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 *1 : 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 （2 ページ）	
2	仮想マシンの起動とシャットダウンの設定 （2 ページ）	
3	ドメイン コントローラ サーバーの作成 （3 ページ）	
4	Cisco Unified CCE Rogger の構成 （6 ページ）	
5	Unified CCE AW-HDS-DDS の構成 （17 ページ）	
6	Unified CCE PG の構成 （23 ページ）	
7	Unified CVP の構成 （36 ページ）	
8	Cisco IOS Enterprise 音声ゲートウェイの構成 （57 ページ）	

順序	タスク	完了したか
9	Unified Communications Manager の構成 （63 ページ）	
10	Unified Intelligence Center Coresident 展開の構成 （69 ページ）	
11	Cisco Finesse の構成 （86 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 （2 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 （115 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」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 （7 ページ）	
2	ドメイン内マシンの検証 （9 ページ）	
3	ドメインマネージャの構成 （10 ページ）	
4	Unified CCE 暗号化ユーティリティの構成 （11 ページ）	
5	CCE コンポーネント用 SQL Server の設定 （12 ページ）	
6	セカンダリドライブの構成 （12 ページ）	
7	Unified CCE Logger の構成 （13 ページ）	
8	Unified CCE ルーターの構成 （15 ページ）	
9	基本構成のロード （16 ページ）	
10	Cisco Diagnostic Framework Portico の検証 （32 ページ）	
11	Cisco SNMP の設定 （32 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 （9 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 （12 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 （15 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 2: 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」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 *3:* 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 （7 ページ）	
2	ネットワーク カードの検証 （37 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （11 ページ）	
4	CCE コンポーネント用 SQL Server の設定 （12 ページ）	
5	セカンダリドライブの構成 （12 ページ）	
6	AW-HDS-DDS （18 ページ）	
7		
8	Cisco Diagnostic Framework Portico の検証 （32 ページ）	
9	Cisco SNMP の設定 （32 ページ）	
10	HCS for CC 展開タイプの設定 （22 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 4 : データおよびログファイルのサイズ （22 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 *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
<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 *5* : 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 （7 ページ）	
2	ネットワーク カードの検証 （37 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （11 ページ）	
4	Cisco Unified Communications Manager 周辺機器ゲートウェイの構成 （23 ページ）	
5	VRU 周辺機器ゲートウェイの構成 （27 ページ）	
6	MR 周辺機器ゲートウェイの構成 （28 ページ）	
7	CTI サーバーの構成 （30 ページ）	
8	JTAPI のインストール （31 ページ）	
9	Cisco Diagnostic Framework Portico の検証 （32 ページ）	
10	Cisco SNMP の設定 （32 ページ）	
11	Unified CCE サービスの起動 （36 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 （24 ページ）
- PG の追加準備 （24 ページ）
- Cisco Unified Communications Manager PG の追加 （24 ページ）
- Cisco Unified Communications Manager PIM の追加 （25 ページ）
- PIM の作成後 （26 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

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 （28 ページ）
- 2000 エージェント展開にマルチチャネル PIM を追加 （29 ページ）
- アウトバウンド PIM の追加 （30 ページ）
- PIM の作成後 （26 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 （63 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 （33 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 （33 ページ）
- SNMP V1 and V2c のコミュニティ名の設定 （34 ページ）
- SNMP V3 用の SNMP ユーザー名の設定 （34 ページ）

• SNMP トラップの接続先設定 （35 ページ）
• SNMP Syslog の接続先設定 （36 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 （33 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 （33 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 （33 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 （33 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 （33 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 （33 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 （37 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（40 ページ）	
3	Cisco Unified CVP オペレーションコンソールの構成 （46 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 （37 ページ）	
2	Unified CVP メディアサーバー IISの設定 （37 ページ）	
3	FTP サーバーの設定 （39 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

