Cisco BE6000 による Collaboration Edge

テクノロジー設計ガイド

2014 年 4 月

目次

このマニュアルについて

シスコ検証済みデザイン（CVD）は、一般的な使用例や現在のエンジニアリング システムの優先事項に基づいてシステム設計を行う際の基盤となります。CVD には、お客様のニーズに応えるために、幅広いテクノロジー、機能、アプリケーションが組み込まれています。シスコのエンジニアは、より早く、信頼性の高い、想定できる内容で導入できるように、各 CVD の包括的なテストと文書化を実施しています。

テストと検証が完了している設計および導入の詳細を提供するために、CVD には 2 種類のガイドが含まれています。

- **テクノロジー設計ガイド**には、導入の詳細、検証済み製品およびソフトウェアについての情報、および特定のテクノロジーに関するベスト プラクティスが記載されています。
- **ソリューション設計ガイド**には、既存の CVD のまとめや参照のほか、シスコ製品の特徴や機能も記載されています。また、サードパーティ統合についての情報も含まれます。

シスコのパートナーやお客様はこれら 2 種類の CVD を活用し、テスト済みの成果に基づいて、独自の設定と構成でシステム設計と導入を開始できます。

コマンドの読み方

CVD の多くに、ネットワーク デバイスを設定するためのコマンドライン インターフェイス（CLI）の使用方法が記載されています。ここでは、入力する必要のあるコマンドを記載する際の表記規則について説明します。

CLI で入力するコマンドは、次のように表記します。

```
configure terminal
```

変数に値を指定するコマンドは、次のように表記します。

```
ntp server 10.10.48.17
```

ユーザ側で定義する変数を伴うコマンドは、次のように表記します。

```
class-map [highest class name]
```

CLI またはスクリプト プロンプトでのコマンドは、次のように表記します。

```
Router# enable
```

行が折り返される長いコマンドには下線が引かれています。これらを 1 つのコマンドとして入力します。

```
police rate 10000 pps burst 10000 packets conform-action set-discard-
class- transmit 48 exceed-action transmit
```

システム出力またはデバイス コンフィギュレーション ファイルの重要な部分は、次のように強調表示されています。

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

コメントと質問

ガイドについてコメントや質問がある場合は、フィードバック フォームを使用してください。

最新の CVD ガイドについては、次のサイトを参照してください。

http://www.cisco.com/go/cvd/collaboration

CVD Navigator

CVD Navigator には、使用例、テクノロジーの対象範囲、推奨される習熟度や経験、本ガイドに関連する CVD などがまとめられているので、本ガイドを適用できるかどうかを判断する際に役立ちます。このセクションは、クイック リファレンスとなっています。詳細については、「はじめに」を参照してください。

使用例

本ガイドでは、次のテクノロジー使用例を扱っています。

- Mobile & Remote Access と、デスクトップおよび多目的ルーム システムによる Business-to-Business（B2B）コラボレーション - 組織は、フェイスツーフェイスのメリットを失うことなく、リモートの人員から予算や生産性のメリットを得ることを望んでいます。従業員がリモートで仕事をする際に、慣れている対面式のやりとりを同僚や上司と交わせる柔軟性を望んでいます。また、コラボレーションの利点を拡張して、パートナー/サプライヤや顧客との Business-to-Business（B2B）の対話を効果的に行いたいと考えています。

詳細については、本ガイドの「使用例」を参照してください。

対象範囲

このガイドでは、以下の分野のテクノロジーと製品を扱います。

- ユニファイド コール エージェント
- デスクトップ ビデオ エンドポイントとモバイル クライアント
- 多目的ルーム システム
- コラボレーション エッジ システム
- Session Initiation Protocol（SIP）シグナリング

詳細については、本ガイドの「設計の概要」を参照してください。

習熟度

本ガイドは、次の技術的習熟度、またはそれに相当する経験を持つ人を対象としています。

- CCNA Video：音声デバイスおよび 1 画面ビデオ エンドポイントの設定、テレフォニーおよびビデオのアプリケーションのサポート、およびトラブルシューティングの経験 1 ～ 3 年。
- CCNA Voice：音声およびユニファイド コミュニケーションのアプリケーション、デバイス、およびネットワークに関する設計、インストール、およびトラブルシューティングの経験 1 ～ 3 年。

