インストール後の設定

Packaged CCE 2000 エージェント展開

Packaged CCE 2000 エージェント展開のコンポーネントを設定するには、以下の手順を実行します。

手順	タスク
1	CCE コンポーネントの設定 （2 ページ）
2	Cisco Unified Customer Voice Portal の設定 （25 ページ）
3	外部メディア サーバの場合、メディア サーバの設定
4	Cisco Unified Communications Manager の設定 （25 ページ）
5	Cisco Unified Intelligence Center の設定 （35 ページ）
6	Cisco Finesse の設定 （40 ページ）
7	Cisco Unified Customer Voice Portal Reporting Server の設定 （44 ページ） （任意）
8	VVB の設定 （48 ページ） （任意）
9	Cisco IOS Enterprise 音声ゲートウェイの設定 （49 ページ）

手順	タスク
10	IPv6 を設定する （56 ページ）
11	エンタープライズ チャットおよび電子メール（ECE）の設定（オプション） 電子メールおよびチャット

CCE コンポーネントの設定

以下の手順を実行して、コアの CCE コンポーネントを設定します。

手順	タスク
1	CCE コンポーネント用 SQL Server の設定 （2 ページ）
2	組織ユニットの設定 （3 ページ）
3	Packaged CCE 2000 エージェント展開タイプの初期化 （5 ページ）
4	メディア ルーティング ペリフェラル ゲートウェイへの PIM の追加（任意）
5	Cisco SNMP の設定 （21 ページ）（任意）
6	CA 証明書の詳細については、以下を参照してください。 AW マシンに CA 署名付き証明書を生成してインポートする
7	自己署名付き証明書の詳細については、以下を参照してください。 AWマシンで自己署名証明書を生成してインポートする

CCE コンポーネント用 SQL Server の設定

以下の手順を、ロガー、Rogger、および AW マシンで実行する必要があります。

手順

ステップ 1 **Microsoft SQL Server 2014 Management Studio**を開きます。

ステップ 2 ログインします。

ステップ 3 [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 4 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。

組織ユニットの設定

ドメインの追加

ドメイン マネージャ ツールを使用してドメインを追加します。AW サーバ上で以下の手順を 1 回のみ実行します。

手順

ステップ 1 ドメイン管理者権限を持つユーザとしてログインします。

ステップ 2 デスクトップの Unified CCE ツールのショートカットを使用して、**ドメイン マネージャ** ツールを開きます。

ステップ 3 **ドメイン**の下の **選択する**をクリックします。

ステップ 4 **ドメインの選択** ダイアログ ボックスを使用して、ドメインを追加することができます。また、対象ドメインが自動的に検出できない場合は、ドメインを手動で追加することもできます。

[ドメインの選択] ダイアログ ボックスのコントロールを使用してドメインを追加する手順：

a) [ドメインの選択] の下にある左側のペインで、1 つまたは複数のドメインを選択します。
b) **追加** をクリックして選択したドメインを追加するか、**すべて選択** をクリックしてすべてのドメインを追加します。

ドメインの手動追加手順：

a) [ドメイン名を入力してください] の下のフィールドに、追加するドメイン名を完全修飾名で入力します。
b) [追加（Add）] をクリックします。
c) [OK] をクリックします。

組織ユニットの追加

ドメイン マネージャ ツールを使用して、ドメインの Cisco ルート組織単位（OU）を作成し、施設とインスタンスの OU を作成します。

システム ソフトウェアは、常に Cisco_ICM という名前のルート OU を使用します。Cisco_ICM OU は、Unified ICM セントラル コントローラがインストールされたドメイン内のいかなるレベルにも配置することができます。システム ソフトウェア コンポーネントは、この名前を検索することで、ルート OU を特定します。

Cisco Root OU を作成したユーザは、自動的に Cisco ルート OU の設定セキュリティ グループのメンバーとなります。実際には、このユーザにはドメイン内のすべての Unified CCE タスクに対する権限が与えられます。

手順

ステップ 1 ドメイン管理者権限を使用してログインして、デスクトップの Unified CCE ツールのショートカットで **ドメイン マネージャ** ツールを開きます。

ステップ 2 ドメインを選択します。

ステップ 3 この OU が最初のインスタンスである場合は、以下の手順を実行して、Cisco_ICM ルートを追加します。

a) [Cisco ルート] の下の、**追加する**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] ダイアログ ボックスに戻ると、Cisco ルート OU がドメイン ルートまたは選択した OU に表示されます。これでファシリティを追加できます。

ステップ 4 ファシリティ OU の追加手順：

a) ファシリティ OU を作成する Cisco Root OU を選択します。
b) 右側のペインで、[ファシリティ] の下の **追加**をクリックします。
c) ファシリティ名を入力して、**OK**をクリックします。

ステップ 5 インスタンス OUの追加手順：

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) 右側のペインで、[インスタンス] の下の **追加**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 6 [閉じる（Close）] をクリックします。

セキュリティ グループへのユーザの追加

セキュリティ グループにドメイン ユーザを追加するには、以下の手順を実行します。次に、このセキュリティ グループによって制御される機能に対して、ユーザ特権が与えられます。

手順

ステップ 1 ドメイン マネージャ ツールを開き、ユーザを追加するセキュリティ グループを選択します。

ステップ 2 [セキュリティ グループ] で、**メンバー**をクリックします。

ステップ 3 [ユーザ] の下の **追加**をクリックします。

ステップ 4 追加するユーザのドメインを選択します。

ステップ 5 （オプション）**オプションのフィルタ** フィールドで、名前またはユーザのログオン名でさらにフィルタを選択し、検索条件を適用して検索する値を入力します。

ステップ 6 [検索（Search）] をクリックします。

ステップ 7 検索結果でセキュリティ グループに追加するメンバーを選択します。

ステップ 8 [OK] をクリックします。

Packaged CCE 2000 エージェント展開タイプの初期化

Unified CCE Administration を使用して Packaged CCE 導入を初期化します。

Unified CCE Administration への初回ログイン時に、導入のコンポーネントの情報とクレデンシャルを入力する必要があります。Packaged CCE はこの情報を使用して、コンポーネントを設定し、システム インベントリを構築します。

既存の環境を新しいリリースにアップグレードする場合、Packaged CCE で入力が必要になるのは、不明な情報およびクレデンシャルのみです。この場合、必ずしもすべての手順を実行する必要はありません。

（注） システムでは IP アドレスの変更はサポートされていません。IP アドレスの変更が予想される場合は、ホスト名を使用します。これはすべての **ホスト名および IP アドレス** フィールドに適用されます。

手順

ステップ 1 Active Directory のユーザ名（*user@domain*）とパスワードを使用して **Unified CCE Administration** にログインします（`https://<IP` アドレス>/cceadmin、<IP アドレス>はサイド A の Unified CCE AW-HDS-DDS のアドレス）。
[導入を設定する（Configure your deployment）] ポップアップ ウィンドウが自動的に開きます。

ステップ 2 **展開タイプ** ページで、**展開タイプ** および **インスタンス** をそれぞれのドロップダウン リストで選択します。このとき、ユーザは、選択するインスタンスのセットアップセキュリティ グループのメンバーである必要があります。[次へ（Next）] をクリックします。

ステップ 3 **VM ホスト** ページで、サイド A およびサイド B の IP アドレス、ユーザ名、およびパスワードを入力します。

VMware ホストは、ESXi がインストールされた 2 台の UCS サーバを指します。[ユーザ名（username）] と [パスワード（password）] フィールドは、ESXi に設定されたホストのログイン名とパスワードです。

ステップ 4 ハードウェア レイアウト タイプに **M3 あるいは M4 検証済リファレンス設定** または **M5 検証済みリファレンス設定 / 仕様に基づく設定** を選択し、**次へ**をクリックします。

Packaged CCE が導入した VM を検証します。

- **テスト済 M3 または M4 参照設定**を選択すると、システムはハードウェアがサポートされているかどうかを確認し、その VM が参照設計に従って構成されているかどうかを検証します。検証が正常に実行されると、**クレデンシャル** ページが開きます。
- **検証済の M5 リファレンス設定 / 仕様に戻づく設定**を選択すると、システムが VMware ホストのハードウェア仕様を検証し、VM が参照設計に従って構成されているかどうかを確認します。検証が正常に終了したら、**次へ**をクリックして**クレデンシャル(** ページを開きます。ハードウェア仕様については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html の *Cisco Packaged CCE* の仮想化 を参照してください。

  （注）
  - Cisco VM で使用されるデータストアは、他のサードパーティ VM で共有または使用しないでください。
  - Packaged CCE コア コンポーネントには、以下が含まれます。
    - Unified CCE Rogger
    - Unified CCE AW または HDS または DDS
    - Unified CCE PG
    - Unified CVP Server
    - Unified Intelligence Center パブリッシャ （ライブ データおよび IdS と共存）
    - Finesse

    VM アノテーションは、Packaged CCE コア コンポーネントの VM の識別に使用されます。コア コンポーネント VM のデフォルトのアノテーションはいずれも変更しないでください。以下の用語は、コア コンポーネントのアノテーション専用となっています。Finesse、CUIC、および CVP。上記の専用語は、コア コンポーネント VM 以外のアノテーションに使用しないでください。
  - コア コンポーネントは、オンボックスで、その他のすべてのコンポーネントを外部マシンとして追加する必要があります。詳細については、外部マシンの追加を参照してください。

- 検証が失敗した場合は、**ホストの更新** をクリックして、**VM ホスト** ページに移動して値を編集します。既存値で検証を実行するには、**再試行** をクリックします。

ステップ 5 [クレデンシャル（Credentials）] ページで、導入の各コンポーネントの情報を入力します。コンポーネントの情報を入力したら、[次へ（Next）] をクリックします。

入力したクレデンシャルが検証されると、次のコンポーネントの情報を入力するためのフィールドが表示されます。

コンポーネント	必要な情報
Unified CM	次のいずれかを行います。 • オンボックス Unified Communications Manager 導入の Unified CM パブリッシャ。 • 外部 Unified Communications Manager 導入の Unified CM パブリッシャ名と IP アドレス。 （注） • Unified CM クラスタは 1 つのみが、Packaged CCE 展開の単一のサイトに統合することができます。 • **M3 あるいは M4 の検証済のリファレンス設定**は、Unified CM 12.5 をオフボックスでインストールする必要があります。 AXL ユーザ名およびパスワード。
Unified CVP	Unified CVP サーバ (サイド A) Windows 資格情報。 Unified CVP サーバ（サイド B）Windows クレデンシャル。
Unified CCE AW-HDS-DDS	Unified CCE 診断フレームワーク サービスのドメイン、ユーザ名、およびパスワード。 これらのクレデンシャルは、インスタンスのセキュリティ設定グループのメンバーであり、導入内のすべての Unified CCE コンポーネント（Unified CCE Rogger、PG および AW-HDS-DDS）上で有効な、ドメイン ユーザ用であることが必要です。
Unified Intelligence Center	Unified Intelligence Center Administration アプリケーションのユーザ名とパスワード。 Identity Service Administration のユーザ名およびパスワード。
Finesse	Finesse Administration のユーザ名およびパスワード。
CVP レポート	（注） このタブは、Unified CVP レポート サーバが **M3 または M4 の検証済レファレンス設定**でオンボックスの場合にのみ利用可能となります。 Unified CVP レポート サーバの Windows クレデンシャル。

ステップ 6 **設定** ページで、以下を選択します。

- [Mobile Agentコーデック（Mobile Agent Codec）] ドロップダウン メニューから、Mobile Agent コールに使用するコーデックを選択します。選択するコーデックは、音声ゲートウェイで指定されたコーデックと一致する必要があります。

- 外部 Unified Communications Manager がある場合は、[サイド A 接続（Side A Connection）] および [サイド B 接続（Side B Connection）] ドロップダウン メニューから、 の Unified CCE PG が接続する Unified CM サブスクライバを選択します。
- Packaged CCE サーバと同じドメインに既存の Active Directory ユーザのユーザ名とパスワードを入力します。このアカウントはサービス グループに追加されます。

[次へ（Next）]をクリックします。

導入が初期化されます。[詳細（Details）] ダイアログボックスに自動初期化タスクのステータスが表示されます。

詳細については、コンポーネントの自動初期化タスク （8 ページ）を参照してください。

ステップ 7 自動初期化タスクが完了したら、[完了（Done）] をクリックします。

自動初期化タスクのいずれかが失敗した場合は、エラーを修正して [再試行（Retry）]をクリックします。

再試行が成功した場合は、自動初期化が続行されます。

一部のタスクが失敗した場合は、完了済みのすべてのタスクを再試行以前の状態に戻してから再試行する必要があります。このとき、システムを正常な状態に戻す必要があることを通知するメッセージが表示されます。

[OK] をクリックし、システムを正常な状態に戻してから [やり直す（Start Over）] をクリックします。

（注） 初期化が完了したら、[完了（Done）] をクリックします。[システム インベントリ（System Inventory）] が開き、一部のマシンに関するアラートが表示されます。これらのアラートは、Unified Communications Manager を設定するとクリアされます。

次のタスク

の展開を設定後、システム レベルの設定を指定します。例えば、Unified Communications Manager、Unified CVP、および発信コールのラベルを入力できます。その他を参照してください。

コンポーネントの自動初期化タスク

Packaged CCE は初期化中に次のタスクを実行します。

コンポーネント（Component）	自動初期化タスク
Unified CCE Rogger	• ロガーを作成します。 • 必要な基本設定を使用してロガー データベースを作成します。 • ルータを作成します。
Unified CCE PG	• Unified Communications Manager から JTAPI をダウンロードし、Unified CCE PG にインストールします。 • CUCM PIM を使用して CUCM ペリフェラル ゲートウェイ（PG）を作成します。 • メディア ルーティング PG（MR PG）を作成します。 • 2 つの VRU PIM を使用して、VRU PG を作成します。 • CTI サーバを作成します。
Unified CCE AW-HDS-DDS	• AW-HDS-DDS を作成します。 • AW と履歴データベースを作成します。 • Unified Intelligence Center データ ソースに使用される Cisco Unified Intelligence Center SQL ユーザ アカウントを作成します。 • Cisco Finesse データ ソースに使用される Cisco Finesse SQL ユーザ アカウントを作成します。
Unified Communications Manager	• Unified CCE PG の設定に使用されるアプリケーション ユーザを作成します。
Unified Customer Voice Portal	• Unified CVP Call サーバを設定します。 • Unified CVP VXML サーバを設定します。 • Unified CVP Media サーバを設定します。
Unified CVP Reporting Server	• Unified CVP レポート サーバを 初期化 します。
Unified Intelligence Center	• 履歴およびリアルタイム データ ソースを 更新 します。 • AW データベース同期の無効化

コンポーネント（Component）	自動初期化タスク
Cisco Finesse	• CTI サーバ設定を設定します。 • AW データベースへの接続を設定します。 • Finesse 管理の **理由** ガジェットを無効にします。

Packaged CCE 2000 エージェント展開のシステム インベントリ

（注） システム インベントリには、IPv4 アドレスのみが表示されます。

システム インベントリには、仮想マシン ホスト（ESXi サーバ）、サイド A の仮想マシン（VM）、サイド B の VM、外部マシン、ゲートウェイ、および Cisco Virtualized Voice Browser（VVB）を含む、環境内のマシンが視覚的に表示されます。Packaged CCE 導入への変更が完了すると、システム インベントリにアクセスできます。

システム インベントリにアクセスするには、**Unified CCE 管理** > **システム** > **展開**に移動します。

導入タイプを選択または変更したとき、および定期的なシステム スキャンの後で、システム インベントリの内容が更新されます。システム スキャンで Packaged CCE の要件に準拠しない VM が検出されると、[導入の設定（Configure your deployment）] ポップアップ ウィンドウが自動的に開き、エラーの詳細が示されます。エラーを修正し、[導入の設定（Configure your deployment）] ポップアップ ウィンドウにすべての情報を入力すると、システム インベントリに再度アクセスできます。

Packaged CCE の要件の詳細については、**サーバ ステータス** ポップアップ ウィンドウ、Packaged CCE 2000 エージェント展開のサーバ ステータス ルールの監視 （19 ページ）を参照してください。

表 *1:* システム インベントリのレイアウトとアクション

項目	注記	アクション
検証（Validate）	システム スキャンが検証ルールのエラーまたは警告を検出した場合は、エラーを修正し、**検証** をクリックして即時スキャンを実行し、問題が修正されたことを確認します。	[検証（Validate）] をクリックします。

項目	注記	アクション
サイド A（Side A）	このパネルは、サイド A のすべての VM を示します。	

項目	注記	アクション
		システムインベントリには、以下のVMの読み取り専用情報が表示されます。 • **Unified CCE Rogger** • **Unified CCE PG** • **Unified CM サブスクライバ 1** 以下の VM は編集可能です。VM の [鉛筆（pencil）] アイコンをクリックして、次のフィールドを編集します。 （注） Packaged CCE コンポーネントのパスワードを変更した場合は、システム インベントリ内の対応する VM のパスワードを更新する必要があります。 • [Unified CCE AW-HDS-DDS]：診断フレームワーク サービスのドメイン、ユーザ名、およびパスワード。 • [Unified CM パブリッシャ（Unified CM Publisher]：AXL ユーザ名およびパスワード。これらは Unified CM パブリッシャに接続するためのクレデンシャルです。 • [CUIC-LD-IdS パブリッシャ（CUIC-LD-IdS Publisher）]：Unified Intelligence Center Administration のユーザ名とパスワード。Identity Service Administration のユーザ名とパスワードです。 • **Unified CVP サーバ**：Unified CVP サーバ Windows クレデンシャル。 • **Finesse プライマリ**：Cisco Finesse 管理のユーザ名およびパスワード。 VM の [矢印（arrow）] アイコンをクリックして、次の VM の管理ツールを起動できます。 • **CUIC-LD-IdS パブリッシャ** • **Unified CM パブリッシャ** さまざまなコンポーネント設定の完全同期または差分同期を実行することができます。データ同期をサポートするマシンの詳細については、デバイ

項目	注記	アクション
		ス同期喪失アラートを参照してください。

項目	注記	アクション
サイド B（Side B）	このパネルは、サイド B のすべての VM を示します。	

項目	注記	アクション
		システム インベントリには、以下の VM の読み取り専用情報が表示されます。 • **Unified CCE Rogger** • **Unified CCE PG** • **Unified CCE AW-HDS-DDS** • **Unified CM サブスクライバ 2** • **CUIC-LD-IdS サブスクライバ** • **Finesse セカンダリ** • ECE データ サーバ 以下の VM は編集可能です。VM の [鉛筆（pencil）] アイコンをクリックして、次のフィールドを編集します。 （注） Packaged CCE コンポーネントのパスワードを変更した場合は、システム インベントリ内の対応する VM のパスワードを更新する必要があります。 • **Unified CVP**：Unified CVP サーバ Windows クレデンシャル。 • **Unified CVP レポート** ：Cisco Unified CVP レポート サーバ Windows クレデンシャル。 CVP レポート サーバ VM を再イメージまたは再インストールした場合は、CVP レポート サーバを初期化する必要があります。 CVP レポート サーバの を初期化するには、初期化アイコンをクリックして、**はい**をクリックして確定します。 （注） 初期化によって、既存のコール サーバの関連付けおよび設定は削除されます。 コール サーバを CVP レポート サーバに再度関連づけるには、 **概要** > **インフラストラクチャ設定** > **デバイス設定** > **デバイス設定**に移動します。 を再設定するには、**概要** > **機能** > に移動します。

項目	注記	アクション
		さまざまなコンポーネントの設定の完全同期または差分同期を実行することができます。データ同期をサポートするマシンの詳細については、デバイス同期喪失アラートを参照してください。

項目	注記	アクション
外部マシン（External Machines）	このセクションでは、展開環境のすべての外部マシンが表示され、以下のいずれかを含む可能性があります。 • HDS • Unified CM パブリッシャ • Unified CM サブスクライバ • SocialMiner • ECE データ サーバ • ECE Web サーバ • サード パーティ マルチチャネル • Unified CVP レポーティング • MediaSense • Unified SIP Proxy • Virtualized Voice Browser • ゲートウェイ （注） Unified CM サブスクライバのマシンは、コンタクト センター専用です。外部 Unified CM パブリッシャを設定すると、Unified CM サブスクライバはシステム インベントリに自動的に追加されます。	

項目	注記	アクション
		外部 HDS と外部 Unified CM サブスクライバが自動検出されます。これらを追加または削除する必要はありません。 外部マシンの追加または更新については、外部マシンの追加と保守を参照してください。 さまざまなコンポーネントの設定の完全同期または差分同期を実行することができます。データ同期をサポートするマシンの詳細については、デバイス同期喪失アラートを参照してください。 （注） Packaged CCE コンポーネントのパスワードを変更した場合は、システム インベントリ内の対応する VM のパスワードを更新する必要があります。 （注） Unified CM パブリッシャを編集する場合は、パブリッシャに関連付けられた Unified CM サブスクライバが自動的に更新されます。システム インベントリから Unified CM サブスクライバを編集することはできません。 **シングル サインオンを有効にするために、外部 HDS とデフォルトの Cisco Identity Service（IdS）を関連付けるには、以下の手順を実行します。** **1.** 外部 HDS の [鉛筆（pencil）] アイコンをクリックします。 **2.** [デフォルト Identity Service（Default Identity Service）] の横にある [検索（Search）] アイコンをクリックします。 **3.** [検索（Search）] フィールドに Cisco IdS のマシン名を入力するか、リストから Cisco IdS を選択します。 **4.** [保存（Save）] をクリックします。 マシン ボックスの [矢印（arrow）] アイコンをクリックして、次の外部マシンの管理ツールを開くことができます。 • **Unified CM パブリッシャ** • **SocialMiner**

項目	注記	アクション
		• **MediaSense**

Packaged CCE 2000 エージェント展開のサーバ ステータス ルールの監視

Packaged CCE 2000 エージェントの展開では、検証ルールを使用するマシンについて、システム インベントリが上記ルールのアラートの合計数を表示します。アラート カウントをクリックして、[サーバ ステータス（Server Status）] ポップアップ ウィンドウを開きます。そのマシンのすべてのルールが一覧表示され、警告とエラーがあることを示します。ルールはカテゴリ別にグループ化されています。

サーバ ステータスのカテゴリ	説明	ルールの例
設定（Configuration）	コンポーネントのインストールと設定に関するルール。 これらのルールは、コンポーネント間の設定の不一致、不明なサービス、不正に設定されたサービスについて問題を識別します。	**Unified CCE Rogger**：パフォーマンスを確保するには、トレース レベルを標準に設定する必要があります。 **Unified CVP**：Communications Manager アドレスを含む CVP の SIP サーバ グループの名前は、Communications Manager クラスタの完全修飾ドメイン名と一致する必要があります。
操作（Operations）	コンポーネントの実行時ステータスのルール。 これらのルールは、到達できない、動作していない、予期した状態にないプロセスとサービスを識別します。	**Unified CCE Rogger**：中央コントローラ エージェント プロセス（ccagent.exe）が両方のPGで稼働していなければなりません。