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 （37 ページ）	?
2	セカンダリドライブの構成 （12 ページ）	?
3	Unified CVP レポーティングユーザー （41 ページ）	?
4	Cisco Unified CVP レポートデータのデータソースの作成 （43 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 （43 ページ）	
2	Cisco Unified CVP レポートテンプレートの取得（44 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 （45 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 （37 ページ）	
2	Unified CVP オペレーションコンソールの有効化 （46 ページ）	
3	Unified CVP コール サーバー コンポーネントの構成 （47 ページ）	
4	Unified CVP サーバー コンポーネントの構成 （48 ページ）	
5	Unified CVP レポーティングサーバーの構成 （49 ページ）	
6	Unified CVP メディアサーバーの構成 （50 ページ）	
7	Unified CVP ライセンスのインストール （50 ページ）	
8	ゲートウェイの構成 （51 ページ）	
9	Unified CCE デバイスの追加 （52 ページ）	
10	Unified Communications Manager デバイスの追加 （53 ページ）	
11	Unified Intelligence Center デバイスの追加 （53 ページ）	
12	スクリプトおよびメディアファイルの転送 （51 ページ）	
13	SNMP の構成 （52 ページ）	
14	SIP サーバーグループの構成 （54 ページ）	
15	ダイヤル番号パターンの構成 （55 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 （64 ページ）	
2	Unified Communications Manager Subscriber の構成 （65 ページ）	
3	Windows 用 VMware ツールのインストール	
4	Unified Communications Manager ライセンス （66 ページ）	

順序	タスク	完了したか
5	サービスのアクティブ化 （67 ページ）	
6	クラスタ全体のドメイン構成の検証 （68 ページ）	
7	Unified CCE サーバー に JTAPI をインストール （69 ページ）	
8	SNMP の構成 （96 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 （54 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 （31 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 （70 ページ）	
2	Unified Intelligence Center Subscriber の構成 （70 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 （72 ページ）	
4	Windows 用 VMware ツールのインストール	
5	Unified Intelligence Center レポーティングの構成 （73 ページ）	
6	Unified Intelligence Center Administration の設定 （77 ページ）	
7	SNMP の構成 （96 ページ）	
8	ライブデータ AW アクセスの構成 （80 ページ）	
9	Live Data Unified Intelligence データソースの構成 （82 ページ）	
10	ライブデータレポーティング間隔の構成 （83ページ）	
11	Transport Layer Security の設定 （84 ページ）	
12	ライブデータレポートのインポート （84 ページ）	

順序	タスク	完了したか
13	HTTPS ガジェットの証明書の追加 （84 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。

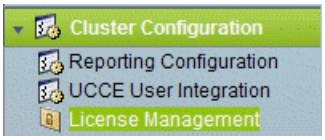
パートナーは一意のライセンスを取得して、カスタマー サイトのインポートされた Unified Intelligence Center サーバーに適用する必要があります。

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 *1:* 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 （41 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 *6:* 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 （73 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 *7:* 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 *8:* 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 *9:* 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 （86 ページ）	
2	-	
3	Cisco Finesse セカンダリノードの構成 （90 ページ）	
4	Windows 用 VMware ツールのインストール	
5	Cisco Finesse 管理の構成 （91 ページ）	
6	SNMP の構成 （96 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 （87 ページ）
- Unified Contact Center Enterprise 管理およびデータサーバーの構成 （89 ページ）
- Cisco Tomcat サービスの再起動 （90 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 *10 : 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 （92 ページ）
- Cisco Finesse 用 自己署名証明書の信頼 （93 ページ）
- Internet Explorer のブラウザ設定 （95 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 *11 : 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 （2 ページ）	
2	仮想マシンの起動とシャットダウンの設定 （2 ページ）	
3	ドメイン コントローラ サーバーの作成 （3 ページ）	
4	Cisco Unified CCE Rogger の構成 （98 ページ）	
5	Unified CCE AW-HDS-DDS の構成 （17 ページ）	
6	Unified CCE PG の構成 （23 ページ）	
7	Unified CVP の構成 （36 ページ）	
8	Cisco IOS Enterprise 音声ゲートウェイの構成 （57 ページ）	
9	Unified Communications Manager の構成 （63 ページ）	
10	Unified Intelligence Center の構成 （99 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 （109 ページ）	
12	Cisco Finesse の構成 （86 ページ）	
13	Cisco Identity Service の構成 （100 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 （7 ページ）	
2	ドメイン内マシンの検証 （9 ページ）	
3	ドメインマネージャの構成 （10 ページ）	
4	Unified CCE 暗号化ユーティリティの構成 （11 ページ）	
5	CCE コンポーネント用 SQL Server の設定 （12 ページ）	
6	セカンダリドライブの構成 （12 ページ）	
7	Unified CCE Logger の構成 （13 ページ）	
8	Unified CCE ルーターの構成 （15 ページ）	
9	基本構成のロード （98 ページ）	
10	Cisco Diagnostic Framework Portico の検証 （32 ページ）	
11	Cisco SNMP の設定 （32 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」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 （70 ページ）	
2	Unified Intelligence Center Subscriber の構成 （70 ページ）	
3	Windows 用 VMware ツールのインストール	
4	Unified Intelligence Center レポーティングの構成 （73 ページ）	

