ名、有効開始日、有効終了日のグローバルカラムは使用しません。

カラム名	データ タイプ	必須かどうか	説明
セキュリティ	CSS 形式のリスト	なし	アップロードするフォルダにセキュリティを設定できます。このフィールドのシンタックスの例については、「セキュリティフィールドの例」項を参照してください。

ユーザーテンプレート

（注） ユーザーは、グローバルテンプレートの「パス」および「説明」のグローバル列のみを使用します。

カラム名	データ タイプ	必須かどうか	説明
LoginName	SNC	可能	アプリケーションにログインする際に使用するユーザーのログイン名
Password	パスワード（Password）	はい	新規ユーザーアカウントのパスワード
AdvancedMode	ブール	なし	ユーザが上級ユーザかどうかを判断します
FirstName	SNC	なし	ユーザの名
LastName	SNC	なし	ユーザの姓
ChangePasswordOnNextLogon	ブール	なし	最初のログイン後に、ユーザのパスワードをリセットするように指示するプロンプトを表示するかどうかを判断します
PasswordNeverExpires	ブール	なし	このユーザのパスワードに有効期限を設定するかどうかを決定します
HomeFolder	パス	なし	ユーザのホーム フォルダとして使用されるフォルダへのフォルダ パス
CreateNewUserFolder	ブール	なし	HomeFolder ロケーションのユーザーホームフォルダに新規フォルダを作成するかを決定

カラム名	データ タイプ	必須かどうか	説明
グループ	グループ名	なし	ユーザが追加されるグループ名（およびそれらのパス）のセミコロンによって区切られたリスト。グループ名は一意ではないため、/Folder1/Admins;/Folder2/Admins などのように、パスも指定する必要があります
InternetScriptEditorEnabled	ブール	なし	ユーザーがシスコの Internet Script Editor にアクセスできる Unified CCE ユーザーにリンクされるかどうか。該当する場合、次のことが適用されます。 • ログイン名が既存の Windows Active Directory ユーザーと一致する必要があります。 • インストールでシングルサインオンが使用されていない場合、指定したパスワードが対応する Active Directory ユーザーのパスワードと一致する必要があります。

プレシジョン属性テンプレート

次の表に、バルクプレシジョン属性のロードに必要な列を示します。

カラム名	データ タイプ	必須かどうか	説明
AttributeDataType	数値	可能	以下のいずれかの属性に関連付けられるデータのタイプ。 3：ブーリアン（true または false のみ） 4：習熟度（数値範囲）。
DefaultValue	属性データ型に応じたブール値または数値	はい	明示的に指定された値がない場合に、エージェントに属性が割り当てられる際に使用されるデフォルト値。
DepartmentMember	エンタープライズ名（Enterprise Name）	×	この属性が表す部署。

プレシジョン キュー テンプレート

次の表に、プレシジョンキューの一括ロードに必要なカラムを示します。

カラム名	データ タイプ	必須かどうか	説明
手順	—	可能	このプレシジョンキューの手順の仕様です。「プレシジョンキュー手順用シンタックス（269ページ）」を参照してください。
AgentOrdering	数値	可能	複数のエージェントがプレシジョンキューの条件を満たしている場合に、コールを処理するエージェントは次の順番で選択されます。 1：最も長い間、対応可能状態のエージェント 2：最もスキルが高いエージェント 3：最もスキルが低いエージェント
ServiceLevelThreshold	数値	×	0～2147483647のプレシジョンキューのルールを使用して、適切なエージェントにコールを割り当てるための、秒単位のサービスレベルしきい値。

カラム名	データ タイプ	必須かどうか	説明
ServiceLevelType	数値	なし	サービスレベルの計算で放棄されたコールは、次の順序で処理されます。 1：放棄呼を無視する 2：放棄呼をマイナスの影響（つまり、サービスレベルしきい値を超過する）として処理 3：放棄呼をプラスの影響（つまり、サービスレベルしきい値を満たす）として処理
DepartmentMember	エンタープライズ名（Enterprise Name）	×	このプレシジョンキューが表す部署。

プレシジョンキュー手順用シンタックス

[プレシジョンキュー手順（Precision Queue Steps）] フィールドは、1 つ以上の手順で構成されています。各手順は、以下の部分に分かれています。

- **Consider If** 式（オプション。ただし、手順がひとつしかない場合は無効、複数の手順がある場合は最後の手順で無効とします）。存在する場合は、この条件は手順が適用される状況を指定します。たとえば、その日に通常よりも多くの未応答通話がある場合のみ手順が適用される場合があります。
- **条件式**（各手順で常に必須）。この条件は、エージェントが通話を受信するために必要な属性を指定します。これは、単純な比較の場合もありますし、*and* または *or* によってリンクされた複数の比較が含まれる場合もあります。たとえば、条件式はスペイン語を話し、住宅ローンを販売する訓練を受け、ロンドン在住のエージェントを指定する場合があります。
- **Wait Time**（最後の手順を除き常に必要）この条件は、この手順で条件を満たすことができない場合に、次の手順に移る前の秒単位の時間を指定します。たとえば、待機時間の値が 20 の場合、20 秒が経過した時点でその手順の条件と一致するエージェントがない場合は、次の手順が検討されることを意味します。

（注） これらのコンポーネントから [手順（Steps）] フィールドを構築するには、以下の例で示されているとおり、各手順をセミコロン（;）で区切り、各手順の部分をコロン（:）で区切ります。

例： ENGLISH1==5:WaitTime=22;ENGLISH1==5:WaitTime=20;ENGLISH==5

「English1」および「English」は、プレシジョン属性のエンタープライズ名を示します。

次の例は、3 つの手順を含む [手順（Steps）] フィールドを示しています。最初の手順には、**Wait Time** 式と条件式があります。 2 つ目には、**Consider If** 式と **Wait Time** 式、そして条件式があります。3 つ目は、最後の手順であるため、条件式のみがあります。

最初の手順：

手順の条件を満たすために待機する時間を秒単位で指定します。このシンタックスるは、手順の一部なので、コロンで終了します。

```
WaitTime=10:
```

使用される条件式を指定します。このシンタックスは、手順の最後なので、セミコロンで終了します。

```
Spanish >= 5 && MortgageTrained == True && Location == London;
```

2 つ目の手順：

この手順を考慮する状況を指定します。このシンタックスは、手順の一部なので、コロンで終了します。Consider If ステートメントのシンタックスについては、以下の注意を参照してください。

```
ConsiderIf=TestforSituation:
```

手順の条件を満たすために待機する時間を秒単位で指定します。このシンタックスるは、手順の一部なので、コロンで終了します。

```
WaitTime=20:
```

使用される条件式を指定します。このシンタックスは、手順の最後なので、セミコロンで終了します。

```
Spanish >= 5 && MortgageTrained == True;
```

3 つ目の手順：

前の手順に失敗した場合に使用される条件式を指定します。

```
(Spanish >= 5) || (Spanish >=3 && MortgageTrained == True),
```

ロールの管理

ロールは、グループ化し、ユーザーまたはグループに適用できるタスク一式です。タスクと同様に、ロールは、フォルダベースのタスク一式が含まれるフォルダベースにすることも、グローバルタスク一式が含まれるグローバルベースにすることもできます。フォルダロールは常にフォルダに適用されます。特定のフォルダロールを持つユーザーは、そのフォルダ内の項目に対してそのロールのすべてのタスクを実行できます。グローバルロールを持つユーザーは、そのグローバルロールのすべてのタスクを実行できます。

デフォルト ロール

次のデフォルトロールがシステムで提供されます。

- **デフォルトのグローバルロール**
  - **Global Basic** - ユーザーに対して基本的なプロビジョニングと機能管理を許可します。

- **Global Advanced** - ユーザーに対して、詳細なプロビジョニングと機能管理を許可します。これには、global basic role で許可されている操作も含まれます。
- **Global Host** - ユーザーに対して、すべてのライセンス済み機能の使用を許可します。

- デフォルトのフォルダロール
  - **Supervisor** - ユーザーに対して指定したフォルダ内のユーザーとリソースの管理を許可します。
  - **Basic** - ユーザーに対して、大部分のリソースの参照と指定フォルダ内のレポートとパラメーター式の管理を許可します。
  - **Advanced** - ユーザーに対して、指定フォルダ内の大部分のリソースの参照とアクセスを許可します。これには、basic folder role と the supervisor folder role で許可されている操作も含まれます。
  - **Full Permissions** - ユーザーに対して、指定フォルダ内のすべてのライセンス済み機能の使用を許可します。

グローバルロールの作成

グローバルロールを作成するには、以下の手順を実行します。

手順

ステップ 1 管理者として、CCDM ポータルにログインします。
ステップ 2 バーガーアイコンをクリックし、**[セキュリティ（Security）]** > **[ロール（Roles）]** > **[グローバルロール（Global Roles）]** の順に選択します。
ステップ 3 [New] をクリックします。
ステップ 4 **[名前（Name）]** フィールドに、目的のユーザーの権限またはカテゴリを反映する新しいロール名を入力します。
ステップ 5 オプションで、**[説明（Description）]** フィールドに説明を入力します。これは、付与された権限の概要などを入力できます。
ステップ 6 有効化するロールのタスクを選択します。
ステップ 7 [保存（Save）] をクリックします。

グローバルロールの割り当て

グローバルロールを持つユーザーを割り当てるには、以下の手順を実行します。

手順

ステップ 1 管理者としてログインし、次を構成してグローバル権限を付与または削除します。

a) **[グローバルロール（Global Roles）]** ウィンドウで、ユーザーまたはグループに割り当てるグローバルロールを選択します。

b) **[メンバー（Members）]** をクリックします。

c) **[メンバーの追加（Add Members）]** をクリックします。

d) [フォルダツリー（Folder Tree）] パネルで、ユーザーまたはグループを割り当てるフォルダを選択します。

（注） 上部のフィールドを使用すると、ビューをフィルタ処理でき、たとえば、ユーザーだけまたはグループだけを表示したり、特定の名前を検索したりできます。

e) 新規追加されたメンバーのチェックボックスをオンにします。

（注） 複数のフォルダからユーザおよびグループを選択できます。

f) [OK] をクリックします。

g) [保存（Save）] をクリックします。

ステップ 2 このグローバルロールからユーザーまたはグループを削除するには、削除アイコンをクリックし、**[確認（Confirm）]** をクリックします。

グローバルロールの編集

グローバルロールを編集するには、以下の手順を実行します。

手順

ステップ 1 管理者としてログインし、**[セキュリティ（Security）]** > **[ロール（Roles）]** > **[グローバルロール（Global Roles）]** の順に選択します。

ステップ 2 編集するグローバルロールを選択します。

ステップ 3 必要に応じて、**[詳細（Details）]** タブをクリックし、詳細を変更します。

ステップ 4 **[有効（Enabled）]** チェックボックスをオンにし、グローバルロールをユーザーが使用できるようにします。

ステップ 5 **[非表示（Hidden）]** チェックボックスをオンにし、システムユーザーに対してグローバルロールを非表示にします。

ステップ 6 **[タスク（Tasks）]** タブを選択し、グローバルロールに追加したタスクのチェックボックスをオンにし、グローバルロールから削除したタスクのチェックボックスをオフにします。

ステップ 7 [保存（Save）] をクリックします。

グローバルロールの削除

グローバルロールを削除するには、以下の手順を実行します。

手順

ステップ 1 システム管理者としてログインし、セキュリティの **[グローバルロール（Global Roles）]** をクリックします。

ステップ 2 **[グローバルロール（Global Roles）]** ウィンドウで、削除するグローバルロールのチェックボックスをオンにし、**[削除（Delete）]** をクリックします。

ステップ 3 [OK] をクリックして、削除を実行します。

フォルダロールの作成

フォルダロールを作成するには、以下の手順を実行します。

手順

ステップ 1 CCDM ポータルにシステム管理者としてログインします。

ステップ 2 バーガーアイコンをクリックし、**[セキュリティ（Security）]** > **[ロール（Roles）]** の順に選択します。

ステップ 3 **[ロール（Roles）]** ウィンドウで、**[新規（New）]** をクリックします。

ステップ 4 **[名前（Name）]** フィールドに、目的のユーザーの権限またはカテゴリを反映する新しいロール名を入力します。

ステップ 5 オプションで、**[説明（Description）]** フィールドに説明を入力します。これは、付与された権限の概要などを入力できます。

ステップ 6 有効化するロールのタスクを選択します。

ステップ 7 [保存（Save）] をクリックします。

フォルダロールの割り当て

フォルダロールを割り当てるには、以下の手順を実行します。

手順

ステップ 1 CCDM ポータルに管理者としてログインし、**[セキュリティ（Security）]**>**[権限（Permissions）]** の順に選択します。

ステップ 2 [セキュリティマネージャ（Security Manager）] でフォルダロールを割り当てるユーザーまたはグループを含むフォルダツリーのロケーションをクリックします。次に、次のいずれかを実行します。

- [ユーザ（Users）] タブをクリックして、そのフォルダ内のユーザを表示します。（または）
- **[グループ（Groups）]** タブをクリックし、フォルダのユーザーを表示します。

ステップ 3 権限を編集するユーザーまたはグループの横にあるチェックボックスをオンにします。

ステップ 4 [権限の変更（Change Permissions）] をクリックして、選択したユーザまたはグループのフォルダ ロールを変更します。

ステップ 5 現在のフォルダは権限を継承していることを示すメッセージが表示された場合に、このプロセスを停止し、このフォルダに別の権限を設定するには、**[アイテムセキュリティの編集（Edit Item Security）]** をクリックし、**[OK]** クリックして、アクションを確認します。フォルダに別の権限を設定しない場合は、**[キャンセル（Cancel）]** をクリックします。

ステップ 6 フォルダロールの設定を継続する場合は、[フォルダ権限（Folder Permissions）] ダイアログボックスで画面左のフォルダツリーからフォルダロケーションを選択し、画面右で、1つ以上のフォルダロールを選択します。

ステップ 7 変更した権限を選択したフォルダのサブフォルダにもコピーする場合は、**[サブフォルダの権限を変更（Change Permissions for Subfolders）]** チェックボックスをオンにします。

ステップ 8 **[保存（Save）]** をクリックし、変更したフォルダロールのサマリーを表示します。

ステップ 9 [確認（Confirm）] をクリックして、新しいフォルダ ロールを適用します。

フォルダロールの編集

フォルダロールを編集するには、以下の手順を実行します。

手順

ステップ 1 管理者としてCCDMポータルにログインし、**[セキュリティ（Security）]** の **[ロール（Roles）]** をクリックします。

ステップ 2 ロールマネージャで編集するフォルダロール名をクリックします。

ステップ 3 フォルダ ロールに追加するタスクのチェックボックスをオンにして、フォルダ ロールから削除するタスクのチェックボックスをオフにします。

ステップ 4 [保存（Save）] をクリックして変更を保存します。

フォルダロールの削除

フォルダロールを削除するには、以下の手順を実行します。

手順

ステップ 1 フォルダロールを削除するには、ロールマネージャで、削除するフォルダロールの横にあるチェックボックスをオンにします。

ステップ 2 **[削除（Delete）]** > **[OK]** の順に選択します。

使用中のフォルダロールは削除できません。

グローバルロールタスク

基本、上級、ホスト、システム管理者などのグローバルロールは、ユーザーまたはユーザーのグループに適用され、それぞれがアクセス権を持つすべてのフォルダで、同じ機能セットにアクセスできるようにします。次の表に、グローバルロールに構成可能なすべての使用可能なタスクのリストを示します。これらのタスクは、[セキュリティ（Security）] > [グローバル（Global）] の順に選択します。

グローバルタスク名	コメント	Basic 版	Advanced 版
セキュリティマネージャ	ユーザーのツールページにセキュリティマネージャとセキュリティ マネージャ オプションを表示します。		x
サービスマネージャ	ツールページにサービスマネージャを表示します。		x
システムマネージャ	ツールページにシステムマネージャを表示します。		x
上級ユーザー	ユーザー設定ページにチェックボックスを表示し、起動時にツールページを表示する上級ユーザーモードにアクセスできるようにします。		x
拠点管理	設定ページで、ユーザーによるシステム設定、セキュリティ設定、レポーティング設定、プロビジョニング設定の保存を許可します。		
自己スキル	設定ページで、ユーザーによるシステム設定、セキュリティ設定、レポーティング設定、プロビジョニング設定の保存を許可します。		

グローバルタスク名	コメント	Basic 版	Advanced 版
ロールの参照	ロールマネージャとセキュリティマネージャにフォルダベースのロールを表示することをユーザーに許可します。		x
ロールの管理	[セキュリティマネージャ（Security Manager）] > [ロールマネージャ（Role Manager）] の順に選択し、フォルダベースのロールを作成、修正および削除することをユーザーに許可します。		
グローバルロールの参照	グローバルセキュリティマネージャでグローバルロールを表示することをユーザーに許可します。		x
グローバルロールの管理	グローバルセキュリティマネージャを使用して、グローバルロールを追加、編集および削除することをユーザーに許可します。		
グローバルセキュリティの参照	ホームページのセキュリティマネージャツール内で、グローバルセキュリティマネージャを有効化します。アクセスは表示専用です。ロールは編集できません。		x
グローバルセキュリティの管理	ツールページのセキュリティマネージャツール内でグローバルセキュリティマネージャオプションを表示し、ユーザーが、グローバルセキュリティロールの表示と編集をできるようにします。		
ディメンションタイプの参照	レポートにパラメータ設定を作成する際に、エージェントやコールタイプなどのディメンションタイプをユーザーが、[項目タイプ（Item Type）] ドロップダウンリストで選択できるようにします。	x	x
ディメンションの一括インポート	レポートにパラメータ設定を作成する際に、エージェントやコールタイプなどのディメンションタイプをユーザーが、[項目タイプ（Item Type）] ドロップダウンリストで選択できるようにします。		x

グローバルタスク名	コメント	Basic 版	Advanced 版
エージェントのプロビジョニング	指定したフォルダでユーザーに Manage Dimensions への権限が付与され、[接続されたシステムの参照（Browse Connected Systems）] が有効化されている場合に限り、システムマネージャまたはエージェントチームマネージャを使用してエージェントを作成および管理することができます。	x	x
エージェントデスクトップのプロビジョニング	指定したフォルダでユーザーに Manage Dimensions への権限が付与され、[接続されたシステムの参照（Browse Connected Systems）] が有効化されている場合に限り、ユーザーが、システムマネージャで、[新規（New）] > [リソース（Resource）] メニューの順に選択し、エージェントデスクトップを追加することを許可します。		x
エージェントチームのプロビジョニング	システムマネージャの [新規（New）]>[リソース項目（Resource Items）] メニューから [エージェントチーム（Agent Team）] 項目をフォルダ追加することができます。	x	x
コールタイプのプロビジョニング	システムマネージャを使用して、[新規（New）] > [リソース項目（Resource Items）] メニューから、フォルダに新しいコールタイプを追加することができます。		x
着信番号のプロビジョニング	新しい着信番号のプロビジョニングをユーザーに許可します。		x
電話番号のプロビジョニング	新しい電話番号のプロビジョニングをユーザーに許可します。		x
エンタープライズ スキル グループのプロビジョニング	新しいエンタープライズ スキル グループのプロビジョニングをユーザーに許可します。		x
拡張コール変数のプロビジョニング	[拡張コール変数（Expanded Call Variable）] の作成をユーザーに許可し、[システムマネージャ（System Manager）]>[新規リソース（New Resource）] の順に選択し、その設定とアクティブな日付を管理できるようにします。		x

グローバルタスク名	コメント	Basic 版	Advanced 版
ラベルのプロビジョニング	[システムマネージャ（System Manager）] >[リソースフォルダ（Resource Folder）]> [リソースアイテム（Resource Item）] の順に選択し、ユーザーにラベルを作成することを許可します。		x
個人のプロビジョニング	指定したフォルダでユーザーに Manage Dimensions への権限が付与され、[接続されたシステムの参照（Browse Connected Systems）] が有効化されている場合に限り、システムマネージャまたはサービスマネージャを使用してユーザーが個人をプロビジョニングできるようにします。		x
サービスのプロビジョニング	サービスレベルタイプ、関連付けられたスキルグループおよび周辺機器の設定を含むシステムマネージャを使用したサービスのプロビジョニングや管理をユーザーに許可します。		x
スキルグループのプロビジョニング	スキルグループが配置されているフォルダの Manage Dimensions への権限がユーザーに付与されている場合に限り、（サービスマネージャ内の）システムマネージャ、スキルグループマネージャを使用してスキルグループの管理をユーザーに許可します。		x
ユーザー変数のプロビジョニング	システムマネージャを使用してユーザー定義の変数のプロビジョニングをユーザーに許可します。		x

フォルダベースのロール

このロールを特定のフォルダに適用すると、フォルダベースのロールに割り当てられているユーザー、そのフォルダ限定のタスクベースの権限へのアクセス権を保持できます。次の表に、[セキュリティマネージャ（Security Manager）] の [ロールマネージャ（Role Manager）] を使用してフォルダベースのロールを作成するために使用できるタスクを示します。Basic、Supervisor および Advanced 列には、Unified CCDM で事前設定済みロールに対してデフォルトでたしくが有効化されているかどうかが示されます。

名前	コメント	基本	スーパーバイザ	Advanced
フォルダ設定				

フォルダの参照	ユーザーがフォルダツリーのフォルダを参照できるようにします。	x		x
フォルダの管理	ユーザが指定フォルダ内のフォルダを編集、作成および削除できるようにします。			x
ユーザーおよびセキュリティ				
ユーザーの参照	ユーザーが指定フォルダ内のすべてのユーザーの詳細を表示できるようにします。	x		x
ユーザの管理	ユーザーが指定フォルダ内のユーザー設定を変更できるようにします。		x	x
パスワードのリセット	ユーザーが指定フォルダ内の他のユーザーパスワードをリセットできるようにします。			x
テナントの管理	ユーザーが指定フォルダ内のテナント項目を管理できるようにします。			
セキュリティの管理	ユーザーが指定フォルダ内のセキュリティ権限を変更できるようにします。セキュリティ マネージャ ツールへのアクセス権限が必要です。			x
ディメンションとプレフックス				
ディメンションの参照	ユーザーが指定フォルダ内のシステムリソースを一覧できるようにします。	x		x
ディメンションの管理	ユーザーがシステムマネージャを使用して、指定フォルダ内のエージェント、エージェントチーム、スキルグループなどのディメンションを編集、移動、削除できるようにします。		x	x
ディメンション メンバーシップの管理	ユーザーがディメンション メンバーシップを追加、変更、削除できるようにします。			

ディメンションのクローン	ユーザーがエージェントをコピーできるようにします。		x	
プレフィックスの参照	ユーザーがシステムマネージャのテナント項目の [プレフィックス詳細（prefix details）] タブにある指定フォルダ内の自動リソース移動プレフィックスを参照できるようにします。			x
プレフィックスの管理	ユーザーがシステムマネージャのテナント項目の [プレフィックス詳細（prefix details）] タブにある指定フォルダ内の自動リソース移動プレフィックスを追加および削除できるようにします。			

ガジェットの構成

ガジェットを構成するには、以下の操作を実行します。

- ガジェットの作成 （280 ページ）
- ガジェットの編集 （281 ページ）
- ガジェットの削除 （281 ページ）

ガジェットの作成

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして CCDM ポータルにログインします。

ステップ 2 **[ガジェット（Gadget）]** をクリックします。

ステップ 3 ドロップダウンリストで **[ガジェットの追加（Add Gadget）]** を選択します。

ステップ 4 **[リソースマネージャ（Resource Manager）]** をクリックします。

ステップ 5 バーガーアイコンをクリックし、テナントを選択します。

ステップ 6 検索バーのリストからリソースを選択します。

リストには、エージェント、エージェントデスクトップ、エージェントチーム、コールタイプ、部署、ダイヤル番号、エンタープライズ スキル グループ、転送通話変数、ラベル、ネットワーク Vru スクリプト、個人、プレシジョン属性、プレシジョンキュー、サービス、サービス、スキルグループ、およびユーザー変数が含まれます。

ステップ 7 **[ガジェット（Gadget）]** > **[アプリの保存（Save App）]** の順に選択し、ガジェットの名前を入力し、フォルダを参照してガジェットを保存します

ガジェットの編集

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして CCDM ポータルにログインします。

ステップ 2 **[ガジェット（Gadget）]**>**[アプリを開く（Open App）]** の順に選択し、作成するアプリを選択します。

ステップ 3 変更するガジェットを選択します。

ステップ 4 ガジェットを変更するために必要なテナントと必要なリソースを選択します。

ステップ 5 **[アプリ名（App Name）]** > **[アプリを保存（Save App）]** の順に選択し、 **[はい（Yes）]** をクリックし、修正したフィールドを保存します。

ガジェットの削除

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして CCDM ポータルにログインします。

ステップ 2 **[ガジェット（Gadget）]**>**[アプリを開く（Open App）]** の順に選択し、アプリを選択します。

ステップ 3 アプリから削除するガジェットを選択し、**[削除（Delete）]** をクリックします。

ステップ 4 **[保存（Save）]** をクリックしてアプリを保存します。

（注） アプリを削除するには、**[ガジェット（Gadget）]** > **[アプリの削除（Delete App）]** の順に選択し、**[OK]** をクリックします。

Administration Workstation を使用した Unified CCE のプロビジョニング

Administration Workstationを使用して Unified CCE をプロビジョニングするには、以下の手順を実行します。

（注）
- ICMdba ツールを使用してアップロードする基本構成は、Unified CCE のその他必要な要素を自動的にプロビジョニングします。
- Administration Workstations はリモートデスクトップにもアクセスできます。ただし、一度に 1 人のユーザーしか Workstation にアクセスできません。Unified CCE は、同じ Workstation 上の複数のユーザーによる同時アクセスをサポートしていません。

エージェント ターゲット ルールの設定

個々のエージェント ターゲティング ルールを構成するには、以下の手順を実行します。

手順

ステップ 1 構成マネージャで、**[ICMの構成（Configure ICM）]** > **[ターゲット（Targets）]** > **[デバイス ターゲット（Device target）]** > **[エージェントターゲティングルール（Agent Targeting Rule）]** または **[ツール（Tools）]** > **[ツールを一覧（List Tools）]** > **[エージェントターゲティングルール（Agent Targeting Rule）]** の順に選択します。

ステップ 2 [ICMエージェントターゲティングルール（ICM Agent Targeting Rules）] ダイアログボックスで、**[検索（Retrieve）]** をクリックします。

ステップ 3 **[追加（Add）]** をクリックします。

ステップ 4 ルールの名前を入力します。

ステップ 5 ルールを関連付ける周辺機器を選択します。

ステップ 6 [ルールタイプ（Rule Type）] ドロップダウンリストで、**[エージェントの内線番号（Agent Extension）]** を選択します。

ステップ 7 ルート要求を開始できるルーティングクライアントを 1 つ以上選択します。

ステップ 8 エージェントの内線番号の範囲を入力します。

ステップ 9 [保存（Save）] をクリックします。

Web Administration を使用した Unified CCE のプロビジョニング

• 理由コードの設定 （282 ページ）

理由コードの設定

理由コードを構成するには、以下の手順を実行します。

手順

ステップ 1 **CCE Web 管理**ページにログインし、**[管理（Manage）]** > **[理由コード（Reason Codes）]** の順に選択します。

ステップ 2 理由コードの一覧ページで、**[新規（New）]** をクリックし、新規理由コードページを開きます。

ステップ 3 次のようにフィールドに入力します。

a) **[テキスト（Text）]** フィールドに、理由コードに関連するテキストを入力します。

b) **[コード（Code）]** フィールドに、一意の正数を入力します。

c) オプションで、**[説明（Description）]** フィールドに理由コードの説明を入力します。

ステップ 4 理由コードを保存し、リストページに戻ります。ここで、理由コードが正常に作成されたことがメッセージで表示されます。

Internet Script Editor を使用したルーティングスクリプトのプロビジョニング

ISE にログインするには、以下の手順を実行します。

手順

ステップ 1 Launch Internet Script Editor `iscriptEditor.exe` を起動します。

ステップ 2 ユーザー名、パスワードおよびドメインを入力します。

例：

ISE ユーザーの形式が iseuser1@domain.com の場合、ユーザー名はiseuser1 に、ドメインは domain.com になりま

ステップ 3 **接続**をクリックします。

ステップ 4 [AWサーバーアドレス（AW Server Address）]、[ポート（Port）]、および[ICMインスタンス名（ICM Instance Name）] を入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 [OK] をクリックします。

必要に応じて、Internet Script Editor をアップグレードします。

（注） ログイン後、リンクされた Unified CCDM ユーザーが表示できるスクリプト項目のみが表示されます。

Unified CVP Administration

• Unified CCDM を使用した Unified CVP のプロビジョニング （283 ページ）

Unified CCDM を使用した Unified CVP のプロビジョニング

• メディアファイルのアップロード （284 ページ）
• IVR スクリプトのアップロード （284 ページ）

メディアファイルのアップロード

手順

ステップ 1 CCDM ポータルにログインします。

ステップ 2 **[リソースマネージャ（Resource Manager）]** の順に選択し、デフォルトのインポートテナントに割り当てられた CVP に移動します。

ステップ 3 **[リソース（Resource）]** をクリックし、**Mediafile** を選択します。

ステップ 4 ファイルをアップロードするメディアサーバーを選択します。

ステップ 5 **[ファイルを追加（Add file(s)）]** をクリックして、メディアファイルを追加します。

ステップ 6 [保存（Save）] をクリックします。

IVR スクリプトのアップロード

手順

ステップ 1 CCDM ポータルにログインします。

ステップ 2 、**リソースマネージャ**で、デフォルトのインポートテナントに割り当てられた CVP を選択します。

ステップ 3 **[リソース（Resource）]** をクリックし、**IVR アプリ**を選択します。

ステップ 4 IVR スクリプトをアップロードする必要がある VXML サーバーを選択します。

ステップ 5 **[ファイルの追加（Add file(s)）]** をクリックして、IVR ファイル（.zip ファイル）を追加します。

ステップ 6 [保存（Save）] をクリックします。

Unified Communication Manager Administration

UCDM を使用した Unified Communications Manager のプロビジョニング

UCDM オブジェクトの CRUD 操作

次の表に、UCDM オブジェクトの作成、更新、または削除操作の情報を示します。

（注） 一括アップロードは、作成操作でのみでサポートされます。参照 UCDM オブジェクトの CRUD 操作 （285 ページ）

オブジェクト	作成	読み取り	更新	削除	一括アップロード
コンタクトセンターサーバー 参照 コンタクトセンターサーバーの構成 （287 ページ）	x	x	x	x	x
Contact Center Services 参照 コンタクトセンターサービスの構成 （289 ページ）	x	x	x	x	x

オブジェクト	作成	読み取り	更新	削除	一括アップロード
SIP トランク 参照 SIP トランクの構成 （290 ページ）	x	x	x	x	x
[ルート グループ（Route Group）] 参照 ルートグループの構成 （293 ページ）	x	x	x	x	x
[ルート リスト（Route List）] 参照 ルートリストの構成 （295 ページ）	x	x	x	x	x
ルート パターン 参照 ルートパターンの構成 （297 ページ）	x	x	x	x	x
電話番号および回線 参照 電話番号インベントリと回線の構成 （301 ページ）	x	x	x	x	x
[電話（Phones）] 参照 電話機の設定 （302 ページ）	x	x	x	x	x
地域 参照 リージョンの構成 （305 ページ）	x	x	x	x	x

オブジェクト	作成	読み取り	更新	削除	一括アップロード
サービスクラス 参照 サービスクラスの構成（307 ページ）	x	x	x	x	x
[デバイスプール（Device Pools）] 参照 デバイスプールの構成（299 ページ）	x	x	x	x	x

コンタクトセンターサーバーおよびコンタクトセンターサービスのプロビジョニング

ここでは、コンタクトセンターサーバーおよびコンタクトセンターサービスの構成手順に関して説明します。サーバーを構成すると、エージェントからエージェントに通話を転送中にCisco Unified Communications Manager が Contact Center と通信できるようになり、通話を Customer Voice Portal（CVP）にルーティングできます。サービスを構成すると、コンタクトセンタープロセスの CUBE に内部サービスコールをルーティングできます。

コンタクトセンターサーバーの構成

コンタクトセンターサーバーは、特定の Cisco Unified Communications Manager に割り当てられたお客様に対してのみ構成できます。

- コンタクトセンターサーバーの追加（287 ページ）
- コンタクトセンターサーバーの編集（288 ページ）
- コンタクトセンターサーバーの削除（289 ページ）

コンタクトセンターサーバーの追加

手順

ステップ 1 プロバイダまたはリセラーの管理者ログイン情報を使用して UCDM サーバーにログインします。

ステップ 2 カスタマーレベルに応じて階層を設定します。

ステップ 3 **[サービス（Services）]** > **[コンタクトセンター（Contact Center）]** > **[サービス（Services）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 コンタクトセンターサーバー名を入力します。

ステップ 6 **[CUCM]** ドロップダウンリストで適切な Cisco Unified Communications Manager を選択します。

ステップ 7 転送会議パターン番号を入力します。
これにより、CTIルートポイントが作成され、デフォルトのアプリケーションユーザー（pguser）に関連付けられます。

ステップ 8 ネットワーク VRU パターンを入力します。
これにより、CVP トランクと CUBE トランクに関連付けられたルートパターンが作成されます。

ステップ 9 [SIPトランク（SIP trunk）] セクションを展開し、CVP トランクを構成します。

a) **[トランク接続先タイプ（Trunk Destination Type）]** ドロップダウンリストで **[CVP**トランク（CVP Trunk）] を選択します。

b) **[宛先アドレス（Destination Addresses）]** を展開し、トランク宛先アドレスとトランク宛て先ポートを入力します。

c) ドロップダウンリストで適切なトランク セキュリティ プロファイルを選択します。

ステップ 10 [SIPトランク（SIP trunk）] セクションを展開し、CUBEE トランクを構成します。

a) **[トランク接続先タイプ（Trunk Destination Type）]** ドロップダウンリストで **[CUBEE**トランク（CUBEE Trunk）] を選択します。

b) **[宛先アドレス（Destination Addresses）]** を展開し、トランク宛先アドレスとトランク宛て先ポートを入力します。

c) ドロップダウンリストで適切なトランク セキュリティ プロファイルを選択します。

ステップ 11 [保存（Save）] をクリックします。

コンタクトセンターサーバーの編集

手順

ステップ 1 プロバイダまたはリセラーの管理者ログイン情報を使用して UCDM サーバーにログインします。

ステップ 2 カスタマーレベルに応じて階層を設定します。

ステップ 3 **[サービス（Services）]** > **[コンタクトセンター（Contact Center ）]** > **[サービス（Services）]** の順に選択します。

ステップ 4 編集するコンタクトセンターサーバーをクリックし、必須フィールドを変更します。

（注） コンタクトセンターのサーバー名は変更できません。

ステップ 5 [保存（Save）] をクリックします。

コンタクトセンターサーバーの削除

始める前に

コンタクトセンターサーバーに関連付けられているコンタクトセンターサービスとパラメータを削除します。

手順

ステップ 1 プロバイダまたはリセラーの管理者ログイン情報を使用して UCDM サーバーにログインします。

ステップ 2 カスタマーレベルに応じて階層を設定します。

ステップ 3 **[サービス（Services）]** > **[コンタクトセンター（Contact Center ）]** > **[サービス（Services）]** の順に選択します。

ステップ 4 削除するコンタクトサーバーをクリックします。

ステップ 5 [保存（Save）] をクリックします。

コンタクトセンターサービスの構成

- コンタクトセンターサービスの追加 （289 ページ）
- コンタクトセンターサービスの編集 （290 ページ）
- コンタクトセンターサービスの削除 （290 ページ）

コンタクトセンターサービスの追加

手順

ステップ 1 プロバイダまたはリセラーの管理者ログイン情報を使用して UCDM サーバーにログインします。

ステップ 2 階層をお客様または拠点レベルに設定します。

ステップ 3 **[サービス（Services）]** > **[コンタクトセンターサービス（Contact Center Service）]** > **[サービス（Services）]** を選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 コンタクトセンターサービス名を入力します

ステップ 6 ドロップダウンリストで関連付けたコンタクトセンターサービス名を選択します。

ステップ 7 **[内部サービス番号（Internal Service Numbers）]** セクションを展開し、サービス番号パターン（内部サービスコールを CUBE にルーティングするために使用されるパターン）を入力します。

ステップ 8 [保存（Save）] をクリックします。

（注） UCDMにコンタクトセンターサーバーとサービスを追加すると、デフォルト設定としてアプリケーションユーザー、トランク、CTIルートポイント、ルートグループ、ルートパターンが作成されます。

その他のCTIルートポイントについては、「CTIルートポイントの設定 （524ページ）」を参照してください。

コンタクトセンターサービスの編集

手順

ステップ1 プロバイダまたはリセラーの管理者ログイン情報を使用してUnified CDMサーバーにログインします。

ステップ2 カスタマーレベルに応じて階層を設定します。

ステップ3 **[サービス（Services）]** > **[コンタクトセンター（Contact Center ）]** > **[サービス（Services）]** の順に選択します。

ステップ4 編集するコンタクトセンターサービスをクリックし、必須フィールドを変更します。

（注） コンタクトセンターサービス名は変更できません。

ステップ5 [保存（Save）] をクリックします。

コンタクトセンターサービスの削除

手順

ステップ1 プロバイダまたはリセラーの管理者ログイン情報を使用してUnified CDMサーバーにログインします。

ステップ2 カスタマーレベルに応じて階層を設定します。

ステップ3 **[サービス（Services）]** > **[コンタクトセンター（Contact Center ）]** > **[サービス（Services）]** の順に選択します。

ステップ4 削除するコンタクトセンターサービスをクリックします。

ステップ5 [削除（Delete）] をクリックします。

SIPトランクの構成

- SIPトランクの追加 （291ページ）
- SIPトランクの編集 （292ページ）

• SIP トランクの削除 （292 ページ）

SIP トランクの追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[SIP トランク（SIP Trunks）]** に移動します。

- プロバイダまたはリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[SIP トランク（SIP Trunks）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[SIP トランク（SIP Trunks）]** の順に選択します。

ステップ 4 **[追加（Add）]** をクリックし、トランクを作成します。

ステップ 5 **[デバイス情報（Device Information）]** タブで、以下の手順を実行します。

a) SIP トランクを追加する **[Cisco Unified Communications Manager]** ドロップダウンリストから必要な IP アドレスを選択します。
b) **[デバイス名（Device Name）]**フィールドに固有の SIP トランク名を入力します。
c) ドロップダウンリストで、**[デバイスプール（Device Pool）]** を選択します。
d) 必要に応じて、**[すべてのアクティブなUnified CMノードを実行する（Run On All Active Unified CM Nodes）]** チェックボックスをオンにします。

ステップ 6 **[SIP情報（SIP Info）]** タブに移動し、以下を実行します。

a) **[接続先（Destination）]** パネルで **[追加（Add）]** アイコンをクリックします。
b) **[アドレスIPv4（Address IPv4）]** フィールドに宛先 IP アドレスを入力します。

（注） Cisco Unified Communications Manager から CVP、CUBE、またはその他の接続先への SIP トランクを作成するには、それぞれのデバイスの IP アドレスを入力します。

c) 必要に応じて**ポート**を変更します。
d) 複数の接続先を優先順位付けするには、**[ソート順（Sort Order）]** を入力します。

（注） 値が小さいほど、優先順位が高くなります。

e) **[SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]** ドロップダウンリストで適切なオプションを選択します。
f) ドロップダウンリストで、**sip profile** を選択します。

別のトランクを追加するには、この手順を繰り返します。

ステップ 7 [保存（Save）] をクリックします。

SIP トランクの編集

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[SIP トランク（SIP Trunks）]** に移動します。

- プロバイダまたはリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[SIP トランク（SIP Trunks）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[SIP トランク（SIP Trunks）]** の順に選択します。

ステップ 4 編集する SIP トランクをクリックし、必須フィールドを変更します。

ステップ 5 [保存（Save）] をクリックします。

SIP トランクの削除

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[SIP トランク（SIP Trunks）]** に移動します。

- プロバイダまたはリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[SIP トランク（SIP Trunks）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[SIP トランク（SIP Trunks）]** の順に選択します。

ステップ 4 削除する SIP トランクをクリックします。

ステップ 5 [削除（Delete）] をクリックします。

ルートグループの構成

始める前に

SIP トランクが構成されていることを確認します。SIP トランクの構成 （290 ページ）を参照してください。

ルートグループを構成するには、以下の手順を実行します。

- ルートグループの追加 （293 ページ）
- ルートグループの編集 （294 ページ）
- ルートグループの削除 （294 ページ）

ルートグループの追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートグループ（Route Groups）]** に移動します。

- プロバイダとリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[ルートグループ（Route Groups）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートグループ（Route Groups）]** の順に選択します。

ステップ 4 **[追加（Add）]** をクリックして、ルートグループを作成します。

ステップ 5 **[CUCM]** ドロップダウンリストで必要な IP アドレスを選択し、ルートグループを追加します。

ステップ 6 **[ルートグループ名（Route Group Name）]** フィールドに一意の名前を入力します。

ステップ 7 **[メンバー（Members）]** パネルで **[追加（Add）]** アイコンをクリックします。

ステップ 8 **[デバイス名（Device Name）]** ドロップダウンリストで適切な SIP トランクを選択します。

（注） SIP トランクを選択すると、デバイス上のすべてのポートが選択されます。

ステップ 9 [保存（Save）] をクリックします。

ルートグループの編集

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートグループ（Route Groups）]** に移動します。

- プロバイダとリセラー管理者については、**[デバイス管理（Device Management）]** > **[CUCM]** > **[ルートグループ（Route Groups）]** の順に選択します。
- カスタマー管理者については、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートグループ（Route Groups）]** の順に選択します。

ステップ 4 リストで、必要なフィールドを編集および変更するルートグループをクリックします。

ステップ 5 [保存（Save）] をクリックします。

ルートグループの削除

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートグループ（Route Groups）]** に移動します。

- プロバイダとリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[ルートグループ（Route Groups）]** の順に選択します。
- カスタマー管理者については、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートグループ（Route Groups）]** の順に選択します。

ステップ 4 リストから削除するルートグループをクリックします。

ステップ 5 [削除（Delete）] をクリックします。

ルートリストの構成

始める前に

ルートグループが構成されていることを確認します。ルートグループの構成 （293 ページ）を参照してください。

ルートリストを構成するには、以下の手順を実行します。

- ルートリストの追加 （295 ページ）
- ルートリストの編集 （296 ページ）
- ルートリストの削除 （296 ページ）

ルートリストの追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートリスト（Route List）]** に移動します。

- プロバイダとリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[ルートリスト（Route List）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートリスト（Route List）]** の順に選択します。

ステップ 4 **[追加（Add）]** をクリックし、ルートリストを作成します。

ステップ 5 ルートリストを追加するには、**[CUCM]** ドロップダウンリストで必要な IP アドレスを選択します。

ステップ 6 **[名前（Name）]** フィールドに一意のルートリスト名を入力します。

ステップ 7 **[ルートグループ項目（Route Group Items）]** パネルの **[追加（Add）]** アイコンをクリックします。

ステップ 8 **[ルートグループ名（Route Group Name）]** ドロップダウンリストでルートグループを選択します。

ステップ 9 [保存（Save）] をクリックします。

ルートリストの編集

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートリスト（Route List）]** に移動します。

- プロバイダとリセラー管理者の場合は、**[デバイス管理（Device Management）]**>**[CUCM]**>**[ルートリスト（Route List）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートリスト（Route List）]** の順に選択します。

ステップ 4 リストからルートリストをクリックし、必要なフィールドを編集および変更します。

ステップ 5 [保存（Save）] をクリックします。

ルートリストの削除

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートリスト（Route List）]** に移動します。

- プロバイダとリセラー管理者の場合は、**[デバイス管理（Device Management）]**>**[CUCM]**>**[ルートリスト（Route List）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートリスト（Route List）]** の順に選択します。

ステップ 4 リストから削除するルートリストをクリックします。

ステップ 5 [削除（Delete）] をクリックします。

ルートパターンの構成

始める前に

ルートリストが構成されていることを確認します。ルートリストの構成（295ページ）を参照してください。

ルートパターンを構成するには、以下の手順を実行します。

- ルート パターンの追加 （297 ページ）
- ルートパターンの編集 （298 ページ）
- ルートパターンの削除 （298 ページ）

ルート パターンの追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートパターン（Route Patterns）]** に移動します。

- プロバイダまたはリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[ルートパターン（Route Patterns）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートパターン（Route Patterns）]** の順に選択します。

ステップ 4 ルートパターンを作成するには、**[追加（Add）]** をクリックします。

ステップ 5 **[パターン定義（Pattern Defination）]** タブで、以下を実行します。

a) **[CUCM]** ドロップダウンリストでルートパターンを追加する必要な IP アドレスを選択します。

b) **[ルートパターン（Route Pattern）]** フィールドに一意の名前を入力します。

c) **[接続先（ルーティングリストまたはゲートウェイのどちらかのみ選択（Destination (Only Choose Route List or Gateway)）]** パネルにあるドロップダウンリストで、ルートリストまたはトランクを選択します。

ステップ 6 [保存（Save）] をクリックします。

ルートパターンの編集

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートパターン（Route Patterns）]** に移動します。

- プロバイダまたはリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[ルートパターン（Route Patterns）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートパターン（Route Patterns）]** の順に選択します。

ステップ 4 リストからルートパターンをクリックし、必要なフィールドを編集および変更します。

ステップ 5 [保存（Save）] をクリックします。

ルートパターンの削除

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[ルートパターン（Route Patterns）]** に移動します。

- プロバイダまたはリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[ルートパターン（Route Patterns）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[ルートパターン（Route Patterns）]** の順に選択します。

ステップ 4 リストから削除するルートパターンをクリックします。

ステップ 5 [削除（Delete）] をクリックします。

Cisco Unified CM グループの構成

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[Unified CMグループ（Unified CM Groups）]** に移動します。

- プロバイダとリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[Unified CMグループ（Unified CM Groups）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[Unified CMグループ（Unified CM Groups）]** の順に選択します。

ステップ 4 **[名前（Name）]**フィールドに一意の Unified CM グループ名を入力します。

ステップ 5 **[Unified CMグループアイテム（Unified CM Group items）]** パネルで、**[追加（Add）]** アイコンをクリックします。

ステップ 6 **優先順位**を入力します。

ステップ 7 **[選択済み Cisco Unified Communications Manager（Selected Cisco Unified Communications Manager）]** フィールドで、適切な Cisco Unified Communications Manager を選択します。

ステップ 8 [保存（Save）] をクリックします。

デバイスプールの構成

Cisco Unified CM グループが構成されていることを確認します。Cisco Unified CM グループの構成 （299 ページ）を参照してください。

- デバイスプールの追加 （299 ページ）
- デバイスプールの編集 （300 ページ）
- デバイスプールの削除 （301 ページ）

デバイスプールの追加

手順

ステップ 1 プロバイダ、リセラーまたはカスタマー管理者としてCisco Unified Communications Domain Managerにログインします。

ステップ 2 Cisco Unified Communications Manager を構成するノードに階層が設定されていることを確認します。

ステップ 3 **[デバイスプール（Device pool）]** に移動します。

- プロバイダ/リセラーの場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[デバイスプール（Device Pools）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[デバイスプール（Device Pools）]**の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 ドロップダウンリストで、**[ネットワークデバイスリスト（Network Device List）]** を選択します。

ステップ 6 **[デバイスプール設定（Device Pool Settings）]** タブで、以下の手順を実行します。

a) **デバイスプール名** を入力します。

b) **[Cisco Unified Communication Manager]** ドロップダウンリストでコールマネージャグループを選択します。

ステップ 7 **[ローミング感度設定（Roaming Sensitive Settings）]** タブで、以下の手順を実行します。

a) ドロップダウンリストで、**[日時グループ（Date/Time Group）]** を選択します。

b) ドロップダウンリストで **[リージョン（Region）]** を選択します。

c) ドロップダウンリストで、**[SRSTリファレンス（SRST Reference）]** を選択します。

ステップ 8 [保存（Save）] をクリックします。

デバイスプールの編集

手順

ステップ 1 プロバイダ、リセラーまたはカスタマー管理者として Cisco Unified Communications Domain Manager にログインします。

ステップ 2 **[デバイスプール（Device pool）]** に移動します。

- プロバイダ、リセラーの場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[デバイスプール（Device Pools）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[デバイスプール（Device Pools）]**の順に選択します。

ステップ 3 リストから編集するデバイスプールをクリックし、必要なフィールドを編集および変更します。

ステップ 4 [保存（Save）] をクリックします。

デバイスプールの削除

手順

ステップ 1 プロバイダ、リセラーまたはカスタマー管理者として Cisco Unified Communications Domain Manager にログインします。

ステップ 2 **[デバイスプール（Device pool）]** に移動します。

- プロバイダ/リセラーの場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[デバイスプール（Device Pools）]**の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[デバイスプール（Device Pools）]**の順に選択します。

ステップ 3 削除するデバイスプールをリストからクリックします。

ステップ 4 [削除（Delete）] をクリックします。

電話番号インベントリと回線の構成

電話番号インベントリの追加

始める前に

サイトダイヤルプランが作成されていることを確認してください。「サイトダイヤルプランの追加 （191 ページ）」を参照してください。

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層パスが適切なカスタマーに設定されていることを確認します。

ステップ 3 **[ダイヤルプラン管理（Dial Plan Management）]** > **[カスタマー（Customer）]** > **[番号管理（Number Management）]** > **[電話番号インベントリの追加（Add Directory Number Inventory）]** の順に選択します。

ステップ 4 ドロップダウンリストで電話番号を追加する**拠点**を選択します。

ステップ 5 **内線番号の開始**値を入力します。

ステップ 6 範囲を設定する場合は、**内線番号の終了**値を入力します。

ステップ 7 [保存（Save）] をクリックします。

インベントリに新しく追加された電話番号は、電話機に関連付けられていない限り、Cisco Unified Communication Manager に電話番号を追加しません。

回線の編集

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層パスが適切なカスタマーに設定されていることを確認します。

ステップ 3 **[サブスクライバ管理（Subscriber Managemet）] > [回線（Lines）]** の順に選択します。

ステップ 4 必要なフィールドを編集および変更するリストの行をクリックします。

ステップ 5 [保存（Save）] をクリックします。

回線の削除

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層パスが適切なカスタマーに設定されていることを確認します。

ステップ 3 **[サブスクライバ管理（Subscriber Managemet）] > [回線（Lines）]** の順に選択します。

ステップ 4 リストから削除する回線をクリックします。

ステップ 5 [削除（Delete）] をクリックします。

電話機の設定

始める前に

電話番号インベントリが作成されていることを確認します。「電話番号インベントリの追加（301 ページ）」を参照してください。

電話機を設定するには、以下の手順を実行します。

- 電話機の追加 （303 ページ）
- 電話機の編集 （304 ページ）

- 電話機の削除 （305 ページ）

電話機の追加

プロバイダ、リセラー、またはお客様の電話を追加するには、以下の手順を実行します。

- プロバイダまたはリセラーとして電話を追加 （303 ページ）
- カスタマーとして電話を追加 （304 ページ）

プロバイダまたはリセラーとして電話を追加

手順

ステップ 1 プロバイダまたはリセラーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なサイトに設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[電話機（Phones）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 プレフィックスが SEP の一意の**デバイス名**を入力します。

例：

SEPA1B2C3D4E5F6

ステップ 6 ドロップダウンリストで、**[製品タイプ（Product Type）]** を選択します。

（注） RSM simphone の場合は、ドロップダウンリストから Cisco 7941 SIP 以上のモデルを選択します。

ステップ 7 ドロップダウンリストで、**[デバイスプロトコル（Device Protocol）]** を選択します。

ステップ 8 ドロップダウンリストで、**[コーリングサーチスペース（Calling Search Space ）]** を選択します。

ステップ 9 ドロップダウンリストで、**[デバイスプール（Device Pool）]** を選択します。

ステップ 10 ドロップダウンリストで、**[ロケーション（Location）]** を選択します。

ステップ 11 **[回線（Lines）]** タブに移動し、以下の手順を実行します。

a) **[回線（Lines）]** パネルの **[追加（Add）]** アイコンをクリックして、回線を追加します。

b) **[Dirn]** パネルの **[パターン（Pattern）]** ドロップダウンリストから電話番号を選択します。

c) ドロップダウンリストで、**[ルートパーティション名（Route Partition Name）]** を選択します。

ステップ 12 [保存（Save）] をクリックします。

カスタマーとして電話を追加

手順

ステップ 1 Cisco Unified Communication Domain Manager にカスタマーとしてログインします。

ステップ 2 階層が適切なサイトに設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[電話機（Phones）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 ドロップダウンリストで、**[製品タイプ（Product Type）]** を選択します。

ステップ 6 ドロップダウンリストで、**[プロトコル（Protocol）]** を選択します。

（注） RSM simphone の場合は、ドロップダウンリストで Cisco 7941 SIP 以上のモデルを選択します。

ステップ 7 プレフィックスが SEP の一意の**デバイス名**を入力します。

例：

SEPA1B2C3D4E5F6

ステップ 8 ドロップダウンリストで、**[コーリングサーチスペース（Calling Search Space ）]** を選択します。

ステップ 9 **[詳細情報（Advanced Information）]** タブに移動し、以下の手順を実行します。

a) ドロップダウンリストで、**[デバイスプール（Device Pool）]** を選択します。

b) ドロップダウンリストで、**[ロケーション（Location）]** を選択します。

ステップ 10 **[回線（Lines）]** タブに移動し、以下の手順を実行します。

a) **[回線（Lines）]** パネルの **[追加（Add）]** アイコンをクリックして、回線を追加します。

b) **[Dirn]** パネルの **[パターン（Pattern）]** ドロップダウンリストで電話番号を選択します。

c) ドロップダウンリストで、**[ルートパーティション名（Route Partition Name）]** を選択します。

ステップ 11 [保存（Save）] をクリックします。

電話機の編集

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なサイトに設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[電話機（Phones）]** の順に選択します。

ステップ 4 リストから編集する電話機をクリックし、必要なフィールドを変更します。

ステップ 5 [保存（Save）] をクリックします。

電話機の削除

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なサイトに設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[電話機（Phones）]** の順に選択します。

ステップ 4 リストから削除する電話機をクリックします。

ステップ 5 [削除（Delete）] をクリックします。

リージョンの構成

リージョンの追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[デバイス管理（Device Management）]** > **[CUCM]** > **[リージョン（Regions）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 ドロップダウンリストで **[CUCM]** を選択します。

ステップ 6 **[名前（Name）]** フィールドに一意のリージョン名を入力します。

ステップ 7 **[関連リージョン（Related Regions）]** を展開します。

ステップ 8 **[イマーシブビデオの帯域幅（Kbps）（Immersive Video Bandwidth (Kbps)）]** ドロップダウンリストで **[システムデフォルトを使用（Use System Default）]** を選択します。

ステップ 9 **[オーディオ帯域幅（Kbps）（Audio Bandwidth (Kbps)）]** ドロップダウンリストでは、デフォルトの選択肢のままにします。

ステップ 10 **[ビデオの帯域幅（Kbps）（Video Bandwidth (Kbps)）]**ドロップダウンリストで**[システムデフォルトを使用（Use System Default）]** を選択します。

ステップ 11 **[オーディオコーデック優先設定（Audio Codec Preferrence）]**ドロップダウンリストで**[システムデフォルトを使用（Use System Default）]** を選択します。

デフォルト コーデックは G711U です。

ステップ 12 ドロップダウンリストで、**[リージョン名（Region Name）]** を選択します。

ステップ 13 [保存（Save）] をクリックします。

リージョンの編集

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[デバイス管理（Device Management）]** > **[CUCM]** > **[リージョン（Regions）]** の順に選択します。

ステップ 4 リストから編集するリージョンをクリックし、必要なフィールドを変更します。

ステップ 5 [保存（Save）] をクリックします。

リージョンの削除

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[デバイス管理（Device Management）]** > **[CUCM]** > **[リージョン（Regions）]** の順に選択します。

ステップ 4 削除するリージョンをクリックします。

ステップ 5 [削除（Delete）] をクリックします。

サービスクラスの構成

この手順に従って、新しいコーリングサーチスペース（CSS）を作成するか、サイトに関連付けられている既存の CSS を編集します。CSS は、デバイスまたは回線のサービスクラス（COS）、またはさまざまな機能をフィルタ処理するために COS に依存する他のテンプレートとして使用できます。

サービスクラスの追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が、お客様の有効なサイトに設定されていることを確認します。

ステップ 3 **[ダイヤルプラン管理（Dial Plan Management）]** > **[サイト（Site）]** > **[サービスクラス（Class of Service）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 一意の**サービスクラス名**を入力します。

この名前には、英数字、ピリオド、下線、ハイフン、スペースを使用できます。50 文字を超えることはできません。また、システムで使用可能なマクロを使用して、サービスクラス名を作成することもできます。マクロを使用すると、拠点 ID、カスタマー ID、およびその他のタイプの情報を CSS に動的に追加できます。

例：

Cu1-24HrsCLIP-PT-{{macro.HcsDpSiteName}}

ステップ 6 **[メンバー（Member）]** パネルを展開してパーティションを追加します。

ステップ 7 **[選択したパーティション（Selected Partitions）]** 列のドロップダウンリストでパーティションを選択します。

（注）
- **[追加（Add）]** アイコンをクリックしてさらにパーティションを追加します。このサービスクラスに目的のメンバーを追加するには、この手順を繰り返します。
- **`Cu<CUSTOMER_ID>CC<CC_SERVER_ID>-Xfer4CCServer-PT`** をサービス クラス パーティション メンバー リストに追加します。

ステップ 8 [保存（Save）] をクリックします。

サービスクラスの編集

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が、お客様の有効なサイトに設定されていることを確認します。

ステップ 3 **[ダイヤルプラン管理（Dial Plan Management）] > [サイト（Site）] > [サービスクラス（Class of Service）]** の順に選択します。

ステップ 4 リストから [サービスクラス（Class of Service）] をクリックして、必要なフィールドを編集および変更します。

ステップ 5 [保存（Save）] をクリックします。

サービスクラスの削除

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が、お客様の有効なサイトに設定されていることを確認します。

ステップ 3 **[ダイヤルプラン管理（Dial Plan Management）] > [サイト（Site）] > [サービスクラス（Class of Service）]** の順に選択します。

ステップ 4 削除するリストで [サービスクラス（Class of Service）] をクリックします。

ステップ 5 [削除（Delete）] をクリックします。

アプリケーションユーザーへの電話の関連付け

始める前に

電話を追加する必要があります。「電話機の追加 （303 ページ）」を参照してください。

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なサイトに設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）] > [エージェント回線（Agent Lines）]** の順に選択します。

ステップ 4 **[追加（Add）]** をクリックして、新しいエージェント回線を追加します。
ステップ 5 **[デバイスタイプ（Device Type）]** ドロップダウンリストで **[電話機（Phones）]** を選択します。
ステップ 6 **[デバイス名（Device Name）]** ドロップダウンリストでデバイスを選択します。
ステップ 7 ドロップダウンリストで **[回線（Line）]** を選択します。
ステップ 8 ドロップダウンリストで **[アプリケーションユーザー（Application User）]** を選択します。
ステップ 9 [保存（Save）] をクリックします。

UCDM から Unified Communication Manager の関連付けを解除

Unified Communication Manager の構成を保持するには、お客様を削除する前に以下の手順を実行します。

手順

ステップ 1 プロバイダまたはリセラーとして UCDM にログインします。
ステップ 2 Cisco Unified Communications Manager の関連付けを解除するお客様を階層から選択します。
ステップ 3 **[デバイス管理（Device Management）]** > **[CUCM]** > **[サーバー（Server）]** の順に選択します。
ステップ 4 関連付けを解除する Cisco Unified Communications Manager をクリックします。
ステップ 5 **[ネットワークアドレス（Network Addresses）]** パネルの **[削除（Remove）]** アイコンをクリックします。
ステップ 6 [保存（Save）] をクリックします。

組み込みブリッジ

電話機の組み込みブリッジ（BIB）はデフォルトでは有効になっていません。デフォルトではすべてのカスタマーによって使用されるわけではないため、システムレベルでは無効になっています。これは、コンタクトセンターを持つカスタマーのみが使用します。

コンタクトセンターを持つカスタマーの BIB を有効にするには、プロバイダは、次の手順を実行する必要があります。

（注） カスタマーレベルで新しいフィールド表示ポリシーを作成し、組み込みブリッジをリストに追加します。

- 組み込みブリッジの構成 （310 ページ）
- 組み込みブリッジの有効化または無効化 （310 ページ）

組み込みブリッジの構成

手順

ステップ 1 プロバイダとして **Cisco Unified Communication Domain Manager** にログインします。

ステップ 2 **[ロール管理（Role Management）]** > **[フィールド表示ポリシー（Field Display Policies）]** の順に選択します。

ステップ 3 階層が適切なお客様に設定されていることを確認します。

ステップ 4 **SubscriberPhoneMenuItemProvider** を選択します。

ステップ 5 詳細ページの **[アクション（Action）]** メニューで、**[クローン（Clone）]** をクリックします。

ステップ 6 名前として **SubscriberPhoneMenuItemProvider** を入力します。

ステップ 7 **[ターゲットモデルタイプ（Target Model Type）]** ドロップダウンログインで、**relation/SubscriberPhone** を選択します。

ステップ 8 **[グループ（Groups）]** セクションを展開し、[タイトル（Title）] に対して **[電話機（Phone）]** を入力します。

ステップ 9 **[利用可能（Available）]** リストで、**builtInBridgeStatus** を選択し、**[選択（Select）]** をクリックします。

ステップ 10 [保存（Save）] をクリックします。

組み込みブリッジの有効化または無効化

始める前に

組み込みブリッジが構成されていることを確認してください。組み込みブリッジの構成 （310 ページ）を参照してください。

手順

ステップ 1 プロバイダとして **Cisco Unified Communication Domain Manager** にログインします。

ステップ 2 階層が適切なお客様に設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[電話機（Phones）]** の順に選択し、適切な電話機を選択します。

ステップ 4 **[電話機（Phone）]** タブで、以下の手順を実行します。

- BIB を有効するには、**[組み込みブリッジ（Built in Bridge）]** ドロップダウンリストで **[オン（On）]** を選択します。
- BIB を無効するには、**[組み込みブリッジ（Built in Bridge）]** ドロップダウンリストで **[オフ（Off）]** を選択します。

ステップ 5 [保存（Save）] をクリックします。

UCDM を使用した一括操作

一括アップロードオプションは、多数のリソース項目を Cisco Unified Communications Domain Manager（UCDM）にインポートするために使用されます。これは、.xlsx形式を使用したリソース属性を入力し、UCMD オブジェクトのリソースを生成するために使用されます。すべての .xlsx ファイルには各値の入力先を示すヘッダーが必要です。これらのヘッダーは、UCDM の適切な一括アップロードページからダウンロードできるテンプレートから提供されます。

一括アップロードをプロビジョニングするには、次の 3 つの方法があります。

1. HCS Intelligent Loader（HIL）
2. Cisco Unified Communications Domain Manager 管理ツール/一括ローダー
3. Cisco Unified Communications Domain Manager REST API

一括アップロードのプロビジョニングの詳細については、『*Cisco Unified Communications Domain Manager*、一括プロビジョニングガイド』を参照してください。このガイドは、http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-6-1/model.html#~tab-solution-documentation にある **Component Documentation** タブにあります。

Cisco Unified Communications Domain Manager Administration ツール/一括ローダー

- 一括ロードのエクスポート （311 ページ）
- 一括ロードシート （312 ページ）
- 一括アップロードの実行 （312 ページ）

一括ロードのエクスポート

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Unified Communication Domain Manager にログインします。

ステップ 2 階層を必要な UCDM オブジェクトに対して適切なレベルに設定します。

ステップ 3 一括ロードに対応している UCDM オブジェクトの必要なフォームに移動します。

ステップ 4 **[アクション（Action）]** をクリックし、サブメニューの**一括ロードのエクスポート**テンプレートをクリックします。

ステップ 5 一括ロードテンプレートを .xlsx 形式でローカルドライブに保存します。

一括ロードシート

エクスポートされた一括ロードテンプレートは、単一のシートを含むワークブックであり、一括ロードの基礎として機能します。タブ付きワークブックとして複数のシートを含むワークブックを作成することもできます。

タブ付きワークブックの場合、一括ロードトランザクションは、一番左端のシートまたはタブから一番右端に実行されます。たとえば、お客様の配下に拠点を追加する場合、お客様シートタブは関連する拠点の左側に配置する必要があります。

スプレッドシートワークブックはMicrosoft Excel.xlsx形式です。ファイルの最大アップロードサイズは4 GBです。ワークブックには任意の名前を入力することも、同じファイル名を入力してファイルを複数回ロードすることもできますが、別の名前を使用することをお勧めします。

データを一括ロードするには、事前の手順を実行する必要があります。シート上の既存の情報を確認し、必要なデータを入力してスプレッドシートを準備するために必要な情報を決定します。

一括アップロードの実行

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとしてUnified Communication Domain Managerにログインします。

ステップ 2 階層を必要なUCDMオブジェクトに対して適切なレベルに設定します。

ステップ 3 **[管理ツール（Administrative Tools）]** > **[一括ロード（Bulk Load）]** の順に選択します。

ステップ 4 **[参照（Browse）]** をクリックし、[ファイルアップロード（File Upload）] ダイアログボックスを開きます。

ステップ 5 **[ファイルを一括ロード（Bulk Load File）]** をクリックします。

（注） 一括ロードのステータスを確認するには、**[管理ツール（Administrative Tools）]** > **[トランザクション（Transactions）]** の順に選択します。

SW MTP および SW 会議リソースの増加

手順

ステップ 1 **Cisco Unified Communications Manager Administration** Webページにログインします。

ステップ 2 **[システム（System）]** タブで、**[サービスパラメータ（Service Parameter）]** を選択します。

ステップ 3 ドロップダウンリストで、Cisco Unified Communications Managerサーバーを選択します。

ステップ 4 **Cisco IP 音声メディア ストリーミング アプリ** サービスを選択します。

ステップ 5 [会議ブリッジ（CFB）パラメータ（Conference Bridge (CFB) parameters）] と [メディアターミネーションポイント（MTP）パラメータ（Media Termination Point (MTP) parameters）] フィールドを以下のように変更します。

- SW CFB：

  デフォルトの総会議参加者数：48（16 CFB 3 パーティセッション）

  最大会議参加者数：256（85 CFB 3 パーティセッション）

- SW MTP：

  デフォルトの総 MTP 参加者数：48（各セッションにつき 2 パーティの 24 MTP セッション）

  最大 MTP パーティ：512（256 MTP セッション）

シングルサインオン管理

シングルサインオン用システムインベントリの設定

Cisco Identity Service（Cisco IdS）およびシングルサインオンのコンポーネントを構成する前に、システムインベントリを設定します。

デフォルトでは、システムインベントリには、展開内のすべての AW、ルータ、および周辺機器ゲートウェイのリストが表示されます。プリンシパル AW を選択して、コンポーネントを Cisco IdS に登録し、SSO を有効にする管理をします。残りの SSO 対応マシンをシステムインベントリに追加し、各 SSO 対応 マシンに対するデフォルト Cisco IdS を選択します。

手順

ステップ 1 Unified CCE Administration で、**[システム（System）]**>**[シングルサインオン（Single Sign-On）]** の順に選択します。

ステップ 2 プリンシパル AW を設定するには、以下の手順を実行します。

a) プリンシパル AW にする AW をクリックします。

（注） AW がルータと共在している場合は、ルータ上にプリンシパル AW を設定できます。

[AWの編集（Edit AW）] ポップアップウィンドウが開きます。

b) [一般（General）] タブの **[プリンシパルAW（Principal AW）]** チェックボックスをオンにします。

c) Unified CCE 診断フレームワーク サービス ドメイン、ユーザー名およびパスワードを入力します。

これらのログイン情報は、インスタンスのConfigセキュリティグループのメンバーであるドメインユーザー用です。ログイン情報は、展開に含まれるすべてのCCEコンポーネントで有効である必要があります（ルーター、PG、AW など）。

d) [保存（Save）] をクリックします。

ステップ 3 SSO 対応マシンをシステムインベントリに追加します。

a) [New] をクリックします。
[マシンの追加（Add Machine）] ポップアップウィンドウが開きます。

b) **[タイプ（Type）]** ドロップダウンリストで、以下のいずれかのマシンのタイプを選択します。

- **Finesse プライマリ**
- **Cisco Unified Intelligence Center、LD、IdS Publisher**：2000 エージェント参照デザインを使用している場合の共存可能展開アプリケーション。
- **Unified Intelligence Center Publisher**：スタンドアロンの Unified Intelligence Center を使用している場合。
- **Identity Service Primary**：スタンドアロンの Cisco IdS を使用している場合。

c) **[ホスト名（Hostname）]** フィールドに、FQDN、IPアドレス、またはマシンのホスト名を入力します。

（注） FQDN を入力しない場合、システムは、入力した値を FQDN に変換します。

d) マシンの管理者用ログイン情報を入力します。

e) [保存（Save）] をクリックします。
マシンとそれに関連する Subscriber またはセカンダリマシンはシステムインベントリに追加されます。

f) 展開内のすべての SSO 対応マシンを追加するには、この手順を繰り返します。

ステップ 4 次の各マシンのデフォルトのアイデンティティサービスを選択します。

- すべての Unified CCE AW サーバー
- Finesse プライマリおよびセカンダリ
- Unified Intelligence Center のパブリッシャとサブスクライバ

（注） 共存可能な Cisco Unified Intelligence Center、LD、Ids Publisher および Subscriber を使用している場合は、これらマシンにデフォルトの Cisco IdS を設定する必要はありません。

スタンドアロン展開では、構成するマシンと同じデータセンター再度（A または B）に展開されている Cisco IdS を選択します。たとえば、参照展開の場合：

- AW-HDS-DDS 1、AW-HDS 3、Finesse 1 Pub、Finesse 2 Pub、Cisco Unified Intelligence Center Pub および Cisco Unified Intelligence Center Sub 1 のアイデンティティサービス Publisher（IdS A）を選択します。
- AW-HDS-DDS 2、AW-HDS 4、Finesse 1 Sub、Finesse 2 Sub、Cisco Unified Intelligence Center Sub 2 および Cisco Unified Intelligence Center Sub 3 のアイデンティティサービス Publisher（Ids B）を選択します。

参照展開にかんしては、「https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html」の「*Cisco Unified Contact Center Enterprise* 設計ガイド」を参照してください。

a) マシンをクリックし、[マシンの編集（Edit Machine）] ポップアップ ウィンドウを表示します。
b) **[デフォルトアイデンティティサービス（Default Identity Service）]** の横にある [検索（Search）]アイコンをクリックして、**[アイデンティティーサービスの選択（Select Identity Service）]** ポップアップウィンドウを開きます。
c) [検索] フィールドで、Cisco IdS のマシン名を入力し、リストから、 Cisco IdS を選択します。
d) [保存（Save）] をクリックします。

Cisco Identity Service の設定

Cisco Identity Service（Cisco IdS）は、ID プロバイダ（IdP）とアプリケーションの間で承認を提供します。

Cisco IdS を設定する場合は、Cisco IdS と IdP の間のメタデータ交換を設定します。この信頼関係により、アプリケーションはシングルサインオンに Cisco IdS を使用することができます。この信頼関係は、Cisco IdS からメタデータ ファイルをダウンロードし、IdP にアップロードすることで構築します。その後、セキュリティに関連する設定の選択、Cisco IdS サービスのクライアントの識別、ログ レベルの設定を行うことができます。必要があれば、Syslog 形式を有効にすることができます。

手順

ステップ 1 Administration で、**[システム（System）]** > **[シングルサインオン（Single Sign-On）]** の順に選択します。

（注） *username@FQDN* 形式のログイン名を使用して、 Administration にログインします。

ステップ 2 **[アイデンティティサービス管理（Identity Service Management）]** をクリックします。

結果：

[Ciscoアイデンティティサービス管理（Cisco Identity Service Management）] ウィンドウが開きます。

ステップ 3 ユーザー名を入力し、**[次へ（Next）]** をクリックします。

ステップ 4 パスワードを入力して、**[サインイン（Sign In）]** をクリックします。

左側のペインに、**[ノード（Nodes）]**、**[設定（Settings）]** および **[クライアント（Clients）]** のアイコンが表示された Cisco アイデンティティ サービス管理ページが開きます。