サーバ ステータスのカテゴリ	説明	ルールの例
システムの状態（System Health）	直前 10 分間について ESXi により報告された、コンポーネントの仮想マシン（VM）の CPU、メモリ、ディスク使用率を監視するメトリック。メモリおよび CPU 使用率は、VM 自体によって報告されたシステム ツールからのものと多少異なる場合があります。VM ホストの場合、これらのメトリックには、データストアのパフォーマンス情報が含まれます。 M5 検証済リファレンス構成または仕様を基にした構成の VM ホストの場合、これらのメトリックには、CPU 予約、CPU オーバーサブスクリプション、メモリ予約、データストア使用率といった情報が含まれます。	**すべて**：ESXi が報告したメモリ使用率：17 % M5 検証済 VM ホストのリファレンス設定または仕様を基にした設定の場合： • 最大 CPU 予約：65% • 最大 CPU オーバー サブスクリプション：200% • 最大メモリ予約：80% • データストア毎の最大ストレージ使用率：80%
VM	コンポーネントの VM の要件。	**すべて**：VMware ツールが最新のものである必要があります
システム検証（System Validation）	Unified CCE データベースおよび設定内容に関するルール。 これらのルールは、展開されたオブジェクトの設定が Packaged Contact Center Enterprise の要件と制限に一致しているかを識別します。 （注） システム検証カテゴリは、サイド A の Unified CCE AW-HDS-DDS のみで利用できます。	**サイド A Unified CCE AW-HDS-DDS**：エージェント デスク設定：Ring No Answer 時間を設定してはなりません。 **Unified CCE AW-HDS-DDS サイド A**： アプリケーション ゲートウェイ **サイド A Unified CCE AW-HDS-DDS**：アプリケーション インスタンス：アプリケーションインスタンスを 1 つだけ定義し、アプリケーション タイプを <その他（Other）> に設定する必要があります。

VM 検証（*VM Validation*）

Packaged CCE の検証: 2000 エージェント導入タイプの検証では、ハードウェアのコンプライアンスおよびシスコ提供の OVA ファイルとの一致を確認するために以下のチェックを実行します。

- ホストの場合：

- BIOS
- CPU コアの最小数
- 最小メモリ
- データストア サイズ

- VM の場合：
  - 仮想 CPU コア数
  - 設定済みネットワーク数
  - 仮想ネットワーク カード ドライバ（Unified CM を除く）
  - VM の電源が入っていること
  - CPU の予約
  - 正確なメモリ
  - 正確なディスク サイズ
  - 正確なディスク数
  - VMWare ツール

Cisco Unified Contact Center Enterprise PG の設定

以下の表は、Packaged CCE 2000 Agent を展開するためのメディア ルーティング周辺機器ゲートウェイ用の設定タスクの概要を示しています。

設定作業
メディア ルーティング ペリフェラル ゲートウェイへの PIM の追加（任意）

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 （22 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 （22 ページ）
- SNMP V1 and V2c のコミュニティ名の設定 （22 ページ）
- SNMP V3 用の SNMP ユーザ名の設定 （23 ページ）
- SNMP トラップの宛先の設定 （24 ページ）
- SNMP Syslog の宛先の設定 （24 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パネルで、 **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 （22 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 （22 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 （22 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 （22 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 トラップの宛先の設定

SNMP v1、SNMP v2c、および SNMP v3 の SNMP トラップの宛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。

トラップの宛先を設定するには、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 （22 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 （22 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** > **トラップの宛先** > **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、トラップの宛先を定義します。

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、新しいトラップの宛先を保存します。

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 の宛先の設定

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

Syslog の宛先を設定するには、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 の宛先** > **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、ロガーを再起動します。

Cisco Unified Customer Voice Portal の設定

Packaged 2000 エージェント展開のための Cisco Unified Customer Voice Portal（CVP）の設定タスクの概要を以下の表に示します。

（注） CVP 設定は、サイトによって異なります。サイト毎にサイド A およびサイド B の設定が同じである必要があります。

設定作業
CA 証明書の詳細については、以下を参照してください。 Unified CVP セキュリティ
自己署名付き証明書の詳細については、以下を参照してください。 Cisco Unified CVP サーバにプリンシパル AW 証明書を追加します。
デフォルト設定を変更するには、以下を参照してください。 コール サーバ サービスの設定
メディア サーバの設定
SNMP の設定 （87 ページ）
ライセンス管理 （90 ページ）

Cisco Unified Communications Manager の設定

以下の表は、Packaged CCE 2000 エージェント導入のための Cisco Unified Communications Manager の設定タスクをまとめたものです。

設定作業
CA および自己署名付き証明書の詳細については、以下を参照してください。 CUCM上の通信のセキュリティ保護

設定作業
完全修飾ドメイン名の設定 （26 ページ）
Cisco Unified Communications Manager グループの設定 （26 ページ）
会議ブリッジの設定 （27 ページ）
メディア ターミネーション ポイントの設定 （28 ページ）
Unified CM と IOS ゲートウェイでのトランスコーダの設定 （28 ページ）
メディア リソース グループの設定 （29 ページ）
メディア リソース グループ リストの設定および関連付け （30 ページ）
CTI ルート ポイントの設定 （30 ページ）
ロケーション ベースのコール アドミッション制御のためのイングレス ゲートウェイの設定 （31 ページ）
ルート グループの設定 （31 ページ）
Unified CM での SIP プロファイルの追加 （33 ページ）
トランクの設定 （33 ページ）
サービスのアクティブ化 （34 ページ）

完全修飾ドメイン名の設定

手順

ステップ 1 Cisco Unified Communications Manager を開き、ログインします。

ステップ 2 **[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** に移動します。

ステップ 3 **[クラスタ全体のドメイン設定パラメータ（Clusterwide Domain Configuration）] > [クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）]** にクラスタの完全修飾ドメイン名を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

Cisco Unified Communications Manager グループの設定

Cisco Unified Communications Manager を Unified Communications Manager グループに追加するには、以下の手順を実行します。

手順

ステップ 1 [ナビゲーション（Navigation）] メニューから [Cisco Unified CM Administrator] を選択し、[移動（Go）] をクリックします。

ステップ 2 [システム（System）] > [Cisco Unified CM グループ（Cisco Unified CM Group）] を選択します。

ステップ 3 [検索（Find）] をクリックします。[デフォルト（Default）] をクリックします。

ステップ 4 2 つのサブスクライバを [使用可能（Available）] パネルから [選択済み（Selected）] パネルに移動します。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 [リセット（Reset）] をクリックします。

ステップ 7 **デバイス リセット** ウィンドウで **リセット** 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。

会議ブリッジの設定

この手順は、配置の各ゲートウェイに対して実行します。

手順

ステップ 1 **[メディア リソース（Media Resources）]** > **[会議ブリッジ（Conference bridge）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [Cisco IOS 会議ブリッジ（Cisco IOS Conference Bridge）] の [会議ブリッジ タイプ（Conference Bridge Type）] を選択します。

ステップ 4 [会議ブリッジ名（Conference Bridge name）] フィールドに、ゲートウェイ上の設定と一致する会議ブリッジ名の固有識別子を入力します。

例では、[gw70conf] です。

```
# 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
```

ステップ 5 [デバイス プール（Device Pool）] を選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [設定の適用（Apply Config）] をクリックします。

メディア ターミネーション ポイントの設定

この手順は、配置の各ゲートウェイに対して実行します。

手順

ステップ 1 **[メディア リソース（Media Resources）] > [メディア ターミネーション ポイント（Media Termination Point）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [メディア ターミネーション ポイント名（Media Termination Point Name）] フィールドに、ゲートウェイ上の設定と一致するメディア ターミネーションの固有識別子を入力します。

例では、[gw70mtp] です。

```
# 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
```

ステップ 4 [デバイス プール（Device Pool）] を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 [設定の適用（Apply Config）] をクリックします。

Unified CM と IOS ゲートウェイでのトランスコーダの設定

トランスコーダは、ストリームを G.711 コーデックから G.729 コーデックに変換するマルチコーデック シナリオで必要です。

Unified Communications Manager とゲートウェイでのトランスコーダ設定の詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html の『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure Transcoders and Media Termination Points」の項を参照してください。

トランスコーダの設定

この手順は、配置の各ゲートウェイに対して実行します。

手順

ステップ 1 Unified Communications Manager Administration で、[メディアリソース（Media Resource）] > [トランスコーダ（Transcoder）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [トランスコーダ タイプ（Transcoder Type）] の場合、[Cisco IOS 拡張メディア ターミネーション ポイント（Cisco IOS Enhanced Media Termination Point）] を選択します。

ステップ 4 [デバイス名（Device Name）] フィールドに、ゲートウェイ上の設定と一致するトランスコーダ名の固有識別子を入力します。

以下の例では、これは gw70xcode となっています。

```
# 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
```

ステップ 5 **デバイス プール** フィールドで、適切なデバイス プールを選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [設定の適用（Apply Config）] をクリックします。

イングレス ゲートウェイでの CPU コール サーバ ダイヤル ピアの設定

イングレス ゲートウェイから Unified CVP へのアウトバウンド ダイヤル ピアの設定では、Unified CVP の IPv4 アドレスをセッション ターゲットとして使用します。

メディア リソース グループの設定

手順

ステップ 1 **[メディア リソース（Media Resources）] > [メディア リソース グループ（Media Resource Group）]** を選択します。

ステップ 2 会議ブリッジ用のメディア リソース グループを追加します。

a) [新規追加（Add New）] をクリックします。
b) 名前を入力します。
c) [使用可能（Available）] リストから、導入内にある入力/VXML の組み合わせのゲートウェイごとに設定された Cisco IOS 会議ブリッジ リソースをすべて選択し、それらをグループに追加します。
d) **[保存（Save）]** をクリックします。

ステップ 3 メディア ターミネーション ポイント用のメディア リソース グループを追加します。

a) **[新規追加（Add New）]**をクリックします。
b) 名前を入力します。
c) [使用可能（Available）] リストから、設定されたすべてのハードウェア メディア ターミネーション ポイントを選択し、それらをグループに追加します。
d) [保存（Save）] をクリックします。

ステップ 4 トランスコーダ用のメディア リソース グループを追加します。

a) [新規追加（Add New）] をクリックします。

b) 名前を入力します。
c) [使用可能（Available）] リストから、設定されたすべてのトランスコーダを選択し、それらをグループに追加します。
d) [保存（save）] をクリックします。

ステップ 5 **[保存（Save）]** をクリックします。

メディア リソース グループ リストの設定および関連付け

手順

ステップ 1 **[メディア リソース（Media Resources）]** > **[メディア リソース グループ リスト（Media Resource Group List）]** を選択します。
ステップ 2 [新規追加（Add New）] をクリックし、名前を入力します。
ステップ 3 メディア リソース グループ リストを追加し、すべてのメディア リソース グループを関連付けます。**[保存（Save）]** をクリックします。
ステップ 4 **[システム（System）]** > **[デバイス プール（Device Pool）]** を選択します。[検索（Find）] をクリックします。適切なデバイス プールを選択します。
ステップ 5 [メディア リソース グループ リスト（Media Resource Group List）] ドロップダウン リストから、ステップ 2 で追加したメディア リソース グループ リストを選択します。
ステップ 6 **[保存（Save）]** をクリックします。[リセット（Reset）] をクリックします。

CTI ルート ポイントの設定

エージェントが転送と会議に使用するコンピュータ テレフォニー インテグレーション（CTI）ルート ポイントを追加するには、以下の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理で、**[デバイス（Device）]** > **[CTI ルート ポイント（CTI Route Point）]** を選択します。
ステップ 2 [新規追加（Add New）] をクリックします。
ステップ 3 デバイス名（例：**PCCEInternalDNs**）を設定します。
ステップ 4 [デバイスプール（Device Pool）] で [デフォルト（Default）] を選択します。
ステップ 5 リストからメディア リソース グループ リストを選択します。
ステップ 6 **[保存（Save）]** をクリックします。
ステップ 7 回線 [1] をクリックして、このルート ポイントに関連付けられる電話番号を設定します。

この電話番号は、内部ルーティングされるコール用に Packaged CCE で設定された任意の内部ダイヤル番号と一致するようにパターンで指定します。（例えば、転送用や会議用）。

重要 目的のすべての内部ダイヤル番号と一致するほど柔軟で、ダイヤルプランの他の部分に対して定義した他のルートパターン向けのコールが誤って代行受信されることがないほどに十分限定されたパターンを定義します。内部コールには一意のプレフィックスを使用します。例えば、内部ダイヤル番号 1230000 と 1231111 がある場合、CTI ルート ポイントに入力する適切な回線番号は 123XXXX になります。

ステップ 8 **[ユーザ管理（User Management）] > [アプリケーションユーザ（Application User）]** を選択します。

ステップ 9 Packaged CCE の自動初期化中に作成された *pguser* を選択します。

ステップ 10 [使用可能なデバイス（Available Devices）] リストから [CTIルート ポイント（CTI Route Point）] を選択し、[制御するデバイス（Controlled Devices）] のリストに追加します。

ステップ 11 **[保存（Save）]** をクリックします。

ロケーション ベースのコール アドミッション制御のためのイングレス ゲートウェイの設定

ロケーションベースのコール アドミッション制御（CAC）は、Unified CCE 支社コール フローモデル（別名、集中型モデル）で使用されます。これは、すべてのサーバ（Unified CVP、Unified CCE、Unified Communications Manager、および SIP プロキシ サーバ）が 1 つまたは 2 つのデータセンターおよびそれぞれの支社に集中化されることを意味します。

コールの発信元ロケーションとして Unified CVP ではなくイングレス ゲートウェイを使用するように Unified Communications Manager を設定します。この設定により、CAC が発信側エンドポイントと電話機の場所に基づいて適切に調整されます。

重要 Unified Communications Manager のゲートウェイ デバイスとして Unified CVP を定義しないでください。

手順

Cisco Unified CM Administration で、イングレス ゲートウェイをゲートウェイ デバイスとして定義します。デバイスに正しい場所を割り当てます。

ルート グループの設定

ルート グループを作成するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager で、**[コール ルーティング（Call Routing）] > [ルート ハント（Route Hunt）] > [ルート グループ（Route Group）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ルート グループ名を入力します。例えば、**CVP Route Group**。

ステップ 4 [ルート グループに追加（Add to Route Group）] ボタンを使用して、選択されたデバイスとしてすべての CVP トランクを追加します。

ステップ 5 **[保存（Save）]** をクリックします。

ルート リストの設定

ルート グループにルート リストを追加するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager で、**[コール ルーティング（Call Routing）] > [ルート ハント（Route Hunt）] > [ルート リスト（Route List）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ルート リスト名を入力します（例：**CVP Route List**）。

ステップ 4 [Cisco Unified CMグループ（Cisco Unified Communications Manager Group）] を選択します。

ステップ 5 作成したルート グループを追加します。

ステップ 6 **[保存（Save）]** をクリックします。

ルート パターンの設定

ルート リストにルート パターンを追加するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager で、**[コール ルーティング（Call Routing）] > [ルート ハント（Route Hunt）] > [ルート パターン（Route Pattern）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ルート パターンとして「**8881111000XXXX**」を入力します。

ステップ 4 作成したルート リストを選択します。

ステップ 5 すべてのパネルのすべてのデフォルトをそのまま使用します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 強制承認コードに関するメッセージで、**OK** をクリックします。強制承認コードは必要ありません。

Unified CM での SIP プロファイルの追加

このオプションにより、デュアルスタック SIP トランクが IPv4 と IPv6 の両方のメディアを提供できるようになります。この手順は、IPv6 対応導入でのみ実行します。

手順

ステップ 1 Cisco Unified CM の管理で、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックして、SIP プロファイルの名前を入力します。

ステップ 3 SIP プロファイルで [ANATの有効化（Enable ANAT）] チェック ボックスをオンにします。

ステップ 4 変更を保存します。

トランクの設定

2 台の Unified CVP サーバがあり、各サーバを Unified Communications Manager の SIP トランクに関連付ける必要があります。以下の手順では、それぞれが異なる Unified CVP サーバを対象としている SIP トランクを設定する方法を示します。

実際のサイトトポロジでは、代替 SIP トランク プランの使用が必要になる可能性があります。設定された SIP トランクによって両方の Unified CVP サーバが対象となっている限りサポートされます。

手順

ステップ 1 Unified Cisco CM の管理で、[デバイス（Device）] > [トランク（Trunk）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [トランク タイプ（Trunk Type）] ドロップダウン リストから、[SIP トランク（SIP Trunk）] を選択し、[次へ（Next）] をクリックします。

ステップ 4 [デバイス情報（Device Information）] セクションで次の内容を入力します。

a) [デバイス名（Device Name）] フィールドに、SIP トランクの名前を入力します（例えば、**`sipTrunkCVPA`**）。

b) [デバイスプール（Device Pool）] ドロップダウン リストで、顧客が定義したデバイス プールを選択します。

c) リストからメディア リソース グループ リストを選択します。

d) [メディア ターミネーション ポイントが必須（Media Termination Point Required）] チェック ボックスがオフになっていることを確認します。

ステップ 5 [SIP 情報（SIP Information）] セクションにスクロールします。

a) [接続先（Destination）] テーブルの [行 1（Row 1）] に、CVP サーバの IP アドレスを入力します。5060 のデフォルトの宛先ポートを受け入れます。

b) [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] ドロップダウン リストで、[非セキュア SIP トランク プロファイル（Non Secure SIP Trunk Profile）] を選択します。

c) [SIP プロファイル（SIP Profile）] ドロップダウン リストで、[標準 SIP プロファイル（Standard SIP Profile）] を選択します。

d) **DTMF シグナリング メソッド** ドロップダウン リストで、 **RFC 2833**を選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [リセット（Reset）] をクリックします。

ステップ 8 導入内の残りのすべての Unified CVP サーバに対して繰り返します。

Cisco Unified Communications Manager 用のクラスタの設定

手順

ステップ 1 ブラウザで Unified Communications Manager パブリッシャを起動します（http://<CUCM パブリッシャの IP アドレス>）。

ステップ 2 **[システム（System）]** > **[サーバ（Server）]** > **[新規追加（Add New）]** を選択します。

ステップ 3 [サーバの設定（Server Configuration）] ページで、[サーバタイプ（Server Type）] の [CUCM音声/ビデオ（CUCM Voice/Video）] を選択します。**[次へ]** をクリックします。

ステップ 4 [サーバの設定（Server Configuration）] ページで、サブスクライバの 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。

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、以下の手順を実行します。

手順

ステップ 1 `https://<CUCM パブリッシャの IP アドレス>/ccmadmin` で Cisco Unified CM Administration を開きます。

ステップ 2 [ナビゲーション（Navigation）] メニューから [Cisco Unified Serviceability] を選択し、[移動（Go）] をクリックします。

ステップ 3 **[ツール（Tools）]** > **[サービスのアクティベーション（Service Activation）]** を選択します。

ステップ 4 [サーバ（Server）] ドロップダウン リストから、サービスをアクティブ化するサーバを選択し、[移動（Go）] をクリックします。

ステップ 5 パブリッシャの場合、次のサービスがアクティブ化されていることを確認し、[保存（Save）] をクリックします。

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco Tftp
- Cisco Bulk Provisioning Service
- Cisco AXL Web Service
- Cisco Serviceability Reporter
- Cisco CTL Provider
- Cisco Certificate Authority Proxy Function
- Cisco Dialed Number Analyzer Server

ステップ 6 サブスクライバの場合、次のサービスがアクティブ化されていることを確認し、[保存（Save）] をクリックします。

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco AXL Web Service
- Cisco CTL Provider
- Cisco Dialed Number Analyzer Server

Cisco Unified Intelligence Center の設定

この順序に従って、Packaged CCE 2000 エージェント展開のための Cisco Unified Intelligence Center を設定します。

手順	タスク
1	セキュリティ証明書の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.htmlの *Cisco Unified Intelligence Center* ユーザ ガイドを参照してください。
2	自己署名付き証明書の詳細については、以下を参照してください。 AW マシンに IdS 証明書を追加します
3	Unified Intelligence Center 外部 HDS データ ソースの設定 （36 ページ）
4	レポート バンドルのダウンロード （37 ページ）
5	レポート バンドルのインポート （38 ページ）
6	Unified Intelligence Center Administration の設定 （39 ページ）

Unified Intelligence Center 外部 HDS データ ソースの設定

この手順は、外部 HDS が導入に含まれており、より長い保持期間が必要な場合にのみ実行します。

始める前に

データ ソースを設定する前に、外部 HDSデータベースの Unified Intelligence Center SQL ユーザを設定します（4000 エージェント および 12000 エージェントに適用)。詳細については、以下で、『Cisco Packaged Contact Center Enterprise インストールおよびアップグレード ガイド』の「外部 HDS の Unified Intelligence Center SQL ユーザ アカウントの設定」セクションを参照してください https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html

手順

ステップ 1 Cisco Intelligence Center 管理者アカウント（https://< ホスト名 /CUIC パブリッシャの IP アドレス>:8444/cuicui）で Unified Intelligence Center にログインします。

ステップ 2 **設定** > **データ ソース**を選択します。

ステップ 3 左側のパネルで [データソース（Data Sources）] をクリックします。

ステップ 4 **UCCE 履歴** データ ソースを選択します。[編集（Edit）] をクリックします。

a) **データソースのホスト** フィールドで、外部 HDS サーバの IP アドレスを入力します。

b) [ポート（Port）] フィールドに、**1433** と入力します。
c) **データベース名** フィールドに、**{instance}_hds**と入力します。
d) [インスタンス（Instance）] フィールドはブランクのままにします。
e) **タイム ゾーン**を選択します。
f) **データベース ユーザ ID**に、Cisco Unified Intelligence Center SQL サーバのユーザ アカウントに設定したユーザ名を入力します。
g) SQL Server ユーザの**パスワード**を入力して確認します。
h) SQL サーバ インストールの照合順序に基づいて**文字セット**を選択します。
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。

ステップ 5 [セカンダリ（Secondary）] タブをクリックして、Unified CCE Historical データ ソースを設定します。

a) **フェールオーバーを有効にする** チェック ボックスをオンにします。
b) **データ ソースのホスト** フィールドで、2 つ目の外部 HDS サーバの IP アドレスを入力します。
c) [ポート（Port）] フィールドに、**1433** と入力します。
d) **データベース名** フィールドに、**{instance}_hds**と入力します。
e) その他のフィールドを [プライマリ（Primary）] タブと同様に入力します。
f) [テスト接続（Test Connection）] をクリックします。
g) [保存（Save）] をクリックします。

ステップ 6 4000 または 12000 エージェント展開用の **UCCE リアルタイム** データ ソースについても、この手順を繰り返します。

リアルタイム データ ソースの **データベース名** は、**{instance}_hds** となります。

レポート バンドルのダウンロード

次の Cisco Unified Intelligence Center レポートのバンドルは、Cisco.com からダウンロードとして入手できます（https://software.cisco.com/download/type.html?mdfid=282163829&catid=null）。入手できる次のバンドルをすべて表示するには、[Intelligence Center Reports] リンクをクリックしてください。

- リアルタイムおよび履歴移行テンプレート：新しいユーザ向けの導入テンプレート。これらのテンプレートは、全フィールド テンプレートの簡易バージョンで、他のコンタクト センター ソリューションで使用可能なテンプレートに似ています。
- リアルタイムおよび履歴全フィールドテンプレート：データベースのすべてのフィールドのデータを提供するテンプレート。これらのテンプレートは、カスタム レポート テンプレートを作成するためのベースとして特に有用です。
- ライブ データ テンプレート：コンタクト センターのアクティビティの最新のデータを提供するテンプレート。