順序	タスク	完了したか
5	Unified Intelligence Center Administration の設定 （77 ページ）	
6	SNMP の構成 （96 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 （80 ページ）	
2	ライブデータ マシン サービスの構成 （81 ページ）	
3	Live Data Unified Intelligence データ ソースの構成 （82 ページ）	
4	ライブデータ レポーティング間隔の構成 （83 ページ）	
5	Transport Layer Security の設定 （84 ページ）	
6	ライブデータ レポートのインポート （84 ページ）	
7	HTTPS ガジェットの証明書の追加 （84 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 （100 ページ）	
2	IDS サブスクライバ ノードの設定 （101 ページ）	
3	Ids Subscriber の構成 （102 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 *12 : 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 （2 ページ）	
2	仮想マシンの起動とシャットダウンの設定 （2 ページ）	
3	ドメイン コントローラ サーバーの作成 （3 ページ）	
4	Unified CCE Logger の構成 （103 ページ）	

順序	タスク	完了したか
5	Unified CCE ルーターの構成 （105 ページ）	
6	Unified CCE AW-HDS の構成 （105 ページ）	
7	Unified CCE HDS-DDS の構成 （107 ページ）	
8	Unified CCE PG の構成 （23 ページ）	
9	Unified CVP の構成 （36 ページ）	
10	Cisco IOS Enterprise 音声ゲートウェイの構成 （57 ページ）	
11	Unified Communications Manager の構成 （63 ページ）	
12	Unified Intelligence Center の構成 （99 ページ）	
13	ライブ データ レポーティング システムの構成 （109 ページ）	
14	Cisco Finesse の構成 （86 ページ）	
15	シングルサインオン管理	
16	Cisco Identity Service の構成 （100 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 （7 ページ）	
2	ドメイン内マシンの検証 （9 ページ）	
3	ドメインマネージャの構成 （10 ページ）	
4	Unified CCE 暗号化ユーティリティの構成 （11 ページ）	
5	CCE コンポーネント用 SQL Server の設定 （12 ページ）	
6	セカンダリドライブの構成 （12 ページ）	
7	Unified CCE Logger の構成 （13 ページ）	
8	基本構成のロード （104 ページ）	
9	Cisco Diagnostic Framework Portico の検証 （32 ページ）	

順序	タスク	完了したか
10	Cisco SNMP の設定 （32 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」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 （7 ページ）	
2	ネットワーク カードの検証 （37 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （11 ページ）	
4	Unified CCE ルーターの構成 （15 ページ）	
5	Cisco Diagnostic Framework Portico の検証 （32 ページ）	
6	Cisco SNMP の設定 （32 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 *13* : 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 （7 ページ）	
2	ドメイン内マシンの検証 （9 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （11 ページ）	
4	CCE コンポーネント用 SQL Server の設定 （12 ページ）	
5	セカンダリ ドライブの構成 （12 ページ）	
6	AW-HDS （105 ページ）	
7	Cisco Diagnostic Framework Portico の検証 （32 ページ）	
8	Cisco SNMP の設定 （32 ページ）	
9	HCS for CC 展開タイプの設定 （22 ページ）	