関連する CVD ガイド

『Cisco Preferred Architecture for Collaboration（シスコが推奨するコラボレーション用アーキテクチャ）』

『Unified Communications Using Cisco BE6000 Technology Design Guide（Cisco BE6000 を使用したユニファイド コミュニケーション テクノロジー設計ガイド）』

『Cisco BE 6000 を使用したビデオ会議』

関連する CVD ガイドを確認するには、各タイトルをクリックするか、以下のサイトを参照してください。
http://www.cisco.com/go/cvd/collaboration

はじめに

モビリティの台頭により、チーム、従業員、お客様が互いにつながり、コラボレーションするための新たな手法が生まれています。この新しい世界で成功を収める鍵は、どのような環境でもオープンでアクセスしやすいコミュニケーションを確立することです。物理的なオフィス、フェイスツーフェイスのビデオ通話、音声通話、Cisco Jabber 等による接続のいずれにも制約されないことが重要です。今日の組織には、モバイル ワーカーのサポートとして、モビリティを中心に設計されたコラボレーション テクノロジーを提供できることが求められます。

コラボレーションにビデオを組み合わせることで、ユーザの意思疎通のレベルが高まります。インターネットを利用してこのような機能をモバイル ユーザに提供する手法が、ここ数年で急増しています。多くの組織にとって、接続性は、日常業務を遂行するうえでの基本的な要件になっています。さらに、モバイル ワーカーやリモート サイト ワーカー同士、または本社への安全な接続は、組織がビジネス目標を達成するために欠かせない機能となっています。

シスコのリモート ワーカー向けソリューションは、以前から VPN クライアントを利用して、企業ネットワークにセキュアなトンネルを提供してきました。このトンネルでは、さまざまなプロトコルをサービス提供のトランスポート メカニズムに伝送することが可能です。

さらに、VPN がない在宅勤務者は、Cisco TelePresence デバイスを使用して、自宅でもオフィスにいるときと変わらないほど簡単にコラボレーションできます。Cisco Expressway によってエンド ユーザ エクスペリエンスが簡略化され、社外でのコラボレーションが社内の場合と同じく容易になります。Jabber モバイル ユーザは、Transport Layer Security（TLS）をベースにしたセキュアなモバイル アクセスを使用しているため、VPN に伴う追加的な手順なしで、あらゆるコラボレーション ワークロード（ビデオ、音声、コンテンツ、インスタント メッセージ、およびプレゼンス）にアクセスでき、他のトラフィックはインターネットを介して直接ルーティングできる柔軟性を享受できます。

つまり、ユーザは、場所の制約を受けることなく、シスコ コラボレーション ツールのすべてに瞬時にアクセスでき、コミュニケーションのスピードと効率を上げることができるのです。

テクノロジーの使用例

Cisco Collaboration Edge は、企業ファイアウォールの外側におけるビデオ、音声、コンテンツ、インスタント メッセージ、およびプレゼンスへのシンプルで高度なセキュア アクセスを可能にします。関係者のコミュニティをつなぐのに役立つだけでなく、リモート ワーカーやモバイル ワーカーは自分で選んだデバイスで Cisco Jabber を使用してコラボレーションの効果を高めることができます。

使用例：Mobile & Remote Access と、デスクトップおよび多目的ルーム システムによる Business-to-Business（B2B）コラボレーション

組織は、フェイスツーフェイスのメリットはそのままに、リモートの人員から予算や生産性におけるメリットを得ることを望んでいます。従業員がリモートで仕事をする際に、慣れている対面式のやりとりを同僚や上司と交わせる柔軟性を望んでいます。会議室、役員室、講堂、その他の共有環境での、コラボレーション エクスペリエンスの改善も望んでいます。迅速に導入できて簡単に一元管理でき、かつリモート サイトに高価なコンポーネントを重複して準備する必要がないソリューションを望んでいます。