- リアルタイムおよび履歴アウトバウンド テンプレート：アウトバウンド オプションのアクティビティに関するレポートを作成するテンプレート。展開にアウトバウンドオプションが含まれている場合、このテンプレートをインポートします。
- リアルタイムおよび履歴 Cisco SocialMiner テンプレート：SocialMiner アクティビティを報告するテンプレート。展開に SocialMiner が含まれている場合、このテンプレートをインポートします。
- Cisco Unified Intelligence Center Admin Security テンプレート：Cisco Unified Intelligence Server 監査証跡、許可、テンプレートの所有権に関する報告をするテンプレート。

これらのバンドルのテンプレートの一部は、Cisco Packaged CCE 展開に適用されません。Packaged CCE 導入で使用されるテンプレートの詳細については、https://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html の *Cisco Packaged Contact Center Enterprise* レポート ユーザ ガイド を参照してください。

また、サンプルのカスタム レポート テンプレートは、Cisco DeNet（https://developer.cisco.com/site/reporting/documentation/）で入手可能です。以下のテンプレートが利用できます。

- エンタープライズ チャットおよび電子メール
- Cisco Unified Customer Voice Portal（Unified CVP）

レポート テンプレート バンドルをダウンロードするときには、コンタクト センターに導入されているソフトウェアのバージョンに対応したバンドルを選択してください。

レポート バンドルのインポート

手順

ステップ 1 https://<hostname/CUIC パブリッシャの IP アドレス>: 8444/cuicui で Unified Intelligence Center にログインして、左側ペインの **レポート** をクリックします。

ステップ 2 **新規** > **インポート**をクリックします。
レガシー インターフェイスにリダイレクトされます。

ステップ 3 レポートをインポートするフォルダに移動して、**レポートのインポート**をクリックします。

ステップ 4 **[ファイル名（XMLまたはZIPファイル）（File Name (XML or ZIP file)）]** フィールドで、[参照（Browse）] をクリックします。

ステップ 5 ブラウズし、レポート バンドル zip ファイルを選択して、[開く（Open）] をクリックします。

コンタクト センターに導入されているソフトウェア バージョンに対応するレポート バンドルを選択します。

ステップ 6 ファイルを保存する場所を選択します。

ステップ 7 [インポート（Import）] をクリックします。

ステップ 8 次のいずれかを実行します。

- レポートがまだ作成されていない場合、データ ソースを指定する必要があります。[値リストのデータソース（Data Source for ValueList）] ドロップダウン リストから、使用するデータ ソースを選択します。次に [インポート（Import）] をクリックします。

  （注） 値リストのデータ ソースがレポート定義と同じデータ ソースを使用しない場合のみ、そのデータ ソースを選択する必要があります。LiveData レポートの場合、ReportDefinition のデータ ソースが LiveData ストリーミングであり、ValueList のデータ ソースが UCCE Realtime です。リアルタイム レポートでは、データ ソースが UCCE Realtime です。履歴レポートでは、データ ソースが UCCE Historical です。

- レポートが存在する場合、既存のレポートを置換するかどうかを確認するメッセージが表示されます（置換すると、レポートに関連付けられているレポート定義の変更はすべて上書きされます）。**[はい（Yes）]**、**[すべてはい（Yes to All）]**、**[いいえ（No）]**、または **[すべていいえ（No to All）]** をクリックします。

Unified Intelligence Center Administration の設定

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 [クラスタ設定（Cluster Configuration）]>[レポート設定（Reporting Configuration）] から [Active Directory] タブを設定します。

a) プライマリ Active Directory サーバのホスト アドレスを入力します。
b) [ポート（Port）] のデフォルト値のままにします。
c) [マネージャの識別名（Manager Distinguished Name）] フィールドに情報を入力します。
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、検索するドメインの識別名または組織ユニットを指定します。
f) [ユーザ ID の属性] で、必要なオプションを選択します。
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）]** を選択します。
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。
   - [サービスアビリティの設定の編集（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]** を選択します。
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 ストリング
   - 通知先

Cisco Finesse の設定

以下の手順に従って、Packaged CCE 2000 エージェント展開用の Cisco Finesse を設定します。

手順	タスク
1	CA 証明書の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.htmlの *Cisco Finesse* 管理ガイド を参照してください。
2	自己署名付き証明書の詳細については、以下を参照してください。 Finesse 証明書を AW マシンに追加します
3	ライブ データ レポートのためのコンタクト センター エージェントおよびルーティングの設定 （41 ページ）
4	ライブ データ レポート （41 ページ）

ライブ データ レポートのためのコンタクト センター エージェントおよびルーティングの設定

Finesseデスクトップでライブデータ レポートをテストするには、Unified CCE管理（https://<サイド *A* またはサイド *B* の *Unified CCE AW-HDS-DDS* の *IP* アドレス>/cceadmin）で、以下を設定します。

- エージェント
- スキル グループまたはプレシジョン キュー
- コール タイプ
- ダイヤル番号
- ネットワーク VRU スクリプト
- ルーティング スクリプト

（注） ルーティング スクリプトは、スクリプト エディタに設定します。エディタは、[Unified CCE 管理ツール] から開くことができます。

ライブ データ レポート

Cisco Unified Intelligence Center は、Finesse デスクトップに追加できる Live Data のリアルタイム レポートを提供します。

Finesse へのライブ データ レポートの追加

ここでは、Finesseデスクトップにライブデータ レポートを追加する方法について説明します。実行する手順は、以下の表に示すさまざまな要因に応じて異なります。

手順	使用するケース
デフォルトのデスクトップ レイアウトへの Live Data レポートの追加	新規インストール後、または（デフォルトのデスクトップのレイアウトをカスタマイズしていない場合は）アップグレード後にLive Dataレポートを Finesseデスクトップに追加する場合は、この手順を使用します。
カスタム デスクトップ レイアウトへの Live Data レポートの追加	Finesse デスクトップのレイアウトをカスタマイズしている場合は、この手順を使用します。
チームのレイアウトへの Live Data レポートの追加	特定のチームのみのデスクトップのレイアウトに Live Data レポートを追加する場合は、この手順を使用します。

デフォルト デスクトップ レイアウトへのライブ データ レポートの追加

Finesse デフォルト レイアウト XML には、Finesse デスクトップで Live Data レポート ガジェット用のコメントされた XML コードが含まれています。これらのガジェットは、HTTPS バージョンの Live Data レポート ガジェットと HTTP バージョンの Live Data レポート ガジェットの 2 つのカテゴリーに分類されます。

この手順では、デフォルトのデスクトップ レイアウトに Live Data レポート ガジェットを追加する方法について説明します。Finesse の新規インストール後にこの手順を使用します。Finesse をアップグレードしたものの、カスタム デスクトップ レイアウトがない場合は、[デスクトップ レイアウトの管理（Manage Desktop Layout）]ガジェットで [デフォルト レイアウトに戻す（Restore Default Layout）] をクリックし、この手順に従ってください。テキストの例での改行や空白は、読みやすさのために示されているものであるため、実際のコードには含めないでください。

手順

ステップ 1 **Unified CCE 管理**で、 **デスクトップ** > **リソース**に移動します。

ステップ 2 [デスクトップ レイアウト（Desktop Layout）] タブをクリックします。

ステップ 3 デスクトップのレイアウトに追加する各レポートからコメント文字（<!-- および -->）を削除します。エージェントが Finesse デスクトップ（HTTP または HTTPS）にアクセスするために使用する方法に一致するレポートを選択していることを確認します。

ステップ 4 my-cuic-server を Cisco Unified Intelligence Center サーバの完全修飾ドメイン名と置き換えます。

ステップ 5 任意で、ガジェットの高さを変更します。

例：

Live Data ガジェットの URL で指定されている高さは 310 ピクセルです。高さを変更する場合は、URL の gadgetHeight パラメータを適切な値に変更します。例えば、ガジェットの高さを 400 ピクセルにするには、以下の通りコードを変更し、310 を 400 に置き換えます。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

スクロールバーを含むガジェットの最適な表示を維持するには、ガジェットの高さとして 200 ピクセル以上の値を設定してください。レポートでスクロールバーが不要な場合（1 行だけのレポートなど）は、ガジェットの高さをこれよりも小さい値（100 ピクセルなど）に設定できます。ガジェットの高さを指定しない場合（URL から 310 を削除する場合）、デフォルトで高さは 170 ピクセルに設定されます。

ステップ 6 [保存（save）] をクリックします。

カスタム デスクトップ レイアウトへのライブ レポートの追加

Finesse デフォルト レイアウト XML には、Finesse デスクトップで Live Data レポート ガジェット用のコメントされた XML コードが含まれています。これらのガジェットは、HTTPS バージョンの Live Data レポート ガジェットと HTTP バージョンの Live Data レポート ガジェットの 2 つのカテゴリーに分類されます。

この手順では、カスタム デスクトップのレイアウトへのライブ データ レポート ガジェットの追加方法について説明します。テキストの例での改行や空白は、読みやすさのために示されているものであるため、実際のコードには含めないでください。

手順

ステップ 1 **Unified CCE Administration** では、**デスクトップ** > **リソース**に移動します。

ステップ 2 [デスクトップ レイアウト（Desktop Layout）] タブをクリックします。

ステップ 3 デフォルト レイアウト XML を表示するには、[Finesse Default Layout XML] をクリックします。

ステップ 4 Finesse のデフォルト レイアウト XML から追加するレポートの XML コードをコピーします。

例：

HTTPS 向けのエージェント レポートを追加するには、次の内容をコピーします。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6C8E2100001410000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&
        viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
</gadget>
```

ステップ 5 この XML コードを表示するタブのタグ内に貼り付けます。

例：

エージェント デスクトップの [ホーム（Home）] タブにレポートを追加するには、以下の手順を実行します。

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
              gadgetHeight=310&viewId_1=99E6C8E2100001410000000D80A0006C4&
              filterId_1=agent.id=CL%20teamName&
              viewId_2=9AB7848B10000141000001C50A0006C4&
              filterId_2=agent.id=CL%20teamName
      </gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
```

```
  </tabs>
</layout>
```

ステップ 6 my-cuic-server を Cisco Unified Intelligence Center サーバの完全修飾ドメイン名と置き換えます。

ステップ 7 任意で、ガジェットの高さを変更します。

例：

Live Data ガジェットの URL で指定されている高さは 310 ピクセルです。高さを変更する場合は、URL の gadgetHeight パラメータを目的の値に変更します。例えば、ガジェットの高さを 400 ピクセルにする場合、以下の通りコードを変更します。

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

スクロールバーのあるガジェットが最適に表示されるようにするには、ガジェットの高さとして 200 ピクセル以上の値を設定します。レポートでスクロール バーが不要な場合（1 行だけのレポートなど）は、ガジェットの高さをこれよりも小さい値（100 ピクセルなど）に設定できます。ガジェットの高さを指定しない場合（URL から 310 を削除する場合）、デフォルトで高さは 170 ピクセルに設定されます。

ステップ 8 [保存（save）] をクリックします。

（注） ガジェットを追加したら、Finesse デスクトップにサインインして、適切に表示されることを確認します。多数の行が含まれているレポートを使用する場合、レポートが見やすくなり、スクロールしなくても画面に多くの行が表示されるように、デスクトップへのアクセスに使用するコンピュータ上でガジェットの高さや画面解像度を調整してください。

デスクトップのレイアウトの変更時にサインインしていたエージェントのデスクトップには、サインアウトして再びサインインするまで変更が反映されません。

Cisco Unified Customer Voice Portal Reporting Server の設定

この順序に従って、Packaged CCE 導入用に Cisco Unified Customer Voice Portal レポート サーバを 設定します。

（注） サービス コールバック を使用し、Unified CVP コールおよびアプリケーション レポートを実行するカスタマーには、Unified CVP Reporting VM が必要です。

手順	タスク
1	CVP レポート サーバの CA 証明書の説明は、CVP のコール サーバに似ています。詳細については、Unified CVP セキュリティを参照してください。
2	自己署名の詳細については、以下を参照してください。 CVP レポート サーバ証明書を AW マシンに追加します
3	Cisco Unified Customer Voice Portal レポート テンプレートの取得 （45 ページ）
4	Cisco Unified CVP レポート データのデータ ソースの作成 （45 ページ）
5	Unified Intelligence Center への Unified CVP レポート テンプレートのインポート （47 ページ）

Cisco Unified Customer Voice Portal レポート テンプレートの取得

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

手順

ステップ 1 Unified CVP レポーティング サーバで、[開始（Started）] をクリックします。

ステップ 2 検索ボックスで、**%CVP_HOME%\CVP_Reporting_Templates** を入力して、[入力（Enter）] キーを押します。

ステップ 3 レポートのみを zip フォルダに圧縮して、Unified Intelligence Center 管理を実行するシステムにコピーします。

Cisco Unified CVP レポート データのデータ ソースの作成

データ ソースを作成するには、以下の手順を実行します。

手順

ステップ 1 `https://<ホスト名/ CUIC パブリッシャの IP アドレス>:8444/cuicui` で Unified Intelligence Center にログインします。

ステップ 2 左側のナビゲーション ペインで、**設定** > **データ ソース**を選択します。

ステップ 3 **新規**をクリックして、[新しいデータ ソース] ウィンドウを開きます。

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（Name）]	このデータ ソースの名前を入力します。 レポート作成者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（Description）]	このデータ ソースの説明を入力します。
データ ソース 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。
ホストの設定	
データベースホスト	Unified CVP レポート サーバの IP アドレスまたはホスト名を入力します。
[ポート（Port）]	ポート番号を入力します。通常、ポートは 1526 です。 CVP Reporting Server ファイアウォールで、このポートを開くことが必要になる場合があります（[Window ファイアウォール]>[インバウンド ルール]>[新しいルール]）。
データベース名	Unified CVP Reporting Server 上のレポーティング データベースの名前を入力します。データベース名には `cvp_data` または `callback` を使用できます。
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。
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。 （注） CVP データ ソースのタイム ゾーン設定を CUIC 条で UTC 形式に設定します。
認証の設定	

フィールド	値
データベース ユーザ ID	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。
最大プール サイズ	最大プール サイズを選択します。 値の範囲は 5 ～ 200 です。デフォルトの最大プール サイズの値は 100 で、プライマリとセカンダリの両方のデータ ソース タブで共通です。

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、「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。

Unified Intelligence Center への Unified CVP レポート テンプレートのインポート

レポート（XML）および関連するテンプレート ヘルプ ファイル（ZIP 形式）を CUIC にインポートすることができます。

手順

ステップ 1 `https://<CUIC パブリッシャのホスト名または IP アドレス>:8444/cuic` で Unified Intelligence Center Web アプリケーションを起動します。

ステップ 2 左側のナビゲーション ウィンドウで、**レポート**をクリックします。

ステップ 3 [レポート] ツールバーで、**新規**> **インポート**をクリックします。
レガシー インターフェイスにリダイレクトされます。

ステップ 4 レポートをインポートするフォルダに移動します。

（注） Cisco.com からストック レポート バンドルをインポートする場合は、[レポート] フォルダのレベルに配置する必要があります。

ステップ 5 [レポートのインポート（Import Report）] をクリックします。

ステップ 6 **ファイル名（XML または ZIP ファイル）** フィールドで、**ファイルの選択**をクリックします。

ステップ 7 XML または圧縮レポート ファイルを参照して選択し、[開く] をクリックします。

ステップ 8 **[レポート定義のデータ ソース（Data source for ReportDefinition）]** ドロップダウン リストから、レポート定義で使用されるデータ ソースを選択します。

（注） このフィールドは、インポートするレポートのレポート定義が現在 Unified Intelligence Center で定義されていない場合にのみ表示されます。

ステップ 9 [値リストのデータソース（Data Source for ValueList）] ドロップダウン リストから、レポート定義内で定義されている値リストで使用されるデータ ソースを選択します。

（注） レポート定義と同じデータ ソースを使用しない場合のみ、値リストのデータ ソースを選択する必要があります。リアルタイム ストリーミングのレポート定義については、値リストのデータ ソース選択が必須となります。

ステップ 10 [保存先（Save To）] フィールドで、インポートしたレポート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 11 [インポート（Import）] をクリックします。

（注） 異なるバージョンの Unified Intelligence Center へのレポートのインポートはサポートされていません。ただし、Unified Intelligence Center をアップグレードすると、アップグレード後のバージョンでレポート テンプレートが引き続き機能します。

VVB の設定

Cisco の仮想化音声ブラウザ（VVB）の設定は、サイトによって異なります。サイト内の VVB はすべて同じ設定である必要があります。

仮想化音声ブラウザは、外部マシンとして追加することができます。詳細については、外部マシンの追加を参照してください。

デフォルト設定を変更するには、Cisco Virtualized Voice Browser（VVB）を参照してください。

Cisco IOS Enterprise 音声ゲートウェイの設定

Packaged CCE 導入用の Cisco IOS Enterprise 音声ゲートウェイの設定タスク

タスク
イングレス ゲートウェイおよび VXML ゲートウェイの共通設定 （49 ページ）
イングレス ゲートウェイの設定 （50 ページ）
VXML ゲートウェイの設定 （53 ページ）
イングレス ゲートウェイおよび VXML ゲートウェイの A-law コーデックの設定 （54 ページ）

イングレス ゲートウェイおよび VXML ゲートウェイの設定について

イングレス ゲートウェイおよび VXML ゲートウェイを設定するには、以下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。

いずれのゲートウェイも外部のマシンとして追加することができます。詳細については、外部マシンの追加を参照してください。

（注） すべての設定手順を **enable** > **設定端末** モードで実行します。

イングレス ゲートウェイおよび VXML ゲートウェイの共通設定

```
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 ゲートウェイの設定

手順

ステップ 1 グローバル設定を以下の通り設定します。

```
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 プリファレンスを以下の通り設定します。

```
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以下の通り設定します。

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

ステップ 4 ゲートウェイおよび sip-ua タイマーを以下の通り設定します。

```
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 ダイヤルピアを以下の通り設定します。

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

（注） これは TDM ゲートウェイでのみ必要です。

ステップ 6 スイッチ レッグを以下の通り設定します。

```
#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 CVP, 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 70022 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 CVP, 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）を以下の通り設定します。

（注） この設定セクションは、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 2 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 <gatewaynamemtp>
     associate profile 1 register <gatewaynameconf>
     associate profile 3 register <gatewaynamexcode>

# 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
```

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 # CVPA
     rai target ipv4:###.###.###.### resource-group1 # CVPB
     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 ダイアルピアを以下の通り設定します。

```
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
```

（注） これは、CUBE の場合にのみ必要です。

VXML ゲートウェイの設定

手順

ステップ 1 グローバル設定を以下の通り設定します。

```
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 デフォルトの Unified CVP サービスを以下の通り設定します。

```
#Default Unified 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
     service handoff flash:handoff.tcl
```

ステップ 3 ダイヤルピアを以下の通り設定します。

（注） VXML ゲートウェイの設定時には、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 設定を行います。

```
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

vxml tree memory 500
vxml audioerror
vxml version 2.0
```

ステップ 5 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 6 設定モードを閉じて、Cisco IOS CLI コマンド **call application voice load <service_Name>** を使用して、転送した Unified CVP ファイルを 各 Unified CV サービスについて Cisco IOS メモリに読み込みます。

- call application voice load new-call
- call application voice load CVPSelfService
- call application voice load
- call application voice load cvperror
- call application voice load
- call application voice load

イングレス ゲートウェイおよび VXML ゲートウェイの A-law コーデックの設定

この項の手順は、A-law コーデックを使用する場合にだけ実行してください。

イングレス ゲートウェイの設定

手順

ステップ 1 ダイヤルピアでコーデック設定を行うため、音声クラス コーデック 1 を追加します。

```
voice class codec 1
     codec preference 1 g729r8
     codec preference 2 g711alaw
```

例：

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

ステップ 2 ダイヤルピアを変更し、ダイヤルピアに対しコーデックを明示的に指定します。

```
dial-peer voice 9 voip
     description For Outbound Call for Customer
     destination-pattern <Customer Phone Number Pattern>
     session protocol sipv2
     session target ipv4:<Customer SIP Cloud IP Address>
     session transport tcp
     voice-class sip rel1xx supported "100rel"
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 10 voip
     description ***To CUCM Agent Extension For Outbound***
     destination-pattern <Agent Extension Pattern to CUCM>
     session protocol sipv2
     session target ipv4:<CUCM IP Address>
     voice-class sip rel1xx supported "100rel"
     dtmf-relay rtp-nte
     codec g711alaw
```

VXML ゲートウェイの設定

手順

次のダイヤルピアを変更し、ダイヤルピアに対しコーデックを明示的に指定します。

```
dial-peer voice 919191 voip
     description Unified CVP SIP ringtone dial-peer
```

```
      service ringtone
      incoming called-number 9191T
      voice-class sip rel1xx disable
      dtmf-relay rtp-nte
      codec g711alaw
      no vad

dial-peer voice 929292 voip
      description CVP SIP error dial-peer
      service cvperror
      incoming called-number 9292T
      voice-class sip rel1xx disable
      dtmf-relay rtp-nte
      codec g711alaw
      no vad

dial-peer voice 7777 voip
      description Used for VRU leg #Configure VXML leg where the incoming called
      service bootstrap
      incoming called-number 7777T
      dtmf-relay rtp-nte
      codec g711alaw
      no vad
```

IPv6 を設定する

Packaged CCE の展開用に IPv6 を設定するためのタスク

タスク
VOS ベースのコンタクト センター アプリケーションの IPv6 のセットアップ （57 ページ）
IPv6 が有効化された展開の NAT64 の設定 （58 ページ）
Unified CVP コール サーバでの IPv6 の設定 （60 ページ）
ゲートウェイでの IPv6 サポートの設定 （61 ページ）
Unified Communications Manager での IPv6 の設定 （62 ページ）

IPv6 設定

Packaged CCE は、エージェントおよびスーパーバイザの Finesse デスクトップと電話で IPv6 接続をサポートできます。IPv6 対応の導入では、使用するエンドポイントをすべて IPv6 にするか、または IPv4 と IPV6 エンドポイントを混合することができます。これらのエンドポイントと通信するサーバは、IPv4 接続と IPv6 接続の両方を受け入れることができます。サーバ間の通信では、引き続き IPv4 接続が使用されます。

この章では、IPv6 対応の導入で実行する設定手順について説明します。

VOS ベースのコンタクト センター アプリケーションの IPv6 のセットアップ

デフォルトでは、Unified Communications Manager、Finesse、および Unified Intelligence Center では IPv4 のみが有効となっています。

これらのアプリケーションで IPv6 を有効にする場合は、パブリッシャ/プライマリ ノードとサブスクライバ/セカンダリ ノードの両方で、アプリケーションに対して IPv6 を有効にする必要があります。

Cisco Unified Operating System Administration または CLI を使用して IPv6 を有効にできます。

Packaged CCE 導入での IPv6 のサポートの詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html の *Cisco Packaged Contact Center Enterprise* ソリューション設計ガイド を参照してください。

Cisco Unified Operating System Administration を使用した IPv6 の設定

Cisco Unified Operating System Administration を使用して IPv6 を設定するには、プライマリとセカンダリの VOS サーバで以下の手順を実行します。

手順

ステップ 1 パブリッシャ/プライマリ ノードで Cisco Unified Operating System Administration にサインインします。

- Unified Communications Manager および Unified Intelligence Center：`https://<パブリッシャまたはプライマリ ノードのホスト名または IP アドレス>/cmplatform`
- Finesse：`https://プライマリ ノードの FQDN:8443/cmplatform`

ステップ 2 **[設定（Settings）] > [IP] > [イーサネットIPv6（Ethernet IPv6）]** を選択します。

ステップ 3 [IPv6を有効にする（Enable IPv6）] チェック ボックスをオンにします。

ステップ 4 [IPv6アドレス（IPv6 Address）]、[プレフィックスの長さ（Prefix Length）]、および [デフォルトゲートウェイ（Default gateway）] の各フィールドに値を入力します。

ステップ 5 **[Update with Reboot（リブートを使用した更新）]** チェック ボックスをオンにします。

ステップ 6 **[保存（Save）]**をクリックします。
サーバが再起動します。

ステップ 7 サブスクライバ/セカンダリ ノードに対してこの手順を繰り返します。

CLI を使用した VOS ベース アプリケーションの IPv6 のセットアップ

CLI を使用して IPv6 を設定するには、プライマリ VOS サーバとセカンダリ VOS サーバの両方で以下の手順を実行します。

手順

ステップ 1 VOS サーバで CLI にアクセスします。

ステップ 2 IPv6 を有効または無効にするには、以下の通り入力します。
set network ipv6 service {enable | disable}

ステップ 3 次のコマンドを実行して、IPv6 アドレスとプレフィックス長を設定します。
set network ipv6 static_address *addr mask*

例：