ステップ 5 **[ノード（Nodes）]** をクリックします。

ノードページが開き、全体的なノードレベルを表示して、どのノードがサービスに所属しているかを特定することができます。またこのページでは、各ノードの **SAML 証明書の有効期限** の詳細を表示して、証明書の有効期限が切れる期日を確認することもできます。ノードの **ステータス** オプションには、**未設定**、**稼働中**、**一部稼働中**、および **不使用**があります。詳細については、[ステータス]をクリックしてください。ノード名の右側にある星印は、プライマリパブリッシャであるノードを示します。

ステップ 6 [設定（Settings）] をクリックします。

ステップ 7 **IdSの信頼性**をクリックします。

ステップ 8 Cisco IdS と IdP 間の Cisco IdS 信頼関係を設定するには、**メタデータ ファイルのダウンロード** をクリックして、Cisco IdS サーバからファイルをダウンロードします。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 信頼メタデータファイルをIdPからアップロードするには、ファイルを検索して特定します。IdPへのパスが含まれる**メタデータのアップロード**ページが開きます。ファイルのアップロードが完了すると、通知メッセージが表示されます。これでメタデータの交換が完了し、信頼関係が確立されます。

ステップ 11 ブラウザのキャッシュをクリアします。

ステップ 12 ページが IdP にリダイレクトされるときに、有効なログイン情報を入力します。

ステップ 13 [次へ（Next）] をクリックします。

SSO 設定のテスト ページが開きます。

ステップ 14 **SSO 設定のテスト**をクリックします。

Cisco IdS の構成が正常に完了したことを通知するメッセージが表示されます。

ステップ 15 [設定（Settings）] をクリックします。

ステップ 16 [セキュリティ（Security）] をクリックします。

ステップ 17 **トークン**をクリックします。

以下の設定の期間を入力します。

- **トークンの有効期限の更新**：デフォルト値は 10 時間です。最小値は 2 時間です。最大値は 24 時間です。

- **承認コードの有効期限**：デフォルト値は 1 分で、これが最小値となります。最大値は 10 分です。
- **アクセス トークンの有効期限**：デフォルト値は 60 分です。最小値は 5 分です。最大値は 120 分です。

ステップ 18 **暗号化トークン**（オプション）：デフォルト設定は **オン**です。

ステップ 19 **[保存（Save）]** をクリックします。

ステップ 20 **キーおよび証明書**をクリックします。
キーおよびSAML 証明書の生成 ページが開き、以下が可能になります。

- **再生成**をクリックして、**暗号化および署名キー**を再生します。トークンの登録が正常に完了したというメッセージが表示され、構成を完了するためにシステムを再起動するように勧められます。
- **再生成**をクリックして、**SAML 証明書** を再生成します。SAML 証明書の再生成が正常に行われたというメッセージが表示されます。

ステップ 21 **[保存（Save）]** をクリックします。

ステップ 22 **[クライアント（Clients）]** をクリックします。
クライアントページでは、クライアント名、クライアント ID、およびリダイレクト URL を含む既存の Cisco IdS クライアントが表示されます。特定のクライアントを検索するには、名前の一覧の上部にある検索アイコンをクリックして、クライアント名を入力します。

ステップ 23 クライアントを追加するには、以下の手順を実行します。

a) **[クライアントの追加（Add Client）]** > の順に選択します。
b) クライアントの名前を入力します。
c) リダイレクト URL を入力します。複数の URL を追加するには、プラスのアイコンをクリックします。
d) **追加** をクリックします（もしくは**クリア** をクリックして、「X」をクリックして、クライアントを追加せずにページを閉じます）。

ステップ 24 クライアントを編集または削除するには、クライアントの行を強調表示して、**アクション**の下の省略記号をクリックします。実行されるアクション

- **編集** をクリックして、クライアントの名前、ID、またはリダイレクト URL を編集します。**クライアント編集** ページで、変更を行い、**保存** をクリックします（もしくは **クリア** をクリックして、変更を保存せずにページを閉じます）。
- **削除** をクリックしてクライアントを削除します。

ステップ 25 [設定（Settings）] をクリックします。

ステップ 26 **設定**ページで、**[トラブルシューティング（Troubleshooting）]**をクリックし、オプションのトラブルシューティングを実行します。

ステップ 27 **[エラー（Error）]**、**[警告（Warning）]**、**[情報（Info）]**（デフォルト）**[デバッグ（Debug）]** または **[トレース（Trace）]** のいずれかをローカルログレベルに設定します。

ステップ 28 Syslog形式のエラーを受信するには、リモートSyslogサーバ名をホスト（オプション）フィールドに入力します。

ステップ 29 **[保存（Save）]** をクリックします。

次の作業に進んでください。

- Cisco IdS を使用してコンポーネントを登録します。
- 展開全体の SSO を有効（または無効）にします。

コンポーネントを登録して、シングルサインオン モードを設定します。

コンポーネントを Cisco IdS に登録してからシステムインベントリに SSO 対応マシンを追加すると、それらのマシンは自動的に登録されます。

始める前に

- Cisco Identity Service（Cisco IdS）の構成
- ポップアップ ブロッカを無効にします。すべてのテスト結果を正しく表示できます。
- Internet Explorer を使用している場合は、次のことを確認します。
  - 互換モードではない。
  - AW の完全修飾ドメイン名を使用して CCE Administration にアクセスしている（例：**https://<FQDN>/cceadmin**）。

手順

ステップ 1 Unified CCE Administration で、**[システム（System）]** > **[シングルサインオン（Single Sign-On）]** の順に選択します。

ステップ 2 Unified CCE 管理のシングルサインオン ツールで、**登録** ボタンをクリックして、すべての SSO 互換コンポーネントを Cisco IdS に登録します。

コンポーネント ステータステーブルに、各コンポーネントの登録ステータスが表示されます。

コンポーネントの登録に失敗した場合は、エラーを修正して、**再試行**をクリックします。

ステップ 3 [テスト（Test）] ボタンをクリックします。新しいブラウザ タブが開くと、証明書を承認するためのプロンプトが表示されることがあります。ページをロードするためには、すべての証明書を承認します。次に、[ログイン] ダイアログボックスが表示されたら、SSO ログイン情報を持つユーザとしてログインします。

テスト プロセスでは、各コンポーネントが正しく設定されていて ID プロバイダーにアクセスできること、および Cisco IdS によってアクセス トークンが正常に生成されることが確認されます。SSO に設定している各コンポーネントがテストされます。

コンポーネントのステータステーブルには、各コンポーネントのテストのステータスが表示されます。

テストが失敗した場合は、エラーを修正して、再度 **テスト** をクリックします。

テスト結果は保存されません。ページを更新する場合は、SSO を有効にする前にテストを再度実行します。

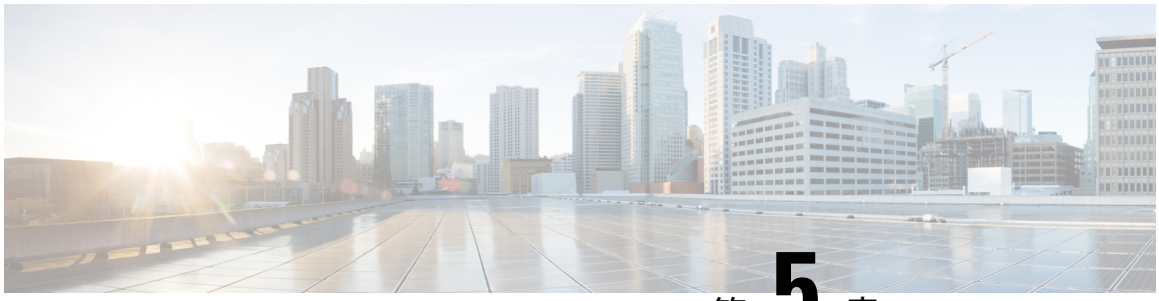
ステップ 4 [モードの設定（Set Mode）] ドロップダウン メニューから、システムに設定する SSO モードを選択します。

- [非 SSO（Non-SSO）]：このモードでは、すべてのエージェントとスーパーバイザの SSO が無効になります。ユーザーは、既存の Active Directory ベースの認証およびローカル認証を使用し、ログインします。
- [ハイブリッド（Hybrid）]：このモードでは、エージェントとスーパーバイザの SSO を選択的に有効にできます。
- SSO：このモードはすべてのエージェントおよびスーパーバイザで SSO を有効にします。

コンポーネントのステータス テーブルには、各コンポーネントで設定されている SSO モードのステータスが表示されます。

コンポーネントの SSO モードの設定に失敗した場合は、エラーを修正して、再度モードを選択します。

コンポーネントを登録して、シングルサインオン モードを設定します。



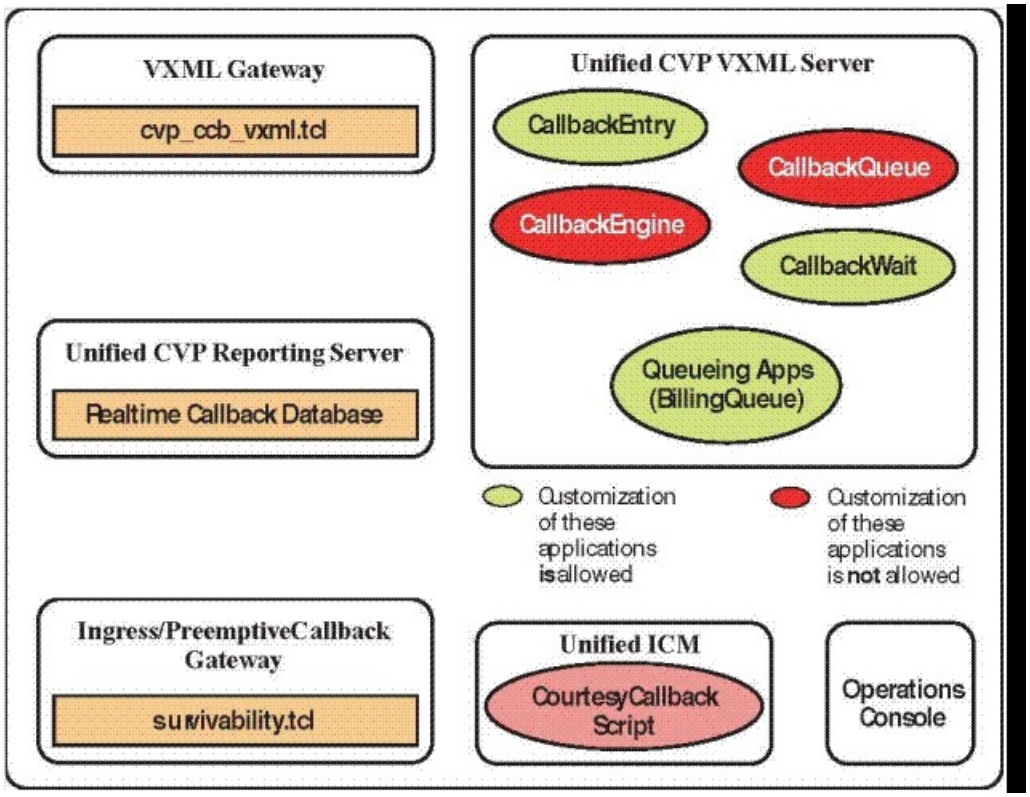
第 5 章

コアコンポーネントの統合オプションの構成

Courtesy Callback の設定

次の図に、サービス コールバック用に構成する必要があるコンポーネントを示します。

図 *9:* サービス コールバック コンポーネント



サービス コールバックを構成するには、以下の手順を実行します。

- ゲートウェイの構成 （322 ページ）
- Unified CVP の構成 （326 ページ）
- 設定 Unified CCE （330 ページ）

ゲートウェイの構成

サービス コールバック用 VXML ゲートウェイの構成

サービス コールバック用 VXML ゲートウェイを構成するには、以下の手順を実行します。

手順

ステップ 1 以下のように CVP オペレーションコンソールからゲートウェイのフラッシュメモリーに **cvp_ccb_vxml.tcl** をコピーします。

a) **[一括管理（Bulk Administration）] > [ファイル転送（File Transfer）] > [スクリプトとメディア（Scripts and Media）]** を選択します。

b) [デバイスの関連付け（Device Association）] で、デバイスタイプとして **[ゲートウェイ（Gateway）]** を選択します。
c) [使用可能（Available）] リストから必要なゲートウェイを選択します。
d) 右矢印アイコンをクリックして、使用可能なゲートウェイを [選択済み（Selected）] リストに移動します。
e) デフォルトゲートウェイファイルで、**cvp_ccb_vxml.tcl** を強調表示します。
f) [転送（Transfer）] をクリックします。

ステップ 2 VXML ゲートウェイにログインします。

ステップ 3 cvp_cc service を **service cvp_cc flash:cvp_ccb_vxml.tcl** の構成に追加します。

このサービスにはパラメータは必要ありません。

ステップ 4 以下のコマンドを入力して、アプリケーションをロードします。

call application voice load cvp_cc

ステップ 5 Unified CCE からの VRU を定義する VoIP ダイヤルピアで、コーデックが録音に使用できることを確認します。

例：

次の例では、g711ulaw がサービス コールバックでの録音に使用できることを確認します。

```
dial-peer voice 123 voip
 service bootstrap
 incoming called-number 123T
 dtmf-relay rte-nte
 h245-signal
 h245-alphanumeric
 codec g711ulaw
 no vad!
```

ステップ 6 SIP INFO メッセージングを転送するように SIP が設定されていることを確認するには、次を構成します。

```
voice service voip
 signaling forward unconditional
```

ステップ 7 ビープ音を再生して、発信者に BillingQueue サンプルに 名前を録音するように促すには、構成に以下のテキストを追加します。

vxml version 2.0

（注） ゲートウェイで vxml version 2.0 を有効化すると、vxml audioerror はデフォルトで、**オフ**になります。オーディオファイルを再生できない場合、error.badfetch はオーディオエラーイベントを生成**しません**。

ゲートウェイでエラーを生成するには、vxmlaudioerror を有効にします。

例：

次の例では、config terminal モードを使用して両方のコマンドを追加します。

```
config t
vxml version 2.0
```

```
vxml audioerror
exit
```

サービス コールバック用イングレスゲートウェイの構成

サービス コールバックのイングレスゲートウェイを構成するには、以下の手順を実行します。

手順

ステップ 1 以下のように surviability.tcl をオペレーションコンソールからゲートウェイのフラッシュメモリーにコピーします。

a) **[一括管理（Bulk Administration）] > [ファイル転送（File Transfer）] > [スクリプトとメディア（Scripts and Media）]** の順に選択します。
b) [デバイスの関連付け（Device Association）] で、デバイスタイプとして **[ゲートウェイ（Gateway）]** を選択します。
c) [使用可能（Available）] リストから必要なゲートウェイを選択します。
d) 右矢印アイコンをクリックして、使用可能なゲートウェイを [選択済み（Selected）] リストに移動します。
e) デフォルト ゲートウェイ ファイルで、**survivability.tcl** を強調表示します。
f) [転送（Transfer）] をクリックします。

ステップ 2 イングレスゲートウェイにログインします。

ステップ 3 存続可能性サービスに以下を追加します。

```
param ccb id:<host name or ip of this gateway>;loc:<location name>;trunks:<number of
callback trunks>
```

- **id ―** このゲートウェイの一意の識別子で、元のコールバック要求を処理したゲートウェイを示すためにデータベースに記録されます。
- **loc ―** このゲートウェイのロケーションを指定する任意のロケーション名。
- **Trunks ―** このゲートウェイでコールバック用に予約されている DS0 数。T1/E1トランク数を制限して、システムがコールバックに許可されるリソースを制限できるようにします。

例：

以下の例では、基本設定が示されています。

```
service cvp-survivability flash:survivability.tcl
param ccb id:10.86.132.177;loc:doclab;trunks:1!
```

ステップ 4 着信 POTS ダイヤルピアを作成するか、着信 POTS ダイヤルピアで存続可能性サービスが使用されていることを確認します。

例：

次の例を参考にしてください。

```
dial-peer voice 978555 pots
service cvp-survivability
incoming called-number 9785551234
direct-inward-dial!
```

ステップ 5 コールバック用の発信 POTS ダイヤルピアを作成します。これらは、実際のコールを PSTN に戻すダイヤルピアです。

例：

次の例を参考にしてください。

```
dial-peer voice 978555 pots
destination-pattern 978555....
no digit-strip port 0/0/1:23!
```

ステップ 6 SIP INFO メッセージングを転送するように SIP が設定されていることを確認するには、次の構成を使用します。

voice service voip signaling forward unconditional

サービス コールバック用 CUBE-E の構成

（注） CUBE-E を使用している場合は、SIP プロファイル構成が必要であり、cvp を介してアウトバウンドダイヤルピアに適用します。以下の例を参照してください。

「sip-profile」構成は、ISR CUBE E でサービス コールバック機能に対して必要です。
「sip-profile」を構成するには、以下を追加する必要があります。

```
voice class sip-profiles 103

request INVITE sip-header Call-Info add "X-Cisco-CCBProbe: <ccb param>"
```

「<ccb param>」は、サバイバビリティサービスに定義される「CCB」パラメータです。この「sip-profile」を CVP へのアウトバウンドダイヤルピアに追加します。

次に、構成例を示します。

```
voice class sip-profiles 103

request INVITE sip-header Call-Info add "X-Cisco-CCBProbe: id:10.10.10.180;sydlab;trunks:4"

dial-peer voice 5001 voip

description Comprehensive outbound route to CVP

destination-pattern 5001

session protocol sipv2

session target ipv4:10.10.10.10

dtmf-relay rtp-nte

voice-class sip profiles 103
```

```
codec g711ulaw

no vad
```

上記の例では、**10.10.10.180** がCUBE IP で、**10.10.10.10** が CVP コールサーバー IP です。

（注） CUBE E がサービスコールバックに使用される場合、CUBE E の音声サービス voip クラスには、サービスコールバックが動作するためのメディアフロースルーが必要です。

Unified CVP の構成

サービス コールバック用レポーティングサーバーの構成

レポーティングサーバーは、サービス コールバック機能に対して必要です。サービス コールバックに対してレポーティングサーバーを構成するには、以下の手順を実行します。

始める前に

レポーティングサーバーをインストールして構成します。

手順

ステップ 1 オペレーションコンソールで、**[システム（System）] > [サービス コールバック（Courtesy Callback）]** の順に選択します。

サービス コールバック構成ページが表示されます。

ステップ 2 [General] タブを選択します。

ステップ 3 **[Unified CVP レポーティングサーバー（Unified CVP Reporting Server）]** ドロップダウンリストで、レポーティングサーバーをセンタ記して、サービス コールバックデータを保存します。

ステップ 4 必要に応じて、**[サービス コールバック データベースへのセキュア通信を有効化（Enable secure communication with the Courtesy Callback database）]** を選択します。

ステップ 5 許可および無効なダイヤル番号を構成します。

これらは、システムが発信者にサービス コールバックを発信するときに発信する必要がある番号です。

（注） 最初は、サービス コールバック機能に許可されるダイヤル番号はありません。[不一致のダイヤル番号を許可（Allow Unmatched Dialed Numbers）] の選択が解除され、[許可されたダイヤル番号（Allowed Dialed Numbers）] ウィンドウが空になります。

ステップ 6 [発信者番号ごとの最大通話数（Maximum Number of Calls per Calling Number）] を目的の番号に調整します。

デフォルトでは0に設定されており、制限はありません。この設定により、同じ発信番号からコールバックを受ける通話数を制限することができます。

このフィールドが正の数（X）に設定されている場合、Courtesy Callback Validate 要素では、発信番号ごとに X のコールバックのみがpreemptive exit 状態を通過できます。

発信番号に対してすでに X コールバックがある場合、新しい通話はValidate 要素の none exit 状態を通過できます。

また、通話に使用可能な発信番号がない場合、通話は常に Validate 要素の none exit 状態を通過します。

ステップ 7 **[コールサーバー展開（Call Server Deployment）]** タブを選択し、サービス コールバックに使用するコールサーバーを [利用可能（Available）] ボックスから [選択済み（Selected）] ボックスに移動します。

ステップ 8 [保存（Save）] をクリックします。

構成は、次回レポーティングサーバーが再起動したときにアクティブになります（展開されます）。

ステップ 9 **[保存して展開（Save & Deploy）]** をクリックすると、新しいレポーティングサーバー構成をすぐに展開できます。

（注） すべての更新を構成したら、レポーティングサーバーを再起動して構成を更新します。

サービス コールバック用 Call Studio スクリプトの構成

サービス コールバック機能は、Call Studio スクリプトと ICM スクリプトの組み合わせにより制御されます。Call Studio スクリプトを構成するには、以下の手順を実行します。

手順

ステップ 1 `C:\Cisco\CVP\OPSConsoleServer\StudioDownloads\CourtesyCallbackStudioScripts.zip` の CVP OAMP マシンから .zip ファイルにアクセスします。

ステップ 2 CourtesyCallbackStudioScripts.zip に含まれる Call Studio Courtesy Callback スクリプトサンプルを、CallStudio が実行されているコンピュータにあるフォルダに解凍します。

各フォルダには、フォルダを同名の Call Studio プロジェクトが含まれています。5 つの個別プロジェクトは、サービス コールバック機能から構成されています。

（注） CallbackEngine および CallbackQueue スクリプトは、変更しないでください。

ステップ 3 ビジネスニーズに合わせて、**BillingQueue, CallbackEntry** および **CallbackWait** スクリプトを変更します。

ステップ 4 **[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [Cisco Unified Call Studio]** の順に選択して、Call Studioを起動します。

ステップ 5 **[ファイル（File）] > [インポート（Import）]** の順に選択します。

[インポート（Import）] ダイアログボックスが表示されます。

ステップ 6 **Call Studio** フォルダを展開し、ワークスペースの **[既存Call Studio（Existing Call Studio）]** プロジェクトを選択します。

ステップ 7 **[次へ（Next）]** をクリックします。

[ファイルシステムからCall Studioプロジェクトをインポート（Import Call Studio Project From File System）] が表示されます。

ステップ 8 Call Studio プロジェクトを抽出した場所を参照します。解凍された各フォルダで、フォルダ（BillingQueueなど）を選択し、**[完了（Finish）]** を選択します。

プロジェクトが Call Studio にインポートされます。

ステップ 9 5 つのフォルダのそれぞれに対して、前の手順のアクションを繰り返します。

[ナビゲータ（Navigator）] Windowsの左上に 5 つのプロジェクトが表示されます。

ステップ 10 Call Studio の [デフォルトオーディオパスURI（Default Audio Path URI）] フィールドを更新して、メディアサーバの IP アドレスとポート値を含めます。

ステップ 11 以前に解凍した Call Studio プロジェクトごとに、以下の手順を実行します。

a) Call Studio の [ナビゲータ（Navigator）] ウィンドウでプロジェクトを選択します。
b) **[プロジェクト（Project）] > [プロパティ（Properties）] > [Call Studio] > [オーディオ設定（Audio Settings）]** の順に選択します。
c) [オーディオ設定（Audio Settings）] ウィンドウで、[オーディオパスURI（Audio Path URI）] フィールドを http://<media-server >/en-us/VL/ に変更します。
d) **[適用（Apply）] > [OK]** の順に選択します。

ステップ 12 **[BillingQueueプロジェクト（BillingQueue Project）]**で、必要に応じて保留中に発信者に再生する音楽を変更します。

a) プロジェクトのツリー構造を展開し、**app.callflow** をクリックします。
b) **Audio_01** ノードをクリックします。
c) **[要素構成（Element Configuration）] > [オーディオ（Audio）] > [オーディオグループ（Audio Groups）]** の順に選択し、ツリー構造を展開したら、**audio item 1** をクリックします、**[デフォルトオーディオパス（Default Audio Path）]** を使用して再生する .wav ファイルを変更します。

ステップ 13 CallbackEntry プロジェクトで、必要に応じて、 **SetQueueDefault_01** ノードの発信者インタラクション設定を変更します。

a) Call Studio の [ナビゲータ（Navigator）] パネルで、**CallBackEntry** プロジェクトを開き、**app.callflow** をダブルクリックして、[スクリプト（Script）] ウィンドウにアプリケーション要素を表示します。
b) [スクリプト表示（Script Display）] ウィンドウの下部にあるタブを使用して、スクリプトのコールの開始ページを開きます。
c) **SetQueueDefault_01** ノードを選択します。

d) [要素構成（Element Configuration）] パネルで、**[設定（Setting）]** タブを選択し、必要に応じてデフォルト設定を変更します。

ステップ 14 CallbackEntry プロジェクトのコールバックをするページで、次の項目を構成します。

a) [レコード名（Record Name）] ノードを強調表示し、**[設定（Settings）]** タブを選択します。
b) [パス（Path）] 設定で、発信者の録音名を保存する場所へのパスを変更します。
c) **Add Callback to DB 1** ノードを強調表示します。
d) 前の手順で作成した録音フォルダの場所と一致するように、録音名ファイルの設定を変更します。
e) **キープアライブ間隔**（秒単位）が、再生されるキューの音楽の長さよりも長いことを確認します。**通話の開始**ページでのデフォルトは以下のとおりです。

SetQueueDefaults_01 ノード のデフォルト値は 120 秒です。

f) CallbackEntry プロジェクトを保存します。
g) CallbackWait プロジェクトで、CallbackWait アプリケーションの値を変更します。

このアプリケーションでは、実際のコールバック時に発信者が受信する IVR インタラクションを変更できます。CallbackWait > AskIfCallerReady ページの発信者インタラクション要素は変更される場合があります。変更後、プロジェクトを保存します。

h) サービス コールバック機能に関連付けられている 5 つのプロジェクトのを検証し、VXML サーバーに展開します。

ステップ 15 **[ナビゲータ（Navigator）]** ウィンドウで各サービス コールバック プロジェクトを右クリックし、**[検証（Validate）]** を選択します。

ステップ 16 プロジェクトの 1 つを右クリックし、**[展開（Deploy）]** をクリックします。

ステップ 17 各プロジェクトのチェックボックスをオンにして、必要なプロジェクトを選択します。

ステップ 18 [展開先（Deploy Destination）] 領域で、**[アーカイブファイル（Archive File）]** を選択し、**[参照（Browse）]** をクリックします。

ステップ 19 設定したアーカイブフォルダに移動します。

例：

C:\Users\Administrator\Desktop\Sample。

ステップ 20 ファイルの名前を入力します。

例：

たとえば、Samplefile.zip です。

ステップ 21 [保存（Save）] をクリックします。

ステップ 22 [展開先（Deploy Destination）] 領域で、**[完了（Finish）]** をクリックします。

ステップ 23 OAMP にログインし、**[一括管理（Bulk Administration）] > [ファイル転送（File Transfer）] > [VXMLアプリケーション（VXMLApplications）]** の順に選択します。

ステップ 24 アプリケーションを展開する VXML サーバーを選択します。

ステップ 25 アプリケーションを含む zip ファイルを選択します。

例：

Samplefile.zip。

ステップ 26 [転送（Transfer）] をクリックします。

ステップ 27 各プロジェクトを右クリックし、**[展開（Deploy）]** をクリックして、**[完了（Finish）]** をクリックします。

ステップ 28 Windows Explorer を使用して、`%CVP_HOME%\VXMLServer\applications` に移動します。

ステップ 29 5 つのサービス コールバック アプリケーションで、%CVP_Home%\VXMLServer\applications にあるプロジェクトの管理者フォルダを開き、**deployApp.bat** をダブルクリックして、 VXML サーバーにアプリケーションを展開します。

ステップ 30 `%CVP_HOME%\VXMLServer\admin` に移動し、すべてのアプリケーションが実行されているか確認したら、**status.bat** をダブルクリックします。5 つすべてののアプリケーションが、[アプリケーション名（Application Name）] 配下で、ステータスが [実行中（Running）] として表示されます。

サービス コールバック用メディアサーバーの構成

サービス コールバックのサンプルスクリプトには、サービス コールバック固有のメディアファイルがいくつか含まれています。サービス コールバック用にメディアサーバを構成するには、以下の手順を実行します。

手順

ステップ 1 Unified CVPのインストール中、メディアファイルは `%CVP_HOME%\OPSConsoleServer\CCBDownloads\CCBAudioFiles.zip` としてコピーされます。

ステップ 2 特殊なオーディオファイルを解凍し、メディアサーバー `VXMLServer\Tomcat\webapps\CVP\audio` にコピーします。

サンプルスクリプトは、オーディオファイルのデフォルトロケーションである「\CVP\audio」を使用するように設定されています。

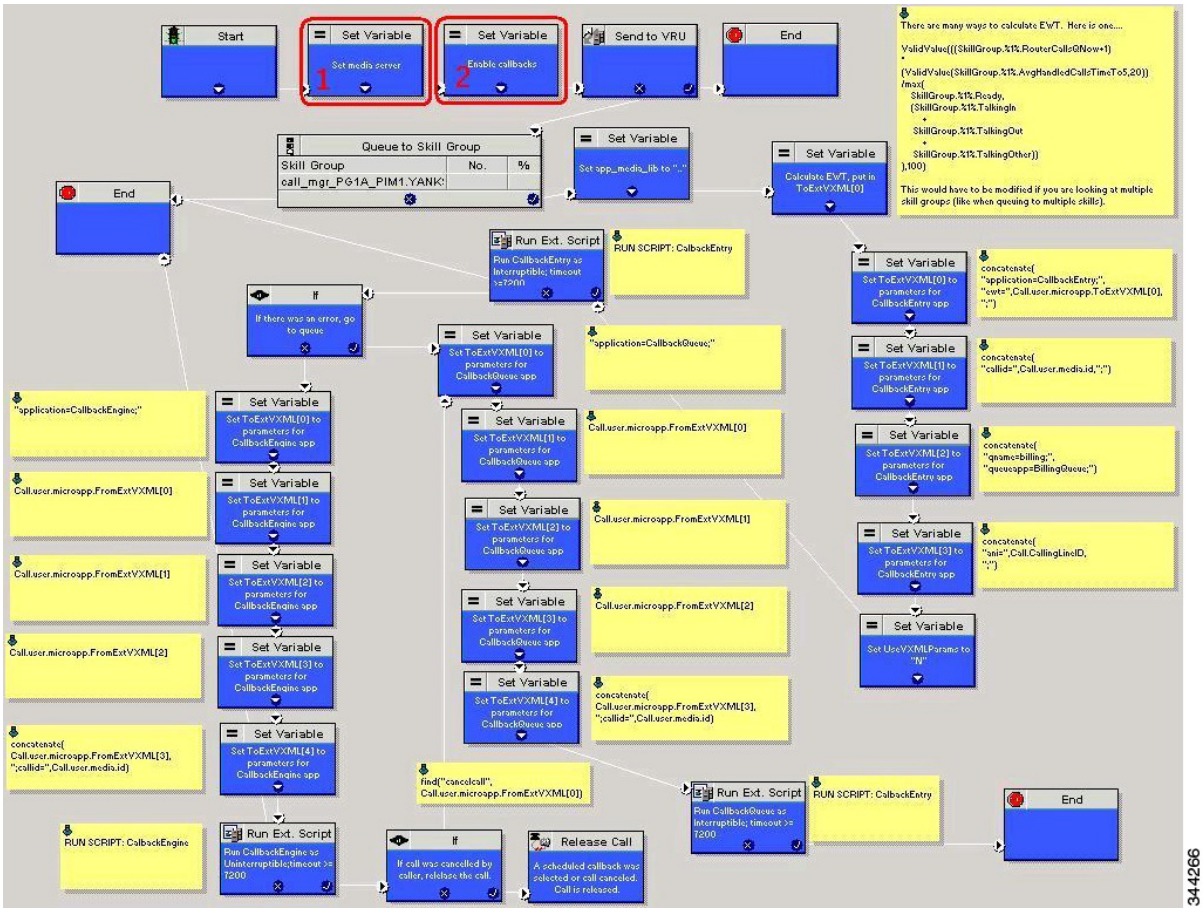
ステップ 3 サンプルスクリプトのオーディオファイルのデフォルトロケーションをメディアサーバーパスに変更します。

設定 Unified CCE

サービス コールバック用 ICM スクリプトの構成

以下の図は、サンプルのサービス コールバック ICM スクリプトを示しています。

図 *10* : サービス コールバック *ICM* スクリプトのサンプル



ICM を構成して、サンプル サービス コールバック ICM スクリプトを使用するには、以下の手順を実行します。

手順

ステップ 1 CCE サンプルスクリプトと **CourtesyCallback.ICMS** を CCE Admin Workstation にコピーします。
CCE スクリプトの例は、以下の場所にあります。

- \CVP\Downloads and Samples\ の CVP インストールメディア。
- **%CVP_HOME%\OPSConsoleServer\ICMDownloads** のオペレーションコンソールから。
- [インポートスクリプトー手動オブジェクトマッピング（Import Script - Manual Object Mapping）] ウィンドウで、ルーティングとスキルグループをサービスコールバックに使用可能なルートとスキルグループにマッピングします。

（注） Small Contact Center 導入モデルの場合は、Internet Script Editor がインストールされているデスクトップに CourtesyCallback.ICMS ルーティングスクリプトをコピーします。

ステップ 2 Script Editor で、**[ファイル（File）] > [スクリプトのインポート...（Import Script...）]** の順に選択します。

（注） Small Contact Center 導入モデルの場合は、以下の手順を実行します。

1. サブカスタマーユーザーで ISE にログインし、[ファイル（File）]>[スクリプトのインポート（Import Script）] の順に選択します。
2. デスクトップ **CourtesyCallback.ICMS** にコピーされたルーティングスクリプトを選択します。

ステップ 3 [スクリプトの場所（Script Location）] ダイアログボックスで、**CourtesyCallback.ICMS** を選択し、**[開く（Open）]** をクリックします。VXML サーバー、コールサーバー、およびメディアサーバーが同じ場所に配置されているため、図 10 : サービス コールバック ICM スクリプトのサンプル （331 ページ） で番号 1 ノードとして強調表示されている**設定変数「Set media server」**をバイパスできます。

ステップ 4 サービス コールバックに対して新しい ECC 変数を定義します。

新しい ECC 変数は、発信者がキューに入り、コールバックを提供できるかどうかを判断するために使用されます。

ステップ 5 **[ICM Admin Workstation] > [ICM構成マネージャ（ICM Configuration Manager）] > [拡張コール変数リストツール（Expanded Call Variable List tool）]** の順に選択し、サービス コールバック専用の ECC 変数である **user.CourtesyCallbackEnabled** を作成します。

ステップ 6 CallbackEntry（VXML アプリケーション）に渡される以下のパラメータを設定します。

例：

- ToExtVXML[0] =concatenate("application=CallbackEntry",";ewt=",Call.user.microapp.ToExtVXML[0])
- ToExtVXML[1] = "qname=billing";
- ToExtVXML[2] = "queueapp=BillingQueue;"
- ToExtVXML[3] = concatenate("ani=",Call.CallingLineID,";");

CallbackEntry は、実行される VXML サーバーアプリケーションの名前です。

ewt は **Block #2** で計算されます。

qname は、コールが配置される VXML サーバーキューの名前です。一意のリソースプールキューごとに一意の qname が必要です。

queueapp は、このキューに対して実行される VXML サーバー キューイング アプリケーションの名前です。

ani は、発信者の発信側回線 ID です。

ステップ 7 ネットワーク VRU スクリプトを作成します。

ステップ 8 **[ICM構成マネージャ（ICM Configuration Manager）] > [ネットワークCRUスクリプトリストツール（Network VRU Script List tool）]** の順に選択し、以下の割り込み可能スクリプトネットワーク VRU スクリプトを作成します。

名前：**VXML_Server_Interruptible**

ネットワーク VRU：Type 10 CVP VRU を選択します。

VRU スクリプト名：**GS、サーバー、V、割り込み可**

タイムアウト：**9000 秒**

割り込み可能：**オン**

ステップ 9 **[ICM構成マネージャ（ICM Configuration Manager）] > [ネットワークCRUスクリプトリストツール（Network VRU Script List tool）]** の順に選択し、以下の割り込み不可スクリプトネットワーク VRU スクリプトを作成します。

名前：**VXML_Server_NonInterruptible**

ネットワーク VRU：Type 10 CVP VRU を選択します。

VRU スクリプト名：**GS、サーバー、V、割り込み不可**

タイムアウト：**9000 秒（Unified CVP の最大コールライフよりも長くする必要があります）**

割り込み可能：**オフ**

ステップ 10 user.microapp.ToExtVXMLECC 変数が最小サイズ 60 文字の 5 つの項目の配列に設定され、user.microapp.FromExtVXML 変数が最小サイズ 60 文字の 4 つの配列に設定されていることを確認します。

（注）

サンプルスクリプトのルートとスキルグループにマッピングするために、少なくとも 1 つの使用可能なルートとスキルグループがあることを確認します。

ステップ 11 スクリプトを保存し、コールタイプを関連付けてスクリプトをスケジュールします。

（注） Small Contact Center 導入モデルの場合、ネットワーク VRU スクリプト、ECC 編集などのルーティングスクリプトで使用されるリソースがサブカスタマーに対して一意であることを確認してください。

エージェントグリーティングの構成

エージェントグリーティングを使用するには、電話機が次の要件を満たしている必要があります。

- 電話機に BiB 機能があること。
- 電話機が、Unified CM 8.5(1) 以降で提供されるファームウェアバージョンを使用すること。

  （ほとんどの場合、Unified CM インストールのアップグレードの際に、電話機のファームウェアも自動でアップグレードされます。）

エージェントグリーティングを構成するには、以下の手順を実行します。

ゲートウェイの構成

tcl スクリプトを VXML ゲートウェイに再発行

Unified CVP と共に出荷される .tcl スクリプトファイルには、エージェントグリーティングをサポートするための更新が含まれていますこれらの更新されたファイルを VXML ゲートウェイに再パブリッシュする必要があります。

VXML ゲートウェイへのスクリプトの再公開は、CVP 更新において標準のタスクです。エージェントグリーティングを使用する前に、スクリプトを再公開する必要があります。

手順

ステップ 1 Unified CVP オペレーションコンソールで **[一括管理（Bulk Administration）]** > **[ファイル転送（File Transfer）]** > **[スクリプトおよびメディア（Scripts and Media）]** の順に選択します。
ステップ 2 [デバイス（Device）] を [ゲートウェイ（Gateway）] に設定します。
ステップ 3 更新するゲートウェイを選択します。通常は、特定の理由がない限り、すべてを選択します。
ステップ 4 **[デフォルトゲートウェイファイル（Default Gateway files）]** を選択します。
ステップ 5 [転送（Transfer）] をクリックします。

VXML ゲートウェイのキャッシュサイズの設定

十分なパフォーマンスを保証するには、VXML ゲートウェイで最大に許容されるキャッシュのサイズを設定します。最大サイズは 100 メガバイトです。デフォルトは 15 キロバイトです。VXML ゲートウェイで最大に許容されるキャッシュのサイズの設定に失敗すると、メディアサーバへのトラフィックの増加に対するパフォーマンスが遅くなる可能性があります。

VXML ゲートウェイで次の Cisco IOS コマンドを使用して、キャッシュサイズをリセットします。

```
conf t
http client cache memory pool 100000
exit
wr
```

キャッシュサイズの構成詳細については、「https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html」の「*Configuration Guide for Cisco Unified Customer Voice Portal*」を参照してください。

Unified CVP の構成

Unified CVP を構成するには、以下の手順を実行します。

- サーバーマネージャで FTP を有効化 （335 ページ）
- Unified CVP メディアサーバーの構成 （74 ページ）
- 録音エージェントグリーティング用 Call Studio スクリプトの構成 （337 ページ）

サーバーマネージャで FTP を有効化

サーバマネージャで FTP を構成するには、以下の手順を実行します。

手順

ステップ 1 サーバーマネージャの左側のナビゲーションペインで、**[ロール（Roles）]** を右クリックします。

ステップ 2 **[ロールの追加（Add Role）]** をクリックします。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 **[Webサーバー（IIS）（Web Server (IIS)）]** チェックボックスをオンにし、**[次へ（Next）]** をクリックします。

ステップ 5 **[FTPサーバー（FTP Server）] チェックボックスをオンにし、[次へ（Next）]** をクリックします。

ステップ 6 インストールが正常に完了したら、**[閉じる（Close）]** をクリックします。

ステップ 7 FTP と IIS が同じルートディレクトリを共有していることを確認します。これは、録音アプリケーションがファイルをメディアサーバーのディレクトリ構造に書き込み、グリーティング再生コールが IIS を使用してファイルを取得するためです。en-us/app ディレクトリは、FTP と IIS の同じルートディレクトリ配下にある必要があります。

ステップ 8 グリーティングファイルを保存する専用のディレクトリをサーバーに作成します。

これにより、エージェント グリーティング ファイルのキャッシュタイムアウトを 5 分に設定できます。これは、他のディレクトリから提供される他の静的ファイルには影響しません。デフォルトでは、Record Greeting アプリケーションは、web/ftp ルートディレクトリは以下の en-us/app ディレクトリに .wav ファイルをポストします。en-us/app ディレクトリの下に ag_gr などの専用ディレクトリを作成し、録音アプリケーションを呼び出す Unified CCE スクリプトでこれを指定できます。ECC 変数である **call.user.microapp.ToExtVXML** のアレイを使用して、ftpPath パラメータを録音アプリケーションに送信します。ECC 変数の長さが十分に長いことを確認してください。そうしないと、切り捨てられて失敗する場合があります。

ステップ 9 IIS Manager で、専用ディレクトリのキャッシュ有効期限をVXML ゲートウェイからメディアサーバーへのデータ要求を最小限に抑えながら、再録音されたグリーティングを適切な時間内に前のメッセージに置き換えることができる値に設定します。

理想的な値は、サポートするエージェント数と、グリーティングを再録音する頻度によって異なります。2 分が妥当な開始点です。

ステップ 10 使用しているサイトを検索し、作成したエージェントグリーティングフォルダ（ag_gr）に移動して、[HTTP Response Headers]を選択します。

ステップ 11 **[追加（Add）]** > **[共通ヘッダーの設定（Set Common Headers）]** の順に選択します。

録音グリーティング用音声プロンプトの作成

エージェントがグリーティングの録音時に聞く各ボイスプロンプトのオーディオファイルを作成します。必要なプロンプトの数はさまざまですが、一般的なセットは次のとおりです。

- ウェルカムの後に、使用するグリーティングを選択するプロンプトが表示されます（これは、エージェントごとに複数のグリーティングをサポートしていることを前提としています）。
- 現在のバージョンを聞くか、新しいバージョンを録音するか、メインメニューに戻るかを選択するプロンプト
- 現在のグリーティングが見つからない場合に再生するプロンプト。

録音グリーティング用の音声プロンプトを作成するには、以下の手順を実行します。

手順

ステップ 1 選択した録音ツールを使用してファイルを作成します。ファイルを録音する場合：

- メディアファイルの形式は、`.wav`にする必要があります。`.wav`ファイルは、Unified CVP エンコーディングおよび形式の要件（G.711、CCITT A-Law 8 kHz、8 ビット、モノラル）と一致する必要があります。
- オーディオファイルをテストします。クリップされていないこと、および音量とトーンが一貫していることを確認します。

ステップ 2 録音後、ファイルを Unified CVP メディアサーバーに展開します。デフォルトの展開場所は、*<web_server_root>*\en-us\app ディレクトリです。

ステップ 3 ファイルの名前と、メディアサーバーでファイルを展開した場所をメモします。スクリプト作成者は、エージェント グリーティング スクリプトにこの情報を必要とします。

組み込み録音プロンプト

エージェントグリーティングの録音に使用する Unified CVP Get Speech micro-application には、以下の組み込みプロンプトが含まれます。

- エージェントが録音した内容を再生するために使用できるプロンプト

- グリーティングの保存、再録音、またはメインメニューに戻るためのプロンプト
- 保存を確認するプロンプト。切断するか、メインメニューに戻るかを選択できます。

これらの .wav ファイルを独自のファイルに置き換えることができます。詳細については、「https://www.cisco.com/c/en/us/support/unified-communications/unified-call-studio/tsd-products-support-series-home.html」の「Unified Customer Voice Portal Call Studio」の書類を参照してください。

録音エージェントグリーティング用 Call Studio スクリプトの構成

録音エージェントグリーティングは、Call Studio スクリプトと ICM スクリプトの組み合わせによって制御されます。Call Studio スクリプトを構成するには、以下の手順を実行します。

手順

ステップ 1 `C:\Cisco\CVP\OPSConsoleServer\StudioDownloads\RecordAgentGreeting.zip` の CVP OAMP マシンから.zip ファイルにアクセスします。

ステップ 2 RecordAgentGreeting.zip に含まれる Call Studio Record Agent Greeting スクリプトの例を、CallStudio が実行されているコンピュータにある任意のフォルダ抽出します。フォルダには、フォルダと同じ名前の CallStudio プロジェクトが含まれています。

ステップ 3 **[スタート（Start）]** > **[プログラム（Programs）]** > **[Cisco]** > **[Cisco Unified Call Studio]** の順に選択して、Call Studio を起動します。

ステップ 4 **[ファイル（File）]** > **[インポート（Import）]** の順に選択します。
[インポート（Import）] ダイアログボックスが表示されます。

ステップ 5 **Call Studio** フォルダを展開し、ワークスペースの **[既存Call Studio（Existing Call Studio）]** プロジェクトを選択します。

ステップ 6 [次へ（Next）] をクリックします。
[ファイルシステムからCall Studioプロジェクトをインポート（Import Call Studio Project From File System）] が表示されます。

ステップ 7 Call Studio プロジェクトを抽出した場所を参照します。フォルダを選択し、**[完了（Finish）]** を選択します。

例：

RecordAgentGreeting

ステップ 8 以下の手順に従って、定義されたパスにファイルを保存します。

a) **[Call Studioナビゲータ（Call Studio Navigator）]** パネルで、**RecordAgentGreeting** プロジェクトを開き、**app.callflow** をダブルクリックして、**[スクリプト（Script）]** ウィンドウにアプリケーション要素を表示します。

b) **Record Greeting With Confirm** ノードを選択します。

c) **[要素構成（Element Configuration）]** パネルで、**[設定（Setting）]** タブを選択し、デフォルトパス設定を `c:\inetpub\wwwroot\en-us\app\ag_gr` に修正します。変更後、プロジェクトを保存します。

d) **録音エージェントグリーティング**に関連付けられているプロジェクトを検証し、VXML サーバーに展開します。

ステップ 9 **[ナビゲータ（Navigator）]** ウィンドウの**録音エージェントグリーティング**プロジェクトを右クリックし、**[検証（Validate）]** を選択します。

ステップ 10 **[録音エージェントグリーティング（Record Agent Greeting）]** プロジェクトを右クリックし、**[展開（Deploy）]** をクリックします。

ステップ 11 **[展開先（Deploy Destination）]** 領域で、**[アーカイブファイル（Archive File）]** を選択し、**[参照（Browse）]** をクリックします。

ステップ 12 設定したアーカイブフォルダに移動します。

例：

`C:\Users\Administrator\Desktop\Sample.`

ステップ 13 ファイルの名前を入力します。

例：

Samplefile.zip

ステップ 14 [保存（Save）] をクリックします。

ステップ 15 **[展開先（Deploy Destination）]** 領域で、**[完了（Finish）]** をクリックします。

ステップ 16 **OAMP** にログインし、**[一括管理（Bulk Administration）] > [ファイル転送（File Transfer）] > [VXMLアプリケーション（VXMLApplications）]** の順に選択します。

ステップ 17 アプリケーションを展開する **VXML サーバー**を選択します。

ステップ 18 アプリケーションを含む zip ファイルを選択します。

例：

Samplefile.zip

ステップ 19 [転送（Transfer）] をクリックします。

ステップ 20 各プロジェクトを右クリックし、**[展開（Deploy）]** をクリックして、**[完了（Finish）]** をクリックします。

ステップ 21 Windows Explorer を使用して、`%CVP_HOME%\VXMLServer\applications\RecordAgentGreeting` に移動し、プロジェクトの admin フォルダを開いたら、deployApp.bat をダブルクリックしてアプリケーションを VXML サーバーに展開します。

ステップ 22 アプリケーション
が、`%CVP_HOME%\VXMLServer\applications\RecordAgentGreeting\admin` パスで実行されていることを確認したら、**status.bat** をダブルクリックします。[アプリケーション名（Application Name）] 配下に、ステータスが [実行中（Running）] のアプリケーションが表示されます。

メディアの IIS（Windows サーバー）でのコンテンツの有効期限の設定

Windows Server 上の IIS でコンテンツの有効期限を設定するには、以下の手順を実行します。

手順

ステップ 1 デスクトップの **My Computer** を右クリックし、**[管理（Manage）]** を選択します。

ステップ 2 **[サーバーマネージャ（Server Manager）]** > **[ロール（Roles）]** > **[Webサーバー（Web Server (IIS)）]**>**[インターネットインフォメーションサービス（IIS）マネージャ（Internet Information Services (IIS) Manager）]** の順に選択します。

ステップ 3 デフォルトの Webサイトを選択し、**[機能ビュー（Features View）]** に移動します。

ステップ 4 **[HTTP応答ヘッダー（HTTP Response Headers）]** をダブルクリックします。

ステップ 5 **[アクション（Actions）]** で、**[共通ヘッダーの設定…（Set Common Headers…）]** を選択します。

ステップ 6 **[共通HTTP応答ヘッダーの設定（Set Common HTTP Response Headers）]** で、**[HTTPキープアライブの有効化（Enable HTTP keep-alive）]** と **[Webコンテンツの期限切れ（Expire Web content）]** を選択し、**[5分後（After 5 minutes）]** を設定します。

設定 Unified CCE

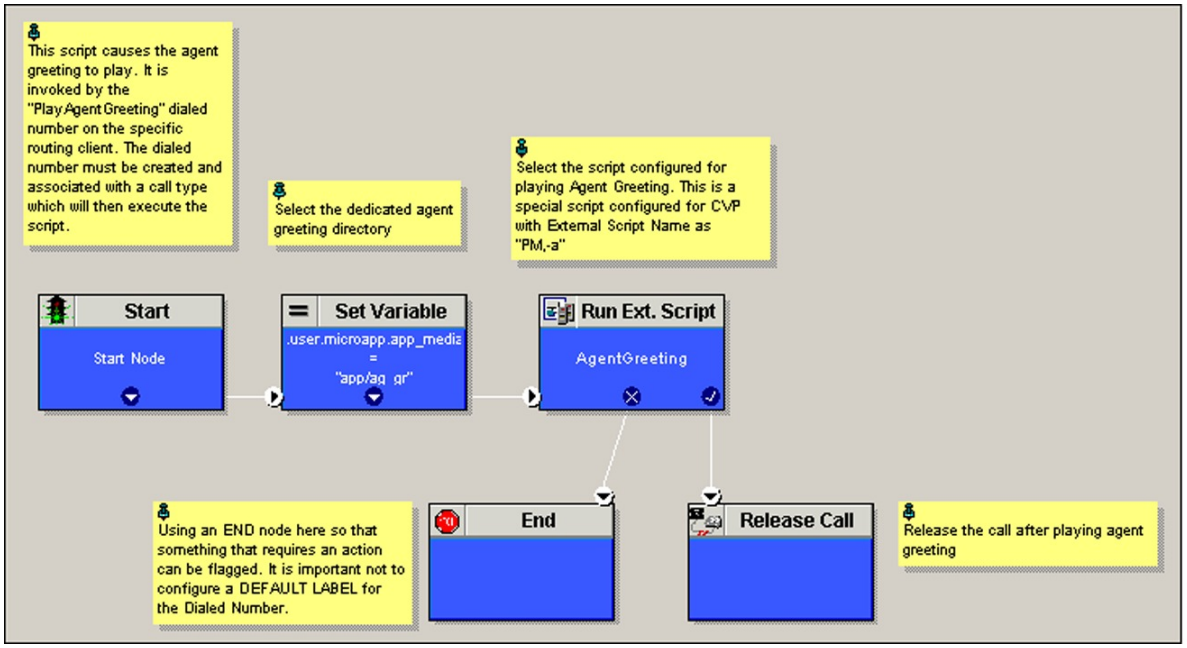
Unified CCE を構成するには、以下の手順を実行します。

- エージェントグリーティング再生スクリプトの作成 （339 ページ）
- エージェントグリーティング録音スクリプトの作成 （340 ページ）
- エージェント グリーティング スクリプト サンプルのインポート （341 ページ）

エージェントグリーティング再生スクリプトの作成

専用ルーティングスクリプトがエージェントグリーティングを再生します。このスクリプトは、特定のルーティングクライアントで PlayAgent Greeting がダイヤルした番号によって呼び出されます。ダイヤル番号を作成し、スクリプトを実行するコールタイプに関連付ける必要があります。

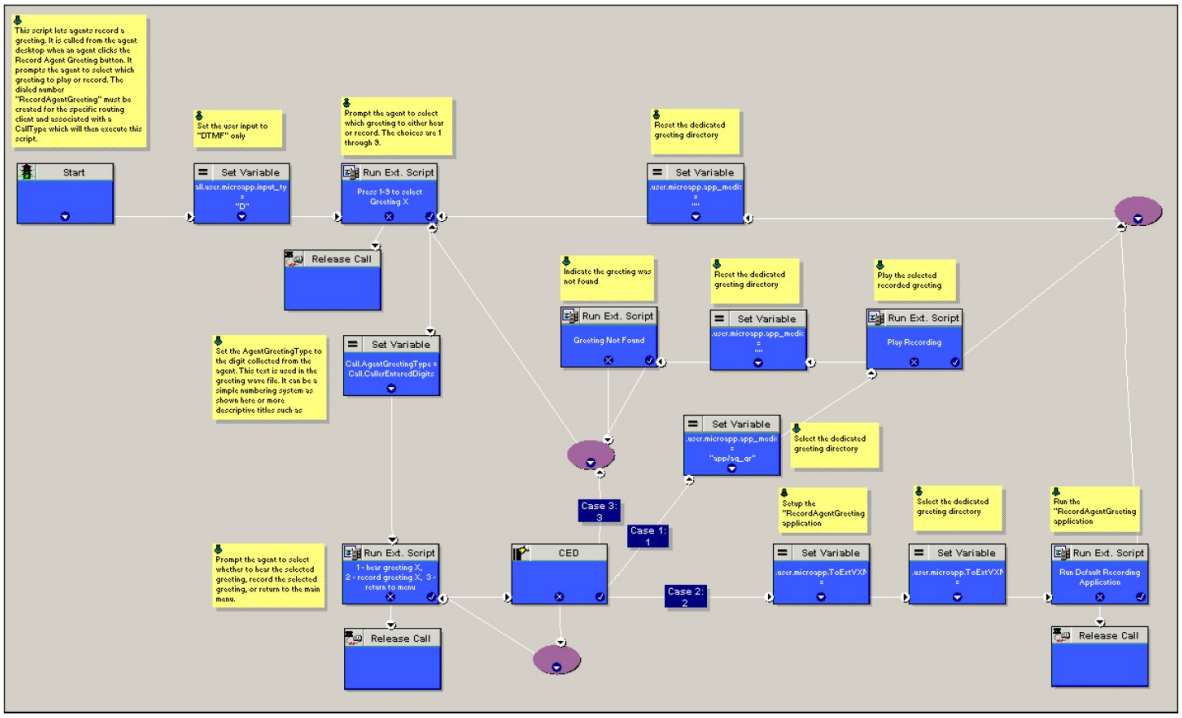
図 *11* : エージェントグリーティング再生スクリプト



エージェントグリーティング録音スクリプトの作成

エージェントグリーティング録音スクリプトを使用すると、エージェントはグリーティングを録音できます。エージェントデスクトップは、エージェントが [エージェントグリーティングの録音（Record Agent Greeting）] ボタンをクリックすると、エージェントに再生または録音するグリーティングの選択を求め、スクリプトを呼び出します。特定のルーティングクライアントのダイヤル番号 RecordAgentGreeting を作成し、このスクリプトを実行するコールタイプに関連付けます。

図 *12* : エージェントグリーティング録音スクリプト



録音エージェントグリーティングに対する Unified CCE の構成

- **user.microapp.ToExtVXML** ：これは、エージェント グリーティング レコードに使用します。1 回目は Unified CVP Record Agent Greeting をキューに入れ、2 回目は、greeting ファイルの保存場所を録音アプリケーションに通知します。サイズ 3 のアレイとして構成します。Unified CCE 管理を使用して、この変数に 100 と Enabled が最大長として含まれていることを確認します。
- **user.microapp.app_media_lib**：これは、エージェント グリーティング レコードおよび再生スクリプトに必要で、greeting ファイルが保存されているメディアサーバーで専用のディレクトリを指定します。最大長は、100 と Enabled です。
- **user.microapp.input_type**：これは、エージェント グリーティング レコード スクリプトに必要で、許容入力タイプを DTMF に制限します。最大長は、100 と Enabled です。

（注） ECC 変数を有効にするには、「拡張コール変数の構成（233 ページ）」を参照してください。

エージェント グリーティング スクリプト サンプルのインポート

サンプルのエージェント グリーティング スクリプトを表示または使用するには、まず Unified CCE Script Editor にスクリプトをインポートする必要があります。サンプルのエージェント グリーティング スクリプトをインポートするには、以下の手順を実行します。

手順

ステップ 1 **Script Editor** を起動します。

ステップ 2 **[ファイル（File）]**>**[スクリプトのインポート（Import Script）]** の順に選択し、インポートする以下のスクリプトを選択します。

a) エージェントグリーティング再生スクリプト

b) エージェントグリーティング録音スクリプト

スクリプトは、データサーバー（DS）ノードの icm\bin ディレクトリにあります。

ステップ 3 残りのスクリプトについてもこれを繰り返します。

（注） Small Contact Center 導入モデルの場合、デフォルト ルーティング スクリプトはパートナーコミュニティで使用できます。ISE がインストールされているデスクトップにルーティングスクリプトをダウンロードしたら、サブカスタマーユーザーとして ISE にログインし、手順 2 と 3 を実行します。すべての導入モデルのルーティングスクリプトファイル（https://software.cisco.com/download/navigator.html?mdfid=284526699）をダウンロードします。

（注） Small Contact Center 導入モデルの場合、ネットワーク VRU スクリプト、ECC 編集などのルーティングスクリプトで使用されるリソースがサブカスタマーに対して一意であることを確認してください。

コール タイプの設定

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして **Unified CCDM ポータル**にログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 コールタイプを作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** > **[コールタイプ（Call Types）]** の順に選択します。

ステップ 5 エージェントグリーティングを録音するコールタイプを作成し、**RecordAgentGreeting** と名前を付けます。

ステップ 6 エージェントグリーティングを再生するコールタイプを作成し、**PlayAgentGreeting** と名前を付けます。

着信番号の設定

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして **Unified CCDM ポータル**にログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 ダイヤル番号を作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** > **[ダイヤル番号（Dialed Number）]** の順に選択します。

ステップ 5 エージェントグリーティングを録音するダイヤル番号を作成し、名前として**RecordAgentGreeting** を入力します。

ステップ 6 エージェントグリーティングを再生するダイヤル番号を作成し、名前として **PlayAgentGreeting** を入力します。

ステップ 7 ダイヤル番号ごとに以下の手順を実行します。

a) ルーティングタイプとして **[内部音声（Internal Voice）]** を選択します。

b) デフォルトのドメイン値を保持します。

c) ダイヤル番号に適したコールタイプを選択します。

これにより、各番号をそのコールタイプと実行するスクリプトに関連付けることができます。

スクリプトのスケジュール

手順

ステップ 1 **Script Editor** で、**[スクリプト（Script）]** > **[コールタイプマネージャ（Call Type Manager）]** の順に選択します。

ステップ 2 [コールタイプマネージャ（Call Type Manager）] 画面で、**[スケジュール（Schedules）]** タブを選択します。

ステップ 3 [コールタイプ（Call type）]ドロップダウンリストで、PlayAgentGreeting など、スクリプトに関連付けるコールタイプを選択します。

ステップ 4 **[追加（Add）]** をクリックし、[スクリプト（Scripts）] ボックスから目的のスクリプトを選択します。

ステップ 5 **[OK]** を 2 回クリックし終了します。

エージェントグリーティングの構成

この項では、エージェントグリーティング機能の展開および構成方法に関して説明します。

エージェントグリーティング展開タスク

手順

ステップ 1 システムが、「システム要件と制限事項」の項で説明されているソフトウェア、ハードウェア、および構成の基準要件を満たしていることを確認します。

ステップ 2 メディアサーバーで IIS と FTP を構成します。

ステップ 3 Unified CVP で、メディアサーバーを追加し、FTP 接続情報を構成し、メディアサーバーを展開します。

ステップ 4 まだ構成していない場合は、Unified CVP メディアサーバーを構成します。Unified CVP メディアサーバーの構成 （74 ページ）を参照してください。

ステップ 5 Unified CVP オペレーションコンソールで、更新されたエージェント グリーティング サポートを使用して VXML Gateway.tcl スクリプトを再公開します。エージェント グリーティング サポートについては、「tcl スクリプトを VXML ゲートウェイに再発行 （334 ページ）」を参照してください。

ステップ 6 VXML ゲートウェイのキャッシュ サイズを設定します。VXML ゲートウェイのキャッシュサイズの設定 （334 ページ）を参照してください。

ステップ 7 エージェントがグリーティングを録音するときにエージェントに再生する音声プロンプトを録音し、メディアサーバーに音声ファイルを展開します。「録音グリーティング用音声プロンプトの作成 （336 ページ）」を参照してください。

ステップ 8 コールタイプの設定 （342 ページ）、エージェントグリーティングを録音および再生します。

ステップ 9 着信番号の設定 （343 ページ）、エージェントグリーティングを録音および再生します。

ステップ 10 スクリプトのスケジュール （343 ページ）

ステップ 11 Script Editor で：

- インストールしたスクリプトを使用してエージェントグリッパーを録音再生するには、「エージェント グリーティング スクリプト サンプルのインポート （341 ページ）」を参照してください。

ステップ 12 Unified CCE コールルーティングスクリプトを修正してエージェントグリーティング再生スクリプトを使用 （344 ページ）.