この設計ガイドによって、以下を実現します。

- 実証済みの、高度なセキュア ファイアウォール越えテクノロジーを活用することで、コラボレーションを組織全体に広げることができます。
- Business-to-Business（B2B）接続を構築できます。
- 単独の VPN クライアントを必要としない、リモート ワーカー向け包括的コラボレーションへのセッション ベース アクセスを実現します。
- スマートフォン、タブレット、デスクトップ向けの Cisco Jabber と連携し多様なデバイスをサポートします。
- 遠隔地のモバイル ワーカー向けの、個人所有の持ち込みデバイス（BYOD）戦略を促進します。

設計の概要

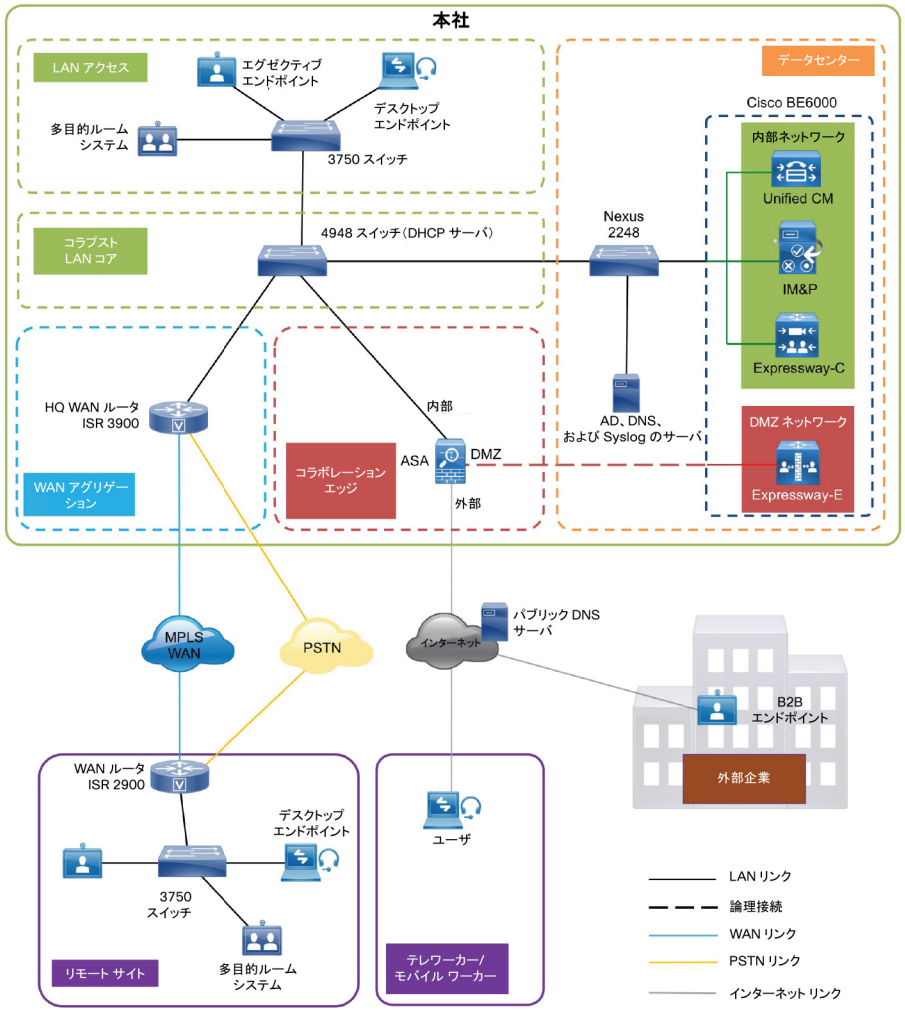
エンドツーエンドの Cisco Collaboration Edge ソリューションには、エンドポイント、インフラストラクチャ コンポーネント、および一元管理ツールが組み込まれています。