```
set network ipv6 static_address 2001:db8:2::a 64
```

ステップ 4 デフォルト ゲートウェイを設定します。
set network ipv6 gateway *addr*

ステップ 5 システムを再起動し、変更を有効にします。
utils system restart

ステップ 6 IPv6 設定を表示するには、以下の通り入力します。
show network ipv6 settings

IPv6 が有効化された展開の NAT64 の設定

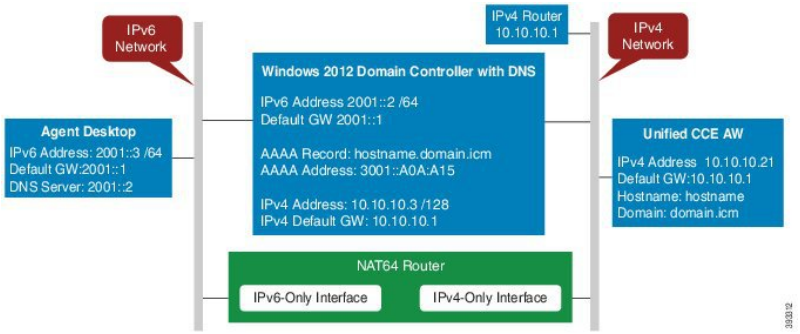
NAT64 により、IPv6 ネットワークと IPv4 ネットワーク間の通信が可能になります。IPv6 対応の導入では、IPv6 ネットワークのスーパーバイザが、IPv4 ネットワーク上の Unified CCE Administration Web ツールにアクセスできるように、NAT64 を設定する必要があります。

ステートフルまたはステートレスのいずれかの NAT64 を使用できます。ご使用の導入にとって最適な変換タイプについては、表 2 を参照してください。ステートレスとステートフルの NAT64 の比較： https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

（注） NAT64 は M トレイン IOS ではサポートされません。T トレインが必要です。

詳細については、http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Packaged_CCEhttps://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.htmlで Packaged Contact Center Enterprise の互換性マトリックスを参照してください。

次に示すネットワーク構成図とインターフェイス設定の例は、IPv6 ネットワークと IPv4 ネットワーク間でのステートフル NAT64 への変換を示します。




```
interface GigabitEthernet0/0
description ipv4-only interface
 ip address 10.10.10.81 255.255.255.128
 duplex auto
 speed auto
 nat64 enable
 no mop enabled

interface GigabitEthernet0/1
description ipv6-only interface
 no ip address
 duplex auto
 speed auto
 nat64 enable
 ipv6 address 2001::1/64
 ipv6 enable

ipv6 unicast-routing
ipv6 cef
!
nat64 prefix stateful 3001::/96
nat64 v4 pool POOL1 10.10.10.129 10.10.10.250
nat64 v6v4 list V6ACL1 pool POOL1 overload
ipv6 router rip RIPv6
!
ipv6 router rip RIP

!
ipv6 access-list V6ACL1
 permit ipv6 2001::/64 any
```

IPv6 の DNS の設定

FQDN が Unified CCE 管理にアクセスする要件を満たすため、Unified CCE AW-HDS-DDS サーバおよび任意の外部 HDS サーバの前方参照 AAAA レコードが DNS に作成されている必要があります。

この手順のステップは、Windows DNS サーバを対象としています。

手順

ステップ 1 Windows で [管理ツール（Administrative Tools）] > [DNS] を選択します。DNS マネージャが起動されます。

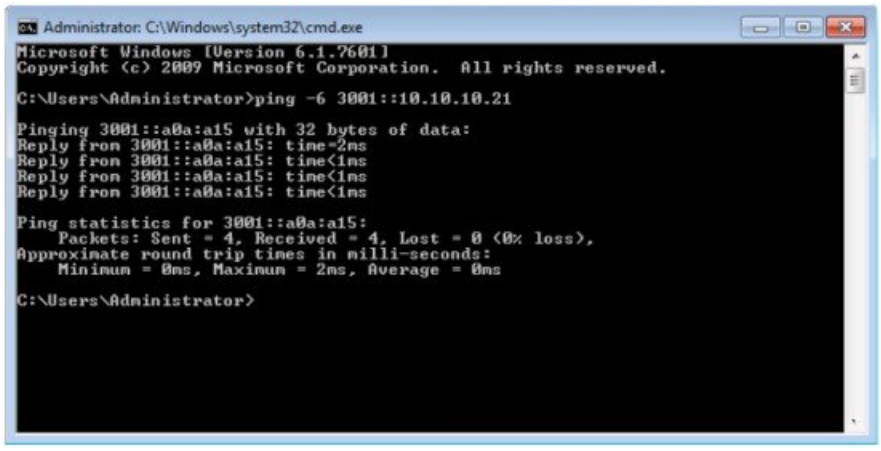
ステップ 2 [前方参照ゾーン（Forward lookup zone）] で、導入のドメイン名に移動します。

ステップ 3 ドメイン名を右クリックし、[新しいホスト（A または AAAA）（New Host (A or AAAA)）] を選択します。

ステップ 4 [新しいホスト] ダイアログ ボックスで、Unified CCE データ サーバおよび任意の外部 AW-HDS-DDS サーバのコンピュータ名および IP アドレスを入力します。[ホストの追加（Add Host）] をクリックします。

DNS エントリの *IPv4* アドレスの *IPv6* 変換の決定

AAAA DNS レコードに必要な IPv6 アドレスを判別するには、Windows マシンで混合表記を使用して ping コマンドを実行します。「ping -6」と入力し、その後 IPv6 Nat64 プレフィックス、2 つのコロン、IPv4 アドレスの順に入力します。



ping に対する応答では、IPv4 アドレスが 16 進数の文字列に変換されます。静的 AAAA レコードでこのアドレスを使用します。

（注） オプションで、静的 DNS エントリの代わりに DNS64 を使用できます。DNS64 を使用すると、A リソース レコードからの AAAA リソース レコードを合成することで、IPv6 ネットワークと IPv4 ネットワーク間での変換が促進されます。

『*NAT64 Technology: Connecting IPv6 and IPv4 Networks*』ホワイトペーパーに、DNS64 の概要と、DNS64 を IPv6 と共に使用する方法が記載されています（https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html）。

Unified CVP コール サーバでの IPv6 の設定

IPv6 対応導入では、IPv6 アドレスをご使用の Unified CVP コール サーバの既存のネットワーク インターフェイスに追加する必要があります。

この手順は、IPv6 対応導入を使用している場合にだけ実行します。

手順

ステップ 1 Unified CVP コール サーバで **[コントロールパネル（Control Panel）]** > **[ネットワークと共有（Network and Sharing）]** を選択します。

ステップ 2 [イーサネット（Ethernet）] をクリックします。

ステップ 3 [イーサネットのステータス（Ethernet Status）] ウィンドウで [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)）] 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 5 [次のIPv6アドレスを使う（Use the following IPv6 address）] オプション ボタンをオンにします。

ステップ 6 [IPv6アドレス（IPv6 address）]、[サブネット プレフィックスの長さ（Subnet prefix length）]、および [デフォルトゲートウェイ（Default gateway）] の各フィールドに値を入力します。

ステップ 7 プロンプトが表示されたら、[OK] をクリックして Windows を再起動します。

ゲートウェイでの IPv6 サポートの設定

IPv6 対応導入では、IPv6 アドレッシングを有効にするようにイングレス ゲートウェイと VXML ゲートウェイを設定する必要があります。

インターフェイスでの IPv6 プロトコル スタックのサポートの設定

この手順は、イングレス ゲートウェイと VXML ゲートウェイの両方に適用されます。

手順

ゲートウェイで次の設定を行います。

```
>Enable
>configure terminal
>interface type number
>ipv6 address{ ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}
>ipv6 enable
```

イングレス ゲートウェイでの ANAT の有効化

手順

ゲートウェイで次の設定を行います。

```
>conf t
>voice service voip
>SIP
```

```
>ANAT
>bind control source-interface GigabitEthernet0/2
>bind media source-interface GigabitEthernet0/2
```

イングレス ゲートウェイでのデュアル スタックの有効化

手順

ゲートウェイで次の設定を行います。