AW-HDS

- インスタンスの作成 （18 ページ）

• HDS データベースの作成 （19 ページ）
• AW-HDS の構成 （106 ページ）
• データベースとログファイルのサイズ （21 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 *14* : 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 （7 ページ）	
2	ネットワーク カードの検証 （37 ページ）	
3	Unified CCE 暗号化ユーティリティの構成 （11 ページ）	
4	CCE コンポーネント用 SQL Server の設定 （12 ページ）	
5	セカンダリ ドライブの構成 （12 ページ）	
6	HDS-DDS （107 ページ）	
7	Cisco Diagnostic Framework Portico の検証 （32 ページ）	
8	Cisco SNMP の設定 （32 ページ）	

HDS-DDS

- インスタンスの作成 （18 ページ）
- HDS データベースの作成 （19 ページ）

• HDS-DDS の構成 （108 ページ）
• データベースとログファイルのサイズ （21 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 （70 ページ）	
2	Unified Intelligence Center Subscriber の構成 （70 ページ）	
3	Windows 用 VMware ツールのインストール	
4	Unified Intelligence Center レポーティングの構成 （73 ページ）	
5	Unified Intelligence Center Administration の設定 （77 ページ）	
6	SNMP の構成 （96 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 （80 ページ）	
2	ライブ データ マシン サービスの構成 （81 ページ）	
3	Live Data Unified Intelligence データ ソースの構成 （82 ページ）	
4	ライブデータ レポーティング間隔の構成 （83 ページ）	

順序	タスク	完了したか
6	HTTPS ガジェットの証明書の追加 （84 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 *15*：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 （2 ページ）	
2	仮想マシンの起動とシャットダウンの設定 （2 ページ）	
3	Small Contact Center 展開の Finesse 用 DNS サーバーの作成 （115 ページ）	
4	Small Contact Center エージェント展開用 Unified CCE Rogger の構成 （111 ページ）	
5	Unified CCE AW-HDS-DDS の構成 （17 ページ）	
6	VRU 周辺機器ゲートウェイの構成 （27 ページ）	
7	Unified CVP の構成 （36 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 （117 ページ）	
9	Unified Intelligence Center の構成 （99 ページ）	
10	ライブ データ レポーティング システムの構成 （100 ページ）	

表 *16*：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 （2 ページ）	
2	Unified CCE PG の構成 （23 ページ）	

順序	タスク	完了
3	Unified Communications Manager の構成 （63 ページ）	
4	SW MTP および SW 会議リソースの増加	
5	Cisco Finesse の構成 （86 ページ）	
6	Cisco Identity Service の構成 （100 ページ）	

表 *17* : 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 （2 ページ）	
2	Unified CCE PG の構成 （23 ページ）	
3	Shared Unified Communications Manager の構成 （114 ページ）	
4	Cisco Finesse の構成 （86 ページ）	
5	Cisco Identity Service の構成 （100 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」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 （7 ページ）	
2	ドメイン内マシンの検証 （9 ページ）	
3	ドメインマネージャの構成 （10 ページ）	
4	Unified CCE 暗号化ユーティリティの構成 （11 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 （12 ページ）	
6	セカンダリ ドライブの構成 （12 ページ）	
7	Unified CCE Logger の構成 （13 ページ）	
8	Small Contact Center 向け Unified CCE ルーターの構成 （113 ページ）	
9	基本構成のロード （112 ページ）	
10	Cisco Diagnostic Framework Portico の検証 （32 ページ）	
11	Cisco SNMP の設定 （32 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」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 （64 ページ）	
2	Unified Communications Manager Subscriber の構成 （65 ページ）	
3	Windows 用 VMware ツールのインストール	
4	Unified Communications Manager ライセンス （66 ページ）	
5	サービスのアクティブ化 （67 ページ）	
6	クラスタ全体のドメイン構成の検証 （68 ページ）	
7	Unified CCE サーバー に JTAPI をインストール （69 ページ）	
8	SNMP の構成 （96 ページ）	
9	パーティションの設定	
10	コーリングサーチスペースの設定	
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	
12	CSS とトランクの関連付け	

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 （115 ページ）
• DNS サーバーの構成 （115 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
```