ソリューションの詳細

この『*Cisco BE6000 による Collaboration Edge テクノロジー設計ガイド*』には、以下のコンポーネントが含まれています。

- Cisco Unified Communications Manager（CUCM）。コール制御と SIP エンドポイント登録用
- Cisco Expressway-C および Cisco Expressway-E。VPN を使用しない Mobile & Remote Access 用
- Cisco Expressway-E。Business-to-Business（B2B）コラボレーション用
- ネットワーク タイム プロトコル（NTP）サーバ。クロック同期用
- パブリックおよび社内ドメイン ネーム システム（DNS）サーバ。エンドポイントが Cisco Expressway サーバを検出する際に使用するホスト名から IP への解決および SRV レコード用

図 1：概要ブロック図



Cisco Unified Communications Manager

CUCM（旧称 *Cisco Unified CallManager*）は、ソフトウェア ベースの呼制御装置として機能します。CUCM は、企業のテレフォニー機能を、IP 電話などのパケット テレフォニー ネットワーク デバイス、メディア処理デバイス、Voice-over-IP（VoIP）ゲートウェイ、マルチメディア アプリケーションに拡張します。統合メッセージング、マルチメディア会議、コラボレーティブ コンタクト センター、インタラクティブ マルチメディア レスポンス システムなどの、追加のデータ、音声、ビデオ サービスは、CUCM のオープンなアプリケーション プログラム インターフェイス（API）を通じて通信します。

CUCM は、この CVD における主要な呼制御装置です。CUCM は Session Initiation Protocol（SIP）をサポートするため、本ドキュメント内の設定では、エンドポイントのシグナリング プロトコルとして SIP を使用しています。

シスコのビデオ エンドポイントおよび TelePresence エンドポイント

シスコのビデオ エンドポイントは、IP テレフォニーに似た IP ビデオ テレフォニー機能を提供します。ユーザはポイントツーポイントおよびポイントツーマルチポイントのビデオ コールを利用できます。シスコのビデオ エンドポイントは、それがサポートする機能、ハードウェア画面のサイズ、および導入される環境に基づいてファミリ分けされています。

現時点で Mobile & Remote Access をサポートしているのは、Jabber for Windows および Jabber for iOS のみですが、今後の TC 7.x リリースでは、TC ソフトウェアをサポートするすべてのデバイスで Mobile & Remote Access がサポートされる予定です。

本ドキュメントでは、2 種類のエンドポイントに言及しています。

- **デスクトップ ビデオ エンドポイント** – Cisco Jabber for Windows などの Cisco Jabber ソフトウェアベース デスクトップ クライアントでは、内蔵の前面カメラや USB 接続の外部カメラを使用してビデオを送信できます。Cisco TelePresence System EX シリーズ ビデオ エンドポイントは、フル HD のビデオ コールをサポートするほか、コンテンツ共有などの機能もサポートされ、パーソナル デスクトップ ソリューションのエクスペリエンスを次のレベルへと高めています。EX シリーズのモデルには、Cisco TelePresence System EX60 および EX90 があります。EX90 は画面が広く、マルチサイト機能をサポートしています。デュアル画面機能をサポートしている為、コンテンツ画像や多地点接続拠点をデュアル画面に表示させることが可能になっています。
- **コラボレーション ルーム エンドポイント** – Cisco TelePresence SX20 Quick Set は、多くのフラットパネル ディスプレイを強力な Cisco TelePresence システムに変えることができる柔軟性の高いシステムです。SX20 Quick Set は、フル HD ビデオおよび多地点接続会議用に設計されています。さまざまな大きさの部屋に対応できる柔軟性を備えています。

Cisco Expressway-E および Expressway-C

Cisco Expressway シリーズは、CUCM への Mobile & Remote Access を可能にするファイアウォール トラバーサル ソリューションです。Cisco Jabber ユーザは、このソリューションを通じて、VPN を介さずに社内との接続が可能となります。在宅勤務者は、VPN がなくても、オフィスにいるときと同じように、個人用の TelePresence エンドポイントを使用できます。また、このソリューションでは B2B 接続も行えます。Cisco Expressway シリーズは、Cisco Expressway-E と Cisco Expressway-C で構成されています。

Cisco Expressway-E はトラバーサル サーバとして機能し、ビジネス用にセキュアな通信を実現するとともに、DNS SRV ルックアップなどのサービスも提供します。