```
>conf t
>sip-ua
>protocol mode dual-stack preference ipv6
```

Unified Communications Manager での IPv6 の設定

IPv6 対応環境では、この項の手順を実行して Unified Communications Manager で IPv6 を設定する必要があります。

Unified CM Administration でのクラスタ全体の設定

クラスタ全体でのメディアおよびシグナリング用のアドレッシング モード設定として IPv6 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 各 Unified Communications Manager サーバのクラスタ全体の IPv6 設定を構成するには、**Cisco Unified CM 管理**で、**システム** > **エンタープライズ パラメータ** > **IPv6 設定モード** を選択します。

ステップ 2 **IPv6を有効にする** ドロップダウンリストで、**はい**を選択します。

ステップ 3 [メディア用のIPアドレッシングモード設定（IP Addressing Mode Preference for Media）] ドロップダウンリストから [IPv6] を選択します。

ステップ 4 [シグナリング用のIPアドレッシングモード設定（IP Addressing Mode Preference for Signaling）] ドロップダウンリストから [IPv6] を選択します。

ステップ 5 [電話の自動設定を許可（Allow Auto-configuration for Phones）] ドロップダウンリストから [オフ（Off）] を選択します。

ステップ 6 変更を保存します。

トランスコーディング

IPv6 対応環境では、次のシナリオでトランスコーダが必要です。

- IPv6 エンドポイントにログインしているエージェントが、IPv4 エンドポイントにログインしているエージェントとの間で転送を送受信する必要がある。
- IPv6 エンドポイントにログインしているエージェントが、セルフ サービスのために VXML ゲートウェイに接続する必要がある。

Unified Communications Manager での共通デバイス設定プロファイルの追加

IPv6 対応環境では、IPv4 デバイスと IPv6 デバイスの両方を使用できます。

Unified Communications Manager で IPv4、IPv6、またはデュアル スタックの共通デバイス設定プロファイルを追加するには、以下の手順を実行します。

手順

ステップ 1 **Cisco Unified CM 管理**で、**デバイス** > **デバイスの設定** > **共通デバイス設定**を選択します。

ステップ 2 [新規追加（Add New）] をクリックして、新しい共通デバイス設定プロファイルの名前を入力します。

ステップ 3 [IPアドレッシングモード（IP Addressing Mode）] ドロップダウンリストから次の操作を実行します。

- Unified Communications Manager で IPv6 共通デバイス設定プロファイルを追加するには、[IPv6のみ（IPv6 only）] を選択します。
- Unified Communications Manager で IPv4 共通デバイス設定プロファイルを追加するには、[IPv4のみ（IPv4 only）] を選択します。
- Unified Communications Manager でデュアル スタック共通デバイス設定プロファイルを追加するには、[IPv4とIPv6（IPv4 and IPv6）] を選択します。[シグナリング用のIPアドレッシングモード設定（IP Addressing Mode Preference for Signaling）] ドロップダウンリストから [IPv4] を選択します。

ステップ 4 変更を保存します。

ゲートウェイ トランクへの共通デバイス設定プロファイルの関連付け

ゲートウェイ トランクに共通デバイス設定プロファイルを関連付けるには、以下の手順を実行します。この手順は、イングレス ゲートウェイに適用されます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunk）]** を選択します。

ステップ 2 [検索（Find）] をクリックします。
表示するトランク プロファイルを選択します。

ステップ 3 [共通デバイス設定（Common Device Configuration）] ドロップダウン リストから次の操作を実行します。

- ゲートウェイ トランクに IPv6 共通デバイス設定プロファイルを関連付けるには、IPv6 共通デバイス設定プロファイルを選択します。
- ゲートウェイ トランクに IPv4 共通デバイス設定プロファイルを関連付けるには、IPv4 共通デバイス設定プロファイルを選択します。

（注） Unified CM ゲートウェイ トランクでは IPv4 または IPv6 トランクだけがサポートされています。Unified CM ゲートウェイ トランクにデュアル スタック共通デバイス設定プロファイルを関連付けることはできません。

ステップ 4 [接続先アドレスIPv6（Destination Address IPv6）] フィールドに IPv6 アドレスを入力します。

（注） Unified CM からゲートウェイへのトランクでは、標準 SIP プロファイルだけがサポートされており、ANAT 対応デュアルスタック SIP トランクはサポートされていません。

ステップ 5 変更を保存します。

IPv4 または IPv6 電話への共通デバイス設定プロファイルの関連付け

手順

ステップ 1 [Cisco Unified CMの管理（Cisco Unified CM Administration）] から、**[デバイス（Device）] > [電話（Phone）]**を選択します。

ステップ 2 [検索（Find）] をクリックします。
表示するトランク プロファイルを選択します。

ステップ 3 [共通デバイス設定（Common Device Configuration）] ドロップダウン リストから、IPv6 共通デバイス設定プロファイルを選択します。

- IPv6 電話に IPv6 共通デバイス設定プロファイルを関連付けるには、IPv6 共通デバイス設定プロファイルを選択します。
- IPv4 電話に IPv4 共通デバイス設定プロファイルを関連付けるには、IPv4 共通デバイス設定プロファイルを選択します。

ステップ 4 変更を保存します。

Unified CM での SIP プロファイルの関連付け

IPv6 対応の導入では、Unified CVP に対して設定したトランクに SIP プロファイルを関連付ける必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。

ステップ 2 [検索（Find）] をクリックします。表示するトランク プロファイルを選択します。

ステップ 3 [SIPプロファイル（SIP Profile）] ドロップダウン リストから、作成した SIP プロファイルを選択します。

（注） SIP プロファイルの作成方法の詳細については、以下を参照してください。

Cisco のパッケージ化されたコンタクト センターの [エンタープライズ管理とコンフィギュレーション ガイド ()] にhttps://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html、SIP プロファイルを統合 CM セクションに追加します。

ステップ 4 変更を保存します。

SIP トランクへのデュアル スタック共通デバイス設定プロファイルの関連付け

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。

ステップ 2 [検索（Find）] をクリックします。表示するトランク プロファイルを選択します。

ステップ 3 [共通デバイス設定（Common Device Configuration）] ドロップダウン リストから、デュアル スタック共通デバイス設定プロファイルを選択します。

（注） デュアル スタック共通デバイス設定プロファイルの追加方法の詳細については、Unified Communications Manager での共通デバイス設定プロファイルの追加 （63 ページ）を参照してください。

ステップ 4 変更を保存します。

Packaged CCE 4000 エージェント展開

Packaged CCE 4000 エージェント展開のコンポーネントを設定するには、以下の手順を実行します。

手順	タスク
1	CCE コンポーネントの設定 （66 ページ）

手順	タスク
2	Cisco Unified Customer Voice Portal の設定 （87 ページ）
3	外部メディア サーバの場合、メディア サーバの設定
4	Cisco Unified Communications Manager の設定（90 ページ）
5	Cisco Unified Intelligence Center の設定 （96 ページ）
6	Cisco Finesse の設定 （97 ページ）
7	ライブ データの設定 （102 ページ）
8	Cisco Identity Serviceの設定 （105 ページ）
9	Cisco Unified Customer Voice Portal Reporting Server の設定 （44 ページ） （任意）
10	VVB の設定 （48 ページ） （任意）
11	Cisco IOS Enterprise 音声ゲートウェイの設定（49 ページ）
12	IPv6 を設定する （56 ページ）
13	エンタープライズ チャットおよび電子メール（ECE）の設定（オプション） 電子メールおよびチャット

CCE コンポーネントの設定

Packaged CCE 4000 エージェント展開のコンポーネントを設定するには、以下の手順を実行します。

手順	タスク
1	Roggerの設定 （67 ページ）
2	AW-HDS-DDS の設定 （72 ページ）
3	Unified CCE サービスの開始 （72 ページ）

手順	タスク
4	PG VM がインストールされている場合は、すべての PG VM に対してUnified CCE インスタンスの追加 （82 ページ）
5	Packaged CCE の展開タイプの設定 （76 ページ）
6	Cisco Unified Contact Center Enterprise PG の設定 （82 ページ）
7	Configuration Managerを使用した設定については、以下を参照してください。 PCCE 4000 または 12000 でサポートされるツール
8	CA 証明書の詳細については、以下を参照してください。 AW マシンに CA 署名付き証明書を生成してインポートする
9	自己署名付き証明書の詳細については、以下を参照してください。 AWマシンで自己署名証明書を生成してインポートする

Roggerの設定

Packaged CCE 4000 エージェント展開の Rogger を設定するには、以下の手順を実行します。

手順	タスク
1	CCE コンポーネント用 SQL Server の設定 （2 ページ）
2	組織ユニットの設定 （3 ページ）
3	Unified CCE インスタンスの追加 （82 ページ）
4	ロガー データベースの作成 （68 ページ）
5	アウトバウンド オプションを使用するには、以下を参照してください。 アウトバウンド オプション データベースの作成 （69 ページ）
6	ロガー コンポーネントのインスタンスへの追加 （69 ページ）
7	ロガー コンポーネントのインスタンスへの追加 （71 ページ）

手順	タスク
8	ICM データベース ルックアップの設定 （119 ページ） （任意）
9	Cisco SNMP の設定 （21 ページ） （任意）

ロガー データベースの作成

サイド Aおよび サイド B Rogger VMでこの手順を実行します。

手順

ステップ 1 ICMDBA ツールを開き、表示される警告のいずれにも **はい** をクリックします。

ステップ 2 デスクトップの Unified CCE ツール フォルダで **サーバ > インスタンス** に移動します。

ステップ 3 インスタンス名を右クリックして、**作成** を選択してロガー データベースを作成します。

ステップ 4 [コンポーネントの選択] ダイアログ ボックスで、処理するロガーを選択します（ロガー A またはロガー B）。[OK] をクリックします。

ステップ 5 要求された場合 「SQL Server が適切に設定されていません。今すぐ設定しますか？」には、**はい**をクリックして確定します。

ステップ 6 [設定] ページの SQL Server 設定ペインの **メモリ（MB）および リカバリ間隔**をオンにします。[OK] をクリックします。

ステップ 7 [サーバの停止] ページで、**はい** をクリックしてサービスを停止します。

ステップ 8 [ロガータイプの選択]ダイアログボックスで、**エンタープライズ** を選択します。**OK**をクリックして、[データベースの作成] ダイアログ ボックスを開きます。

ステップ 9 ロガーのデータベースを作成し、以下の通りログを作成します。

a) [DB タイプ]フィールドで、サイド A または B を選択します。
b) [地域（region）] フィールドで、地域を選択します。
c) [データベースの作成] ダイアログ ボックスで、**追加** をクリックして [デバイスの追加] ダイアログ ボックスを開きます。
d) **データ**をクリックします
e) データベースを作成するドライブ (例えば、E ドライブ) を選択します。
f) **サイズ** フィールドで、デフォルト（1.4 GB、かなり最小サイズ）を選択するか、データベース サイズ決定ツールを使用して、導入に適した値を計算するかを検討します。値を計算する場合は、計算結果をここに入力します。
g) **OK** をクリックして、[データベースの作成] ダイアログ ボックスに戻ります。
h) 再度 **追加** をクリックします。
i) [デバイスの追加] ダイアログ ボックスで、**ログ**をクリックします。
j) データベースを作成したドライブを選択します。
k) **サイズ** フィールドでは、デフォルト設定を選択するか、独自の展開に沿った適切なサイズの値がある場合は、その値を入力します。
l) **OK** をクリックして、[データベースの作成] ダイアログ ボックスに戻ります。

ステップ 10 [データベースの作成] ダイアログ ボックスで、**作成する**をクリックして、**スタート**をクリックします。

ステップ 11 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。

アウトバウンド オプション データベースの作成

アウトバウンド オプションでは、ロガー 上で独自の SQL データベースを使用します。サイド A のロガーのみで、以下の手順を実行します。

この手順を完了したら、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html の *Unified Contact Center Enterprise* アウトバウンド オプション ガイド を参照してください。

手順

ステップ 1 ICMDBA ツールを開き、いずれの警告にも **はい** をクリックします。

ステップ 2 **サーバ** > **<ロガー サーバ>** > **インスタンス** > **<Unified CCE インスタンス>** > **ロガー A**に移動します。[インスタンス名] を右クリックして、**データベース** > **作成**を選択します。

ステップ 3 [サーバの停止] メッセージで、**はい** をクリックしてサービスを停止します。

ステップ 4 [データベースの作成] ダイアログ ボックスで、**追加** をクリックして [デバイスの追加] ダイアログ ボックスを開きます。

ステップ 5 **データ** をクリックして、データベースを作成するドライブ （例えば、E ドライブ）を選択します。DB サイズは、デフォルト値のままにして、**OK** をクリックして、[データベースの作成] ダイアログ ボックスに戻ります。

ステップ 6 [デバイスの追加] ダイアログ ボックスで、**ログ**をクリックします。使用するドライブを選択します。ログ サイズはデフォルト値のままにして、**OK** をクリックして [データベースの作成] ダイアログ ボックスに戻ります。

ステップ 7 [データベースの作成] ダイアログ ボックスで、**作成する**をクリックして、**スタート**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。

ロガー コンポーネントのインスタンスへの追加

サイド A とサイド B のロガーでこの手順を実行します。

手順

ステップ 1 Web セットアップ ツールを開きます。

ステップ 2 **コンポーネント管理** > **ロガー**を選択します。**追加**をクリックして、インスタンスを選択します。

ステップ 3 [導入（Deployment）]ページで、ロガー（AまたはB）を選択します。**デュプレックス**をクリックして、**次へ**をクリックします。

ステップ 4 [セントラル コントローラの接続] ページで、**ルータ プライベート インターフェイス** および **ロガー 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ます。**次へ**をクリックします。

ステップ 5 確認 **データのレプリケーションの履歴および詳細を有効にする**をオンにします。

ステップ 6 [その他のオプション] のページで、 **データベースの消去設定手順の表示**をクリックします。

ステップ 7 、**アウトバウンド オプションを有効にする** チェック ボックスをクリックします。

（注） このロガーが Rogger サーバに追加されている場合、パブリック ネットワーク インターフェイス カード（IP ベースの優先順位付け用）に 2 つの IP アドレスが設定されている場合、パブリック イーサネット カードの [この接続のアドレスを DNS に登録する] をオフにします。また、DNS サーバに、通常の優先順位の IP アドレスにマップされるサーバのホスト名に対応する A-レコード エントリが 1 つのみ存在することを確認します。これは、キャンペーンマネージャのプロセス、および Logger サービスの一部として実行されているレプリケーションで、クライアント接続用の適切なインターフェイス IP アドレスをリッスンするために必要です。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [データ保持（Data Retention）] ページで、[データベース保持設定（Database Retention Configuration）] テーブルを変更します。

a) 以下ののテーブルでは、保持時間が「40」に設定されています。

- Application_Event
- イベント
- Network_Event
- Route_Call_Detail
- Route_Call_Variable
- Termination_Call_Detail
- Termination_Call_Variable

b) その他すべての設定はデフォルトのまま確定します。コンタクト センターで、長期間にデータにアクセスする必要がある場合には、適切な値を入力します。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 [データの消去] ページで、システム上で需要が低い曜日および時間の消去を指定します。

ステップ 12 デフォルトの **上限（%）に達した場合は自動で消去する**で確定します。

ステップ 13 [次へ（Next）] をクリックします。

ステップ 14 **概要** ウィンドウで、**サービス アカウントの作成** オプションを選択して、以下の手順を実行します。

a) ドメイン ユーザのアカウント名を入力します。

指定したドメインにユーザが作成されていることを確認します。

b) 有効なパスワードを入力します。

c) サマリーを確認して、**終了**をクリックします。

注意 すべてのディストリビュータ サービスおよびロガー サービスに同じドメイン ユーザ アカウントを使用します。ロガーとディストリビュータに異なるドメインアカウントを使用する場合は、ディストリビュータ サービスのユーザ アカウントがサイド A とサイド B のローカル ロガー `UcceService`グループに追加されていることを確認してください。

ロガー コンポーネントのインスタンスへの追加

サイド A とサイド B のルータに対してこの手順を実行します。

手順

ステップ 1 Web セットアップ ツールで、**コンポーネント管理 > ルータ**を選択します。

ステップ 2 **追加** 。

ステップ 3 **展開** ページで、現在のインスタンスを選択します。

ステップ 4 **展開** ダイアログで、適切なサイドを選択します。

ステップ 5 **デュプレックス**をクリックして、**次へ**をクリックします。

ステップ 6 **ルータ接続** ダイアログで、プライベート インターフェイスとパブリック 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。

（注） アドレス入力フィールドでは、IPアドレスの代わりに完全修飾ドメイン名を使用します。

パブリック ネットワーク インターフェイス カードに 2 つの IP アドレスが（IP ベースの優先順位付けのために）設定されている場合は、DNS サーバに 2 つの A レコードを手動で追加します。一方の A レコードは高優先順位の IP アドレスで、もう一方の A レコードは通常の優先順位の IP アドレス用です。2 つの DNS エントリのホスト部分は、Windows サーバのホスト名と異なる必要があります。新しい DNS エントリを使用して、インターフェイスを設定します。このメモは、ルータおよびすべての PG マシンに適用されます。

ステップ 7 **周辺機器ゲートウェイを** フィールドを空白のままにして、 **次へ**をクリックします。

ステップ 8 **ルータ オプション** ダイアログで、**Quality of Service （QoS）を有効にする** チェック ボックスを適切に設定して、**次へ**をクリックします。

すべての Unified CCE プライベート ネットワーク トラフィックに対して QoS を有効にします。可視（パブリック） ネットワーク トラフィックの QoS は、ほとんどの展開では無効にします。詳細については、
https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

で、 *Cisco Packaged Contact Center Enterprise* ソリューション設計ガイドの適切なセクションを参照してください。

ステップ 9 **ルータ Quality of Service** ダイアログで、 **次へ**をクリックします。

ステップ 10 **サマリー** ダイアログで、ルータ サマリーが正しいことを確認して、 **完了**をクリックします。

Unified CCE サービスの開始

Unified CCE コンポーネントは、ホスト コンピュータ上で Windows サービスとして実行されます。デスクトップ上の **Unified CCE サービス コントロール ツール**で、上記サービスを開始、停止、または周期化させることができます。

（注） この手順は、 Unified CCE サービスを有効化する場合に必要です。ただし、展開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、このタスクは保留する必要があります。

手順

ステップ 1 各 Unified CCE サーバ 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 以下の順序で、各 **CCE コンポーネント**を選択し、**スタート**をクリックします。

1. ロガー A
2. ルータ A
3. ロガー B
4. ルータ B
5. 管理およびデータ サーバ

AW-HDS-DDS の設定

以下の手順を実行して、 Packaged CCE 4000展開用 AW-HDS-DDS を設定します。

手順	タスク
1	CCE コンポーネント用 SQL Server の設定 （2 ページ）
2	Unified CCE インスタンスの追加 （82 ページ）
3	HDS データベースの作成 （73 ページ）

手順	タスク
4	管理およびデータ サーバ コンポーネントのインスタンスへの追加 （74 ページ）
5	ICM データベース ルックアップの設定 （119 ページ） （任意）
6	Cisco SNMP の設定 （21 ページ） （任意）

HDS データベースの作成

HDS データベースを作成する管理およびデータ サーバ上でこの手順を実行します。

手順

ステップ 1 [ICMDBA ツール] を開き、表示される警告のいずれにも **はい** をクリックします。

ステップ 2 **サーバ** > **インスタンス**に移動します。

ステップ 3 インスタンス名を右クリックし、**作成**を選択します。

ステップ 4 [コンポーネントの選択] ダイアログ ボックスで、**管理およびデータ サーバ**を選択します。[OK] をクリックします。

ステップ 5 要求された場合 「SQL Server が適切に設定されていません。今すぐ設定しますか？」 には、**はい**をクリックします。

ステップ 6 [設定] ダイアログボックスで、**OK**をクリックします。

ステップ 7 [AW タイプの選択] ダイアログ ボックスで、**エンタープライズ**を選択します。**OK** をクリックして、[データベースの作成] ダイアログ ボックスを開きます。

ステップ 8 以下の通りに、HDS データベースを作成します。

a) [DB タイプ] ドロップダウンリストで、**HDS**を選択します。

b) [追加（Add）] をクリックします。

c) [デバイスの追加] ダイアログ ボックスで、**データ**を選択します。

d) [利用可能なドライブ] リストから、データベースをインストールするドライブを選択します。

e) [サイズ] フィールドでは、デフォルト値をそのまま使用することも、導入に沿った適切なサイズを入力することもできます。

（注） データベース サイズ推定ツールを使用すると、導入に適したサイズを計算できます。

f) **OK** をクリックして、[データベースの作成] ダイアログ ボックスに戻ります。

g) [追加（Add）] をクリックします。

h) [デバイスの追加] ダイアログ ボックスで、**ログ**を選択します。

i) [利用可能なドライブ] リストから、データベースを作成するドライブを選択します。

j) [サイズ] フィールドでは、デフォルト値をそのまま使用することも、導入に沿った適切なサイズを入力することもできます。
k) **OK** をクリックして、[データベースの作成] ダイアログ ボックスに戻ります。

ステップ 9 [データベースの作成]ダイアログボックスで、**作成する**をクリックして、**スタート**をクリックします。

ステップ 10 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。

管理およびデータ サーバ コンポーネントのインスタンスへの追加

手順

ステップ 1 Web セットアップ ツールを開きます。

ステップ 2 **コンポーネント管理 > 管理およびデータ サーバ**を選択します。[追加（Add）] をクリックします。

ステップ 3 **展開** ページで、現在のインスタンスを選択します。

ステップ 4 **管理及びデータ サーバの追加** ページ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) 展開サイズを選択します。

以下の管理およびデータ サーバ タイプは、**小規模から中規模の展開サイズ** を選択します。

- 管理サーバ、リアルタイムおよび履歴データ サーバ、および詳細データ サーバ（AW-HDS-DDS）

以下の管理およびデータ サーバ タイプに **大規模展開** を選択します。

- 管理サーバ、リアルタイムおよび履歴データ サーバ（AW-HDS）
- 履歴データ サーバ（HDS）

c) [次へ（Next）] をクリックします。

ステップ 5 **サーバの役割**で、以下のいずれかを実行します。

a) **小規模から中規模の展開**で、**管理サーバ リアルタイムおよび履歴データ サーバ、および詳細データ サーバ（AW-HDS-DDS）**を選択します。
b) **大規模展開**で、展開内容に応じて、**管理サーバとリアルタイムおよび履歴データ サーバ（AW-HDS）** あるいは **履歴および詳細データ サーバ（HDS-DDS）** を選択します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 サイド A またはサイド B のプライマリ サーバとセカンダリ サーバを指定します。

サイド A またはサイド B サーバを指定するには、[管理およびデータ サーバ 接続] ページで、以下を実行します。

a) **プライマリまたはセカンダリの管理およびデータ サーバ** エリアの下で、デフォルトで、**プライマリ** オプション ボタンが選択されています。
b) **管理およびデータ サーバ接続**エリアの下：

プライマリ 管理およびデータ サーバ フィールドで、サイド A サーバのホスト名を入力します。

セカンダリ 管理およびデータ サーバ フィールドで、サイド B サーバのホスト名を入力します。

プライマリおよびセカンダリ管理およびデータ サーバの共通サイト名 フィールドで、一意の名前を入力します。

c) [次へ（Next）] をクリックします。

ステップ 8 Database and Options 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「C」を選択します。
b) **設定管理サービス（CMS）ノード** を確認します（オプション）。
c) **Internet Script Editor（ISE）サーバ** を確認します（オプション）。
d) [次へ（Next）] をクリックします。

ステップ 9 [Central Controller Connectivity] ページで、以下の通り設定します。

（注） Pacakged CCE 4000 エージェント展開では、ルータとロガーの IP アドレスは同じです。

a) **ルータ サイド A**には、ルータ サイド A の IP アドレスを入力します。
b) **ルータ サイド B**には、ルータ サイド B の IP アドレスを入力します。
c) **ロガー サイド A**には、ロガー サイド A の IP アドレスを入力します。
d) **ロガー サイド B**には、ロガー サイド B の IP アドレスを入力します。
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 サイド A を優先する** または **セントラル コントローラ サイド B を優先する**を選択します。
g) [次へ（Next）] をクリックします。

ステップ 10 **概要** ウィンドウで、[サービス アカウントの作成] オプションを選択して、以下の手順を実行します。

a) ドメイン ユーザ アカウントを作成します。作成したドメイン ユーザを入力します。
b) 有効なパスワードを入力します。
c) サマリーを確認して、**終了**をクリックします。

注意 すべてのディストリビュータ サービスおよびロガー サービスに同じドメイン ユーザ アカウントを使用します。ロガーとディストリビュータに異なるドメインアカウントを使用する場合は、ディストリビュータ サービスのユーザ アカウントがサイド A とサイド B のローカル ロガー `UcceService`グループに追加されていることを確認してください。

Packaged CCE の展開タイプの設定

Packaged CCE 4000 エージェント および 12000 エージェントの展開タイプの設定の際は、メインサイトを追加しなければなりません。メインサイトには、0 個以上の周辺機器セットが関連付けられている場合があります。周辺機器セットは、例えば、Finesse、CVPなど、周辺機器ゲートウェイ（周辺機器ゲートウェイ自体を含む）に依存するすべてのコンポーネントのコレクションです。周辺機器セットの追加方法については、周辺機器セットの追加と保守を参照してください。

4000 エージェントまたは 12000 エージェント展開タイプでのメイン サイトの追加および保守

手順

ステップ 1 **Unified CCE 管理** > **概要** > **インフラストラクチャ設定** > **展開設定**に移動します。

ステップ 2 **展開タイプ**の歯車のアイコンをクリックします。
展開の設定 ウィザード画面が開きます。

ステップ 3 ドロップダウン リストで、展開タイプを *Packaged CCE*：*4000* エージェント または *Packaged CCE*：*12000* を千tなくします。

ステップ 4 **ダウンロード テンプレート**を使用して、選択した展開の種類の CSV テンプレートを取得します。

ステップ 5 ファイルの詳細を入力して保存します。

表 *2: CSV* テンプレートの詳細

カラム	説明	必須かどうか	許容値
[名前（Name）]	マシン名	はい	名前の先頭はアルファベットにする必要があります。A ～ Z、0 ～ 9、ドット (.)、またはハイフン (-) がサポートされています。最大長は 128 文字です。

カラム	説明	必須かどうか	許容値
マシン タイプ	マシン タイプ列挙体名	はい	必須マシン： • CCE_ROGGER（4000 エージェント展開に適用可） • CCE_ROUTER（12000 エージェント展開に適用可） • CCE_LOGGER（12000 エージェント展開に適用可） • CCE_AW • CUIC_PUBLISHER • CUIC_SUBSCRIBER • LIVE_DATA • IDS_PUBLISHER • IDS_SUBSCRIBER オプションのマシン： • CCE_PG • CVP • FINESSE_PRIMARY • FINESSE_SECONDARY • CM_PUBLISHER • CM_SUBSCRIBER • HDS • ECE（ECE データ サーバを参照） • ECE_WEB_SERVER • CVP_REPORTING • GATEWAY • CVVB • CUSP • SOCIAL_MINER • THIRD_PARTY_ MULTICHANNEL

カラム	説明	必須かどうか	許容値
publicAddress	パブリック アドレス	はい	有効な IP アドレス
connectionInfo	マシンの接続情報	AW、CM_PUBLISHER、CUIC_PUBLISHER、FINESSE_PRIMARY、ECE_WEB_SERVER、CVP、CVP_REPORTING、IDS_PUBLISHER、CUSP、ゲートウェイ、VVB および SOCIAL_MINER の場合は必須	userName=<user@domain.com> &password=<pass>&port=<1234> （注） • ユーザ名は「administrator」です。 • ポートはオプションとなります。ポートを指定しない場合は、デフォルトのポートが使用されます。アンパサンド (&) および等号 (=) が、ユーザ名文字列とパスワード文字列で使用され、URL エンコーディングを使用してエンコードする必要があります。 • CCE_AW および EXTERNAL_HDS のデフォルトポートは、7890、CUIC_PUBLISHER、IDS_PUBLISHER、LIVE_DATA、CM_PUBLISHER、FINESSE_PRIMARY は、8443、CVP および CVP_REPORTING は、8111、EXTERNAL_CVVB、EXTERNAL_SOCIAL_MINER、および ECE_WEB_SERVER は、443 です。 • ECE_WEB_SERVER のアプリケーションインスタンスを指定します。

カラム	説明	必須かどうか	許容値
privateAddress	プライベート アドレス	ROGGER、ルータ、ロガー、およびPGでは必須です。	有効な IP アドレス
peripheralSetName	周辺機器セット名	PG、CUCM、Finesse、CVP に必須です。	名前はアルファベット（A ～ Z）または数字（0 ～ 9）で開始することができます。ドット(.)またはハイフン(-)がサポートされています。最大長は10文字です。
side	サイド情報	はい	sideA sideB

ステップ 6 ファイルをアップロードして、**次へ**をクリックします。

ステップ 7 検証が完了するまで待機します。次のタスクが実行されます。

コンポーネント（**Component**）	自動初期化タスク
Unified CCE PG	• CUCM PIM を使用して CUCM ペリフェラル ゲートウェイ（PG）を作成します。 • メディア ルーティング PG（MR PG）を作成します。 • VRU PIM を使用して、VRU PG を作成します。 • 各周辺機器のルーティング クライアントを作成します。 （**注**） 必要なラベルは、設定管理ツールの[ラベル リスト]オプションで作成する必要があります。
Unified Customer Voice Portal	• Unified CVP コール サーバのコンポーネントを設定します。 • Unified CVP VXML サーバのコンポーネントを設定します。 • Unified CVP Media Server のコンポーネントを設定します。
Unified CVP Reporting Server	Unified CVP Reporting Server のコンポーネントを設定します（使用する場合）。
ライブ データ	ライブ データを再展開します。

（**注**） 実行されたタスクのいずれかが失敗した場合は、すべてのタスクが元に戻されます。

検証が失敗した場合は、**戻る**をクリックしてファイル内の問題を修正し、もう一度ファイルをアップロードして、**完了**をクリックします。

これで、メイン サイトが作成され、[インベントリ] ページに追加されます。

Packaged CCE 4000 エージェントおよび 12000 エージェント展開のシステム インベントリ

Packaged CCE 導入への変更が完了すると、インベントリにアクセスできます。

インベントリにアクセスするには、**Unified CCE 管理** > **システム** > **展開**に移動します。

導入タイプを選択または変更したとき、および定期的なシステム スキャンの後で、システム インベントリの内容が更新されます。システム スキャンで Packaged CCE の要件に準拠しない VM が検出されると、[導入の設定（Configure your deployment）] ポップアップ ウィンドウが自動的に開き、エラーの詳細が示されます。エラーを修正し、**展開の設定** ポップアップ ウィンドウの入力を完了すると、再びインベントリにアクセスすることができます。

サーバ ステータスルールの詳細については、Packaged CCE 4000 エージェントおよび 12000 エージェント展開のサーバ ステータス ルールの監視 （82 ページ）を参照してください。

表 *3:* システム インベントリのレイアウトとアクション

項目	注記	アクション
プリンシパル AW の設定	同時にプリンシパル AW にできるのは 1 台の AW マシンだけです。	プリンシパル AW は必ず指定する必要があります。展開時には、CSV ファイルの最初の AW マシンがプリンシパル AW となります。 プリンシパル AW は以下の機能で使用されます。 • ファイル転送 • コンテキスト サービス登録 • SSO の登録および有効化 • 差分同期 導入後は、インベントリで別の AW を選択して、プリンシパル AW を変更することができます。設定変更のほとんどを行う AW をプリンシパル AW として選択します。 **プリンシパル AW を設定するには、以下の手順を実行します。** **1.** [AW] をクリックして [AW の編集] ポップアップ ウィンドウを開きます。 **2.** **PrincipalAW** チェック ボックスをオンにします。 **3.** Unified CCE 診断フレームワーク サービスのクレデンシャルを入力します。 入力する Unified CCE 診断フレームワーク サービスのクレデンシャルは、インスタンスの設定セキュリティ グループ メンバーであるドメイン ユーザ向けである必要があります。クレデンシャルは展開内のすべての CCE コンポーネント（ルータ、PG、AW など）で有効な必要があります。 各 Unified CCE サーバで Unified CCE 診断フレームワーク サービスが実行中であることを確認します。 **4.** [保存（Save）] をクリックします。

（注） Packaged CCE コンポーネントのパスワードを変更した場合は、システム インベントリ内の対応する VM のパスワードを更新する必要があります。

Unified CCE インスタンスの追加

手順

ステップ 1 デスクトップのショートカットから、 Unified CCE Web セットアップツールを開きます。

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

ステップ 3 **インスタンス管理**をクリックして、**追加**をクリックします。

ステップ 4 **インスタンスの追加** ページで、ドロップダウンリストから顧客 **ファシリティとインスタンス** を選択します。

ステップ 5 インスタンス番号を入力します。

同じインスタンス名が 1 つのドメインに複数回出現する可能性があるため、インスタンス番号によって一意性が保たれます。インスタンス番号は 0 ～ 24 の範囲でなければなりません。インスタンス番号は、同じインスタンスに対して展開全体で一致している必要があります。エンタープライズ（シングルインスタンス）展開の場合は、別の値を選択する理由がある場合以外は、0 を選択します。

ステップ 6 **[保存（Save）]** をクリックします。

（注） 上記のインスタンスを追加する手順は、ICM コンポーネントをホストする各 Windows サーバ VM で繰り返す必要があります。

Packaged CCE 4000 エージェントおよび 12000 エージェント展開のサーバ ステータス ルールの監視

Packaged CCE 4000 および 12000 エージェント展開の場合、インベントリ テーブルには、主要な AW マシンのアラート アイコンが表示されます。アラート アイコンの上にマウスのカーソルを合わせると、マシンのステータスが表示されます。

Cisco Unified Contact Center Enterprise PG の設定

（注） 周辺機器セットをメイン サイトまたはリモート サイトに追加する毎に、以下の手順を繰り返します。周辺機器セットの詳細については、周辺機器セットの追加と保守 を参照してください。

設定作業
周辺機器セットに CUCM PG が含まれている場合： アプリケーション ユーザの設定 （92 ページ） Unified Communications Manager、リリース 12.5 への Cisco JTAPI クライアントのインストール （83 ページ） CTI サーバの設定 （84 ページ）
周辺機器セットに VRU PG が含まれている場合は、手動で CVP サーバを再起動します。
周辺機器セットに MR PG が含まれている場合、メディア ルーティング ペリフェラル ゲートウェイへの PIM の追加

Unified Communications Manager、リリース 12.5 への Cisco JTAPI クライアントのインストール

以下の手順を実行できるのは、Cisco Unified Communications Manager リリース 12.5 に接続するために JTAPI クライアントをインストールする場合のみです。

始める前に

JTAPI クライアントをインストールする前に、以前のバージョンがアンインストールされていることを確認してください。

手順

ステップ 1 PG マシン上でブラウザ ウィンドウを開きます。

ステップ 2 Unified Communications Manager Administration アプリケーションを起動するには、各コール サーバの Web ブラウザに以下の URL を入力します。http://<*Unified Communications Manager* マシン名>/ccmadmin

ステップ 3 Unified Communications Manager のインストールおよび設定時に作成したユーザ名とパスワードを入力します。

ステップ 4 **アプリケーション** > **プラグイン**を選択します。[検索（Find）] をクリックします。

ステップ 5 **Cisco JTAPI （Windows）のダウンロード** のよこにあるリンクをクリックします。. 64 ビット版のみをダウンロードします。

32 ビット版のみをダウンロードします。

ステップ 6 **保存** を選択して、プラグイン ファイルを任意の場所に保存します。

ステップ 7 JTAPI プラグインの zip ファイルをデフォルトの場所または選択した場所で解凍します。

解凍されたフォルダには、`CiscoJTAPIx32`と`CiscoJTAPIx64` の 2 つのフォルダが作成されます。

ステップ 8 `CiscoJTAPIx32` フォルダで `install32` ファイルを実行します。

インストーラーが JTAPI クライアントをインストールするデフォルトの場所を控えておきます。

ステップ 9 デフォルトのインストール パスをそのまま使用する場合は、[入力（Enter）] をクリックして続行します。

指示に従って操作します。手順に従って、必要に応じて 入力 をクリックします。

プロンプトが表示されたら、TFTP サーバの IP アドレスを指定します。4000 および 12000 展開の場合、IP アドレスは、CUCM PIM で提供されている CUCM IP アドレスと同じでなければなりません。

JTAPI クライアントのインストールは、デフォルトの場所で完了します。次のメッセージが表示されます。

□□□□□□□□□□□□□□□

ステップ 10 マシンをリブートします。

次のタスク

（注） JTAPI クライアントがインストールされているデフォルトの場所には、`uninstall32` ファイルも含まれています。このファイルは、必要に応じて、このバージョンのクライアントをアンインストールするために使用します。

CTI サーバの設定

PG セットアップ ツールを使用して CTI サーバをセットアップします。

CTI サーバ コンポーネントの追加

手順

ステップ 1 デスクトップ上の **Unified CCE ツール** から周辺機器ゲートウェイ セットアップ ツールを開きます。

ステップ 2 インスタンス コンポーネント セクションで、**追加** をクリックします。

ICM コンポーネント選択ダイアログ ボックスが開きます。

ステップ 3 **CTI サーバ**をクリックして、**OK**をクリックします。

CTI サーバのプロパティ ダイアログ ボックスが開きます。

CTI サーバ プロパティの設定

手順

ステップ 1 Unified CCE サポート プロバイダが特に指定しない限り、CTI サーバのプロパティ ダイアログ ボックスで、**実稼働モード** および **システム起動時の自動開始** をオンにします。上記の設定により、CTI サーバ サービスの起動タイプが [自動] に設定されるため、マシンの起動時に CTI サーバが自動的に起動します。

ステップ 2 冗長 CTI サーバ マシンを設定する場合は、**デュプレックス CTI サーバ** オプションをオンにします。

ステップ 3 [CG ノード プロパティ] セクションで、CG ノードの**ID** の数字部分は、PG ノード ID と一致していなければなりません（例えば、CG 1 と PG 1等）。

ステップ 4 **ICM システム ID** は、CTI ゲートウェイに関連付けられている PG のデバイス管理プロトコル（DMP）番号です。通常、この番号は、ステップ 3 の CG ID に関連付けられた番号です。

ステップ 5 追加する CTI サーバがデュプレックスの場合、サイド A または サイド B のどちら **側**を設定するかを指定します。CTI サーバがシンプレックスの場合は、サイド A を選択します。

ステップ 6 [次へ（Next）] をクリックします。

CTI サーバ コンポーネントのプロパティ ダイアログ ボックスが開きます。

CTI サーバ プロパティの設定

CTI サーバ コンポーネントの [プロパティ] ダイアログ ボックスでは、以下の接続モードをサポートしています。

- **セキュアまたはセキュアでない接合（混合モード）**：CTI サーバと CTI クライアント間では、セキュアまたは非セキュア接続が許可されます。
- **セキュア専用接続**：CTI サーバと CTI クライアント間でセキュアな接続を許可します。

重要 非セキュア専用モードはサポートされません。

（注） コンポーネント間の安全な接続を有効にするには、セキュリティ証明書管理プロセスが完了していることを確認してください。

詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html で *Cisco Unified ICM/Contact Center Enterprise* セキュリティ ガイド を参照してください。

[CTI サーバ コンポーネントのプロパティ] ダイアログ ボックスで、セットアップが自動的にデフォルトの **セキュアな接続ポート** および **非セキュアな接続ポート** の値を表示します。これ

らの値を使用するか、必要なポート番号に変更します。CTI クライアントは、これらのポートを使用して CTI サーバに接続します。

単一のマシンで複数 CTI サーバを稼働している場合は、各 CTI サーバは、セキュアな接続 および 混合モード接続 に別のポート番号セットを使用しなければなりません。

手順

ステップ 1 適切な接続タイプを選択します。

a) セキュアな接続の場合は、 **セキュア専用モード** チェック ボックスをオンにします。

このオプションは、**非セキュア接続ポート** フィールドを無効にします。

b) 混合モード接続の場合は、**セキュア専用モードを有効にする** チェック ボックスをオフにします。

これはデフォルトの接続モードです。

ステップ 2 クライアントがCTIサーバからイベントを受信する前にエージェントがクライアントにログインしていることを確認するには、**クライアント イベントに対して必要なエージェント ログイン**チェック ボックスをオンにします。これにより、クライアントは、他のエージェントのデータにアクセスできなくなります。

ステップ 3 **次へ**をクリックします。

[CTI サーバ ネットワーク インターフェイスのプロパティ] ダイアログ ボックスが開きます。

CTI サーバ ネットワーク インターフェイス プロパティの設定

手順

ステップ 1 CTI サーバ ネットワーク インターフェイスのプロパティ ダイアログ ボックスの **PG パブリック インターフェイス** セクションで、CTIサーバに関連付けられたPGのパブリック ネットワーク アドレスを入力します。

ステップ 2 **CG プライベート インターフェイス** セクションで、CTI サーバのプライベート ネットワーク アドレスを入力します。

ステップ 3 **CG 可視インターフェイス** セクションで、CTI サーバのパブリック ネットワーク アドレスを入力します。

ステップ 4 [次へ（Next）] をクリックします。

設定情報確認ウィンドウが開きます。

CTI サーバのセットアップの完了

手順

ステップ 1 [設定情報の確認] ウィンドウで、設定が意図した通りに表示されていることを確認します。先に進む前に設定を変更する場合は、**戻る** ボタンを使用します。

ステップ 2 設定が正しい場合は、**完了**をクリックします。

ステップ 3 最後の画面には、ノード マネージャをすぐに起動するかどうかの確認が表示されます。

ステップ 4 **完了** をクリックして、セットアップを終了します（必要に応じてノード マネージャを起動します）。

起動を選択した場合、ノード マネージャが CTI サーバ上の他の Unified CCE プロセスを自動的に開始します。

Cisco Unified Customer Voice Portal の設定

Packaged 4000 エージェントあるいは 12000 エージェント展開のための Cisco Unified Customer Voice Portal（CVP）の設定タスクの概要を以下の表に示します。

（注） CVP 設定は、サイトによって異なります。サイト毎にサイド A およびサイド B の設定が同じである必要があります。

設定作業
CA のセキュリティの詳細については、以下を参照してください。 Unified CVP セキュリティ
自己署名付き証明書の詳細については、以下を参照してください。 Cisco Unified CVP サーバにプリンシパル AW 証明書を追加します。
コール サーバ サービスの設定
メディア サーバの設定
SNMP の設定 （87 ページ）
ライセンス管理 （90 ページ）

SNMP の設定

Cisco Customer Voice Portal（CVP）サーバから SNMP トラップを受信するには、Simple Network Management Protocol（SNMP）の設定を使用します。設定ファイルを使用して CVP サーバでこの設定を行うことができます。

手順

ステップ 1 管理者クレデンシャルを使用して、SCVMM サーバにログインします。

ステップ 2 C:\Cisco\CVP\conf\SNMPD.CNFに移動します。

ステップ 3 SNMP 設定を行うには、以下のパラメータを入力します。

（注） パラメータ値を改行しないで 1 行で入力します。

表 *4: SNMP* 設定パラメータ

パラメータ	説明	書式
snmpCommunityEntry	SNMP 管理ステーションと通信する V1/V2 SNMP プロトコルを使用するために Unified CVP デバイス上で実行する SNMP エージェントを設定します。SNMP V1/V2c コミュニティストリングを追加および削除し、SNMP 管理ステーションから SNMP 通知を受信する宛先を設定して、コミュニティストリングとデバイスを関連付けます。	snmpCommunityEntry <snmpCommunityIndex> <snmpCommunityName> <snmpCommunitySecurityName> <snmpCommunityContextEngineID> <snmpCommunityContextName> <snmpCommunityTransportTag> <snmpCommunityStorageType> 例： v2ccvp cvp cvp localSnmpID - - readOnly
vacmSecurityToGroupEntry	V1 または V2C SNMP プロトコルの認証グループを設定します。	vacmSecurityToGroupEntry <vacmSecurityModel> <vacmSecurityName> <vacmGroupName> <vacmSecurityToGroupStorageType> 例： vacmSecurityToGroupEntry snmpv2c cvp v2cNoAuthNoPrivGroup nonVolatile
snmpNotifyEntry	V1 または V2 SNMPプロトコルを使用して SNMP 管理ステーションと通信するように、Unified CVP デバイスで実行される SNMP エージェントを設定し、SNMP 管理ステーションから SNMP 通知を受信するように宛先を設定します。	snmpNotifyEntry <snmpNotifyName> <snmpNotifyTag> <snmpNotifyType> <snmpNotifyStorageType> 例： snmpNotifyEntry Descvp Descvp-TrapTag trap readOnly

パラメータ	説明	書式

usmUserEntry	V3 SNMPプロトコルを使用して SNMP 管理ステーションと通信するように、Unified CVP デバイスで実行される SNMP エージェントを設定します。SNMP ユーザを追加および削除し、アクセス権限を設定し、SNMP ユーザをデバイスに関連付けます。	`usmUserEntry <usmUserEngineID> <usmUserName> <usmUserAuthProtocol> <usmUserPrivProtocol> <usmUserStorageType> <usmTargetTag> <AuthKey> <PrivKey>`
		例：
		`usmUserEntry localSnmpID cvp usmNoAuthProtocol usmNoPrivProtocol readOnly`

snmpNotifyEntry	V3 SNMPプロトコルを使用して SNMP 管理ステーションと通信するように、Unified CVP デバイスで実行される SNMP エージェントを設定し、SNMP 管理ステーションから SNMP 通知を受信するように宛先を設定します。	`snmpNotifyEntry <snmpNotifyName> <snmpNotifyTag> <snmpNotifyType> <snmpNotifyStorageType>`
		例：
		`snmpNotifyEntry Descvp Descvp-TrapTag trap readOnly`

sysLocation	MIB2 システム グループのシステム ロケーション設定を構成し、MIB2 システム グループとデバイスを関連付けます。	`<octetString>`
		例：
		`MIBLoc`

sysContact	MIB2 システム グループのシステム コンタクト設定を構成し、MIB2 システム グループとデバイスを関連付けます。	`<octetString>`
		次に例を示します。
		`MIBContact`

snmpTargetAddrEntry	SNMP トラップ レシーバのターゲット IP を設定します。	`snmpTargetAddrEntry <snmpTargetAddrName> <snmpTargetAddrTDomain> <snmpTargetAddrTAddress> <snmpTargetAddrTimeout> <snmpTargetAddrRetryCount> <snmpTargetAddrTagList> <snmpTargetAddrParams> <snmpTargetAddrStorageType> <snmpTargetAddrTMask> <snmpTargetAddrMMS>`
		例：
		`snmpTargetAddrEntry  targetDesV2-Addr1`
		`snmpUDPDomain 10.100.10.100:0 0 0 \ targetDesV2-TrapTag targetDesV2-TrapParams readOnly 255.255.255.255:0 2048`

ステップ 4 変更を保存します。

ステップ 5 サービス に移動し、`Cisco CVP SNMP` 管理を再起動します。

ライセンス管理

CVP サーバ（コール サーバまたはレポート サーバ）でライセンスを設定するには、以下の手順を実行します。

手順

ステップ 1 CVP サーバ（コール サーバまたはレポート サーバ）にログインします。

ステップ 2 ライセンス ファイルを `C:\Cisco\CVP\conf\license`にコピーします。

ステップ 3 対応するサーバを再起動します。

Cisco Unified Communications Manager の設定

Packaged CCE 4000 エージェントあるいは 12000 エージェント展開のための Cisco Unified Communications Manager の設定タスクの概要を以下の表に示します。

.

タスク
CA および自己署名付き証明書の詳細については、以下を参照してください。 CUCM上の通信のセキュリティ保護
アプリケーション ユーザの設定 （92 ページ）
完全修飾ドメイン名の設定 （26 ページ）
Cisco Unified Communications Manager グループの設定 （26 ページ）
デバイス プールの設定 （91 ページ）
会議ブリッジの設定 （27 ページ）
メディア ターミネーション ポイントの設定 （28 ページ）
Unified CM と IOS ゲートウェイでのトランスコーダの設定 （28 ページ）
メディア リソース グループの設定 （29 ページ）
メディア リソース グループ リストの設定および関連付け （30 ページ）
CTI ルート ポイントの設定 （30 ページ）

タスク
エンタープライズ パラメータの設定 （91 ページ）
ロケーション ベースのコール アドミッション制御のためのイングレス ゲートウェイの設定（31 ページ）
ルート グループの設定 （31 ページ）
Unified CM での SIP プロファイルの追加 （33 ページ）
トランクの設定 （33 ページ）
サービスのアクティブ化 （34 ページ）
エージェント デスクの設定 （93 ページ）
A-Law コーデックの設定 （94 ページ）
SNMP の設定 （95 ページ）

デバイス プールの設定

デバイス プールを設定するには、以下の手順を実行します。

手順

ステップ 1 **システム** > **デバイス プール**を選択します。
ステップ 2 [新規追加（Add New）] をクリックします。
ステップ 3 デバイス プール名に適切な **デバイス プール名**を指定します。
ステップ 4 対応するコール管理グループを **Cisco Unified Communications Manager グループ**で選択します。
ステップ 5 適切な**日付および時刻グループ**と**地域**を選択します。
ステップ 6 適切なメディア リソース グループ リストを **メディア リソース グループ リストから選択します。**
ステップ 7 **[保存（Save）]** をクリックします。

エンタープライズ パラメータの設定

手順

ステップ 1 **システム** > **エンタープライズ パラメータ**を選択します。

ステップ 2 クラスタの完全修飾ドメイン名を設定します。

例：

ccm.hcscc.icm

（注） クラスタの完全修飾ドメイン名は、Unified CVP で定義されている Unified Communications Manager サーバ グループの名前です。

アプリケーション ユーザの設定

手順

ステップ 1 Unified Communications Managerで、 **ユーザ管理** > **アプリケーション ユーザ**を選択します。

ステップ 2 [アプリケーション ユーザの設定（Application User Configuration）] ウィンドウで、[新規追加（Add New）] をクリックします。

ステップ 3 周辺ゲートウェイのセットアップで設定されたユーザ ID を入力します。

（注） 周辺機器セットの作成時に、Pguser は PIM に設定されます。

ステップ 4 パスワードを入力します。

ステップ 5 CUCM PIM 用の周辺機器ゲートウェイの設定にに同じパスワード セットを入力する必要があります。

ステップ 6 アプリケーション ユーザを次のとおり有効な標準 CTI グループおよびロールに追加します。

a) [アクセス コントロール グループに追加（Add to Access Control Group）] をクリックします。

b) **標準 CTI を有効にする**グループを選択します。

c) **標準 CTI Connected Xferおよび conf をサポートする電話制御を許可する** グループを選択します。

d) **標準 CTI ロールオーバー モードをサポートする電話制御を許可する** グループを選択します。

e) [選択項目の追加（Add Selected）] をクリックします。

f) **[保存（Save）]** をクリックします。

ステップ 7 アプリケーション ユーザに CTI ルート ポイントと電話を関連付けます。

ステップ 8 **[保存（Save）]** をクリックします。

エージェント デスクの設定

手順

ステップ 1 Configuration Managerで、 **ICM の設定** > **Enterprise** > **エージェント デスクの設定** > **エージェント デスクの設定リスト**を選択します。

[エージェント デスク設定リスト] ダイアログ ボックスが開きます。

ステップ 2 **取得** をクリックして、**追加**をクリックします。

ステップ 3 [属性] タブに情報を入力します。

名前。企業内で一意になるように、エージェント デスクの設定名を入力します。

応答なしの呼び出し時間。エージェントのステーションで呼び出し音が鳴る秒数（1 ー 120の間の値）を入力します。Unified CVP を展開する場合は、この数が、Unified CVP で設定したルータ再クエリの [応答なし] タイムアウトに設定した数よりも小さいことを確認してください。

このタイマーを設定する場合、エージェントがログインせずに使用させる場合を除き、Unified Communications Manager のエージェント内線番号に対して、無応答時の Unified Communications Manager の自動転送を設定する必要はありません。Unified Communications Manager の無応答時転送を設定した場合は、各 Unified Communications Manager ノードで無応答時の呼び出し時間より少なくとも 3 秒長い値を入力します。

応答なしの呼び出しダイヤル番号。エージェントが応答していないコールの再ルーティングに使用するルーティング スクリプトに関連付けられている Unified CCE DN を入力します。Unified CVP を導入する場合は、このフィールドは空白のままにします。

ログアウト非アクティビティ時間. Unified CCE がエージェントを自動的にログアウトさせる前にエージェントが非対応状態を継続する時間（10 ~ 7200 秒）を入力します。

着信時の作業モード。着信コールの後に後処理が必要かどうかを選択します。ドロップダウンリストからオプションを選択します。

発信時の作業モード。発信コールの後に後処理が必要かどうかを選択します。ドロップダウンリストからオプションを選択します。

後処理時間。エージェントにコールの後処理として割り当てられた時間（秒単位）。

アシスト コール方法。スーパーバイザ アシスタンスの要求に関して、Unified CCEが相談コールまたは匿名会議通話を作成するかを指定します。

緊急アラート方法。緊急コールの要求に関して、Unified CCEが相談コールまたは匿名会議通話を作成するかを選択します。

コールが VRU 上にキューイングされる可能性がある場合、ブラインド会議はサポートされません。

説明。エージェント デスクの設定に関する追加のオプション情報を入力します。

ステップ 4 以下のボックスを使用して、その他の設定を選択または選択解除します。

自動応答。エージェントへのコールが自動的に応答されることを示します。コールに応答するためにエージェントが何らかのアクションを実行する必要はありません。コール中に2番目のコールが着信した場合、そのコールは自動的には応答されません。これは、Unified Communications Manager の場合と同じ動作です。

自動応答を有効にする場合は、Unified Communications Manager で、スピーカーフォンまたはヘッドセット（またはその両方）をオンにするようにエージェントの電話機を設定する必要があります。ヘッドセット のみ をオンにする場合は、エージェントが電話機の [ヘッドセット] ボタンをオンにする必要もあります。

自動応答が選択されているマルチ回線対応環境では、非 ACD 回線でコールを受信した場合、そのコールは自動応答 しません。ただし、[Unified Communications Manager] 自動応答をオンにすると、コール応答します。

アイドル状態の理由を要求する。エージェントはアイドル状態に入る前に待受停止の理由を入力する必要があることを示します。

ログアウトの理由が必要。エージェントはアイドル状態に入る前に待受停止の理由を入力する必要があることを示します。

緊急時の自動記録。緊急コール要求の開始時に、レコードリクエストが自動的に送信されることを示します。

Cisco Unified Mobile Agent（チェック ボックス）。Unified Mobile Agent 機能を有効にして、エージェントがリモート ログインして、どの電話機でもコールを受信することができるようにします。Unified Mobile Agent の詳細については、https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_feature_guides_list.htmlの *Cisco Unified Contact Center Enterprise* 機能ガイド を参照してください。

ステップ 5 **保存** をクリックして、 **閉じる**をクリックします。

A-Law コーデックの設定

Unified Communications Managerを設定するには、以下の手順を実行します。

手順

ステップ 1 **システム**をクリックします。
ステップ 2 **サービス パラメータ**を選択します。
ステップ 3 サーバを選択します。
ステップ 4 サービスを **Cisco Call Manager**（有効）として選択します。
ステップ 5 クラスタ全体のパラメータ（システム：場所と地域）の下で、以下を確認します。

- **G.711 A-law コーデックを有効にする** が **有効になっていること**。
- **G 7.11 mu-law コーデック**が**無効**になっていること。

ステップ 6 [保存（Save）] をクリックします。

SNMP の設定

手順

ステップ 1 管理者クレデンシャルを使用して、Cisco Unified Serviceability*(https://hostname of primary server/ccmservice)* にログインしていること。

ステップ 2 **[SNMP]** > **[V1/V2c]** > **[コミュニティ ストリング（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マスター 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 マスター エージェントを再起動せずに設定を続行するには、[キャンセル（Cancel）] をクリックします。SNMP マスター 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**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から、**[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**] フィールドで、**コミュニティ文字列** ドロップダウン リストから、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マスター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 マスター エージェントを再起動せずに設定を続行するには、[キャンセル（Cancel）] をクリックします。SNMP マスター 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。

Cisco Unified Intelligence Center の設定

この順序に従って、Packaged CCE 4000 エージェントおよび 12000 エージェント展開のための Cisco Unified Intelligence Center を設定します。

手順	タスク
1	セキュリティ証明書の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.htmlの *Cisco Unified Intelligence Center* ユーザ ガイド を参照してください。
2	Unified Intelligence Center 外部 HDS データ ソースの設定 （36 ページ）
3	レポート バンドルのダウンロード （37 ページ）
4	レポート バンドルのインポート （38 ページ）
5	Unified Intelligence Center Administration の設定（39 ページ）

Cisco Finesse の設定

以下の手順に従って、Packaged CCE 4000 エージェントおよび 12000 エージェント展開の Cisco Finesse を設定します。

手順	タスク
1	CA 証明書の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.htmlの *Cisco Finesse* 管理ガイド を参照してください。
2	自己署名付き証明書の詳細については、以下を参照してください。 Finesse 証明書を AW マシンに追加します
3	**インフラストラクチャ設定** > **デバイス設定** > **Finesse** に移動して設定し、Finess サーバの **サイト** および **周辺機器セット** を選択します。 Contact Center Enterprise 管理およびデータ サーバの設定の構成 での Contact Center Enterprise CTI サーバ設定の設定
4	ライブ データ レポートのためのコンタクト センター エージェントおよびルーティングの設定 （41 ページ）
5	Cisco Tomcat サービスを再起動します。 （97 ページ）
6	ライブ データ レポート （41 ページ）
7	SNMP の設定 （95 ページ）

Cisco Tomcat サービスを再起動します。

Contact Center Enterprise 管理サーバ設定でいずれかの値を変更して保存したら、プライマリ Cisco Finesse サーバで Cisco Tomcat Service を再起動する必要があります。

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。

Cisco Finesse 管理の設定

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。

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://hostname of primary Finesse server/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 > 証明書管理 > CSRのダウンロード**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://hostname of secondary Finesse server/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、CSA を無効にしてサービスを再起動します。権限を持つエージェントは、Cisco Finesse Agent Desktop 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 ブラウザに次の URL を入力します。`http://Finesse サーバのホスト名/`。

ステップ 2 HTTPS を使用して管理コンソール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 **ログイン** 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。 **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。

ブラウザ	説明
	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。

ライブ データの設定

手順	タスク
1	ライブ データの初期設定 （102 ページ）
2	ライブ データの設定 （102 ページ）
3	CA および自己署名付き証明書の詳細については、以下を参照してください。 Live Data の証明書
4	AW のライブ データの設定 （102 ページ）
5	ライブ データ マシン サービスの設定 （104 ページ）
6	Unified Intelligence Center データ ソースの設定 （105 ページ）
7	ライブデータの再起動 （105 ページ）

ライブ データの初期設定

Packaged CCE 4000 および 12000 エージェント展開でライブ データが動作するには、サイド A およびサイド B の Logger で以下の手順を実行します。

手順

ステップ 1 `C:\icm\install` フォルダに移動します。

ステップ 2 **LiveDataMachineServiceCorrection.sql** ファイルを実行します。

（注） AW マシンから、ローカルデータベースの初期化ツールを実行します。

AW のライブ データの設定

AW を使用してライブ データを設定すると、プライマリ AW データベースとセカンダリ AW DB にアクセスすることができます。このコマンドは、プライマリまたはセカンダリ AW への

接続を自動的に検証し、設定されたユーザがAWデータベースへの適切なアクセス権を持っているかどうかを確認して、その結果を報告します。

検証を実行しない場合は、オプションのテスト省略（skip-test）パラメータを使用して、テストを実行しない設定にすることができます。「skip-test」パラメータを含める場合、設定されたユーザに適切な AW DB アクセスがあるかどうかはコマンドによって確認されず、結果が報告されません。

（注） パブリッシャおよびサブスクライバの両方で AW DB を設定する必要はありません。この設定は、パブリッシャおよびサブスクライバで複製されます。

始める前に

ライブ データを設定する前に、まず（特別な権限を持つ）SQL ユーザ がライブ データを取り扱えるように設定する必要があります。

SQL 管理者ユーザ「sa」または sysadmin 権限を持つユーザは、以下の SQL クエリをライブ データを使用するように設定された SQL ユーザのマスター システム データベース上で実行する必要があります。