Unified CCE コールルーティングスクリプトを修正してエージェントグリーティング再生スクリプトを使用

エージェントグリーティング再生スクリプトを実行する際は、AgentGreetingType Set Variable ノードを既存の Unified CCE コールルーティングスクリプトに追加する必要があります。この変数値は、グリーティングを再生するオーディオファイルを選択するために使用します。エージェントへのコールをキューイングするスクリプトノード（つまり、[スキルグループまたはプレシジョンキューへの] キュー、キューエージェント、ルート選択、または選択ノード）の前に変数を設定します。

AgentGreetingType コール変数の指定

スクリプトにエージェントグリーティングを含めるには、AgentGreetingType コール変数を参照する Set Variable ノードを挿入します。AgentGreetingType 変数は、グリーティングを再生し、使用するオーディオファイルを指定します。変数値は、スキルグループまたはプレシジョンキューのグリーティングタイプの名前に対応します。たとえば、営業担当者のスキルグループまたはプレシジョンキューがあり、営業のグリーティングタイプが「5」の場合、変数値は 5 になります。

1 つのコールタイプ全体で 1 つのグリーティングプロンプトを使用できます。その結果、スクリプトごとに 1 つの AgentGreetingType セットノードを使用します。ただし、必要に応じて、スクリプトの複数の場所で変数を設定して、異なるエンドポイントで異なるグリーティングを再生できます。たとえば、スキルベースのルーティングを行う場合、特定のスキルグループまたはプレシジョンキューを選択するために使用する各決定ポイントで変数を指定できます。

（注） 各コールで再生できるグリーティングは 1 つのみです。スクリプトが AgentGreetingType 変数を参照し、スクリプトを通過する単一パスで複数回設定した場合、最後に設定される値が再生されます。

エージェントグリーティングの Set Variable ノードでこれら設定を使用します。

- オブジェクトタイプ：コール。
- 変数：AgentGreetingType 変数を使用する必要があります。
- タイプ：PersonID_AgentGreetingType タイプを使用する必要があります。
- 値：再生するグリーティングタイプに対応する値を指定します。例：「2」 または「フランス語」
  - 値は引用符で囲む必要があります。
  - 大文字と小文字は区別されません。
  - この値には、URL エンコーディングを必要とするスペースや文字を含めることはできません。

Unified Communications Manager の構成

ウィスパーアナウンスメントの構成

ウィスパーアナウンスメントを構成するには、以下の手順を実行します。

- ゲートウェイの構成 （346 ページ）
- Unified CVP の構成 （346 ページ）

• 設定 Unified CCE （346 ページ）

ゲートウェイの構成

ゲートウェイは、ウィスパーアナウンスメントに 2 つの異なるダイヤル番号を使用します。

- 91919191 の番号は、ウィスパーがエージェントに再生している際に、発信者に聞こえる着信音を鳴らします。
- 9191919100 の番号がウィスパー自体を呼び出します。

着信番号 9191919100 および 91919191 のダイヤルピアを次のように構成します。

```
dial-peer voice 919191 voip description CVP SIP ringtone dial-peer service
ringtone incoming called-number 9191T voice-class sip rel1xx disable dtmf-relay
 rtp-nte codec g711ulaw no vad
```

Unified CVP の構成

ウィスパーアナウンスメント サービスのダイヤル番号の構成

Unified CVP は、ウィスパーアナウンスメントに対して 2 つのダイヤル番号を使用します。

最初の番号は、エージェントにウィスパーが再生されている間に発信者に聞こえる着信音サービスを呼び出します。この番号の Unified CVP のデフォルトは 91919191 です。

2 つ目の番号はウィスパー自体を呼び出します。この番号の Unified CVP のデフォルトは 9191919100 です。

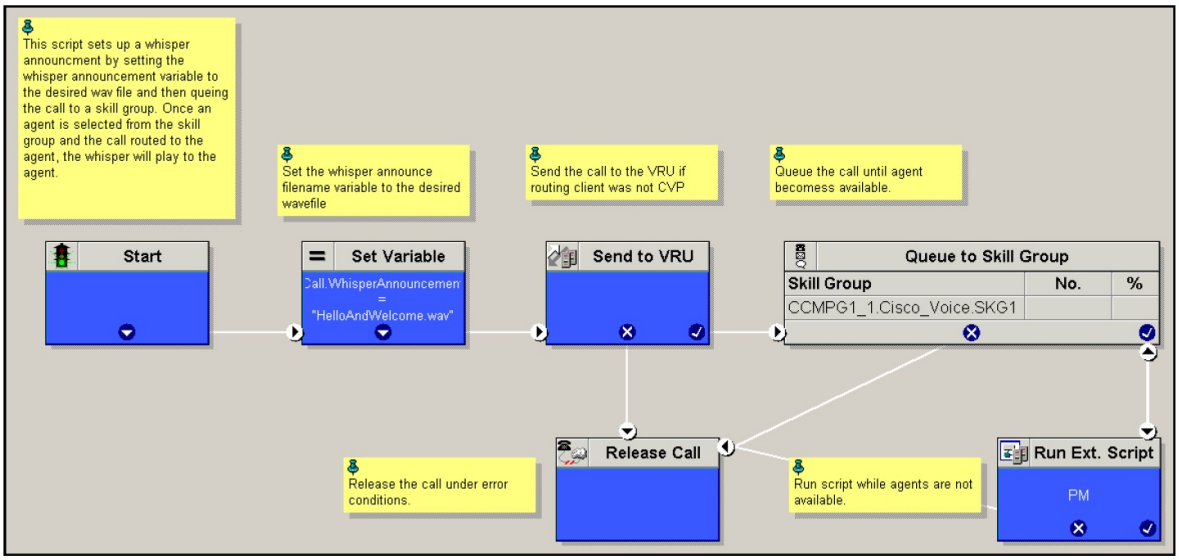
ウィスパーアナウンスメントが機能するには、ダイヤル番号パターンがこれらの番号の両方を網羅する必要があります。9111 *などのワイルドカードを使用すると網羅範囲を簡単に確認できます。ただし、完全に一致するダイヤル番号を使用する場合は、91919191 と9191919100 の両方を指定する必要があります。

設定 Unified CCE

ウィスパーアナウンスメント スクリプトの作成

コール付きのウィスパーアナウンスメントを展開することは非常に重要です。ウィスパーアナウンスメント変数と Unified CCE ルーティングスクリプトの .wav ファイルを設定します。

図 *13* : ウィスパーアナウンスメント スクリプト



データベース統合の構成

データベース統合を構成するには、以下の手順を実行します。

- Unified CVP の構成 （347 ページ）
- 設定 Unified CCE （350 ページ）

（注） Small Contact Center 導入モデルは、CVP データベース統合のみをサポートします。

Unified CVP の構成

VXML データベース要素の構成

VXML データベース要素の構成には、Java Database Connectivity（JDBC）を構成する必要があります。

JDBC を構成するには、以下の手順を実行します。

- JDBCドライバのインストール （348 ページ）
- JNDI コンテキストの追加 （348 ページ）
- VXML スタジオスクリプトの構成 （349 ページ）
- ICM スクリプトの作成 （349 ページ）

JDBCドライバのインストール

JDBC ドライバをインストールするには、以下の手順を実行します。

手順

ステップ 1 Microsoft JDBC Driver for SQL Server の .exe ファイルをダウンロードします。

例：

```
1033\sqljdbc_3.0.1301.101_enu.exe
```

ステップ 2 実行可能な .exe ファイルを実行し、`C:\temp\` にインストールします。

ステップ 3 `C:\temp\sqljdbc_3.0\enu\sqljdbc4.jar` というファイルを Unified CVP VXML サーバーのフォルダがある `C:\Cisco\CVP\VXMLServer\Tomcat\common\lib` にコピーします。

JNDI コンテキストの追加

Java Naming and Directory Interface（JNDI）コンテキスト構成を追加するには、以下の手順を実行します。

手順

ステップ 1 C:\Cisco\CVP\VXMLServer\Tomcat\conf\context.xml file から context.xml file にアクセスします。

ステップ 2 JNDI 名、SQL サーバーアドレス、SQL データベース名、ユーザー名、およびパスワードを入力します。

以下は、SQL authentication context.xml ファイルの例です。

```
<Context>

<WatchedResource>WEB-INF/web.xml</WatchedResource>

<Manager pathname="" />

<Resource name="jdbc/dblookup"

auth="Container"

type="javax.sql.DataSource"

DriverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver"

url="jdbc:sqlserver://<dblookupnode_ipaddress>:1433;databaseName=DBLookup;user=sa;password=sa"

>

</Context>
```

ステップ 3 VXML サーバーサービスを再起動するには、以下の手順を実行します。

a) **[実行（Run）]** ウィンドウに移動して、`services.msc` コマンドを入力します。

b) **[Cisco CVP VXMLサーバー（Cisco CVP VXML Server）]** のオプションを選択します。
c) 右クリックして、**[再起動（Restart）]** のオプションを選択します。

（注） Small Contact Center エージェント導入モデルの場合、リソース名は各カスタマーに対して一意である必要があります。たとえば、Sub-cust1 Resource name = "jdbc/dblookup1" and Sub-cust2 Resource name = "jdbc/dblookup2" です。

VXML スタジオスクリプトの構成

VXML Studio スクリプトを構成するには、以下の手順を実行します。

手順

ステップ 1 database 要素を使用して VXML アプリケーションを作成するには、以下を構成します。

a) **[タイプ（Type）]** で **[シングル（Single）]** を選択します。
b) **[JNDI名（JNDI Name）]** にデータベースルックアップ名を入力します。
c) クエリ SQL：

```
たとえば、select AccountNo from AccountInfo where CustomerNo = {CallData.ANI}

Where AccountNo - Value to be retrieved

AccountInfo - Table name

CustomerNo - condition to be queried

データ：

次の値を使用してデータベース要素を作成します。

Name - AccountNo

Value - {Data.Element.Database_01.AccountNo}
```

ステップ 2 ローカルコンピュータまたはリモートコンピュータ（VXML コールサーバーに直接）にスクリプトを展開して、CVP Subdialog return 要素を作成します。

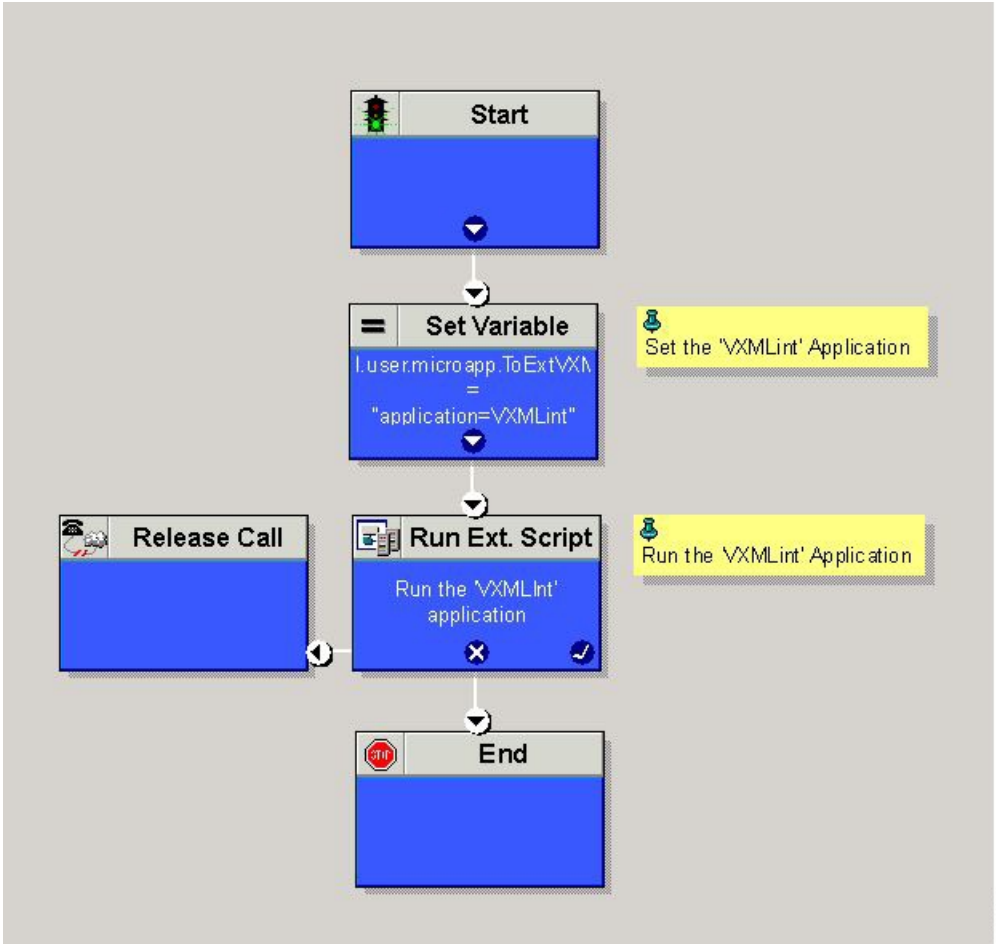
ステップ 3 これをローカルマシンに保存した場合は、フォルダ全体を

<Install dir>:\Cisco\CVP\VXMLServer\applications にコピーし、アプリケーションの admin フォルダ内にある deployApp windows バッチファイルを使用してそれを展開します。

ICM スクリプトの作成

以下の図に示すものと類似する ICM スクリプトの作成

図 *14 : ICM* データベースルックアップを使用したサンプルスクリプト



設定 Unified CCE

ICM データベース ルックアップの設定

ICM データベース ルックアップを設定するには、以下の手順を実行します。

手順

ステップ 1 **ルータ オプション**で**データベース ルーティングを有効にする**を選択して、データベースルックアップの変更に関するルータ設定を編集します。

ステップ 2 Database Lookup explorer の構成：

a) **スタート** > **すべてのプログラム** > **Cisco Unified CCE ツール** > **管理ツール** > **Configuration Manager**をクリックします。

b) **ツール** > **EXPLORER ツール** > **データベース ルックアップ EXPLORER** を開きます。

c) 以下の例に示される通りに、スクリプトテーブルとスクリプトテーブル列を設定します。

スクリプト テーブル：

```
名前：AccountInfo
サイド A：\\dblookup1\DBLookup.AccountInfo
サイド B：< データベースのサイド B をここで更新>
説明：<ここに説明を入力>
```

dblookup1 は外部データベースサーバ名、DBLookup は外部データベース名、AccountInfo はテーブル名です。

スクリプト テーブルの列:

```
カラム名 ：AccountNo
説明：<ここに説明を入力>
```

ステップ 3 Unified CCE でレジストリ設定を変更するには、以下の手順を実行します。

a) **[HKEY_LOCAL_MACHINE] > [ソフトウェア（SOFTWARE ）] > [Cisco Systems, Inc.] > [ICM] > [<Instance Name>] > [ルーターA（RouterA）] > [現在のバージョン（CurrentVersion）] > [構成（Configuration）] > [データベースレジストリ（Database registry）]** の順に選択します。

インスタンス名 は、設定するインスタンスの名前です。

b) 以下の例の通り SQLLogin レジストリキーを設定します。

例：

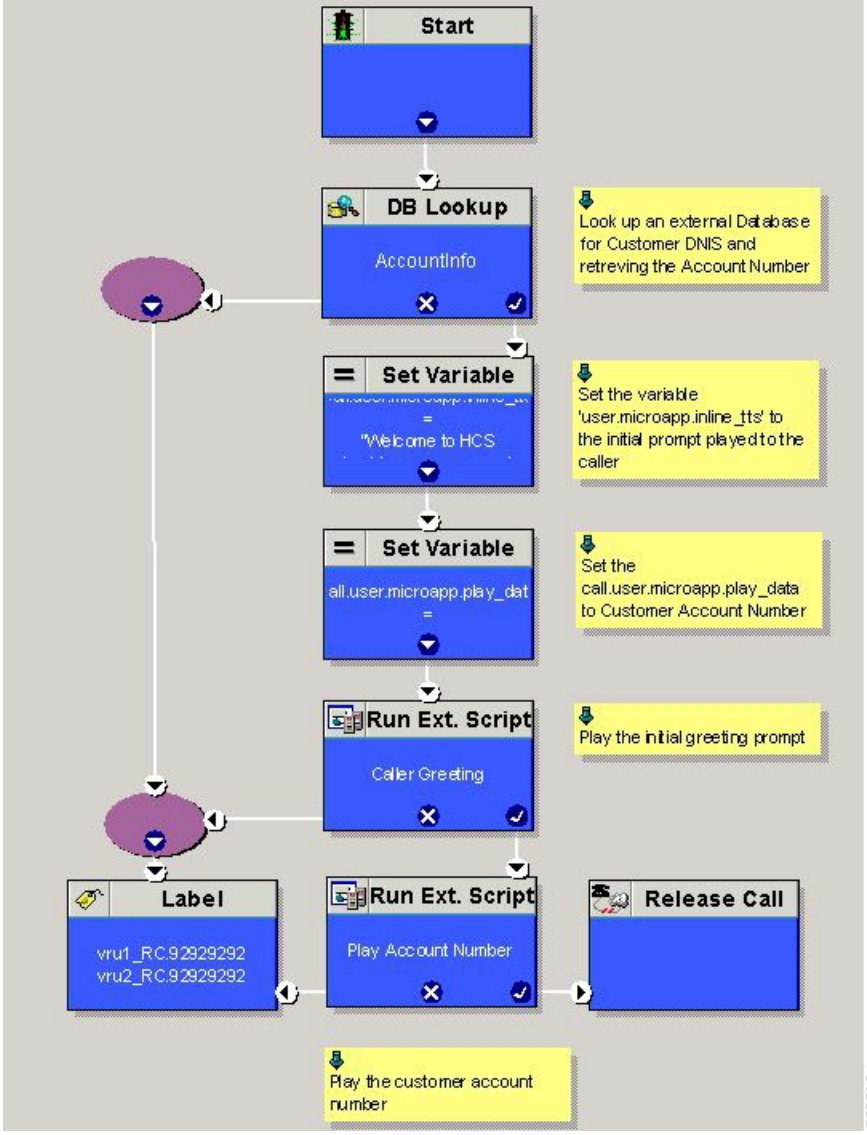
```
\\dblookup1\DBLookup=(sa,sa)
```

DBLookup は、外部データベース名、（sa, sa）は SQL サーバ認証です。

ステップ 4 対応するテーブルとルックアップ値を含むデータベース ルックアップ ノードを含む ICM スクリプトを作成します。

下の図は、ルックアップ値としてのテーブル名および CallingLineID としての AccountInfo を示しています。

図 *15 : ICM* データベース ルックアップの例



Unified Mobile Agent の構成

- VRF を使用した SCC 展開のためのゲートウェイの構成 （353 ページ）
- Unified CCE の構成 （353 ページ）
- Unified Communications Manager の構成 （354 ページ）

VRF を使用した SCC 展開のためのゲートウェイの構成

Sub-Customer1 Cisco Unified Communications Manager のダイヤルピアの構成

```
dial-peer voice 21011 voip
description from CVP towards VRF1 to Sub-Customer1 for mobileagent
destination-pattern 100.
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.100
voice-class sip bind media source-interface GigabitEthernet2.100
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Sub-Customer2 Cisco Unified Communications Manager のダイヤルピアの構成

```
dial-peer voice 22011 voip
description from CVP towards VRF2 to Sub-Customer2 for mobileagent
destination-pattern 300.
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.200
voice-class sip bind media source-interface GigabitEthernet2.200
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Unified CCE の構成

Unified CCE でモバイルエージェントを構成するには、以下の手順を実行します。

手順

ステップ 1 テナントまたはサブカスタマーユーザーとして **Unified CCDM ポータル**にログインします。

ステップ 2 バーガーアイコンをクリックし、**[プロビジョニング（Provisioning）]** > **[リソースマネージャ（Resource Manager）]** の順に選択します。

ステップ 3 エージェントデスクトップを作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** > **[エージェントデスクトップ（Agent Desktop）]** の順に選択します。

ステップ 5 レコードについて最大 32 文字の一意の名前を入力します。

この名前には、英数字、ピリオド、および下線を使用できます。

ステップ 6 **[着信作業モード（Incoming Work mode）]**、**[発信作業モード（Outgoing Work mode）]**、**[後処理時間（Wrap-up time）]** などの必須フィールドを入力します。

ステップ 7 [保存（Save）] をクリックします。

CTI OS サーバーでモバイル エージェント オプションを有効化

CTI OS サーバーでモバイル エージェント オプションを有効にするには、以下の手順を実行します。

手順

ステップ 1 CTI OS サーバーの設定を呼び出します。

ステップ 2 **[周辺機器識別子（Peripheral Identifier）]** ウィンドウで、**[モバイルエージェントの有効化（Enable Mobile Agent）]** チェックボックスをオンにし、ドロップダウンリストで **[モバイルエージェントモード（Mobile Agent Mode）]** を選択します。

ステップ 3 CTI OS サーバーの両サイドで上記手順を繰り返します。

Unified Communications Manager の構成

ユニファイド コミュニケーション マネージャを構成するには、以下の手順を実行します。

- CTI ポートの構成 （354 ページ）
- コンタクトセンター エージェント回線として CTI ポートをタグ付け （357 ページ）

CTI ポートの構成

電話番号が追加されていることを確認します。電話番号インベントリの追加 （301 ページ）を参照してください。

Unified Mobile Agent には、Unified Communications Domain Manager で以下 2 つの構成済み CTI ポートプールが必要です。

- エージェントの仮想拡張としてのローカル CTI ポート
- モバイルエージェントの電話機に電話発信するネットワーク CTI ポート

（注） 12000 エージェント導入モデルの場合は、3 つすべての Unified CM クラスタに CTI ポートを追加します。

CTI ポートを構成するには、以下の手順を実行します。

- プロバイダまたはリセラーとして CTI ポートを構成 （355 ページ）
- カスタマーとして CTI ポートを構成 （356 ページ）

プロバイダまたはリセラーとして CTI ポートを構成

手順

ステップ 1 プロバイダまたはリセラーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なサイトに設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[電話機（Phones）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **[電話機（Phones）]** タブで、以下の手順を実行します。

a) **[デバイス名（Device Name）]** フィールドに、 *LCPxxxxFyyyy* 形式で、ローカル CTI ポートプール名を入力します。

- LCP — ローカルデバイスとして CTI ポートを識別します。
- xxxx ー Unified Communications Manager PIM の周辺機器 ID です。
- yyyy — ローカル CTI ポートです。

b) **[製品タイプ（Product Type）]** ドロップダウンリストで、**[CTIポート（CTI Port）]** を選択します。

c) ドロップダウンリストで、**[コーリングサーチスペース（Calling Search Space ）]** を選択します。

d) ドロップダウンリストで、**[デバイスプール（Device Pool）]** を選択します。

e) ドロップダウンリストで、**[ロケーション（Location）]** を選択します。

ステップ 6 **[回線（Lines）]** タブに移動します。

a) **[回線（Lines）]** パネルの **[追加（Add）]** アイコンをクリックします。

b) **[Drin]** パネルの **[パターン（Pattern）]** ドロップダウンリストで、電話番号を選択します。

c) ドロップダウンリストで、**[ルートパーティション名（Route Partition Name）]** を選択します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

上記の手順を繰り返して、ネットワーク CTI ポートを作成します。**[デバイス名（Device Name）]** フィールドで、*RCPxxxxFyyyy* 形式で、ネットワーク CTI ポートプール名を入力します。

- RCP ー ネットワークデバイスとして CTI ポートを識別します。
- xxxx ー Unified Communications Manager PIM の周辺機器 ID です。
- yyyy ー ネットワーク CTI ポートです。

（注） ローカル CTI ポートとネットワーク CTI ポートは同じである必要があります

カスタマーとして CTI ポートを構成

手順

ステップ 1 カスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なサイトに設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[電話機（Phones）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **[基本情報（Basic Information）]** タブで、以下の手順を実行します。

a) **[製品タイプ（Product Type）]** ドロップダウンリストで、**[CTIポート（CTI Port）]** を選択します。

b) **[デバイス名（Device Name）]** フィールドに、 *LCPxxxxFyyyy* 形式で、ローカル CTI ポートプール名を入力します。

- LCP — ローカルデバイスとして CTI ポートを識別します。
- xxxx — Unified Communications Manager PIM の周辺機器 ID です。
- yyyy — ローカル CTI ポートです。

c) ドロップダウンリストで、**[コーリングサーチスペース（Calling Search Space ）]** を選択します。

ステップ 6 **[詳細情報（Advanced Infromation）]** タブに移動します。

a) ドロップダウンリストで、**[デバイスプール（Device Pool）]** を選択します。

b) ドロップダウンリストで、**[ロケーション（Location）]** を選択します。

ステップ 7 **[回線（Lines）]** タブに移動します。

a) **[回線（Lines）]** パネルの **[追加（Add）]** アイコンをクリックします。

b) **[Drin]** パネルの **[パターン（Pattern）]** ドロップダウンリストで、電話番号を選択します。

c) ドロップダウンリストで、**[ルートパーティション名（Route Partition Name）]** を選択します。

ステップ 8 [保存（Save）] をクリックします。

次のタスク

上記の手順を繰り返して、ネットワーク CTI ポートを作成します。**[デバイス名（Device Name）]** フィールドで、*RCPxxxxFyyyy* 形式で、ネットワーク CTI ポートプール名を入力します。

- RCP ー ネットワークデバイスとして CTI ポートを識別します。

- xxxx ー Unified Communications Manager PIM の周辺機器 ID です。
- yyyy ー ネットワーク CTI ポートです。

（注） ローカル CTI ポートとネットワーク CTI ポートは同じである必要があります

コンタクトセンター エージェント回線として CTI ポートをタグ付け

始める前に

CTI ポートが追加されていることを確認します。参照 CTI ポートの構成 （354 ページ）

（注） 12000 エージェント導入モデルでは、3 つすべての Cisco Unified Communications Manager クラスタの CTI ポートにタグを付ける必要があります。

LCP および RCP CTI ポートの両方に対して、以下の手順を実行します。

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なレベルに設定されていることを確認します。

ステップ 3 **[サブスクライブ管理（Subscribe Management）]** > **[エージェント回線（Agent Lines）]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **[デバイスタイプ（Device Types）]** ドロップダウンリストで、**[電話機（Phones）]** を選択します。

ステップ 6 **[デバイス名（Device Name）]** ドロップダウンリストで**[CTIポート（CTI Ports）]** を選択します。

ステップ 7 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインし、**[システムマネージャ（System Manager）]** を選択します。で

ステップ 8 ドロップダウンリストで **[アプリケーションユーザー（Application User）]** を選択します。

ステップ 9 [保存（Save）] をクリックします。

アウトバウンドダイヤラの構成

アウトバウンドダイヤラを構成するには、以下の手順を実行します。

- ゲートウェイの構成 （358 ページ）
- Unified CVP の構成 （360 ページ）
- Unified CCE の構成 （360 ページ）
- Unified Communications Manager の構成 （375 ページ）

ゲートウェイの構成

（注）
- Small Contact Center 導入モデルでは、お客様が専用または共有アウトバウンドゲートウェイを選択できます。共有ゲートウェイの場合は、PSTN 接続が必要です。
- アウトバウンドダイヤラは A-law をサポートしていません。音声ゲートウェイのインバウンドダイヤルピアで A-law を構成するように指示されていません。

ゲートウェイまたは CUBE(E) を構成するには、以下の手順を実行します。

手順

ステップ 1 次の voip パラメータを使用して音声カプセル化タイプを作成します。

例：

```
voice service voip
     no ip address trusted authenticate
     mode border-element
     allow-connections sip to sip
     no supplementary-service sip refer
     supplementary-service media-renegotiate
     redirect ip2ip
     signaling forward none
sip
     header-passing
     error-passthru
     asymmetric payload full
     options-ping 60
     midcall-signaling passthru
     !
```

ステップ 2 デフォルトでは、ゲートウェイまたは CUBE(E) の CPA が有効になっています。有効になっていない場合は、CUBE(E) の CPA を有効にします。

例：

```
voice service voip
 cpa
```

ステップ 3 音声コーデッククラスの作成

例：

```
voice class codec 1
     codec preference 1 g729r8
     codec preference 2 g711ulaw
```

ステップ 4 カスタマー PSTN 番号に到達するためのダイヤルピア構成を作成します。

例：

```
dial-peer voice 978100 voip
     session protocol sipv2
     incoming called-number <Customer Phone Number Pattern>
     voice-class codec 1
     voice-class sip rel1xx supported "100rel"
     dtmf-relay rtp-nte sip-kpml
     no vad

dial-peer voice 97810 pots
     destination-pattern 97810[1-9]
     port 1/0:23
     forward-digits all
     progress_ind alert enable 8
```

ステップ 5 エージェントの内線番号（VOIP）に到達するためのダイヤルピア構成の作成

例：

```
dial-peer voice 40000 voip
     description ***To CUCM Agent Extension***
     destination-pattern <Agent Extension Pattern to CUCM>
     session protocol sipv2
     session target ipv4:<CUCM IP Address>
     voice-class codec<Codec Preference number>
     voice-class sip rel1xx supported "100rel"
     dtmf-relay rtp-nte
     no vad
     !
```

（注） 12000 エージェント導入モデルでは、3 つの Cisco Unified Communications Manager クラスタすべてにダイヤルピアを作成する必要があります。

ステップ 6 CVP に到達するためのダイヤルピア構成の作成

例：

```
dial-peer voice 99995 voip
     description ******To CVP for IVR OB*****
     destination-pattern 9999500T
     session protocol sipv2
     session target ipv4:10.10.10.10
     codec g711ulaw
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte h245-signal h245-alphanumeric
     no vad
     !
     !
```

（注）

ステップ 7 CUBE E のトランスコーディング プロファイルを構成するには、以下の手順を実行します。

例：

```
dspfarm profile 4 transcode universal
     codec g729r8
```

```
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
maximum sessions 250
associate application CUBE
!
```

Unified CVP の構成

既存の Unified CVP コールサーバーにアウトバウンド構成を追加

既存の Unified CVP コールサーバーにアウトバウンド構成を追加するには、以下の手順を実行します。

手順

ステップ 1 Unified CVP OAMP サーバーに移動し、オペレーション コンソール ページにログインします。

ステップ 2 **[デバイス管理（Device Management）]** タブをクリックし、メニューから Unified CVP コールサーバーを開きます。

ステップ 3 コールサーバーを開き、**[ICM]** タブをクリックして DNIS を追加します。

DNIS 番号は、Unified CCE のアウトバウンド用 Network VRU Explorer で構成されたラベルと一致する必要があります。

ステップ 4 **[保存（Save）]** をクリックして、展開します。

ステップ 5 CVP コールサーバーごとに手順 3 を繰り返します。

Unified CCE の構成

- ICMDBA ツールを使用してアウトバウンドオプションデータベースを追加 （361 ページ）
- アウトバウンドオプションの Logger 構成 （361 ページ）
- アウトバウンドダイヤラの構成 （363 ページ）
- アウトバウンド PIM の作成 （364 ページ）
- SIP アウトバウンドの構成 （364 ページ）
- 周辺機器ゲートウェイの設定を使用した SIP ダイヤラのインストール （372 ページ）
- DNP ホストファイルの追加 （374 ページ）
- アウトバウンド オプション エンタープライズ データ （375 ページ）

ICMDBA ツールを使用してアウトバウンドオプションデータベースを追加

（注）
- 2000、4000 エージェント導入モデルおよび Small Contact Center の場合は、Unified CCE Rogger で構成を実行します。
- 12000 エージェント導入モデルの場合は、Unified CCE Rogger で構成を実行します。

手順

ステップ 1 スタート > すべてのプログラム > **Cisco Unified CCE ツール** > **ICMdba**を選択します。警告に対して **はい** をクリックします。

ステップ 2 **[サーバー（Server）]** > **[インスタンス（Instance）]** > **[Logger]** の順に選択します。インストールされている logger を右クリックたら、**[作成（Create）]** を選択して Outbound Option データベースを作成します。

ステップ 3 **[データベースの作成（Create Database）]** ダイアログボックスで、**[追加（Add）]** を選択し、[デバイスの追加（Add Device）] を開きます。**データ**をクリックしますE ドライブを選択します。DB サイズは、デフォルト値のままにして、**OK** をクリックして、[データベースの作成] ダイアログ ボックスに戻ります。

ステップ 4 **[デバイスの追加（Add Device）]** ダイアログボックスで、**[ログ（Log）]** をクリックします。E ドライブを選択します。[ログサイズ（Log Size）] フィールドはデフォルト値のままにします。**OK** をクリックして、[データベースの作成] ダイアログ ボックスに戻ります。

ステップ 5 **[データベースの作成（Create Database）]** ダイアログボックスで、**[作成（Create）]** > **[スタート（Start）]** の順に選択します。作成成功のメッセージを確認したら、**[OK]** > **[閉じる（Close）]** の順に選択します。

アウトバウンドオプションの Logger 構成

アウトバウンドオプションの Logger を構成するには、以下の手順を実行します。

オプションで、Logger を構成すると、アウトバウンドオプションとアウトバウンドオプションの高可用性を有効化できます。アウトバウンドオプションで高可用性を使用すると、サイド A Logger のアウトバウンド オプション データベースと、サイド B Logger のアウトバウンド オプション データベース間の双方向レプリケーションが容易になります。ICMDBA ツールを使用して、サイド A とサイド B にアウトバウンド データベースを作成したら、Web 設定を使用してレプリケーションを設定します。

サイド A とサイド B の両方の Logger で以下の手順を実行して、アウトバウンドオプションまたはアウトバウンドオプションの高可用性を構成します。両方の Logger マシンが稼働している必要があります。

重要 アウトバウンドオプションの高可用性の Logger を構成する前に、以下の手順を実行します。

- Logger サイド A と Logger サイド B にアウトバウンド オプション データベースが存在することを確認します。
- Microsoft SQL Server ユーザーを作成し、そのユーザーに sysadmin 権限を割り当てます。Logger サイド A と Logger サイド B で同じユーザー名とパスワードを使用します（アウトバウンドオプションを構成し、アウトバウンドオプションの高可用性を有効にするには、以下の手順でこのユーザー名とパスワードを使用します）。
- NT 権限/システムユーザーに sysadmin 権限を割り当てます。

手順

ステップ 1 Web 設定ツールを開きます。

ステップ 2 **[コンポーネント管理（Component Management）] > [Loggers]** の順に選択します。

ステップ 3 構成する Logger を選択し、**[編集（Edit）]** をクリックします。

ステップ 4 [次へ（Next）] を 2 回クリックします。

ステップ 5 追加オプションページで、**[アウトバウンドオプションを有効化（Enable Outbound Option）]** チェックボックスをオンにします。

ステップ 6 **高可用性を有効にする**チェックボックスをクリックして、アウトバウンドオプションの Logger での高可用性を有効にします。このチェックボックスをオンにすると、Logger サイド A のアウトバウンド オプションのデータベースと Logger サイド B のアウトバウンド オプションのデータベース間のアウトバウンドオプションの高可用性双方向レプリケーションが有効になります。双方向レプリケーションでは、Logger サイド A と Logger サイド B の両方に対して追加オプションページでこのチェックボックスをオンにする必要があります。どちらか一方のサイドで、双方向レプリケーションを無効化するには、該当する方のサイドで双方向レプリケーションを無効化します。

アウトバウンド オプションの高可用性を有効にするには、アウトバウンド オプションの高可用性を有効にする必要があります。同様に、高可用性を有効化するには、アウトバウンドオプション（**[アウトバウンドオプションを有効化（Enable Outbound Option）]** チェックボックスをオフにする）を無効化する前に、高可用性を無効化（**[高可用性を有効化（Enable High Availability）]** チェックボックスをオフにする）する必要があります。

ステップ 7 高可用性を有効にする場合は、**Logger サイド A** および **Logger サイド B**の有効なパブリック サーバのホスト名アドレスを入力します。サーバ名のかわりに、サーバの IP アドレスを入力することはできません。

ステップ 8 高可用性を有効化するには、SQL サーバーシステム管理権限を持つユーザーの **SQL サーバー管理ログイン情報（ユーザー名とパスワード）**を入力し、双方向レプリケーションを確立します。Logger サイド A と Logger サイド B では同じログイン情報を使用します。

SQL レプリケーションでは、高可用性を設定するために、正しい SQL サーバーシステム管理ユーザー名とパスワードが必要です。その SQL アカウントのパスワードを変更すると、高可用性を無効にして新しいユーザー名とパスワードで再度有効にするまで、レプリケーションは失敗します。この要件のために、そのアカウントのパスワードを変更するタイミングと方法には注意してください。

任意の有効な SQL サーバーシステム管理アカウントを使用して高可用性を無効化します。無効にすると、高可用性を再度有効化する際に、有効な SQL サーバーシステム管理アカウントを設定できます。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 サマリーページを見直したら、**[完了（Finish）]** をクリックします。

アウトバウンドダイヤラの構成

手順

ステップ 1 Unified CCE Admin Workstation サーバーで、**[スタート（Start）]** > **[Cisco Unified CCEツール（Cisco Unified CCE Tools）]** > **[管理ツール（Administration Tools）]** > **[構成マネージャ（Configuration Manager）]** の順に選択します。

ステップ 2 **[構成マネージャ（Configuration Manager）]** ウィンドウで、**[アウトバウンド（Outbound）]** > **[ダイヤラ（Dialer）]** の順に選択します。

ステップ 3 Small Contact Center の場合は、**[取得（Retrieve）]** > **[追加（Add）]** の順に選択し、以下を構成します。

a) ダイヤラ名を入力します。

b) [ICM周辺機器名（ICM Peripheral Name）] を入力します。

c) [ハングアップ遅延（1-10）（Hangup Delay (1-10)）] の値を **1** と入力します。

d) [ポートスロットル（Port Throttle）] の値を **10** と入力します。

e) [保存（Save）] をクリックします。

ステップ 4 **[ポートマップの選択（Port Map Selection）]** タブをクリックして、ポートマップ構成を表示します。

ステップ 5 **[追加（Add）]** をクリックして、一連のポートと関連する内線番号を構成します。

ステップ 6 [OK] をクリックします。

ステップ 7 **[保存（Save）]** > **[閉じる（Close）]** の順に選択します。

（注） サブカスタマーごとにダイヤラが異なるため、異なるサブカスタマーの場合、ポートと内線番号の範囲を同じにすることができます。

アウトバウンド PIM の作成

メディアルーティング周辺機器ゲートウェイを構成し、アウトバウンド PIM を追加します。詳細については、MR 周辺機器ゲートウェイの構成 （52 ページ）を参照してください。

SIP アウトバウンドの構成

インポートルールの追加

手順

ステップ 1 **Unified CCE データサーバー** または **Unified CCE AW-HDS-DDS** マシンにアクセスします。

ステップ 2 **[構成マネージャ（Configuration Manager）]** > **[アウトバウンドオプション（Outbound Option）]** > **[ルールのインポート（Import Rule）]** の順に選択し、**[取得（Retrieve）]** をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **[一般ルールのインポート（Import Rule General）]** タブで、以下を実行します。

a) **[インポート名（Import Name）]** を入力します。

b) ドロップダウンリストで**[インポートタイプ（Import Type）]**を選択します。

c) **[対象テーブル名（Target Table Name）]** を入力します。

d) **[ファイルパスのインポート（Import File Path）]** を参照します。

（注）
- **Contact** のインポートタイプについては、Contact Import ファイルを参照します。参照 連絡先インポートファイルの作成 （371 ページ）
- **Do Not Call** のインポートタイプについては、Do Not Call List ファイルを参照します。参照 電話禁止リストの作成 （371 ページ）

e) **[データタイプのインポート（Import Data Type）]** パネルから **[カンマ区切り（Comma Delimited）]** を選択します。
f) **[テーブルの上書き（Overwrite Table）]** チェックボックスをオンにします。

（注） キャンペーン中は、**[ファイルパスのインポート（Import File Path）]** オプションも **[上書き（Overwrite）]** オプションも使用しないでください。使用すると、ダイヤラがレコードにアクセスできなくなります。

ステップ 5 **[定義（Definition）]** タブにアクセスします。
a) [追加（Add）] をクリックします。
b) ドロップダウンリストで、**[標準列タイプ（Standard Column Type）]** を選択し、残りのフィールドは、デフォルト値のままにします。

ステップ 6 [保存（Save）] をクリックします。

インポートルールの削除

インポートルールを削除すると、対応する連絡先テーブルが削除されます。

アウトバウンドオプション高可用性を使用し、ルール削除時に、サイド A またはサイド B のいずれかがダウンしている場合でも、そのサイドの対応テーブルは削除されません。ただし、サイドが再起動すると、テーブルは自動的に削除されます。

クエリルールの追加

始める前に

1 つ以上のインポートルールを定義する必要があります。インポートルールの追加 （364 ページ）を参照してください

。

手順

ステップ 1 **Unified CCE データサーバー**または **Unified CCE AW-HDS-DDS** マシンにアクセスします。
ステップ 2 **[構成マネージャ（Configuration Manager）]** > **[アウトバウンドオプション（Outbound Option）]** > **[クエリルール（Query Rule）]** の順に選択し、**[取得（Retrieve）]** を選択します。
ステップ 3 [追加（Add）] をクリックします。
ステップ 4 **クエリルール名**を入力します。
ステップ 5 ドロップダウンリストで、**[インポートルール（Import Rule）]** を選択します。
ステップ 6 **ルール句**を入力します。
ステップ 7 [保存（Save）] をクリックします。

次のタスク

1. **[構成マネージャ（Configuration Manager）] > [ツール（Tools）] > [リストツール（List Tools）] > [コールタイプリスト（Call Tye List）]** の順に選択し、エージェントベースのキャンペーンと IVR ベースのキャンペーンの 2 つのコールタイプを追加します。
2. **[構成マネージャ（Configuration Manager）] > [ツール（Tools）] > [リストツール（List Tools）] > [ダイヤル番号/スクリプトセレクタリスト（Dialed Number/Script Selector List）]** の順に選択し、メディアルーティングドメインの配下に 2 つのダイヤル番号を追加します。ダイヤル番号を前の手順で作成したコールタイプにマッピングします（コールタイプごとに 1 つのダイヤル番号）。
3. **[構成マネージャ（Configuration Manager）] > [ツール（Tools）] > [エクスプローラツール（Explorer Tools）] > [スキルグループエクスプローラ（Skill Group Explorer）]** の順に選択し、通話マネージャ周辺機器の配下にスキルグループを追加します。このスキルグループにルートを追加します。
4. **[構成マネージャ（Configuration Manager）] > [ツール（Tools）] > [エクスプローラツール（Explorer Tools）] > [Agent Explorer]** の順に選択し、エージェントを追加します。前の手順で作成したスキルグループにエージェントを関連付けます。

クエリルールの削除

クエリルールを削除すると、対応するダイヤリングリストテーブルも削除されます。

アウトバウンドオプション高可用性を使用し、ルール削除時に、サイド A またはサイド B のいずれかがダウンしている場合でも、そのサイドの対応テーブルは削除されません。ただし、サイドが再起動すると、テーブルは自動的に削除されます。

キャンペーンの追加

- -
- -

エージェントベースのキャンペーンの追加

手順

ステップ 1 **Unified CCE データサーバー** または **Unified CCE AW-HDS-DDS** マシンにアクセスします。

ステップ 2 **[構成マネージャ（Configuration Manager）] > [アウトバウンドオプション（Outbound Option）] > [ルールのインポート（Import Rule）]** の順に選択し、**[取得（Retrieve）]** をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **キャンペーン名**を入力します。

ステップ 5 **[キャンペーンの目的（Campaign Purpose）]** タブに移動します。

a) **[エージェントベースのキャンペーン（Agent Based Campaign）]** オプションを選択します。
b) **[IP AMDを有効化（Enable IP AMD）]** チェックボックスをオンにします。
c) **[エージェントに転送（Transfer to Agent）]** オプションを選択します。

ステップ 6 **[クエリ規則の選択（Query Rule Selection）]** タブに移動し、**[追加（Add）]** をクリックします。
a) ドロップダウンリストから **[クエリ規則名（Query Rule Name）]** を選択し、**[OK]** をクリックします。

ステップ 7 **[スキルグループの選択（Skill Group Selection）]** タブに移動します。
a) **[周辺機器（Peripheral）]** ドロップダウンリストから適切な CUCM PG を選択し、**[取得（Retrieve）]** をクリックします。
b) ドロップダウンリストで、**[スキルグループ（Skill Group）]** を選択します。
c) **[スキルごとのオーバーフローエージェント（Overflow Agents per Skill）]** の値を入力します。
d) **[ダイヤル番号（Dialed number）]** を入力します。
e) **[キャッシュするレコード（Records to cache）]** の値を入力します。
f) **[IVRポート数（Number of IVR Ports）]** を入力します。
g) [OK] をクリックします。

ステップ 8 **[コールターゲット（Call Target）]** タブに移動し、ドロップダウンリストから **[サマータイムゾーン（Daylight Savings Zone）]** を選択します。

ステップ 9 [保存（Save）] をクリックします。

IVR ベースのキャンペーンの追加

手順

ステップ 1 **Unified CCE データサーバー** または **Unified CCE AW-HDS-DDS** マシンにアクセスします。

ステップ 2 **[構成マネージャ（Configuration Manager）]** > **[アウトバウンドオプション（Outbound Option）]** > **[ルールのインポート（Import Rule）]** の順に選択し、**[取得（Retrieve）]** をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **キャンペーン名**を入力します。

ステップ 5 **[キャンペーンの目的（Campaign Purpose）]** タブに移動します。
a) **[IVRキャンペーンの転送（Tranfer to IVR Campaign）]** オプションを選択します。
b) **[IP AMDを有効化（Enable IP AMD）]** チェックボックスをオンにします。
c) **[IVRルートポイントに転送（Transfer to IVR Route Point）]** オプションを選択します。

ステップ 6 **[クエリ規則の選択（Query Rule Selection）]** タブに移動し、**[追加（Add）]** をクリックします。
a) ドロップダウンリストで **[クエリ規則名（Query Rule Name）]** を選択し、**[OK]** をクリックします。

ステップ 7 **[スキルグループの選択（Skill Group Selection）]** タブに移動します。

a) **[周辺機器（Peripheral）]** ドロップダウンリストで適切な CUCM PG を選択し、**[取得（Retrieve）]** をクリックします。

b) ドロップダウンリストで、**[スキルグループ（Skill Group）]** を選択します。

c) **[スキルごとのオーバーフローエージェント（Overflow Agents per Skill）]** の値を入力します。

d) **[ダイヤル番号（Dialed number）]** を入力します。

e) **[キャッシュするレコード（Records to cache）]** の値を入力します。

f) **[IVRポート数（Number of IVR Ports）]** を入力します。

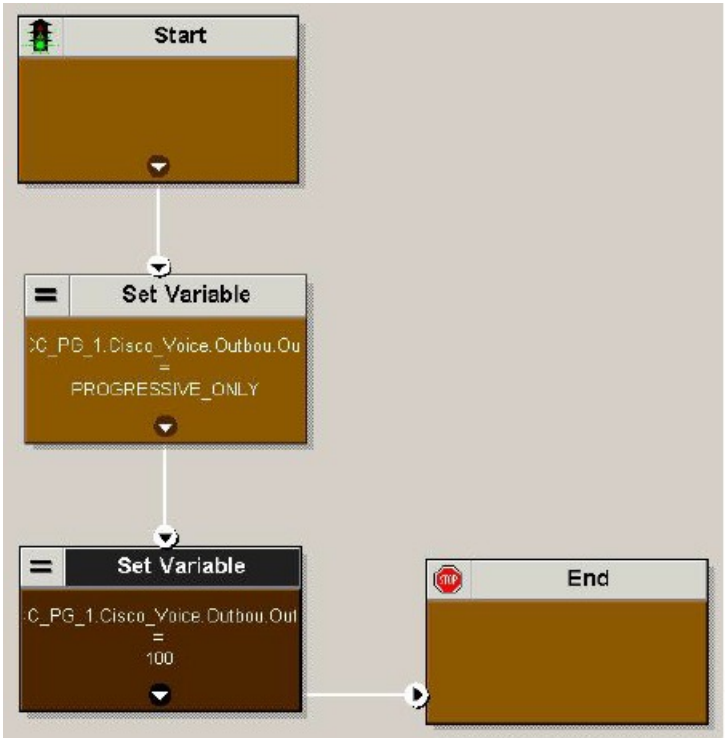
g) [OK] をクリックします。

ステップ 8 **[コールターゲット（Call Target）]** タブに移動し、ドロップダウンリストで **[サマータイムゾーン（Daylight Savings Zone）]** を選択します。

ステップ 9 [保存（Save）] をクリックします。

管理スクリプトの作成

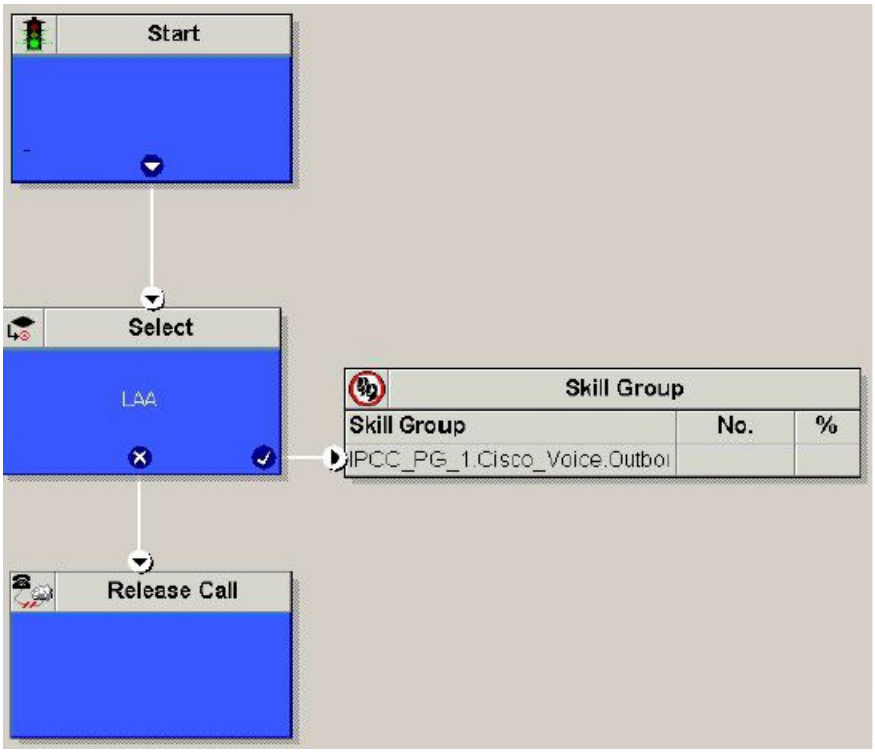
図 *16 :* 管理スクリプトの作成



詳細については、『アウトバウンド オプション ガイド』を参照してください。

エージェントベースのキャンペーンのルーティングスクリプトの追加

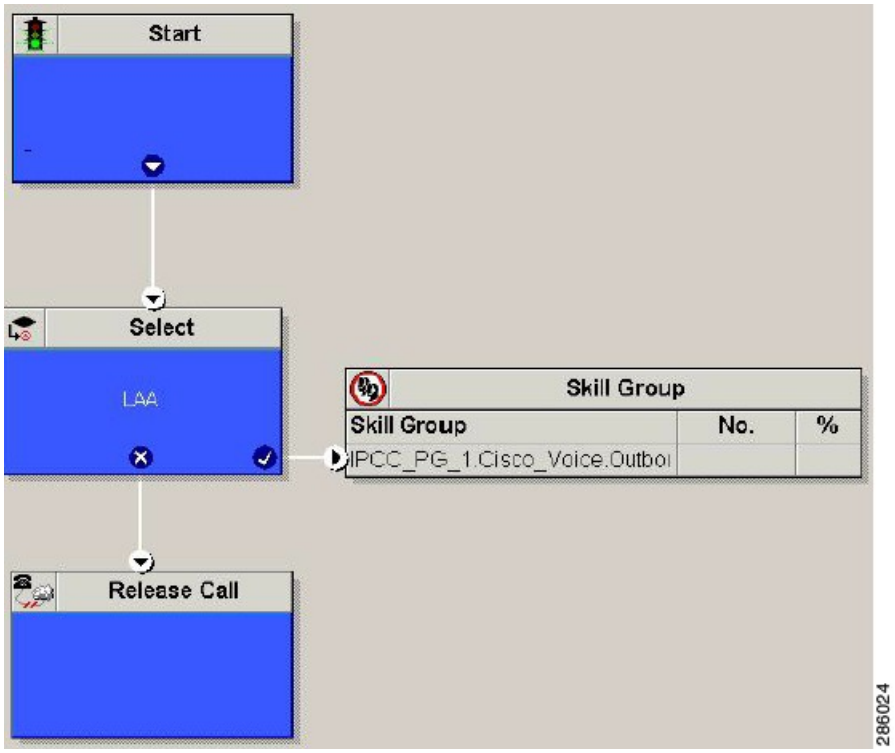
図 *17* : エージェントベースのキャンペーンのルーティングスクリプトの追加



詳細については、『アウトバウンド オプション ガイド』を参照してください。

IVR ベースのキャンペーンのルーティングスクリプトの追加

図 *18 : IVR* ベースのキャンペーンのルーティングスクリプトの追加



IVR ベースのキャンペーンに対して次を構成します。

手順

ステップ 1 構成マネージャツールから Network VRU Explorer ツールを開きます。ラベル（CVP コールサーバーで構成した DNIS 値に一致するラベル）をタイプ 10 の既存ネットワーク VRU に追加し、ドロップダウンリストで、メディアルーティングタイプに対して「アウトバウンド」を選択します。

ステップ 2 IVR ベースのキャンペーンを追加します。

次のタスク

- 連絡先インポートファイルの作成 （371 ページ）
- 電話禁止リストの作成 （371 ページ）

連絡先インポートファイルの作成

連絡先インポートファイルを作成する場合は、[インポートルールの定義（Import Rule Definition）] タブページで設定したデータベースルールに従って設計した形式に従ってください。

次の例では、AccountNumber、FirstName、LastName、およびPhone列タイプの連絡先情報があることを前提としています。

手順

ステップ1 テキストエディタを使用して、これらのフィールドの情報を含むテキストファイルを作成します。

ステップ2 新しい行の各エントリのアカウント番号、名、姓、電話番号を入力します。

[インポートルール一般（Import Rule General）] タブページで定義されているように、カンマ区切り、または固定形式のいずれかを使用します。

ステップ3 テキストファイルをローカルサーバーに保存します。

例

次に、カンマ区切り形式の連絡先インポートファイルの例を示します。

```
6782,Henry,Martin,2225554444
3456,Michele,Smith,2225559999
4569,Walker,Evans,2225552000
```

以下は、次の列定義を使用した固定形式の同じ例です。

- Custom - VARCHAR(4)
- FirstName - VARCHAR(10)
- LastName - VARCHAR(20)
- Phone - VARCHAR(20)

```
6782HenryMartin2225554444
3456MicheleSmith2225559999
4569WalkerEvans2225552000
```

電話禁止リストの作成

Do_Not_Call list ファイルの作成時は、以下の指示に従って正しくフォーマットします。

手順

ステップ 1 テキストエディタを使用して、電話禁止の電話番号をすべて含むテキストファイルを作成します。

ステップ 2 新しい回線の各電話禁止エントリに電話番号を入力します。

ステップ 3 電話禁止エントリごとに、次の特性を確認します。

- 各電話番号の最大長は 20 文字です。
-

ステップ 4 テキストファイルをローカルサーバーに保存します。

次に、電話禁止リストの例を示します。

```
2225554444

2225556666

2225559999
```

このリストをお客様に追加するには、電話禁止リストをインポートします。

キャンペーン マネージャは、電話禁止テーブルから読み取ります。Campaign Manager がダイヤリングリストのエントリをフェッチし、桁が完全に一致する場合のみ、ダイヤリングリストのエントリは、電話禁止エントリとしてマークされます。これにより、ダイヤリングリストを再構築せずにキャンペーンの実行中に電話禁止をインポートできます。

（注） ダイヤリングリストに基本電話番号と内線番号が含まれる場合、このエントリは、同じ基本電話番号と同じ内線番号の電話禁止エントリと一致する必要があります。ダイヤラは内線番号をダイヤルしません。

（注） [電話禁止（Do Not Call）]リストをクリアするには、[テーブルの上書き（Overwrite table）] オプションを有効にして空のファイルをインポートします。

周辺機器ゲートウェイの設定を使用した SIP ダイヤラのインストール

手順

ステップ 1 すべての ICM サービスを停止します。

ステップ 2 Unified CCE PG サイド A とサイド B で、周辺機器ゲートウェイ設定を実行します。**[スタート（Start）] > [すべてのプログラム（All programs）] > [Cisco Unified CCE ツール（Cisco Unified**

CCE Tools）] > **[周辺機器ゲートウェイの設定（Peripheral Gateway Setup）]** の順に選択します。

ステップ 3 **[Cisco Unified ICM/コンタクトセンターエンタープライズ&ホストコンポーネント設定（Cisco Unified ICM/Contact Center Enterprise & Hosted Components Setup）]** ダイアログボックスの**インスタンス**列の左側で、インスタンスを選択します。

ステップ 4 「**インスタンス**コンポーネント」セクションで、[追加 (Add)] をクリックします。

[ICMコンポーネントの選択（ICM Component Selection）] ダイアログボックスが開きます。

ステップ 5 **[アウトバウンドオプションダイヤラ（Outbound Option Dialer）]** をクリックします。

[アウトバウンドオプションダイヤラプロパティ（Outbound Option Dialer Properties）] ダイアログボックスが開きます。

ステップ 6 Unified ICM サポートプロバイダからの指定が特にない場合、**[生産モード（Production Mode）]** および **[システム起動時に自動起動（Auto start at system startup）]** をオンにします。 これらオプションにより ダイヤラサービス起動タイプが「自動」に設定され、マシン起動時にダイヤラも自動で起動します。

SIP（Session Initiation Protocol） ダイヤラタイプ は自動で選択されます。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 **[アウトバウンドオプションダイヤラプロパティ（Outbound Option Dialer Properties）]** ダイアログで、以下の情報を指定します。

- **アウトバウンド オプション サーバー** — Unified CCE のアウトバウンド オプション サーバーのホスト名または IP アドレス。このサーバーは通常、Outbound Option Campaign Manager（データサーバーのサイド A）が配置されているのと同じ VM です。
- **キャンペーン マネージャ サーバー A** ー キャンペーン マネージャ がデュプレックスとして設定されている場合、サイドA キャンペーンマネージャが配置されているマシンのホスト名または IP アドレスを入力します。キャンペーン マネージャがシンプレックスとして設定されている場合は、このフィールドと **[キャンペーンマネージャサーバーB（Campaign Manager server B）]** フィールドに同じホスト名または IP アドレスを入力します。このフィールドに値を入力する必要があります。
- **キャンペーン マネージャ サーバー B** ー キャンペーン マネージャ がデュプレックスとして設定されている場合、サイドB キャンペーンマネージャが配置されているマシンのホスト名または IP アドレスを入力します。キャンペーン マネージャがシンプレックスとして設定されている場合は、このフィールドと **[キャンペーンマネージャサーバーA（Campaign Manager server A）]** フィールドに同じホスト名または IP アドレスを入力します。このフィールドに値を入力する必要があります。
- **CTI サーバー A** — CTI サーバーサイド A の VM のホスト名または IP アドレス。これは、通常 PG が配置されている（コールサーバーサイド A）のと同じ VM です。
- **CTI サーバーポート A** — CTI サーバーサイド A へのインターフェイスを作成するためにダイヤラが使用するポート番号。デフォルトは、42027 です。CTI サーバーポートと CG 構成が一致していることを確認します。コールサーバーマシンから**診断フレームワーク**

ページを実行し、**[ListProcesses]** を選択して、CTI OS サーバーのポート番号を見つけます。

- **CTI サーバー B** — CTI サーバーサイド B の VM のホスト名または IP アドレス。
- **CTI サーバーポート B** — CTI サーバーサイド B へのインターフェイスを作成するためにダイヤラが使用するポート番号。デフォルトは、43027 です。
- **ハートビート** ー CTI サーバーへの接続のダイヤラチェック間隔（ミリ秒単位）。デフォルト値は 500 です。
- **メディアルーティングポート** ーダイヤラがメディアルーティング PG のメディアルーティング PIM へのインターフェイスを作成するために使用するポート番号。デフォルトは、38001 です。メディアルーティングポートが MR PG 構成のポートと一致していることを確認します。たとえば、`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\mango\PG3A\PG\CurrentVersion\PIMS\pim1\MRData\Config\ApplicationTcpServiceName1` のレジストリキーにアクセスできます。

ステップ 9 [次へ（Next）] をクリックします。**[Summary（概要）]** 画面が表示されます。

ステップ 10 **[次へ（Next）]** をクリックし、ダイヤラのインストールを開始します。

オプション ー AutoAnswer のダイヤラレジストリ値の編集

zip トーンを使用してCallManagerで自動応答を有効にした場合、ダイヤラで自動応答を無効にする必要があります。複数のダイヤラがある場合は、複数のダイヤラで自動応答を無効にする必要があります。zip トーンは、お客様が接続されようとしていることを示すためにエージェントの電話機に送信されるトーンです。

ダイヤラで自動応答を無効にするには、ダイヤラプロセスの初回実行後に、次のレジストリキーの値を 0 に変更します。

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\pra01\Dialer\AutoAnswerCall

ダイヤラレジストリ設定については、『*Unified Contact Center Enterprise* アウトバウンド オプション ガイド』を参照してください。

DNP ホストファイルの追加

DNP ホストファイルを追加するには、以下の手順を実行します。

手順

ステップ 1 ダイヤラがインストールされている仮想マシンの C ドライブで、\icm\customerInstanceName\Dialer ディレクトリに移動します。

ステップ 2 静的ルートマッピングの DNP ホストファイルを変更します。

静的ルートの形式は、ワイルドカードパターン、ダイヤラに接続するゲートウェイの IP アドレスまたはホスト名、説明です。

例：7????? (ダイヤルパターン)、10.86.227.144 (ゲートウェイ IP)、エージェントの内線番号にコール

（注） 各サブカスタマーダイヤラに対してこれらの手順を繰り返します。

アウトバウンド オプション エンタープライズ データ

[Cisco Agent Desktop エンタープライズデータ（Cisco Agent Desktop Enterprise Data）] ウィンドウにアウトバウンド オプション エンタープライズ データを表示するには、管理者は、デフォルトのレイアウトを編集して、一部またはすべてのアウトバウンドオプション変数を含める必要があります。これら変数の先頭には「BA」が付きます。（Cisco Desktop Administrator でデフォルトのエンタープライズ データ レイアウトを編集します）。

- BAAccountNumber
- BABuddyName
- BACampaign
- BADialedListID
- BAResponse
- BAStatus
- BATimeZone

（注） ECC 変数を有効にするには、「拡張コール変数の構成（233 ページ）」を参照してください。BAStatus フィールドは必須です。その他すべての BA フィールドは、Progressive および Predictive モードではオプションです。Preview モードの場合、BADialedListID が有効化されていなければ [スキップ（Skip）] ボタンは機能しません。

- 呼び出されるお客様の名前を表示する場合は、BABuddyName フィールドが必要です。
- 通話が、Preview dialing モードキャンペーンの一環である場合、BAStatus フィールドのエントリの初めの文字は、P となります。通話が Direct Preview dialing モードキャンペーンの一環である場合は、BAStatus フィールドのエントリの初めの文字は、D となります。

Unified Communications Manager の構成

正規化スクリプトを追加します

このスクリプトは、SIP コールのエージェントへの転送中にリングバックを無効にするために必要です。

手順

ステップ 1 **Unified Communications Manager Administration** ページにログインします。

ステップ 2 **[デバイス（Device）] > [デバイス設定（Device Settings）] > [SIP正規化スクリプト（SIP Normalization Script）]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。
SIP正規化スクリプトページを表示します。

ステップ 4 スクリプトの**名前**を入力します。

ステップ 5 **[コンテンツ（Content）]** フィールドに次のスクリプトを入力します。

```
M = {}
function M.outbound_180_INVITE(msg)
msg:setResponseCode(183, "Session in Progress")
end
return M
```

ステップ 6 残りのフィールドはデフォルト値のままにします。

ステップ 7 [保存（Save）] をクリックします。

アウトバウンドゲートウェイにトランクを構成

アウトバウンドゲートウェイにトランクを構成するには、「SIP トランクの追加 （291 ページ）」を参照してください。**[SIP情報（SIP info）]** タブを更新中：

手順

ステップ 1 **[アドレスIPv4（Address IPv4）]** フィールドにアウトバウンドゲートウェイの IP アドレスを入力します。

ステップ 2 ドロップダウンリストで、新しく追加した **[SIP正規化スクリプト（SIP Normalization Scripts）]** を選択します。

ポストコール調査の構成

ポストコール調査を構成するには、以下の手順を実行します。

- CVP でポストコール調査を構成 （376 ページ）
- 設定 Unified CCE （377 ページ）

CVP でポストコール調査を構成

Unified CVP でポストコール調査を構成するには、以下の手順を実行します。

Procedure

ステップ 1 Unified CVP オペレーションコンソールにログインし、**[システム（System）]** > **[ダイヤル番号パターン（Dialed Number Pattern）]** の順に選択します。

ステップ 2 着信ダイヤル番号を調査番号に関連付けるには、次の構成設定を入力します。

- **ｄ相やる番号パターン** ー 適切なダイヤル番号を入力します。

  ダイヤルしたポストコール調査に転送される電話の着信ダイヤル番号。これは、調査にリダイレクトするダイヤル番号です。

- **着信電話に対してポストコール調査を有効化** ー これを選択すると、着信電話に対してポストコール調査が有効化されます。
- **調査ダイヤル番号パターン** ー ポストコール調査のダイヤル番号を入力します。これは、通常のコールフロー完了後に、通話を転送するダイヤル番号となります。
- **[保存（Save）]** をクリックすると、ダイヤル番号パターンが保存されます。

ステップ 3 **[展開（Deploy）]** をクリックすると、Unified CVP コールサーバーデバイスの構成が展開されます。

設定 Unified CCE

ECC 変数の構成

ポストコール調査使用するために Unified CCE を構成する必要はありませんが、ECC 変数である **user.microapp.isPostCallSurvey** を使用して ICM スクリプト内で機能を無効化（または有効化）できます。 n または y の大文字小文字を区別する値を使用すると、機能を無効化または再度有効化できます。

ラベルノードの前、またはキューからスキルグループノードの前に ECC 変数を n または y に構成します。これにより、エージェントの転送前に Unified CVP に正しい値が送信されます。この ECC 変数は、ポストコール調査コールを開始するためには必要ありませんが、オペレーションコンソールを使用してポストコール調査を構成する場合は、この変数を使用して機能を制御できます。

DN がポストコール調査のオペレーションコンソールにマッピングされると、コールは自動的に構成済みのポストコール調査 DN に転送されます。

ポストコール調査を有効または無効にするには、以下の手順を実行します。

手順

ステップ 1 Unified CCE Administration Workstation で、構成マネージャを使用して、**[拡張コール変数リストツール（Expanded Call Variable List Tool）]** を選択します。

ステップ 2 **Name:user.microapp.isPostCallSurvey** という ECC 変数を作成します。

ステップ 3 **[最大長（Maximum Length）]** を 1 に設定します。

ステップ 4 **[有効化（Enabled）]** チェックボックスをオンにしたら、**[保存（Save）]** をクリックします。

a-Law コーデックの構成

a-law コーデックをサポートするには、シスコ HCS for CC コアコンポーネントで次の項目を構成します。

- ゲートウェイの構成 （378 ページ）
- Unified CVP の構成 （380 ページ）
- Unified Communication Manager の構成 （382 ページ）

ゲートウェイの構成

- イングレスゲートウェイの構成 （378 ページ）
- VXML ゲートウェイの構成 （379 ページ）

イングレスゲートウェイの構成

手順

ステップ 1 ダイヤルピアでコーデック設定を行うため、音声クラス コーデック 1 を追加します。

例：

```
voice class codec 1
     codec preference 1 g729r8
     codec preference 2 g711alaw
     codec preference 3 g711ulaw

dial-peer voice 70021 voip
     description Used for Switch leg SIP Direct
     preference 1
     max-conn 225
     destination-pattern xxxx..... # Customer specific destination
     session protocol sipv2
     session target ipv4:###.###.###.### # IP Address for Unified CVP
     session transport tcp
     voice class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad
```

ステップ 2 ダイヤルピアを変更し、ダイヤルピアに対しコーデックを明示的に指定します。

```
dial-peer voice 9 voip
     description For Outbound Call for Customer
     destination-pattern <Customer Phone Number Pattern>
     session protocol sipv2
     session target ipv4:<Customer SIP Cloud IP Address>
```

```
     session transport tcp
     voice-class sip rel1xx supported "100rel"
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 10 voip
     description ***To CUCM Agent Extension For Outbound***
     destination-pattern <Agent Extension Pattern to CUCM>
     session protocol sipv2
     session target ipv4:<CUCM IP Address>
     voice-class sip rel1xx supported "100rel"
     dtmf-relay rtp-nte
     codec g711alaw
```

VXML ゲートウェイの構成

手順

次のダイヤルピアを変更し、ダイヤルピアに対しコーデックを明示的に指定します。

```
dial-peer voice 919191 voip
     description Unified CVP SIP ringtone dial-peer
     service ringtone
     incoming called-number 9191T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 929292 voip
     description CVP SIP error dial-peer
     service cvperror
     incoming called-number 9292T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 7777 voip
     description Used for VRU leg #Configure VXML leg where the incoming called
     service bootstrap
     incoming called-number 7777T
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 5 voip
     description for SIP TTS Media Call
     preference 1
     session protocol sipv2
     session target ipv4: <ASR primary server IP>
     destination uri tts
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad
```

```
dial-peer voice 6 voip
     description for SIP ASR Media Call
     preference 1
     session protocol sipv2
     session target ipv4: <TTS primary server IP>
     destination uri asr
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 7 voip
     description for SIP TTS Media Call
     preference 2
     session protocol sipv2
     session target ipv4: <ASR secondary server IP>
     destination uri tts
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 8 voip
     description for SIP ASR Media Call
     preference 2
     session protocol sipv2
     session target ipv4: <TTS secondary server IP>
     destination uri asr
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad
```

Unified CVP の構成

Unified CVP では、OAMP での特定の構成は必要ありません。

次のファイルを A-law に変換する必要があります。

1. C:\inetpub\wwwroot\en-us\app
2. C:\inetpub\wwwroot\en-us\app\ag_gr
3. C:\inetpub\wwwroot\en-us\sys
4. OAMP サーバーの C:\Cisco\CVP\OPSConsoleServer\GWDownloads
5. C:\Cisco\CVP\VXMLServer\Tomcat\webapps\CVP\audio
6. C:\inetpub\wwwroot\en-us\VL（オプション。RSM のみに適用）

（注）

- OAMP サーバーでファイルを変換した後Unified CVP OAMP ページにアクセスして、新しく変換した A-law ファイルをゲートウェイにアップロードします。
- 以前にu-lawにゲートウェイを使用していた場合は、ゲートウェイを再起動してゲートウェイキャッシュ内の u-law ファイルを削除します。

μ-law オーディオファイルを a-law 形式に変換するには、以下の手順を実行します。

手順

ステップ 1 Unified CVP からローカルデスクトップに wav ファイルをコピーします。

ステップ 2 **[すべてのプログラム（All programs）]** > **[アクセサリ（Accessories）]** > **[エンターテイメント（Entertainment）]** の順に選択します。

ステップ 3 **[サウンドレコーダー（Sound Recorder）]** を開きます。

ステップ 4 **[ファイル（File）]** を選択して、**[開く（Open）]** をクリックします。

ステップ 5 μ-law オーディオファイルを参照し、**[開く（Open）]** をクリックします。

ステップ 6 **[プロパティ（Properties）]** に移動します。

ステップ 7 **[今すぐ変換（Convert Now）]** をクリックします。

ステップ 8 **[形式（Format）]** から **[CCITT A-Law]** を選択します。

ステップ 9 [OK] をクリックします。

ステップ 10 **[ファイル（Files）]** > **[名前を付けて保存（Save As）]** の順に選択し、ファイル名を指定します。

ステップ 11 新しい a-law 形式のファイルをメディアサーバーの以下のディレクトリにコピーします。

```
C:\inetpub\wwwroot\en-us\app
```

エージェントグリーティングとサービス コールバックに録音を有効化

エージェントグリーティングとサービス コールバックの録音を有効にするには、以下の手順を実行します。

手順

ステップ 1 Call Studio を開き、コールバック エントリ アプリケーションに移動します。

ステップ 2 **app.callflow** ダブルクリックします。

ステップ 3 **[レコード名（Record Name）]** 要素の設定に移動し、[ファイルタイプ（File Type）] を **[その他（Other）]** に変更します（デフォルトは wav）。

ステップ 4 MIME タイプを **audio/x-alaw-basic** に設定します。

ステップ 5 ファイル拡張子を **wav** に設定します

ステップ 6 **RecordAgentGreeting** アプリケーションを開き、**app.callflow** をダブルクリックします。

ステップ 7 **[確認してグリーティングを録音（Record Greeting with Confirm）]** 要素設定に移動し、[ファイルタイプ（File Type）] を **[その他（Other）]** に変更します（デフォルトは wav）。

ステップ 8 MIME タイプを **audio/x-alaw-basic** に設定します。

ステップ 9 ファイル拡張子を **wav** に設定します。

ステップ 10 アプリケーションを検証、保存、および展開します。

ステップ 11 Unified CVP サービスを再起動します。

Unified Communication Manager の構成

Cisco Unified Communications Manager を介して a-Law をプロビジョニングするには、以下の手順を実行します。

手順

ステップ 1 **Cisco Unified Communication Manager Administration** ページにログインします。

ステップ 2 **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

ステップ 3 **[サーバー（Server）]** ドロップダウンリストでパブリッシャサーバーを選択します。

ステップ 4 **[サービス（Service）]** ドロップダウンリストで **[Cisco CallManager（アクティブ）（Cisco CallManager (Active)）]** を選択します。

ステップ 5 **[ClusterWideパラメータ（システムーロケーションおよびリージョン）ClusterWide Parameters (System - Location and region)）]** の **[G.711 A-law コーデックの有効化（G.711 A-law Codec Enabled）]** ドロップダウンリストで **[すべてのデバイスを有効化（Enabled for All Devices）]** を選択します。

ステップ 6 次のドロップダウンリストで **[無効化（Disable）]** を選択します。

- **G.711 μ-law コーデックの有効化**
- **G722 Codec 対応**
- **iLBC コーデックの有効化**
- **iSAC コーデックの有効化**

ステップ 7 [保存（Save）] をクリックします。

Unified CM ベース サイレント モニタリングの構成

Unified CM ベースのサイレントモニタリングを構成するには、以下の手順を実行します。

- 組み込みブリッジを有効または無効にします。参照 組み込みブリッジの有効化または無効化 （310 ページ）
- デバイス用モニタリング コーリング サーチ スペースの追加

モニタリング用コーリングサーチスペースの追加

始める前に

エージェントの電話が追加されていることを確認します。

（注） CTIOS サーバーのインストール時に、**IPCC サイレントモニタタイプ**として **[CCM ベース（CCM Based）]** を選択します。

手順

ステップ 1 プロバイダ、リセラー、またはカスタマーとして Unified Communication Domain Manager にログインします。

ステップ 2 モニタリングのためにコーリングサーチスペースを追加します。

ステップ 3 **[回線（Lines）]** を編集したら、ドロップダウンリストで、新しく追加した **コーリングサーチスペース** を選択します。

ステップ 4 [保存（Save）] をクリックします。

例

このセクションで一覧されているタスクの実行方法に関する詳細は、https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-and-configuration-guides-list.html で記載されている『*Cisco Hosted Collaboration Solution Contact Center* 構成ガイド』、を参照してください。

保留音の構成

Unified Communication Manager の構成

Unified Communications Manager Music On Hold（MoH）サーバーではオーディオファイルまたは固定ソースから MoH ストリームを生成できます。オーディオファイルまたは固定ソースのいずれでも unicast または multicast として送信できます。

MoH サーバーは 2 つのモードで展開できます。

1. CM クラスタ内のユーザーが 1250 人未満の HCS for CC 展開用の同じサーバ上の UnifiedCM と連動。
2. CM クラスタ内のユーザーが 1250 人以上の HCS for CC 展開用のスタンドアロンノード（TFTP/MoH サーバー）として。

保留音サーバーオーディオソースの構成

手順

ステップ 1 **Cisco Unified Communications Manager Administration** ページにログインします。

ステップ 2 **[メディアリソース（Media Resources）]** > **[保留音オーディオソース（Music On Hold Audio Source）]** の順に選択します。

ステップ 3 デフォルトのサンプルオーディオソースを保持します。

ステップ 4 ドロップダウンリストで **[最初のアナウンス（Initial Announcement）]** を選択します（オプション）。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 新規オーディオソースを作成するには、以下の手順を実行します。

a) [新規追加（Add New）] をクリックします。
b) ドロップダウンリストで MOH オーディオストリーム番号を選択します。
c) ドロップダウンリストで MOH オーディオソースファイルを選択します。
d) MOH ソース名を入力します。
e) ドロップダウンリストで、**[最初のアナウンス（Initial Announcement）]** を選択します。
f) [保存（Save）] をクリックします。

保留音用サービスパラメータの設定

手順

ステップ 1 **Cisco Unified Communications Manager Administration** ページにログインします。

ステップ 2 **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

ステップ 3 ドロップダウンリストで、MoH サーバーを選択します。

ステップ 4 ドロップダウンリストで、**[Cisco IP音声メディアストリーミングアプリサービス（Cisco IP Voice Media Streaming App Service）]** を選択します。

ステップ 5 **[対応MOHコーデック（Supported MOH Codecs）]** フィールドで、必要なコーデックを選択し、**[OK]** をクリックします。

ステップ 6 [保存（Save）] をクリックします。

保留音用電話機構成の設定

手順

ステップ 1 **Cisco Unified Communications Manager Administration** ページにログインします。

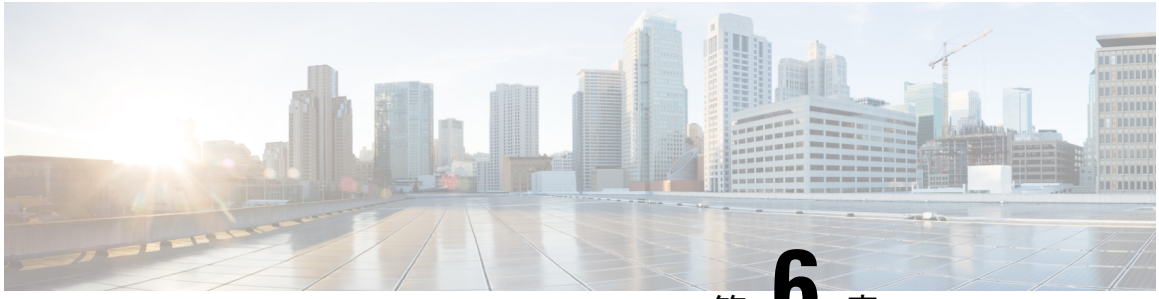
ステップ 2 **[デバイス（Device）]** > **[電話機（Phone）]** の順に選択します。

ステップ 3 MOH を構成する電話機を選択します。

ステップ 4 **[ユーザー保留MOHオーディオソース（User Hold MOH Audio Source）]** ドロップダウンリストでオーディオソースを選択します。

ステップ 5 **[ネットワーク保留MOHオーディオソース（Network Hold MOH Audio Source）]** ドロップダウンリストでオーディオソースを選択します。

ステップ 6 **[保存（Save）]** > **[適用（Apply）]** の順にクリックして電話機をリセットします。



第 6 章

オプションのシスココンポーネントのインストールと構成

SPAN ベースのサイレントモニタリング

SPAN ベースのサイレントモニタリングのインストール

手順

ステップ 1 Cisco Unified CCE CTI ISO イメージをマウントします。

ステップ 2 `setup.exe` ファイルを実行して、SPAN ベースのサイレントモニタリングにインストールします。

ステップ 3 **CTIOS サイレント モニタリング サービス**ページで、**[はい（Yes）]** をクリックし、CTIOS サイレント モニター プロセスを停止します。

ステップ 4 ソフトウェアライセンス契約書を承諾し、**[続行（Continue）]** をクリックします。

ステップ 5 MR パッチの参照場所を入力し、**[次へ（Next）]** をクリックします。

MR パッチの参照場所がわからない場合は、フィールドを空白のままにして **[次へ（Next）]** をクリックします。

ステップ 6 **接続先場所の選択**ページで、インストールするディレクトリを参照し、**[次へ（Next）]** をクリックします。

ステップ 7 **[Cisco CTIOSサイレントモニター - InstallShield ウィザード（Cisco CTIOS Silent Monitor - Install Shield Wizard）]** ウィンドウで、以下の手順を実行します。

a) **[ホスト名/IP アドレス（Hostname\IP Address）]** フィールドで、サイレントモニターサーバーのホスト名を入力します。

b) **[ポート（Port）]** フィールドで、サイレントモニターサービスが着信接続をリッスンするポート番号 **42228** を入力します。

c) **[サイレントモニターサーバー（Silent Monitor Server）]**チェックボックスをオンにすると、サイレントモニターサービスは、複数のモバイルエージェントを同時に監視できるようになります。

d) ピア情報を入力します。このサイレントモニターサービスがサイレントモニターサービスのクラスタの一部である場合に選択します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 **CTIOSサイレントモニター**ページで **[セキュリティを有効化（Enable Security）]** チェックボックスをオフにし、**[OK]** をクリックします。

ステップ 10 **[完了（Finish）]** をクリックします。

SPAN ベースのサイレントモニタリングの構成

ゲートウェイからの SPAN の構成

ここでは、モバイルエージェント展開に必要な追加構成に関して説明します。

1. モバイルエージェントの場合、音声パスは公衆電話交換網（PSTN）と 2 つのゲートウェイを通過します。

   1 つのゲートウェイはお客様の電話機からの通話を制御します。もう 1 つのゲートウェイは、エージェントゲートウェイと呼ばれるエージェントからの通話を制御します。

   モバイルエージェントでは、サイレントモニターサービスは SPAN ポートを使用して、エージェントゲートウェイを通過する音声トラフィックを受信します。これには、サイレントモニターサービスを実行するコンピュータに、クライアントとの通信を処理する NIC カードと、スイッチからスパンされるすべてのトラフィックを受信する NIC カードの 2 つの NIC カードが必要です。

   たとえば、エージェントゲートウェイがポート 1 に接続されていて、SPAN トラフィックを受信するサイレントモニターサーバーの NIC がポート 10 に接続されている場合は、以下のコマンドを使用して SPAN セッションを構成します。

```
monitor session 1 source interface fastEthernet0/1

monitor session 1 destination interface fastEthernet0/10
```

2. モバイルエージェント用サイレントモニタリングを展開するには、エージェントトラフィック用と発信者トラフィック用の 2 つのゲートウェイが必要です。

   エージェントと発信者トラフィックにひとつのゲートウェイを使用する場合、音声トラフィックはゲートウェイから出ず、通過しないので、サイレントモードで監視できなくなります。

   たとえば、エージェント間およびモバイルエージェント間の電話相談は、同じゲートウェイを共有するので、サイレントモードで監視できません。ほとんどのモバイルエージェント展開では、エージェントとお客様間の通話のサイレントモニタリングのみ許可されます。