Cisco Expressway-C は Cisco Expressway-E のトラバーサル クライアントとして機能します（すべての Cisco Expressway E 導入環境に必要）。業界標準の H.264 SVC、H.323、AVC のサードパーティ製デバイスやシステム（Microsoft Lync 2013 など）とのインターワーキングを提供するビデオ ゲートウェイの機能を果たします。

この設計では、Mobile & Remote Access 用と Business-to-Business（B2B）コミュニケーション用にそれぞれトラバーサル クライアント ゾーンおよびトラバーサル サーバ ゾーンを作成します。

ドメイン ネーム システム サーバ

この設計には、2 つの DNS サーバがあります。内部 DNS サーバ（社内 DNS サーバ）は **192.168.1.10**、パブリック DNS サーバは **192.168.6.5** です。

Cisco Adaptive Security Appliance（ASA）

この設計では、セキュリティ アプライアンスとして Cisco Adaptive Security Appliance（Cisco ASA）を使用します。このアプライアンスは、3 ポート ファイアウォール モードで展開されます。ポートのうち 1 つは内部ネットワークに、もう 1 つは外部インターフェイスに、3 つ目は DMZ インターフェイスに接続します。Cisco Expressway-E は、Cisco ASA の DMZ インターフェイスに接続します。Expressway-C および他のコラボレーション コンポーネントは、Cisco ASA アプライアンスの *内部に*配置されます。Expressway-E はパブリック IP にスタティック NAT を使用して接続されます。Expressway-E への通信はすべて NAT 変換済み IP をベースにします。つまり、Cisco ASA では、内部からのトラフィックが NAT 変換済み IP を使用して DMZ に到達します。この手法は *NAT リフレクション*とも呼ばれています。

Cisco Expressway-E との間でネットワーク トラフィックを送受信する Cisco ASA アプライアンスでは、SIP ALG および H.323 ALG を無効にしています。これらを有効にすると、Cisco Expressway-E に組み込まれているトラバーサル機能に悪影響が及んでいる事例が多く見られています。これは、SIP メッセージの多くが暗号化されており、Cisco ASA がペイロードを検査できなくなるためです。

ダイヤル プラン

この設計は、単一クラスタ集中呼処理モデルに準じています。エンドポイントでは、ダイヤリングに 7 桁の電話番号が使用されます。これにより、数字ダイヤリングしかサポートしていないデバイスからのコールも引き続き着信できます。番号は次のパターンになります。

800xxxx

URI ダイヤリングについては、エンドポイントに以下の形式で URI が割り当てられます。

800xxxx@cisco.local

この設計では、以下のサンプル ドメインを使用します。

cisco.local

Business-to-Business（B2B）コールについては、以下のサンプル外部ドメインを使用します。

cisco.com

導入の詳細

このガイドは、サーバ インストール、Mobile & Remote Access の導入、Business-to-Business（B2B）コラボレーションの導入といった複数のセクションに分かれています。各セクションに、システムを最初から設定するための手順とステップが記載されています。

本書を使用して、Mobile & Remote Access と、Business-to-Business（B2B）コラボレーションの両方を導入できます。ただし、Mobile & Remote Access 導入する場合は、以下のプロセスに従ってください。

- Cisco Expressway-C の設置
- Cisco Expressway-E の設置
- CUCM の設定
- Mobile & Remote Access の導入

Business-to-Business（B2B）のみを導入する場合は、以下のプロセスに従ってください。

- Cisco Expressway-C の設置
- Cisco Expressway-E の設置
- CUCM の設定
- B2B の導入

プロセス

Cisco Expressway-C の設置

1. ホストへの OVA 導入
2. VM ゲストの設定
3. ライセンスの適用
4. システム名、DNS、および NTP の設定

手順を開始する前に、構築するサイトに固有の情報を予め用意する必要があります。以下の表を埋めてください。以下の手順では例として以下の表の CVD 設定の値を入力値として記載しています。