```
USE master
GO
GRANT CONTROL ON CERTIFICATE :: UCCESymmetricKeyCertificate TO "<user>"
GRANT VIEW DEFINITION ON SYMMETRIC KEY :: UCCESymmetricKey TO "<user>"
```

手順

ステップ 1 ライブ データ サーバにログインします。

ステップ 2 以下のコマンドを実行し、プライマリ AW DB を使用してライブ データを設定します。このコマンドは、ライブデータからの接続を自動的に検証して、ユーザの権限を確認し、結果を表示します。

（「skip-test」のパラメータはオプションです。検証を実行しない場合にのみ、含めます。）

set live-data aw-access primary *addr port db user* [*skip-test*]

ステップ 3 以下のコマンドを実行して、セカンダリ AW DB を使用してライブ データを設定します。このコマンドは、ライブデータからの接続を自動的に検証して、ユーザの権限を確認し、結果を表示します。

（「skip-test」のパラメータはオプションです。検証を実行しない場合にのみ、含めます。）

set live-data aw-access secondary *addr port db user* [*skip-test*]
必要があれば、随時以下のコマンドを実行して、ライブデータからプライマリおよびセカンダリ AW DB に設定した AW 設定を表示して検証することができます。

（「skip-test」のパラメータはオプションです。検証を実行しない場合にのみ、含めます。）

show live-data aw-access [*skip-test*]

ライブ データ マシン サービスの設定

このコマンドは、ライブ データ マシン サービスが配置される AW を示します。

（注） set live-data machine-servicesを実行する際は常に、set live-data cuic-datasource を実行して、Unified Intelligence Center のライブ データ ソースを再設定します。Unified Intelligence Center データ ソースの設定 （105 ページ）を参照してください。

手順

ステップ 1 ライブ データ サーバにログインします。

ステップ 2 以下のコマンドを実行して、ライブ データ マシン サービスを設定します。

set live-data machine-services *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 ユーザを`user@domain` の形式で指定します。ドメインは完全修飾ドメイン名（FQDN）で、ユーザ名はユーザ プリンシパル名を使用します。ユーザは、Unified CCE 設定を変更する権限を持っていなければなりません。

（注）
- ライブ データをサポートする UCCE の導入には、ルータおよび周辺機器ゲートウェイ（PG）の TIP および TOS 接続情報が自動的に入力されます。
- Cisco Unified Communications Manager（CUCM）PG、CUCM 周辺機器を含む汎用 PG、 Unified CCE Gateway PG、Avaya PG は、ライブ データがサポートされています。

（注） ライブ データ サーバのホスト名を更新した後は、以下の一連のコマンドを再実行する必要があります。でないと、新しいホスト名は受け入れられません。

set live-data machine-services *awdb-user*

set live-data cuic-datasource *cuic-addr cuic-port cuic-user*

「show machine-services」のホスト名が変更されていることを確認します。

一連のコマンドを再実行しなければなりません。でないと、ライブデータ マシン サービスは新しいホスト名で更新されません。

Unified Intelligence Center データ ソースの設定

このコマンドは、ライブ データへのアクセス方法を Unified Intelligence Center に通知します。

手順

ステップ 1 ライブ データ サーバにログインします。

ステップ 2 以下のコマンドを実行して、Unified Intelligence Center ライブ データのデータ ソースを設定します。

set live-data cuic-datasource *cuic-addr cuic-port cuic-user*

ライブデータの再起動

AW、ライブ データ マシン サービス、および Unified Intelligence Center のデータ ソースの設定手順を完了したら、ライブ データ システムを再起動して変更を有効にします。

手順

CLI にアクセスして、以下のコマンドを実行します。

utils system restart

（注） ライブデータをサポートする新しい周辺機器ゲートウェイが導入され、作動する際、フィードはライブデータサーバで自動的に利用できなくなります。ライブデータ サーバを再起動して、新たに導入した周辺機器ゲートウェイからフィードを開始します。

ライブ データの証明書の設定

HTTPS を使用して Finesse サーバ、Cisco Unified Intelligence Center サーバ、Live Data サーバ間でセキュアな通信を行うには、セキュリティ証明書をセットアップする必要があります。Finesse サーバおよびCisco Unified Intelligence Centerサーバをライブ データ サーバと通信させるには、ライブ データ証明書と Cisco Unified Intelligence Center 証明書を Finesse にインポートし、ライブ データ証明書を Cisco Unified Intelligence Center にインポートする必要があります。詳細については、 Live Data の証明書を参照してください。

Cisco Identity Serviceの設定

Packaged 4000 エージェントから 12000 エージェント展開のための Cisco Identity Service 設定タスクの概要を以下の表に示します。

.

設定作業
自己署名付き証明書の詳細については、以下を参照してください。 AW マシンに IdS 証明書を追加します
シングル サインオン機能の設定については、https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.htmlの *Cisco Packaged Contact Center Enterprise* 機能ガイド を参照してください。

アイデンティティ プロバイダ（IdP）の設定

コンタクト センター ソリューションで SSO をサポートするには、セキュリティ アサーション マークアップ言語 2.0（SAML v2）Oasis 標準と互換性がある ID プロバイダ（IdP）をインストールして設定する必要があります。IdP はユーザ プロファイルを保存して認証サービスを提供し、SSO サインオンをサポートします。

このセクションでは、Microsoft AD FS の設定に関するサンプル情報を提供します。

以下の一連のタスクに従って、ID プロバイダを設定します。

手順	タスク
1	Active Directory フェデレーション サービスのインストールおよび設定 （106 ページ）
2	認証タイプを設定します。認証タイプ （107 ページ）を参照してください。
3	Cisco IdS の共有管理 AD FS への統合 （107 ページ）
4	SAML アサーションの署名の有効化 （109 ページ）
5	必要があれば、Windows Server 2012 R2 の AD FS のログイン ページをカスタマイズして、ユーザ ID を許可することもできます。 （110 ページ）

Active Directory フェデレーション サービスのインストールおよび設定

Microsoft の手順とガイドラインに従って、Microsoft Active Directory Federation Services（AD FS）をインストールします。

例えば、https://technet.microsoft.com/en-us/library/hh831502(v=ws.11).aspxの *Active Directory* フェデレーションサービスの概要 を参照してください。

（注） 以下の間の署名検証に使用されるセキュア ハッシュ アルゴリズム (SHA)。

- IdP および Cisco Id：SHA-1、SHA-256
- Cisco IdS およびアプリケーション ブラウザ：SHA-256

認証タイプ

Cisco Identity Service では、フォーム ベースの認証を提供するために ID プロバイダが必要です。

- Windows Server 2012 の AD FS で、認証タイプをフォーム ベースの認証（FBA）に設定します。以下の Microsoft TechNet の資料を参照してください。 http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx
- Windows 2012 R2 の AD FS で、認証ポリシーをフォーム認証に設定します。以下の Microsoft TechNet の資料を参照してください。 https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

Cisco IdS の共有管理 *AD FS* への統合

手順

ステップ 1 AD FS では、デフォルトの認証タイプが [フォーム] に設定されていることを確認します。（Cisco Identity Service では、フォーム ベースの認証を提供するために ID プロバイダが必要です。）詳細については、Microsoft AD FS のドキュメントを参照してください。

ステップ 2 AD FS サーバで、**AD FS 管理を開きます**。

ステップ 3 **AD FS** -> **信頼関係** -> **信頼当事者証明を右クリックします**。

ステップ 4 メニューで、**信頼当事者証明の追加** を選択して、**信頼当事者証明の追加ウィザード**を起動します。

ステップ 5 **データ ソースの選択** 手順で、**信頼当事者についてのデータをファイルからインポートする**オプションを選択します。

ステップ 6 Cisco Identity Server からダウンロードした `sp.xml` ファイルに**移動して**、インポートを完了し、信頼当事者の信頼を確立します。

ステップ 7 **表示名の指定**手順を選択し、信頼当事者証明を識別するために使用できる有意の名前を追加します。

ステップ 8 Windows Server 2012 R2 の AD FS の **今すぐ多要素認証を設定する**手順で、**この時点では信頼当事者の多要素認証設定を設定しない**オプションを選択します。

この手順は AD FS 2.0 または 2.1 では表示されません。以下の手順に進んでください。

ステップ 9 [発行認証規則の選択] 手順で、**すべてのユーザに対してこの信頼当事者へのアクセスを許可する** オプションを選択して、**次へ**をクリックします。

ステップ 10 **次へ** をもう一度クリックして、信頼当事者の追加を完了します。

ステップ 11 **信頼当事者証明** を右クリックして、**プロパティ**をクリックします。**識別子** タブを選択します。

ステップ 12 [識別子] タブで、**表示名** を信頼当事者証明の作成時に指定した名前に設定して、**信頼当事者識別子** を `sp.xml` をダウンロードした Cisco Identity Server の **完全修飾ホスト名** に設定します。

ステップ 13 さらに **プロパティ**で、**詳細設定** タブを選択します。

ステップ 14 **セキュア ハッシュ アルゴリズム** に **SHA-1** を選択して、**OK**をクリックします。

（注） 以下の手順では、2 つの要求ルールを設定して、AD FS から Cisco Identity Service に送信される要求を、正常な SAML アサーションの一部として指定します。

- アサーションには、次のカスタムクレームを含む要求ルールが属性ステートメントとして含まれています。
  - **uid**：アプリケーションに送信されるクレーム内の認証済みのユーザを識別します。
  - **user_principal**：Cisco Identity Serviceに送信されたアサーション内のユーザーの認証領域を識別します。
- 2 番目の要求ルールは、AD FS サーバと Cisco ID サーバの完全修飾ドメイン名を指定する NameID カスタム要求ルールです。

QoS を設定する手順は、以下の通りです。

ステップ 15 **信頼当事者証明**で、作成した信頼当事者証明を右クリックして、**要求ルールの編集**をクリックします。

ステップ 16 この手順に従って、**LDAP 属性を要求として送信する** で要求ルール テンプレートとしてルールを追加します。

a) **発行変換ルール** タブで、**ルールの追加**をクリックします。
b) **ルール タイプの選択** 手順で、**LDAP 属性をクレームとして送信する** の要求ルールテンプレートを選択して、**次へ**をクリックします。
c) **要求ルールの設定** 手順で、**要求ルール名** フィールドで、**NameID**を入力します。
d) **属性ストア** ドロップダウンを **Active Directory**に設定します。
e) **LDAP属性の発信要求タイプへのマッピング** テーブルを適切な **LDAP属性** に、使用するユーザ識別子タイプに応じた **発信要求タイプ** を設定します。

- 識別子が **SAM-Account-Name** 属性として保存される場合：
  1. **SAM-Account-Name**の **LDAP 属性**を選択し、対応する **発信要求タイプ** を **uid**（小文字）に設定します。
  2. **User-Principal-Name** の 2 つ目の **LDAP 属性** を選択して、対応する **発信要求タイプ** を **user_principal**（小文字）に設定します。
- 識別子が UPN の場合：
  1. **User-Principal-Name**の **LDAP 属性**を選択し、対応する **発信要求タイプ** を **uid**（小文字）に設定します。
  2. **User-Principal-Name** の 2 つ目の **LDAP 属性**を選択して、対応する **発信要求タイプ** を **user_principal**（小文字）に設定します。

（注） SAM-Account-Name または UPN の選択は、AW で設定したユーザ ID に基づきます。

ステップ 17 この手順に従って、**カスタム要求ルール**テンプレートで 2 つ目のルールを追加します。

a) **要求ルールの編集** ウィンドウで、**ルールの追加** を選択します。

b) **カスタム ルールを使用して要求を送信する**を選択します。

c) ルール名を Cisco Identity Server のパブリッシャ（プライマリ）ノードの **完全修飾ドメイン名（FQDN）** に設定します。

d) 以下のルール テキストを追加します。

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>
 issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",

 Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
 Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 =
 "http://<AD FS Server FQDN>/adfs/services/trust",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
 "<fully qualified domain name of Cisco IdS>");
```