3. スーパーバイザデスクトップにサイレントモニターサービスをインストールしますが、モバイルエージェントにサイレントモニターサービスを構成する必要はありません。1 つ以上のサイレントモニターサービスを使用するようにCTI OS サーバー設定プログラムでエージェントを構成する必要があります。

4. モバイルエージェントと通常のエージェントの両方であるエージェントには、少なくとも 2 つのプロファイルが必要です。

   通常のエージェントのプロファイルには、サイレントモニターサービス情報は含まれません。

   モバイルエージェントのプロファイルには、サイレントモニターサービスの接続に使用する情報が含まれます。

サイレント モニタ サービス クラスタ

1 つ以上のエージェントゲートウェイがコールセンターに存在する場合で、エージェントがいずれかのゲートウェイを使用してログインできる場合、以下のようにサイレントモニターをサポートするようにサイレントモニターサービスをクラスタ化します。

1. 各ゲートウェイには個別のサイレントモニターサーバーを展開します。
2. 前の項の説明に従って、それぞれのサイレントモニターサーバーに、SPAN ポートを構成します。
3. サイレント モニター サーバー インストーラを実行して、ピアとしてサイレントモニターサーバーをインストールし、構成します。
4. 以下を構成して、接続プロファイルを設定し、エージェントデスクトップにそのピアのひとつを接続するように指示します。
   1. [ピア情報の入力（Enter peers information）] チェックボックスをオンにします。
   2. ホスト名/IP アドレスに別のサイレントモニターサービスの IP アドレスを入力します。

CallManager から SPAN を構成

この導入モデルでは Cisco Unified Communications Manager ソフトウェアリソースが使用されているため、小規模エージェントのコンタクトセンターには CallManager からのスパンを使用します。

始める前に

Cisco Unified Communications Manager からスパンするには、SM サーバーが Cisco Unified Communications Manager と同じブレード上にある必要があります。エージェントがゲートウェイを介して電話機にログインする際、Cisco Unified Communications Manager が独自の mtp リソースを使用することを確認します。

これには、サイレントモニタ サービスを実行しているコンピュータが 2 つの NIC カードを持つ必要があります。一方はクライアントとの通信を処理し、もう一方はNexusからスパンされるすべてのトラフィックを受信するものです。

手順

Nexus で LOCAL SPAN セッションを構成するには、次のコマンドを使用します。

```
monitor session 1
description LOCAL-SPAN
source interface Vethernet76 both
```

上記では、Vethernet76 は、スイッチ上の Cisco Unified Communications Manager のインターフェイスとなります。

Cisco RSM

Cisco Remote Silent Monitoring 用ゴールデンテンプレートの作成

Cisco RSM サーバーのゴールデンテンプレートを作成するには、この一連のタスクを実行します。

各タスクの後で、このページに戻ってそのタスクを「「完了」」としてマークしたら、次の手順に進みます。

順序	完了したか	タスク	注意事項
1		UCCE_11.6_Win2012_vmv9_v1.0.ova のダウンロード	OVA ファイルのダウンロード（392 ページ）を参照してください。
2		Cisco RSM サーバーの仮想マシンを作成します。	仮想マシンの作成（392 ページ）の手順を実行します。
3		Microsoft Windows Server のインストール	Microsoft Windows Server のインストール（393 ページ）の手順を実行します。
5		ウイルス対策ソフトウェアをインストールします。	ウイルス対策ソフトウェアのインストール（28 ページ）の手順を実行します。
6		JTAPI クライアントをインストールします。	JTAPI クライアントのインストール（395 ページ）の手順を実行します。
7		Cisco RSM の SNMP トラップの構成	Cisco RSM 用 SNMP トラップの構成（396 ページ）の手順を実行します。
8		Cisco RSM サーバーをインストールします。	Cisco RSM サーバーのインストール（396 ページ）の手順を実行します。
9		仮想マシンをテンプレートに変換します。	仮想マシンをゴールデンテンプレートに変換（397 ページ）の手順を実行します。

すべてのゴールデンテンプレートの作成後、自動化プロセス（自動化クローニングと OS のカスタマイズ（2 ページ））を実行できます。自動化プロセスを実行後、接続先システムで Cisco RSM サーバーを構成できます。「Cisco RSM の構成（398 ページ）」を参照してください。

OVA ファイルのダウンロード

ゴールデンテンプレートには、オープン仮想化フォーマットファイル（OVA）が必要です。Cisco HCS for Contact Center は作成された対応する VM の基本構造を定義する OVA を使用します。構造定義には、CPU、RAM、ディスク容量、CPU の予約、およびメモリーの予約が含まれます。

（注） VM とソフトウェアコンポーネントは、Cisco HCS for Contact Center に対して最適化されます。Cisco HCS for Contact Center 用の OVA を保持する必要があります。

始める前に

Cisco.com プロファイルに関連付ける有効なサービス契約が必要です。

手順

ステップ 1 Cisco.com で、*Hosted Collaboration Solution for Contact Center* > ソフトウェアのダウンロードページの順に選択します。

ステップ 2 必要なソフトウェアタイプを選択します。

ステップ 3 **[ダウンロード（Download）]** をクリックして、ローカルドライブに OVA ファイルを保存します。VM を作成する場合は、アプリケーションに必要な OVA を選択します。

仮想マシンの作成

手順

ステップ 1 VMware vSphere クライアントを起動し、**[ファイル（File）]** > **[OVF テンプレートの展開（Deploy OVF Template）]** の順に選択します。

ステップ 2 ローカルドライブ上で OVA が保存されている場所を参照します。**[開く（Open）]** をクリックして、OVA ファイルを選択したら、**[次へ（Next）]** をクリックします。

ステップ 3 **OVF テンプレートの詳細**ページで、**[次へ（Next）]** をクリックします。

ステップ 4 **名前と場所**ページの **[名前（Name）]** フィールドに仮想マシンの名前を入力し、**[次へ（Next）]** をクリックします。

（注） 入力できる最大文字数は、32 文字までで、特殊文字は入力できません。

ステップ 5 **展開の構成**ページのドロップダウンリストで適切な構成を選択したら、**[次へ（Next）]** をクリックします。

ステップ 6 **リソースプール**ページで、必要なリソースプールを選択し、**[次へ（Next）]** をクリックします。

（注） ホストサーバーにリソースプールが割り当てられていない場合は、この手順を省略します。

ステップ 7 **ストレージ**ページで、新しい仮想マシンに展開するデータストアを選択し、**[次へ（Next）]** をクリックします。

ステップ 8 **ディスクのフォーマット**ページで、**[Thick provisioned Lazy Zeroed]** を選択し、**[次へ（Next）]** をクリックします。

（注） シンプロビジョニングフォーマットはテンプレートの作成プロセスで使用されます。実稼働での使用はサポートされていません。

ステップ 9 **ネットワークマッピング**ページの **[接続先ネットワーク（Destination Network）]** ドロップダウンリストで適切なネットワークを選択し、**[次へ（Next）]** をクリックします。

（注） Unified Contact Center Enterprise マシンについては、**ネットワークマッピング**ページが正しいか確認してください。

- 公共ネットワークから表示ネットワーク
- プライベートネットワークからプライベートネットワーク

ステップ 10 **[完了（Finish）]** をクリックします。

Microsoft Windows Server のインストール

手順

ステップ 1 Microsoft Windows Server ISO イメージを仮想マシンにマウントします。

ステップ 2 仮想マシンのスイッチをオンにします。

ステップ 3 **[言語（Language）]**、**[時刻と通貨の形式（Time and Currency Format）]**、および **[キーボード設定（Keyboard settings）]** を入力し、**[次へ（Next）]** をクリックします。

ステップ 4 **[今すぐインストール（Install Now）]** をクリックします。

ステップ 5 製品アクティベーションキーを入力し、**[次へ（Next）]** をクリックします。

ステップ 6 インストールする Windows Server を選択し、**[次へ（Next）]** をクリックします。

ステップ 7 使用許諾契約に同意して、**[次へ（Next）]** をクリックします。

ステップ 8 **[カスタム：Windowsのみをインストール（詳細）（Custom: Install Windows Only (Advanced)）]** を選択し、**[次へ（Next）]** をクリックします。
インストールが開始されます。

ステップ 9 管理者用パスワードを入力して確認したら、**[完了（Finish）]** をクリックします。

ステップ 10 VMware ツールをインストールするには、関連項目を参照してください。

ステップ 11 **[リモートデスクトップ接続（Remote Desktop Connection）]** を有効にするには、以下の手順を実行します。

a) **[スタート（Start）]** > **[コントロール パネル（Control Panel）]** > **[システムとセキュリティ（System and Security）]** の順に選択します。
b) **[リモートアクセスを許可（Allow remote access）]** > **[OK]** の順に選択します。
c) **[リモートデスクトップの任意のバージョンが実行されているコンピュータからの接続を許可（Allow connections from computers running any version of Remote Desktop）]** を選択し、**[適用（Apply）]** をクリックします。
d) [OK] をクリックします。

ステップ 12 **ネットワークと共有センター**を開き、**[イーサネット（Ethernet）]** を選択します。

ステップ 13 **[イーサネットステータス（Ethernet Status）]** ダイアログボックスで、ネットワーク設定とドメインネームシステム（DNS）データを構成します。

a) [プロパティ（Properties）] を選択します。**[インターネットプロトコルバージョン6（TCP/IPV6）（Internet Protocol Version 6 (TCP/IPV6)）]** をオフにします。
b) **[インターネットプロトコルバージョン4（TCP/IPv4）（Internet Protocol Version 4 (TCP/IPv4)）]** を選択し **[プロパティ（Properties）]**をクリックします。
c) **[次のIPアドレスを使用する（Use the following IP Address）]** オプションを選択します。
d) IP アドレス、サブネットマスク、およびデフォルトゲートウェイを入力します。
e) **[次のDNSサーバーアドレスを使用する（Use the following DNS Server Address）]** オプションを選択します。
f) **優先する DNS サーバー** アドレスを入力して、**[OK]** をクリックします。

（注） すべてのネットワーク構成が新しい設定で上書きされます。

ステップ 14 Microsoft Windows アップデートを実行します。

アップデートが完了したら、**[自動更新を有効にしない（Do not enable automatic updates）]** をオンにします。

Windows 用 VMware ツールのインストール

この手順は、ゴールデンテンプレートおよび直接インストールの両方のオプションに対して実行します。

CC アプリケーションの HCS for CC の動作とパフォーマンスを保証するには、VMware ツールをインストールし、VMware vSphere ホストを最新の状態にする必要があります。

手順

ステップ 1 vSphere Client で、仮想マシンを右クリックし、**[電源（Power）]** を選択して、**[電源を投入（Power On）]** をクリックします。

ステップ 2 [サマリー（Summary）] タブをクリックします。

[全般（General）] セクションの [VMwareツール（VMware Tools）] フィールドは、VMware ツールが次のいずれであるかを示します。

- インストール済みおよび最新
- インストール済みで最新ではない
- 未インストール

ステップ 3 **[コンソール（Console）]** タブをクリックし、ゲスト オペレーティング システムが正常に起動していることを確認します。プロンプトが表示されたらログインします。

ステップ 4 仮想マシンを右クリックし、**[ゲストOS（Guest OS）]** > **[VMwareツールのインストール/アップグレード（Install/Upgrade VMware Tools）]** の順に選択します。**[VMware ツールのインストール/アップグレード（Install/Upgrade VMware Tools）]** ウィンドウが表示され、[インタラクティブツールのアップグレード（Interactive Tools Upgrade）] および [自動ツールのアップグレード（Automatic Tools Upgrade）] オプションが表示されます。

a) VMwareツールを手動でインストールまたはアップグレードするには、**[インタラクティブツールのアップグレード（Interactive Tools Upgrade）]** オプションを選択し、**[OK]** をクリックします。画面の指示に従って VMware ツールをインストールまたはアップグレードし、プロンプトが表示されたら仮想マシンを再起動します。

b) VMware ツールを自動的にインストールまたはアップグレードするには、**[自動ツールのアップグレード（Automatic Tools Upgrade）]** オプションを選択し、**[OK]** をクリックします。このプロセスは完了までに数分かかり、プロンプトが表示されたら仮想マシンを再起動します。

JTAPI クライアントのインストール

Cisco RSM サーバーに JTAPI をインストールするには、以下の手順を実行します。

手順

ステップ 1 ブラウザで、**Unified Communications Manager Administration** アプリケーションを起動します。

ステップ 2 管理者のログイン情報を使用してログインします。

ステップ 3 **[アプリケーション（Application）]**> **[プラグイン（Plugins）]** > **[検索（Find）]** の順に選択します。

ステップ 4 Windows 向けの Cisco JTAPI 32-bit Client をダウンロードします。

ステップ 5 ダウンロードしたファイルをインストールし、すべてをデフォルト設定のままにします。

（注）
- **[Cisco TFTP IP アドレス（Cisco TFTP IP Address）]** テキストボックスに、Cisco Unified Communications Manager Subscriber の IP アドレスを入力します。
- Small Contact Center エージェント導入モデルでは、RSM を複数のサブカスタマー Cisco Unified Communications Manager クラスタに接続する必要があるため、これはオプションです。

Cisco RSM サーバーのインストール

Cisco RSM サーバーをインストールするには、以下の手順を実行します。

手順

ステップ 1 Cisco RSM ISO イメージを仮想マシンにマウントします。詳細については、ISO ファイルのマウントおよびアンマウント （581 ページ）を参照してください。

ステップ 2 setup.exe ファイルを実行して RSM サーバーをインストールします。
RSM インストーラプログラムが起動し、Cisco Remote Silent Monitoring（RSM）InstallShield ウィンドウが表示されます。

ステップ 3 [次へ（Next）] をクリックします。
ライセンス同意ページが表示されます。

ステップ 4 ライセンス同意ページで、ライセンスに同意します。[次へ（Next）] をクリックします。

ステップ 5 サービスログイン情報ページで、RSM 仮想マシンの管理者ログイン情報を入力します。[次へ（Next）] をクリックします。

ステップ 6 構成設定の起動ページの設定から **[終了（Exit）]** をクリックします。ポップアップウィンドウで **[はい（Yes）]** をクリックします。

ステップ 7 **[完了（Finish）]** をクリックします。

次のタスク

RSM の構成 （400 ページ）

Cisco RSM 用 SNMP トラップの構成

Simple Network Management Protocol（SNMP）トラップは、選択したイベントを SNMP モニターに送信するように Windows を構成することで、Cisco RSM から発生する場合があります。これは、evntwin.exe という Windows ユーティリティを使用して実現されます。このユーティリティは、Windows イベントログに書き込まれたイベントを SNMP トラップに変換します。このトラップは Windows SNMP サービスによって発生し、SNMP 管理ツールに転送されます。

Cisco RSM を使用するために SNMP トラップを構成するには、以下の手順を実行します。

- トラップ転送用 SNMP サービスの構成 （397 ページ）

• MIB での SNMP エージェントの構成 （397 ページ）

トラップ転送用 SNMP サービスの構成

レポートおよびアラートに使用される管理ツールにトラップを転送するようにSNMPサービスを構成します。

手順

ステップ 1 MMCコンソールで、**[ファイル（Files）]>[スナップインの追加/削除...（Add/Remove Snap-in...）]** の順に選択します。

ステップ 2 **[使用可能なスナップイン（Available Snap-ins）]** リストから **[サービス（Services）]** を選択し、**[追加（Add）]** をクリックします。

ステップ 3 **[サービス（Services）]** ダイアログボックスで **[ローカルコンピュータ（Local Computer）]** を選択して、**[完了（Finish）]** をクリックします。

ステップ 4 [OK] をクリックします。
サービス（ローカル）ノードが**コンソールルート**ノードに追加されます。

ステップ 5 **[サービス（ローカル）（Services（Local））]** を選択し、表示される **[サービス（ローカル）（Services（Local））]** タブで、**[SNMPサービス（SNMP Services）]** を右クリックし、**[プロパティ（Properties）]** を選択します。
[SNMPサービスプロパティ（SNMP Service Properties）] ダイアログボックスが表示されます。

ステップ 6 **[トラップ（Traps）]** タブの **[コミュニティ名（Community Name）]** フィールドに **`public`** と入力し、**[リストに追加（Add to list）]** をクリックします。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 **[SNMPサービスの構成（SNMP Service Configuration）]** ダイアログボックスで、トラップ情報を受信するシステムのホスト名または IP アドレスを入力します。これは、管理エージェントまたはレポーティングおよびアラートツールをホストするサーバーです。**[追加（Add）]** をクリックして、トラップ接続先を追加します。

ステップ 9 複数のシステムがある場合は、トラップ情報を受信する必要があり、すべてのシステムでトラップ転送用の SNMP サービスを構成します。

ステップ 10 [OK] をクリックします。

MIB での SNMP エージェントの構成

次の情報は、RSM SNMP エージェントを接続し、MIB オブジェクトをルート化するためのものです。

- **RSM SNMP エージェント接続**： < *RSM Server IP* >:33161
- **RSM SNMP エージェントルート OID**： .1.3.6.1.4.1.9.9.2776 - ciscoRSMMIB

仮想マシンをゴールデンテンプレートに変換

ゴールデンテンプレート インストール オプションに対してこの手順を実行します。

（注） VMwareでは、テンプレートという用語を使用します。Contact Center 用 HCS では、Contact Center用HCSに使用されるアプリケーションとオペレーティングシステムで構成されるテンプレートにゴールデンテンプレートという用語を使用します。

始める前に

Windows ベースのテンプレート仮想マシンが WORKGROUP にあることを確認します。

手順

ステップ 1 VM の電源がオフになっていない場合は、**[VM]** メニューから、**[電源（Power）]** > **[ゲストをシャットダウン（Shut down the guest）]** の順に選択します。

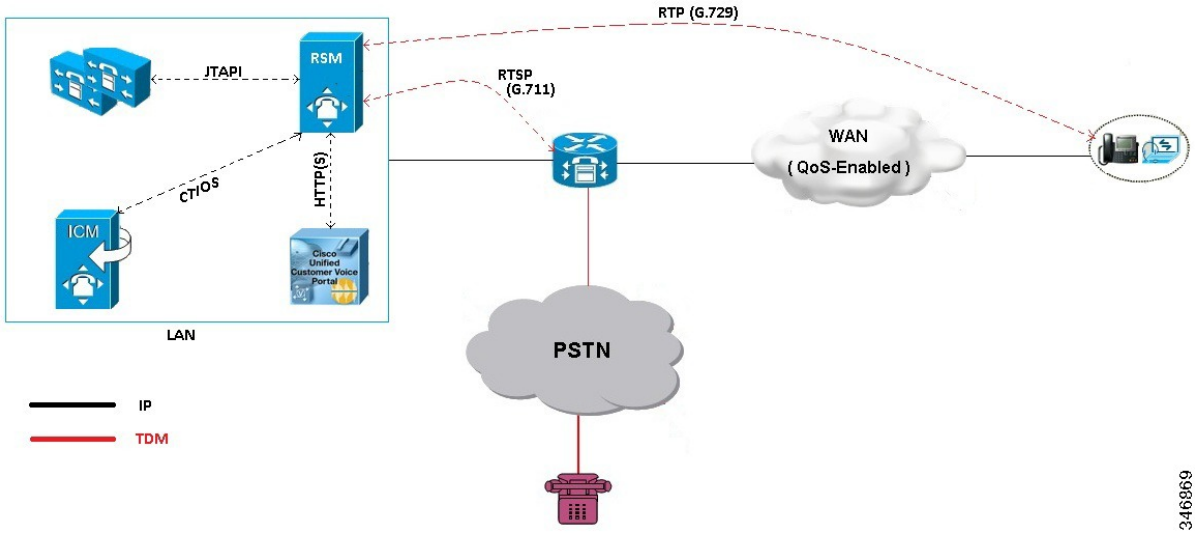
ステップ 2 [VMware vCenterインベントリ（VMware vCenter Inventory）] メニューで、仮想マシンを右クリックし、**[テンプレート（Template）]** > **[テンプレートに変換（Convert to Template）]** の順に選択します。

Cisco RSM の構成

- 2000 エージェント展開用 Cisco RSM の構成 （399 ページ）
- 4000 エージェント展開用 Cisco RSM の構成 （410 ページ）
- Small Contact Center 展開用 Cisco RSM の構成 （415 ページ）
- 12000 エージェント展開用 Cisco RSM の構成 （414 ページ）
- A-Law コーデック用 Cisco RSM の構成 （419 ページ）

次の図に、Remote Silent Monitoring 構成トポロジを示します。

図 *19 : Cisco Remote Silent Monitoring* 構成トポロジ



2000 エージェント展開用 Cisco RSM の構成

2000 エージェント展開に対する Cisco RSM（リモート サイレント モニタリング）サーバーを分散モードで構成するには、以下の手順を実行します。

ソフトウェア要件	タスク
RSM の構成	2000 エージェント展開用 RSM構成設定の設定（400 ページ）
	JTAPI クライアント優先設定の構成 （403 ページ）
	レジストリ設定の編集 （403 ページ）
ゲートウェイの構成	VXML ゲートウェイの構成 （403 ページ）
Unified CVP の構成	RSM プロンプトのアップロード （404 ページ）
	CVP コールフローの統合 （404 ページ）
	コールフローの展開 （406 ページ）
Unified CCE の構成	エージェント ターゲット ルールの設定 （407 ページ）
	スーパーバイザ ログイン アカウントの作成 （408 ページ）
	RSM 用ルーティングスクリプトの作成 （408 ページ）

ソフトウェア要件	タスク
Unified CallManager の構成	シミュレーションする電話機の構成（409ページ）
	ログインプール Simphone の設定 （410 ページ）
	RSM アプリケーションユーザーの作成 （549 ページ）

RSM の構成

2000 エージェント展開用 *RSM*構成設定の設定

手順

ステップ 1 メールサーバー構成設定を完了するには、以下を実行します。

a) **[スタート（Start）]** > **[CiscoRSM]** > **[RSM構成マネージャ（RSM Configuration Manager）]** の順に選択します。

b) **[Eメールアラートの送信（Send Email Alert）]** チェックボックスをオンにします。

c) **[メールサーバーのホスト名/IP（Mail Server Host Name/IP）]** テキストボックスに、メールサーバーのホスト名/IPアドレスを入力します。

d) **[ポート（Port）]** テキストボックスに、E メールポート番号を入力します。

e) **[送信者のEメールアドレス（Sender Email Address）]** テキストボックスに送信者の E メール ID を入力します。

f) **[受信者のEメールアドレス（Receiver Email Address）]** テキストボックスに受信者の E メール ID を入力します。

g) [次へ（Next）] をクリックします。

ステップ 2 その他の構成設定を完了するには、以下を実行します。

a) **[問題の通話の最短期間（Problem Call Minimum Duration）]** テキストボックスに **1800** と入力します。

b) **[問題の通話の最短保留（Problem Call Min Holds）]** テキストボックスに **4** と入力します。

c) **[古い通話の最長期間（Max Stale Call Duration）]** テキストボックスに **3600**と入力します。

d) **[CTI OSトレースマスク（CTI OS TraceMask）]** の値を空欄にします。

e) VL エンジンの **[ログレベル（Log Level）]** ドロップダウンリストで、**[INFO]** を選択します。

f) VL エンジンの **[HTTPリッスンポート（HTTP Listen Port）]** テキストボックスに **8080** と入力します。

g) PhoneSim の **[VRUへのオーディオバッファ長（Audio Buffer Len To VRU）]** テキストボックスに **480** と入力します。

（注） VRUへのオーディオバッファ長のデフォルト値は160です。CVP環境の場合、値は480に設定されます。

h) PhoneSimの **[ログレベル（Log Level）]** ドロップダウンリストで **[INFO]** を選択します。
i) PhoneSimの **[HTTPリッスンポート（HTTP Listen Port）]** テキストボックスに **29001** と入力します。
j) PhoneSimの **[RTSPリッスンポート（RTSP Listen Port）]** テキストボックスに **29554** と入力します。
k) Phonesimの **[オーディオエンコーディング（Audio Encoding）]** ドロップダウンリストで、**[RTSP u-law]** を選択します。
l) PhoneSimの **[HTTPチャンク化転送の実行（Do HTTP Chunked Transfers）]** ドロップダウンリストで **[いいえ（No）]** を選択します。
m) **[ホストデータIP（Host Data IP）]** テキストボックスでRSMサーバーのIPアドレスを入力します。
n) [次へ（Next）] をクリックします。

ステップ3 クラスタ構成設定を定義します。

これらの設定は、RSMが監視するエージェントで各Unified Communications Managerクラスタを構成するために使用されます。

a) **[クラスタの追加（Add Cluster）]** をクリックします。
b) **[ClusterN_Name]** テキストボックスに、クラスタ名を入力します。

（注） 名前は英数字にする必要があります。

c) **[Simphonesへのログインプール数（No. of Login Pool Simphones）]** テキストボックスに **5** と入力します。
d) **[監視電話数（No. of Monitoring Phones）]** テキストボックスに **60** と入力します。（これは、同時に60の電話を監視します）。
e) **[周辺機器ID（[Peripheral ID）]** テキストボックスに **5000** と入力します。
f) **[JTAPIユーザー名（JTAPI Username）]** テキストボックスにrsmuserと入力します。
g) **[JTAPI パスワード（JTAPI Password）]** テキストボックスにrsmuserパスワードを入力します。
h) **[MAC範囲の開始（Start MAC Range）]** テキストボックスに、simphoneデバイス名のMAC範囲の自動生成に使用する最初のMACアドレスを入力します。
i) **[回線番号範囲の開始（Start Line Num Range）]** テキストボックスに、simphone DNの回線内線番号範囲の自動生成に使用する最初の内線番号を入力します。

（注） **1.** 回線内線番号範囲はクラスタ間で重複してはなりません。ClusterN_PhoneSim_StartMACRange値に関連付けられます。
2. [開始回線番号範囲（Start Line Num Range）] は4ー15桁にする必要があります。

j) **[SIP転送（SIP Transport）]** ドロップダウンリストで **[TCP]** を選択します。
k) [次へ（Next）] をクリックします。

ステップ 4 Unified Communications Manager 構成設定を定義するには以下を実行します。

a) **[ホスト名/IP（Host Name/IP）]** テキストボックスに CUCM1 サーバー（Subscriber1）のホスト名/IP アドレスを入力します。

b) **[ポート（Port）]** テキストボックスで CUCM1 ポートに対して **5060** と入力します。

c) **[ホスト名/IP（Host Name/IP）]** テキストボックスに CUCM2 サーバー（Subscriber2）のホスト名/IP アドレスを入力します。

d) **[ポート（Port）]** テキストボックスで CUCM2 ポートに対して **5060** と入力します。

e) [次へ（Next）] をクリックします。

ステップ 5 UCCE 統合ページで、[UCCEとCTIOSを統合（UCCE integrate with CTIOS）] または [UCCEとCTIを統合（UCCE integrate with CTI）] を選択します。

a) [UCCEとCTIOSを統合（UCCE integrate with CTIOS）] を選択した場合は、以下の手順を実行します。

1. **[CTIOS 1Aホスト名/IP（CTIOS 1A Hostname/IP）]** テキストボックスに CTIOS 1A のホスト名/IP アドレスを入力します。
2. **[CTIOS 1Aポート（CTIOS 1A Port）]** テキストボックスに、**42028** と入力します。
3. **[CTIOS 1Bホスト名/IP（CTIOS 1B Hostname/IP）]** テキストボックスに、CTIOS 1B のホスト名/IP アドレスを入力します。」
4. **[CTIOS 1Bポート（CTIOS 1A Port）]** テキストボックスに、**42028** と入力します。
5. [次へ（Next）] をクリックします。

a) [UCCEとCTIを統合（UCCE integrate with CTI）] を選択した場合は、以下の手順を実行します。

1. **[CTIOS 1Aホスト名/IP（CTIOS 1A Hostname/IP）]** テキストボックスに CTI 1A のホスト名/IP アドレスを入力します。
2. **[CTI 1Aポート（CTI 1A Port）]** テキストボックスに、**42027** と入力します。
3. **[CTIOS 1Bホスト名/IP（CTIOS 1B Hostname/IP）]** テキストボックスに CTI 1B のホスト名/IP アドレスを入力します。
4. **[CTI 1Bポート（CTI 1B Port）]** テキストボックスに、**43027** と入力します。
5. [次へ（Next）] をクリックします。

ステップ 6 **[次へ（Next）]** をクリックし、**[PhoneSimサービスの起動（Start PhoneSim Service）]** と **[VLEngineサービスの起動（Start VLEngine Service）]** チェックボックスをオンにします。

ステップ 7 **[完了（Finish）]** をクリックします。

JTAPI クライアント優先設定の構成

手順

ステップ 1 **[スタート（Start）]** > **[すべてのプログラム（All Programs）]** > **[Cisco JTAPI]** の順に選択し、**[Cisco Unified Communications Manager JTAPI 優先設定（Cisco Unified Communications Manager JTAPI Preferences）]** をクリックします。

ステップ 2 **[言語（Language）]** タブをクリックします。

ステップ 3 [言語の設定（Select Language）] ドロップダウンロストで、**[英語（English）]** を選択します。

ステップ 4 **TFTP サーバーの IP アドレス**を入力します。

ステップ 5 [OK] をクリックします。

レジストリ設定の編集

RSM では、ユーザーが電話でログインできるように、数値のスーパーバイザアカウントが必要です。ただし、Unified CCE スーパーバイザ エージェント アカウントは Active Directory ユーザーアカウントでもあり、Active Directory セキュリティポリシーは数字のみのアカウントを防止できます。この問題を解決するには、「VLEngine_PassPrefix」パラメータを変更します。

手順

ステップ 1 **[スタート（Start）]** > **[実行（Run）]** > **[Regedit]** の順に選択し、Registry Editor にアクセスします。

ステップ 2 **[HKEY_Local_Machine]** > **[ソフトウェア（Software）]** > **[Wow6432Node]** > **[Cisco Systems, Inc.]** > **[Remote Silent Monitoring]** の順に選択します。

ステップ 3 **VLEngine_PassPrefix** CTI OS 検証のために送信する前にパスワードを付加する文字列を設定します。

たとえば、「"VLEngine_PassPrefix」文字列が **RSM1RSM** に設定されており、スーパーバイザが、**1234** の PIN でログインする場合は、スーパーバイザのパスワードは、**RSM1RSM1234** に設定されます。

（注） 有効な値は、文字、数字、および有効なパスワード記号の文字列です（空白文字と制御文字は使用できません）。

ゲートウェイの構成

VXML ゲートウェイの構成

RSM は、CVP をサポートする Cisco IOS の VXML ゲートウェイモデルおよびバージョンでサポートされます。イングレス/VXML ゲートウェイは、 RSM と他の機能間で共有できます。

RSM に対して VXML ゲートウェイを設定するには、 **ivr prompt memory 8000** コマンドを発行して、IVR プロンプトメモリーが 8 Mb以上であることを確認します。

（注） ゲートウェイが他の機能とともに RSM と共有されている場合、ゲートウェイのパフォーマンスは 20% 低下します。

Unified CVP の構成

RSM プロンプトのアップロード

手順

ステップ 1 C:\inetpub\wwwroot\en-us\ でメディアサーバーディレクトリに移動し、VL という名前の新規ディレクトを作成します。

ステップ 2 RSM サーバーに移動し、C:\ CiscoRSM\callflows から prompts.zip をコピーし、コンテンツをメディアサーバーの VL ディレクトリに解凍します。

ステップ 3 VL ディレクトリを右クリックし、**[プロパティ（[Properties）]** をクリックします。

ステップ 4 [セキュリティ（Security）] タブの **[詳細（Advanced）]** で **[権限の変更（Change Permission）]** をクリックします。

ステップ 5 **[オブジェクトの親からの継承可能な権限を含める（Include inheritable privilege from object's parent）]** と **[すべての子オブジェクトの権限をこのオブジェクトからの継承可能な権限で置き換える（Replace all child object permission with inheritable permissions from this object）]** をチェックボックスをオンにします。

ステップ 6 **[OK]** をクリックし、Windows セキュリティ ポップアップウィンドウで **[はい（Yes）]** をクリックします。

ステップ 7 Web ブラウザを開き、メディアサーバーの VL ディレクトリ（ http://<SERVER IP>/en-us/VL）に移動します。プロンプトファイルがリストされ、アクセス可能であることを確認します。

CVP コールフローの統合

手順

ステップ 1 RSM サーバーで、C:\CiscoRSM\callflows\vxml-cvp フォルダに移動します。

ステップ 2 フォルダ内のすべてのコンテンツを Cisco Unified Call Studio ソフトウェアをホストしているデスクトップマシンからアクセスできるディレクトリ（C:\RSM-Callflow など）にコピーします。

ステップ 3 Call Studio を起動します。メニューバーで、**[ファイル（File）]** > **[インポート（Import）]** > **[Call Studio]** > **[既存のCall Studioプロジェクト（Existing Call Studio Project）]** の順に選択し、RSM プロジェクトをワークスペースにインポートしたら、**[次へ（Next）]** をクリックします。

ステップ 4 vxml-cvp フォルダを参照し、**[完了（Finish）]** をクリックします。

ステップ 5 RSM プロジェクトの [コールフローエディタナビゲータ（Callflow Editor Navigator）] ペインの **DoLogin** ページに移動します。

ステップ 6 SetBaseSessionVars 要素を選択したら、**[要素の構成（Element Configuration）]** 配下の **[データ（Data）]** をクリックします。

ステップ 7 RSM プロジェクトの **VoiceXML 変数設定**を以下のように変更します。

（注） 以下の変数設定を修正後は、必ず**[更新（Update）]**をクリックしてください。クリックしないと、フィールドにデフォルト値が入力されます。

- **VL_VLENGINE_HOSTNAME** — VLEngine サービスで実行されるサーバーのホスト名または IP アドレス。
- **VL_VLENGINE_PORT** — VLEngine サービスが使用するポート番号。ポート値は 8080 です。
- **VL_PHONESIM_HOSTNAME** — PhoneSim サービスで実行するサーバーのホスト名または IP アドレス。値は VL_VLENGINE_HOSTNAME と同じ値です。
- **VL_PHONESIM_RTSP_PORT** — PhoneSim サービスで使用する RTSP ポート番号。通常は 29554 です。
- **VL_PHONESIM_HTTP_PORT** — PhoneSim サービスで使用する HTTP ポート番号。通常は 29001 です。
- **MAX_NUM_LOGIN_ATTEMPTS**— RSM がユーザーを切断するまでに許可するログイン試行最大失敗回数。
- **CVP_MEDIASVR_AUDIO_PATH** — RSM プロンプトがアップロードされる URL パスを指します（たとえば /en-us/VL）。

  （注） このパスと RSM CVP プロジェクトの **[オーディオ設定ーデフォルトオーディオパスURL（Audio Settings - Default Audio Path URL）]** テキストフィールドで指定されたパスコンポーネントは同一である必要があります。

- **CVP_MEDIASVR_HOSTNAME** — /en-us/VL ディレクトリにある RSM プロンプトが表示される CVP メディアサーバーのホスト名または IP アドレス。
- **MAIN_MENU_TIMEOUT** — 秒単位の時間。これは通常 12 秒です。
- **CVP_VXMLSVR_HOSTNAME** — VXML サーバーで実行するサーバーのホスト名または IP アドレス。
- **CVP_VXMLSVR_PORT** —VXML サーバーで使用するポート番号。
- **CVP_MEDIASVR_PORT** — メディアサーバードメインのポート番号。通常は、ポート 80 です。
- **MONITOR_NEWEST_REPOLL_PERIOD** — 新規エージェントの会話を開始する前の秒単位の時間。この値は通常 4 秒に設定されます。

- **MONITOR_NEWEST_PROMPT_TO_END_EVERYN** — 進行プロンプトが発信者に通知されるまでのポーリング回数（つまり、「システムがまだビジーです。任意のキーを押して、メインメニューに戻るかこのまま保留にします。」）。通常、この値は3に設定されます。
- **SUPERVISOR_LOGIN_TIMEOUT** — スーパーバイザログインのタイムアウト。通常、この値は 1500 に設定されます。

ステップ 8 **[保存（Save）]** をクリックし、RSM プロジェクトを保存します。

ステップ 9 [ナビゲータ（Navigator）] ペインで **[RSMプロジェクト（RSM Project）]** を右クリックし、**[プロパティ（Properties）]** をクリックします。

ステップ 10 **[Call Studio]** で、**[オーディオ設定（Audio Settings）]** をクリックします。

ステップ 11 [デフォルトオーディオパスURI（Default Audio Path URI）] テキストフィールドで、`http://<cvp_media_server_IP_address>/en-us/VL` などのメディアサーバー上の VL ディレクトリを入力します。[OK] をクリックします。

ステップ 12 上記の手順を繰り返して、展開内の各 CVP サーバーの RSM プロジェクトを作成します。

（注） Small Contact Center 展開に関しては。手順 1 ～ 11 ｍでを繰り返し、ＣＶＰ サーバーの各サブカスタマーに対して一意の RSM プロジェクトを作成します。

コールフローの展開

コールフロースクリプトを CVP サーバーにインストールしたら、CVP VXML サーバーで使用するために展開する必要があります。

コールフロースクリプトを展開する手順を実行します。

（注） 適切な CVP_VXMLSVR_HOSTNAME を使用して、すべての CVP ボックスに VXML スクリプトを展開します。

手順

ステップ 1 Cisco Unified Call Studio を開きます。

ステップ 2 ナビゲータペインで **[RSMプロジェクト（RSM Project）]** を右クリックし、**[展開（Deploy）]** をクリックします。

ステップ 3 **[アーカイブファイル（Archive File）]** ラジオボタンを選択します。

ステップ 4 VXML アプリケーションファイルを保存する場所を参照します。

ステップ 5 [完了（Finish）] をクリックします。コールフロースクリプトは、指定した場所に保存されます。

ステップ 6 CVP OAMP ポータルを開きます。

ステップ 7 **[一括管理（Bulk Administration）]** > **[ファイル転送（File Transfer）]** > **[VXMLアプリケーション（VXML application）]** の順に選択します。

ステップ 8 **[使用可能（Available）]** から **[選択済み（Selected）]** まで目的の CVP VXML サーバーを選択し、手順 4 で保存した VXML アプリケーションファイルを参照します。

ステップ 9 **[転送（Transfer）]** をクリックし、**[ファイル転送ステータス（File Transfer Status）]** をクリックしてステータスを確認します。

ステップ 10 SCC-CVP-SVR-A サーバーに移動し、CVP コールサーバーの C:\Cisco\CVP\VXMLServer\applications\RSM\admin ディレクトリに移動したら、**deployApp.bat** ファイルをダブルクリックします。バッチファイルは、別の DOS ウィンドウで実行されます。

ステップ 11 アプリケーションを展開するよう求められた場合は、「はい」の意味である **Y** と入力します。これで、CVP VXML サーバーからコールフロースクリプトにアクセスできます。

ステップ 12 VXML ゲートウェイで適切なマイクロアプリケーション（VXML ゲートウェイダイヤルピア、Unified Communication Manager ルートパターンなど）を構成して、スクリプトにアクセスできるようにします。

Unified CCE の構成

エージェント ターゲット ルールの設定

（注） Unified CCE の 1 日目の構成に内線番号の範囲が含まれている場合は、この手順を省略します。

手順

ステップ 1 Administration Workstation（AW）で、**[スタート（Start）]** > **[すべてのプログラム（All Programs）]** > **[構成マネージャ（Configuration Manager）]** の順に選択します。

ステップ 2 **[ツール（Tools）]** > **[ツールを一覧（List Tools）]** の順に展開します。**[エージェントターゲティングルール（Agent Targeting Rule）]** をダブルクリックします。

ステップ 3 **[取得（Retrieve）]** をクリックして、環境内の既存のすべてのエージェント ターゲット リストを返します。

ステップ 4 既存のエージェント ターゲティング ルールを強調表示します。内線番号の範囲で **[追加（Add）]** をクリックします。空白の内線番号の範囲セクションが表示されます。

ステップ 5 内線番号の範囲（DN）を追加し、**[OK]** をクリックします。

ステップ 6 [保存（Save）] をクリックします。

（注） 4000 展開では、Cisco Unified Communications Manager アプリケーションユーザーに基づいて構成された、Cisco Unified Communications Manager PG が 2 つあります。ATR は Cisco Unified Communications Manager PG に基づいて構成されます。したがって、2 つの ATR がロードベース構成の一部として事前構成されており、アプリケーションユーザーに基づいて内線番号を ATR に追加する必要があります。

スーパーバイザ ログイン アカウントの作成

現在の CTI OS スーパーバイザ/エージェントアカウントに従って、RSM を使用するスーパーバイザごとに新しいアカウントを作成する必要があります。CTI OS 認証を使用する場合は、ダイヤルインスーパーバイザがシステムにログインできるように、Unified CCE 環境で別のスーパーバイザ エージェント アカウントを作成する必要があります。

スーパーバイザ ログイン アカウントを作成するには、エージェントの作成 （216 ページ） の手順に従います。

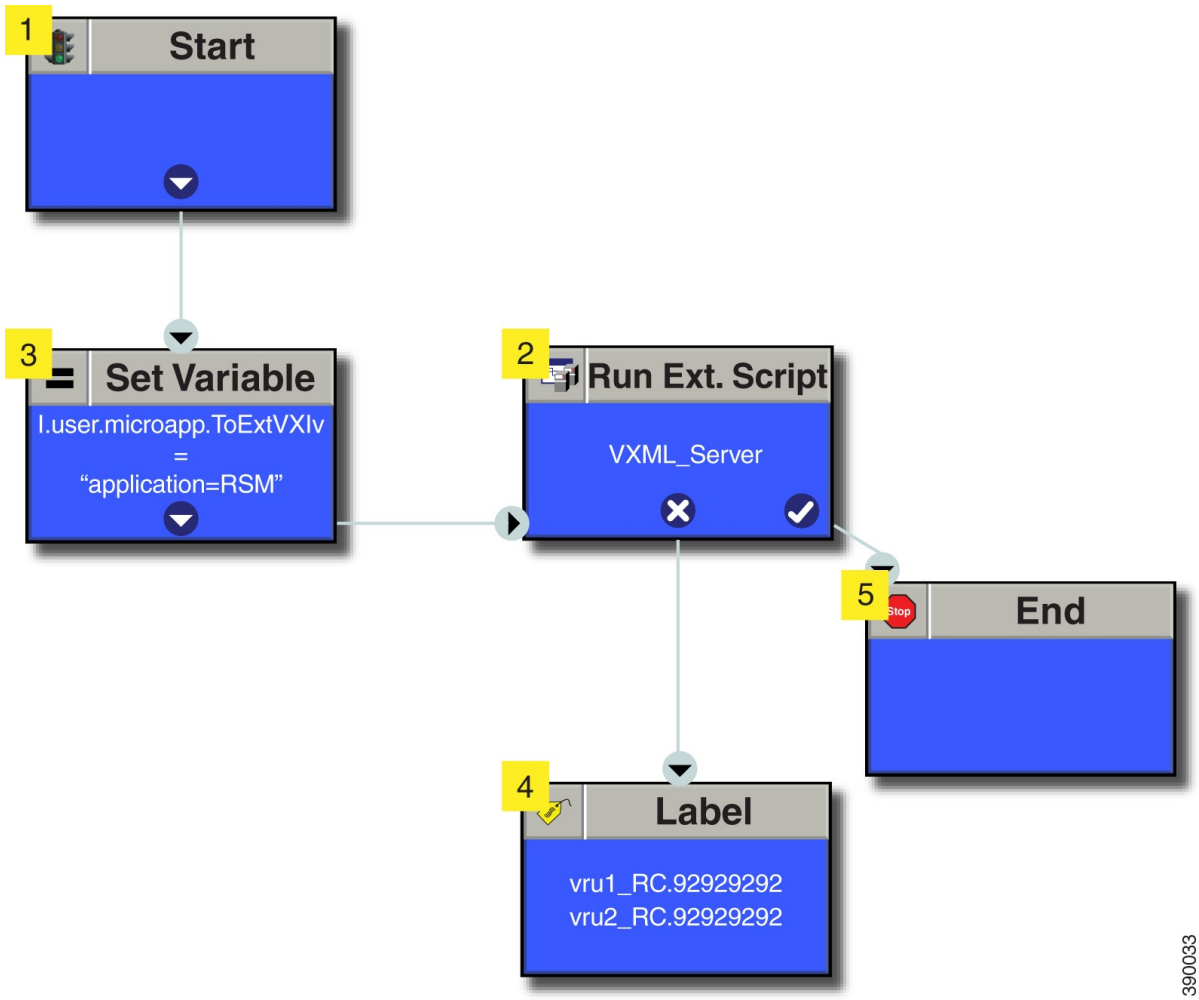
（注）

1. [スーパーバイザ（Supervisor）]チェックボックスをオンにして、スーパーバイザパスワードが AD パスワードポリシーを満たしていることを確認します。
2. エージェントパスワードが任意の長さの数字であることを確認します。
3. スーパーバイザがチームリストに追加されていることを確認します。

RSM 用ルーティングスクリプトの作成

Cisco RSM には、次のルーティングスクリプトが使用されます。

図 *20 : Cisco RSM* に使用されるルーティングスクリプト



Unified Communication Manager の構成

シミュレーションする電話機の構成

始める前に

各 Unified Communications Manager クラスタに割り当てるシミュレートされた電話機（simphone とも呼ばれる）の数を決定する必要があります。各クラスタには、クラスタの RSM を介して同時に監視されるエージェントの最大数以上の simphone が必要です。ここでは、次の情報を提供します。

- Simphone デバイスの依存関係の構成
- Simphone デバイスの作成

RSM に新規クラスタを追加するには、以下の手順を実行します。

Simphone デバイスの依存関係の作成

次の手順を実行して、Simphone デバイスの依存関係を作成します。

- Cisco Unified CM グループの構成 （299 ページ）
- リージョンの追加 （305 ページ）
- デバイスプールの追加 （299 ページ）

Simphone デバイスの作成

Simphone デバイスを作成するには、以下の手順を実行します。

- 電話機の追加 （303 ページ）
- 組み込みブリッジの無効化については、「組み込みブリッジの有効化または無効化 （310 ページ）」を参照してください。

ログインプール *Simphone* の設定

各クラスタに作成された最初の 5 つの simphone デバイスは VLEngine のログイン プールに自動で割り当てられます。VLEngine の認証メカニズムをサポートするために発信者が RSM で認証されると、ログイン プールは CTI OS にログイン テストを実行します。CTI OS のログインは、これらの simphone デバイスで実行されるため、それぞれの Unified Communications Manager クラスタの pguser アカウントに関連付ける必要があります。また、Cisco Unified Intelligent Contact Management Enterprise デバイスターゲットが作成されている必要があります。

次のタスク

- RSM アプリケーションユーザーの作成 （549 ページ）
- 最初の 5 台の電話機をアプリケーションユーザに関連付けます。「アプリケーションユーザーへの電話の関連付け （308 ページ）」を参照してください。

を選択します。

4000 エージェント展開用 Cisco RSM の構成

4000 エージェント展開に対する Cisco RSM（リモート サイレント モニタリング）サーバーを分散モードで構成するには、以下の手順を実行します。

ソフトウェア要件	タスク
RSM の構成	4000 および12000 エージェント展開用 RSM 構成設定の設定 （411 ページ）
	JTAPI クライアント優先設定の構成 （403 ページ）
	レジストリ設定の編集 （403 ページ）

ソフトウェア要件	タスク
ゲートウェイの構成	VXML ゲートウェイの構成 （403 ページ）
Unified CVP の構成	RSMプロンプトのアップロード（404ページ）
	CVP コールフローの統合 （404 ページ）
	コールフローの展開 （406 ページ）
Unified CCE の構成	エージェント ターゲット ルールの設定 （407 ページ）
	スーパーバイザ ログイン アカウントの作成 （408 ページ）
	RSM 用ルーティングスクリプトの作成 （408 ページ）
Unified CallManager の構成	シミュレーションする電話機の構成（409ページ）
	ログインプール Simphone の設定 （410 ページ）
	RSM アプリケーションユーザーの作成 （549 ページ）

4000 および12000 エージェント展開用 RSM 構成設定の設定

手順

ステップ 1 メールサーバー構成設定を完了するには、以下を実行します。

a) **[スタート（Start）]** > **[CiscoRSM]** > **[RSM構成マネージャ（RSM Configuration Manager）]** の順に選択します。

b) **[Eメールアラートの送信（Send Email Alert）]** チェックボックスをオンにします。

c) **[メールサーバーのホスト名/IP（Mail Server Host Name/IP）]** テキストボックスに、メールサーバーのホスト名/IPアドレスを入力します。

d) **[ポート（Port）]** テキストボックスに、E メールポート番号を入力します。

e) **[送信者のEメールアドレス（Sender Email Address）]** テキストボックスに送信者の E メール ID を入力します。

f) **[受信者のEメールアドレス（Receiver Email Address）]** テキストボックスに受信者の E メール ID を入力します。

g) [次へ（Next）] をクリックします。

ステップ 2 その他の構成設定を完了するには、以下を実行します。

a) **[問題のコールの最短期間（Problem Call Minimum Duration）]** テキストボックスに **1800** と入力します。
b) **[問題のコールの最短保留（Problem Call Min Holds）]** テキストボックスに **4** と入力します。
c) **[古いコールの最長期間（Max Stale Call Duration）]** テキストボックスに **3600** と入力します。
d) **[CTI OSトレースマスク（CTI OS TraceMask）]** の値を空欄にします。
e) VL エンジンの **[ログレベル（Log Level）]** ドロップダウンリストから **[INFO]** を選択します。
f) VL エンジンの **[HTTPリスニングポート（HTTP Listen Port）]** テキストボックスに **8080** と入力します。
g) PhoneSim の **[VRUへのオーディオバッファ長（Audio Buffer Len To VRU）]** テキストボックスに **480** と入力します。

（注） VRUへのオーディオバッファ長のデフォルト値は 160 です。CVP 環境の場合、値は 480 に設定されます。

h) PhoneSim の **[ログレベル（Log Level）]** ドロップダウンリストから **[INFO]** を選択します。
i) PhoneSim の **[HTTPリッスンポート（HTTP Listen Port）]** テキストボックスに **29001** と入力します。
j) PhoneSim の **[RTSPリッスンポート（RTSP Listen Port）]** テキストボックスに **29001** と入力します。
k) [Phonesim] ドロップダウンリストで、**RTSP u-law** に対して、**[オーディオエンコーディング（Audio Encoding）]** を選択します。
l) PhoneSim の **[HTTPチャンク化転送の実行（Do HTTP Chunked Transfers）]** ドロップダウンリストで **[いいえ（No）]** を選択します。
m) **[ホストデータIP（Host Data IP）]** テキストボックスで RSM サーバーの IP アドレスを入力します。
n) [次へ（Next）] をクリックします。

ステップ 3 最初のクラスタ構成設定を定義します。

これらの設定は、RSM がモニターするエージェントで Unified Communications Manager クラスタを構成するために使用されます。

a) **[クラスタの追加（Add Cluster）]** をクリックします。
b) **[ClusterN_Name]** テキストボックスにクラスタ名を入力します。

（注） 名前は英数字にする必要があります。

c) **[Simphonesへのログインプール数（No. of Login Pool Simphones）]** テキストボックスに **5**と入力します。
d) **[監視電話数（No. of Monitoring Phones）]** テキストボックスに **60** と入力します。（これは、同時に 60 の電話を監視します）。
e) **[周辺機器ID（[Peripheral ID）]** テキストボックスに **5000** と入力します。

f) **[JTAPIユーザー名（JTAPI Username）]** テキストボックスに **rsmuser1** と入力します。
g) **[JTAPIパスワード（JTAPI Password）]** テキストボックスに、rsmuser1 のパスワードを入力します。
h) **[MAC範囲の開始（Start MAC Range）]** テキストボックスに、simphone デバイス名の MAC 範囲の自動生成に使用する最初の MAC アドレスを入力します。
i) **[回線番号範囲の開始（Start Line Num Range）]** テキストボックスに、simphone DN の回線内線番号範囲の自動生成に使用する最初の内線番号を入力します。

（注） **1.** 回線内線番号範囲はクラスタ間で重複してはなりません。ClusterN_PhoneSim_StartMACRange 値に関連付けられます。
2. [開始回線番号範囲（Start Line Num Range）] は 4 ー 15 桁にする必要があります。

j) **[SIP転送（SIP Transport）]** ドロップダウンリストから **[TCP]** を選択します。
k) [次へ（Next）] をクリックします。

ステップ 4 最初のクラスタの Unified Communications Manager 構成設定を定義します。

a) **[ホスト名/IP（Host Name/IP）]** テキストボックスに CUCM1 サーバー（Subscriber1）のホスト名/IP アドレスを入力します。
b) **[ポート（Port）]** テキストボックスで CUCM1 ポートに対して **5060** と入力します。
c) **[ホスト名/IP（Host Name/IP）]** テキストボックスに CUCM2 サーバー（Subscriber 2）のホスト名/IP アドレスを入力します。
d) **[ポート（Port）]** テキストボックスで CUCM2 ポートに対して **5060** と入力します。
e) [次へ（Next）] をクリックします。

ステップ 5 UCCE 統合ページで、[UCCEとCTIの統合（UCCEate with CTI）]を選択します。

a) **[CTI 1Aホスト名/IP（CTI 1A Host Name/IP）]** に CTI 1A のホスト名/IP アドレスを入力します。
b) **[CTI 1Aポート（CTI 1A Port）]** テキストボックスに **42027** と入力します。
c) **[CTI 1Bホスト名/IP（CTI 1B Host Name/IP）]** に CTI 1B のホスト名/IP アドレスを入力します。
d) **[CTI 1Bポート（CTI 1B Port）]** テキストボックスに **43027** と入力します。
e) [次へ（Next）] をクリックします。

ステップ 6 2 番目のクラスタ構成設定を定義します。

これらの設定は、RSM がモニターするエージェントで Unified Communications Manager クラスタを構成するために使用されます。

a) **[クラスタの追加（Add Cluster）]** をクリックします。
b) **[ClusterN_Name]** テキストボックスにクラスタ名を入力します。

（注） 名前は英数字にする必要があります。

c) **[Simphonesへのログインプール数（No. of Login Pool Simphones）]** テキストボックスに **5**と入力します。

d) **[監視電話数（No. of Monitoring Phones）]** テキストボックスに **60** と入力します。（これは、同時に 60 の電話を監視します）。
e) **[周辺機器ID（[Peripheral ID）]** テキストボックスに **5001** と入力します。
f) **[JTAPIユーザー名（JTAPI Username）]** テキストボックスに **rsmuser2** と入力します。
g) **[JTAPIパスワード（JTAPI Password）]** テキストボックスに、rsmuser2 のパスワードを入力します。
h) **[MAC範囲の開始（Start MAC Range）]** テキストボックスに、simphone デバイス名の MAC 範囲の自動生成に使用する最初の MAC アドレスを入力します。
i) **[回線番号範囲の開始（Start Line Num Range）]** テキストボックスに、simphone DN の回線内線番号範囲の自動生成に使用する最初の内線番号を入力します。

（注） **1.** 回線内線番号範囲はクラスタ間で重複してはなりません。ClusterN_PhoneSim_StartMACRange 値に関連付けられます。
2. [開始回線番号範囲（Start Line Num Range）] は 4 ー 6 桁です。

j) **[SIP転送（SIP Transport）]** ドロップダウンリストから **[TCP]** を選択します。
k) [次へ（Next）] をクリックします。

ステップ 7 UCCE 統合ページで、**[UCCEとCTIの統合（UCCEate with CTI）]** を選択します。

a) **[CTI 1Aホスト名/IP（CTI 1A Host Name/IP）]** に CG 2A のホスト名/IP アドレスを入力します。
b) **[CTI 1Aポート（CTI 1A Port）]** テキストボックスに **42027** と入力します。
c) **[CTI 1Bホスト名/IP（CTI 1B Host Name/IP）]** に CG 2B のホスト名/IP アドレスを入力します。
d) **[CTI 1Bポート（CTI 1B Port）]** テキストボックスに **43027** と入力します。
e) [次へ（Next）] をクリックします。

ステップ 8 **[PhoneSimサービスの起動（Start PhoneSim Service）]** と **[VLEngineサービスの起動（Start VLEngine Service）]** チェックボックスをオンにします。

ステップ 9 [完了（Finish）] をクリックします。

（注） 12000 エージェント導入モデルの場合は、手順 3 からの手順を繰り返して新しいクラスタを追加します。

12000 エージェント展開用 Cisco RSM の構成

12000 エージェント展開に対する Cisco RSM（リモート サイレント モニタリング）サーバーを分散モードで構成するには、以下の手順を実行します。

ソフトウェア要件	タスク
RSM の構成	4000 および12000 エージェント展開用 RSM 構成設定の設定 （411 ページ）
	JTAPI クライアント優先設定の構成 （403 ページ）
	レジストリ設定の編集 （403 ページ）
ゲートウェイの構成	VXML ゲートウェイの構成 （403 ページ）
Unified CVP の構成	RSM プロンプトのアップロード （404 ページ）
	CVP コールフローの統合 （404 ページ）
	コールフローの展開 （406 ページ）
Unified CCE の構成	エージェント ターゲット ルールの設定 （407 ページ）
	スーパーバイザ ログイン アカウントの作成 （408 ページ）
	RSM 用ルーティングスクリプトの作成 （408 ページ）
Unified CallManager の構成	シミュレーションする電話機の構成 （409 ページ）
	ログインプール Simphone の設定 （410 ページ）
	RSM アプリケーションユーザーの作成 （549 ページ）

Small Contact Center 展開用 Cisco RSM の構成

Small Contact Center 展開用の Cisco RSM（リモート サイレント モニタリング）サーバーを分散モードで次の順序で構成します。

（注） 各サブカスタマーには個別の RSM が構成されます。

ソフトウェア要件	タスク
RSM の構成	Small Contact Center 展開用 RSM 構成設定の設定 （416 ページ）
	JTAPI クライアント優先設定の構成 （403 ページ）
	レジストリ設定の編集 （403 ページ）
ゲートウェイの構成	VXML ゲートウェイの構成 （403 ページ）
Unified CVP の構成	RSM プロンプトのアップロード （404 ページ）
	CVP コールフローの統合 （404 ページ）
	コールフローの展開 （406 ページ）
Unified CCE の構成	エージェント ターゲット ルールの設定 （407 ページ）
	スーパーバイザ ログイン アカウントの作成 （408 ページ）
	RSM 用ルーティングスクリプトの作成 （408 ページ）
Unified CallManager の構成	シミュレーションする電話機の構成 （409 ページ）
	ログインプール Simphone の設定 （410 ページ）
	RSM アプリケーションユーザーの作成 （549 ページ）

Small Contact Center 展開用 RSM 構成設定の設定

手順

ステップ 1 メールサーバー構成設定を完了するには、以下を実行します。

a) **[スタート（Start）]** > **[CiscoRSM]** > **[RSM構成マネージャ（RSM Configuration Manager）]** の順に選択します。

b) **[Eメールアラートの送信（Send Email Alert）]** チェックボックスをオンにします。

c) **[メールサーバーのホスト名/IP（Mail Server Host Name/IP）]** テキストボックスに、メールサーバーのホスト名/IPアドレスを入力します。

d) **[ポート（Port）]** テキストボックスに、E メールポート番号を入力します。

e) **[送信者のEメールアドレス（Sender Email Address）]** テキストボックスに送信者の E メール ID を入力します。
f) **[受信者のEメールアドレス（Receiver Email Address）]** テキストボックスに受信者の E メール ID を入力します。
g) [次へ（Next）] をクリックします。

ステップ 2 その他の構成設定を完了するには、以下を実行します。

a) **[問題のコールの最短期間（Problem Call Minimum Duration）]** テキストボックスに **1800** と入力します。
b) **[問題のコールの最短保留（Problem Call Min Holds）]** テキストボックスに **4** と入力します。
c) **[古いコールの最長期間（Max Stale Call Duration）]** テキストボックスに **3600** と入力します。
d) **[CTI OSトレースマスク（CTI OS TraceMask）]** の値を空欄にします。
e) VL エンジンの **[ログレベル（Log Level）]** ドロップダウンリストで **[INFO]** を選択します。
f) VL エンジンの **[HTTPリスニングポート（HTTP Listen Port）]** テキストボックスに **8080** と入力します。
g) PhoneSim の **[VRUへのオーディオバッファ長（Audio Buffer Len To VRU）]** テキストボックスに **480** と入力します。

（注） VRU へのオーディオバッファ長のデフォルト値は 160 です。CVP 環境の場合、値は 480 に設定されます。

h) PhoneSim の **[ログレベル（Log Level）]** ドロップダウンリストで **[INFO]** を選択します。
i) PhoneSim の **[HTTPリッスンポート（HTTP Listen Port）]** テキストボックスに **29001** と入力します。
j) PhoneSim の **[RTSPリッスンポート（RTSP Listen Port）]** テキストボックスに **29554** と入力します。
k) Phonesim のドロップダウンリストで、**オーディオエンコーディング VRU** に対して **RTSP u-law** を選択します。
l) PhoneSim の **[HTTPチャンク化転送の実行（Do HTTP Chunked Transfers）]** ドロップダウンリストで **[いいえ（No）]** を選択します。
m) **[ホストデータIP（Host Data IP）]** テキストボックスで RSM サーバーの IP アドレスを入力します。
n) [次へ（Next）] をクリックします。

ステップ 3 クラスタ構成設定を定義します。

これらの設定は、RSM がモニターするエージェントで Unified Communications Manager クラスタを構成するために使用されます。

a) **[クラスタの追加（Add Cluster）]** をクリックします。
b) **[ClusterN_Name]** テキストボックスにクラスタ名を入力します。

（注）
- 名前は英数字にする必要があります。
- N はクラスタ番号を表します。

c) **[Simphonesへのログインプール数（No. of Login Pool Simphones）]** テキストボックスに **5**と入力します。

d) **[監視電話数（No. of Monitoring Phones）]** テキストボックスに **10** と入力します。（これは、同時に 10 の電話を監視します）。

e) **[周辺機器ID（Peripheral ID）]** テキストボックスに、エージェント PG の周辺機器 ID を入力します。

f) **[JTAPI ユーザー名（JTAPI Username）]** テキストボックスに **rsmuser** と入力します。

g) **[JTAPI パスワード（JTAPI Password）]** テキストボックスに rsmuser パスワードを入力します。

h) **[MAC範囲の開始（Start MAC Range）]** テキストボックスに、simphone デバイス名の MAC 範囲の自動生成に使用する最初の MAC アドレスを入力します。

i) **[回線番号範囲の開始（Start Line Num Range）]** テキストボックスに、simphone DN の回線内線番号範囲の自動生成に使用する最初の内線番号を入力します。

（注） **1.** 回線内線番号範囲はクラスタ間で重複してはなりません。ClusterN_PhoneSim_StartMACRange 値に関連付けられます。

2. [開始回線番号範囲（Start Line Num Range）] は 4 ー 15 桁にする必要があります。

j) **[SIP転送（SIP Transport）]** ドロップダウンリストで **[TCP]** を選択します。

k) [次へ（Next）] をクリックします。

ステップ 4 クラスタに対して Unified Communications Manager 構成設定を定義するには以下を実行します。

a) **[ホスト名/IP（Host Name/IP）]** テキストボックスに CUCM 1 サーバー（Publisher）のホスト名/IPアドレスを入力します。

b) **[ポート（Port）]** テキストボックスで CUCM 1 ポート に対して **5060** と入力します。

c) **[ホスト名/IP（Host Name/IP）]** テキストボックスに CUCM 2 サーバー（Subscriber 1）のホスト名/IPアドレスを入力します。

d) **[ポート（Port）]** テキストボックスで CUCM 1 ポート に対して **5060** と入力します。

e) [次へ（Next）] をクリックします。

ステップ 5 **[UCCE 統合（UCCE Integration）]** ウィンドウで [UCCE を CTI に統合（UCCE Integration with CTI）] を選択し、次のように入力します。

a) **[CTI 1Aホスト名/IP（CTI 1A Host Name/IP）]** にエージェント PG 1A のホスト名/IP アドレスを入力します。

b) **[CTI 1Aポート（CTI 1A Port）]** テキストボックスに **42027** と入力します。

c) **[CTIOS 1Bホスト名/IP（CTIOS 1B Host Name/IP）]** にエージェント PG 1B のホスト名/IP アドレスを入力します。

d) **[CTI 1Bポート（CTI 1B Port）]** テキストボックスに **43027** と入力します。

e) [次へ（Next）] をクリックします。

ステップ 6 **[PhoneSimサービスの起動（Start PhoneSim Service）]** と **[VLEngineサービスの起動（Start VLEngine Service）]** チェックボックスをオンにします。

ステップ 7 **[完了（Finish）]** をクリックします。

A-Law コーデック用 Cisco RSM の構成

- RSM の構成 （419 ページ）
- ゲートウェイの構成 （419 ページ）
- Unified CVP の構成 （419 ページ）
- Unified Communications Manager の構成 （419 ページ）

RSM の構成

Cisco RSM の構成詳細については、「RSM の構成 （400 ページ）」を参照してください。

（注） RSM 構成の**その他の設定（手順 2-k）**に **rtsp-alaw** を選択していることを確認します。

ゲートウェイの構成

詳細については、ゲートウェイの構成 （378 ページ） を参照してください。

Unified CVP の構成

詳細については、Unified CVP の構成 （380 ページ）を参照してください。

Unified Communications Manager の構成

- サービスパラメータの設定 （419 ページ）
- リージョンの構成 （305 ページ）

サービスパラメータの設定

詳細については、Unified Communication Manager の構成 （382 ページ）を参照してください。

Cisco MediaSense

- Cisco MediaSense 用 ゴールデンテンプレートの作成 （420 ページ）
- 自動化クローニングと OS のカスタマイズ （2 ページ）
- Cisco MediaSense の構成 （421 ページ）

Cisco MediaSense 用 ゴールデンテンプレートの作成

次の手順に従ってタスクを実行し、Cisco MediaSense のゴールデンテンプレートを作成します。各タスクの後で、このページに戻ってそのタスクを「完了」としてマークしたら、次の手順に進みます。

順序	完了したか	タスク	注意事項
1		ダウンロード Ora_11.5.1_vmv8_v1.0.ova	OVA ファイルのダウンロード （392 ページ）を参照してください。
2		OVA から仮想マシンを作成します。	仮想マシンの作成 （392 ページ）の手順を実行します。
3		Cisco MediaSense をインストールします。	ゴールデンテンプレートの VOS アプリケーションのインストール手順は以下のとおりです。、 OS ベースアプリケーションのインストール （420 ページ）を参照してください。
4		仮想マシンをゴールデンテンプレートに変換します。	仮想マシンをゴールデンテンプレートに変換 （397 ページ）の手順を実行します。

すべてのゴールデンテンプレートを作成したら、自動化プロセス（ 自動化クローニングと OS のカスタマイズ （2 ページ）） を実行できます。自動化プロセスを実行した後、接続先システムで Cisco MediaSense を構成できます。「Cisco MediaSense の構成 （421 ページ）」を参照してください。

、 OS ベースアプリケーションのインストール

音声 OS ベースアプリケーションをインストールするには、以下の手順を実行します。

- Cisco MediaSense
- シスコ仮想化音声ブラウザ

手順

ステップ 1 ISO ファイルを仮想マシンにマウントし、スイッチをオンにします。

ステップ 2 インストール ウィザードの指示に従います。

a) **ディスクが見つかりました**ページで、**[OK]** をクリックし、インストール前にメディアを確認します。
b) [OK] をクリックします。
c) **製品導入の選択**ページで、必要な製品を選択し、**[OK]** をクリックします。
d) **インストールを続行**ページで、**[はい（Yes）]** をクリックします。
e) **プラットフォームインストールウィザード**ページで、**[スキップ（Skip）]** を選択します。

インストール後、**既存の構成情報**ページが表示されます。

f) **Ctrl+Alt** を押して、カーソルを解放します。

ステップ 3 仮想マシンをシャット ダウンします。

ステップ 4 ISO イメージをアンマウントします。

Cisco MediaSense の構成

Cisco MediaSense Primary

Cisco MediaSense Primary の構成

始める前に

自動化スプレッドシートのオプションの DNS_IP_NIC1 セルに値がある場合は、正引きルックアップおよび逆引きルックアップでマシンを追加して DNS サーバーを構成します。詳細については、DNS サーバーの構成 （140 ページ）を参照してください。

手順

ステップ 1 ネットワークアダプタおよびフロッピードライブの **[電源投入時に接続（Connect at Power On）]** がオンになっていることを確認したら、**[OK]** をクリックします。

ステップ 2 プライマリで電源をオンにします。`.flp` ファイルの情報に基づいてインストールが始まります。インストールが自動的に始まり、ユーザの操作なしで実行されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 3 VM の **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、Publisher マシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 4 設定を編集し、フロッピードライブの**[電源投入時に接続（Connect at Power On）]** をオフにします。

（注） Publisher/プライマリをカスタマイズすると、ユーザー名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

- OS 管理者のデフォルトパスワード：c1sco@123
- アプリケーションユーザー名：Administrator
- アプリケーションユーザーのデフォルトパスワード：c1sco@123
- Sftp パスワード：c1sco@123
- IPSec パスワード：c1sco@123

リブート後、VM のインストールが完了し、VM のスプレッドシートにすべてのパラメータが記載されます。

プライマリサーバーの設定の完了

MediaSense 展開でプライマリサーバーの設定を完了するには、以下の手順を実行します。

手順

ステップ 1 インストール手順が完了すると、システムは自動的に再起動します。プライマリサーバーの MediaSense Administration にサインインします。(`https://<server>:8443/oraadmin`)

[MediaSense の 1つ目のサーバーの設定（MediaSense First Server Setup）] ウィザードの [ようこそ（Welcome）] 画面が表示されます。

ステップ 2 続行する場合は、**[次へ（Next）]** をクリックします。

[サービスの有効化（Service Activation）] 画面が表示されます。

ステップ 3 このサーバーの IP アドレスがシステム内部で検証され、このサーバーの MediaSense 機能サービスが自動的に有効化されます。[サービスの有効化（Service Activation）] ウィンドウで、すべての機能サービスが有効化として表示されるまで待ちます。すべてのサービスが正常に有効化されたら、**[次へ（Next）]** をクリックします。

[次へ（Next）] をクリックすると、**[AXLサービスプロバイダ（AXL Service Provider）]** 画面が表示されます。

ステップ 4 MediaSense と通信する Unified CM の各フィールドに AXL サービスプロバイダー（IPアドレス）と AXL 管理者のユーザー名とパスワードを入力し、**[次へ（Next）]** をクリックすると、**[呼制御サービスプロバイダ（Call Control Service Provider）]** 画面が表示されます。認証によって、Unified CM クラスタの入力と、そのクラスタ内の Unified CM サーバーリストの取得ができるようになります。

AXL 管理者のユーザー名は、そのクラスタの Unified CM 管理者のユーザー名とは異なる場合があります。Unified CM の標準 Unified CM 管理者グループおよび「Standard AXL API Access」ロールに AXL 管理者のユーザー名を追加してください。

ステップ 5 [対応可能呼制御サービスプロバイダ（Available Call Control Service Providers）] ウィンドウで通話制御サービスの Unified CM IP アドレスを選択し、**[選択した呼制御サービスプロバイダ（Selected Call Control Service Providers）]** ウィンドウに移動し、**[次へ（Next）]** をクリックします。

ステップ 6 正常に構成されたサービスを示す [MediaSense 設定サマリー（MediaSense Setup Summary）] ウィンドウが表示されます。[完了（Done）] をクリックしてプライマリサーバーの初期設定を完了します。

MediaSense サーバーのインストール後のプロセスが完了したら、展開用の Unified CM サーバーにアクセスする必要があります。SIP トランク、ルートパターン、ルートグループ、ルートリスト、録音プロファイル、およびエンドユーザーを構成する必要があります。

これで、MediaSense のプライマリサーバーの初期設定は完了です。

セカンダリサーバーまたは拡張サーバー上に MediaSense をインストールする前に、これらのサーバーの詳細をプライマリサーバーに構成する必要があります。MediaSense Administration ユーザーインターフェイスを使用してこれらサーバーの詳細を構成します。

ステップ 7 **[MediaSense Administration]** にログインし、**[APIユーザー構成（API User Configuration）]** を選択します。

ステップ 8 対応可能な Unified CM ユーザーを選択し、MediaSense API ユーザーリストに追加します。

このユーザーを使用して、検索と再生にログインできます。

次のタスク

着信通話の構成 （423 ページ）.

着信通話の構成

手順

ステップ 1 Cisco MediaSense Administration ページにログインします。

ステップ 2 **着信通話構成**ページに移動します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **[アドレス（Address）]** フィールドの Cisco Unified Communications Manager で作成された録音プロファイル番号を入力します。

ステップ 5 **[アクション（Action）]** ドロップダウンリストで **[録音（Record）]** を選択します。

ステップ 6 [保存（Save）] をクリックします。

Cisco MediaSense Secondary

始める前に

自動化スプレッドシートのオプションの DNS_IP_NIC1 セルに値がある場合は、正引きルックアップおよび逆引きルックアップでマシンを追加して DNS サーバーを構成します。DNS サーバーの構成 （140 ページ）を参照してください。

手順

ステップ 1 ネットワークアダプタおよびフロッピードライブの **[電源投入時に接続（Connect at Power On）]** がオンになっていることを確認したら、**[OK]** をクリックします。

ステップ 2 セカンダリの電源をオンにします。.flp ファイルの情報に基づいてインストールが始まります。インストールが自動的に始まり、ユーザの操作なしで実行されます。1 時間以上経過した後、インストールの成功を示すメッセージが表示されます。

ステップ 3 VM の **[コンソール（Console）]** タブをクリックします。管理者ユーザーのログイン情報を使用して、セカンダリマシンにログインします。CLI インターフェイスに対してマシンが開かれます。

ステップ 4 VM を右クリックし、**[設定の編集（Edit settings）]** を選択し、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

セカンダリ ノードをカスタマイズすると、ユーザ名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

- OS 管理者のデフォルトパスワード：cisco@123
- アプリケーションユーザー名：Administrator
- アプリケーションユーザーのデフォルトパスワード：cisco@123
- Sftp パスワード：c1sco@123
- IPSec パスワード：c1sco@123

リブート後、VM のインストールが完了し、VM のスプレッドシートにすべてのパラメータが記載されます。

セカンダリノードの追加

手順

ステップ 1 MediaSense の Web ポータルにログインします。

ステップ 2 左側の **[システム（System）]** メニューで、**[MediaSenseサーバー構成（MediaSense Server Configuration）]** を選択します。

ステップ 3 **[MediaSenseサーバー構成（MediaSense Server Configuration）]** 画面で、**[MediaSenseサーバーを追加（Add MediaSense Server）]** をクリックします。

プライマリノードで**[MediaSenseサーバーを追加（Add MediaSense Server）]**画面を開きます。

ステップ 4 インストールで DNS サフィックスを使用する場合は、追加するサーバーのホスト名を入力します。

ステップ 5 インストールで DNS サフィックスを使用しない場合は、追加するサーバーの IP アドレスを入力します。

ステップ 6 任意で、追加するサーバーの説明を入力します。

ステップ 7 任意で追加するサーバーの MAC アドレスを入力します。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 **[MediaSenseサーバーリストに戻る（Back to MediaSense Server List）]** をクリックします。

MediaSense が確認メッセージを表示します。**[MediaSenseサーバーリスト（MediaSense Server List）]** で追加したサーバーの構成詳細が表示されます。

（注） この Web ページではサーバータイプを割り当てることはできません。サーバータイプはインストール後の手順でのみ割り当てることができます。新規サーバーが MediaSense サーバーリストに追加され、インストール後の手順が正常に完了するまでの間は、新規サーバーのタイプは不明のままです。

Cisco MediaSense Secondary の構成

始める前に

自動化スプレッドシートのオプションの DNS_IP_NIC1 セルに値がある場合は、正引きルックアップおよび逆引きルックアップでマシンを追加して DNS サーバーを構成します。DNS サーバーの構成 （140 ページ）を参照してください。

手順

ステップ 1 自動化ツールを実行したクライアントコンピュータで、`C:\GoldenTemplateTool_10\PlatformConfigRepository\MediaSense` に移動します。

ステップ 2 `MEDIASENSE_SECONDARY_platformConfig.xml` という名前のファイルをコピーします。

ステップ 3 それを他の任意の場所に貼り付け、`platformConfig.xml` に名前を変更します。

ステップ 4 WinImage を起動し、**[ファイル（File）]** > **[新規（New）]** > **[1.44 MB]** の順に選択し、**[OK]** をクリックします。

ステップ 5 `platformConfig.xml` をドラッグし、WinImage にドロップします。

a) ファイルを挿入するかどうかを確認するメッセージで、**[はい（Yes）]**をクリックします。

b) **[ファイル（File）]**>**[保存（Save）]**の順に選択し、ファイル名が `platformConfig.flp` のファイルを仮想化フロッピー画像として保存します。

ヒント ドラッグアンドドロップが機能しない場合は、**[画像（Image）]** > **[挿入（Inject）]** の順に選択し、ファイルを参照します。

ステップ 6 vSphere インフラストラクチャ クライアントを開き、vCenter に接続します。VM が展開されているお客様の ESXi ホストに移動します。

ステップ 7 [構成（Configuration）] タブに移動し、ストレージセクションで [データストア（Datastore）] を右クリックし、[データストアを参照（Browse Datastore）] を選択します。

ステップ 8 `CMS_SEC` というフォルダを作成し、そのフォルダに `platformConfig.flp` をアップロードします。

ステップ 9 Unified Communications Manager Subscriber VM の仮想マシン設定を編集します。

ステップ 10 **[ハードウェア（Hardware）]** タブで、フロッピードライブをクリックし、**[データストアの既存のフロッピー画像を使用する（Use The Existing Floppy Image in Datastore）]** ラジオボタンを選択し、データストアの `CMS_SEC` フォルダから `platformConfig.flp` をマウントします。

ステップ 11 ネットワークアダプタおよびフロッピードライブの **[電源投入時に接続（Connect at Power On）]** がオンになっていることを確認します。**[OK]** をクリックし、VM の電源をオンにします。

これにより、インストールが始まり、`.flp` ファイルの情報に基づいてインストールがカスタマイズされます。

ステップ 12 自動化スプレッドシートのオプションの DNS_IP_NIC1 セルに値がある場合は、正引きルックアップおよび逆引きルックアップでマシンを追加して DNS サーバーを構成します。

（注） サブスクライバノードのカスタマイズ中、ユーザー名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

ステップ 13 インストールが完了したら、フロッピードライブの **[電源投入時に接続（Connect at Power on）]** をオフにします。

（注） Publisher/プライマリをカスタマイズすると、ユーザー名とパスワードが次のように変更されます。お客様がパスワードを変更する必要があります。

リブート後、VM のインストールが完了し、VM のスプレッドシートにすべてのパラメータが記載されます。

セカンダリサーバーの設定の完了

MediaSense 展開でセカンダリサーバーの設定を完了するには、以下の手順を実行します。

手順

ステップ 1 前の項のインストール手順を完了すると、システムが自動的に再起動し、セカンダリサーバーの MediaSense Administration にサインインする必要があります。サインインすると、MediaSense Secondary サーバー設定ウィザードで **[ようこそ（Welcome）]** 画面が表示されます。

ステップ 2 続行する場合は、**[次へ（Next）]** をクリックします。

[ようこそ（Welcome）] 画面では、サーバーの種類を決定します。

サーバーの種類に対して、**[セカンダリ（Secondary）]** を選択したら、**[次へ（Next）]** をクリックします。**[サービスの有効化（Service Activation）]** 画面が表示されます。

ステップ 3 サービスが有効化されたら、**[完了（Finish）]** をクリックして、後続サーバーの初期設定を完了します。

[MediaSense設定サマリー（MediaSense Setup Summary）] 画面には、初期設定の結果が表示され、MediaSense が再起動します。

これで後続サーバーの初期設定が完了です。この後続サーバーで、録音する準備が整いました。

クラスタ内の各拡張サーバーに対して、この設定手順を繰り返します。

MediaSense Forking の構成

- Cisco MediaSense BIB Forking 用 Cisco Unified CM のプロビジョニング （427 ページ）
- Cisco MediaSense CUBE Forking 用 Cisco Unified Border Element のプロビジョニング （428 ページ）
- Media Forking 用 TDM ゲートウェイのプロビジョニング （436 ページ）

Cisco MediaSense BIB Forking 用 Cisco Unified CM のプロビジョニング

順序	タスク	完了したか
1	SIPオプションの設定 （526 ページ）	
2	SIP トランクの追加 （291 ページ）	
3	ルート パターンの追加 （297 ページ）	
4	録音プロファイルの設定 （530 ページ）	
5	デバイスの構成 （428 ページ）	
6	録音デバイスに対して iLBC、iSAC および g.722 を無効化 （531 ページ）	
7	エンドユーザーの設定 （428 ページ）	

デバイスの構成

手順

ステップ 1 プロバイダとして Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なカスタマーレベルに設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[電話機（Phones）]** の順に選択します。

ステップ 4 構成する電話をリストから選択します。

ステップ 5 **[組み込みブリッジ（Built-in Bridge）]** ドロップダウンログインで **[オン（On）]** を選択し、組み込みブリッジを有効化します。

ステップ 6 **[回線（Lines）]** タブの **[録音フラグ（Recording Flag）]**ドロップダウンリストで **[自動コール録音を有効にする（Automatic Call Recording Enabled）]** を選択します。

ステップ 7 **録音プロファイル名**を入力します。

（注） Cisco Unified Communications Manager で作成された録音プロファイル名と同じ名前を入力します。

ステップ 8 [保存（Save）] をクリックします。

エンドユーザーの設定

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 階層が適切なカスタマー/拠点に設定されていることを確認します。

ステップ 3 **[Subscriber管理（Subscriber Management）]** > **[Subscribers]** の順に選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **[ユーザー（User）]** タブで、一意の**ユーザー ID** と**姓** を入力します。

ステップ 6 **パスワード**と**確認用パスワード**を入力します。

ステップ 7 [保存（Save）] をクリックします。

Cisco MediaSense CUBE Forking 用 Cisco Unified Border Element のプロビジョニング

- HCS 導入モデルに対する Cisco MediaSense CUBE Forking 用 Cisco Unified Border Element のプロビジョニング （429 ページ）
- SCC 導入モデルに対する Cisco MediaSense CUBE Forking 用 Cisco Unified Border Element のプロビジョニング （434 ページ）

HCS 導入モデルに対する *Cisco MediaSense CUBE Forking* 用 *Cisco Unified Border Element* のプロビジョニング

順序	タスク	完了したか
1	グローバルレベルの設定 （429 ページ）	
2	ダイヤルピアレベルの設定 （430 ページ）	
3	MediaSense 展開用 CUBE ダイヤルピアの設定 （430 ページ）	

グローバルレベルの設定

手順

ステップ 1 SSH または Telnet を使用して CUBE ゲートウェイに接続します。

ステップ 2 グローバル構成モードを開始します。

```
cube# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
cube(config)#
```

ステップ 3 VoIP 音声サービス構成モードを入力します。

```
cube(config)# voice service voip
cube(config-voi-serv)#
```

ステップ 4 通話料金詐欺セキュリティが正しく構成されていない場合、通話は 403 Forbidden の応答によって拒否される可能性があります。ソリューションは、信頼できるエンドポイントとして IP アドレスを追加することです。追加しない場合は、次の構成エントリを使用して IP アドレスによる信頼できるリストの認証を無効化します。

```
cube(config-voi-serv)# no ip address trusted authenticate
```

ステップ 5 CUBE と CUBE 冗長性を有効にします。

```
cube(config-voi-serv)# mode border-element
cube(config-voi-serv)# allow-connections sip to sip
cube(config-voi-serv)# sip
cube(config-voi-serv)# asymmetric payload full
cube(config-voi-serv)# video screening
```

上記の例では、最後の 3 行は、ビデオ通話が CUBE を通す場合にのみ必要です。

ステップ 6 この時点で、CUBE の構成を保存し、CUBE をリブートする必要があります。

注意 CUBE のリブートは、オフピーク中に行ってください。

a) CUBE の構成を保存します。

```
cube# copy run start
```

b) CUBE をリブートします。

```
cube# reload
```

ステップ 7 CUBE をリブート後、メディアクラスを構成して録音する通話を指定します。

```
cube(config-voi-serv)# media class 3
cube(config-voi-serv)# recorder parameter
cube(config-voi-serv)# media-recording 3000
```

ステップ 8 VoIP 音声サービス構成モードを終了します。

```
cube(config-voi-serv)# exit
```

ステップ 9 音声コーデッククラスを 1 つ作成すると、5 つのコーデックを取り込みます（ビデオ用の 1 つを含む）。これらのコーデックは、音声クラスを指定するためにインバウンド/アウトバウンドダイヤルピアが使用します。

```
cube(config)# voice class codec 3
cube(config)# codec preference 1 mp4a-latm
cube(config)# codec preference 2 g711ulaw
cube(config)# codec preference 3 g722-64
cube(config)# codec preference 4 g729br8
cube(config)# video codec h264
```

上記の例では、最初のコーデックの優先設定とビデオコーデックの定義は、AAC-LD/LATM メディアがお客様のコールフローの一部の場合にのみ必要になります。

ステップ 10 デバッグを簡素化するため、CUBE の現地時間を Cisco MediaSense サーバーの現地時間と同期する必要があります。たとえば、NTP サーバーを 10.10.10.5 に指定した場合、CUBE では次のコマンドを使用します。

```
cube(config)# ntp update-calendar
cube(config)# sntp server 10.10.10.5
```

ダイヤルピアレベルの設定

（注） この情報は、構成例について説明します。CUBE は、別の方法でも展開できます。

CUBE の各 Cisco MediaSense 展開には、3 つのダイヤルピアが含まれます。

- 着信ダイヤルピア：この例での一意の名前は、1000 です。
- 発信ダイヤルピア：この例での一意の名前は、2000 です。
- 分岐ダイヤルピア：この例での一意の名前は 3000 です

この手順を実行する前に、CUBE 管理者からこれら 3 つのダイヤルピアの詳細を入手してください。

（注） 3 つのダイヤルピアの構成順序は任意です。

MediaSense 展開用 CUBE ダイヤルピアの設定

この手順は、3 つのダイヤルピアの設定方法の例を示します。使用される特定の名前および値は、説明のみを目的として使用されています。

注意 この手順は、実際のCUBEマニュアルに置き換わるものではありません。これは、MediaSense用の CUBE の構成に関する詳細情報を説明するチュートリアルです。最新情報については、http://www.cisco.com/go/cube から入手できる CUBE のマニュアルを参照してください。

手順

ステップ 1 インバウンドダイヤルピアでメディア分岐を構成します。

a) インバウンドダイヤルピアに固有の名前を割り当てます。この例では、名前は「1000」に設定されます。

```
cube(config)# dial-peer voice 1000 voip
```

このコマンドによってダイヤルピア構成モードに移行し、「1000」という名前の VoIP ダイヤルピアが構成されます。

b) このインバウンドダイヤルピアのセッションプロトコルを「sipv2」に指定します（この値は任意ではありません）。

```
cube(config-dial-peer)# session protocol sipv2
```

このコマンドは、エンドポイントの SIP セッションプロトコルが動作し、通話処理に使用できるかどうかを判定します。セッションプロトコルと VoIP レイヤーは、IP レイヤーに応じて最適なローカルアドレスを設定し、複数のインターフェイスが宛先アドレスへのルートをサポートできる場合でも、このアドレスをシグナリング、メディア、または両方の送信元アドレスとして使用します。

c) 着信通話の SIP Invite URL を指定します。この例では、着信通話、録音可能通話は 6 桁であるとします。ここでは、最初の 3 桁に「123」を割り当て、最後の 3 桁は発信者が（ダイヤルする接続先 DN の一部として）任意に選択できるようにします。このコマンドは、着信通話をダイヤルピアと関連付けます。

```
cube(config-dial-peer)# incoming called-number 123...$
```

d) 複数のコーデックを使用する場合は、コーデックの選択順序を定義する音声クラスを作成する必要があります。これにより、各ダイヤルピアにクラスを適用するために音声クラスを適用できます。この例では、使用されているタグは「1」です。

```
cube(config-dial-peer)# voice-class codec 1
```

このタグは、このコーデックを一意に識別します。範囲は 1 ～ 10000 です。

e) 通話が転送される場合は、必ずメタデータを MediaSense に共有してください。これを行うには、このダイヤルピアの発信ヘッダーで PAI ヘッダーへの変換を有効にします。

```
cube(config-dial-peer)# voice-class sip asserted-id pai
```

f) インバウンドダイヤルピアを通過するすべての通話が分岐できるように指定します。グローバル分岐を設定するために使用する番号と同じ番号を使用します（「グローバルレベルの設定」を参照）。この例では、メディアクラスの番号は「3」です。

```
cube(config-dial-peer)# media-class 3
```

g) このインバウンドダイヤルピアの構成を終了します。

```
cube(config-dial-peer)# exit
cube(config)#
```

ステップ 2 アウトバウンドダイヤルピアを構成します。

a) アウトバウンドダイヤルピアに固有の名前を割り当てます。この例では、名前は「2000」に設定されます。

```
cube(config)# dial-peer voice 2000 voip
```

このコマンドによってダイヤルピア構成モードに移行し、「2000」という名前の VoIP ダイヤルピアが構成されます。

b) このアウトバウンドダイヤルピアのセッションプロトコルを「sipv2」に指定します（この値は任意ではありません）。

```
cube(config-dial-peer)# session protocol sipv2
```

c) 着信側番号に対応する接続先を指定します。この例では、「123...」です。

```
cube(config-dial-peer)# destination-pattern 123...$
```

d) 複数のコーデックを使用する場合は、コーデックの選択順序を定義する音声クラスを作成する必要があります。これにより、各ダイヤルピアにクラスを適用するために音声クラスを適用できます。インバウンドダイヤルピアと同じタグを使用します。この例では、使用されているタグは「1」です。

```
cube(config-dial-peer)# voice-class codec 1
```

e) このコールに対してプライマリ接続先を指定します。この例では、接続先を「ipv4:10.1.1.10:5060」に設定します。

```
cube(config-dial-peer)# session target ipv4:10.1.1.10:5060
```

f) このアウトバウンドダイヤルピアの構成を終了します。

```
cube(config-dial-peer)# exit
cube(config)#
```

ステップ 3 分岐ダイヤルピアを構成します。

a) 分岐ダイヤルピアに固有の名前を割り当てます。この例では、名前は「3000」に設定されます。

```
cube(config)# dial-peer voice 3000 voip
```

このコマンドによってダイヤルピア構成モードに移行し、「3000」という名前の VoIP ダイヤルピアが構成されます。オプションで、任意の英語フレーズを使用して、このダイヤルピアが実行する内容の説明を入力します。

```
cube(config-dial-peer)# description This is the forking dial-peer media sense
```

b) 任意の接続先パターンを指定します。ワイルドカードは使用できません。この CUBE から録音された通話は、この内線番号から発信されます。（MediaSense 着信通話構成テーブルでは、この番号は[アドレス（Address）]フィールドに対応します）。この例では、「3000」に設定します。

```
cube(config-dial-peer)# destination-pattern 3000
```

c) CUBE が INVITE のマルチパート本文を MediaSense に送信しないようにしてください。

```
cube(config-dial-peer)# signaling forward none
```

d) この分岐ダイヤルピアのセッションプロトコルを「sipv2」に指定します（この値は任意ではありません）。

```
cube(config-dial-peer)# session protocol sipv2
```

e) MediaSense 拡張サーバーの 1 つの IP アドレスを、CUBE トラフィックの接続先として指定します（該当する場合）。この例では、IP アドレス 10.2.2.20 の MediaSense サーバーを使用します。

```
cube(config-dial-peer)# session target ipv4:10.2.2.20:5060
```

（注） これらのサーバーは CUBE の負荷を伝送するため、この手順ではプライマリまたはセカンダリ MediaSense サーバーを使用することを避けてください。データベースサーバーへの負荷を増やさないことをお勧めします。

f) MediaSense と通信するセッション転送タイプ（UDP または TCP）を設定します。デフォルトは UDP です。session transport コマンドで指定するトランスポートプロトコルと transport コマンドで指定するプロトコルは同一である必要があります。

```
cube(config-dial-peer)# session transport tcp
```

g) 複数のコーデックを使用する場合は、コーデックの選択順序を定義する音声クラスを作成する必要があります。これにより、各ダイヤルピアにクラスを適用するために音声クラスを適用できます。インバウンドダイヤルピアと同じタグを使用します。この例では、「1」です。

```
cube(config-dial-peer)# voice-class codec 1
```

h) 送信元インターフェイスへの制御およびメディアバインディングを構成します。

```
cube(config-dial-peer)# voice-class sip bind control source-interface
GigabitEthernet1
cube(config-dial-peer)# voice-class sip bind media source-interface GigabitEthernet1
```

i) エンドポイント間の接続を監視するハートビートメカニズムを構成します。汎用ハートビートメカニズムでは、Cisco Unified Border Element が MediaSense サーバーまたはエンドポイントの状態を監視し、ハートビート障害が発生した場合にダイヤルピアをタイムアウトするオプションを提供できます。

（注） 同じ接続先パターンに代替ダイヤルピアを構成した場合、通話は次の優先ダイヤルピアにフェールオーバーします。それ以外の場合、コールは拒否されます。フェールオーバー ダイヤルピアを構成していない場合、キープアライブ オプションを構成しないでください。

```
cube(config-dial-peer)# voice-class sip options-keepalive
```

j) この分岐ダイヤルピアの構成を終了します。

```
cube(config-dial-peer)# exit
cube(config)#
```

k) 構成モードを終了します。

```
cube(config)# exit
cube#
```

l) CUBE の構成を保存します。

```
cube# copy run start
```

SCC 導入モデルに対する *Cisco MediaSense CUBE Forking* 用 *Cisco Unified Border Element* のプロビジョニング

順序	タスク	完了したか
1	グローバルレベルの設定 （429 ページ）	
2	ダイヤルピアレベルの設定 （430 ページ）	
3	Small Contact Center 展開用 CUBE ダイヤルピアの設定 （434 ページ）	

Small Contact Center 展開用 CUBE ダイヤルピアの設定

MediaSense のインバウンドダイヤルピアは、サブカスタマーごとに作成する必要があります。インバウンドダイヤルピアを作成するには、以下の手順を実行します。

手順

ステップ 1 インバウンドダイヤルピアでメディア分岐を構成します。

a) インバウンドダイヤルピアに固有の名前を割り当てます。この例では、名前は「1000」に設定されます。

```
cube(config)# dial-peer voice 1000 voip
```

このコマンドによってダイヤルピア構成モードに移行し、「1000」という名前の VoIP ダイヤルピアが構成されます。

b) このインバウンドダイヤルピアのセッションプロトコルを「sipv2」に指定します（この値は任意ではありません）。

```
cube(config-dial-peer)# session protocol sipv2
```

このコマンドは、エンドポイントの SIP セッションプロトコルが動作し、通話処理に使用できるかどうかを判定します。セッションプロトコルと VoIP レイヤーは、IP レイヤーに応じて最適なローカルアドレスを設定し、複数のインターフェイスが宛先アドレスへのルートをサポートできる場合でも、このアドレスをシグナリング、メディア、または両方の送信元アドレスとして使用します。

c) 着信通話の SIP Invite URL を指定します。この例では、着信、録音可能通話は 6 桁であるとします。ここでは、最初の 3 桁に「123」を割り当て、最後の 3 桁は発信者が（ダイヤルする接続先 DN の一部として）任意に選択できるようにします。このコマンドは、着信通話をダイヤルピアと関連付けます。

```
cube(config-dial-peer)# incoming called-number 123...$
```

d) 複数のコーデックを使用する場合は、コーデックの選択順序を定義する音声クラスを作成する必要があります。これにより、各ダイヤルピアにクラスを適用するために音声クラスを適用できます。この例では、使用されているタグは「1」です。

```
cube(config-dial-peer)# voice-class codec 1
```

このタグは、このコーデックを一意に識別します。範囲は 1 ～ 10000 です。

e) コールが転送される場合は、必ずMediaSenseにメタデータを伝播してください。これを行うには、このダイヤルピアの発信ヘッダーで PAI ヘッダーへの変換を有効にします。

```
cube(config-dial-peer)# voice-class sip asserted-id pai
```

f) インバウンドダイヤルピアを通過するすべての通話が分岐できるように指定します。グローバル分岐を設定するために使用する番号と同じ番号を使用します（「グローバルレベルの設定」を参照）。この例では、メディアクラスの番号は「3」です。

```
cube(config-dial-peer)# media-class 3
```

g) このインバウンドダイヤルピアの構成を終了します。

```
cube(config-dial-peer)# exit
cube(config)#
```

ステップ 2 分岐ダイヤルピアを構成します。

a) 分岐ダイヤルピアに固有の名前を割り当てます。この例では、名前は「3000」に設定されます。

```
cube(config)# dial-peer voice 3000 voip
```

このコマンドによってダイヤルピア構成モードに移行し、「3000」という名前の VoIP ダイヤルピアが構成されます。オプションで、任意の英語フレーズを使用して、このダイヤルピアが実行する内容の説明を入力します。

```
cube(config-dial-peer)# description This is the forking dial-peer
```

b) この分岐ダイヤルピアのセッションプロトコルを「sipv2」に指定します（この値は任意ではありません）。

```
cube(config-dial-peer)# session protocol sipv2
```

c) 任意の接続先パターンを指定します。ワイルドカードは使用できません。この CUBE から録音された通話は、この内線番号から発信されます。（MediaSense 着信通話構成テーブルでは、この番号は[アドレス（Address）]フィールドに対応します）。この例では、「3000」に設定します。

```
cube(config-dial-peer)# destination-pattern 3000
```

d) 複数のコーデックを使用する場合は、コーデックの選択順序を定義する音声クラスを作成する必要があります。その後、音声クラスを適用して、個々のダイヤルピアにクラスを適用できます。インバウンドダイヤルピアと同じタグを使用します。この例では、「1」です。

```
cube(config-dial-peer)# voice-class codec 1
```

e) MediaSense 拡張サーバーの 1 つの IP アドレスを、CUBE トラフィックの接続先として指定します（該当する場合）。この例では、IP アドレス 10.2.2.20 の MediaSense サーバーを使用します。

（注） これらのサーバーは CUBE の負荷を伝送するため、この手順ではプライマリまたはセカンダリ MediaSense サーバーを使用することを避けてください。データベースサーバーへの負荷を増やさないことをお勧めします。

```
cube(config-dial-peer)# session target ipv4:10.2.2.20:5060
```

f) MediaSense と通信するセッション転送タイプ（UDP または TCP）を設定します。デフォルトは UDP です。session transport コマンドで指定するトランスポートプロトコルと transport コマンドで指定するプロトコルは同一である必要があります。

```
cube(config-dial-peer)# session transport tcp
```

g) エンドポイント間の接続を監視するハートビートメカニズムを構成します。汎用ハートビートメカニズムでは、Cisco Unified Border Element が MediaSense サーバーまたはエンドポイントの状態を監視し、ハートビート障害が発生した場合にダイヤルピアをタイムアウトするオプションを提供できます。

（注） 同じ接続先パターンに代替ダイヤルピアを構成した場合、通話は次の優先ダイヤルピアにフェールオーバーします。それ以外の場合、コールは拒否されます。フェールオーバー ダイヤルピアを構成していない場合、キープアライブ オプションを構成しないでください。

```
cube(config-dial-peer)# voice-class sip options-keepalive
```

h) CUBE が INVITE のマルチパート本文を MediaSense に送信しないようにしてください。

```
cube(config-dial-peer)# signaling forward none
```

i) この分岐ダイヤルピアの構成を終了します。

```
cube(config-dial-peer)# exit
cube(config)#
```

j) 構成モードを終了します。

```
cube(config)# exit
cube#
```

k) CUBE の構成を保存します。

```
cube# copy run start
```

Media Forking 用 TDM ゲートウェイのプロビジョニング

次のセクションでは、TDM トランク上のコールのメディア録音の構成方法に関する詳細なガイドラインを示します。統合プラットフォームである CUBE (E) は、TDM トランク接続を提供し、同時にセッション ボーダー コントローラとして機能します。

このソリューションが機能させるには、PSTN からのコールがそれ自体にループバックされるため、CUBE への着信 VoIP SIP レグを作成します。次に、通話をエンタープライズネットワー

クのコールエージェントに送信し、発信VoIP SIP レグを作成します。したがって、ゲートウェイを使用して TDM レグを終端し、コールエージェントに対して IP レグを発信します。

（注） このフローでは、通話はルーターの規定キャパシティを実質的に半分にするため、同じ通話数に対して2倍のルーターキャパシティが必要になります。通話に対してルーターのフルキャパシティを使用する場合は、2 台のルーターが必要になります。両方のルーターを両方の目的に使用するのではなく、個々の目的に合わせて 2 台のルーターを構成してください。

TDM ゲートウェイを構成するには、次の手順に従います。

順序	タスク	完了したか
1	変換ルールとプロファイルの構成	
2	ループバック インターフェイスの構成	
3	メディアクラスの構成	
4	ダイヤルピアの構成	

手順

ステップ 1 変換ルールとプロファイルの構成

a) 音声コールの発信者番号（ANI）または着信者番号（DNIS）の変換ルールを構成します。

```
voice translation-rule 1
rule 1 /^966//8966/
voice translation-rule 2
rule 2 /^8966//966/
```

最初に定義されたルールはルール1で、966は一致して置換する必要があるパターンです。8966 は 966 に置き換えられるパターンです。

b) translation-profile の構成

ルールに示された照合パターン、番号計画、およびタイプに番号が一致する場合、変換ルールは、入力番号のサブ文字列を置き換えます。

```
voice translation-profile prefix
translate called 1
voice translation-profile strip
translate called 2
```

変換プロファイルプレフィックスは、変換ルール 1 に基づいて着信番号にプレフィックスを追加します。同様に、変換プロファイルストリップは、変換ルール 2 に基づいて着信番号からプレフィックスを削除します。

ステップ 2 ループバック インターフェイスの構成

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
```

ステップ 3 メディアクラスの構成

録音する通話を決定するメディアクラスを構成します。

```
cube(config-voi-serv)# media class 3
cube(config-voi-serv)# recorder parameter
cube(config-voi-serv)# media-recording 20
```

ステップ 4 ダイヤルピアの構成

a) 着信 PSTN 通話のポットダイヤルピアを構成

```
dial-peer voice 1 pots
description Incoming dial peer for PSTN calls
translation-profile incoming prefix
incoming called-number 9660000001
port 0/2/1:23
```

b) 着信 PSTN 通話をループバックするように VoIP ダイヤルピアを構成

```
dial-peer voice 8966 voip
description To loop incoming PSTN calls back to itself.
destination-pattern 89660000001
session protocol sipv2
session target ipv4:1.1.1.1 # loop back Ip address of the TDM gateway
session transport tcp
voice-class codec 1
dtmf-relay rtp-nte
no vad
```

c) 新しく発信した SIP 通話レグのインバウンドダイヤルピアを構成

```
dial-peer voice 89660 voip
description inbound dial-peer for the newly originated SIP call leg
translation-profile incoming strip
session protocol sipv2
session target sip-server
session transport tcp
incoming called-number 89660000001
voice-class codec 1
dtmf-relay rtp-nte
no vad
```

d) 新しく発信した SIP 通話のアウトバウンドダイヤルピアを構成

```
dial-peer voice 9660 voip
description Outgoing dial peer for looped call to contact center
destination-pattern 9660000001
session protocol sipv2
session target ipv4:192.1.10.1 #IP address of CVP server
session transport tcp
voice-class codec 1
dtmf-relay rtp-nte
media-class 3
no vad
```

e) 通話レグを分岐するためのアウトバウンドダイヤルピアの構成

```
dial-peer voice 20 voip
description Forking leg to MediaSense server.
preference 1
destination-pattern 99999
signaling forward none
```

```
session protocol sipv2
session target ipv4:192.1.9.1 #Ip address of MediaSense server
session transport tcp
voice-class sip options-keepalive
```

Cisco Unified SIP プロキシ

Cisco Unified SIP プロキシのインストール

CUSP のインストール

手順

ステップ 1 すべての Cisco Unified SIP プロキシ 8.5.7 ソフトウェアファイルをダウンロードします。

ステップ 2 ファイルを FTP サーバにコピーします。

ステップ 3 ルーター EXEC モードから、次のように入力します。

```
ping <ftp_server_ip_address>
```

ステップ 4 次を入力し、ソフトウェアをインストールします。

```
Service-Module 1/0 install url ftp://<ftp_server_ip_address>/cusp-k9.sme.8.5.7.pkg
```

ステップ 5 **y** と入力して、インストールを確認します。

ステップ 6 Cisco Unified SIP Proxy Service Module と入力して、インストールを監視し、完了します。

サービスモジュールへのインストール例

```
CUSP#service-nodule SM4/0 inst
CUSP#$ule SM4/0 install url ftp://10.10.10.203/cusp-k9.snc.8.5.7.pkg
Delete the installed Cisco Unified SIP Proxy and proceed with new installation?
[no]:yes
Loading cusp-k9.snc.8.5.7.pkg.install.src !
```

```
[OK - 1850/4096 bytes]
cur_cpu: 1862
cur_disk: 953880
cur_nem: 4113488
cur_pkg_name: cusp-k9.sne.8.5.7.pkg
cur_ios_version: 15.2<4>M5,
cur_image_name:c3900e-universalk9-mz
cur_pid: SM-SRE-900-K9
bl_str:
inst_str:
app_str:
key_filename: cusp-k9.sne.8.5.7.key
helper_filename:cusp-helper.sme.8.5.7
Resource check passed…
```

インストール後の構成ツール

CUSP#service-module SM 4/0 session のコマンドを実行し、最初のセッションを開きます。

最初のセッションを開くと、ポストインストール構成ツールが起動し、すぐに設定を開始するかをきいてきます。

適切な応答（yまたはn）を入力します。 nを入力すると、システムは停止します。「y」を入力すると、システムから確認を求められ、対話式ポストインストール構成プロセスが開始されます。

次に、例を示します。

```
IMPORTANT::
IMPORTANT:: Welcome to Cisco Systems Service Engine
IMPORTANT:: post installation configuration tool.
IMPORTANT::
IMPORTANT:: This is a one time process which will guide
IMPORTANT:: you through initial setup of your Service Engine.
IMPORTANT:: Once run, this process will have configured
IMPORTANT:: the system for your location.
IMPORTANT::
IMPORTANT:: If you do not wish to continue, the system will be halted
IMPORTANT:: so it can be safely removed from the router.
IMPORTANT::

Do you wish to start configuration now (y,n)? yes
Are you sure (y,n)? yes

IMPORTANT::
IMPORTANT:: A configuration has been found in flash. You can choose
IMPORTANT:: to restore this configuration into the current image.
IMPORTANT::
IMPORTANT:: A stored configuration contains some of the data from a
IMPORTANT:: previous installation, but not as much as a backup.
IMPORTANT::
IMPORTANT:: If you are recovering from a disaster and do not have a
IMPORTANT:: backup, you can restore the saved configuration.
IMPORTANT::
IMPORTANT:: If you choose not to restore the saved configuration, it
IMPORTANT:: will be erased from flash.
IMPORTANT::

Would you like to restore the saved configuration? (y,n) n

Erasing old configuration...done.
```

```
IMPORTANT::
IMPORTANT:: The old configuration has been erased.
IMPORTANT:: As soon as you finish configuring the system please use the
IMPORTANT:: "write memory" command to save the new configuration to flash.
IMPORTANT::

Enter Hostname
(my-hostname, or enter to use se-10-50-30-125):
Using se-10-50-30-125 as default

Enter Domain Name
(mydomain.com, or enter to use localdomain): cusp

IMPORTANT:: DNS Configuration:
IMPORTANT::
IMPORTANT:: This allows the entry of hostnames, for example foo.cisco.com, instead
IMPORTANT:: of IP addresses like 1.100.10.205 for application configuration. In order
IMPORTANT:: to set up DNS you must know the IP address of at least one of your
IMPORTANT:: DNS Servers.

Would you like to use DNS (y,n)?y

Enter IP Address of the Primary DNS Server
(IP address): 180.180.180.50
Found server 180.180.180.50

Enter IP Address of the Secondary DNS Server (other than Primary)
(IP address, or enter to bypass):

E

Enter Fully Qualified Domain Name(FQDN: e.g. myhost.mydomain.com)
or IP address of the Primary NTP server
(FQDN or IP address, or enter for 10.50.30.1): 10.50.10.1
Found server 10.50.10.1

Enter Fully Qualified Domain Name(FQDN: e.g. myhost.mydomain.com)
or IP address of the Secondary NTP Server
(FQDN or IP address, or enter to bypass):

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa 4) Arctic Ocean 7) Australia 10) Pacific Ocean
2) Americas 5) Asia 8) Europe
3) Antarctica 6) Atlantic Ocean 9) Indian Ocean
#? 2
Please select a country.
1) Anguilla 27) Honduras
2) Antigua & Barbuda 28) Jamaica
3) Argentina 29) Martinique
4) Aruba 30) Mexico
5) Bahamas 31) Montserrat
6) Barbados 32) Netherlands Antilles
7) Belize 33) Nicaragua
8) Bolivia 34) Panama
9) Brazil 35) Paraguay
10) Canada 36) Peru
11) Cayman Islands 37) Puerto Rico
12) Chile 38) St Barthelemy
13) Colombia 39) St Kitts & Nevis
14) Costa Rica 40) St Lucia
15) Cuba 41) St Martin (French part)
16) Dominica 42) St Pierre & Miquelon
```

```
17) Dominican Republic 43) St Vincent
18) Ecuador 44) Suriname
19) El Salvador 45) Trinidad & Tobago
20) French Guiana 46) Turks & Caicos Is
21) Greenland 47) United States
22) Grenada 48) Uruguay
23) Guadeloupe 49) Venezuela
24) Guatemala 50) Virgin Islands (UK)
25) Guyana 51) Virgin Islands (US)
26) Haiti
#? 47
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Pulaski County
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Mountain Time
18) Mountain Time - south Idaho & east Oregon
19) Mountain Time - Navajo
20) Mountain Standard Time - Arizona
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - Alaska panhandle neck
25) Alaska Time - west Alaska
26) Aleutian Islands
27) Hawaii
#? 21

The following information has been given:
United States
Pacific Time

Therefore TZ='America/Los_Angeles' will be used.
Is the above information OK?
1) Yes
2) No
#? 1

Local time is now: Mon Apr 5 11:20:17 PDT 2010.
Universal Time is now: Mon Apr 5 18:20:17 UTC 2010.
executing app post_install
executing app post_install done
Configuring the system. Please wait...
Changing owners and file permissions.
Tightening file permissions ...
Change owners and permissions complete.
Creating Postgres database .... done.
INIT: Switching to runlevel: 4
INIT: Sending processes the TERM signal
==> Starting CDP
STARTED: cli_server.sh
```

```
STARTED: ntp_startup.sh
STARTED: LDAP_startup.sh
STARTED: SQL_startup.sh
STARTED: dwnldr_startup.sh
STARTED: HTTP_startup.sh
STARTED: probe
STARTED: fndn_udins_wrapper
STARTED: superthread_startup.sh
STARTED: /bin/products/umg/umg_startup.sh

Waiting 49 ...

IMPORTANT::
IMPORTANT:: Administrator Account Creation
IMPORTANT::
IMPORTANT:: Create an administrator account.
IMPORTANT:: With this account, you can log in to the
IMPORTANT:: Cisco Unified SIP Proxy
IMPORTANT:: GUI and run the initialization wizard.

IMPORTANT::

Enter administrator user ID:
(user ID): test
tesEnter password for test:
(password):
Confirm password for test by reentering it:
(password):

SYSTEM ONLINE
cusp-sre-49# show software version
Cisco Unified SIP Proxy version <8.5.7>
Technical Support: http://www.cisco.com/techsupport Copyright <c> 1986-2008 by Cisco
Systems,Inc.
Cusp-src-49# show software packages

Installed Packages:
- Installer <Installer application >  <8.5.7.0>
- Infrastructure <Service Engine Infrastructure> <8.5.7>
- Global <Global manifest > <8.5.7>
- Bootloader <Secondary> <Service Engine Bootloader> <2.1.30>
- Core <Service Engine OS Core > <8.5.7>
- GPL Infrastrucutre <Service Engine GPL Infrastructure > <8.5.7>
```

新規または追加ライセンスの取得

必須情報

CSL ライセンスを新規または追加で取得する前に、次の情報を収集してください。

- 必要な機能の SKU。SKU は、 必要な Cisco Unified SIP プロキシ機能に対応した必要なライセンスを指定するために、注文処理で使用します。

- デバイスから製品ID（PID）とシリアル番号（SN）を入力します。この2つを合わせて一意のデバイス ID（UDI）になります。UDI は、ほとんどのシスコ ハードウェア デバイスの背面にあるラベル、または現場交換可能マザーボードの前面パネルにあるラベル トレイに印刷されています。UDIは、ソフトウェアで確認することもできます。確認には、特権 EXEC モードで show license udi コマンドを使用します。

ライセンシング ポータルを使用した追加機能またはアプリケーションのライセンスの取得

（注） 次の手順で使用する URL のいくつかは、Cisco.com のパスワードがないとアクセスできません。

Cisco Unified SIP プロキシ Release 8.5.7 の機能の追加ライセンスを取得するには、以下の手順を実行します。

手順

ステップ 1 http://www.cisco.com/web/ordering/root/index.html に移動し、発注プロセスのいずれか（パートナー、シスコダイレクトなど）のいずれかを選択して、ライセンスを発注します。ライセンスを購入すると、製品アクティベーション キー（PAK）が送られてきます。PAK は英数字の文字列で、ライセンスを購入したことを示します。

ステップ 2 ライセンスを取得するには、http://www.cisco.com/web/ordering/root/index.html の**シスコ製品ライセンス登録ポータル**に戻ります。プロンプトが表示されたら、PAK と、ライセンスをインストールするデバイスの一意のデバイス ID（UDI）を入力します。

ステップ 3 ライセンス ファイルをダウンロードするか、電子メールでライセンス ファイルを受け取ります。

ステップ 4 ライセンス ファイルを FTP または TFTP サーバにコピーします。

CLI を使用した Cisco Unified SIP プロキシ リリース 8.5.7 ライセンスのインストール

Cisco Unified SIP プロキシのライセンスをインストールするには、次の手順に従います。

手順

ステップ 1 CLI にログインします。

ステップ 2 `license install` <*URL*> と入力します。この場合、 <*URL*> とは前の手順でライセンスをコピーした FTP URL です。

ステップ 3 `show license` または `show software licenses` と入力して、ライセンスを検証します。

ステップ 4 `license activate` と入力して、新しいライセンスを有効化します。

ステップ 5 `reload` と入力して、実際にモジュールをリロードすることを確認して、モジュールをリロードします。

（注）　評価ライセンスは削除できません。

Cisco Unified SIP プロキシサーバーの構成

CUSP ポータル（*http://<cusp module IP>/admin/Common/HomePage.do*）にログインし、以下の順序で Cisco Unified SIP プロキシサーバーを構成します。

ソフトウェア要件	タスク
CUSP の構成	Cisco Unified SIP プロキシの構成 （445 ページ）
ゲートウェイの構成	ゲートウェイの構成 （452 ページ）
Unified CVP の構成	Unified CVP の構成 （453 ページ）
UCDM を介した Unified CallManager の構成	Cisco Unified Communications Manager の構成 （454 ページ）

Cisco Unified SIP プロキシの構成

Unified SIP プロキシを構成するには、以下の手順を実行します。

順序	完了したか	タスク	注意事項
1		ネットワークの構成 （446 ページ）	
2		トリガーの構成 （446 ページ）	
3		サーバーグループの構成 （447 ページ）	
4		ルートテーブルの構成 （448 ページ）	
5		ルートポリシーの構成 （449 ページ）	
6		ルートトリガーの構成 （449 ページ）	

Cisco Unified SIP プロキシの構成詳細については、「Cisco Unified SIP プロキシのフル構成 （450 ページ）」を参照してください。

表 *20 : CUSP* 展開詳細の例

サーバ名（Server Name）	[IPアドレス（IP Address）]	[FQDN]
CUSP	10.10.10.49	cusp.hcsdc1.icm
CVP	10.10.10.10	cvp.hcsdc1.icm
CUCM	10.10.10.30	ccm.hcsdc1.icm
ゲートウェイ	10.10.10.180	gw.hcsdc1.icm

ネットワークの構成

手順

ステップ 1 CUSP ポータルにログインします。

ステップ 2 **[構成（Configure）]** > **[ネットワーク（Networks）]** の順に選択し、**[追加（Add）]** をクリックします。

ステップ 3 ネットワークに一意の名前を入力します。

例：

hcs

ステップ 4 **[タイプ（TYPE）]** ドロップダウンリストで、**[標準（Standard）]** を選択します。

ステップ 5 **[アウトバウンド接続を許可（Allow Outbound Connections）]** を有効化します。

ステップ 6 **[SIPリッスンポイント（SIP Listen Points）]** タブで **[追加（Add）]** をクリックします。

ステップ 7 新しく追加された**ネットワーク**を選択し、**[SIPリッスンポイント（SIP Listen Points）]** タブを選択します。

ステップ 8 **[IPアドレス（IP address）]** ドロップダウンリストで CUSP の IP アドレスを選択します。「表 20 : CUSP 展開詳細の例 （446 ページ）」を参照してください。

ステップ 9 デフォルトポートである 5060 のままにします。

ステップ 10 **[TCP]** として **[転送タイプ（Transport Type）]** を選択したら、**[追加（Add）]** をクリックします。

ステップ 11 **手順 6 ー 8**を繰り返し、UDP として **[転送タイプ（Transport Type）]** を選択したら、**[追加（Add）]** をクリックします。

ステップ 12 **[SIPレコード—ルート（SIP Record-Route）]** を無効化し、コールフローを含む CVP 用のすべてのネットワークを選択し、無効化します。

トリガーの構成

手順

ステップ 1 CUSP ポータルにログインします。

ステップ 2 **[構成（Configure）]** > **[トリガー（Triggers）]** の順に選択し、**[追加（Add）]** をクリックします。

ステップ 3 トリガー名を入力し、**[追加（Add）]** をクリックします。

例：

hcs trigger in

ステップ 4 ドロップダウンリストで適切な**トリガー条件**を選択します。

例：

Inbound Network、

Is exactly および

hcs

ステップ 5 [追加（Add）] をクリックします。

サーバーグループの構成

手順

ステップ 1 CUSP ポータルにログインします。

ステップ 2 **[構成（Configure）]** > **[サーバーグループ（Server Groups）]** > **[グループ（Groups）]** の順に選択します。

ステップ 3 **サーバーグループ**の名前（FQDN）を入力します。

例：

ccm.hcsdc1.icm

ステップ 4 **[ロード バランシングスキーム（Load Balancing Scheme）]** ドロップダウンリストで、**[グローバル（デフォルト）（global (default)）]** を選択します。

ステップ 5 **[ネットワーク（Network）]** ドロップダウンリストで、**hcs** を選択します。

ステップ 6 **[ピングを許可（Pinging Allowed）]** チェックボックスをオンにします。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 新しく追加された**サーバーグループ**を選択して、それぞれのサーバーグループの要素を追加します。

ステップ 9 **[要素（Elements）]** タブを選択し、**[追加（Add）]** をクリックします。

ステップ 10 **<IP Address>** テキストボックスに、サーバーBluetoothの IP アドレスを入力します。「表 20 : CUSP 展開詳細の例 （446 ページ）」を参照してください。

ステップ 11 **[ポート（Port）]** テキストボックスに、ポートの値を入力します。

ステップ 12 **[転送タイプ（Transport Type）]** ドロップダウンリストで、**tcp** を選択します。

ステップ 13 **[Q-Value]** テキストボックスに、Q-Value を `1.0` と入力します。

ステップ 14 **[重み（Weight）]** テキストボックスに重み `10` を入力します。

ステップ 15 [追加（Add）] をクリックします。

ステップ 16 上記の手順を繰り返して、cvp、gateway、ccm サーバーグループを構成します。

ルートテーブルの構成

表 *21 :* ルートテーブルの例

[キー（Key）]	説明	ホスト/サーバーグループ（FQDN）	ネットワーク
4000	エージェントの内線番号	ccm.hcsdc1.icm	hcs
7777	CVP クライアントのネットワーク VRU ラベル	gw.hcsdc1.icm	hcs
8881	Cisco Unified Communications Manager クライアントのネットワーク VRU ラベル	cvp.hcsdc1.icm	hcs
811	ダイヤル番号	cvp.hcsdc1.icm	hcs
912	ポストコール調査のダイヤル番号	cvp.hcsdc1.icm	hcs
9191	呼出音	gw.hcsdc1.icm	hcs
9292	エラー音	gw.hcsdc1.icm	hcs
6661111000	MR クライアントのネットワーク VRU ラベル	cvp.hcsdc1.icm	hcs
978	カスタマーダイヤル番号	out.hcsdc1.icm	hcs

手順

ステップ 1 CUSP ポータルにログインします。

ステップ 2 **[構成（Configure）]** > **[ルートテーブル（Route Tables）]** の順に選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 ルートテーブルの名前を入力し、**[追加（Add）]** をクリックします。

例：

hcs

ステップ 5 各ルートテーブルのルールを追加するには、**[ルートテーブル（Route Table）]** を選択します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 **[キー（Key）]** テキストボックスに、キーを入力します。「表 21 : ルートテーブルの例 （448 ページ）」を参照してください。

ステップ 8 **[ルートタイプ（Route Type）]** ドロップダウンリストで、**[接続先（Destination）]** を選択します。

ステップ 9 **[ホスト/サーバーグループ（Host / Server Group）]** テキストボックスに、ホスト名（FQDN）または IP アドレスを入力します。「表 20 : CUSP 展開詳細の例 （446 ページ）」を参照してください。

ステップ 10 **[ポート（Port）]** テキストボックスに、ポートの値を入力します。

ステップ 11 ドロップダウンリストで、適切な**転送タイプ**を選択します。

ステップ 12 ドロップダウンリストで、適切な**ネットワーク**を選択します。

ルートポリシーの構成

手順

ステップ 1 CUSP ポータルにログインします。

ステップ 2 **[構成（Configure）]** > **[ルートポリシー（Route Policies）]** の順に選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 ルートポリシーの名前を入力し、**[追加（Add）]** をクリックします。

ステップ 5 ドロップダウンリストで **[名前（Name）]** を選択します。

ステップ 6 ドロップダウンリストで **[ルックアップキーの一致（Lookup Key Matches）]** を選択します。

ステップ 7 ドロップダウンリストで **[ルックアップキー（Lookup Key）]** を選択します。

ステップ 8 [追加（Add）] をクリックします。

ルートトリガーの構成

手順

ステップ 1 CUSP ポータルにログインします。

ステップ 2 **[構成（Configure）]** > **[ルートトリガー（Route Triggers）]** の順に選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 ドロップダウンリストで、**[ルーティングトリガー（Routing Trigger）]** を選択します。

ステップ 5 ドロップダウンリストで、**[トリガー（Trigger）]** を選択します。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 新しく追加した**トリガー**を選択し、トリガー条件を追加します。

ステップ 8 ドロップダウンリストで、**[トリガー条件（Trigger Condition）]** を選択します。

ステップ 9 [追加（Add）] をクリックします。

Cisco Unified SIP プロキシのフル構成

```
cusp(cusp)# show configuration active ver
cusp(cusp)# show configuration active verbose
Building CUSP configuration...
!
server-group sip global-load-balance call-id
server-group sip retry-after 0
server-group sip element-retries udp 2
server-group sip element-retries tls 1
server-group sip element-retries tcp 1
sip dns-srv
 enable
 no naptr
 end dns
!
no sip header-compaction
no sip logging
!
sip max-forwards 70
sip network hcs standard
 no non-invite-provisional
 allow-connections
 retransmit-count invite-client-transaction 3
 retransmit-count invite-server-transaction 5
 retransmit-count non-invite-client-transaction 3
 retransmit-timer T1 500
 retransmit-timer T2 4000
 retransmit-timer T4 5000
 retransmit-timer TU1 5000
 retransmit-timer TU2 32000
 retransmit-timer clientTn 64000
 retransmit-timer serverTn 64000
 tcp connection-setup-timeout 0
 udp max-datagram-size 1500
 end network
!
sip overload reject retry-after 0
!
no sip peg-counting
!
sip privacy service
sip queue message
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue radius
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue request
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue response
```

```
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 20
 end queue
!
sip queue st-callback
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 10
 end queue
!
sip queue timer
 drop-policy none
 low-threshold 80
 size 2500
 thread-count 8
 end queue
!
sip queue xcl
 drop-policy head
 low-threshold 80
 size 2000
 thread-count 2
 end queue
!
route recursion
!
sip tcp connection-timeout 30
sip tcp max-connections 256
!
no sip tls
!
sip tls connection-setup-timeout 1
!
trigger condition hcs_trigger_in
 sequence 1
  in-network ^\Qhcs\E$
  end sequence
 end trigger condition
!
trigger condition hcs_trigger_out
 sequence 1
  out-network ^\Qhcs\E$
  end sequence
 end trigger condition
!
trigger condition mid-dialog
 sequence 1
  mid-dialog
  end sequence
 end trigger condition
!
accounting
 no enable
 no client-side
 no server-side
 end accounting
!
server-group sip group ccm.hcsdc1.icm hcs
 element ip-address 10.10.10.31 5060 tcp q-value 1.0 weight 10
 element ip-address 10.10.10.131 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
```

```
 lbtype global
 ping
 end server-group
!
server-group sip group cvp.hcsdc1.icm hcs
 element ip-address 10.10.10.10 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
!
server-group sip group gw.hcsdc1.icm hcs
 element ip-address 10.10.10.180 5060 tcp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
!
route table hcs
 key 4000 target-destination ccm.hcsdc1.icm hcs
 key 77777 target-destination gw.hcsdc1.icm hcs
 key 8881 target-destination cvp.hcsdc1.icm hcs
 key 91100 target-destination cvp.hcsdc1.icm hcs
 end route table
!
policy lookup hcs_policy
 sequence 100 hcs request-uri uri-component user
  rule prefix
  end sequence
 end policy
!
trigger routing sequence 1 by-pass condition mid-dialog
trigger routing sequence 3 policy hcs_policy condition hcs_trigger_out
trigger routing sequence 4 policy hcs_policy condition mid-dialog
trigger routing sequence 5 policy hcs_policy condition hcs_trigger_in
!
server-group sip ping-options hcs 10.10.10.49 4000
 method OPTIONS
 ping-type proactive 5000
 timeout 2000
 end ping
!
server-group sip global-ping
sip cac session-timeout 720
sip cac hcs 10.10.10.10 5060 tcp limit -1
sip cac hcs 10.10.10.131 5060 tcp limit -1
sip cac hcs 10.10.10.180 5060 tcp limit -1
sip cac hcs 10.10.10.31 5060 tcp limit -1
!
no sip cac
!
sip listen hcs tcp 10.10.10.49 5060
sip listen hcs udp 10.10.10.49 5060
!
call-rate-limit 200
!
end
cusp(cusp)#
```

ゲートウェイの構成

• CUSP IP を使用した SIP サーバーの作成 （453 ページ）

• ダイヤルピアの作成 （453 ページ）

CUSP IP を使用した SIP サーバーの作成

```
sip-ua
 retry invite 2
 retry bye 1
 timers expires 60000
 timers connect 1000
 sip-server ipv4:10.10.10.49:5060
 reason-header override
```

ダイヤルピアの作成

```
dial-peer voice 9110 voip
 description Used for CUSP
 preference 1
 destination-pattern 911T
 session protocol sipv2
 session target sip-server
 session transport tcp
 voice-class codec 1
 dtmf-relay rtp-nte
 no vad
```

Unified CVP の構成

• SIP プロキシの構成 （453 ページ）
• SIP サーバーグループの構成 （453 ページ）
• コールサーバーの構成 （454 ページ）

SIP プロキシの構成

手順

ステップ 1 Unified Customer Voice Portal にログインします。

ステップ 2 **[デバイス管理（Device Management）]** > **[SIPプロキシサーバー（SIP Proxy Server）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

ステップ 3 IP アドレスとホスト名を入力します。**[デバイスタイプ（Device Type）]** ドロップダウンリストで **[Cisco Unified SIPプロキシ（Cisco Unified SIP Proxy）]** を選択します。

ステップ 4 [保存（Save）] をクリックします。

SIP サーバーグループの構成

手順

ステップ 1 Unified Customer Voice Portal にログインします。

ステップ 2 **[システム（System）]** > **[SIPサーバーグループ（SIP Server Groups）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

ステップ 3 FQDN の名前、IP アドレス、ポート、優先順位、CUSP の重みを入力し、**[追加（Add）]** をクリックします。

ステップ 4 [保存（Save）] をクリックします。

コールサーバーの構成

手順

ステップ 1 Unified Customer Voice Portal にログインします。

ステップ 2 **[デバイス管理（Device Management）]** > **[コールサーバー（Call Server）]** の順に選択します。

ステップ 3 **[コールサーバー（Call Server）]** > **[編集をクリック（Click Edit）]** > **[SIPをクリック（Click SIP）] タブ** の順に選択します。

ステップ 4 **[はい（Yes）]** を選択して、アウトバウンド プロキシ サーバーを有効にします。

ステップ 5 **Outbound SRV domain name / Server Group Name (FQDN)** と入力し、**[保存して展開（Save and Deploy）]** をクリックします。

（注） CUSP は集中型ダイヤルプランを提供するため、既存のダイヤル番号パターンを削除します。

Cisco Unified Communications Manager の構成

Unified Communications Domain Manager 管理インターフェイスにログインし、以下の手順を実行して Unified CUSP サーバーへのルート構成を完了します。

- CVP にトランクを追加 （454 ページ）
- CUSP にトランクを追加 （455 ページ）

CVP にトランクを追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[SIP トランク（SIP Trunks）]** に移動します。

- プロバイダまたはリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[SIP トランク（SIP Trunks）]** の順に選択します。
- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[SIP トランク（SIP Trunks）]** の順に選択します。

ステップ 4 **[追加（Add）]** をクリックし、トランクを作成します。

ステップ 5 **[デバイス情報（Device Information）]** タブで、以下の手順を実行します。

a) SIP トランクを追加する **[Cisco Unified Communications Manager]** ドロップダウンリストから必要な IP アドレスを選択します。
b) **[デバイス名（Device Name）]**フィールドに固有の SIP トランク名を入力します。
c) ドロップダウンリストで、**[デバイスプール（Device Pool）]** を選択します。
d) **[すべてのアクティブな Unified CM ノードを実行する（Run On All Active Unified CM Nodes）]** チェックボックスをオンにします。

ステップ 6 **[SIP 情報（SIP Info）]** タブに移動し、以下を実行します。

a) **[接続先（Destination）]** パネルで **[追加（Add）]** アイコンをクリックします。
b) **[アドレス IPv4（Address IPv4）]** フィールドに宛先 IP アドレスを入力します。
c) **ポート**を 5090 に変更します。
d) 複数の接続先を優先順位付けするには、**[ソート順（Sort Order）]** を入力します。

（注） 値が小さいほど、優先順位が高くなります。

e) ドロップダウンリストで、新しく追加された **SIP トランク セキュリティ プロファイル**を選択します。
f) ドロップダウンリストで、**sip profile** を選択します。

別のトランクを追加するには、この手順を繰り返します。

ステップ 7 [保存（Save）] をクリックします。

CUSP にトランクを追加

手順

ステップ 1 プロバイダ、リセラー、またはカスタマー管理者として Cisco Unified Communication Domain Manager にログインします。

ステップ 2 Unified Communication Manager が構成されているノードに階層が設定されていることを確認します。

ステップ 3 **[SIP トランク（SIP Trunks）]** に移動します。

- プロバイダまたはリセラー管理者の場合は、**[デバイス管理（Device Management）]** > **[CUCM]** > **[SIP トランク（SIP Trunks）]** の順に選択します。

- カスタマー管理者の場合は、**[デバイス管理（Device Management）]** > **[詳細設定（Advanced）]** > **[SIP トランク（SIP Trunks）]** の順に選択します。

ステップ 4 **[追加（Add）]** をクリックし、トランクを作成します。

ステップ 5 **[デバイス情報（Device Information）]** タブで、以下の手順を実行します。

a) SIP トランクを追加する **[Cisco Unified Communications Manager]** ドロップダウンリストで必要な IP アドレスを選択します。
b) **[デバイス名（Device Name）]**フィールドに固有の SIP トランク名を入力します。
c) ドロップダウンリストで、**[デバイスプール（Device Pool）]** を選択します。
d) **[すべてのアクティブなUnified CMノードで実行（Run on All Active Unified CM Nodes）]** チェックボックスをオンにします。

ステップ 6 **[SIP情報（SIP Info）]** タブに移動し、以下を実行します。

a) **[接続先（Destination）]** パネルで **[追加（Add）]** アイコンをクリックします。
b) **[アドレスIPv4（Address IPv4）]** フィールドに CUSP の宛先 IP アドレスを入力します。
c) 必要に応じて**ポート**を変更します。
d) 複数の接続先を優先順位付けするには、**[ソート順（Sort Order）]** を入力します。

（注） 値が小さいほど、優先順位が高くなります。

e) ドロップダウンリストで、新しく追加された**SIP トランク セキュリティ プロファイル**を選択します。
f) ドロップダウンリストで、**sip profile** を選択します。

別のトランクを追加するには、この手順を繰り返します。

ステップ 7 [保存（Save）] をクリックします。

Cisco Unified SIP プロキシを使用したアウトバウンドの構成

設定 Unified CCE

手順

ステップ 1 **[スタート（Start）]**>**[すべてのプログラム（All programs）]**>**[Cisco Unified CCEツール（Cisco Unified CCE Tools）]** > **[周辺機器ゲートウェイの設定（Peripheral Gateway Setup）]** の順に選択します。

ステップ 2 **[インスタンスコンポーネント（Instance Component）]** で **[追加（Add）]** をクリックし、**[アウトバウンドダイヤラ（Outbound Dialer）]** をクリックしてダイヤラを追加します。

ステップ 3 **アウトバウンドダイヤラのプロパティ**ページで、**[SIP]** ラジオボタンが選択されていることを確認し、**[次へ（Next）]**をクリックします。

ステップ 4 **[SIPダイヤラ名（SIP Dialer Name）]**テキストボックスにある、**[構成マネージャ（Configuration Manager）]** の **[ダイヤラツール（Dialer Tool）]** で設定されている SIP ダイヤラ名と同じ SIP ダイヤラ名を正確に入力します。

ステップ 5 **[SIPサーバータイプ（SIP Server Type）]** で、**(CUSP)/(CUBE)** が選択されていることを確認します。

ステップ 6 **[SIPサーバー（SIP Server）]**テキストボックスに **CUSP IP** と入力し、**[次へ（Next）]** をクリックします。

ステップ 7 **[Campaign Managerサーバー（Campaign Manager Server）]**テキストボックスに、**Unified CCE DataserverA /RoggerA サイドの IP** アドレスを入力します。

ステップ 8 **[CTIサーバーA（CTI Server A）]** テキストボックスに、**A サイド CTIOS サーバー IP アドレス**を入力します。 **[CTIサーバーポートA（CTI Server Port A）]** テキストボックスにポート番号として **42027** を入力します。

ステップ 9 **[CTIサーバーB（CTI Server B）]** テキストボックスに、**B サイド CTIOS サーバー IP アドレス**を入力します。 **[CTIサーバーポートB（CTI Server Port A）]** テキストボックスに、ポート番号として **43027** を入力します。

ステップ 10 他のフィールドはすべて**デフォルト値**のままとし、**[次へ（Next）]** をクリックします。次のウィンドウで、**[次へ（Next）]** をクリックしてインストールを完了します。

ゲートウェイの構成

```
dial-peer voice 811 voip
 description ******To CUCM*****
 destination-pattern 811T
 session protocol sipv2
 session target sip-server
 voice-class codec 1
 voice-class sip rel1xx supported "100rel"
 dtmf-relay rtp-nte h245-signal h245-alphanumeric
 no vad
!