e) スクリプトを以下の通りに編集します。

- **<ADFS Server FQDN>** を置き換えて、ADFS サーバの FQDN（完全修飾ドメイン名）と（大文字小文字の区別も含めて）完全に一致させます。
- **<Cisco IdS server FQDN>** を置き換えて、（大文字小文字の区別も含めて）Cisco Identity サーバの FQDN と完全に一致させます。

ステップ 18 [OK] をクリックします。

SAML アサーションの署名の有効化

信頼当事者証明（Cisco Identity Service）の SAML アサーションの署名を有効化します。

手順

ステップ 1 **スタート** をクリックして、**powershell** を [検索フィールド] に入力して、Windows Powershell を表示させます。

ステップ 2 Windows Powershell プログラム アイコンを右クリックして、**管理者として実行する**を選択します。

（注） このプロシージャ内のすべての PowerShell コマンドは、管理者モードで実行する必要があります。

ステップ 3 **Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Display Name> -SamlResponseSignature "MessageAndAssertion"**コマンドを実行します。

（注） <信頼当事者証明表示名> を、信頼当事者証明プロパティの識別子タブと（大文字と小文字を含めて）完全に一致させます。

必要があれば、*Windows Server 2012 R2* の *AD FS* のログイン ページをカスタマイズして、ユーザ *ID* を許可することもできます。

デフォルトでは、Windows Server 2012 R2 内の AD FS によって SSO ユーザに表示されるサインインページには、UPN であるユーザ名が必要となります。通常これは、例えば、user@Cisco.com という電子メールの形式です。コンタクトセンターソリューションが単一ドメイン内にある場合は、サインインページを変更して、ユーザ名の一部としてドメイン名を含まない単純なユーザ ID をユーザが入力できるようにすることができます。

AD FS サインイン ページをカスタマイズするには、数種類の方法を使用できます。代替ログイン ID を設定して、AD FS サインイン ページをカスタマイズする方法の詳細と手順については、Windows Server 2012 R2 ドキュメントの Microsoft AD FS を参照してください。

以下の手順は、1 つのソリューションの例です。

手順

ステップ 1 [AD FS] の **信頼当事者証明**で、選択した LDAP 属性を **uid** にマップするように [NameID 要求ルール] を変更します。

ステップ 2 Windows の **スタート** コントロールをクリックして、**powershell** を [検索フィールド] に入力して、Windows Powershell を表示させます。

ステップ 3 Windows Powershell プログラム アイコンを右クリックして、**管理者として実行する**を選択します。

このプロシージャ内のすべての PowerShell コマンドは、管理者モードで実行する必要があります。

ステップ 4 SAMAccountName を使用して AD FS へのサインインを許可するには、以下の Powershell コマンドを実行します。

```
Set-AdfsClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID
sAMAccountName -LookupForests myDomain.com
```

LookupForests パラメータ内で、ユーザが所属するフォレスト DNS を `myDomain.com` に置き換えます。

ステップ 5 以下のコマンドを実行して、テーマをエクスポートします。

```
mkdir C:\themeExport-AdfsWebTheme -Name default -DirectoryPath c:\theme
```

ステップ 6 C:\theme\script の onload.js を編集して、以下のコードをファイルの最後に追加します。このコードはテーマを変更し、AD FS のサインイン ページでユーザ名にドメイン名またはアンパサンド ("@") が必要としないようにします。

```
// Update the placeholder text to not include the domain
var userNameInput = document.getElementById("userNameInput");
if (userNameInput) {
 userNameInput.setAttribute("placeholder", "Username");
}

// Override submitLoginRequest to not have the "@" check
Login.submitLoginRequest = function () {
 var u = new InputUtil();
 var e = new LoginErrors();
 var userName = document.getElementById(Login.userNameInput);
 var password = document.getElementById(Login.passwordInput);
 if (!userName.value) {
  u.setError(userName, e.userNameFormatError);
  return false;
 }
 if (!password.value) {
  u.setError(password, e.passwordEmpty);
  return false;
 }
 document.forms['loginForm'].submit();
 return false;
};
```

ステップ 7 Windows PowerShell で以下のコマンドを実行して、テーマを更新し、有効化します。

```
Set-AdfsWebTheme -TargetName custom -AdditionalFileResource
@{Uri='/adfs/portal/script/onload.js';path="c:\theme\script\onload.js"}

Set-AdfsWebConfig -ActiveThemeName custom
```

Cisco Identity Service の設定

Cisco Identity Service（Cisco IdS）は、ID プロバイダ（IdP）とアプリケーションの間で認証を提供します。

Cisco IdS を設定する場合は、Cisco IdS と IdP の間のメタデータ交換を設定します。この信頼関係により、アプリケーションは SSO に Cisco IdS を使用することができます。この信頼関係は、Cisco IdS からメタデータ ファイルをダウンロードし、IdP にアップロードすることで構築します。その後、セキュリティに関連する設定の選択、Cisco IdS サービスのクライアントの識別、ログ レベルの設定を行うことができます。必要があれば、Syslog 形式を有効にすることができます。

（注） Cisco IdS クラスタを使用している場合は、Cisco IdS プライマリ パブリッシャ ノード上で以下の手順を実行します。

Packaged CCE 4000 エージェントまたは 12000 エージェントを導入する場合は、Unified CCE 管理でシングル サインオン ツールを使用する前に、プリンシパル AW が設定され、機能していることを確認してください。また、SSO 対応のマシンをインベントリに追加し、各 SSO 対応マシンのデフォルトの Cisco IdS を選択します。詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html で、*Cisco Packaged Contact Center Enterprise* 機能ガイド 中の **シングル サインオンのシステム インベントリの設定** セクションを参照してください。

手順

ステップ 1 Unified CCE 管理で、**概要** > **インフラストラクチャの設定** > **デバイスの設定** > **シングル サインオンの設定**を選択します。

（注） *username@FQDN*形式のログイン名を使用して、Unified CCE 管理にログインします。

アイデンティティ サービスのノード、**アイデンティティ サービスの設定** および **アイデンティティ サービスのクライアント** タブが表示されます。

ステップ 2 **アイデンティティ サービス**をクリックします。
全体的なノード レベルを表示して、どのノードがサービスに所属しているかを特定することができます。各ノードの **SAML 証明書の有効期限** の詳細を表示して、証明書の有効期限が切れる期日を確認することもできます。ノードの **ステータス** オプションには、**未設定**、**稼働中**、**一部稼働中**、および**不使用**があります。詳細については、[ステータス]をクリックしてください。ノード名の右側にある星印は、プライマリ パブリッシャであるノードを示します。

ステップ 3 **アイデンティティ サービスの設定**をクリックします。

ステップ 4 **IdSの信頼性**をクリックします。

ステップ 5 Cisco IdS と IdP 間の Cisco IdS 信頼関係を設定するには、**メタデータ ファイルのダウンロード** をクリックして、Cisco IdS サーバからファイルをダウンロードします。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 信頼メタデータ ファイルを IdP からアップロードするには、ファイルを検索して特定します。IdP へのパスが含まれる **メタデータのアップロード** ページが開きます。ファイルのアップロードが完了すると、通知メッセージが表示されます。これでメタデータの交換が完了し、信頼関係が確立されます。

ステップ 8 [セキュリティ（Security）] をクリックします。

ステップ 9 **トークン**をクリックします。
以下の設定の期間を入力します。

- **トークンの有効期限の更新**：デフォルト値は 10 時間です。最小値は 2 時間です。最大値は 24 時間です。

- **承認コードの有効期限**：デフォルト値は 1 分で、これが最小値となります。最大値は 10 分です。
- **アクセス トークンの有効期限**：デフォルト値は 60 分です。最小値は 5 分です。最大値は 120 分です。

ステップ 10 **暗号化トークン**（オプション）：デフォルト設定は **オン**です。

ステップ 11 **[保存（Save）]** をクリックします。

ステップ 12 **キーおよび証明書**をクリックします。
キーおよびSAML 証明書の生成 ページが開き、以下が可能になります。

- **再生成**をクリックして、**暗号化および署名キー**を再生します。トークンの登録が正常に完了したというメッセージが表示され、設定を完了するためにシステムを再起動するように勧められます。
- **再生成**をクリックして、**SAML 証明書** を再生成します。SAML 証明書の再生成が正常に行われたというメッセージが表示されます。

ステップ 13 **[保存（Save）]** をクリックします。

ステップ 14 **アイデンティティ サービス**をクリックします。
Identity Service クライアント タブには、クライアント名、クライアント ID、およびリダイレクト URL を含む既存の Cisco IdS クライアントが表示されます。特定のクライアントを検索するには、名前の一覧の上部にある検索アイコンをクリックして、クライアント名を入力します。

ステップ 15 **Identity Service クライアント** タブでのクライアントの追加：

a) [新規（New）] をクリックします。
b) クライアントの名前を入力します。
c) リダイレクト URL を入力します。複数の URL を追加するには、プラスのアイコンをクリックします。
d) **追加**をクリックします（もしくは**クリア**をクリックして、「X」をクリックして、クライアントを追加せずにページを閉じます）。

ステップ 16 クライアントを編集または削除するには、クライアントの行を強調表示して、**アクション**の下の省略記号をクリックします。実行されるアクション

- **編集** をクリックして、クライアントの名前、ID、またはリダイレクト URL を編集します。**クライアント編集** ページで、変更を行い、**保存** をクリックします（もしくは **クリア** をクリックして、変更を保存せずにページを閉じます）。
- **削除** をクリックしてクライアントを削除します。

ステップ 17 **アイデンティティ サービスの設定**をクリックします。

ステップ 18 **トラブルシューティング** をクリックして、オプションのトラブルシューティングを実行します。

ステップ 19 **ログ レベル** ドロップダウンリストで、ロジカル ログのレベルを **エラー**、**警告**、**情報**（デフォルト値）、**デバッグ**、もしくは **トレース**から選択します。

ステップ 20 Syslog形式のエラーを受信するには、リモートSyslogサーバ名を**ホスト**（オプション）フィールドに入力します。

ステップ 21 **[保存（Save）]** をクリックします。

次の作業に進んでください。

- Cisco IdS を使用してコンポーネントを登録します。
- 展開全体の SSO を有効（または無効）にします。

コンポーネントを登録して、シングル サインオン モードを設定します。

コンポーネントを Cisco IdS に登録した後に、SSO 互換マシンをシステム インベントリに追加すると、それらのマシンは自動的に登録されます。

始める前に

- Cisco Identity Service（Cisco IdS）の設定
- ポップアップブロッカーを無効にします。これは、すべてのテスト結果を正しく表示するために行う必要があります。
- Internet Explorerを使用している場合は、互換モードでないこと、およびAWの完全修飾ドメイン名を使用して、CCE 管理にアクセスしていることを確認します（例えば、**https://fully-qualified-name.com/cceadmin**）。

手順

ステップ 1 Unified CCE 管理で、**概要** > **インフラストラクチャ設定** > **デバイス設定** > **シングル サインオンのセットアップ**に移動します。

ステップ 2 Unified CCE管理のシングルサインオンツールで、**登録**ボタンをクリックして、すべてのSSO互換コンポーネントを Cisco IdS に登録します。