 sip-ua
retry invite  2
retry bye 1
timers expires 60000
timers connect 1000
sip-server dns:out.hcsdc1.icm
reason header override
permit hostname dns:out.hcsdc1.icm
```

IVR ベースキャンペーン用の Cisco Unified SIP プロキシの構成

手順

ステップ 1 CUSP ポータルにログインします。

ステップ 2 **[構成（Configure）] > [ルートテーブル（Route Tables）]** の順に選択します。

ステップ 3 既存のルートテーブルをクリックします。

例：

HCS.

ステップ 4 各ルートテーブルのルールを追加するには、[ルートテーブル（Route Table）] を選択します。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 **[キー（Key）]** テキストボックスに、key, 8881 と入力します。

ステップ 7 **[ルートタイプ（Route Type）]** ドロップダウンリストで **[接続先（Destination）]** を選択します。

ステップ 8 **[ホスト/サーバーグループ（Host / Server Group）]** テキストボックスに、CVPのホスト名（FQDN）または IP アドレスを入力します。

例：

cvp.hcsdc1.icm

ステップ 9 **[ポート（Port）]** テキストボックスに、ポートの値を入力します。

ステップ 10 ドロップダウンリストで、適切な**転送タイプ**を選択します。

ステップ 11 ドロップダウンリストで、適切な**ネットワーク**を選択します。

（注） CUSP は集中型ダイヤルプラン管理を提供するため、IVR コールを CVP に直接ルーティングできます。

Avaya PG

4000 および 12000 エージェント導入モデルの場合は、以下の手順を実行します。

- Avaya PG 用ゴールデンテンプレートの作成 （458 ページ）
- Avaya PG の構成 （460 ページ）

Avaya PG 用ゴールデンテンプレートの作成

Avaya PG のゴールデンテンプレートを作成するには、以下の一連のタスクに従います。各タスクの後で、このページに戻ってそのタスクを「完了」としてマークしたら、次の手順に進みます。

順序	完了したか	タスク	注意事項
1		UCCE_11.6_Win2012_vmv9_v1.0.ova のダウンロード UCCE_12.0_Win2016_vmv11_v1.1.OVA のダウンロード	OVA ファイルのダウンロード（392ページ）を参照してください。
2		Unified CCE Avaya PG の仮想マシンを作成します。	仮想マシンの作成 （392 ページ）の手順を実行します。
3		Microsoft Windows Server のインストール	Microsoft Windows Server のインストール （393ページ）の手順を実行します。
4		ウイルス対策ソフトウェアのインストール	ウイルス対策ソフトウェアのインストール （28ページ）の手順を実行します。
5		Unified Contact Center Enterprise のインストール	Unified Contact Center Enterprise のインストール （459ページ）の手順を実行します。
6		仮想マシンをテンプレートに変換します。	仮想マシンをゴールデンテンプレートに変換 （397ページ）の手順を実行します。

すべてのゴールデンテンプレートの作成後、自動化プロセス（自動化クローニングと OS のカスタマイズ （2 ページ））を実行できます。自動化プロセスの実行後、接続先システムで Avaya PG サーバーを構成できます。「Avaya PG の構成 （460 ページ）」を参照してください。

Unified Contact Center Enterprise のインストール

手順

ステップ 1 仮想マシンテンプレートをドメインに追加します。

ステップ 2 Unified Contact Center Enterprise ISO イメージを仮想マシンにマウントします。

ステップ 3 ICM-CCE-CCH インストーラーディレクトリから、setup.exe を実行し、InstallShield の手順に従います。

ステップ 4 **[インストール方法を選択（Select the installation method）]** ウィンドウで、**Fresh Install** を選択したら、**[次へ（Next）]** をクリックします。

ステップ 5 **[メンテナンスリリース（MR）（Maintenance Release (MR)）]** ウィンドウの **[メンテナンスリリースロケーション（Maintenance Release Location）]**フィールドを空欄西、**[次へ（Next）]** をクリックします。

ステップ 6 **[インストールロケーション（Installation Location）]** ウィンドウで、ドライブ c を選択したら、**[次へ（Next）]** をクリックします。

ステップ 7 **[ファイルのコピー準備完了（Ready to Copy Files）]** ウィンドウで、**[インストール（Install）]** をクリックします。

ステップ 8 **[インストールの完了（Installation Complete）]** ウィンドウで、**[はい、今すぐコンピュータを再起動します（Yes、I want to restart your computer now）]** > **[完了（Finish）]** の順に選択します。

ステップ 9 Windows Server 2016 で PCCE または UCCE 12.0(1) を新規インストールまたはテクノロジーリフレッシュアップグレードする場合は、ES を適用する前に必須の更新を実行します。新規インストール/テクノロジーリフレッシュに対する CCE 12.0 必須の更新 は、https://software.cisco.com/download/home/268439622/type/280840583/release/12.0(1) からダウンロードできます。

ステップ 10 必要に応じて、Unified Contact Center Enterpriseメンテナンスリリースを適用します。

ステップ 11 Unified Contact Center Enterprise ISO イメージをアンマウントします。

ステップ 12 仮想マシンテンプレートをワークグループに戻します。

Avaya PG の構成

このセクションでは、Avaya PG で実行する構成手順について説明します。

順序	完了したか	タスク	注意事項
1		ネットワークカードの構成	ネットワークカードの構成（31 ページ）の手順を実行します。
2		ドメイン内マシンの検証	ドメイン内マシンの検証（33 ページ）の手順を実行します。
3		Unified CCE 暗号化ユーティリティの構成	Unified CCE 暗号化ユーティリティの構成（35 ページ）の手順を実行します。
4		構成マネージャから Avaya PG を追加	Avaya PG の追加（461 ページ）の手順を実行します。
5		Avaya PG の設定	Avaya PG の設定（462 ページ）の手順を実行します。
6		CTI サーバーの構成	CTI サーバーの構成（54 ページ）の手順を実行します。

順序	完了したか	タスク	注意事項
7		CTI OS サーバーの構成	CTI OS サーバーの構成 （464 ページ）の手順を実行します。
8		Avaya ACD の構成	https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/e9288eff-12af-4b91-b9f7-2c28528860cf にある「*Supplement for Avaya* コミュニティマネージャ用 *Cisco Unified ICM ACD* サプリメント」の「*ACD* 構成」と「*Unified ICM* ソフトウェア構成」セクションの手順に従います。
9		Cisco Diagnostic Framework Portico の検証	Cisco Diagnostic Framework Portico の検証 （56 ページ）の手順を実行します。
10		Cisco SNMP の設定	Cisco SNMP の設定 （56 ページ）の手順を実行します。

Avaya PG の追加

Unified CCE 構成マネージャを使用してAvaya PG を追加するには、以下の手順を実行します。

手順

ステップ 1 Unified CCE Admin Workstation サーバーにログインし、**[スタート（Start）]** > **[Cisco Unified CCEツール（Cisco Unified CCE Tools）** > **[管理ツール（Administration Tools）]** > **[構成マネージャ（Configuration Manager）]** の順に選択します。

ステップ 2 **[ツール（Tools）]**>**[エクスプローラツール（Explorer Tools）]** の順に選択し、**[構成マネージャ（Configuration Manager）]** ウィンドウの **PG Explorer** を開きます。

ステップ 3 **[PGの追加（Add PG）]** をクリックし、**[ロジカルコントローラ（Logical Controller）]** ペインに次の値を入力します。

a) **[周辺機器名（Peripheral Name）]** フィールドに、 *Avaya_PG_XX* と入力します。XX は Avaya PG 番号に置き換えてください。

b) **[クライアントタイプ（Client Type）]** フィールドで、**Avaya (Definity)** を選択します。

ステップ 4 **[周辺機器（Peripheral）]** をクリックして表示される **[周辺機器（Peripheral）]** タブで、以下の値を入力します。

a) **[デフォルトデスク設定（Default Desk Settings）]** フィールドで **[None]** を選択します。
b) **[ポストルーティングの有効化（Enable post routing）]** をオンにします。

ステップ 5 **[ルーティングクライアント（Routing Client）]** タブをキリックし、ルーティングクライアントの名前を入力します。

ステップ 6 **[保存（Save）]** > **[閉じる（Close）]** の順に選択します。

Avaya PG の設定

手順

ステップ 1 **[スタート（Start）]** > **[すべてのプログラム（All programs）]** > **[Cisco Unified CCE ツール（Cisco Unified CCE Tools）]** > **[周辺機器ゲートウェイの設定（Peripheral Gateway Setup）]** の順に選択します。

ステップ 2 **[インスタンスコンポーネント（Instance Components）]** ペインで、**[追加（Add）]** をクリックし、**[周辺機器ゲートウェイ（Peripheral Gateway）]** を選択します。

ステップ 3 **[周辺機器ゲートウェイプロパティ（Peripheral Gateway Properties）]** ダイアログボックスで、以下を選択します。

a) **[生産モード（Production Mode）]** をオンにします。
b) **[システム起動自動開始（Auto start system startup）]** をオンにします。
c) **[デュプレックス周辺機器ゲートウェイ（Duplexed Peripheral Gateway）]** をオンにします。
d) [PGノードプロパティID（PG node Properties ID）] ドロップダウンリストで適切な PG を選択します。
e) 該当するサイド（**サイド A** または**サイド B**）を適宜選択します。
f) [クライアントタイプ（Client Type）] ペインで、選択したタイプに **Avaya（Definity）** を追加します。
g) **[次へ（Next）]** をクリックします。

PIM1（Avaya PIM）の追加

手順

ステップ 1 **[周辺機器ゲートウェイ構成（Peripheral Gateway Configuration）]** ペインにロジカルコントローラ ID を入力します。

ステップ 2 **[EAS-PHDモード（EAS-PHD Mode）]** を選択し、**[Avaya（Definity）ECS設定（Avaya (Definity)ECS Setting）]** ペインで **[MAPDを使用（Using MAPD）]** チェックボックスをオンにします。

ステップ 3 **[周辺機器インターフェイスマネージャ（Peripheral Interface Manager）]** ペインで、**[追加（Add）]** をクリックします。

ステップ 4 **Avaya(Definity)** と **PIM1** を選択し、**[OK]** をクリックします。

ステップ 5 **[Avaya(Definity) ECS PIM構成（Avaya(Definity) ECS PIM Configuration）]** ダイアログボックスで、**[有効化（Enabled）]** をオンにします。

ステップ 6 **[周辺機器名（Peripheral Name）]** フィールドに周辺機器名を入力します。

ステップ 7 **[周辺機器ID（Peripheral ID）]** フィールドに周辺機器 ID を入力します。

ステップ 8 **[CMSを有効化（CMS Enabled）]** をオンにし、**[通話管理システム（CMS）構成（Call Management System (CMS) Configuration）]** ペインにある **[リッスンするポート番号（Port number to listen on）]** フィールドにポート番号を入力します。

ステップ 9 **[CVLAN/MAPD構成（CVLAN/MAPD Configuration）]** ペインで、**[Host1]** に対して **[Enabled（有効化）]** をオンにします。

ステップ 10 ASAI リンクの**ホスト名**を入力したら、**Monitor ASAI** リンクと **Post-Route ASAI** リンクに対して構成した ASAI リンク番号を確認します。

ステップ 11 **OK** をクリックし、**Next** をクリックします。

ステップ 12 **[デバイス管理プロトコルプロパティ（Device Management Protocol Properties）]** ダイアログボックスで優先するサイドを選択します。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 **[周辺機器ゲートウェイネットワークインターフェイス（Peripheral Gateway Network Interfaces）]** ダイアログボックスで、[PG Private Interfaces] および [PG Public (Visible) Interfaces] と入力します。

ステップ 15 サイド A のプライベート インターフェイス セクションの [QoS] ボタンをクリックし、**[QoSの有効化（Enable QoS）]** をオンにしたら、**[OK]** をクリックします。

この手順は、サイド A にのみ適用します。

ステップ 16 サイド A のパブリック インターフェイス セクションの [QoS] ボタンをクリックし、**[QoSの有効化（Enable QoS）]** をオンにしたら、**[OK]** をクリックします。

この手順は、サイド A にのみ適用します。

ステップ 17 **[次へ（Next）]** > **[完了（Finish）]** の順に選択します。

（注） すべての ICM コンポーネントがインストールされるまで Unified **ICM/CCNodeManager** を起動しないでください。

CTI OS サーバーの構成

手順

ステップ 1 エージェント PG を使用した Unified CCE マシン m p ローカルドライブに CTI OS ISO イメージをマウントするか、CTI OS インストーラをコピーします。に移動します。

ステップ 2 CTI OS のメンテナンスリリースがある場合、のローカルドライブにメンテナンスリリースをコピーします。

ステップ 3 **%Home\CTIOS\Installs\CTIOS Server** に移動し、setup.exe を実行します。サービスがいったん停止し、インストール完了後に再開するという内容の警告に対して、**[はい（Yes）]** をクリックします。

ステップ 4 ソフトウェア ライセンス契約を受諾します。

ステップ 5 最新のメンテナンスリリースがある場合は、その場所を参照します。[次へ（Next）] をクリックします。

ステップ 6 [CTI OSインスタンス（CTI OS Instance）] ダイアログボックスで、[CTI OSインスタンス リスト（CTI OS Instance List）] ペインをクリックします。[CTIOSサーバーインスタンスの追加（Add CTIOS Server Instance）] ウィンドウで、インスタンス名を入力し、**[OK]** をクリックします。

（注） CTIOS インスタンス名は ICM インスタンス名と一致する必要があります。一致しない場合、Diagnostics portico に反映されません。

ステップ 7 [CTI OSサーバーリスト（CTI OS Server List）] ペインで **[追加（Add）]** をクリックし、**[OK]** をクリックします。

ステップ 8 [デスクトップドライブの入力（Enter Desktop Drive）] ダイアログボックスで、ドライブ C を選択したら、**[OK]** をクリックします。

ステップ 9 [CTIサーバー情報（CTI Server Information）] ダイアログボックスで、CTI サーバーがインストールされている Unified CCE マシンの IP アドレスを入力し、サイド A には、**42027** のポート番号を、サイド B には、**43027** のポート番号を入力します。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [周辺機器ID（Peripheral Identifier）] ダイアログボックスで、以下の値を入力し、**[次へ（Next）]** をクリックします。

a) 各 PG の周辺機器 ID を入力します。
b) Avaya PG の周辺機器津として **G3** を選択します。
c) **[エージェントID（Agent ID）]** を選択します。

ステップ 12 [接続情報（Connect Information）] ダイアログボックスで、リッスンポート **42028** を入力し、すべてのデフォルト値をそのままにしたら、**[次へ（Next）]** をクリックします。

ステップ 13 [統計情報（Statistics Information）] ダイアログボックスで、**[通話終了時にエージェント統計情報についてポーリング（Polling for Agent Statistics at End Call）]** をオンにし、**[次へ（Next）]** をクリックします。

ステップ 14 [IPCC Silent Monitor Type] ダイアログボックスで、Silent Monitor Type を **CCM Based** に設定したら、**[次へ（Next）]** をクリックします。

ステップ 15 [ピアCTI OSサーバー（Peer CTI OS Server）] ダイアログボックスで、以下のように構成します。

a) **[デュプレックスCTIOSインストール（Duplex CTIOS Install）]** をオンにします。

b) [CTIOS サーバー（CTIOS Server）] フィールドで、デュプレックス構成の他方の *CTIOS* サーバーのホスト名/*IP* アドレスを入力します。

c) [ポート（Port）] フィールドに、**42028** と入力します。

ステップ 16 [完了（Finish）] をクリックします。

ステップ 17 [Cisco CTI OS サーバーセキュリティ（Cisco CTI OS Server Security）] ダイアログボックスで、**[セキュリティの有効化（Enable Security）]** をオフにします。[OK] をクリックします。

ステップ 18 [CTI OSセキュリティ（CTI OS Security）] の ダイアログボックスで、**[完了（Finish）]** をクリックします。

ステップ 19 コンピュータを再起動することを要求するプロンプトが表示されたら、[はい（Yes）] をクリックします。メンテナンスリリースがある場合は、そのインストールが自動的に始まります。

ステップ 20 メンテナンスリリースがある場合は、画面の指示に従ってインストールします。

ステップ 21 メンテナンスリリースのインストールが完了したら、**[完了（Finish）]** をクリックし、プロンプトに従って再起動します。

ステップ 22 **[スタート（Start）] > [実行（Run）] > [regedit]** の順に選択し、Registry Editor にアクセスします

ステップ 23 **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,Inc.\Ctios\CTIOS_<instance name>\CTIOS1\Server\Agent** に移動します。

ステップ 24 **forceLogoutOnSessionClose** を **1** に設定します。

Avaya の変換ルート

変換ルートは、コールの一時的な接続先であり、コールとともにコール情報を配信できます。ネットワークブラインド転送は、送信元 CVP ルーティングクライアントに接続先ラベルを返すために使用されます。

Unified CCE の構成

ネットワーク優先転送の有効化

Avaya、CVP、および Cisco Unified Communications Manager PIM に対して以下の手順を実行します。

手順

ステップ 1 Unified CCE Admin Workstation サーバーで、**[スタート（Start）]** > **[Cisco Unified CCEツール（Cisco Unified CCE Tools）]** > **[管理ツール（Administration Tools）]** > **[構成マネージャ（Configuration Manager）]** の順に選択します。

ステップ 2 **[ツール（Tools）]** > **[エクスプローラツール（Explorer Tools）]** > **[PGエクスプローラ（PG Explorer）]** の順に選択します。

ステップ 3 リストから適切な PG を選択し、PG を展開します。

ステップ 4 リストから適切な PIM を選択します。

ステップ 5 **[ルーティングクライアント（Routing Client）]** タブに移動し、**[ネットワーク転送優先（Network Transfer Preferred）]** チェックボックスをオンにします。

サービスの作成

手順

ステップ 1 Unified CCDM ポータルにテナントまたはサブカスタマーとしてログインします。

ステップ 2 **[リソースマネージャ（Resource Manager）]** を選択します。

ステップ 3 左側のパネルからサービスを作成するフォルダを選択します。

ステップ 4 **[リソース（Resource）]** ドロップダウンリストで **[サービス（Service）]** を選択します。

ステップ 5 **名前** を入力します。

ステップ 6 **[周辺機器（Peripheral）]** ドロップダウンリストで適切な Avaya 周辺機器を選択します。

ステップ 7 **[詳細（Advanced）]** タブにある **[メディアルーティングドメイン（Media Routing Domain）]** ドロップダウンリストで **Cisco_Voice** を選択します。

ステップ 8 [保存（Save）] をクリックします。

変換ルートの構成

手順

ステップ 1 Unified CCE Admin Workstation サーバーで、**[スタート（Start）]** > **[Cisco Unified CCEツール（Cisco Unified CCE Tools）]** > **[管理ツール（Administration Tools）]** > **[構成マネージャ（Configuration Manager）]** の順に選択します。

ステップ 2 **[ツール（Tools）]** > **[エクスプローラツール（Explorer Tools）]** > **[変換ルートエクスプローラ（Translation Route Explorer）]** の順に選択します。

ステップ 3 **[変換ルート（Translation Route）]** タブで、以下の手順を実行します。

a) **名前** を入力します。

b) **[タイプ（Type）]** ドロップダウンリストで、**DNIS** を選択します。

ステップ 4 [ルートを追加（Add Route）] をクリックします。

ステップ 5 **[ルート（Route）]** タブで、以下の手順を実行します。

a) **名前** を入力します。

b) **[サービス（Service）]** ドロップダウンリストで新しく作成したサービスを選択します。

ステップ 6 **[周辺機器ターゲットを追加（Add Peripheral Target）]** をクリックします。

ステップ 7 **[周辺機器ターゲット（Peripheral Target）]** タブで、以下の手順を実行します。

a) **DNIS** と入力します。

（注） DNIS はラベルと同じである必要があります。

b) ドロップダウンリストで、**[ネットワークトランクグループ（Network Trunk Group）]** を選択します。

ステップ 8 [ラベルの追加（Add Label）] をクリックします。

ステップ 9 **[ラベル（ Label）]** タブで、以下の手順を実行します。

a) ドロップダウンリストで **[ルーティングクライアント（Routing Client）]** を選択します。

b) **ラベル**を入力します

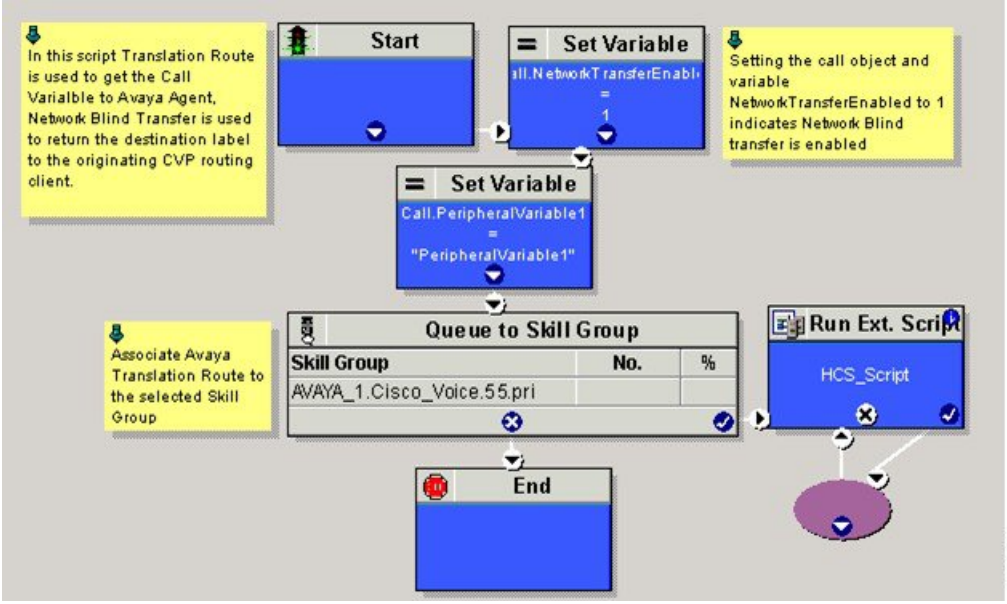
（注） ポストルート VDN は、CVP ルーティングクライアントのラベルとして作成する必要があります。

ステップ 10 [保存（Save）] をクリックします。

スクリプトの構成

次の図では、スクリプトの構成方法に関して説明します。

図 *21* : 設定スクリプト



シスコ仮想化音声ブラウザ

- シスコ仮想化音声ブラウザ用ゴールデンテンプレートの作成 （468 ページ）
- Unified CVP の構成 （469 ページ）
- シスコ仮想化音声ブラウザの構成 （470 ページ）

シスコ仮想化音声ブラウザ用ゴールデンテンプレートの作成

次の手順に従ってタスクを実行し、音声ブラウザのゴールデンテンプレートを作成します。各タスクの後で、このページに戻ってそのタスクを「完了」としてマークしたら、次の手順に進みます。

順序	完了したか	タスク	注意事項
1		VVB_12.0_vmv11_v2.5.ova のダウンロード VB_11.0_vmv8_v2.5.ova のダウンロード VVB_11.6_vmv8_v2.5.ova のダウンロード	OVA ファイルのダウンロード （392 ページ）を参照してください。

2		シスコ仮想化音声ブラウザの仮想マシンを作成します。	仮想マシンの作成（392 ページ）の手順を実行します。
3		シスコ仮想化音声ブラウザをインストールします。	ゴールデンテンプレートの VOS アプリケーションのインストール手順は以下のとおりです。、 OS ベースアプリケーションのインストール （420 ページ）を参照してください。
4		仮想マシンをゴールデンテンプレートに変換します。	仮想マシンをゴールデンテンプレートに変換（397 ページ）の手順を実行します。

すべてのゴールデンテンプレートを作成したら、以下の手順を実行します。

手順

ステップ 1 自動化プロセスを実行します。 自動化クローニングと OS のカスタマイズ （2 ページ）を参照してください。

ステップ 2 シスコ仮想化音声ブラウザを構成します。「シスコ仮想化音声ブラウザの構成（470ページ）」を参照してください。

Unified CVP の構成

- シスコ仮想化音声ブラウザの追加 （469 ページ）
- ダイヤル番号パターンの関連付け （470 ページ）

シスコ仮想化音声ブラウザの追加

手順

ステップ 1 CVP オペレーションコンソールにログインします。

ステップ 2 **[デバイス管理（Device Management）] > [ゲートウェイ（Gateway）] > [仮想化音声ブラウザ（Virtualized Voice Browser）]** の順に選択します。

ステップ 3 シスコ仮想化音声ブラウザのIPアドレスとホスト名を入力します。

ステップ 4 **[グループID（Group ID）]** フィールドでは、デフォルトのトランクオプションのままにします。
ステップ 5 **ユーザー名**と**パスワード**を入力します。
ステップ 6 **[パスワードの有効化（Enable Password）]** を入力します。
ステップ 7 **[ポート（Port）]** フィールドは、デフォルトのオプションのままにします。
ステップ 8 [サインイン（Sign In）] をクリックします。
ステップ 9 [保存（Save）] をクリックします。

ダイヤル番号パターンの関連付け

手順

ステップ 1 CVP オペレーションコンソールにログインします。
ステップ 2 **[システム（System）]**>**[ダイヤル番号パターン（Dialed Number Pattern）]** の順に選択します。
ステップ 3 リストで関連付ける**ダイヤル番号パターン**を選択します。
ステップ 4 **[ルートからデバイス（Route to Device）]** ドロップダウンリストで、[シスコ仮想化音声ブラウザIP（Cisco Virtualized Voice Browser IP）] を選択します。
ステップ 5 [保存（Save）] をクリックします。
ステップ 6 [展開（Deploy）] をクリックします。

シスコ仮想化音声ブラウザの構成

仮想化 VB 管理 Web インターフェイスへのアクセス

Cisco Virtualized VB Administration Web インターフェイスの Web ページでは、仮想化 VB システムとそのサブシステムを構成および管理できます。

次の手順に従ってサーバーに移動し、仮想化 VB 管理 Web インターフェイスにログインします。

手順

ステップ 1 Webブラウザからシスコ仮想化音声ブラウザ管理認証ページを開き、大文字小文字を区別した *https://<servername>/appadmin* の URL を入力します。

この場合、*<servername>* をホスト名または必要な仮想化 VB サーバーの IP アドレスに置き換えます。

[セキュリティアラート（Security Alert）] ダイアログボックスが表示されます。

ステップ 2 ログイン情報を使用して、**Cisco Virtualized VB Administration** にログインします。

（注）
- 始めて Virtualized VB にアクセスする場合、Virtualized VB のインストール中に指定したアプリケーションユーザーのログイン情報を入力します。
- セキュリティ上の理由から、非アクティブな状態が 30 分続くと Cisco Virtualized VB Administration からログアウトされます。
- Virtalized VB Administration は Web ベースのクロスサイト リクエスト フォージェリ攻撃を検出し悪意のあるクライアントリクエストを拒否します。この場合、「試行された処理はセキュリティポリシーに違反するため許可されません（The attempted action is not allowed because it violates security policies）」というエラーメッセージが表示されます。

ステップ 3 ライセンスファイルをインポートし、**[次へ（Next）]** をクリックして構成します。
コンポーネントの有効化ページが表示されます。

ステップ 4 すべてのコンポーネントステータスが**[有効（Activated）]** になったら、**[次へ（Next）]** をクリックします。
システムパラメータ構成ページが表示されます。

ステップ 5 ドロップダウンリストで**コーデック**を選択し、**[次へ（Next）]** をクリックします。
言語の確認ページが表示されます。

ステップ 6 ドロップダウンリストの **[言語（Language）]** を選択し、適切な言語を選択します。

ステップ 7 **[次へ（Next）]** をクリックします。

仮想化 VB サービサビリティ Web ページへのアクセス

Virtualized VB Serviceability は、仮想化 VB サービスのアラームおよびトレース定義を表示するために使用されます。これは、仮想化 VB エンジンの起動と停止、仮想化されたVBエンジンのアクティビティの監視、サービスをアクティブ化および非アクティブ化します。 Cisco Virtualized VB Administration Web ページにログインすると、Virtualized VB Serviceability にアクセスできます。

- [ナビゲーション（Navigation）]ドロップダウンリスト、または

- Web ブラウザで *https://<server name or IP address>/uccxservice/* と入力します。

SIP トリガーの追加

SIP トリガーを追加するには、次の手順に従います。

手順

ステップ 1 **シスコ仮想化音声ブラウザ管理**ページにログインします

ステップ 2 **[サブシステム（Subsystems）] > [SIPテレフォニー（SIP Telephony）] > [SIPトリガー（SIP Triggers）]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 **[ディレクトリ情報（Directory Information）]** タブに、**電話番号** を入力します。

ステップ 5 ドロップダウンリストで、**[言語（Language）]** を選択します。

ステップ 6 ドロップダウンリストで、**[アプリケーション名（Application Name）]** を選択します。

ステップ 7 オプションで、**[詳細を表示（Show More）]** をクリックし、ASR のトリガーを関連付けます。

ステップ 8 **[メディア終了のオーバーライド（Override Media Termination）]** フィールドで、**[はい（Yes）]** オプションを選択します。

ステップ 9 **Select Dialog Groups** および **Available Dialog Groups** 間で、必要なダイアロググループを移動します。

ステップ 10 **[追加（Add）]** または、**[更新（Update）]** をクリックし、変更を保存します。

エージェントグリーティングの構成

- Unified CVP の構成 （502 ページ）
- 設定 Unified CCE （456 ページ）

ウィスパーアナウンスメントの構成

手順

ステップ 1 シスコ子仮想化音声ブラウザ管理ページにサインインします。

ステップ 2 **[アプリケーション（Application）] > [アプリケーション管理（Application Management）]** の順に選択します。

ステップ 3 **着信音**アプリケーションが一覧され、`919191*` のトリガーに関連付けられていることを確認します。

次のタスク

- Unified CVP の構成 （502 ページ）
- 設定 Unified CCE （456 ページ）

ASR と TTS の構成

シスコ仮想化音声ブラウザは、2 つのサブシステムを介して ASR と TTS をサポートします。ASR および TTS サブシステムを構成するには、以下の手順を実行します。

- ASR サブシステムの構成 （473 ページ）
- TTS サブシステムの構成 （473 ページ）

ASR サブシステムの構成

ASR サブシステムでは、IVR を使用してオプションを選択できます。

手順

ステップ 1 **シスコ仮想化音声ブラウザ管理**ページにログインします。
ステップ 2 **[サブシステム（Subsystems）]** > **[スピーチサーバー（Speech Servers）]** > **[ASRサーバー（ASR Servers）]** の順に選択します。
ステップ 3 [新規追加（Add New）] をクリックします。
ステップ 4 **[サーバー名（Server Name）]** フィールドに、ホスト名または IP アドレスを入力します。
ステップ 5 **ポート番号**を入力します。
ステップ 6 ドロップダウンリストで、**[場所（Locales）]** を選択し、**[言語の追加（Add Language）]** をクリックします。
ステップ 7 **[有効な言語（Enabled Languages）]** チェックボックスをオンにします。
ステップ 8 [追加（Add）] をクリックします。

TTS サブシステムの構成

TTS サブシステムはプレーンテキスト（UNICODE）を IVR に変換します。

手順

ステップ 1 **シスコ仮想化音声ブラウザ管理**ページにログインします。
ステップ 2 **[サブシステム（Subsystems）]** > **[スピーチサーバー（Speech Servers）]** > **[TTSサーバー（TTS Servers）]** の順に選択します。
ステップ 3 [新規追加（Add New）] をクリックします。
ステップ 4 **[サーバー名（Server Name）]** フィールドに、ホスト名または IP アドレスを入力します。

ステップ 5 **ポート番号**を入力します。

ステップ 6 ドロップダウンリストで、**[場所（Locales）]** を選択し、**[言語の追加（Add Language）]** をクリックします。

ステップ 7 **[有効な言語（Enabled Languages）]** チェックボックスをオンにします。

ステップ 8 次のオプションから **[性別（Gender）]** を選択します。

- オス型
- メス型
- どちらでもない

（注） 有効な言語ごとに少なくとも 1 つの性別を選択します。

ステップ 9 [追加（Add）] をクリックします。

（注） **[アップデート（Update）]** をクリックし、既存構成を修正します。

Cisco VVB 用サービス コールバックの構成

手順

ステップ 1 **シスコ仮想化音声ブラウザ管理**ページにログインします。

ステップ 2 **[アプリケーション（Application）]** > **[アプリケーション管理（Application Management）]** の順に選択します。

ステップ 3 リストから、**[包括（Comprehensive）]** を選択します。

ステップ 4 **包括**アプリケーションが、トリガー **777777777*** に関連付けられていることを確認してください。

次のタスク

ゲートウェイ、 Unified CVP および Unified CCE に対するサービス コールバックの構成

SocialMiner

SocialMiner のインストール

以下の手順を実行して、SocialMiner をインストールします。

手順

ステップ 1 VMware Open Virtual Format テンプレートを使用して仮想マシンを作成します。

ステップ 2 SocialMiner リリースの新規インストールには、OVA テンプレート **Cisco_SocialMiner_v11.6_VMv9.ova** を使用します。

a) https://software.cisco.com/download/type.html?mdfid=283613136&flowid=73189 に移動して、このテンプレートをダウンロードします。

Cisco SocialMiner 11.6(1) 仮想サーバーテンプレート（OVA）は、SocialMiner 11.6(1) リリースでサポートされている仮想マシン構成を定義します。この OVA には、このリリースでサポートされるすべての仮想マシン構成が含まれます。

ステップ 3 テンプレートを展開する場合は、ドロップダウンリストで大規模または小規模のいずれかの展開を選択します。

ステップ 4 SocialMiner DVD または ISO ファイルを仮想マシンにマウントし、SocialMiner DVD から起動するように仮想マシンを設定します。インストール ウィザードが開きます。Tab キーを使用して要素間を移動し、スペースバーまたは Enter キーを押して要素を選択して続行します。

ステップ 5 プロンプトが表示されたら、メディアチェックを実行します。

ステップ 6 画面に表示される指示に従い、**[はい（Yes）]** か **[続行（Continue）]** を選択します。

ステップ 7 矢印キーを使用して正しいタイムゾーンを強調表示し、Tab を使用して**[OK]** ボタンに移動します。**Enter** を押して次に進みます。

ステップ 8 SocialMiner のネットワーク情報を入力します。一致する IP アドレスを持つ有効なホスト名を指定する必要があります。システムは、インストールプロセスの後半で、ホスト名が IP アドレスと一致することを確認します。

ステップ 9 SocialMiner の DNS クライアント設定を指定するには、**[はい（Yes）]** を選択します。DNS サーバーとドメインを指定します。[OK] を選択します。DNS 構成は必須です。

ステップ 10 管理者 ID とパスワードを入力します。このログイン情報は、プラットフォーム（Unified OS）管理用です。

ステップ 11 組織に関する情報を提供します。この情報により、このサーバのセキュリティ（SSL）証明書が生成されます。

ステップ 12 少なくとも 1 つの NTP サーバーを提供する必要があります。NTP ホストアドレスを入力し、**[OK]** を選択します。

ステップ 13 セキュリティパスワードを入力します。

ステップ 14 SocialMiner 管理者用のユーザー名とパスワードを入力します。SocialMiner のインストールが完了したら、Active Directory から追加のSocialMiner ユーザーをインポートできます。

ステップ 15 確認ウィンドウが開きます。**[戻る（Back）]** を選択して設定を変更するか、**[OK]** を選択してインストールを完了できます。インストールには最大 2 時間かかります。サーバーを再起動して、インストール手順を完了します。ISO ファイルからインストールし、「切断する（ロックをオーバーライドする）（Disconnect anyway (and override the lock)）？」という仮想マシンメッセージが表示された場合は、**[はい（Yes）]** を選択します。

サーバーコンソールにサインインプロンプトが表示されます。

ステップ 16 インストールが完了したら、追加構成オプション （476ページ）に一覧されるワンタイム設定タスクを実行します。

追加構成オプション

手順

ステップ 1 システムがファイアウォールの背後にインストールされている場合は、フィードがインターネット上のサイトにアクセスできるように HTTP プロキシを設定します。

ステップ 2 追加ユーザーがサインインできるように Active Directory を構成します。

ステップ 3 Cisco Unified Intelligence Center を使用する場合は、レポーティングツールがレポーティングデータベースにアクセスできるようにレポーティングユーザーを設定します。

タスク ルーティング 設定

初期設定

手順	タスク	注意事項
CCE の設定		
1	ネットワーク VRU とネットワーク VRU スクリプトを構成します。 ネットワーク VRU and ネットワーク VRU スクリプトの構成 （478 ページ）を参照してください。	
2	MR PG および PIM を構成します。 メディアルーティング PG および PIM の構成 （479 ページ）を参照してください。	
3	SocialMiner の MR PG および PIM を設定します。 メディアルーティング PG および PIM の設定 （479 ページ）を参照してください。	

手順	タスク	注意事項
4	システムインベントリで SocialMiner を外部マシンとして追加します。 外部マシンとして、SocialMiner を追加します。（480 ページ）を参照してください。	システムは、SocialMiner Administrationで次の構成を自動的に行います。 • **CCEマルチチャネルルーティング設定**を有効にして構成します。 • タスク ルーティング機能に必要なタスクフィードと関連するキャンペーンおよび Connection to CCE 通知を設定します。
5	Unified CCEAdministration、Unified CCE構成マネージャ、または Unified CCDM ポータルで以下を構成します。 • メディア ルーティング ドメイン • エージェント デスク設定 • コール タイプ • スキル グループまたはプレシジョン キュー • ダイヤル番号 • ECC 変数 Unified CCE Administration、Unified CCE 構成マネージャ および Unified CCDM ポータルの構成（481 ページ）を参照してください。	
6	プレシジョンキューを使用しており、E メールなどの潜在的に長いタスクを送信する場合は、TCDTimeout レジストリキーの値を増やします。 TCDTimeout 値の増加（483 ページ）を参照してください。	
7	Cisco Context Service の構成（オプション） コンテキストサービス（484ページ）を参照してください。	Context Service を使用して タスク ルーティング タスクのカスタマーインタラクションデータを保存する場合は、SocialMiner を Cisco Context Service に登録します。

手順	タスク	注意事項
8	ルーティングスクリプトの作成 タスク ルーティング に対するルーティングスクリプトの作成 （487 ページ）を参照してください。	
SocialMiner および Finesse アプリケーションの作成		
9	タスクリクエストを開始する SocialMiner マルチチャネル アプリケーションを作成します。 サンプル SocialMiner HTML タスクアプリケーション（488 ページ）を参照してください。	
10	非音声エージェントとダイアログ状態を管理する Finesse アプリケーションを作成します。 タスク ルーティング に対するサンプル Finesse コード （488 ページ）を参照してください。	
Finesse の設定		
11	Finesse デスクトップガジェットをデスクトップレイアウトにアップロードします（オプション）。 http://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html の *Cisco Finesse* アドミニストレーション ガイド を参照してください。	

ネットワーク VRU and ネットワーク VRU スクリプトの構成

ネットワーク VRU は、エージェントが処理できない音声以外のタスクをキューに入れるために使用されます。ネットワーク VRU スクリプトは、推定待機時間をお客様に返すために使用されます。推定待機時間を返すルーティングスクリプトの作成の詳細については、「https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html」の『 *Cisco Unified ICM/Contact Center Enterprise* スクリプティングおよびメディア ルーティング ガイド』を参照してください。

ネットワーク VRU スクリプトの構成時に、割り込み可能かどうかを指定します。ネットワーク VRU スクリプトの**割り込み可能**設定は、スクリプトに割り込みできるかどうかを制御します（エージェントが対応可能になった場合など）。この設定は、メディアルーティングドメインの**割り込み可能**設定とは関係ありません。メディアルーティングドメイン割り込み可能設定は、その MRD 内のタスクで作業しているエージェントが、割り込み不可の MRD からのタスクによって割り込み可能かどうかを制御します。

手順

ステップ 1 構成マネージャで、**Network VRU Explorer** ツールを使用してタイプ 2 VRUを構成および保存します。

ステップ 2 **ネットワーク VRU スクリプト**一覧ツールを使用して、このネットワーク VRU を参照するネットワーク VRU スクリプトを追加します。

デフォルト値を使用します。

メディアルーティング PG および PIM の構成

手順

ステップ 1 構成マネージャで、PG Explorer ツールを開き、メディアルーティング PG を構成します。

ステップ 2 SocialMiner 用メディアルーティング PIM およびルーティングクライアントを作成します。

ロジカルコントローラ ID と周辺機器 ID をメモします。これは、PG の設定時に使用します。

ステップ 3 PG Explorer ツールの [周辺機器（Peripheral）] タブにある **[ポストルーティングを有効化（Enable post routing）]** チェックボックスをオンにします。

ステップ 4 PG Explorer ツールの [ルーティングクライアント（Routing Client）] タブにある **[ルーティングタイプ（Routing Type）]** ドロップダウンリストボックスで **[マルチチャネル（Multichannel）]** を選択します。

ステップ 5 PG Explorer ツールの [詳細（Advanced）] タブで、作成したタイプ 2 ネットワーク VRU を選択します。

メディアルーティング PG および PIM の設定

メディアルーティング PG および PIM の設定

手順

ステップ 1 Cisco Unified CCE ツールから、**[周辺機器ゲートウェイ設定（Peripheral Gateway Setup）]** を選択します。

ステップ 2 [コンポーネントの設定（Components Setup）] 画面の [インスタンスコンポーネント（Instance Components）] パネルで、[PGインスタンス（PG Instance）] コンポーネントを選択します。PG が存在しない場合は、**[追加（Add）]** をクリックします。存在する場合は、**[編集（Edit）]** をクリックします。

ステップ 3 [周辺機器ゲートウェイプロパティ（Peripheral Gateways Properties）] 画面で、**[メディアルーティング（Media Routing）]** をクリックします。[次へ（Next）] をクリックします。

ステップ 4 サービスを停止するには、プロンプトで**[はい（Yes）]** をクリックします。

ステップ 5 [周辺機器ゲートウェイコンポーネントプロパティ（Peripheral Gateway Component Properties）] 画面で、**[追加（Add）]** をクリックし、次の PIM を選択したら、以下のようにメディアルーティングのクライアントタイプを構成します。

a) **[有効化（Enabled）]** をオンにします。
b) **[周辺機器名（Peripheral Name）]** フィールドに、**MR** と入力します。
c) **[周辺機器ID（Peripheral ID）]** フィールドに、メディアルーティング PG および PIM 構成時に記録した周辺機器 ID を入力します。
d) **[アプリケーションホスト名（1）（Application Hostname (1)）]**には、SocialMiner のホスト名と IP アドレスを入力します。
e) デフォルトで、SocialMiner は**アプリケーション接続ポート** 38001 の MR 接続を受け入れます。SocialMiner のアプリケーション接続ポートの設定は、MR PG の設定と一致する必要があります。接続の一方のポートを変更する場合は、もう一方のポートも変更する必要があります。
f) **[アプリケーションホスト名（2）（Application Hostname (2)）]** フィールドは空欄のままにします。
g) その他の値はすべて保持します。
h) [OK] をクリックします。

ステップ 6 [周辺機器ゲートウェイコンポーネントプロパティ（Peripheral Gateway Component Properties）] 画面で、メディアルーティング PG および PIM の構成時に記録した論理コントローラ ID を入力します。

ステップ 7 デフォルトを受け入れ、[設定の完了（Setup Complete）] 画面が開くまで **[次へ（Next）]** をクリックします。

ステップ 8 [設定の完了（Setup Complete）]画面で、**[はい（Yes）]** をオンにしてサービスを開始します。[完了（Finish）] をクリックします。

ステップ 9 **[設定を終了（Exit Setup）]** をクリックします。

ステップ 10 サイド B にもこの手順を繰り返します。

外部マシンとして、SocialMiner を追加します。

外部マシンとして、Unified CCE 管理システムインベントリに SocialMiner を追加する際、システムは以下の SocialMiner 構成を自動で実行します。

- SocialMiner 管理で **[マルチチャネルルーティングのCCE構成（CCE Configuration for Multichannel Routing）]** 設定を有効化し、構成します。

  これらの設定には、MR PGのホスト名と、MR PGおよびPIM設定時に指定したアプリケーション接続ポートが含まれます。

- タスクルーティング機能に必要なタスクフィードと関連するキャンペーンおよびConnection to CCE 通知を次の名前で構成します。

  - **タスクフィード**： Cisco_Default_Task_Feed

- **キャンペーン**： Cisco_Default_Task_Campaign
- **通知**： Cisco_Default_Task_Notification
- **タグ**： cisco_task_tag

注 タスクフィードが別のタグを使用するように構成されている場合、Connection to CCE 通知はそのタグを使用するように構成されます。

手順

ステップ 1 **Unified CCE 管理** > **インフラストラクチャ** > **インベントリ**に移動します。

ステップ 2 [追加（Add）]をクリックします

ステップ 3 ドロップダウンリストで SocialMiner を選択します。

ステップ 4 **[ホスト名（Hostname）]** フィールドに、完全修飾ドメイン名（FQDN）、ホスト名または IP アドレスのいずれかを入力します。

（注） システムは、入力する値を FQDN に変換しようとします。

ステップ 5 SocialMiner 管理ユーザー名とパスワードを入力します。

ステップ 6 **サイド A** と**サイド B** のメディアルーティング PG を選択します。

ステップ 7 MR PG および PIM 設定時に指定したアプリケーションポートを入力します。デフォルト値は 38001 です。

ステップ 8 [保存（Save）] をクリックします。

Unified CCE Administration、Unified CCE 構成マネージャ および Unified CCDM ポータルの構成

このトピックでは、タスク ルーティング の構成が必要な Unified CCE Administration、構成マネージャ、および Unified CCDM ポータルツールについて説明します。

始める前に

これらの手順の詳細については、Unified CCE Administration のオンラインヘルプ、構成マネージャのオンラインヘルプ、および Unified CCDM ポータルのオンラインヘルプを参照してください。

手順

ステップ 1 Unified CCE の管理にサインインします。

ステップ 2 **[管理（Manage）]** メニューから、次を構成します。

構成する項目	詳細（Details）
メディア ルーティング ドメイン	サードパーティ製マルチチャネルアプリケーションがCCEに送信するタスクのタイプごとにMRDを作成します（Eメール、チャットなど）。

ステップ 3 構成マネージャを起動します。

ステップ 4 以下を設定します。

構成する項目	詳細（Details）
エージェント デスク設定	エージェントが Finesse デスクトップでタスク ルーティング ガジェットを使用する場合は、それらのエージェントの**[ログアウト非アクティブ時間（Logout inactivity time）]** 設定を空白のままにするか、既存の値を削除します。 それ以外の場合、エージェントが音声 MRD の**ログアウト非アクティブ時間**を超えると、エージェントは非音声 MRD からのタスクの作業中でも、Cisco Finesse デスクトップからログアウトされます。非音声タスクの作業を続行するには、エージェントはデスクトップに再度ログインする必要があります。

ステップ 5 テナントまたはサブカスタマーユーザーとして Unified CCDM ポータルにログインします。

ステップ 6 以下を設定します。

構成する項目	詳細（Details）
コール タイプ	タスク ルーティング に対してコールタイプを作成します。
ダイヤル番号	タスク ルーティングのダイアル番号を作成します。サードパーティ製マルチチャネル アプリケーションがタスク要求を送信するときに使用する番号または文字列を追加します。 • **[メディアルーティングドメイン（Media Routing Domain）]** で、タスク ルーティング MRDのいずれかを選択します。 • **[コールタイプ（Call Type）]** で、タスク ルーティング に対して作成したコールタイプを選択します。 **重要** 各ダイヤル番号は、コールタイプに関連付ける必要があります。デフォルトのコールタイプは、タスク ルーティング APIで送信されたタスクではサポートされません。

構成する項目	詳細（Details）
スキル グループ	スキルグループまたはプレシジョンキューを構成します。 スキルグループを構成する場合： • **[メディアルーティングドメイン（Media Routing Domain）]** で、作成した タスク ルーティング MRDのいずれかを選択します。 • エージェントにスキルグループを割り当てます。
プレシジョン キュー	スキルグループまたはプレシジョンキューを構成します。 プレシジョンキューを構成する場合： • **[メディアルーティングドメイン（Media Routing Domain）]** で、作成した タスク ルーティング MRDのいずれかを選択します。 • プレシジョンキュー手順の一部である属性にエージェントを関連付けます。
拡張コール変数	サードパーティ製マルチチャネルアプリケーションのニーズに応じて、既存の拡張コール変数を使用することも、タスク ルーティング 向けの拡張コール変数を作成することもできます。 （注） アレイは タスク ルーティング 機能ではサポートされていません。 CCE ソリューションでは、Finesse および SocialMiner で使用される拡張コールコンテキスト変数およびコール変数について、Latin 1 文字一式のみがサポートされています。

TCDTimeout 値の増加

この手順は、プレシジョンキューを使用し、E メールのように継続時間が長い可能性があるタスクをルーティングする場合にのみ実行します。

Termination_Call_Detail レコードのいくつかの [プレシジョンキュー（Precision Queue）] フィールドは、タスクの終了まで完了しません。これらの [プレシジョンキュー（Precision Queue）] フィールドは、TCDTimeout レジストリキー値を超える期間のタスクで空欄になります。TCDTimeout レジストリキーのデフォルト値は 9,000 秒（2.5 時間）です。

E メールまたはその他長期タスクを処理するようにシステムを構成する場合は、TCDTimeout レジストリキー値を最大値である 86,400 秒（24 時間）まで増やします。

サイド A または B ルーターのどちらかのレジストリキーを変更します。

手順

次のレジストリキーを修正します：`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Icm\<instance name>\Router<A/B>\Router\CurrentVersion\Configuration\Global\TCDTimeout`。

コンテキストサービス

Cisco Context Service は、Cisco Contact Center Enterprise ソリューション向けのクラウドベースのオムニチャンネル ソリューションです。これにより、どのチャネルでもカスタマー インタラクション データを柔軟に格納して、顧客のインタラクション履歴を把握できます。

CCE ソリューション内のさまざまなコンポーネントによって、追加設定なしで Context Service と統合できます。また Context Service は、独自のアプリケーションやサードパーティ製アプリケーションとの統合をサポートする API を提供し、エンドツーエンドのカスタマー インタラクション データをキャプチャします。

Context Service の詳細とサービスの可用性については、https://cisco.com/go/contextservice を参照してください。

コンテキストサービス設定の詳細については、「コンテキストサービス」章を参照してください。

タスク ルーティング タスクのコンテキストサービス

コンテキストサービスは、タスク ルーティング タスクコンタクトのデータを登録できます。コンテキストサービスが有効になっている場合、SocialMiner は着信タスク要求からデータを選択し、アクティビティをクラウドに保存します。

タスク要求で要求のメディアタイプを指定できます。メディアタイプを指定しない場合、メディアタイプはデフォルトで 「event」 になります。

要求にタスク要求情報をすでに保存し、タスク要求にその参照 URL を含めている場合、SocialMiner は新しいアクティビティを作成しません。SocialMiner は、Finesse クライアントで使用するために既存の要求 ID を直接 Unified CCE に渡します。

新しい連絡先を作成すると、SocialMiner は SocialMiner ソーシャル連絡先の作成者フィールドでお客様を検索します。ルックアップの結果によって、連絡先にお客様のリファレンスが含まれるかどうかが次のように決まります。

- 返されたお客様がゼロまたは多数の場合、連絡先にはお客様のリファレンスは含まれません。
- 1 人のお客様が返された場合、連絡歳に派、お客様のリファレンスが含まれます。

SocialMiner は、タスク ルーティング タスクの連絡先に設定されている [Context Service cisco.base.pod] フィールドから以下のフィールドに値を入力します。

- **Context_Notes**：このフィールドには、SocialContact.description の値が入力されます。

- **Context_POD_Source_Cust_Name**：このフィールドには、SocialContact.author の値が入力されます。
- **Context_POD_Source_Email**：このフィールドを入力するため、SocialMiner は [SocialContact.author] フィールドを使用して E メールアドレスを検索します。

コンテキスト サービス ネットワーク接続の要件

Context Service はクラウドベースのサービスであり、Context Service を使用するコール センターのコンポーネントがパブリック インターネットに接続できるようにする必要があります。

Context Service はポート 443（HTTPS）を使用します。

コンタクトセンターのコンポーネントがコンテキストサービスに接続でき、コンテキストサービスからデータを受信できるように、次の URL をファイアウォールでリストに登録する必要があります。

- `*.webex.com`
- `*.wbx2.com`
- `*.ciscoccservice.com`

（注） コンテキスト サービスは複数のサブ ドメインからアクセスされるため、ホワイトリストにはワイルドカード URL を使用します。コンテキスト サービスのサブドメイン名は、動的に変更できます。

プロキシ設定オプションを有効にして Context Service 登録を行う場合は、Context Service 管理ガジェットで指定された URL を使用してブラウザ プロキシを設定します。関連するブラウザのプロキシ設定を構成するには、以下のリンクを参照してください。

Chrome	https://support.google.com/chrome/answer/96815?hl=en
Firefox	https://support.mozilla.org/en-US/kb/advanced-panel-settings-in-firefox
Internet Explorer	http://windows.microsoft.com/en-in/windows/change-internet-explorer-proxy-server-settings#1TC=windows-7

コンテキストサービスのプリンシパル AW の構成

Unified CCE Administration でコンテキストサービスに登録する前に、どの管理およびデータ サーバー（AW）がコンテキストサービスのログイン情報を使用するかを設定します。

手順

ステップ 1 **Unified CCE Administration** で、**[インフラストラクチャ（Infrastructure）]** > **[インベントリ（Inventory）]** の順に選択します。

ステップ 2 **システムインベントリ**で、コンテキストサービスの Cisco Spark Control Hub 管理者ログイン情報を管理する AW をクリックします。

ステップ 3 **[AW の編集（Edit AW）]** ポップアップウィンドウで、**[プリンシパル（Principal）]** チェックボックスをオンにします。

ステップ 4 ソリューションの**診断フレームワーク**ログイン情報を入力します。

ステップ 5 [保存（Save）] をクリックします。

コンテキスト サービスの設定

コンテキストサービス管理ガジェットを使用して、Cisco Finesse をコンテキストサービスに登録します。

手順

ステップ 1 まだサインインしていない場合は、Cisco Finesse 管理コンソールにログインします。

ステップ 2 Cisco Finesse をコンテキストサービスに登録するには、コンテキスト サービス管理ガジェットで **[登録（Register）]** をクリックします。

（注） コンテキストサービスの登録を開始する前に、ポップアップが有効になっていることを確認します。

ブラウザのポップアップウィンドウのブロック設定で Finesse FQDN が例外として追加されていない場合、登録および登録解除のポップアップウィンドウは自動的に閉じません。ポップアップウィンドウを手動で閉じる必要があります。

[登録（Register）] ボタンが表示されず、ページを更新するように求めるメッセージが表示された場合は、ブラウザのキャッシュをクリアしてから再試行してください。

コンテキストサービスのプロキシサーバーを構成する場合は、**[プロキシ設定の有効化（Enable Proxy Setting）]** オプションをオンにし、次のクライアント設定パラメータを入力して **[保存（Save）]** をクリックします。

フィールド	説明
プロキシサーバーの URL	プロキシサーバーのアドレス
タイムアウト	コンテキストサービスクラウドの接続を拒否する前にシステムが待機するミリ秒（ms）。 デフォルト：1000 ミリ秒 範囲：200 ー 15,000ミリ秒。

フィールド	説明
ラボ モード（Lab Mode）	ラジオボタンは、コンテキストサービスが実稼働モードかラボモードかを示します。 • 有効—コンテキストサービスがラボモードに切り替わります。 • 無効（デフォルト）—コンテキストサービスは実稼働モードです。

[登録（Register）] をクリックし、コンテキストサービスで Cisco Finesse を構成します。

（注） コンテキスト サービス パラメータを変更した場合は、コンテキストサービスの接続に 30 秒以上かかる場合を除き、再登録しないでください。

ステップ 3 登録を完了するには、Cisco Cloud Collaboration Management 管理者のログイン情報を入力し、サインインします。

ステップ 4 登録が正常に完了したら、**[再登録（Deregister）]** をクリックするとコンテキストサービスから登録を解除できます。

（注） 登録プロセス中に登録をキャンセルする場合は、**[キャンセル（Cancel）]** をクリックします。

登録が失敗した場合、またはコンテキストサービスに到達できない場合は、**[登録（Register）]** ボタンをクリックして再登録できます。

（注） Firefox を使用している場合は、**dom.allow_scripts_to_close_windows** 構成を有効にして、コンテキストサービス登録用に開いた追加のタブが想定どおりに閉じるようにします。手順は次のとおりです。

1. Firefox ブラウザで `about:config` と入力します。
2. **[リスクを容認（I accept the Risk）]** をクリックします。
3. `dom.allow_scripts_to_close_windows` 構成を検索します。
4. [値（Value）] フィールドをダブルクリックし、`[True]` に変更します。
5. ブラウザを再起動します。

タスク ルーティング に対するルーティングスクリプトの作成

マルチチャネルスクリプトの詳細については、「https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html」の「*Cisco Unified ICM/Contact Center Enterprise* スクリプティングおよびメディア ルーティング ガイド」を参照してください。

重要 スクリプトでルーティングできるすべてのタイプのタスクを処理するために、適切なメディアルーティング ドメインからのスキルグループまたはプレシジョンキューがルーティングスクリプトに含まれていることを確認します。たとえば、E メールタスクのルーティングにスクリプトを使用する場合は、スクリプトに E メール MRD からのスキルグループまたはプレシジョンキューが含まれていることを確認します。

タスク ルーティング に対するサンプルコード

シスコでは、SocialMiner および Finesse のサンプルタスク ルーティング アプリケーション コードを、独自のアプリケーションを構築するための基準として使用できるようにしています。

サンプル SocialMiner HTML タスクアプリケーション

サンプル SocialMiner HTML タスクアプリケーション：

- CCE にタスク要求を送信します。
- CCE で構成されている場合、推定待機時間を取得して表示します。

（注） このコードをコピーして貼り付けて、アプリケーションを機能させることはできません。これは単なるガイドラインです。

サンプルアプリケーションはタスク API を使用します。タスク API の使用方法の詳細については、「https://developer.cisco.com/site/socialminer/documentation/」の『*Cisco SocialMiner Developer Guide*』を参照してください。

手順

ステップ 1 DevNet：https://developer.cisco.com/site/task-routing/ からサンプルの HTML タスクアプリケーションをダウンロードします。

ステップ 2 サンプルアプリケーションの **readme.txt** ファイルを読んで、前提条件を満たし、サンプルアプリケーションを使用します。

タスク ルーティング に対するサンプル Finesse コード

Finesse サンプルタスク管理ガジェットアプリケーションでは、エージェントが個々の非音声メディア ルーティング ドメインで次のアクションを実行できます。

- サインインとサインアウト。
- 状態の変更。

- タスクの処理。

サンプルガジェットは、カスタマーレコードを表示するようにカスタマー コンテキスト ガジェットにも通知します。

（注） このコードをコピーして貼り付けて、アプリケーションを機能させることはできません。これは単なるガイドラインです。

タスク ルーティング で使用可能な API の使用方法については、「https://developer.cisco.com/site/finesse/」の「*Cisco Finesse Web Services* 開発者ガイド」を参照してください。

手順

ステップ 1 DevNet：https://developer.cisco.com/site/task-routing/ からサンプルタスク管理ガジェットアプリケーション（TaskManagementGadget-x.x.zip）をダウンロードします。

ステップ 2 サンプルアプリケーションの **readme.txt** ファイルを読んで、前提条件を満たし、サンプルアプリケーションを使用します。

サードパーティガジェットを Finesse サーバーにアップロードする方法については、「https://developer.cisco.com/site/finesse/」の『*Cisco Finesse Web Services* 開発者ガイド』に記載されている「サードパーティガジェット」章を参照してください。

Finesse デスクトップにサードパーティガジェットを追加する方法については、「https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/tsd-products-support-series-home.html」の『*Cisco Finesse* アドミニストレーション ガイド』に記載されている「サードパーティガジェットの管理」項を参照してください。

タスク ルーティング レポート

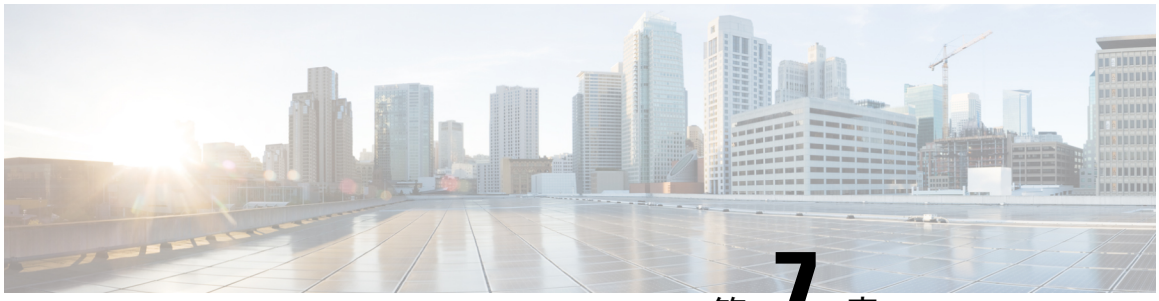
Cisco Unified Intelligence Center CCE レポートには、音声コールと非音声 タスク ルーティング タスクのデータが含まれます。

メディア ルーティング ドメインによって、次のすべてのフィールドおよびライブ データ レポート テンプレートをフィルタ処理できます。

- エージェント-リアルタイム
- エージェントスキルグループ-リアルタイム
- エンタープライズスキルグループ-リアルタイム
- 周辺機器スキルグループ-リアルタイム全フィールド
- プレシジョンキュー-リアルタイム全フィールド

- エージェントプレシジョンキュー-履歴全フィールド
- エージェントスキルグループ-履歴全フィールド
- 周辺機器スキルグループ-履歴全フィールド
- プレシジョンキュー放棄/応答分布-履歴
- プレシジョンキューのインターバル全フィールド
- スキルグループ放棄/応答分布-履歴
- プレシジョンキュー - ライブデータ
- スキルグループ - ライブデータ

マルチチャネル レポーティング データについては、「https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html」の「*Cisco Unified ICM/Contact Center Enterprise* レポートの概念」を参照してください。



第 7 章

リモート展開オプション

グローバル導入

グローバル展開では、サービスプロバイダが中央管理されたリモートサイトを展開できます。以下のグローバル展開トポロジは、CC 導入モデルの標準 HCS for CC でサポートされています。

リモート CVP 導入

リモート CVP 展開では、リモートサイトに次のサーバーを展開する必要があります。WAN 上の中央コントローラでの最大 RTT は、400 ミリ秒に制限されています。

前提条件：データセンターの CC 導入モデル用標準 HCS for CC

リモート CVP 展開用 Unified CVP サーバー

ゴールデンテンプレートからリモート CVP サーバーを展開するには、ゴールデン テンプレート ツールを使用します。このセクションでは、リモートサイトで Unified CVP サーバーを構成する方法を説明します。

リモート CVP サーバーの構成

リモート CVP サーバーを構成するには、「Unified CVP サーバーの構成 （61 ページ）」を参照してください。

リモート展開向けリモート CVP 用オペレーションコンソールの構成

CVP OAMP にリモート CVP サーバコンポーネントを追加し、UDP 送信、ハートビートプロパティを変更します。

順序	タスク	完了したか
1	ネットワーク カードの検証 （61 ページ）	
2	Unified CVP オペレーションコンソールの有効化 （70 ページ）	
3	リモート展開用 Unified CVP コールサーバーの構成 （493 ページ）	
4	Unified CVP サーバー コンポーネントの構成 （72 ページ）	
5	Unified CVP レポーティングサーバーの構成 （73 ページ）	
6	Unified CVP メディアサーバーの構成 （74 ページ）	
7	Unified CVP ライセンスのインストール （74 ページ）	
8	ゲートウェイの構成 （75 ページ）	
9	Unified CCE デバイスの追加 （76 ページ）	
10	Unified Communications Manager デバイスの追加 （77 ページ）	
11	Unified Intelligence Center デバイスの追加 （77 ページ）	
12	スクリプトおよびメディアファイルの転送 （75 ページ）	
13	SNMP の構成 （76 ページ）	
14	リモート展開用 SIP サーバーグループの構成 （494 ページ）	
15	ダイヤル番号パターンの構成 （79 ページ）	

リモート展開用 *Unified CVP* コールサーバーの構成

手順

ステップ 1 Unified CVP OAMP サーバーで、**[スタート（Start）]**>**[すべてのプログラム（All Programs）]**>**[Cisco Unified Customer Voice Portal]** の順に選択します。

ステップ 2 **[オペレーションコンソール（Operations Console）]** をクリックして、ログインします。

ステップ 3 **[デバイス管理（Device Management）]** > **[Unified CVPコールサーバー（Unified CVP Call Server）]** の順に選択します。

ステップ 4 [新規追加（Add New）] をクリックします。

ステップ 5 [一般（General）] タブで、Cisco Unified CVP サーバー のIP アドレスとホスト名を入力します。**[ICM]**、**[IVR]** および **[SIP]** にチェックを入れます。[次へ（Next）] をクリックします。

ステップ 6 **[ICM]** タブをクリックします。各 Cisco Unified CVP コールサーバーで、VRU 接続ポートのデフォルトポートを 5000 のままにします。

ステップ 7 **[SIP]** タブをクリックします。

a) [アウトバウンドプロキシを有効にする（Enable outbound proxy）] フィールドで、**[いいえ（No）]** を選択します。

b) [DNS SRVタイプクエリの使用（Use DNS SRV type query）] フィールドで、**[はい（Yes）]** を選択します。

c) **[SRVレコードをローカルに解決（Resolve SRV records locally）]** をオンにします。

d) [詳細構成（Advanced Configuration）] で [UDPの再送信数（UDP Retransmission Count）] を 3 に設定します。

ステップ 8 **[デバイスプール（Device Pool）]** タブをクリックします。デフォルトのデバイス プールが選択されていることを確認してください。

ステップ 9 （オプション）**[インフラストラクチャ（Infrastructure）]** タブをクリックします。[Syslog設定の構成（Configuration Syslog Settings）] ペインで、これらのフィールドを次のように構成します。

a) syslog サーバの IP アドレスまたはホスト名を入力します。

例：

プライムサーバー

b) syslog サーバーのポート番号に **514** と入力します。

c) Reporting Server がログ メッセージを書き込むバックアップサーバーの名前を入力します。

d) [バックアップサーバーポート番号（Backup server port number）] フィールドに、バックアップ syslog サーバーのポート番号を入力します。

ステップ 10 [保存して展開（Save & Deploy）] をクリックします。

ステップ 11 残りの Unified CVP コールサーバーに対してこの手順を繰り返します。

リモート展開用 *SIP* サーバーグループの構成

SIP サーバーグループは、Cisco Unified Communications Manager およびゲートウェイで必要となります。

手順

ステップ 1 Unified CVP オペレーションコンソールで、**[システム（System）]**>**[SIPサーバーグループ（SIP Server Group）]** の順に選択します。

ステップ 2 Cisco Unified Communications Manager デバイス用のサーバーグループを作成します。

a) [一般（General）] タブで、**[新規追加（Add New）]** をクリックします。

b) **[SRVドメイン名FQDN（SRV Domain Name FQDN）]** フィールドに、Communications Manager の エンタープライズパラメータの Cluster FQDN 設定でも使用する値を入力します。たとえば、cucm.cisco.com のようになります。

c) **[IPアドレス/ホスト名（IP Address/Hostname）]** フィールドに、Unified Communications Manager ノードの IP アドレスまたはホスト名を入力します。

d) [追加（Add）] をクリックします。

e) Unified Communications Manager サブスクライバごとに手順 c と d を繰り返します。[保存（Save）] をクリックします。

（注） サーバーグループに Publisher ノードを置かないでください。

Communications Manager 用の SIP サーバーグループは SCC 展開に対して必要ありません。これは、Communications Manager から SCC モデルの CVP に作成された直接 SIP トランクが存在しないからです。

ステップ 3 ゲートウェイ デバイス用にサーバーグループを作成します。

a) [一般（General）] タブで、**[新規追加（Add New）]** をクリックします。

b) **[SRVドメイン名FQDN（SRV Domain Name FQDN）]** フィールドに、SRV ドメイン名 FQDN を入力します。たとえば、vxmlgw.cisco.com のように入力します。

c) **[IPアドレス/ホスト名（IP Address/Hostname）]** フィールドに、各ゲートウェイの IP アドレスまたはホスト名を入力します。

d) [追加（Add）] をクリックします。

e) ゲートウェイごとに手順 c と d を繰り返します。[保存（Save）] をクリックします。

展開と分岐に適切な VXML ゲートウェイをすべて追加します。すべての VXML ゲートウェイをサーバーグループに追加すると、すべてのメンバー サーバー グループ ゲートウェイに対してコールのロードバランスが行われます。

ステップ 4 これらサーバーグループをすべての Unified CVP コールサーバーに関連付けます。

a) **[コールサーバー展開（Call Server Deployment）]** タブで、すべての Unified CVP コールサーバーを **[利用可能（Available）]** リストから **[選択済み（Selected）]** リストに移動します。

b) [保存して展開（Save and Deploy）] をクリックします。

ステップ 5 **[ハートビートプロパティ（Heartbeat Properties）]** をクリックし、次の変更を行います。それ以外の場合は、この手順を省略できます。

a) **[到達不能ステータス（Unreachable Status）]** フィールドの **[失敗したハートビート数（Number of Failed Heartbeats）]** を 3 に変更します。

b) **[ハートビートタイムアウト（Heartbeat Timeout）]** フィールドを **800 ms** に変更します。

ステップ 6 [展開ステータス（Deployment Status）] をクリックして、構成が適用されていることを確認します。

（注） Small Contact Center エージェント展開の場合、CUBE(SP) は FQDN 構成に対応していないため、各サブカスタマーに対して CUBE(SP) を指す SIP サーバーグループを作成できません。

リモート CVP 展開用 Unified CCE サービス

ゴールデンテンプレートからリモート CCE VRU PG を展開するには、ゴールデン テンプレート ツールを使用します。このセクションでは、リモート拠点で Unified CCE を構成する手順を説明します。

Unified CCE ルータの変更

「Unified CCE ルーターの構成 （39 ページ）」を参照し、**[周辺機器ゲートウェイの有効化（Enable Peripheral Gateways）]** ダイアログボックスで値を増分して値を修正します。

Unified CCE 構成マネージャを使用してリモート VRU PG を追加

Unified CCE 構成マネージャを使用してリモート VRU PG を追加するには、以下の手順を実行します。

手順

ステップ 1 Unified CCE Admin Workstation サーバーで、**[スタート（Start）] > [Cisco Unified CCEツール（Cisco Unified CCE Tools）] > [管理ツール（Administration Tools）] > [構成マネージャ（Configuration Manager）]** の順に選択します。

ステップ 2 [構成マネージャ（Configuration Manager）] ウィンドウで、**[ツール（Tools）] > [エクスプローラツール（Explorer Tools）]** の順に選択し、**[PG Explorer]** を開きます。リモート VRU PG、PIM およびルーティングクライアントを追加します。

ステップ 3 **[ツール（Tools）] > [エクスプローラツール（Explorer Tools）]** の順に選択し、**Network VRU Explorer** を開きます。ネットワーク VRU ラベルをリモート VRU PG ルーティングクライアントに関連付けます。

ステップ 4 **[ツール（Tools）] > [リストツール（List Tools）]** の順に選択し、**Expanded Call Variable List** を開きます。ECC 変数 である user.microapp.media_server を有効にします。

ステップ 5 **[ツール（Tools）] > [リストツール（List Tools）]** の順に選択し、**Agent Targeting Rule** を開きます。リモート VRU PG ルーティングクライアントを追加します。

リモート CVP 展開用の VRU PG の構成

サイド A で PG サーバー用の Unified CCE 周辺機器ゲートウェイを構成するには以下の手順を実行します。サイド B でも同じ手順を繰り返します。

手順

ステップ 1 **[スタート（Start）] > [すべてのプログラム（All programs）] > [Cisco Unified CCEツール（Cisco Unified CCE Tools）] > [周辺機器ゲートウェイの設定（Peripheral Gateway Setup）]** の順に選択します。

ステップ 2 [ICMインスタンス（ICM Instances）] ペインで **[追加（Add）]** をクリックします。

a) [インスタンスの追加（Add Instance）] ウィンドウのドロップダウンリストで、**[ファシリティ（Facility）]** と **[インスタンス（Instance）]** を選択します。

b) [インスタンス番号（Instance Number）] フィールドに **0** と入力します。[保存（Save）] をクリックします。

ステップ 3 [インスタンスコンポーネント（Instance Components）] ペインで **[追加（Add）]** をクリックし、[コンポーネントの選択（Component Selection）] ダイアログボックスで **[周辺機器ゲートウェイ（Peripheral Gateway）]** を選択します。

ステップ 4 [周辺機器ゲートウェイプロパティ（Peripheral Gateway Properties）] ダイアログボックスで、以下の手順を実行します。

a) [生産モード（Production Mode）] を**オン**にします。

b) [システム起動自動開始（Auto start system startup）] を**オフ**にします。

c) [デュプレックス周辺機器ゲートウェイ（Duplexed Peripheral Gateway）] を**オン**にします。

d) [PGノードプロパティID（PG node Properties ID）] フィールドで **[PGXX]** を選択します。

e) 適切なサイド（**サイド A** または**サイド B**）をクリックします。

f) [クライアントタイプ（Client Type）] ペインで、選択したタイプに対して、**[VRU]** を追加します。

g) **[次へ（Next）]** をクリックします。

ステップ 5 [周辺機器ゲートウェイコンポーネントプロパティ（Peripheral Gateway Component Properties）] ダイアログボックスの [周辺機器インターフェイスマネージャ（Peripheral Interface Manager）] ペインで、**[追加（Add）]** をクリックし、クライアントタイプが VRU の PIM1 を次のように設定します。

a) **[有効化（Enabled）]** をオンにします。

b) [周辺機器名（Peripheral Name）] フィールドに任意の名前を入力します。

c) [周辺機器ID（Peripheral ID）] フィールドで、PG Explorer を参照し、値を入力します。

d) [VRUホスト名（VRU hostname）] フィールドに、リモート CVP サーバーのホスト名を入力します。

e) [VRU接続ポート（VRU Connect port）] フィールドに **5000** と入力します。
f) [再接続間隔（秒）（Reconnect interval (sec)）] フィールドに **10** と入力します。
g) [ハートビート間隔（秒）（Heartbeat interval (sec)）] フィールドに **5** と入力します
h) [DSCP] フィールドで **[CS3(24)]** を選択します。
i) [OK] をクリックします。

ステップ 6 PG Explorer を参照し、[ロジカルコントローラID（Logical Controller ID）]フィールドに値を入力します。

ステップ 7 [CTIコール後処理データ遅延（CTI Call Wrapup Data delay）] フィールドに **0** と入力します。

ステップ 8 [VRU レポーティング（VRU Reporting）]ペインで、**[サービスコントロール（Service Control）]** を選択し、**[キューレポーティング（Queue Reporting）]** をオンにしたら、**[次へ（Next）]** をクリックします。

ステップ 9 [デバイス管理プロトコルプロパティ（Device Management Protocol Properties）] ダイアログボックスで、次のように設定します。

a) サイドA を構成する場合は **[サイドAを優先（Side A Preferred）]** をクリックし、サイドB を構成する場合は **[サイドBを優先（Side B Preferred）]** をクリックします。
b) [サイドAプロパティ（Side A Properties）] パネルで、**[コールルーターはリモート（Call Router is Remote）]** を選択します。
c) [サイドBプロパティ（Side B Properties）] パネルで、**[コールルーターはリモート（Call Router is Remote）]** を選択します。
d) [使用可能な帯域幅（kbps）（Usable Bandwidth (kbps)）] フィールドは、デフォルト値のままにしておきます。
e) [ハートビート間隔（100 ms）（Heartbeat Interval (100ms)）] フィールドに **4** と入力します。**[次へ（Next）]** をクリックします。

ステップ 10 [周辺機器ゲートウェイネットワークインターフェイス（Peripheral Gateway Network Interfaces）] ダイアログボックスで、[PG Private Interfaces] および [PG Public (Visible) Interfaces] と入力します。

a) サイドAのプライベートインターフェイスセクションの **[QoS]** ボタンをクリックします。[PGプライベートリンクQoS設定（PG Private Link QoS Settings）] で **[QoSの有効化（Enable QoS）]** をオンにし、**[OK]** をクリックします。この手順は、サイドA にのみ適用します。
b) パブリック（表示）インターフェイス セクションで **[QoS]** ボタンをクリックします。[PG表示リンクQoS設定（PG Visible Link Qos Settings）] で、**[QoSの有効化（Enable QoS）]** をオンにし、**[OK]** をクリックします。この手順は、サイドA にのみ適用します。
c) [周辺機器ゲートウェイネットワークインターフェイス（Peripheral Gateway Network Interfaces）] ダイアログボックスで、**[次へ（Next）]** をクリックします。

ステップ 11 [設定情報の確認（Check Setup Information）] ダイアログボックスで **[次へ（Next）]** をクリックします。

ステップ 12 [設定完了（Setup Complete）] ダイアログボックスで、**[完了（Finish）]** をクリックします。

（注） すべてのUnified CCE コンポーネントがインストールされるまでUnified CCE/CC Node Manager を起動しないでください。

リモート CVP および Cisco Unified Communications Manager 展開

リモート CVP および Cisco Unified Communications Manager 展開では、リモートサイトで以下のサーバーを展開する必要があります。WAN 上の中央コントローラでの最大 RTT は、400 ミリ秒に制限されています。ゴールデンテンプレートツールを使用して、ゴールデンテンプレートからリモート CCE、CVP、Cisco Unified Communications Manager、および Finesse サーバーを展開します。

前提条件：データセンターの CC 導入モデル用標準 HCS for CC

- Unified CVP の構成 （60 ページ）
- リモート CVP および Cisco Unified Communications Manager 展開用 Unified CCE サービス （498 ページ）
- Unified Communications Manager の構成 （87 ページ）
- Cisco IOS Enterprise 音声ゲートウェイの構成 （81 ページ）
- Cisco Finesse の構成 （110 ページ）

リモート CVP および Cisco Unified Communications Manager 展開用 Unified CCE サービス

ゴールデンテンプレートからリモート CCE エージェント PG を展開するには、ゴールデン テンプレート ツールを使用します。このセクションでは、リモートサイトで Unified CCE サーバーを構成する方法を説明します。

Unified CCE ルータの変更

「Unified CCE ルーターの構成 （39 ページ）」を参照し、**[周辺機器ゲートウェイの有効化（Enable Peripheral Gateways）]** ダイアログボックスで値を増分して値を修正します。

Unified CCE 構成マネージャを使用したリモート エージェント PG の追加

Unified CCE 構成マネージャを使用してリモートエージェント PG を追加するには、以下の手順を実行します。

手順

ステップ 1 Unified CCE Admin Workstation サーバーで、**[スタート（Start）] > [Cisco Unified CCEツール（Cisco Unified CCE Tools）] > [管理ツール（Administration Tools）] > [構成マネージャ（Configuration Manager）]** の順に選択します。

ステップ 2 [構成マネージャ（Configuration Manager）] ウィンドウで、**[ツール（Tools）] > [エクスプローラツール（Explorer Tools）]** の順に選択し、**[PG Explorer]** を開きます。リモート、エージェント PG、Cisco Unified Communications Manager、 VRUPIM そしてそれらのルーティングクライアントを追加します。

ステップ 3 **[ツール（Tools）] > [エクスプローラツール（Explorer Tools）]** の順に選択し、**Network VRU Explorer** を開きます。ネットワーク VRU ラベルとリモート、エージェント PG ルーティングクライアントを関連付けます。

ステップ 4 **[ツール（Tools）] > [リストツール（List Tools）]** の順に選択し、**Expanded Call Variable List** を開きます。ECC 変数 である user.microapp.media_server を有効にします。

ステップ 5 **[ツール（Tools）] > [リストツール（List Tools）]** の順に選択し、 **Agent Targeting Rule** を開きます。リモート、エージェント PG ルーティングクライアントを追加します。

リモート CVP および Cisco Unified Communications Manager 展開用の およびエージェント PGの構成

サイド A で PG サーバー用の Unified CCE 周辺機器ゲートウェイを構成するには以下の手順を実行します。サイド B でも同じ手順を繰り返します。

手順

ステップ 1 **[スタート（Start）] > [すべてのプログラム（All programs）] > [Cisco Unified CCEツール（Cisco Unified CCE Tools）] > [周辺機器ゲートウェイの設定（Peripheral Gateway Setup）]** の順に選択します。

ステップ 2 [ICMインスタンス（ICM Instances）] ペインで [追加（Add）] をクリックします。

a) [インスタンスの追加（Add Instance）] ウィンドウのドロップダウンリストで、**[ファシリティ（Facility）]** と **[インスタンス（Instance）]** を選択します。

b) [インスタンス番号（Instance Number）] フィールドに **0** と入力します。[保存（Save）] をクリックします。

ステップ 3 [インスタンスコンポーネント（Instance Components）] ペインで、**[追加（Add）]** をクリックし、[コンポーネントの選択（Component Selection）] ダイアログボックスで、**[周辺機器ゲートウェイ（Peripheral Gateway）]** を選択します。

ステップ 4 [周辺機器ゲートウェイプロパティ（Peripheral Gateway Properties）] ダイアログボックスで、以下の手順を実行します。

a) [生産モード（Production Mode）] を**オン**にします。

b) [システム起動自動開始（Auto start system startup）] を**オフ**にします。

c) [デュプレックス周辺機器ゲートウェイ（Duplexed Peripheral Gateway）] を**オン**にします。

d) [PGノードプロパティID（PG node Properties ID）] フィールドで **[PGXX]** を選択します。

e) 適切なサイド（**サイド A** または**サイド B**）をクリックします。

f) [クライアントタイプ（Client Type）] ペインで、選択したタイプに対して、**[デュプレックス]** および **[VRU]** を追加します。

g) [次へ（Next）] をクリックします。

ステップ 5 [周辺機器ゲートウェイコンポーネントプロパティ（Peripheral Gateway Component Properties）] ダイアログボックスの [周辺機器インターフェイスマネージャ（Peripheral Interface Manager）] ペインで、**[追加（Add）]** をクリックし、次のようにクライアントタイプが CUCM の PIM1 を構成します。

a) [有効化（Enabled）] を**オン**にします。
b) [周辺機器名（Peripheral name）] フィールドに任意の名前を入力します。
c) [周辺機器ID（Peripheral ID）] フィールドで、PG Explorer を参照し、値を入力します。
d) [エージェントの内線番号の長さ（Agent extension length] フィールドに、この展開の内線番号の長さを入力します。
e) [Unified Communications Manager パラメータ（Unified Communications Manager Parameters）] ペインで、以下のように構成します。
   - [サービス（Service）] フィールドに、Unified Communications Manager Subscriber のホスト名を入力します。
   - [ユーザーID（User ID）] フィールドに、pguser と入力します。
   - [ユーザーパスワード（User Password）] フィールドに、Unified Communications Manager で作成するユーザーのパスワードを入力します。
f) [モバイルエージェントコーデック（Mobile Agent Codec）] フィールドで、[G711 ULAW/ALAW] または [G.729] を選択します。
g) [OK] をクリックします。

ステップ 6 [周辺機器ゲートウェイコンポーネントプロパティ（Peripheral Gateway Component Properties）] ダイアログボックスの [周辺機器インターフェイスマネージャ（Peripheral Interface Manager）] ペインで、**[追加（Add）]** をクリックし、クライアントタイプが VRU の PIM2 を次のように設定します。

a) [有効化（Enabled）] を**オン**にします。
b) [周辺機器名（Peripheral name）] フィールドに任意の名前を入力します。
c) [周辺機器ID（Peripheral ID）] フィールドで、PG Explorer を参照し、値を入力します。
d) [VRUホスト名（VRU hostname）] フィールドに、リモート CVP サーバーのホスト名を入力します。
e) [VRU接続ポート（VRU Connect port）] フィールドに **5000** と入力します。
f) [再接続間隔（秒）（Reconnect interval (sec)）] フィールドに **10** と入力します。
g) [ハートビート間隔（秒）（Heartbeat interval (sec)）] フィールドに **5** と入力します。
h) [DSCP] フィールドで **[CS3(24)]** を選択します。
i) [OK] をクリックします。

ステップ 7 PG Explorer を参照し、[ロジカルコントローラID（Logical Controller ID）] フィールドに値を入力します。

ステップ 8 [CTIコール後処理データ遅延（CTI Call Wrapup Data delay）] フィールドに **0** と入力します。

ステップ 9 [VRUレポーティング（VRU Reporting）] ペインで、**[サービスコントロール（Service Control）]** を選択し、**[キューレポーティング（Queue Reporting）]** をオンにします。[次へ（Next）] をクリックします。

ステップ 10 [デバイス管理プロトコルプロパティ（Device Management Protocol Properties）] ダイアログボックスで、次のように設定します。

a) サイド A を構成する場合は **[サイドAを優先（Side A Preferred）]** をクリックし、サイド B を構成する場合は **[サイドBを優先（Side B Preferred）]** をクリックします。

b) [サイドAプロパティ（Side A Properties）] パネルで、**[コールルーターはリモート（Call Router is Remote）]** を選択します。
c) [サイドBプロパティ（Side B Properties）] パネルで、**[コールルーターはリモート（Call Router is Remote）]** を選択します。
d) [使用可能な帯域幅（kbps）（Usable Bandwidth (kbps)）] フィールドは、デフォルト値のままにしておきます。
e) [ハートビート間隔（100 ms）（Heartbeat Interval (100ms)）] フィールドに **4** と入力します。[次へ（Next）] をクリックします。

ステップ 11 [周辺機器ゲートウェイネットワークインターフェイス（Peripheral Gateway Network Interfaces）] ダイアログボックスで、[PG Private Interfaces] および [PG Public (Visible) Interfaces] と入力します。

a) サイドAのプライベートインターフェイスセクションの **[QoS]** ボタンをクリックします。[PGプライベートリンクQoS設定（PG Private Link QoS Settings）] で **[QoSの有効化（Enable QoS）]** をオンにし、**[OK]** をクリックします。この手順は、サイドAにのみ適用します。
b) パブリック（表示）インターフェイス セクションで **[QoS]** ボタンをクリックします。[PG表示リンクQoS設定（PG Visible Link Qos Settings）] で、**[QoSの有効化（Enable QoS）]** をオンにし、**[OK]** をクリックします。この手順は、サイドAにのみ適用します。
c) [周辺機器ゲートウェイネットワークインターフェイス（Peripheral Gateway Network Interfaces）] ダイアログボックスで、**[次へ（Next）]** をクリックします。

ステップ 12 [設定情報の確認（Check Setup Information）] ダイアログボックスで **[次へ（Next）]** をクリックします。

ステップ 13 [設定完了（Setup Complete）] ダイアログボックスで、[完了（Finish）] をクリックします。

（注） すべてのUnified CCEコンポーネントがインストールされるまでUnified CCE/CC Node Managerを起動しないでください。

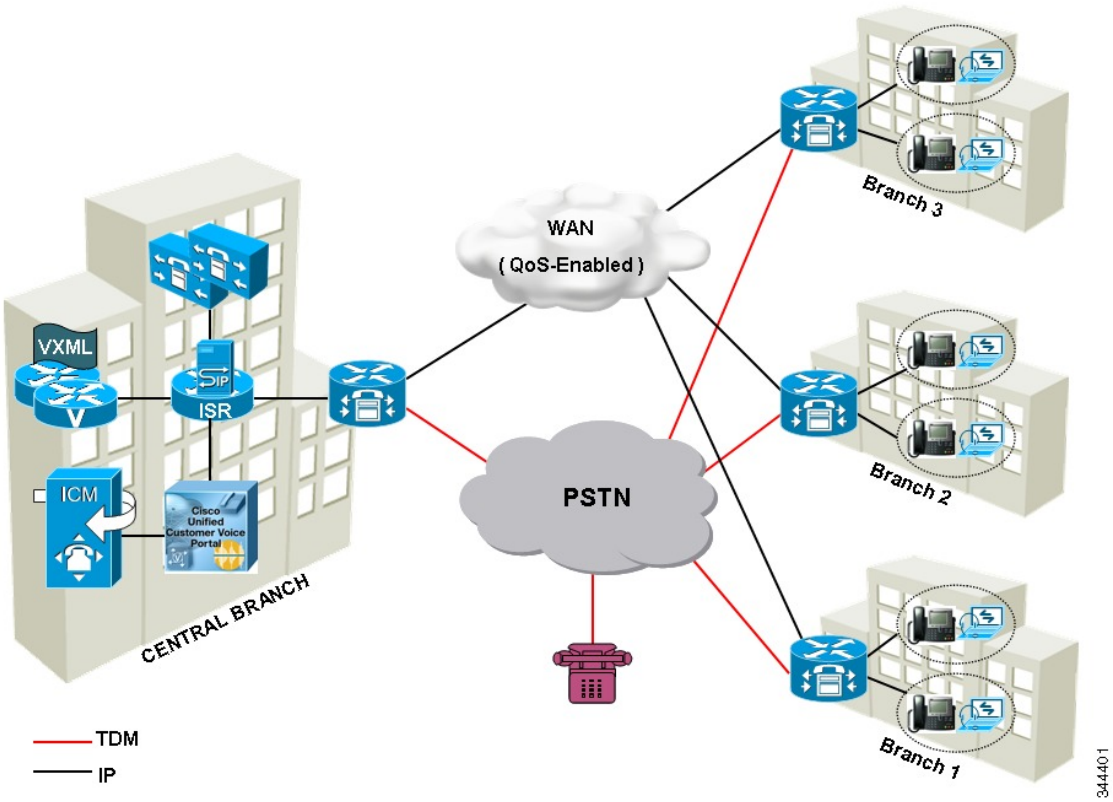
ローカル トランクの設定

ローカルトランクを構成するには、以下の手順を実行します。

• Unified CVP の構成 （502 ページ）
• Unified Communications Manager の構成 （503 ページ）

次の図に、ローカルトランクの構成を示します。

図 *22 :* ローカルトランクの構成



Unified CVP の構成

ローカルトランクに操作コンソールを使用して Unified CVP を構成するには、以下の手順を実行します。

手順

ステップ 1 **[デバイス管理（Device Management）] > [Unified CM] > [そのロケーションで同期を有効化（Enable Synchronization for Location）]** の順に選択し、同期を有効化したら、ログインに必要なログイン情報を入力します。

ステップ 2 **[システム（System）] > [ロケーション（Location）]** の順に選択し、**[同期（Synchronize）]** をクリックすると Unified CM（Publisher）で定義したロケーションを取得できます。

ステップ 3 **[システム（System）] > [ロケーション（Location）]** の順に選択し、ロケーションが Unified CM（Publisher）から同期されているか確認します。

ステップ 4 **[デバイス管理（Device Management）] > [ゲートウェイ（Gateway）]** の順に選択し、ゲートウェイイングレス、VXML および音声ブラウザ を定義します。

ステップ 5 **[システム（System）] > [ロケーション（Location）]** の順に選択し、ロケーションを選択します。

a) 拠点 ID とロケーション ID をロケーションに割り当てたら、関連するゲートウェイであるイングレス、VXML および音声ブラウザをロケーションに追加します。

ステップ 6 **[システム（System）]**>**[ロケーション（Location）]** の順に選択し、[コールサーバー展開（Call Server Deployment）] に移動したら、構成を展開するコールサーバーを選択します。

ステップ 7 [保存して展開（Save and Deploy）] をクリックします。

ステップ 8 SiteID の挿入ポイントには、ネットワーク VRU ラベルと相関 ID の間のデフォルト場所を使用します。

ステップ 9 **[システム（System）]** > **[ダイヤル番号パターン（Dialed Number Pattern）]** の順に選択し、静的ルートを作成し、通話をのブランチVXML ゲートウェイまたは音声ブラウザに送信します。Unified CVP ルーティングクライアントのネットワーク VRU ラベルに拠点 IDを追加します。

例：

Unified CVP ルーティングクライアントの Unified CCE ネットワーク VRU ラベルが 9999331010 であるとします。キューイングのために、CVP ルートはブランチ 1 の電話機からブランチ 1 の VXML ゲートウェイまたは音声ブラウザに送信され、ブランチ 1 の拠点コードとして「001」を使用します。またこの拠点コードは、着信音とエラーのルートを定義し、ローカルブランチ VXML ゲートウェイまたは音声ブラウザに送信します。

Unified Communications Manager の構成

ローカルトランクに対して、Unified Communications Manager を構成するには、以下の手順を実行します。

- ロケーションの追加 （503 ページ）
- アプリケーション ユーザー ロールの確認 （504 ページ）
- LBCAC 用 SIP プロファイルの構成 （504 ページ）
  - 中央ブランチ用 SIP トランクの展開 （505 ページ）
  - ローカルブランチ用 SIP トランクの展開 （505 ページ）
- ロケーション帯域幅マネージャの構成 （506 ページ）

ロケーションの追加

手順

ステップ 1 **Cisco Unified Communication Manager 管理** コンソールにログインします。

ステップ 2 **[システム（System）]** > **[ロケーション情報（Location Info）]** > **[ロケーション（Location）]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 **[ロケーション情報（Location Information）]** パネルの **[名前（Name）]** フィールドにロケーション名を入力します。

ステップ 5 **[リンクーこのロケーションと隣接ロケーション間の帯域幅（Links - Bandwidth Between This Location and Adjacent Locations）]** パネルで、以下を入力します。

a) ロケーションを選択します。

b) 帯域幅構成を入力します。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

電話機で作成したロケーションを選択します。「電話機の追加 （303 ページ）」を参照してください。

アプリケーション ユーザー ロールの確認

手順

ステップ 1 **Cisco Unified Communications Manager Administration** ページにログインします。

ステップ 2 **[ナビゲーション（Navigation）]** ドロップダウンリストで、**[Unified Serviceability]** を選択して、**[移動（Go）]** をクリックします。

ステップ 3 **[ツール（Tools）]** > **[コントロールセンター（Control Center）]** > **[機能サービス（Feature Services）]** の順に選択します。

ステップ 4 ドロップダウンリストで、**[サーバー（Server）]** を選択します。

ステップ 5 **Cisco AXL Web サービス**を起動していない場合は、起動します。

ステップ 6 **[ナビゲーション（Navigation）]** ドロップダウンリストで、**[Cisco Unified CM Administration]** を選択したら、**[移動（Go）]** をクリックします。

ステップ 7 **[ユーザー管理（User Management）]** > **[アプリケーションユーザー（Application User）]** の順に選択します。

ステップ 8 **[権限情報（Permissions Information）]** パネルで、標準 AXL API アクセスのロールを持つアプリケーションユーザーがあるかどうかを確認し、存在しない場合は、新しいアプリケーションユーザを作成するか、標準 AXL API アクセスのロールを持つグループにユーザーを追加します。

LBCAC 用 SIP プロファイルの構成

手順

ステップ 1 **Cisco Unified Communication Manager Administration** ページにログインします。

ステップ 2 **[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[SIP プロファイル（SIP Profile）]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 SIP プロファイルの名前を入力します。

ステップ 5 **[トランク固有構成（Trunk Specific Configuration）]** パネルにある **[次の基づき着信要求を新規トランクに再ルート（Reroute Incoming Request to New Trunk Based on）]** ドロップダウンリストで、**[x-cisco-origIP同様の通話情報ヘッダー（Call-Info Header with the Equal to x-cisco-origIP）]** を選択します。

ステップ 6 **[SIP OPTIONS Ping]** パネルで、**[OPTIONS Pingを有効にしてサービスタイプが「なし（デフォルト）」のトランクの接続先ステータスを監視する（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None(Default)"）]** チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

中央ブランチ用 SIP トランクの展開

手順

ステップ 1 SIP トランク セキュリティ プロファイルを作成するには、「SIP トランク セキュリティ プロファイルの作成 （539 ページ）」を参照してください。

ステップ 2 CVP/SIP プロキシサーバーに対する SIP トランクを作成します。

（注）
1. SIP トランクの作成の手順 5 で、**[すべての有効なUnified CMノードで実行（Run On All Active Unified CM Nodes）]** チェックボックスをオンにします。
2. SIP トランクに SIP プロファイルを関連付けます。SIP トランクの作成 （540 ページ）を参照してください。

これは、Unified Communications Manager ルーティングクライアントの ネットワーク VRU ラベルを Unified CVP サーバーにルーティングします。

ステップ 3 Unified Communications Manager ルーティングクライアントのネットワーク VRU ラベルを、CVP/SIP プロキシへの SIP トランクにポインティングするルートパターンを作成するには、「ルート パターンの追加 （297 ページ）」を参照してください。

ローカルブランチ用 SIP トランクの展開

手順

各イングレスゲートウェイへの SIP トランクを作成し、これらのイングレス TDM-IP ゲートウェイのロケーションを実際のブランチロケーションに割り当てます。

（注）
1. SIPトランクの作成の手順 5 で、**[すべての有効なUnified CMノードで実行（Run On All Active Unified CM Nodes）]** チェックボックスをオンにします。
2. SIP トランクに SIP プロファイルを関連付けます。SIP トランクの作成（540 ページ）を参照してください。

ロケーション帯域幅マネージャの構成

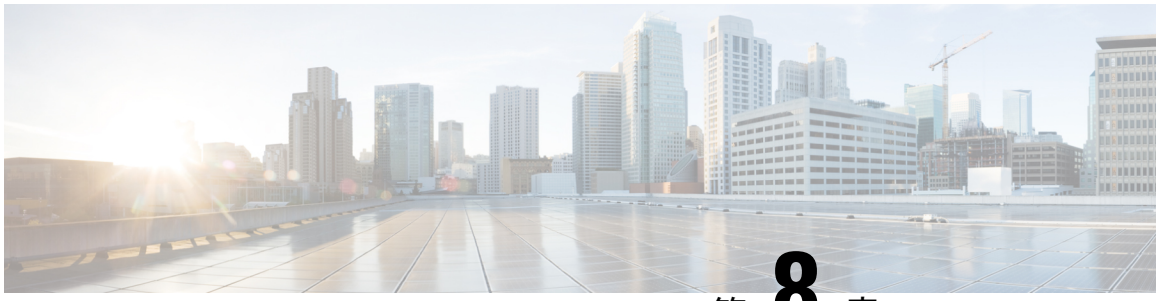
手順

ステップ 1 Cisco Unified Serviceability で、**[ツール（Tools）]** > **[コントロールセンター（Control Center）]** > **[機能サービス（Feature Services）]** の順に選択します。

ステップ 2 **Cisco Location Bandwidth Manager** が起動していない場合は、起動します。

ステップ 3 Cisco Unified CM Administration から、**[システム（System）]** > **[ロケーション情報（Location Info）]** > **[ロケーション帯域幅マネージャ グループ（Location Bandwidth Manager Group）]** の順に選択します。

ステップ 4 **[新規追加（Add New）]** をクリックして名前を入力し、アクティブおよびスタンバイメンバー（Cisco Unified Communications Manager ノード）を選択して **[保存（Save）]** をクリックします。



第 8 章

ソリューションの有用性

システムパフォーマンスの監視

監視システムのパーソナライズは、システム保守に役立つ 1 つの手順です。vCenter を使用して次の重要な HCS for CC コンポーネントを監視し、仮想マシンがシステムの許容範囲内で動作することを確認します。

- CPU
- メモリー
- ディスク
- ネットワーク

仮想マシンパフォーマンスの監視

仮想マシンは、次の表に示す仮想マシン パフォーマンス カウンタの指定された制限内で動作する必要があります。

表 *22 :* 仮想マシンのパフォーマンスカウンタ

カテゴリ	カウンタ	説明	しきい値
CPU	CPU 使用率（平均）	VM および各 vCPU の平均 CPU 使用率（パーセンテージ）。	65%
	CPU 使用率（MHz）（平均）	CPU 平均使用率（MHz）。	95 パーセンタイルは、VM で使用可能な合計 MHz の 65% 未満です。 合計 MHz = vCPU x（クロック速度）。
	CPU Ready	仮想マシンまたはその他のプロセスが CPU でスケジュールできるようになる前に、実行可能状態のキューで待機する時間。	150 ミリ秒
メモリー	メモリー使用率（平均）	メモリー使用率 = アクティブ/許可済み * 100	80 %
	アクティブなメモリー（平均）	ゲスト OS とそのアプリケーションがアクティブに使用または参照するメモリー。サーバーは、ホストのメモリー量を超えるとスワップを開始します。	95 パーセンタイルは、付与されたメモリーの 80% 未満です。
	メモリーバルーン（平均）	ESXi は、バルーンドライバを使用して、メモリーをあまり使用しない VM からメモリーを回復するため、アクティブなメモリー一式が大きい場合に使用できます。	0
	使用済みメモリースワップ（平均）	ESX サーバーのスワップ使用率。RAM スワップにディスクを使用します。	0

カテゴリ	カウンタ	説明	しきい値
ディスク	ディスク使用率（平均）	ディスク使用率=ディスク読み取り速度+ディスク書き込み速度	SAN がこの量のディスク I/O を処理するように構成されていることを確認します。
	ディスク読み取り速度	ディスクからデータを読み取る速度。	SAN がこの量のディスク I/O を処理するように構成されていることを確認します。
	ディスク書き込み速度	ディスクへのデータの書き込み速度。	SAN がこの量のディスク I/O を処理するように構成されていることを確認します。
	発行されたディスクコマンド	期間中にこのディスクで発行されたディスクコマンドの数。	ディスク IO/秒 IOPS＝発行されたディスクコマンド/20 SAN がこの量のディスク I/O を処理するように構成されていることを確認します。
	ディスクコマンドの停止	期間内にこのディスクで中止されたディスクコマンドの数。ディスクアレイによるコマンドへの応答に時間がかかり過ぎた場合、ディスクコマンドは中止されます。（コマンドタイムアウト）。	0
ネットワーク	ネットワーク使用率（平均）	ネットワーク使用率=データ受信率＋データ送信率	使用可能なネットワーク帯域幅の 30%。
	ネットワークデータ受信速度	このイーサネットポートでデータを受信する平均レート。	使用可能なネットワーク帯域幅の 30%。
	ネットワークデータ送信レート	このイーサネットポートでデータが送信される平均レート。	使用可能なネットワーク帯域幅の 30%。

ESXi パフォーマンスモニタリング

仮想マシンは、次の表に示す ESXi パフォーマンスカウンタの指定された制限内で動作する必要があります。リストされているカウンタは、コンタクトセンターコンポーネントを含むすべてのホストに適用されます。

表 *23 : ESXi* パフォーマンスカウンタ

カテゴリ	カウンタ	説明	しきい値
CPU	CPU 使用率（平均）	ESXi サーバー全体および各 CPU プロセッサの平均 CPU 使用率（パーセンテージ）。	60%
	CPU 使用率（MHz）（平均）	ESXi サーバー全体および各 CPU プロセッサの CPU 使用率の平均（MHz）。	使用可能な CPU クロックサイクルの 60%。
メモリー	メモリー使用率（平均）*	メモリー使用率 = アクティブ/許可済み * 100	80%
	VMKernel で使用されるメモリー	VMKernel で使用されるメモリー	95 パーセンタイルは 2GB の 80% 未満です。
	メモリーバルーン（平均）	ESX バルーンドライバを使用して、メモリーをあまり使用しない VM からメモリーを回復するため、アクティブなメモリーセットが大きい場合に使用できます。	0
	SwapUsed	ESX サーバーのスワップ使用率。RAM スワップにディスクを使用します。	0

カテゴリ	カウンタ	説明	しきい値
ディスク	発行されたディスクコマンド	期間内にこのディスクで発行されたディスクコマンドの数。	ディスク IO/秒 IOPS＝発行されたディスクコマンド/20
	中止されたディスクコマンド	期間内にこのディスクで中止されたディスクコマンドの数。 ディスクアレイによるコマンドへの応答に時間がかかり過ぎた場合、ディスクコマンドは、中止されます。（コマンドタイムアウト）。	0
	ディスクコマンド遅延	ゲスト OS の観点から見たコマンドにかかる平均時間。 ディスクコマンド遅延 = Kernel コマンド遅延+ 物理的デバイスのコマンド遅延。	20 ミリ秒。
	Kernel ディスクコマンド遅延	ESXi Server VMKernel で 1 コマンドあたりに費やされた平均処理時間	Kernel コマンド遅延は、物理的デバイスのコマンド遅延と比べて非常に小さく、ゼロに近い値である必要があります。
ネットワーク	ネットワーク使用率（平均）	ネットワーク使用率=データ受信率 + データ送信率	使用可能なネットワーク帯域幅の 30%。
	ネットワークデータ受信速度	このイーサネットポートでデータを受信する平均レート。	使用可能なネットワーク帯域幅の 30%。
	ネットワークデータ送信レート	このイーサネットポートでデータが送信される平均レート。	使用可能なネットワーク帯域幅の 30%。
	droppedTx	ドロップされた送信パケットの数。	0
	droppedRx	ドロップされた受信パケットの数。	0

* Java 仮想マシンのメモリー使用量が原因で、CVP 仮想マシンが、80% のメモリー使用量しきい値を超えています。

Unified System CLI を使用したシステム診断情報の収集

Unified Contact Center 操作で問題が発生した場合、Unified System CLI ツールを使用すると、シスコのエンジニアが確認するためのデータを収集できます。

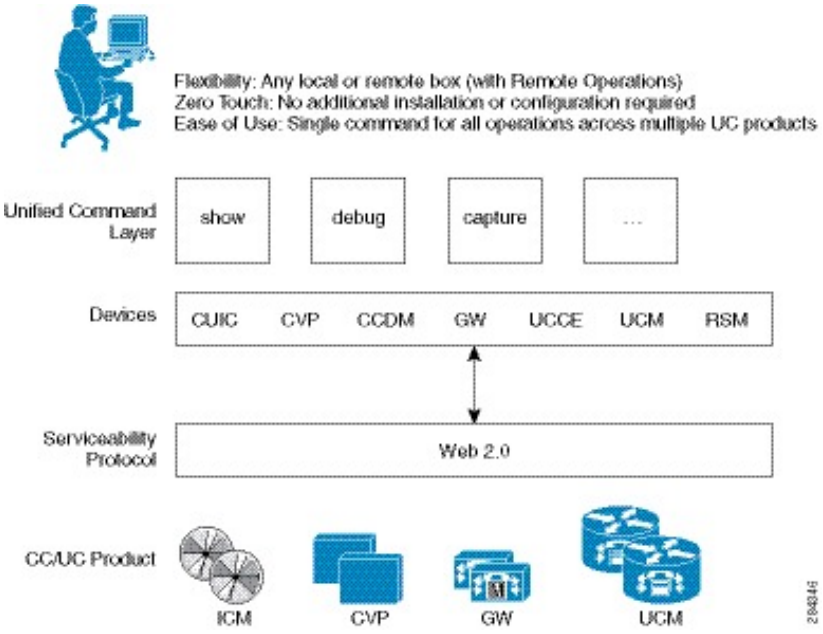
たとえば、コールが適切に処理されていないと考えられる場合に、System CLI を使用できます。この場合、**show tech-support** システムコマンドを使用すると、データを収集して、シスコサポートにそのデータを送信できます。

The Unified System CLI には、以下の機能が含まれます。

- すべての Unified CCE および Unified CVP サーバーに自動的にインストールされます。
- Unified CCDM/OAMP サーバーからソリューショントポロジ全体を自動的に取得します。
- どの製品やサーバーでも一貫したコマンドを使用します。
- Windows のスケジュールジョブとして実行します。

以下の図では、Unified System CLI が通信するデバイスと Cisco Unified 製品が表示されています。

図 *23 : Unified System CLI* コマンド



コンポーネントからシステム診断情報を収集するには、以下の手順を実行します。

- ローカルマシンで Unified System CLI を実行 （513 ページ）
- リモートマシンで Unified System CLI を実行 （513 ページ）

ローカルマシンで Unified System CLI を実行

手順

ステップ 1 Unified CCE サーバーからシステム CLI を起動します。

a) **[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Unified CCEツール（Cisco Unified CCE Tools）] > [Unified System CLI]** の順に選択します。

b) ユーザー名（domain.com\username）とパスワードを入力します。

c) インスタンスを入力して（任意）、**[入力（Enter）]** をクリックします。

ステップ 2 Unified CVP サーバーからシステム CLI を起動します。

a) **[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Unified カスタマー音声ポータル（Cisco Unified Customer Voice Portal）] > [Unified System CLI]** の順に選択します。

b) wsmadmin ユーザーのユーザー名（wsmadmin）とパスワードを入力します。

c) Enter を押します。

ステップ 3 CCDM サーバーからシステム CLI を起動します。

a) **[スタート（Start）] > [すべてのプログラム（All Programs）] > [ドメインマネージャ（Domain Manager）] > [Unified System CLI]** の順に選択します。

b) wsmadmin ユーザーのユーザー名（wsmadmin）とパスワードを入力します。

c) インスタンスを入力して（任意）、**[入力（Enter）]** をクリックします。

リモートマシンで Unified System CLI を実行

手順

ステップ 1 別のネットワーク管理仮想マシンに Unified CVP Operations Console Resource Manager（ORM）をインストールすると、ログ収集中に、重要なコンポーネントのパフォーマンスが影響を受けないようになります。

ステップ 2 Unified CVP OAMP を使用して、ネットワーク管理マシンを Web サービスとして追加し、展開します。

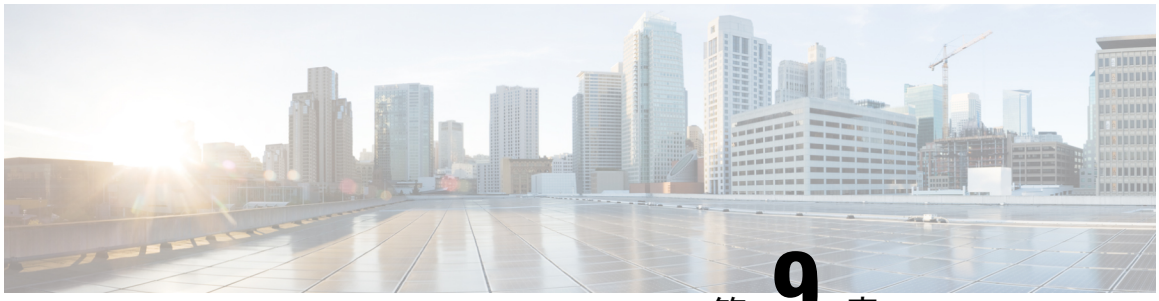
ステップ 3 次の項の説明に従って、OAMP を使用してすべてのソリューション コンポーネントをデバイスとして追加したことを確認します。

- Unified CCE デバイスの追加 （76 ページ）
- Unified Communications Manager デバイスの追加 （77 ページ）
- Unified Intelligence Center デバイスの追加 （77 ページ）

- Unified CVP レポーティングサーバーの構成 （73 ページ）

ステップ 4 Unified System CLI を実行して、いずれかのコンポーネントからシステム診断情報を収集します。

show tech-support システムコマンドを使用すると、一部またはすべてのコンポーネントからすべての情報とログを収集できます。他のコマンドを使用して、情報のサブセットを収集できます。



第 9 章

付録

新しいドメインに CCE サーバーを移行

仮想マシンと新しいドメインの関連付け

次の手順を実行して、仮想マシンを新しいドメインに関連付けます。

手順

ステップ 1 ローカル管理者アカウントを使用してマシンにログインします。

ステップ 2 **Server Manger** を起動し、**[システムプロパティの変更（Change System Properties）]** をクリックします。

ステップ 3 古いドメインからマシンを削除し、再起動します。

ステップ 4 ローカル管理者アカウントを使用して、マシンに再度ログインします。

ステップ 5 **Server Manger** を起動し、**[システムプロパティの変更（Change System Properties）]** をクリックします。

ステップ 6 **[全修飾ドメイン名（`Fully Qualified Domain Name`）]** を入力したら、**[OK]** をクリックします。

ステップ 7 ドメイン管理者のユーザー名とパスワードを入力します。

ステップ 8 サーバーをリブートして、ドメインのログイン情報を使用してログインします。

Unified CCE に新しいドメインに関連付ける

以下の手順に従い、 Unified CCE を新規ドメインに関連付けます。

手順

ステップ 1 **Cisco Unified CCE Tools** フォルダから、**ドメイン マネージャ** アプリケーションを開きます。

ステップ 2 **[すべてのプログラム（All Programs）]** > **[Cisco Unified CCEツール（Cisco Unified CCE Tools）]** > **[ドメインマネージャ（Domein Manager）]** の順に選択します。

ステップ 3 [Domain Name] を選択します。

ステップ 4 シスコルート組織単位（OU）、ファシリティ組織単位（OU）、およびインスタンス組織単位（OU）を追加します。

ステップ 5 以下を構成して、Unified CCE アプリケーション向けのドメインを変更します。

a) Web Setup を実行します。

b) **[インスタンス管理（Instance Management）]** を選択します。

c) 変更するインスタンスを選択し、**[ドメインの変更（Change Domain）]** をクリックします。

ドメインの変更ページが開き、現在構成されているドメインと新規ドメイン名が表示されます。

d) [保存（Save）] をクリックします。

クエリーが送信され、ドメインを変更するかどうかが確認されます。

e) **[はい（Yes）]** をクリックします。

インスタンスリストページが表示されます。

（注） Loggers and Administration & Data Servers コンポーネントのサービス操作を実行するために、ドメインユーザーが新しいドメインで作成されていることを確認します。

注意 すべてのディストリビュータ サービスおよび Logger サービスに同じドメイン ユーザ アカウントを使用します。Logger とディストリビュータに異なるドメインアカウントを使用する場合は、ディストリビュータ サービスのユーザ アカウントがサイド A とサイド B のローカル Logger `UcceService` グループに追加されていることを確認してください。

Cisco Unified Communications Manager SUBSCRIBER Mobile Agent コールフローの追加

この例では、サブカスタマーの 1 つである SUBCUST1-CUCM-SUB-MOBILE-AGENT に対して隣接関係（アジャセンシー）を作成します。モバイル エージェント ログインの場合。

```
config
 sbc
  signaling
   adjacency sip SUBCUST1-CUCM-SUB-MOBILE-AGENT
        description "Trunk SUBCUSTOMER 1 CUCM subscriber for Mobile Agent call flow"
        account cust1
        interop
          preferred-transport tcp
          message-manipulation
            edit-profiles inbound he-dtmf
        force-signaling-peer all-requests
        adjacency-type preset-core
        service-address SA-cust1
          # service-network 1
          # signaling-local-address ipv4 20.20.20.2
        signaling-local-port 5078
        signaling-peer 20.20.20.130
        signaling-peer-port 5060
        statistics-setting summary
        activate
```

HCS for CC でサポートされているガジェット

ガジェットにアクセスするには、管理およびデータサーバーで、**[スタート（Start）]** をクリックし、**[すべてのプログラム（All Programs）] > [Cisco Unified CCE ツール（Cisco Unified CCE Tools）] > [管理ツール（Administration Tools）]** の順に選択したら、Unified CCE Web 管理ツールを開きます。以下の表では、HCS for CC ガジェットでサポートされている CRUD 操作を示しています。

ガジェット	作成	読み取り	更新	削除
エージェント		x	x（属性割り当てのみ）	
エージェント状態のトレース		x	x	
属性	x	x	x	x
バケット間隔	x	x	x	x
一括ジョブ	x	x	x	x
コンテキストサービス		x	x	
展開	x	x	x	x
メディア ルーティング ドメイン	x	x	x	x
ネットワーク VRU スクリプト	x	x	x	x
プレシジョンキュー	x	x	x	x
理由コード	x	x	x	x
設定（輻輳制御）		x	x	
シングルサインオン		x	x	

x：サポートされているの略

HCS for CC 対応 API

（注） エージェントは属性のみを更新できます。

API フィルタは、URL と導入モデルを参照して API にアクセスできるかどうかを判断するために構築されます。また、読み取り/書き込み（GET/PUT/POST/DELETE）または各 API への読み取り専用アクセスにも対応しています。

以下のテーブルに、HCS for CC 導入モデル対応の API を示します。

表 *24 : HCS for CC* 対応 *API*

API	作成	読み取り	更新	削除
Active Directory ドメイン（Active Directory Domain）		x		
管理者	x	x	x	x
エージェント		x	x （属性割り当てのみ）	
エージェント状態のトレース		x	x	
エージェント チーム		x		
属性	x	x	x	x
バケット間隔	x	x	x	x
一括ジョブ	x	x	x	x
輻輳制御		x	x	
コンテキストサービス構成		x	x	
コンテキスト サービス登録		x	x	
展開タイプの情報		x	x	
ダイヤル番号		x		
マシンインベントリ	x	x	x	x
メディア ルーティング ドメイン	x	x	x	x
ネットワーク VRU スクリプト	x	x	x	x
オペレーション	x	x	x	x
アウトバウンドAPI：アウトバウンドキャンペーン	x	x	x	x
アウトバウンドAPI：キャンペーンステータス		x		

API	作成	読み取り	更新	削除
アウトバウンドAPI：電話禁止	x	x	x	x
アウトバウンドAPI：インポート	x	x		x
アウトバウンドAPI：パーソナルコールバック	x	x	x	x
アウトバウンドAPI：タイムゾーン		x		
周辺機器ゲートウェイ		x		
プレシジョンキュー	x	x	x	x
理由コード	x	x	x	x
スキャン			x	
有用性		x		
シングルサインオンのグローバルステータス		x	x	
シングルサインオン登録		x	x	
シングルサインオンステータス		x	x	
スキルグループ		x	x	
ステータス		x		

x：サポートされているの略

HCS for CC でサポートされているガジェット

ガジェットにアクセスするには、管理およびデータサーバーで、**[スタート（Start）]**をクリックし、**[すべてのプログラム（All Programs）] > [Cisco Unified CCEツール（Cisco Unified CCE Tools）] > [管理ツール（Administration Tools）]** の順に選択したら、Unified CCE Web 管理ツールを開きます。以下の表では、HCS for CC ガジェットでサポートされている CRUD 操作を示しています。

ガジェット	作成	読み取り	更新	削除
エージェント		x	x（属性割り当てのみ）	

ガジェット	作成	読み取り	更新	削除
エージェント状態のトレース		x	x	
属性	x	x	x	x
バケット間隔	x	x	x	x
一括ジョブ	x	x	x	x
コンテキストサービス		x	x	
展開	x	x	x	x
メディア ルーティング ドメイン	x	x	x	x
ネットワーク VRU スクリプト	x	x	x	x
プレシジョン キュー	x	x	x	x
理由コード	x	x	x	x
設定（輻輳制御）		x	x	
シングルサインオン		x	x	

x：サポートされているの略

管理者 API

管理者は、システムへのアクセス権が付与された Active Directory ユーザーです。

管理者 API を使用して、データベースで現在定義されている管理者をリストし、新しい管理者を定義し、既存の管理者を表示、編集、および削除します。

URL