コンポーネントステータステーブルに、各コンポーネントの登録ステータスが表示されます。

コンポーネントの登録に失敗した場合は、エラーを修正して、**再試行**をクリックします。

ステップ 3 [テスト（Test）] ボタンをクリックします。新しいブラウザ タブが開くと、証明書を承認するためのプロンプトが表示されることがあります。ページをロードするためには、すべての証明書を承認します。次に、[ログイン]ダイアログボックスが表示されたら、SSOクレデンシャルを持つユーザとしてログインします。

テスト プロセスでは、各コンポーネントが正しく設定されていて ID プロバイダーにアクセスできること、および Cisco IdS によってアクセス トークンが正常に生成されることが確認されます。SSO に対してセットアップしている各コンポーネントがテストされます。

コンポーネント ステータス テーブルに、各コンポーネントのテスト ステータスが表示されます。

テストが失敗した場合は、エラーを修正して、再度 **テスト** をクリックします。

テスト結果は保存されません。ページを更新した場合は、SSO を有効にする前に、再度テストを実行します。

ステップ 4 [モードの設定（Set Mode）] ドロップダウン メニューから、システムの SSO モードを選択します。

- [非 SSO（Non-SSO）]：このモードでは、すべてのエージェントとスーパーバイザの SSO が無効になります。ユーザは、既存の Active Directory ベースの認証およびローカル認証を使用します。
- [ハイブリッド（Hybrid）]：このモードでは、エージェントとスーパーバイザの SSO を選択的に有効にできます。
- [SSO]：このモードでは、すべてのエージェントとスーパーバイザに対して SSO が有効になります。

コンポーネント ステータス テーブルに、各コンポーネントの SSO モードの設定ステータスが表示されます。

コンポーネントの SSO モードの設定に失敗した場合は、エラーを修正して、再度モードを選択します。

Packaged CCE 12000 エージェント展開

Packaged CCE 12000 エージェント展開のコンポーネントを設定するには、以下の手順を実行します。

手順	タスク
1	CCE コンポーネントの設定 （116 ページ）
2	Cisco Unified Customer Voice Portal の設定 （87 ページ）
3	外部メディア サーバの場合、メディア サーバの設定
4	Cisco Unified Communications Manager の設定 （90 ページ）
5	Cisco Unified Intelligence Center の設定 （96 ページ）

手順	タスク
6	Cisco Finesse の設定 （97 ページ）
7	ライブ データの設定 （102 ページ）
8	Cisco Identity Serviceの設定 （105 ページ）
9	Cisco Unified Customer Voice Portal Reporting Server の設定 （44 ページ） （任意）
10	VVB の設定 （48 ページ） （任意）
11	Cisco IOS Enterprise 音声ゲートウェイの設定 （49 ページ）
12	IPv6 を設定する （56 ページ）
13	エンタープライズ チャットおよび電子メール（ECE）の設定（オプション） 電子メールおよびチャット

CCE コンポーネントの設定

Packaged CCE 12000 エージェント展開のコンポーネントを設定するには、以下の手順を実行します。

手順	タスク
1	ロガーの設定 （117 ページ）
2	ルータの設定 （117 ページ）
3	AW-HDS の設定 （118 ページ）
4	HDS-DDS の設定 （118 ページ）
5	Unified CCE サービスの開始 （72 ページ）
6	PG VM がインストールされている場合は、すべての PG VM に対してUnified CCE インスタンスの追加 （82 ページ）
7	Packaged CCE の展開タイプの設定 （76 ページ）
8	Cisco Unified Contact Center Enterprise PG の設定 （82 ページ）

手順	タスク
9	Configuration Managerを使用した設定については、以下を参照してください。 PCCE 4000 または 12000 でサポートされるツール
10	CA 署名証明書の詳細については、以下を参照してください。 AW マシンに CA 署名付き証明書を生成してインポートする
11	自己署名付き証明書の詳細については、以下を参照してください。 AWマシンで自己署名証明書を生成してインポートする

ロガーの設定

Packaged CCE 12000 エージェント展開のロガーを設定するには、以下の手順を実行します。

手順	タスク
1	CCE コンポーネント用 SQL Server の設定 （2 ページ）
2	組織ユニットの設定 （3 ページ）
3	Unified CCE インスタンスの追加 （82 ページ）
4	ロガー データベースの作成 （68 ページ）
5	アウトバウンド オプションを使用するには、以下を参照してください。 アウトバウンド オプション データベースの作成 （69 ページ）
6	ロガー コンポーネントのインスタンスへの追加 （69 ページ）
7	ICM データベース ルックアップの設定 （119 ページ） （任意）
8	Cisco SNMP の設定 （21 ページ） （任意）

ルータの設定

Packaged CCE 12000 エージェント展開のルータを設定するには、以下の手順を実行します。

手順	タスク
1	Unified CCE インスタンスの追加 （82 ページ）

手順	タスク
2	ロガー コンポーネントのインスタンスへの追加 （71 ページ）
3	ICM データベース ルックアップの設定 （119 ページ） （任意）
4	Cisco SNMP の設定 （21 ページ） （任意）

HDS-DDS の設定

Packaged CCE 12000 エージェント展開の HDS-DDS を設定するには、以下の手順を実行します。

手順	タスク
1	CCE コンポーネント用 SQL Server の設定 （2 ページ）
2	Unified CCE インスタンスの追加 （82 ページ）
3	HDS データベースの作成 （73 ページ）
4	管理およびデータ サーバ コンポーネントのインスタンスへの追加 （74 ページ）
5	ICM データベース ルックアップの設定 （119 ページ） （任意）
6	Cisco SNMP の設定 （21 ページ） （任意）

AW-HDS の設定

Packaged CCE 12000 エージェント展開の AW-HDS を設定するには、以下の手順を実行します。

手順	タスク
1	CCE コンポーネント用 SQL Server の設定 （2 ページ）
2	Unified CCE インスタンスの追加 （82 ページ）
3	HDS データベースの作成 （73 ページ）
4	管理およびデータ サーバ コンポーネントのインスタンスへの追加 （74 ページ）

手順	タスク
5	ICM データベース ルックアップの設定 （119 ページ） （任意）
6	Cisco SNMP の設定 （21 ページ） （任意）

ICM データベース ルックアップの設定

Configuration Managerのデータベース ルックアップ EXPLORER ツールを使用して、外部データベースのスクリプト テーブルを表示、定義、削除、または編集することができます。

ICM データベース ルックアップを設定するには、以下の手順を実行します。

手順

ステップ 1 Unified CCE Web セットアップ ツールを起動します。

ステップ 2 [ルータのオプション] ウィンドウで、**データベース ルーティングを有効にする** を選択します。

ステップ 3 データベース ルックアップ EXPLORERの設定：

a) **スタート** > **すべてのプログラム** > **Cisco Unified CCE ツール** > **管理ツール** > **Configuration Manager**をクリックします。

b) **ツール** > **EXPLORER ツール** > **データベース ルックアップ EXPLORER を開きます。**

c) 以下の例に示される通りに、スクリプトテーブルとスクリプトテーブル列を設定します。

スクリプト テーブル：

```
名前：AccountInfo
サイド A：\\dblookup1\DBLookup.AccountInfo
サイド B：< データベースのサイド B をここで更新>
説明：<ここに説明を入力>
```

dblookup1 は外部データベースサーバ名、DBLookup は外部データベース名、AccountInfo はテーブル名です。

スクリプト テーブルの列:

```
列名：AccountNo
説明：<ここに説明を入力>
```

ステップ 4 Unified CCE のレジストリ設定を変更するには、以下の設定を行います。

a) **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems, Inc. > ICM > <インスタンス名 > > RouterA > Router > CurrentVersion > Configuration > Database registry**に移動します。

インスタンス名 は、設定するインスタンスの名前です。

b) 以下の例の通り SQLLogin レジストリキーを設定します。

例：

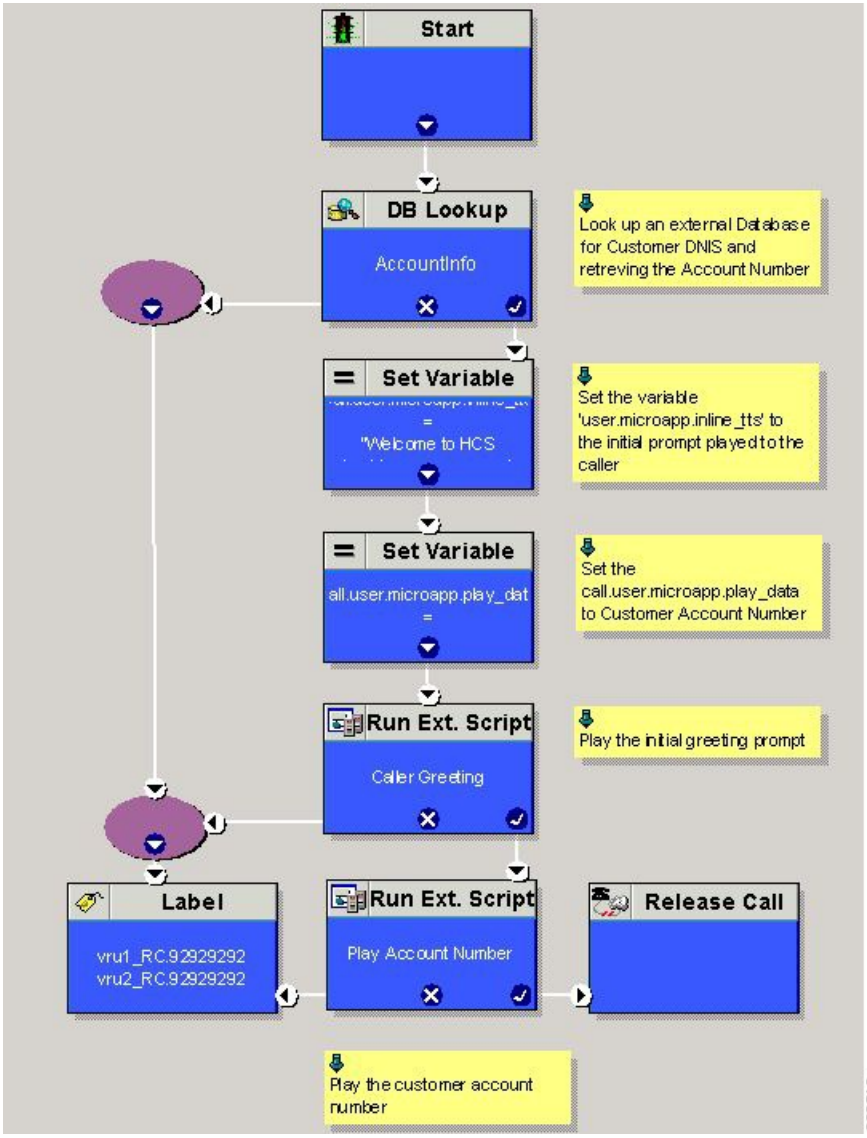
```
\\dblookup1\DBLookup=(sa,sa)
```

DBLookup は、外部データベース名、（sa, sa）は SQL サーバ認証です。

ステップ 5 対応するテーブルとルックアップ値を含むデータベース ルックアップ ノードを含む ICM スクリプトを作成します。

下の図は、ルックアップ値としてのテーブル名および CallingLineID としての AccountInfo を示しています。

図 *1 : ICM* データベース ルックアップの例



Packaged CCE Lab Only 展開

Packaged Contact Center Enterprise（Packaged CCE）の機能を試験的に使用するには、Packaged CCE Lab 導入を使用します。

Unified CCE 管理 Web ベースのツールを使用してコンタクト センターの操作を設定および管理する手順については、Packaged CCE 管理を参照してください。

次の Unified CCE Administration 機能は、Packaged CCE Lab 導入に変更した時点では最初は利用することができません。

- **インベントリ** ページで利用可能なシステム インベントリ
- ログ収集（Log Collection）
- ライブ データ
- シングル サインオン（Single sign-on）

Packaged CCE Lab Only 導入

Packaged CCE Lab Only 導入では、2000 エージェントを展開する場合にのみ、シンプレックス システムまたはデュプレックス システムとして設定することができます。シンプレックス システムでは、すべてのコンポーネントがサイド A に取り付けられており、サイド B は存在しません。デュプレックス システムでは、コンポーネントはサイド A およびサイド B にインストールされます。

シンプレックス モード

Lab Only のシンプレックス導入は、以下のコンポーネントで構成する必要があります。

- Unified CCE Rogger1
- Unified CCE AW-HDS-DDS 1
- Unified CCE PG 1
- Unified CVP サーバ 1

（注） Unified CCE 管理で展開を初期化した後、Unified CVP サーバを再起動する必要があります。

- Cisco Unified CM 1、パブリッシャとサブスクライバを一が統合された機能
- Cisco Unified Intelligence Center 1、パブリッシャとサブスクライバが統合された機能
- Cisco Finesse 1 は、パブリッシャとしてもサブスクライバとしても機能

- 0 個以上のゲートウェイ
- Cisco SocialMiner 0 個以上
- Cisco Unified CVP Reporting 0 個以上
- Cisco MediaSense 0 個以上
- Cisco 0 個以上 エンタープライズ チャットおよび電子メール
- サードパーティ マルチチャネル 0 個以上

（注） システム インベントリでは、Packaged Contact Center Enterprise Lab Only 外のマシンに適用されるステータス ルールは、Lab Only の展開によって、ブロックされたステータスを返します。ESXi ホストが必要なステータス ルールはブロックのステータスを返します。

メイン サイトとリモート サイトの場合は、以下の外部マシンを追加することができます。

- Cisco Virtualized Voice Browser 0 個以上
- Cisco Unified SIP Proxy 0 個以上
- ゲートウェイ 0 個以上
- MediaSense 0 個または 1 個

（注） MediaSense は、メイン サイトに対してのみ追加することができます。

- Cisco SocialMiner 0 個または 1 個
- Cisco Unified CVP Reporting 0 個または 1 個
- Cisco Enterprise チャットおよび電子メール 0 個または 1 個
- サードパーティ マルチチャネル 0 個または 1 個

二重モード（Duplex Mode）

Lab Only デュプレックスは、以下のコンポーネントで構成されています。

（注） Lab モードでは、CCE をパッケージしても、ESXi ホストは検証されません。

サイド A

サイド A には、以下が必要です。

- Unified CCE Rogger 1 個
- Unified CCE AW-HDS-DDS 1 個
- Unified CCE PG 1 個
- Cisco Unified CVP サーバ 1 台
- Unified Communications Manager パブリッシャ 1 個
- Unified Communications Manager サブスクライバ 1 個
- Unified Intelligence Center パブリッシャ 1 個
- Finesse プライマリ 1 個

サイド B

サイド B には、以下が必要です。

- Unified CCE Rogger 1 個
- Unified CCE AW-HDS-DDS 1 個
- Unified CCE PG 1 個
- Cisco Unified CVP サーバ 1 台
- Unified Communications Manager サブスクライバ 1 個
- Unified Intelligence Center サブスクライバ 1 個
- Finesse セカンダリ 1 個

External

Lab Only デュプレックス モードでは、以下の外部マシンを使用することができます。

- 0 個以上のゲートウェイ
- Cisco Virtualized Voice Browser 0 個または 1 個
- Cisco Unified SIP Proxy 0 個以上
- SocialMiner 0 個または 1 個
- Cisco Enterprise チャットおよび電子メール 0 個または 1 個
- Unified CVP Reporting 0 個または 1 個
- MediaSense 0 個または 1 個
- サードパーティ マルチチャネル 0 個または 1 個

（注） ESXi ホストが必要なステータス ルールはブロックのステータスを返します。

リモート サイトの場合は、以下の外部マシンを追加することができます。

- Cisco SocialMiner 0 個または 1 個
- Cisco Unified CVP Reporting 0 個または 1 個
- Cisco Enterprise チャットおよび電子メール 0 個または 1 個
- サードパーティ マルチチャネル 0 個または 1 個
- ゲートウェイ 0 個以上
- Cisco Virtualized Voice Browser 0 個以上
- Cisco Unified SIP Proxy 0 個以上

Packaged CCE Lab モード導入の初期化

Unified CCE Administration に初めてログインすると、導入のコンポーネントの情報とクレデンシャルを入力するように求められます。Packaged CCE はこの情報を使用して、コンポーネントを設定し、システム インベントリを構築します。

手順

ステップ 1 **インベントリ** ページの **展開タイプ** ドロップダウンリストで **Packaged CCE: Lab Mode** を選択し、ドメイン マネージャを使用して作成したインスタンスを **インスタンス** ドロップダウンリストから選択します。[次へ（Next）] をクリックします。

ステップ 2 **テンプレート** ドロップダウンリストの以下のオプションからいずれか一つを選択します。

- シンプレックス Lab Mode 展開の シンプレックス インベントリ
- デュプレックス Lab Mode 展開のデュプレックス インベントリ

ダウンロード をクリックして、インベントリ コンテンツ ファイル テンプレートをダウンロードします。必要事項を入力し、コンピュータにテンプレートを保存します。目的の [コンテンツファイル（Content File）] フィールドで、完了したコンテンツ ファイルを参照します。インベントリが作成される前に、コンテンツ ファイルが検証されます。[次へ（Next）] をクリックします。

インベントリ コンテンツ ファイル テンプレートの入力の詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html の *Cisco Packaged Contact Center Enterprise* 管理およびコンフィギュレーション ガイド を参照してください。

ステップ 3 [設定（Settings）] ページで、以下の手順を実行します。

- [Mobile Agentコーデック（Mobile Agent Codec）] ドロップダウン リストから、Mobile Agent コールに使用するコーデックを選択します。Lab Only 展開では、**サイド A 接続** および **サイド B 接続**ドロップダウン リストは無効化されています。
- **サービス アカウントの自動作成**チェック ボックスで、以下のいずれかを選択します。
  - 自動初期化タスクで Active Directory にサービス アカウントを作成するには、このチェック ボックスをオンのままにします。

    作成されたアカウントはサービス グループに追加されます。
  - 既存の Active Directory アカウントを使用する場合は、このチェック ボックスをオフにします。Packaged CCE サーバと同じドメインに既存の Active Directory ユーザのユーザ名とパスワードを入力します。

    このアカウントはサービス グループに追加されます。

[次へ（Next）]をクリックします。

導入が初期化されます。[詳細（Details）] ダイアログボックスに自動初期化タスクのステータスが表示されます。

ステップ 4 自動初期化タスクが完了したら、[完了（Done）] をクリックします。

自動初期化タスクのいずれかが失敗した場合は、エラーを修正して [再試行（Retry）] をクリックします。

再試行が成功した場合は、自動初期化が続行されます。

一部のタスクが失敗した場合は、完了済みのすべてのタスクを再試行以前の状態に戻してから再試行する必要があります。このとき、システムを正常な状態に戻す必要があることを通知するメッセージが表示されます。

[OK] をクリックし、システムが正常な状態になったら、[やり直す（Start Over）] をクリックします。

（注） Unified CVP サーバは再起動すべきです。

シンプレックスまたはデュプレックスのラボ モード展開を実行した後、**インベントリ** ページで、メイン サイトに以下の外部マシンを追加することもできます。

- Unified CM パブリッシャ
- Unified CVP Reporting Server
- Unified SIP Proxy
- Virtualized Voice Browser
- ゲートウェイ
- SocialMiner
- MediaSense
- エンタープライズ チャットおよび電子メール

- サードパーティ マルチチャネル

メイン サイトの外部マシンを追加、編集、または削除する手順は、Packaged CCE 2000 エージェント展開のシステム インベントリ （10 ページ）を参照してください。

インベントリコンテンツファイルを使用したシステムインベントリ、ログ収集、ライブ データの有効化

以下の Unified CCE 管理機能をデモで使用するには、導入環境内のマシンの情報および資格情報を含む Packaged CCE を提供する必要があります。

- システム インベントリ（**インベントリ** ページで利用可）
- ログ収集（Log Collection）
- ライブ データ
- シングル サインオン

この情報は、インベントリ コンテンツファイルを使用して指定します。

インストール プロセスの一部として、Packaged CCE Only 展開を Unified CCE Administration 内に設定している場合は、インベントリのコンテンツ ファイルの入力を完了して、アップロードするように要求されます。

その他の展開から Packaged CCE Lab Only の展開に切り替える場合、一括 インポートツールでコンテンツ インベントリ ファイルの入力を完了してアップロードされます。

一括インポートでコンテンツ インベントリ ファイルの入力を完了してアップロードする手順は、以下の通りです。

手順

ステップ 1 Unified CCE Web 管理で、に移動して、**概要** ページの**一括インポート** カードをクリックします。インベントリ コンテンツ ファイル テンプレートをダウンロードします。

ステップ 2 Microsoft Excel でファイルを開いて、[インベントリ コンテンツ ファイル] の説明に従ってコンテンツ ファイル フィールドに入力します。

ステップ 3 変更を保存します。

ステップ 4 **一括ジョブ**で新しい一括ジョブを作成します。**コンテンツ ファイル** フィールドで、作成したインベントリ コンテンツ ファイルを選択して **保存**をクリックします。

関連トピック

一括ジョブの管理

インベントリ コンテンツ ファイル

インベントリ コンテンツ ファイル テンプレートには、以下のフィールドが含まれています。

（注） ユーザ名とパスワードに「=」または「&」文字が含まれている場合は、「% 3d」のエンコードされた値または「% 26」を使用します。

フィールド	説明
operation	デフォルトは「作成」です。この操作は変更しないでください。
名前（Name）	マシン名は変更しないでください。 （注） このフィールドは、デュプレックス モードにのみで適用されます。
machineType	マシン タイプは変更しないでください。
publicAddress	各マシンのパブリック IP アドレスを入力します。

フィールド	説明
publicAddressServices	**CCE_ROGGER** : このフィールドは変更しないでください。 **CCE_PG** : このフィールドでは、 Unified CCE PG に必要なサービスを指定します。UCM PG のロジカル コントローラ ID がデフォルトの 5000 ではない場合は、TIP_PG サービスと TIP_PG_TOS サービスのペアリング値を、ロジカル コントローラ ID と一致するように変更します。（ロジカル コントローラ ID は、[システム > 情報] の周辺機器ゲートウェイのタブにあります。） **CCE_AW** : このフィールドでは、Unified CCE の診断フレームワークのクレデンシャルを指定します。インスタンスの設定セキュリティ グループのメンバーであるドメイン ユーザのクレデンシャルを使用して user@domain.com とパスワードを置き換えます。クレデンシャルは、展開内のすべての Unified CCE マシンで有効になっている必要があります。 **CVP** : このフィールドには、Unified CVP のクレデンシャルを指定します。 **CM_PUBLISHER** : このフィールドには、AXL クレデンシャルを指定します。ユーザとパスワードを正しいクレデンシャルに置き換えます。 **CUIC_PUBLISHER** : このフィールドでは、Unified Intelligence Centerのサービスを指定します。管理者のクレデンシャルと Cisco Identity Service のクレデンシャルについては、ユーザとパスワードを正しいクレデンシャルに置き換えます。その他のすべてのサービスについては、デフォルト値を変更しないでください。 **FINESSE** : このフィールドでは、FINESSE 管理者の資格情報を指定します。ユーザとパスワードを正しいクレデンシャルに置き換えます。
privateAddress	**CCE_PG** および **CCE_ROGGER** のプライベート IP アドレスを入力します。他のすべてのマシンに対してこのフィールドを空白のままにします。

フィールド	説明
side	サイド A または サイド B を入力します。