```
https://<server>:<serverport>/unifiedconfig/config/administrator
```

管理者 API の詳細については、https://developer.cisco.com/site/packaged-contact-center/documentation/index.gsp の「*Cisco Packaged Contact Center Enterprise* 開発者リファレンス ガイド」を参照してください。

Cisco Unified Communications Manager の構成

Cisco Unified Communications Manager のプロビジョニング

Unified Communications Manager をプロビジョニングするには、以下の手順を実行します。

（注） このセクションは参照目的のみに使用してください。Unified Communications Domain Manager を使用して Unified CM を構成する必要があります。

デバイス プールの設定

デバイス プールを設定するには、以下の手順を実行します。

手順

ステップ 1 **[システム（System）] > [デバイスプール（Device Pool）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 デバイス プール名に適切な **デバイス プール名**を指定します。

ステップ 4 対応する CallManager グループを **Cisco Unified Communications Manager グループ**で選択します。

ステップ 5 適切な**日付および時刻グループ**と**地域**を選択します。

ステップ 6 適切なメディア リソース グループ リストを **メディア リソース グループ リストから選択します。**

ステップ 7 [保存（Save）] をクリックします。

Unified Communications Manager グループの設定

Unified Communications Manager を Unified Communications Manager グループに追加するには、以下の手順を実行します。

Unified Communications Manager グループを構成する前に、そのグループにメンバーとして割り当てる Unified Communications Managers を構成する必要があります。

手順

ステップ 1 **Cisco Unified Communication Manager Administration** ページにログインし、**[システム（System）] > [サーバー（Server）]** の順に選択します。

ステップ 2 Publisher と Subscriber の両方を構成したことを確認してください。

a) [新規追加（Add New）] をクリックします。

b) Cisco Unified Communications Manager 音声/ビデオなどの適切なサーバータイプを選択し、**[次へ（Next）]** をクリックします。

c) **ホスト名/IP アドレス** を入力します。

d) [保存（Save）] をクリックします。

ステップ 3 **[システム（System）] > [Cisco Unified CM]** の順に選択します。

ステップ 4 [検索（Find）] をクリックします。

ステップ 5 Publisher と Subscriber の両方を構成したことを確認してください。

ステップ 6 **[システム（System）] > [Cisco Unified CMグループ（Cisco Unified CM Group）]** の順に選択します。

ステップ 7 両方の Cisco Unified Communications Manager をデフォルトの Unified Communications Manager グループに追加します。**[デフォルト（Default）]** を選択し、[利用可能な Cisco unified communication managers（Available Cisco unified communication managers）] で、Selected Cisco Unified Communications Managers に対して Publisher と Subscriber の両方を選択します。

ステップ 8 [保存（Save）] をクリックします。

CTI ルートポイントの設定

エージェントが転送と会議に使用するコンピュータテレフォニーインテグレーション（CTI）ルートポイントを追加するには、以下の手順を実行します。

手順

ステップ 1 **[デバイス（Device）]** > **[CTIルートポイント（CTI Route Point）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ワイルドカード文字列である **XXXXX** を使用して、Unified CCE で構成したダイヤル番号の桁を表します。

（注） たとえば、エージェントの電話用に Unified CCE で事前設定された着信番号は 10112 です。

ステップ 4 適切なデバイス プールを選択します。

ステップ 5 [保存（Save）] をクリックします。

トランクの設定

Unified CVP サーバーのトランクを構成するには、以下の手順を実行します。

手順

ステップ 1 **[デバイス（Device）]** > **[トランク（Trunk）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [トランク タイプ（Trunk Type）] ドロップダウンリストで、[SIP トランク（SIP Trunk）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [デバイス名（Device Name）] フィールドに、SIP トランク名を入力します。

ステップ 5 [説明（Description）] フィールドに、SIP トランクの説明を入力します。

a) [デバイス名（Device Name）] フィールドに、SIP トランク名を入力します。

b) 適切なデバイスプールを選択します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [トランク構成（Trunk Configuration）] ウィンドウで、適切な設定を入力します。

a) **[メディア終了ポイント必須（Media Termination Point Required）]** チェックボックスをオフにします。

b) **宛先アドレス**を入力します。

c) 適切な SIP トランク セキュリティ プロファイルを選択します。
d) **[SIPプロファイル（SIP Profile）]** ドロップダウンリストで、**[Standard SIP Profile]** を選択します。
e) [DTMFシグナリングメソッド（DTMF Signaling Method）] ドロップダウンリストで **[RFC 2833]** を選択します。

ステップ 8 [保存（Save）] をクリックします。

アプリケーションユーザーの設定

手順

ステップ 1 で、**[ユーザー管理（User Management）]** > **[アプリケーションユーザー（Application User）]** の順に選択します。

ステップ 2 [アプリケーションユーザーの構成（Application User Configuration）] ウィンドウで、[新規追加（Add New）] をクリックします。

ステップ 3 エンタープライズ パラメータの設定 （529 ページ） で入力したユーザー ID を入力します。Unified CCE は、ユーザー ID を pguser として定義します。

ステップ 4 **cisco** または選択した を [パスワード（Password）] フィールドに入力します。

（注） Unified CCE でこのユーザー ID またはパスワードを変更した場合は、Unified Communications Manager アプリケーションユーザー構成も変更する必要があります。

ステップ 5 アプリケーションユーザを Standard CTI Enabled グループとロールに追加します：

a) [アクセス制御グループに追加（Add to Access Control Group）] をクリックします。
b) **標準 CTI を有効にする**グループを選択します。
c) **標準 CTI Connected Xferおよび conf をサポートする電話制御を許可する** グループを選択します。
d) **標準 CTI ロールオーバー モードをサポートする電話制御を許可する** グループを選択します。
e) [選択項目の追加（Add Selected）] をクリックします。
f) [保存（Save）] をクリックします。

ステップ 6 CTI ルートポイントと電話機をアプリケーションのユーザに関連付けます。

ステップ 7 [保存（Save）] をクリックします。

SIPオプションの設定

手順

ステップ 1 Cisco Unified Communications Manager Administration ページにログインします。

ステップ 2 **[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[SIP プロファイル（SIP Profile）]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 **名前** を入力します。

ステップ 5 **[SIP OPTIONS Ping]** パネルで、**[OPTIONS Pingを有効にしてサービスタイプが「なし（デフォルト）」のトランクの接続先ステータスを監視する（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None(Default)"）]** チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

（注） SIP プロファイルが作成されたら、新しく追加された SIP プロファイルをエージェントの電話機にマッピングします。

ルートパターンの設定

手順

ステップ 1 **[コールルーティング（Call Routing）]** > **[ルートハント（Route Hunt）]** > **[ルートパターン（Route Pattern）]** の順に選択します。

ステップ 2 Unified CVP ルーティングクライアントのルートパターンを以下のように追加します。

a) [新規追加（Add New）] をクリックします。

b) [ルートパターン（Route Pattern）] フィールドに **7777777777!** と入力します。

c) **[ゲートウェイ/ルートリスト（Gateway/Route List）]** フィールドで、**SIPTRK_to_CVP_1** を選択します。

d) [保存（Save）] をクリックします。

ステップ 3 Cisco Unified Communications Manager のルーティング クライアントのルートパターンを追加します。

a) [新規追加（Add New）] をクリックします。

b) [ルートパターン（Route Pattern）] フィールドに **8881111!** と入力します。

c) **[ゲートウェイ/ルートリスト（Gateway/Route List）]** フィールドで、**SIPTRK_to_CVP_1** を選択します。

d) [保存（Save）] をクリックします。

（注） ルートパターンは、Unified CCE で定義したネットワーク VRU ラベルと一致する必要があります。

会議ブリッジの設定

手順

ステップ 1 **[メディアリソース（Media Resources）]** > **[会議ブリッジ（Conference bridge）]** の順に選択します。

ステップ 2 配置内の入力/VXML ゲートウェイの組み合わせごとに、会議ブリッジを追加します。

ステップ 3 [会議ブリッジ名（Conference Bridge name）] フィールドに、ゲートウェイでの構成と一致する会議ブリッジ名の固有識別子を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [設定の適用（Apply Config）] をクリックします。

メディア ターミネーション ポイントの設定

手順

ステップ 1 **[メディアリソース（Media Resources）]** > **[メディアターミネーションポイント（Media Termination Point）]** の順に選択します。

ステップ 2 配置内の入力/VXML ゲートウェイの組み合わせごとに、メディア ターミネーション ポイントを追加します。

ステップ 3 配置内の入力/VXML ゲートウェイの組み合わせごとに、[Media Termination Point Name] フィールドにメディア ターミネーション ポイント名を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [設定の適用（Apply Config）] をクリックします。

トランスコーダの設定

手順

ステップ 1 **[メディアリソース（Media Resources）]** > **[トランスコーダ（Transcoder）]** の順に選択します。

ステップ 2 配置内の入力/VXML コンボ ゲートウェイごとに、トランスコーダを追加します。

ステップ 3 [デバイス名（Device Name）] フィールドに、ゲートウェイ上の構成と一致するトランスコーダ名の固有識別子を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 [設定の適用（Apply Config）] をクリックします。

メディアリソースグループの設定

会議ブリッジ、メディアターミネーションポイント、およびトランスコーダのメディアリソースグループを設定するには、次の手順を実行します。

手順

ステップ 1 **[メディアリソース（Media Resources）]>[メディアリソースグループ（Media Resource Group）]** を選択します。

ステップ 2 会議ブリッジ用メディアリソースグループを追加します。

ステップ 3 配置内の入力/VXML ゲートウェイの組み合わせごとに設定されたハードウェア会議ブリッジリソースをすべて選択して、グループに追加します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 **[メディアリソース（Media Resources）]>[メディアリソースグループ（Media Resource Group）]** を選択します。

ステップ 6 メディア ターミネーション ポイント用メディアリソースグループを追加します。

ステップ 7 配置内の入力/VXML ゲートウェイの組み合わせごとに設定された、ハードウェア メディア ターミネーション ポイントをすべて選択し、グループに追加します。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 **[メディアリソース（Media Resources）]>[メディアリソースグループ（Media Resource Group）]** を選択します。

ステップ 10 トランスコーダ用メディアリソースグループを追加します。

ステップ 11 配置内の入力/VXML ゲートウェイの組み合わせごとに設定されたトランスコーダをすべて選択して、グループに追加します。

ステップ 12 [保存（Save）] をクリックします。

メディア リソース グループ リストの設定と関連付け

メディアリソース グループ リストを設定し、関連付けるには、次の手順を実行します。メディア リソース グループ リストを次のデバイスとデバイス プールに追加します。

手順

ステップ 1 **[メディアリソース（Media Resources）]** > **[メディアリソースグループリスト（Media Resource Group List）]** の順に選択します。

ステップ 2 メディアリソースグループリストを追加し、すべてのメディアリソースグループを関連付けます。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 **[システム（System）]** > **[デバイスプール（Device Pool）]** の順に選択します。

ステップ 5 [デフォルト（Default）] をクリックします。

ステップ 6 [メディアリソースグループリスト（Media Resource Group List）] ドロップダウンリストで、ステップ 2 で追加したメディアリソースグループを選択します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 [リセット（Reset）] をクリックします。

ステップ 9 **[デバイス（Device）]** > **[CTIルートポイント（CTI Route Point）]** の順に選択します。

ステップ 10 設定されている CTI ルートポイントをクリックします。詳細については、CTI ルートポイントの設定 （524 ページ）を参照してください。

ステップ 11 [メディアリソースグループリスト（Media Resource Group List）] ドロップダウンリストで、ステップ 2 で追加したメディアリソースグループを選択します。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 [リセット（Reset）] をクリックします。

ステップ 14 **[デバイス（Device）]** > **[SIP トランク（SIP Trunk）]** の順に選択します。

ステップ 15 に構成した SIP トランクをクリックします。詳細については、トランクの設定 （524 ページ）を参照してください。

ステップ 16 [メディアリソースグループリスト（Media Resource Group List）] ドロップダウンリストで、ステップ 2 で追加したメディアリソースグループを選択します。

ステップ 17 [保存（Save）] をクリックします。

ステップ 18 [リセット（Reset）] をクリックします。

エンタープライズ パラメータの設定

手順

ステップ 1 **システム** > **エンタープライズ パラメータ** を選択します。

ステップ 2 クラスタの完全修飾ドメイン名を設定します。

例：

ccm.hcscc.icm

（注） クラスタの完全修飾ドメイン名は、Unified CVP で定義されている Unified Communications Manager サーバーグループの名前です。

サービスパラメータの設定

会議ブリッジがサポートする会議参加者の最大数と、メディアターミネーションポイントがサポートするコールパーティの最大数を変更するには、以下の手順を実行します。このパラメータの変更は、SCC 導入モデルでのみ必要です。

手順

ステップ 1 Cisco Unified Communications Manager Administration ページにログインします。

ステップ 2 [システム（System）] タブで、**[サービスパラメータ（Service Parameter）]** を選択します。

ステップ 3 ドロップダウンリストで、Cisco Unified Communications Manager サーバーを選択します。

ステップ 4 「Cisco IP Voice Media Streaming App」というサービスを選択します。

ステップ 5 [会議ブリッジ（CFB）パラメータ（Conference Bridge (CFB) Parameters）] で、「Call Count」パラメータのデフォルト値を変更します（0 ー 256）。

ステップ 6 [メディアターミネーションポイント（MTP）パラメータ（Media Termination Point（MTP）Parameters）] で、「Call Count」パラメータのデフォルト値（0 ー 512）を変更します。

録音プロファイルの設定

手順

ステップ 1 Cisco Unified Communications Manager Administration ページにログインします。

ステップ 2 **[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[録音プロファイル（Recording Profile）]** の順に選択します。

ステップ 3 録音プロファイル名と録音宛先アドレスを設定し（MediaSenseに構成したルートパターン番号を入力）、**[保存（Save）]** をクリックします。

デバイスの構成

手順

ステップ 1 音声分岐電話を選択します。

ステップ 2 このデバイスの**組み込みブリッジ**構成を選択し、設定を **[オン（ON）]** に変更します。

ステップ 3 録音する回線の**電話番号構成**ページにアクセスします。

ステップ 4 録音パートナーを使用する場合は、録音パートナーの推奨事項に従って、ドロップダウンリストで、**[通話の自動録音を有効化（Automatic Call Recording Enabled）]** または **[アプリケーション（Application）]**、**[呼び出し通話録音の有効化（Invoked Call Recording Enabled）]** のいずれかを選択します。録音パートナーを使用しない場合は、**[通話の自動録音を有効化**（Automatic Call Recording Enabled）] を選択します。

ステップ 5 前の手順で作成した録音プロファイルを選択します。

録音デバイスに対して iLBC、iSAC および g.722 を無効化

以下の対応コーデックを使用した Cisco MediaSense 録音セッション

- オーディオ録音：g.711（aLaw または μLaw）または g.729（a または b）コーデック
- ビデオ録画：h.264 基準（48k Hz サンプリングレートのみ）コーデック

⚠

注意 Cisco MediaSense は、internet Low Bit Rate Codec (iLBC) または internet Speech Audio Codec (iSAC) をサポートしません。その結果、Cisco MediaSense 構成に進む前に、Unified CM でこれらの機能を無効化する必要があります。

手順

ステップ 1 Cisco Unified Communications Manager Administration ページにログインします。

ステップ 2 **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

ステップ 3 ドロップダウンリストで、**[サーバー（Server）]** を選択します。

ステップ 4 ドロップダウンリストで、**[サービス（Service）]** を選択します。
サービスパラメータ構成ページが表示されます。

ステップ 5 **[クラスタ全体のパラメータ（システム ー ロケーションおよびリージョン）（Cluster-wide parameters (System - Location and Region)）]** パネルで、以下のドロップダウンリストで **[録音可能なデバイスを除くすべてのデバイス（Enable for All Devices Except Recording-Enabled Devices）]** を選択します。

- **iLBC コーデックの有効化**
- **iSAC コーデックの有効化**
- **G722 Codec 対応**

ステップ 6 [保存（Save）] をクリックします。

保留音サーバーのオーディオソースの設定

手順

ステップ 1 **[メディアリソース（Media Resources）]** > **[保留音オーディオソース（Music On Hold Audio Source）]** の順に選択します。

ステップ 2 デフォルトのサンプルオーディオソースを選択します。

ステップ 3 ドロップダウンリストで **[最初のアナウンス（Initial Announcement）]** を選択します。これはオプションです。

ステップ 4 [保存（Save）] をクリックします。

（注） 新規オーディオソースを作成する場合は以下の手順に従います。

a) [新規追加（Add New）] をクリックします。
b) ドロップダウンリストで、**[MOHオーディオストリーム番号（MOH Audio Stream Number）]** を選択します。
c) ドロップダウンリストで、**[MOHオーディオソースファイル（MOH Audio Source File）]** を選択します。
d) **[MOHソース名（MOH Source Name）]** を入力します。
e) ドロップダウンリストで、**[最初のアナウンス（Initial Announcement）]** を選択します。
f) [保存（Save）] をクリックします。

保留音用サービスパラメータの設定

手順

ステップ 1 **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

ステップ 2 **[MOHサーバー（MOH Server）]** を選択します。

ステップ 3 **Cisco IP 音声メディア ストリーミング アプリ** サービスを選択します。

ステップ 4 **[対応MOHコーデック（Supported MOH Codecs）]** Finesse で、必要な**コーデック**を選択し、ポップアップウィンドウで **[OK]** をクリックします。

ステップ 5 [保存（Save）] をクリックします。

保留音用電話機構成の設定

手順

ステップ 1 **[デバイス（Device）]** > **[電話機（Phone）]** の順に選択します。

ステップ 2 MOH を構成する電話機を選択します。

ステップ 3 **[ユーザー保留MOHオーディオソース（User Hold MOH Audio Source）]** に対して、**[保留音サーバーオーディオソースの追加（Add Music on Hold Server Audio Source）]** セクションで追加された**オーディオソース**を選択します。

ステップ 4 **[ネットワーク保留MOHオーディオソース（Network Hold MOH Audio Source）]** に対して、**[保留音サーバーのオーディオソースの追加（Add Music on Hold Server Audio Source）]** セクションで追加した**オーディオソース**を選択します。

ステップ 5 **[保存して構成を適用（Save and Apply Config）]** をクリックし、電話機をリセットします。

パーティションの設定

サブカスタマーごとに以下の手順を実行します。

手順

ステップ 1 **Cisco Unified Communications 管理ページ**にログインします。

ステップ 2 **[コールルーティング（Call Routing）]** > **[コントロールのクラス（Class of Control）]** > **[パーティション（Partition）]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 **[名前（Name）]** フィールドにパーティション名を入力します。

ステップ 5 [保存（Save）] をクリックします。

コーリングサーチスペースの設定

サブカスタマーごとに以下の手順を実行します。

手順

ステップ 1 **Cisco Unified Communications Manager Administration ページ**にログインします。

ステップ 2 **[コールルーティング（Call Routing）]** > **[コントロールのクラス（Class Of Control）]** > **[コーリングサーチスペース（Calling Space Search）]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 **[名前（Name）]** フィールドに、コーリングサーチスペース名を入力します。

ステップ 5 **[使用可能なパーティション（Available Partitions）]** から **[選択したパーティション（Selected Partitions）]** に、必要なパーティションを移動します。

ステップ 6 [保存（Save）] をクリックします。

CSS およびパーティションと電話および回線の関連付け

サブカスタマーごとに以下の手順を実行します。

手順

ステップ 1 **Cisco Unified Communications Manager Administration** ページにログインします。
ステップ 2 **[デバイス（Device）] > [電話機（Phone）] > [検索（Find）]** の順に選択します。
ステップ 3 パーティションと CSS を関連付ける電話機をリストから選択します。
ステップ 4 ドロップダウンリストで、必要な**コーリング サーチ スペース**を選択します。
ステップ 5 **[SUBSCRIBEコーリングサーチスペース（SUBSCRIBE Calling Search Space）]** ドロップダウンリストで、必要なコーリングサーチスペースを選択します。
ステップ 6 リストからパーティションと CSS を関連付ける**電話番号回線**を選択します。
ステップ 7 ドロップダウンリストで、必要な**ルートパーティション**を選択します。
ステップ 8 ドロップダウンリストで、必要な**コーリングサーチスペース**を選択します。
ステップ 9 **[設定の適用（Apply Config）]** をクリックします。
ステップ 10 **[リセット（Reset）] > [閉じる（Close）]** の順に選択します。

次のタスク

必要なサブ カスタマー パーティションを CSS と関連付けるには、「コーリングサーチスペースの設定 （533 ページ）」を参照してください。

CSS とトランクの関連付け

手順

ステップ 1 **Cisco Unified Communications Manager Administration ページ**にログインします。
ステップ 2 **[デバイス（Device）] > [トランク（Trunk）]** の順に選択します。
ステップ 3 CSS を関連付けるトランクを選択します。
ステップ 4 **[コーリングサーチスペース（Calling Search Space）]** ドロップダウンログインで、必要な CSS を選択します。

（注） すべてのサブカスタマーパーティションが関連付けられている CSS を選択します。

ステップ 5 [保存（Save）] をクリックします。
ステップ 6 **[リセット（Reset）] > [閉じる（Close）]** の順に選択します。

（注） トランクに関連付けられたルートパターンは、デフォルトパーティションに存在する必要があります。

コアコンポーネント統合オプション用 Cisco Unified Communications Manager のプロビジョニング

エージェントグリーティングの構成

手順

ステップ 1 ローカルエージェントの電話機がエージェントグリーティングをサポートするように、**組み込みブリッジ**を有効にします。

ステップ 2 **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

ステップ 3 **[サーバー（Server）]** ドロップダウンリストで、Unified Communications Manager サーバーを選択します。

ステップ 4 **[サービス（Service）]** ドロップダウンリストで、Cisco CallManager(Active) を選択します。

ステップ 5 [クラスタ全体パラメータ（デバイス一電話機）（Clusterwide Parameters (Device-Phone)）] の [組み込みブリッジの有効化（Built-in-Bridge Enable）] で **[オン（On）]** を選択します。

ステップ 6 [保存（Save）] をクリックします。

モバイルエージェントの構成

Unified Mobile Agent の CTI ポートを設定するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager Administration で **[デバイス（Device）]** > **[電話機（Phone）]** の順に選択します。

ステップ 2 [新規電話を追加（Add a New Phone）] をクリックします。

ステップ 3 **[電話機タイプ（Phone Type）]** ドロップダウンリストで、**[CTIポート（CTI Port）]** を選択します。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [デバイス名（Device Name）] で、ローカル CTI ポートプール名の一意の名前を入力したら、**[OK]** をクリックします。

サンプルの命名規則 LCPxxxxFyyyy を使用します。

a) LCP はローカル デバイスとしての CTI ポートを示します。
b) xxxx は Unified Communications Manager PIM の周辺機器 ID です。
c) yyyy はローカル CTI ポートです。

LCP5000F0000 という名前は、周辺機器 ID 5000 の Unified Communications Manager PIM に対して、ローカル CTI ポート プールの CTI ポート 0 を表します。

ステップ 6 [説明（Description）] に、ローカル CTI ポート プールを特定するテキストを入力します。

ステップ 7 **[デバイスプール（Device Pool）]** ドロップダウンリストで、ネットワーク CTI ポートプールを割り当てるデバイスプールを選択します。（デバイスプールはデバイスの共通の特性一式を定義します。）

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 レコードを強調表示し、[新規DNを追加（Add a new DN）] を選択します。

ステップ 10 ここで作成した CTI ポートの一意の電話番号を追加します。

ステップ 11 完了したら、[保存（Save）] と [閉じる（Close）] をクリックします。

ステップ 12 ネットワーク CTI ポートプールを構成するには、上記の手順を繰り返します。

ステップ 13 [デバイス名（Device Name）] で、ローカル CTI ポートプール名の一意の名前を入力したら、**[OK]** をクリックします。

以下が適用されるサンプル命名規則形式である RCPxxxxFyyyy を使用します。

a) RCP は、ネットワーク デバイスとしての CTI ポートを示します。
b) xxxx は Unified Communications Manager PIM の周辺機器 ID です。
c) yyyy はネットワーク CTI ポートです。

RCP5000F0000 という名前は、周辺機器 ID 5000 の Unified Communications Manager PIM に対して、ネットワーク CTI ポート プールの CTI ポート 0 を表します。

ステップ 14 [説明（Description）] に、ネットワーク CTI ポートプールを識別するテキストを入力します。

ステップ 15 **[デバイスプール（Device Pool）]** ドロップダウンリストで、ネットワーク CTI ポートプールを割り当てるデバイスプールを選択します。（デバイスプールはデバイスの共通の特性一式を定義します。）

ステップ 16 [保存（Save）] をクリックします。

ステップ 17 レコードを強調表示し、**[新規 DN を追加（Add a new DN）]** を選択します。

ステップ 18 ここで作成した CTI ポートの一意の電話番号を追加します。

ステップ 19 完了したら、[保存（Save）] と [閉じる（Close）] をクリックします。

ローカル トランクの設定

ローカルトランクに対して、Unified Communications Manager を構成するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager Administration で、**[システム（System）] > [ロケーション情報（Location info）] > [ロケーション（Location）]** の順に選択します。

ステップ 2 [検索（Find）] をクリックしてロケーションをリスト表示し、適切な帯域幅（8000）の新しいロケーションを追加します。

ステップ 3 ブランチの電話機で、各電話機がその電話機のブランチのロケーションに割り当てられるよう設定します。

a) **[デバイス（Device）] > [電話機（Phone）]** の順に選択します。
b) [検索（Find）] をクリックして、電話機を表示します。
c) 電話機を選択し、[ロケーション（Location）] フィールドを設定します。

ステップ 4 Cisco AXL Web サービスが起動していること、およびアプリケーション ユーザが定義されていて Standard AXL API Access のロールを持っていることを確認します。

a) **[ナビゲーション（Navigation）]** ドロップダウンリストで、**Cisco Unified Serviceability** を選択したら、**[移動（Go）]** をクリックします。
b) **[ツール（Tools）] > [コントロールセンター（Control Center）] > [機能サービス（Feature Services）]** の順に選択します。
c) Cisco AXL Web サービスを起動していない場合は、起動します。
d) Unified Communications Manager Administration から、**[ユーザー管理（User Management）] > [アプリケーションユーザー（Application User）]** の順に選択します。Standard AXL API Access のロールが自分にあることを確認する、または新しいユーザを作成してそのユーザを Standard AXL API Access のロールを持つグループに追加します。

SIP トランクの展開

ローカルトランクの SIP トランクを展開するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager を使用して、SIP プロキシサーバーへの SIP トランクを作成し、ファントムロケーションを選択します。

ステップ 2 各イングレスゲートウェイへの SIP トランクを作成し、これらのイングレス TDM-IP ゲートウェイのロケーションを実際のブランチ ロケーションにします。

ステップ 3 Unified Communications Manager ルーティング クライアントのネットワーク VRU ラベルを、SIP プロキシへの SIP トランクにポインティングするルート パターンを作成します。

SIP プロキシは、Unified Communications Manager ルーティング クライアントの ネットワーク VRU ラベルを Unified CVP サーバにルーティングします。

ステップ 4 IP を使用するコールの場合は、Unified Communications Manager ルートパターンを SIP トランクと関連付けます。

ステップ 5 Unified Communications Manager Administration を使用して、**[デバイス（Device）] > [デバイス設定（Device Settings）] > [SIPプロファイル（SIP Profile）] > [トランク固有の構成（Trunk Specific Configuration）] > [次に基づき、着信要求を新規トランクに再ルート（Reroute Incoming Request to new Trunk based on）] > [x-cisco-origIと同様の目的がある通話情報ヘッダー（Call-Info header with the purpose equal to x-cisco-origIP）]** の順に選択します。

ステップ 6 新しい SIP プロファイルを SIP トランクおよび各イングレスゲートウェイと関連付けます。

アウトバウンドダイヤラの構成

Unified Communications Manager を構成するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager 管理ページにログインします。

ステップ 2 **[デバイス（Device）] > [トランク（Trunk）]** の順に選択します。

ステップ 3 SIP トランクをアウトバウンドゲートウェイに作成します。

A-Law コーデックの構成

Unified Communications Manager を構成するには、以下の手順を実行します。

手順

ステップ 1 **システム**をクリックします。

ステップ 2 **サービスパラメータ**を選択します。

ステップ 3 サーバを選択します。

ステップ 4 サービスを **Cisco CallManager**（有効）として選択します。

ステップ 5 クラスタ全体のパラメータ（システム：場所と地域）の下で、以下を確認します。

- **G.711 A-law コーデックを有効にする** が **有効になっていること**。
- **G 7.11 μ-law コーデック**が**無効**になっていること。

ステップ 6 [保存（Save）] をクリックします。

Cisco Unified Communications Manager と CUBE 間に SIP トランクを作成（SP）

- SIP トランク セキュリティ プロファイルの作成 （539 ページ）
- SIP トランクの作成 （540 ページ）

SIP トランク セキュリティ プロファイルの作成

手順

ステップ 1 Cisco Unified Communications Manager Administration ポータルにログインします。

ステップ 2 **[システム（System）]>[セキュリティ（Security-）]>[Sipトランクセキュリティプロファイル（Sip Trunk Security Profile）]** の順に選択します。

ステップ 3 **[新規追加（Add New）]** をクリックします。

ステップ 4 Sipトランク セキュリティ プロファイルに名前を付けます。

ステップ 5 [着信転送タイプ（Incoming Transport Type）] フィールドで、ドロップダウンリストで TCP+UDP を選択します。

ステップ 6 [着信ポート（Incoming Port）] フィールドに、5060 と 5090 以外のポート番号を入力します。

（注）
- 手順 6 で構成したポートは、Cisco Unified Communications Manager PUBLISHER 隣接関係（アジャセンシー）の CUBE(SP) で構成した「シグナリングピアポート」を一致する必要があります。
- SCC モデルの各サブカスタマーのモバイル エージェント コール フローには、一意の SIP トランク セキュリティ プロファイルが必要です。

ステップ 7 **[保存（Save）]** をクリックします。

SIP トランクの作成

手順

ステップ 1 Cisco Unified Communications Manager Administration ポータルにログインします。

ステップ 2 **[デバイス（Device）] > [トランク（Trunk）]** の順に選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 **[トランクタイプ（Trunk Type）]**フィールドのドロップダウンリストで、 SIP トランクを選択し、**[次へ（Next）]** をクリックします。

ステップ 5 SIP トランクの名前を入力し、ドロップダウンリストでデバイスプールを選択したら、ドロップダウンリストで**[メディアリソースグループリスト（Media Resource Group List）]** を選択します。

ステップ 6 [SIPプロファイル（SIP Profile）] フィールドのドロップダウンリストで、**[標準SIPプロファイル（Standard SIP Profile）]** を選択します。**[すべてのアクティブなUnified CMノードを実行する（Run On All Active Unified CM Nodes）]** チェックボックスをオンにします。

ステップ 7 SIP 情報で、モバイル エージェント コール フロー用 Cisco Unified Communications Manager Publisherに対する CUBE(SP) 隣接関係（アジャセンシー）の signaling-address と signaling-port の詳細を入力します。Cisco Unified Communications Manager SUBSCRIBER Mobile Agent コールフローの追加 （517 ページ）を参照してください。

ステップ 8 **[SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]** フィールドで、ドロップダウンリストで上記手順で作成したプロファイルを選択します。

ステップ 9 残りすべてのデフォルト値を保持します。

ステップ 10 [保存（Save）] をクリックします。

保留音の構成

Unified Communication Manager の構成

ユニファイドコミュニケーションマネージャ MoH サーバーでは、オーディオファイルと固定ソースの 2 つのタイプのソースから MoH ストリームを生成でき、これら 2 つのタイプのいずれかをユニキャストまたはマルチキャストとして送信できます。次の2つの展開モードがあります。

1. MoH サーバーは、CM クラスタでユーザーが 1250 人未満の HCS for CC 展開用の同じサーバー上の Unified CM と一緒に展開します。
2. CM クラスタでユーザーが 1250 人以上の HCS for CC 展開の場合、MoH サーバーは、スタンドアロンノード（TFTP/MoH サーバー）として展開されます。

- 保留音サーバーオーディオソースの構成 （541 ページ）
- 保留音のサービスパラメータの構成 （541 ページ）
- 保留音の電話構成の変更 （541 ページ）

保留音サーバーオーディオソースの構成

保留サーバーオーディオソースは、UCDM では MOH トラックとも呼ばれます。

手順

ステップ 1 **[トラック名（Track Name）]** フィールドに、MOH トラックの名前を入力します。
ステップ 2 **トラック ID**を入力します。
ステップ 3 ドロップダウンリストで、**[MOHサーバー（MOH Server）]** を選択します。
ステップ 4 [送信（Submit）] をクリックします。

保留音のサービスパラメータの構成

手順

ステップ 1 **[ネットワーク（Network）]** > **[PBXデバイス（PBX Devices）]** の順に選択します。
ステップ 2 **[CUCMクラスタ（CUCM Cluster）]** > **[属性（Attributes）]** の順に選択し、**[パラメータコーデック（Parameter Codec）]** で検索します。
ステップ 3 以下に一覧されているパラメータの値を **1** に設定します。

- **DefaultMOHCodec**
- **G711ALawCodecEnabled**
- **G711ULawCodecEnabled**

ステップ 4 [変更（Modify）] をクリックします。

保留音の電話構成の変更

手順

ステップ 1 **[アドミニストレーション（Administration）]** > **[電話機の管理（Phone Management）]** の順に選択し、適切なプロバイダ、リセラー、部署そしてロケーションを選択します。
ステップ 2 追加した**デバイス名**（電話機）をクリックします。
ステップ 3 **[保留音（Music On Hold）]** フィールドで、上記構成で構成した MOH トラックを選択します。
ステップ 4 **[変更（Modify）]** をクリックします。

オプションのシスココンポーネント用 Cisco Unified Communication Manager のプロビジョニング

RSM の構成

Cisco Unified Communications Manager を使用して、Cisco Remote Silent Monitoring（RSM）サーバーを分散モードで構成します。

シミュレーションする電話機の構成

各 Unified Communications Manager クラスタに割り当てるシミュレートされた電話機（simphone とも呼ばれる）の数を決定する必要があります。各クラスタには、クラスタの RSM を介して同時に監視されるエージェントの最大数以上の simphone が必要です。ここでは、次の情報を提供します。

- simphone デバイスの依存関係を構成し、Unified Communications Manager グループ、RSM リージョン、デバイスプール、ルートパーティション、およびコーリングサーチスペースを作成します。
- simphone デバイスを作成し、MAC アドレスを割り当てます。
- 回線 DN を simphone デバイスに追加するには、以下の手順を実行します。

この手順では、1 つの simphone とその関連回線 DN の作成方法について説明します。追加の simphone は、Unified Communication Manager のスーパーコピー機能を使用するか、バッチファイルを作成することで作成できます。

（注） 次の手順に従って simphone を構成する前に、Unified Communications Manager クラスタの管理インターフェイスにログインする必要があります。

Simphone デバイスの依存関係の作成

手順

ステップ 1 Unified Communications Manager グループを作成するには、以下の手順を実行します。

a) **[システム（System）]** > **[Cisco Unified CMグループ（Cisco Unified CM Groups）]** の順に選択します。
b) [新規追加（Add New）] をクリックします。
c) Unified Communications Manager グループ名を **RSMSimPhone** にします。
d) グループに必要な Unified Communications Manager を割り当てます。クラスタ内に 1 つ以上の Unified Communications Manager がある場合は、グループの一部としてサブスクライバを選択し、パブリッシャは選択しないでください。
e) [保存（Save）] をクリックします。

ステップ 2 simphone リージョンを作成するには、以下の手順を実行します。

a) **[システム（System）]** > **[リージョン情報（Region Information）]** > **[リージョン（Region）]** の順に選択します。
b) [新規追加（Add New）] をクリックします。
c) リージョン名として **RSMSimPhone** を入力します。必要に応じて、命名規則に従ってプレフィックスまたはサフィックスを追加します。
d) [保存（Save）] をクリックします。
e) 使用している環境の各リージョンにエージェントの電話機との関係を追加します。simphones とエージェント電話機間の通話では、G.729 コーデックを使用する必要があります。
f) [保存（Save）] をクリックします。

ステップ 3 Simphone デバイスプールを作成するには、以下の手順を実行します。

a) [システム（System）] > [デバイス プール（Device Pool）] に移動します。
b) [新規追加（Add New）] をクリックします。
c) デバイスプール名を **RSMSimPhone** にし、必要に応じて、命名規則に従ってプレフィクスまたはサフィックスを追加します。
d) **[デバイスプール設定（Device Pool Settings）]** の **[Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）]** ドロップダウンリストで、**RSMSimPhone** Communications Manager グループを選択します。
e) **[ローミング感度設定（Roaming Sensitive Settings）]** を選択し、**[リージョン（Region）]** ドロップダウンリストで、**RSMSimPhone** リージョンを選択します。
f) 日時グループやユーザーロケールなどの構成に応じて、残りのパラメータを入力します。
g) [保存（Save）] をクリックします。

ステップ 4 デバイス機能グループを作成するには、以下の手順を実行します。

a) **[一般管理（General Administration）]** > **[機能グループ（Feature Groups）]** の順に選択します。
b) カスタマーインスタンスを選択します。たとえば、Customer_1 のようになります。
c) **[追加]** をクリックして次の値を入力します。

1. 名前 ー **CC-RSM**。
2. 説明 ー **Contact Center RSM Group**。
3. 発信通話の制限 ー **National24Hrs-Standard-wCC**。
4. 不在転送の制限 ー **Default CoS**。
5. ボイスメールテンプレート ー **Basic voicemail service type**。
6. 着信通話の制限 ー **Allow two Direct Dial Inward lines**。
7. 内線番号または回線の数 ー **Two Numbers: DDI または Extension**。
8. Idle URL ー None。

d) [値の追加（Value Add）] パネルで、必要に応じて機能を選択します。
e) [共通の回線設定（回線機能）（ Line Settings（Line Feature））] パネルで、[コンタクトセンターエージェントの回線（Contact Center Agent Line）] 機能を確認します。
f) [個人回線の設定 （電話回線機能）Private line settings （phone line feature）] パネルで、**[録音オプション（Recording Option）]**、**[録音プロファイル（Recording Profile）]**、**[通話中ビジートリガー（Call waiting busy trigger）]**、**[最大発信待機（Max calls waiting）]** をオンにします。
g) [ハンドセットパネル**の組み込みブリッジ**チェックボックスチェックボックスの下。
h) [送信（Submit）] をクリックします。

ステップ 5 simphone ルートパーティションを作成するには、以下の手順を実行します。

a) **[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [パーティション（Partition）]** の順に選択します。
b) [新規追加（Add New）] をクリックします。
c) テキスト ボックスに **RSMSimPhone** と入力し、必要に応じて、プレフィックスまたはサフィックスの命名規則を追加します。
d) [保存（Save）] をクリックします。

ステップ 6 Simphone のコーリング サーチ スペースを作成するには、以下の手順を実行します。

a) **[コールルーティング（Call Routing）] > [コントロールのクラス（Class of Control）] > [コーリング サーチ スペース（Calling Search Space）]** の順に選択します。
b) [新規追加（Add New）] をクリックします。
c) コーリング サーチ スペース名として **RSMSimPhone** を入力します。必要に応じて、命名規則に従ってプレフィックスまたはサフィックスを追加します。
d) RSM がモニタするエージェントの電話を含むルート パーティションを、[使用可能なパーティション（Available Partitions）] ボックスで選択して、[選択されたパーティション（Selected Partition）] ボックスに移動します。
e) [保存（Save）] をクリックします。

（注） 4000 エージェント展開については、2 つ目の PG にも同じ手順を繰り返します。

Simphone デバイスの作成

手順

ステップ 1 **[デバイス（Device）]** > **[電話機（Phone）]** の順に選択します。

ステップ 2 **[新規追加（Add New）]** をクリックして新しい電話機を作成します。

ステップ 3 電話機タイプとして **Cisco 7941** を選択し、**[次へ（Next）]** をクリックします。

ステップ 4 デバイスプロトコルに **[SIP]** を選択し、[次へ（Next）] をクリックします。電話構成ページが表示されます。

ステップ 5 MAC アドレスを入力します。

ステップ 6 パラメータを入力します。

パラメータ	設定
デバイスプール（Device Pool）	RSMSimPhone
電話ボタンテンプレート（Phone Button Template）	標準 7941 SIP
場所（Location）	関連する環境
[ビルトインブリッジ（Built In Bridge）]	オフ
[電話機のパーソナライゼーション（Phone Personalization）]	無効
CTI を介したデバイス制御の許可	はい
[プレゼンスグループ（Presence Group）]	標準
[デバイスのセキュリティプロファイル（Device Security Profile）]	Cisco 7941 標準非セキュア SIP
SIPプロファイル（SIP Profile）	標準
Maximum Calls	2（two）
[話中トリガー（Busy Trigger）]	1（one）

ステップ 7 [保存（Save）] をクリックします。

simphone デバイスが作成されます。

（注） リストされていないパラメータは、デフォルト設定のままにすることができます。

Simphone デバイスへの回線 *DN* の関連付け

手順

ステップ 1 **回線 [1] をクリック - 新規 DN** リンクを割当情報パネルに追加します。

ステップ 2 パラメータを入力します。アスタリスク（*）が付いているパラメータはオプションです。リストされていないものは、デフォルト設定のままにすることができます。

パラメータ	設定
電話番号（Directory Number）	5040
[ルート パーティション（Route Partition）]	RSMSimPhone
CTI 制御	はい
ボイス メール プロファイル（Voice Mail Profile）	ボイスメールがありません
コーリングサーチスペース（Calling Search Space）	RSMSimPhone
[プレゼンスグループ（Presence Group）]	標準のプレゼンスグループ
ユーザー保留 MOH 音源 *	1-SampleAudioSource
ネットワーク保留 MOH 音源 *	1-SampleAudioSource
[デバイス上の Line1 <MAC ADDR> モニタリング用コーリングサーチスペース（CSS）	RSM SimPhone

ステップ 3 [保存（Save）] をクリックします。これで、最初の Simphoneとそれに関連付けられた回線 DN が構成されます。

Simphone 一括管理ツールの使用

一括管理ツールを使用するには、最初にカンマ区切り値テンプレートを（RSM インストール CD またはインストールされた RSM のいずれかから）インポートし、必要に応じて Microsoft Excel などのスプレッドシート アプリケーションで編集します。

手順

ステップ 1 C:\CiscoRSM\Extras directory にある RSM のインストール済みインスタンスから rsmsimphones.csv スプレッドシート テンプレートファイルをインポートします。

ステップ 2 スプレッドシート アプリケーションでファイルを開き、作成する必要がある simphone デバイスの数と一致するようにファイル内の行を追加または削除します（デフォルト行 = 75）。

ステップ 3 新しい行を追加する場合は、Device Name および Directory Number 1 列のデータ変更し、前の列から順番に増分してください（たとえば、simphone MAC アドレスの場合は、00005E000001、00005E000002、00005E000003、回線 DN の場合は、5040、5041、5042 など）。

ステップ 4 デバイスプール、パーティション 1、回線 CSS 1 およびモニタリング コーリング サーチ スペース 1 の設定が環境に適していることを確認します（上記の表 3-1 および 3-2 を参照）。

（注） Simphone の構成時に、Simphone デバイスプール、パーティション、および CSS の設定に RSMSimPhone を入力した場合、変更は必要ありません。

ステップ 5 **[一括管理（Bulk Administration）] > [ファイルのアップロード/ダウンロード（Upload/Download Files）]** の順に選択します。

ステップ 6 [新規追加（Add New）] をクリックします。

ステップ 7 **[参照（Browse）]** をクリックし、以前にダウンロードして変更した rsmsimphones.csv ファイルに移動します。

ステップ 8 [選択およびターゲット（Select the Target）] ドロップダウンリストで、**[電話機（Phones）]** を選択します。

ステップ 9 **[トランザクションタイプの選択（Select Transaction Type）]** ドロップダウンリストで、**[電話機の挿入ーすべての詳細（Insert Phones - All Details）]** を選択します。

ステップ 10 [保存（Save）] をクリックします。ファイルがシステムにアップロードされます。

ステップ 11 **[一括管理（Bulk Administration）] > [電話機（Phones）] > [電話機の挿入（Insert Phones）]** の順に選択します。

ステップ 12 **[電話機の挿入ーすべての詳細（Insert Phones-All Details）]** を選択し、**[ファイル名（File Name）]** ドロップダウンリストで、**[rsmsimphones.csv]** を選択します。

ステップ 13 **[ジョブの説明（Job Description）]** に **Insert RSMSimPhones** と入力し、**[今すぐ実行（Run Immediately）]** を選択します。

ステップ 14 [送信（Submit）] をクリックします。

ファイルがシステムにインポートされます。

ステップ 15 **[一括管理（Bulk Administration）] > [ジョブスケジューラ（Job Scheduler）]** の順に選択し、ジョブのステータスが [処理中（Processing）] または [完了（Completed）] であることを確認します。

ステップ 16 ジョブのステータスが **[完了（Completed）]** になったら、**[デバイス（Device）] > [電話機（Phones）]** の順に選択し、作成した電話機を確認します。

ステップ 17 **[電話機の検索（Find Phone）]** テキストボックスに **SEP00005E** と入力し、**[検索（Find）]** をクリックします。

返された結果に、作成した Simphone デバイスが表示されます。

ログインプール Simphone の設定

各クラスタに作成された最初の 5 つの simphone デバイスは VLEngine のログイン プールに自動で割り当てられます。VLEngine の認証メカニズムをサポートするために発信者が RSM で認証されると、ログイン プールは CTI OS にログイン テストを実行します。

CTI OS のログインは、これらの simphone デバイスで実行されるため、それぞれの Unified Communications Manager クラスタの pguser アカウントに関連付ける必要があります。また、Cisco Unified Intelligent Contact Management Enterprise デバイスターゲットも作成する必要があります。

pguser を関連付けるには、以下の手順を実行します。

手順

ステップ 1 **[ユーザー管理（User Management）]** > **[アプリケーションユーザー（Application User）]** の順に選択します。

ステップ 2 **[検索（Find）]** をクリックして、すべてのアプリケーションユーザを表示します。クラスタの pguser アカウントを検索し、クリックします。

ステップ 3 **[デバイス情報（Device Information）]** の **[使用可能なデバイス（Available Devices）]** リストボックスで最初の 5 つの Simphone デバイスを選択します。

ステップ 4 ボックスの上にある下向きの矢印をクリックして、**[制御されているデバイス]** リストボックスにデバイスを移動します。[保存（Save）] をクリックします。

RSM ユーザーグループの作成

RSM ユーザーグループは、RSM が使用する各クラスタに作成する必要があります。これによりシステムは、Unified Communications Manager のスーパー アドミニストレータでなければ使用できない必要なシステム権限をユーザーに付与します。

RSM ユーザーグループをクラスタに追加するには、以下の手順を実行します。

手順

ステップ 1 **[ユーザー管理（User Management）]** > **[ユーザー設定（User Settings）]** > **[アクセス制御グループ（Access Control Group）]** の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [名前（Name）] フィールドに、**Remote Silent Monitoring** と入力し、**[保存（Save）]** をクリックします。

ステップ 4 **[ユーザー管理（User Management）]** > **[ユーザーグループ（User Group）]** の順に選択します。

ステップ 5 [検索（Find）] をクリックして、すべてのユーザーグループを表示します。

ステップ 6 リモート サイレント モニタリング グループの [ロール（Role）] 列のアイコンをクリックします。

ステップ 7 [グループにロールを割り当て（Assign Role to Group）] をクリックします。新しいウィンドウが表示されます。

ステップ 8 [検索（Find）] をクリックして、すべてのグループのロールを表示します。

ステップ 9 次のロールを選択します。

- 標準 CTI 通話モニタリング許可
- 標準 CTI によるすべてのデバイスの制御
- 標準 CTI 対応

ステップ 10 [選択項目の追加（Add Selected）] をクリックします。[ユーザーグループの構成（User Group Configuration）] ウィンドウが表示されます。

ステップ 11 [保存（Save）] をクリックします。

RSM アプリケーションユーザーの作成

RSM のそれぞれの Unified Communications Manager クラスタに rsmuser というアプリケーションユーザを作成する必要があります。このユーザーは、以前作成したユーザーグループから権限を引き継ぎます。クラスタ内のすべての simphone と rsmuser を関連付ける必要があります（ログインプールの simphone を除く）。ユーザーは、RSM がモニターできるすべてのエージェントの電話にも関連付ける必要があります。

ログイン プールにある simphone（最初の 5 つの simphone デバイス）はクラスタの pguser と関連付ける必要があります。 ログイン プールにない他のすべての simphone は RSM アプリケーション ユーザに関連付けられます。

（注）
- 2 PG を備えた 4000 エージェントの導入環境の場合、2 つのアプリケーション ユーザを作成し、エージェント PG にそれぞれ対応させます。
- 新しい ログイン プール外の simphone またはエージェントのデバイスが作成されるたびに、RSM ユーザに関連付ける必要があります。

RSM アプリケーションユーザーをクラスタに追加するには、以下の手順を実行します。

手順

ステップ 1 **[ユーザー管理（User Management）] > [アプリケーションユーザー（Application User）]** の順に選択します。

ステップ 2 **[新規追加（Add New）]** をクリックし、新しいアプリケーションユーザーを作成します。

ステップ 3 rsmuser をユーザIDに入力します。

ステップ 4 パスワードを入力します。パスワードが英数字であり、特殊文字が含まれていないことを確認します。

ステップ 5 [使用可能なデバイス（Available Devices）] セクションでデバイスを選択し、[制御するデバイス（Controlled Devices）] セクションに移動して、クラスタ内のすべての simphone デバイス（ログイン プールのデバイスを除く）をユーザに関連付けます。

ステップ 6 RSM によってモニタするすべてのエージェントの電話デバイスを関連付けます。

ステップ 7 [権限情報（Permissions Information）] ウィンドウで、**[ユーザーグループに追加（Add to User Group）]** をクリックし、以前作成したリモート サイレント モニタリング グループにユーザーを追加します。

ステップ 8 [保存（Save）] をクリックします。

エージェント電話機の設定

RSM が監視するエージェント電話デバイスを構成するには、次のことを確認します。

- Cisco Unified Communications Manager Administration インターフェイスを使用してデバイスを編集し、ビルトイン ブリッジの設定を有効にします。
- デバイスを「rsmuser」に関連付けて、そのデバイスを pguser と関連付けるのと同じようにします。

MediaSense の構成

- トランクの設定 （524 ページ）
- SIPオプションの設定 （526 ページ）
- ルートパターンの設定 （526 ページ）
- 録音プロファイルの設定 （530 ページ）
- デバイスの構成 （530 ページ）
- 録音デバイスに対して iLBC、iSAC および g.722 を無効化 （531 ページ）

基本構成パラメータ

2000 エージェント展開の基本構成パラメータ

Unified CCE Instance Explorer

名前	タイプ	ネットワーク VRU
HCS for CC	標準	CVP_Network_VRU

エージェント デスク設定の一覧（Agent Desk Settings List）

名前	応答なしの呼び出し時間	ログアウト非アクティビティ時間	最大後処理時間
Default_Agent_Desk_Settings	null	null	[7200]

PG Explorer

周辺機器ゲートウェイ	PIM のタイプ	ルーティング クライアント名
Unified Communication Manager PG1	CUCM	CUCMPG1
Unified Voice Response (VRU) PG	VRU	CVPPG1A
	VRU	CVPPG1B
MR PG	MediaRouting	マルチチャネル
	MediaRouting	アウトバウンド
	MediaRouting	SocialMiner

Network VRU Explorer

名前	タイプ	ネットワーク VRU ラベル	ルーティング クライアント名
CVP_Network_VRU	Type10	7777777777	CVPPG1A
		7777777777	CVPPG1B
		8881111000	CUCMPG1
		6661111000	アウトバウンド
MR_Network_VRU	タイプ 2		

ネットワーク VRU マッピング

- すべての Unified CVP ルーティングクライアントは、**Type10** の **CVP_Network_VRU** にマッピングされます。これは、PG Explorer の **[詳細（Advanced）]** タブに表示されます。
- すべてのメディアルーティングクライアントは、**Type2** の **MR_Network_VRU** にマッピングされます。これは、PG Explorer の **[詳細（Advanced）]** タブに表示されます。

ネットワーク VRU スクリプトの一覧

名前	ネットワーク VRU	VRUスクリプト名	時刻 out （秒）	構成 パラメータ	カスタマー	割り込み可能	オーバーライド
VXML_Server	Type 10 CVP VRU	GS、サーバー、V	180	—	HCS for CC	オフ	オフ
VXML_Server_ Interruptible	Type 10 CVP VRU	GS、サーバー、V、割り込み可	9,000	—	HCS for CC	オン	オフ
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS、 サーバー、V、割り込み不可	9,000	—	HCS for CC	オフ	オフ
AgentGreeting	Type 10 CVP VRU	PM、-a	180	なし	HCS for CC	オフ	オフ
GreetingMenu _1_to_9	Type 10 CVP VRU	M、press _1_thru_9 _greeting、A	180	1-9	HCS for CC	オン	オフ
グリーティング SubMenu	Type 10 CVP VRU	M、 press1-press2-press3、A	180	1 ～ 3 年	HCS for CC	オン	オフ
グリーティング _Not_Found	Type10 CVP VRU	PM、no _greeting _recorded、A	180	Y	HCS for CC	オン	オフ
GreetingReview	Type10 CVP VRU	PM、-a、A	180	Y	HCS for CC	オン	オフ
T10_GS_AUDIUM	Type 10 CVP VRU	GS、サーバー、V、FTP	180	Y	HCS for CC	オン	オフ
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	オフ	オフ

アプリケーション インスタンス リスト

アプリケーション インスタンス	名前	アプリケーション タイプ	権限レベル	アプリケーション キー
マルチチャネル	MultiChannel	その他	完全な読み取り/書き込み	cisco123
CCDM	CCDM	シスコ音声	完全な読み取り/書き込み	cisco123

アプリケーション パス

アプリケーション インスタンス	名前	周辺機器ゲートウェイ	アプリケーション パス メンバー	
UQ.Desktop	5000.UQ.Desktop	CUCM_PG	周辺機器	メディア ルーティング ドメイン
			CUCM_PG_1	SocialMiner_Task

マルチチャネルのメディアクラス

- メディアクラスは、次の名前で作成されます。

  Name : CIM_BC

  Name : ECE_Email

  Name : ECE_Outbound

  Name : ECE_Chat

- タスクセクションには、各メディアクラスの次の詳細が含まれます。

  Life : 300

  Start Time out : 30

  Max duration : 28800

メディア ルーティング ドメイン

	[割り込み可能（**Interruptible**）]	キュー内コール数（最大）	コールタイプごとの最大数	キューの最大時間
Cisco_BC	オフ	5000	-	-
ECE_Email	オン	15000	-	-
ECE_Outbound	オン	5000	-	-

	[割り込み可能（Interruptible）]	キュー内コール数（最大）	コールタイプごとの最大数	キューの最大時間
ECE_Chat	オフ	5000	-	-
SocialMiner_Task	オフ	-	-	-

（注） **[コールタイプごとの最大数（Max Per Call Type）]** および **[キュー内の最大時間（Max Time in Queue）]** の値を要件に従って設定します。

拡張コール変数の一覧（Expanded Call Variable List）

名前	有効	永続	最大長（Maximum Length）	説明
user.CourtesyCallbackEnabled	FALSE	FALSE	1	サービス コールバックを発信者に行うかどうかを決定します。
user.cvp_server_info	FALSE	FALSE	15	Unified CCE に要求を送信するコールサーバーの IP アドレスを送信するために Unified CVP が使用します。
user.microapp.app_media_lib	FALSE	FALSE	210	すべてのアプリケーション固有メディアファイルおよび文法ファイルのディレクトリ。 **..** はユーザーをバイパスします。URL パスを記述する場合、microapp.app_media_lib および user.microapp.locale は ECC 変数です。
user.microapp.caller_input	FALSE	FALSE	210	Get Speech から収集された ASR 入力用ストレージ領域。 （注） Get Speech の結果は ECC 変数に書き込まれます。Get Digits または Menu マイクロアプリケーションの結果は CED に書き込まれます。
user.microapp.currency	FALSE	FALSE	6	現在のタイプ。

名前	有効	永続	最大長（Maximum Length）	説明
user.microapp.error_code	FALSE	FALSE	2	実行スクリプトの結果が、Falseの場合、Unified CVP から Unified CCE に返されたエラーステータスコード。
user.microapp.FromExtVXML	FALSE	FALSE	60	この変数配列は、外部 VoiceXML ファイルからの情報を返します。スカラ変数ではなく配列型変数として構成し、配列の長さを 4 に設定する必要があります。
user.microapp.input_type	FALSE	FALSE	1	許可された入力タイプを指定します。有効なコンテンツは、D（DTMF）と B（DTMF と音声の両方）です。B がデフォルトです。ASR を使用していない場合は、この変数を D に設定します。ASR を使用している場合は、この変数を D または B に設定できます。
user.microapp.locale	FALSE	FALSE	5	使用する文法とプロンプトセットを定義する言語と国の組み合わせ。
user.microapp.metadata	FALSE	FALSE	62	メニュー（M）、Get Data（GD）、および Get Speech（GS）マイクロアプリケーションに続いて、Unified CVP はそのマイクロアプリケーションの実行に関する情報を返します。
user.microapp.play_data	FALSE	FALSE	40	Play Data マイクロアプリケーションのデータ用のデフォルトストレージ領域。
user.microapp.sys_media_lib	FALSE	FALSE	10	各桁、月、デフォルトのエラーメッセージなど、すべてのシステムメディアファイルのディレクトリ。

名前	有効	永続	最大長（Maximum Length）	説明
user.microapp.ToExtVXML	FALSE	FALSE	60	この変数配列は、外部 VoiceXML ファイルに情報を送信します。スカラ変数ではなく配列型変数として構成し、配列の長さを 4 に設定する必要があります。
user.microapp.UseVXMLParams	FALSE	FALSE	1	外部 VoiceXML に情報を渡す方法を指定します。
user.microapp.isPostCallSurvey	FALSE	FALSE	1	エージェントが電話を切った後に、ポストコール調査を発信者に提供するかどうかを決定するために使用されます。
user.ece.activity.id	FALSE	FALSE	30	すべてのタイプの WIM および EIM アクティビティに必要です。
user.ece.customer.name	FALSE	FALSE	30	チャット、、コールバック、およびコールバックの遅延アクティビティに必要です。
user.media.id	FALSE	FALSE	36	Unified CCE サービスへのコールを識別する番号（オプションで H.323サービス）。
user.microapp.grammar_choices	FALSE	FALSE	210	発信者が Get Speech マイクロアプリケーションに入力できる ASR 選択肢を指定します。
user.microapp.inline_tts	FALSE	FALSE	210	インライン音声合成（TTS）のテキストを指定します。
user.microapp.media_server	FALSE	FALSE	60	スクリプトで使用されるすべてのメディアファイルおよび外部文法ファイルの URL のルート。
user.microapp.override_cli	FALSE	FALSE	200	発信転送で CLI フィールドを上書きするためにシステムが使用します。
user.microapp.pd_tts	FALSE	FALSE	1	Unifies Text To Speech またはメディアファイルを発信者に対して再生する必要があるかどうかを指定します。

システム情報

- 拡張コールコンテキスト：有効化
- 最小相関番号：1001
- 最大相関番号：9999
- スクリプトバージョンの保持：5

エージェント ターゲティング ルール

属性	
名前	AgentExtensions
周辺機器	CUCM_PG_1
ルールタイプ	エージェントの内線番号
ルーティングクライアント	すべてのルーティングクライアント
内線番号の範囲	000 ー 999 0000 ー 9999 00000 ー 99999 000000 ー 999999 0000000 ー 9999999 00000000 ー 99999999 000000000 ー 999999999 0000000000 ー 9999999999

アウトバウンドダイヤラ

ダイヤラ名	周辺機器名
周辺機器	CUCM_PG_1
ダイヤラ名	SIP_DIALER
有効	はい
ICM 周辺機器名	CUCM_PG_1
ハングアップ遅延（1 ～ 10）	1 秒
ポートスロットル	10

4000 エージェント展開の基本構成パラメータ

Unified CCE Instance Explorer

名前	タイプ	ネットワーク VRU
HCS for CC	標準	CVP_Network_VRU

エージェント デスク設定の一覧（Agent Desk Settings List）

名前	応答なしの呼び出し時間	ログアウト非アクティビティ時間	最大後処理時間
Default_Agent_Desk_Settings	null	null	[7200]

PG Explorer

周辺機器ゲートウェイ	PIM のタイプ	ルーティング クライアント名
Unified Communication Manager PG1	CUCM	CUCMPG1
Unified Communication Manager PG2	CUCM	CUCMPG2
Unified Voice Response (VRU) PG1	VRU	CVPRC01 および CVPRC02
Unified Voice Response (VRU) PG2	VRU	CVPRC03 および CVPRC04
Media Routing (MR) PG 1	MediaRouting	Multichannel1
	MediaRouting	Outbound1
	MediaRouting	SocialMiner1
Media Routing (MR) PG 2	MediaRouting	Multichannel2
	MediaRouting	Outbound2
	MediaRouting	SocialMiner2

Network VRU Explorer

名前	タイプ	ネットワーク VRU ラベル	ルーティングクライアント名
CVP_Network_VRU	Type10	7777777777	CVPRC01
		7777777777	CVPRC02
		7777777777	CVPRC03
		7777777777	CVPRC04
		8881111000	CUCMPG1
		8881111000	CUCMPG2
		6661111000	Outbound1
		6661111000	Outbound2
MR_Network_VRU_Type2	タイプ 2	-	-

ネットワーク VRU マッピング

- すべての Unified CVP ルーティングクライアントは、**Type10** の **CVP_Network_VRU** にマッピングされます。 これは、PG Explorer の **[詳細（Advanced）]** タブに表示されます。
- すべてのメディア ルーティング クライアントは、**Type2** の **MR_Network_VRU_Type2** にマッピングされます。これは、PG Explorer の **[詳細（Advanced）]** タブに表示されます。

ネットワーク VRU スクリプトの一覧

名前	ネットワーク VRU	VRU スクリプト名	時刻 out（秒）	構成パラメータ	カスタマー	割り込み可能	オーバーライド
VXML_Server	Type 10 CVP VRU	GS、サーバー、V	180	—	HCS for CC	オフ	オフ
VXML_Server_ Interruptible	Type 10 CVP VRU	GS、サーバー、V、割り込み可	9,000	—	HCS for CC	オン	オフ
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS、サーバー、V、割り込み不可	9,000	—	HCS for CC	オフ	オフ
AgentGreeting	Type 10 CVP VRU	PM、-a	180	なし	HCS for CC	オフ	オフ

名前	ネットワーク VRU	VRUスクリプト名	時刻 out （秒）	構成 パラメータ	カスタマー	割り込み可能	オーバーライド
GreetingMenu _1_to_9	Type 10 CVP VRU	M、press _1_thru_9 _greeting、A	180	1-9	HCS for CC	オン	オフ
グリーティング SubMenu	Type 10 CVP VRU	M、 press1-press2-press3、A	180	1 ～ 3 年	HCS for CC	オン	オフ
グリーティング _Not_Found	Type10 CVP VRU	PM、no _greeting _recorded、A	180	Y	HCS for CC	オン	オフ
GreetingReview	Type10 CVP VRU	PM、-a、A	180	Y	HCS for CC	オン	オフ
T10_GS_AUDIUM	Type 10 CVP VRU	GS、サーバー、V、FTP	180	Y	HCS for CC	オン	オフ
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	オフ	オフ

アプリケーション インスタンス リスト

アプリケーション インスタンス	名前	アプリケーション タイプ	権限レベル	アプリケーション キー
マルチチャネル	MultiChannel	その他	完全な読み取り/書き込み	cisco123
CCDM	CCDM	シスコ音声	完全な読み取り/書き込み	cisco123

アプリケーションパス 4K

アプリケーション インスタンス	名前	周辺機器ゲートウェイ	アプリケーション パス メンバー	
UQ.Desktop	5000.UQ.Desktop	CUCM_PG	周辺機器	メディア ルーティング ドメイン
			CUCM_PG_1	SocialMiner_Task
			CUCM_PG_2	SocialMiner_Task

マルチチャネルのメディアクラス

- メディアクラスは、次の名前で作成されます。

  Name : CIM_BC

  Name : ECE_Email

  Name : ECE_Outbound

  Name : ECE_Chat

- タスクセクションには、各メディアクラスの次の詳細が含まれます。

  Life : 300

  Start Time out : 30

  Max duration : 28800

メディア ルーティング ドメイン

	[割り込み可能（Interruptible）]	キュー内コール数（最大）	コールタイプごとの最大数	キューの最大時間
Cisco_BC	オフ	5000	-	-
ECE_Email	オン	15000	-	-
ECE_Outbound	オン	5000	-	-
ECE_Chat	オフ	5000	-	-
SocialMiner_Task	オフ	-	-	-

（注） **[コールタイプごとの最大数（Max Per Call Type）]** および **[キュー内の最大時間（Max Time in Queue）]** の値を要件に従って設定します。

拡張コール変数の一覧（Expanded Call Variable List）

名前	有効	永続	最大長（Maximum Length）	説明
user.CourtesyCallbackEnabled	FALSE	FALSE	1	サービス コールバックを発信者に行うかどうかを決定します。
user.cvp_server_info	FALSE	FALSE	15	Unified CCE に要求を送信するコールサーバーの IP アドレスを送信するために Unified CVP が使用します。
user.microapp.app_media_lib	FALSE	FALSE	210	すべてのアプリケーション固有メディアファイルおよび文法ファイルのディレクトリ。 **..** はユーザーをバイパスします。URL パスを記述する場合、microapp.app_media_lib および user.microapp.locale は ECC 変数です。
user.microapp.caller_input	FALSE	FALSE	210	Get Speech から収集された ASR 入力用ストレージ領域。 （注） Get Speech の結果は ECC 変数に書き込まれます。Get Digits または Menu マイクロアプリケーションの結果は CED に書き込まれます。
user.microapp.currency	FALSE	FALSE	6	現在のタイプ。
user.microapp.error_code	FALSE	FALSE	2	実行スクリプトの結果が、False の場合、Unified CVP から Unified CCE に返されたエラーステータスコード。
user.microapp.FromExtVXML	FALSE	FALSE	60	この変数配列は、外部 VoiceXML ファイルからの情報を返します。スカラ変数ではなく配列型変数として構成し、配列の長さを 4 に設定する必要があります。

名前	有効	永続	最大長（Maximum Length）	説明
user.microapp.input_type	FALSE	FALSE	1	許可された入力タイプを指定します。有効なコンテンツは、D（DTMF）とB（DTMFと音声の両方）です。Bがデフォルトです。ASRを使用していない場合は、この変数をDに設定します。ASRを使用している場合は、この変数をDまたはBに設定できます。
user.microapp.locale	FALSE	FALSE	5	使用する文法とプロンプトセットを定義する言語と国の組み合わせ。
user.microapp.metadata	FALSE	FALSE	62	メニュー（M）、Get Data（GD）、およびGet Speech（GS）マイクロアプリケーションに続いて、Unified CVPはそのマイクロアプリケーションの実行に関する情報を返します。
user.microapp.play_data	FALSE	FALSE	40	Play Dataマイクロアプリケーションのデータ用のデフォルトストレージ領域。
user.microapp.sys_media_lib	FALSE	FALSE	10	各桁、月、デフォルトのエラーメッセージなど、すべてのシステムメディアファイルのディレクトリ。
user.microapp.ToExtVXML	FALSE	FALSE	60	この変数配列は、外部VoiceXMLファイルに情報を送信します。スカラ変数ではなく配列型変数として構成し、配列の長さを4に設定する必要があります。
user.microapp.UseVXMLParams	FALSE	FALSE	1	外部VoiceXMLに情報を渡す方法を指定します。
user.microapp.isPostCallSurvey	FALSE	FALSE	1	エージェントが電話を切った後に、ポストコール調査を発信者に提供するかどうかを決定するために使用されます。

名前	有効	永続	最大長（Maximum Length）	説明
user.ece.activity.id	FALSE	FALSE	30	すべてのタイプの WIM および EIM アクティビティに必要です。
user.ece.customer.name	FALSE	FALSE	30	チャット、、コールバック、およびコールバックの遅延アクティビティに必要です。
user.media.id	FALSE	FALSE	36	Unified CCE サービスへのコールを識別する番号（オプションで H.323サービス）。
user.microapp.grammar_choices	FALSE	FALSE	210	発信者が Get Speech マイクロアプリケーションに入力できる ASR 選択肢を指定します。
user.microapp.inline_tts	FALSE	FALSE	210	インライン音声合成（TTS）のテキストを指定します。
user.microapp.media_server	FALSE	FALSE	60	スクリプトで使用されるすべてのメディアファイルおよび外部文法ファイルの URL のルート。
user.microapp.override_cli	FALSE	FALSE	200	発信転送で CLI フィールドを上書きするためにシステムが使用します。
user.microapp.pd_tts	FALSE	FALSE	1	Unifies Text To Speech またはメディアファイルを発信者に対して再生する必要があるかどうかを指定します。

システム情報

- 拡張コールコンテキスト：有効化
- 最小相関番号：1001
- 最大相関番号：9999
- スクリプトバージョンの保持：5

エージェント ターゲティング ルール

属性		
名前	AgentExtension1	AgentExtension2

属性		
周辺機器	CUCM_PG_1	CUCM_PG_2
ルールタイプエージェントの内線番号	エージェントの内線番号	エージェントの内線番号
ルーティングクライアント	すべてのルーティングクライアント	すべてのルーティングクライアント
内線番号の範囲	000 ー 999	000 ー 999
	0000 ー 9999	0000 ー 9999
	00000 ー 99999	00000 ー 99999
	000000 ー 999999	000000 ー 999999
	0000000 ー 9999999	0000000 ー 9999999
	00000000 ー 99999999	00000000 ー 99999999
	000000000 ー 999999999	000000000 ー 999999999
	0000000000 ー 9999999999	0000000000 ー 9999999999

アウトバウンドダイヤラ

ダイヤラ名	周辺機器名
周辺機器	CUCM_PG_1
ダイヤラ名	SIP_DIALER
有効	はい
ICM 周辺機器名	CUCM_PG_1
ハングアップ遅延（1 ～ 10）	1 秒
ポートスロットル	10

12000 エージェント展開の基本構成パラメータ

Unified CCE Instance Explorer

名前	タイプ	ネットワーク VRU
HCS for CC	標準	CVP_Network_VRU

エージェント デスク設定の一覧（Agent Desk Settings List）

名前	応答なしの呼び出し時間	ログアウト非アクティビティ時間	最大後処理時間
Default_Agent_Desk_Settings	null	null	[7200]

PG Explorer

周辺機器ゲートウェイ	PIM のタイプ	ルーティングクライアント名
Unified CommunicationManager PG1	CUCM	CUCMPG1
Unified CommunicationManager PG2	CUCM	CUCMPG2
Unified CommunicationManager PG3	CUCM	CUCMPG3
Unified CommunicationManager PG4	CUCM	CUCMPG4
Unified CommunicationManager PG5	CUCM	CUCMPG5
Unified CommunicationManager PG6	CUCM	CUCMPG6
Unified Voice Response (VRU) PG1	VRU	CVPRC01 および CVPRC02
Unified Voice Response (VRU) PG2	VRU	CVPRC03 および CVPRC04
Unified Voice Response (VRU) PG3	VRU	CVPRC05 および CVPRC06
Unified Voice Response (VRU) PG4	VRU	CVPRC07 および CVPRC08
Unified Voice Response (VRU) PG5	VRU	CVPRC09 および CVPRC10
Unified Voice Response (VRU) PG6	VRU	CVPRC11 および CVPRC12
Media Routing (MR) PG 1	MediaRouting	Multichannel1
	MediaRouting	Outbound1
	MediaRouting	SocialMiner1

周辺機器ゲートウェイ	PIM のタイプ	ルーティングクライアント名
Media Routing (MR) PG 2	MediaRouting	Multichannel2
	MediaRouting	Outbound2
	MediaRouting	SocialMiner2
Media Routing (MR) PG 3	MediaRouting	Multichannel3
	MediaRouting	Outbound3
	MediaRouting	SocialMiner3
Media Routing (MR) PG 4	MediaRouting	Multichannel4
	MediaRouting	Outbound4
	MediaRouting	SocialMiner4
Media Routing (MR) PG 5	MediaRouting	Multichannel5
	MediaRouting	Outbound5
	MediaRouting	SocialMiner5
Media Routing (MR) PG 6	MediaRouting	Multichannel6
	MediaRouting	Outbound6
	MediaRouting	SocialMiner6

Network VRU Explorer

名前	タイプ	ネットワーク VRU ラベル	ルーティング クライアント名
CVP ネットワーク VRU	タイプ 10	7777777777	CVPRC01、CVPRC02 ... CVPRC12
		8881111000	CUCMPG1、CUCMPG2 ... CUCMPG6
		6661111000	Outbound1、Outbound2 ... Outbound6
MR_Network_VRU_Type2	タイプ 2	-	-

ネットワーク VRU マッピング

- すべての Unified CVP ルーティング クライアントは、**Type10** の **CVP_Network_VRU** にマッピングされます。 これは、PG Explorer の **[詳細（Advanced）]** タブに表示されます。
- すべてのメディア ルーティング クライアントは、**Type2** の **MR_Network_VRU_Type2** にマッピングされます。これは、PG Explorer の **[詳細（Advanced）]** タブに表示されます。

ネットワーク VRU スクリプトの一覧

名前	ネットワーク VRU	VRU スクリプト名	時刻 out（秒）	構成パラメータ	カスタマー	割り込み可能	オーバーライド
VXML_Server	Type 10 CVP VRU	GS、サーバー、V	180	__	HCS for CC	オフ	オフ
VXML_Server_ Interruptible	Type 10 CVP VRU	GS、サーバー、V、割り込み可	9,000	__	HCS for CC	オン	オフ
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS、サーバー、V、割り込み不可	9,000	__	HCS for CC	オフ	オフ
AgentGreeting	Type 10 CVP VRU	PM、-a	180	なし	HCS for CC	オフ	オフ
GreetingMenu _1_to_9	Type 10 CVP VRU	M、press _1_thru_9 _greeting、A	180	1-9	HCS for CC	オン	オフ
グリーティング SubMenu	Type 10 CVP VRU	M、press1-press2-press3、A	180	1 ～ 3 年	HCS for CC	オン	オフ
グリーティング _Not_Found	Type10 CVP VRU	PM、no _greeting _recorded、A	180	Y	HCS for CC	オン	オフ
GreetingReview	Type10 CVP VRU	PM、-a、A	180	Y	HCS for CC	オン	オフ
T10_GS_AUDIUM	Type 10 CVP VRU	GS、サーバー、V、FTP	180	Y	HCS for CC	オン	オフ

名前	ネットワーク **VRU**	**VRU** スクリプト名	時刻 **out**（秒）	構成パラメータ	カスタマー	割り込み可能	オーバーライド
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	オフ	オフ

アプリケーション インスタンス リスト

アプリケーション インスタンス	名前	アプリケーション タイプ	権限レベル	アプリケーション キー
マルチチャネル	MultiChannel	その他	完全な読み取り/書き込み	cisco123
CCDM	CCDM	シスコ音声	完全な読み取り/書き込み	cisco123

アプリケーションパス 12K

アプリケーション インスタンス	名前	周辺機器ゲートウェイ	アプリケーション パス メンバー	
UQ.Desktop	5000.UQ.Desktop	CUCM_PG	周辺機器	メディア ルーティング ドメイン
			CUCM_PG_1	SocialMiner_Task
			CUCM_PG_2	SocialMiner_Task
			CUCM_PG_3	SocialMiner_Task
			CUCM_PG_4	SocialMiner_Task
			CUCM_PG_5	SocialMiner_Task
			CUCM_PG_6	SocialMiner_Task

マルチチャネルのメディアクラス

- メディアクラスは、次の名前で作成されます。

  Name : CIM_BC

  Name : ECE_Email

  Name : ECE_Outbound

Name : ECE_Chat

- タスクセクションには、各メディアクラスの次の詳細が含まれます。

  Life : 300

  Start Time out : 30

  Max duration : 28800

メディア ルーティング ドメイン

	[割り込み可能（Interruptible）]	キュー内コール数（最大）	コールタイプごとの最大数	キューの最大時間
Cisco_BC	オフ	5000	-	-
ECE_Email	オン	15000	-	-
ECE_Outbound	オン	5000	-	-
ECE_Chat	オフ	5000	-	-
SocialMiner_Task	オフ	-	-	-

（注） **[コールタイプごとの最大数（Max Per Call Type）]** および **[キュー内の最大時間（Max Time in Queue）]** の値を要件に従って設定します。

拡張コール変数の一覧（Expanded Call Variable List）

名前	有効	永続	最大長（Maximum Length）	説明
user.CourtesyCallbackEnabled	FALSE	FALSE	1	サービス コールバックを発信者に行うかどうかを決定します。
user.cvp_server_info	FALSE	FALSE	15	Unified CCE に要求を送信するコールサーバーの IP アドレスを送信するために Unified CVP が使用します。

名前	有効	永続	最大長（Maximum Length）	説明
user.microapp.app_media_lib	FALSE	FALSE	210	すべてのアプリケーション固有メディアファイルおよび文法ファイルのディレクトリ。 .. はユーザーをバイパスします。URL パスを記述する場合、microapp.app_media_lib および user.microapp.locale は ECC 変数です。
user.microapp.caller_input	FALSE	FALSE	210	Get Speech から収集された ASR 入力用ストレージ領域。 （注） Get Speech の結果は ECC 変数に書き込まれます。Get Digits または Menu マイクロアプリケーションの結果は CED に書き込まれます。
user.microapp.currency	FALSE	FALSE	6	現在のタイプ。
user.microapp.error_code	FALSE	FALSE	2	実行スクリプトの結果が、False の場合、Unified CVP から Unified CCE に返されたエラーステータスコード。
user.microapp.FromExtVXML	FALSE	FALSE	60	この変数配列は、外部 VoiceXML ファイルからの情報を返します。スカラ変数ではなく配列型変数として構成し、配列の長さを 4 に設定する必要があります。
user.microapp.input_type	FALSE	FALSE	1	許可された入力タイプを指定します。有効なコンテンツは、D（DTMF）と B（DTMF と音声の両方）です。B がデフォルトです。ASR を使用していない場合は、この変数を D に設定します。ASR を使用している場合は、この変数を D または B に設定できます。

名前	有効	永続	最大長（Maximum Length）	説明
user.microapp.locale	FALSE	FALSE	5	使用する文法とプロンプトセットを定義する言語と国の組み合わせ。
user.microapp.metadata	FALSE	FALSE	62	メニュー（M）、Get Data（GD）、および Get Speech（GS）マイクロアプリケーションに続いて、Unified CVP はそのマイクロアプリケーションの実行に関する情報を返します。
user.microapp.play_data	FALSE	FALSE	40	Play Data マイクロアプリケーションのデータ用のデフォルトストレージ領域。
user.microapp.sys_media_lib	FALSE	FALSE	10	各桁、月、デフォルトのエラーメッセージなど、すべてのシステムメディアファイルのディレクトリ。
user.microapp.ToExtVXML	FALSE	FALSE	60	この変数配列は、外部 VoiceXML ファイルに情報を送信します。スカラ変数ではなく配列型変数として構成し、配列の長さを 4 に設定する必要があります。
user.microapp.UseVXMLParams	FALSE	FALSE	1	外部 VoiceXML に情報を渡す方法を指定します。
user.microapp.isPostCallSurvey	FALSE	FALSE	1	エージェントが電話を切った後に、ポストコール調査を発信者に提供するかどうかを決定するために使用されます。
user.ece.activity.id	FALSE	FALSE	30	すべてのタイプの WIM および EIM アクティビティに必要です。
user.ece.customer.name	FALSE	FALSE	30	チャット、、コールバック、およびコールバックの遅延アクティビティに必要です。
user.media.id	FALSE	FALSE	36	Unified CCE サービスへのコールを識別する番号（オプションで H.323サービス）。

名前	有効	永続	最大長（Maximum Length）	説明
user.microapp.grammar_choices	FALSE	FALSE	210	発信者が Get Speech マイクロアプリケーションに入力できる ASR 選択肢を指定します。
user.microapp.inline_tts	FALSE	FALSE	210	インライン音声合成（TTS）のテキストを指定します。
user.microapp.media_server	FALSE	FALSE	60	スクリプトで使用されるすべてのメディアファイルおよび外部文法ファイルの URL のルート。
user.microapp.override_cli	FALSE	FALSE	200	発信転送で CLI フィールドを上書きするためにシステムが使用します。
user.microapp.pd_tts	FALSE	FALSE	1	Unifies Text To Speech またはメディアファイルを発信者に対して再生する必要があるかどうかを指定します。

システム情報

- 拡張コールコンテキスト：有効化
- 最小相関番号：1001
- 最大相関番号：9999
- スクリプトバージョンの保持：5

エージェント ターゲティング ルール

属性	
Name	AgentExtension1、AgentExtension2 … AgentExtension6
周辺機器	CUCM_PG_1、CUCM_PG_2 … CUCM_PG_6
ルールタイプエージェントの内線番号	エージェントの内線番号
ルーティングクライアント	すべてのルーティングクライアント

属性	
内線番号の範囲	000 ー 999 0000 ー 9999 00000 ー 99999 000000 ー 999999 0000000 ー 9999999 00000000 ー 99999999 000000000 ー 999999999 0000000000 ー 9999999999

アウトバウンドダイヤラ

ダイヤラ名	周辺機器名
周辺機器	CUCM_PG_1
ダイヤラ名	SIP_DIALER
有効	はい
ICM 周辺機器名	CUCM_PG_1
ハングアップ遅延（1 ～ 10）	1 秒
ポートスロットル	10

Small Contact Center エージェント展開用基本構成パラメータ

Unified CCE Instance Explorer

名前	タイプ	ネットワーク **VRU**
HCS for CC	標準	CVP_Network_VRU

エージェント デスク設定の一覧（**Agent Desk Settings List**）

名前	応答なしの呼び出し時間	ログアウト非アクティビティ時間	最大後処理時間
Default_Agent_Desk_Settings	null	null	[7200]

PG Explorer

周辺機器ゲートウェイ	PIM のタイプ	ルーティングクライアント名
Unified Communication Manager PG1	CUCM	CUCMPG1
Unified Voice Response (VRU) PG	VRU	CVPRC01
	VRU	CVPRC02
	VRU	CVPRC03
	VRU	CVPRC04

Network VRU Explorer

名前	タイプ	ネットワーク VRU ラベル	ルーティング クライアント名
CVP ネットワーク VRU	タイプ 10	7777777777	CVPRC01
		7777777777	CVPRC02
		7777777777	CVPRC03
		7777777777	CVPRC04
		8881111000	CUCMPG1
MR_Network_VRU	タイプ 2	-	-

ネットワーク VRU マッピング

すべての Unified CVP ルーティングクライアントは、**Type10** の **CVP_Network_VRU** にマッピングされます。これは、PG Explorer の **[詳細（Advanced）]** タブに表示されます。

ネットワーク VRU スクリプトの一覧

名前	ネットワーク VRU	VRU スクリプト名	時刻 out （秒）	構成パラメータ	カスタマー	割り込み可能	オーバーライド
VXML_Server	Type 10 CVP VRU	GS、サーバー、V	180	—	HCS for CC	オフ	オフ
VXML_Server_ Interruptible	Type 10 CVP VRU	GS、サーバー、V、割り込み可	9,000	—	HCS for CC	オン	オフ
VXML_Server_ Noninterruptible	Type 10 CVP VRU	GS、サーバー、V、割り込み不可	9,000	—	HCS for CC	オフ	オフ

名前	ネットワーク **VRU**	**VRU**スクリプト名	時刻 **out**（秒）	構成パラメータ	カスタマー	割り込み可能	オーバーライド
AgentGreeting	Type 10 CVP VRU	PM、-a	180	なし	HCS for CC	オフ	オフ
GreetingMenu _1_to_9	Type 10 CVP VRU	M、press _1_thru_9 _greeting、A	180	1-9	HCS for CC	オン	オフ
グリーティング SubMenu	Type 10 CVP VRU	M、press1-press2-press3、A	180	1 ～ 3 年	HCS for CC	オン	オフ
グリーティング _Not_Found	Type10 CVP VRU	PM、no _greeting _recorded、A	180	Y	HCS for CC	オン	オフ
GreetingReview	Type10 CVP VRU	PM、-a、A	180	Y	HCS for CC	オン	オフ
T10_GS_AUDIUM	Type 10 CVP VRU	GS、サーバー、V、FTP	180	Y	HCS for CC	オン	オフ
CIMExternal ApplicationScript	Type 2 MR VRU	CIMExternal ApplicationScript	180	-	HCS for CC	オフ	オフ

アプリケーション インスタンス リスト

アプリケーション インスタンス	名前	アプリケーション タイプ	権限レベル	アプリケーション キー
マルチチャネル	MultiChannel	その他	完全な読み取り/書き込み	cisco123
CCDM	CCDM	シスコ音声	完全な読み取り/書き込み	cisco123

アプリケーション パス

アプリケーション インスタンス	名前	周辺機器ゲートウェイ	アプリケーション パス メンバー	
UQ.Desktop	5000.UQ.Desktop	CUCM_PG	周辺機器	メディア ルーティング ドメイン
			CUCM_PG_1	SocialMiner_Task

マルチチャネルのメディアクラス

- メディアクラスは、次の名前で作成されます。

  Name : CIM_BC

  Name : ECE_Email

  Name : ECE_Outbound

  Name : ECE_Chat

- タスクセクションには、各メディアクラスの次の詳細が含まれます。

  Life : 300

  Start Time out : 30

  Max duration : 28800

メディア ルーティング ドメイン

	[割り込み可能（**Interruptible**）]	キュー内コール数（最大）	コールタイプごとの最大数	キューの最大時間
Cisco_BC	オフ	5000	-	-
ECE_Email	オン	15000	-	-
ECE_Outbound	オン	5000	-	-
ECE_Chat	オフ	5000	-	-
SocialMiner_Task	オフ	-	-	-

（注） **[コールタイプごとの最大数（Max Per Call Type）]** および **[キュー内の最大時間（Max Time in Queue）]** の値を要件に従って設定します。

拡張コール変数の一覧（Expanded Call Variable List）

名前	有効	永続	最大長（Maximum Length）	説明
user.CourtesyCallbackEnabled	FALSE	FALSE	1	サービス コールバックを発信者に行うかどうかを決定します。
user.cvp_server_info	FALSE	FALSE	15	Unified CCE に要求を送信するコールサーバーの IP アドレスを送信するために Unified CVP が使用します。
user.microapp.app_media_lib	FALSE	FALSE	210	すべてのアプリケーション固有メディアファイルおよび文法ファイルのディレクトリ。 **..** はユーザーをバイパスします。URL パスを記述する場合、microapp.app_media_lib および user.microapp.locale は ECC 変数です。
user.microapp.caller_input	FALSE	FALSE	210	Get Speech から収集された ASR 入力用ストレージ領域。 （注） Get Speech の結果は ECC 変数に書き込まれます。Get Digits または Menu マイクロアプリケーションの結果は CED に書き込まれます。
user.microapp.currency	FALSE	FALSE	6	現在のタイプ。
user.microapp.error_code	FALSE	FALSE	2	実行スクリプトの結果が、False の場合、Unified CVP から Unified CCE に返されたエラーステータスコード。
user.microapp.FromExtVXML	FALSE	FALSE	60	この変数配列は、外部 VoiceXML ファイルからの情報を返します。スカラ変数ではなく配列型変数として構成し、配列の長さを 4 に設定する必要があります。

名前	有効	永続	最大長（Maximum Length）	説明
user.microapp.input_type	FALSE	FALSE	1	許可された入力タイプを指定します。有効なコンテンツは、D（DTMF）とB（DTMFと音声の両方）です。Bがデフォルトです。ASRを使用していない場合は、この変数をDに設定します。ASRを使用している場合は、この変数をDまたはBに設定できます。
user.microapp.locale	FALSE	FALSE	5	使用する文法とプロンプトセットを定義する言語と国の組み合わせ。
user.microapp.metadata	FALSE	FALSE	62	メニュー（M）、Get Data（GD）、およびGet Speech（GS）マイクロアプリケーションに続いて、Unified CVPはそのマイクロアプリケーションの実行に関する情報を返します。
user.microapp.play_data	FALSE	FALSE	40	Play Dataマイクロアプリケーションのデータ用のデフォルトストレージ領域。
user.microapp.sys_media_lib	FALSE	FALSE	10	各桁、月、デフォルトのエラーメッセージなど、すべてのシステムメディアファイルのディレクトリ。
user.microapp.ToExtVXML	FALSE	FALSE	60	この変数配列は、外部VoiceXMLファイルに情報を送信します。スカラ変数ではなく配列型変数として構成し、配列の長さを4に設定する必要があります。
user.microapp.UseVXMLParams	FALSE	FALSE	1	外部VoiceXMLに情報を渡す方法を指定します。
user.microapp.isPostCallSurvey	FALSE	FALSE	1	エージェントが電話を切った後に、ポストコール調査を発信者に提供するかどうかを決定するために使用されます。

名前	有効	永続	最大長（Maximum Length）	説明
user.ece.activity.id	FALSE	FALSE	30	すべてのタイプの WIM および EIM アクティビティに必要です。
user.ece.customer.name	FALSE	FALSE	30	チャット、、コールバック、およびコールバックの遅延アクティビティに必要です。
user.media.id	FALSE	FALSE	36	Unified CCE サービスへのコールを識別する番号（オプションで H.323サービス）。
user.microapp.grammar_choices	FALSE	FALSE	210	発信者が Get Speech マイクロアプリケーションに入力できる ASR 選択肢を指定します。
user.microapp.inline_tts	FALSE	FALSE	210	インライン音声合成（TTS）のテキストを指定します。
user.microapp.media_server	FALSE	FALSE	60	スクリプトで使用されるすべてのメディアファイルおよび外部文法ファイルの URL のルート。
user.microapp.override_cli	FALSE	FALSE	200	発信転送で CLI フィールドを上書きするためにシステムが使用します。
user.microapp.pd_tts	FALSE	FALSE	1	Unifies Text To Speech またはメディアファイルを発信者に対して再生する必要があるかどうかを指定します。

システム情報

- 拡張コールコンテキスト：有効化
- 最小相関番号：1001
- 最大相関番号：9999
- スクリプトバージョンの保持：5

エージェント ターゲティング ルール

属性	
名前	AgentExtensions

属性	
周辺機器	CUCM_PG_1
ルールタイプ	エージェントの内線番号
ルーティングクライアント	すべてのルーティングクライアント
内線番号の範囲	000 ー 999 0000 ー 9999 00000 ー 99999 000000 ー 999999 0000000 ー 9999999 00000000 ー 99999999 000000000 ー 999999999 0000000000 ー 9999999999

Unified Communication Manager の IOPS 値

Unified Communication Managerの IOPS 値は BHCA 値に基づいています。これらの値は、次のシナリオで異なる場合があります。

- 営業時間中のソフトウェアアップグレードでは、定常状態の IOPS に加えて 800 ー 1200 IOPS が生成されます。
- CDR 分析およびレポーティング（CAR）を使用した CDR/CMR：
  - CDR/CMR を外部課金情報サーバーに送信する Unified Communications Manager では、追加の IOPS は発生しません。
  - CAR の継続的負荷の結果、システム上で平均約 300 IOPS が発生します。
  - スケジュールされたアップロードは、Publisher VM の場合のみ約 250 IOPS となります。
- トレース収集は100 IOPSです（トレースが有効になっているすべてのVMで発生します）。
- 夜間バックアップ（通常は Publisher VM のみ）は 50 IOPS です。

ISO ファイルのマウントおよびアンマウント

データストアに ISO イメージをアップロードします。

1. vSphere クライアントでホストを選択し、[構成（Configuration）] をクリックします。次に、左側のパネルで [ストレージ（Storage）] をクリックします。

2. ISO ファイルを保持するデータストアを選択します。
3. 右クリックして、[データストアを参照（Browse datastore）] を選択します。
4. [アップロード（Upload）]アイコンをクリックし、[ファイルのアップロード（Upload file）] を選択します。
5. ISO ファイルを保存したローカル ドライブの場所を参照し、ISO をデータストアにアップロードします。

ISO イメージをマウントします。

1. vSphere クライアントで VM を右クリックし、[仮想マシン設定の編集（Edit virtual machine settings）] を選択します。
2. [ハードウェア（Hardware）] をクリックし、[CD|DVD ドライブ 1（CD|DVD Drive 1）] を選択します。
3. [デバイスのステータス（Device status）] パネル（右上）で **[電源投入時に接続（Connect at Power On）]** をオンにします。
4. **[データストア ISO ファイル（Datastore ISO File）]** オプション ボタンをクリックし、**[参照（Browse）]** をクリックします。
5. ファイルをアップロードするデータストアに移動します。
6. ISO ファイルを選択し、**[OK]** をクリックします。

ISO イメージをアンマウントします。

1. vSphere クライアントで VM を右クリックし、[仮想マシン設定の編集（Edit virtual machine settings）] を選択します。
2. [ハードウェア（Hardware）] をクリックし、[CD|DVD ドライブ 1（CD|DVD Drive 1）] を選択します。
3. [デバイスのステータス（Device status）] パネル（右上）で [電源投入時に接続（Connect at Power On）] をオフにします。

カスタマーサイトで NTP および時刻構成を設定

カスタマーサイドのドメインコントローラは、NTP サーバーを使用して構成する必要があります。 2 台の ESXi host サーバーは、ドメインコントローラとして同じ NTP サーバーを指す必要があります。さらに、ESXi サーバーの時間構成を確認する必要があります。

手順

ステップ 1 NTP サーバーをドメインコントローラに追加するには、以下の手順を実行します。

a) Windows Serverで信頼できるタイムサーバーを構成する方法に関する Microsoft の指示を見つけます。

パブリック NTP サーバがない場合は、インターネット上で利用可能です。

b) 追加する NTP サーバーの IP アドレスまたはドメイン名を書き留めます。

ステップ 2 ESXi コアサーバーがドメインコントローラの NTP サーバーを指すようにするには、以下の手順を実行します。

a) コアサーバーごとに、**[構成（Configuration）]** タブをクリックします。

b) **[時間構成（Time Configuration）] > [プロパティ...（Properties...）] > [オプション（Options）]** の順に選択します。

[一般（General）] と [NTP設定（NTP Settings）] の 2 つのセクションがあるパネルが開きます。

c) [NTP設定（NTP Settings）] をクリックします。次に、**[追加（Add）]** をクリックします。

d) プライマリドメインコントローラの IP アドレスを入力します。[OK] をクリックします。**[再起動（Restart）]** をクリックします。

ステップ 3 NTP サーバーのスタートアップポリシーを構成するには、以下の手順を実行します。

a) **[時間構成（Time Configuration）]** に移動します。**[プロパティ（Properties）]** を選択します。

b) [NTPクライアントの有効化（NTP Client Enabled）] をオンにします。

c) [オプション（Options）] をクリックします。

d) [スタート（Start）] を選択します。[OK] をクリックします。

ステップ 4 ホストサーバーの時間設定を確認するには、以下の手順を実行します。

a) [構成（Configuration）] タブをクリックします。

b) [ソフトウェア（Software）] パネルで、**[時間構成（Time Configuration）]** を選択します。ここには、日時と NTP サーバーが表示されます。

ステップ 5 日付と時刻が正しくない場合は調整します。

a) **[プロパティ...（Properties...）]** をクリックします。
[時間構成（Time Configuration）] ダイアログボックスが開きます。

b) [Time] および [Date] フィールドを変更します。次に [OK] をクリックします。

CCDM ロギングと MaxSizeRollBackups

このセクションでは、CCDM ロギング と MaxSizeRollBackups について説明します。

ロギング

Unified CCDM は、システムの各コンポーネントに広範なロギングフレームワークを提供し、問題発生時のトラブルシューティングを支援します。

ロギングトレースレベルは、個別のコンポーネントごとにレジストリに保存され、次の4つの値のいずれかに設定できます。

ログ レベル	名前	説明
0	エラー	これはロギングの最低レベルです。アプリケーションで発生した例外に関連する情報のみを記録します。
1	警告	警告は、エラーレベルのロギングと、潜在的なシステムの問題に対する警告を発します。
2	情報	情報はデフォルトのロギングレベルです。エラーおよび警告だけでなく、標準の診断情報も提供します。
3	デバッグ	デバッグは、最高レベルのロギングです。実行されるすべての操作の詳細情報を提供します。デバッグロギングはパフォーマンスに悪影響を与えるため、使用は最小限に抑える必要があります。

CCDM サーバーで Unified System CLI してロギングレベルを設定

CCDM サーバーで Unified System CLI を使用してロギングレベルを構成するには、以下の手順を実行します。

手順

ステップ 1 **[スタート（Start）]** > **[すべてのプログラム（All Programs）]** > **[ドメインマネージャ（Domain Manager）]** > **[Unified System CLI]** の順に選択します。

ステップ 2 wsmadmin ユーザーのユーザー名（wsmadmin）とパスワードを入力します。

ステップ 3 オプションでインスタンス名を入力し、**Enter** をクリックします。

ステップ 4 デバッグレベルを入力します（例：debug level 0）。

（注） 値は、上記の表に示す任意のロギングレベルです。

MaxSizeRollBackups

MaxSizeRollBackups 設定は、ログファイルを削除して新しいログファイルを作成する前に保存する1日あたりのログファイル数を定義します。この機能は、大量の例外が短時間でディスクをいっぱいにしないように保護します。

MaxSizeRollBackups パラメータは、アプリケーションサーバー、Web、データ、インポートサーバーサービスの構成ファイルに存在します。パーティショニングサービス、プロビジョニングサービス

Jabber for Windows のインストールと構成

Jabber クライアントのインストールと構成

このインストールプログラムを実行すると、クライアントの単一インスタンスがインストールされ、**[手動設定とサインイン（Manual setup and sign-in）]** ウィンドウで接続設定を指定できます。

手順

ステップ 1 CiscoJabberSetup.msi を起動します。
インストール プログラムにより、インストール プロセスのウィンドウが開きます。

ステップ 2 **[承認してインストール（Accept and Install）]** を選択して、インストールを開始します。

ステップ 3 **[Cisco Jabberを起動（Launch Cisco Jabber）]** をオンにし、**[完了（Finish）]**を選択します。

ステップ 4 **[手動設定とサインイン（Manual setup and sign-in）]** を選択します。

ステップ 5 **[アカウントタイプの選択（Select your Account Type）]** ウィンドウで、**[Cisco Communication Manager（電話機能のみ）（Cisco Communication Manager (Phone capabilities only)）]** をオンにします。

ステップ 6 ログインサーバーで、次のサーバーを選択し、**FTP サーバー**、**CTI サーバー**、**Cisco Unified Communications Manager サーバー**の詳細を入力します。[保存（Save）] をクリックします。

ステップ 7 **ユーザー名**（jabber 電話の Cisco Unified Communications Manager で作成されたエンドユーザー）と**パスワード**を入力し、サインインします。

UCDM を使用した Jabber の構成

エンドユーザーの追加

手順

ステップ 1 プロバイダー/カスタマー管理者としてログインします。

ステップ 2 **[ロケーション管理（Location Administration）]** > **[エンドユーザー（End Users）]** の順に選択します。

ステップ 3 ドロップダウンリストから [ロケーション（Location）] を選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 **[ユーザー名（Username）]**、**[パスワード（Password）]**、**[姓（Lastname）]** を入力したら、ドロップダウンリストで、**[ロール（Role）]** を選択します。

ステップ 6 フォームの残りの部分で、**ユーザー詳細**を入力し、**[次へ（Next）]** をクリックします。

ステップ 7 ユーザーの**電話の PIN** を入力します。

ステップ 8 **[機能グループ（Feature Group）]** を選択します。

ステップ 9 **[アクセスプロファイル（Access Profile）]**、**[セキュリティプロファイル（Security Profile）]**、および **[機能表示ポリシー（Feature Display Policy）]** を選択します。

ステップ 10 [追加（Add）] をクリックします。

シングル サイン オン アカウントへのエージェントおよびスーパーバイザの移行

既存展開で SSO を有効にする場合は、SSO 状態をハイブリッドに設定して、SSO ユーザーと非 SSO ユーザーの混在をサポートできます。ハイブリッドモードでは、SSO に対してエージェントとスーパーバイザを選択的に有効にできます。これにより、段階的にシステムを SSO に移行できます。

Unified CCE Administration Bulk Jobs ツールの SSO 移行コンテンツファイルを使用して、エージェントおよびスーパーバイザのグループを SSO アカウントに移行するには、このセクションの手順を使用します。Administration Bulk Jobs ツールを使用して、SSO アカウントに移行されていないエージェントとスーパーバイザのレコードを含むコンテンツファイルをダウンロードします。ローカルでコンテンツファイルを変更して、既存のエージェントとスーパーバイザの SSO ユーザー名を指定します。Administration Bulk Jobs ツールを再度使用して、コンテンツファイルをアップロードし、エージェントとスーパーバイザのユーザー名を更新します。また SSO に対してユーザーも自動的に有効化されます。

コンテンツファイルは、SSO アカウントに移行されていない初めの 12000 エージェントおよびスーパーバイザを返します。一括ジョブを実行してそのレコードグループからユーザを更新した後は、SSO 移行コンテンツ ファイルを再度ダウンロードして、追加のエージェントおよびスーパーバイザのレコードを更新できます。

ユーザを移行しない場合は、そのユーザの行を削除します。

エージェントまたはスーパーバイザログインの SSO を設定する方法については、「Cisco Identity Service の設定 （315 ページ）」を参照してください。

重要 Finesseエージェントがログインしている間にログイン名を変更すると、エージェントは応答したり電話をかけたりすることができなくなります。この状況では、エージェントを引き続き *[ready]* および *[not_ready]* 状態の間で切り替えることができます。これは、SSO が有効か無効かに関係なく、すべてのアクティブエージェントに影響します。ログイン名を変更する必要がある場合は、対応するエージェントがログアウトしてから行ってください。エージェントがログインしているときは、SSOの移行（ハイブリッドまたはグローバルオンのいずれかによって非 SSO エージェントを SSO 対応に移行すること）は行わないでください。

手順

ステップ 1 Unified CCE Administration で、**[管理（Manage）]** > **[一括ジョブ（Bulk Jobs）]** の順に選択します。

ステップ 2 SSO 移行一括ジョブコンテンツファイルをダウンロードします。

a) **[テンプレート（Templates）]** をクリックします。

[テンプレートのダウンロード（Download Templates）] ポップアップ ウィンドウが開きます。

b) SSO 移行テンプレートの **[ダウンロード（Download）]** アイコンをクリックします。

c) [テンプレートのダウンロード（Download Templates）] ポップアップ ウィンドウを閉じるには、[OK] をクリックします。

ステップ 3 SSO移行 コンテンツファイルに SSO ユーザー名を入力します。

a) Microsoft Excel でテンプレートを開きます。SSO アカウントに移行するエージェントおよびスーパーバイザの **[newUserName]** フィールドを更新します。

SSO 移行の一括ジョブのコンテンツ ファイルには、次のフィールドが含まれます。

フィールド	必須かどうか	説明
userName	はい	ユーザの非 SSO のユーザ名。
firstName	いいえ	ユーザの名。
lastName	いいえ	ユーザの姓。
newUserName	いいえ	ユーザの新しい SSO のユーザ名。255 文字以下の ASCII 文字で入力します。 ユーザに SSO を有効にするが、現在のユーザ名を保持する場合は、[newUserName] を空白のままにするか、または [userName] の値を [newUserName] にコピーします。

b) 入力したファイルをローカルに保存します。

ステップ 4 データベースのユーザー名を更新する一括ジョブを作成します。

a) [新規（New）] をクリックして、[新規一括ジョブ（New Bulk Job）] ウィンドウを開きます。

b) 任意でジョブの**説明**を入力します。

c) **[コンテンツファイル（Content File）]** フィールドで、入力した SSO 移行コンテンツファイルを参照します。

一括ジョブが作成される前に [コンテンツファイル（Content File）] が検証されます。

d) **[保存（Save）]** をクリックします。

新しい一括ジョブが一括ジョブのリストに表示されます。必要に応じて、一括ジョブをクリックして、一括ジョブの詳細とステータスを確認します。一括ジョブのログファイルをダウンロードすることもできます。

一括ジョブが完了すると、エージェントとスーパーバイザの SSO が有効になり、ユーザー名が更新されます。個々のユーザーのレコードを開くと、変更を確認できます。

ステップ 5 必要に応じてこの手順を繰り返し、追加のエージェントとスーパーバイザーを SSO ユーザー名に移行します。

次のタスク

展開内のすべてのエージェントとスーパーバイザが SSO アカウントに移行されたら、展開内で SSO をグローバルに有効にできます。

シングルサインオンの全体的な無効化

SSO またはハイブリッドモードからシングルサインオンを全体的に無効にする必要がある場合は、以下の手順を実行します。

重要 後でエージェントまたはスーパーバイザを SSO 対応から非 SSO に移行する場合：

- SSO 対応として作成された Cisco Unified Intelligence Center スーパーバイザを非 SSO に変更すると、次回のユーザー同期後に、新しい非 SSO ユーザーアカウントがスーパーバイザ用に作成されます。古い SSO 対応のスーパーバイザアカウント（形式が SSO\<loginname>）は、引き続き Cisco Unified Intelligence Center に存在するので、削除する必要があります。スーパーバイザのレポーティングおよび権限を設定するには、Cisco Unified Intelligence Center 管理コンソールで、（Active Directory のスーパーバイザ SAM アカウントと一致する）新規かつ非 SSP スーパーバイザのユーザーアカウントを再度構成する必要があります。

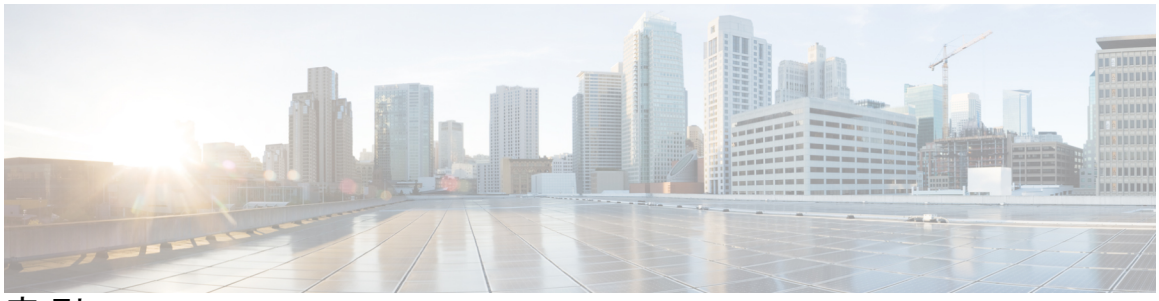
手順

ステップ 1 システムが、**SSP** モードの場合、Unified CCE Administration **シングルサインオン**ツールで、SSO モードを **[ハイブリッド（Hybrid）]** に変更します。

ステップ 2 SSO のエージェントを無効にし、エージェントに新しいパスワードを割り当てます。この手順により、エージェントは Finesse にサインインできます。

ステップ 3 SSO のスーパーバイザを無効にします。この手順によりスーパーバイザは、Unified CCE Administration にサインインして、エージェントの再スキルができるようになります。

ステップ 4 すべてのエージェントまたはスーパーバイザレコードを更新したら、SSO モードを**非 SSO** モードに変更します。



索引

ろ