表 1 :Cisco Expressway-C を設定するのに必要な情報

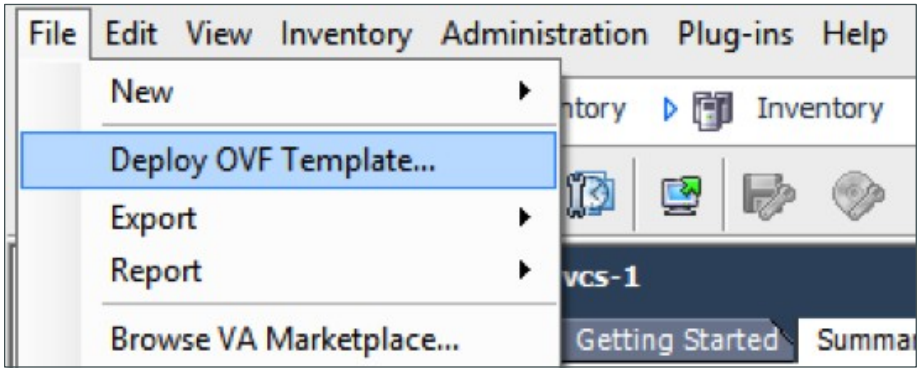
項目	CVD 設定	サイト固有の詳細情報
IPV4 アドレス	192.168.1.29	
IPV4 サブネット	255.255.255.0	
IPV4 デフォルト ゲートウェイ	192.168.1.1	
システム名	EXPc1	
DNS サーバ アドレス	192.168.1.10	
DNS ローカル ホスト名	EXPc1	
DNS ドメイン名	cisco.local	
NTP サーバのアドレス	192.168.1.1	
タイムゾーン	Asia/Calcutta	

手順 1　ホストへの OVA 導入

標準的なインストール手順を示します。[Deploy OVF Template（OVF テンプレートの展開）] は、ホストの設定を反映して動的に変化します。

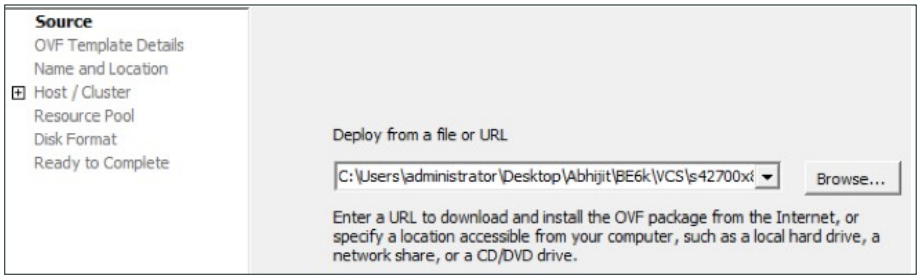
ステップ 1：vSphere にログインし、ESXi ホストにアクセスします。

ステップ 2：[File（ファイル）] > [Deploy OVF Template（OVF テンプレートの展開）] の順に選択します。



ステップ 3：[Browse（参照）] をクリックして .ova ファイルを探し、[Open（開く）] をクリックしてから [Next（次へ）] をクリックします。

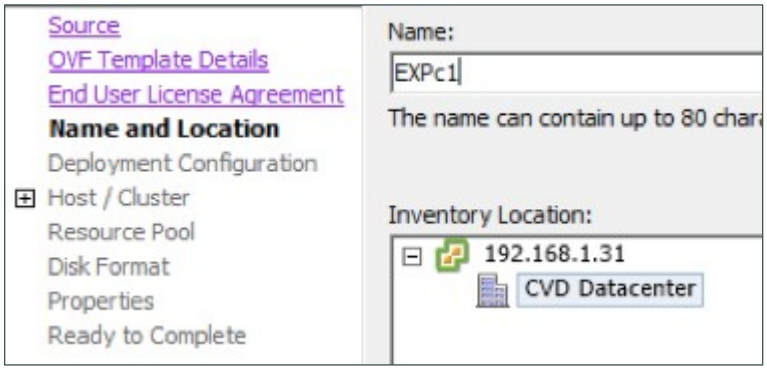
ステップ 4：[Next（次へ）] をクリックします。



ステップ 5：[OVF Template Details（OVF テンプレートの詳細）] ページで、[Next（次へ）] をクリックします。

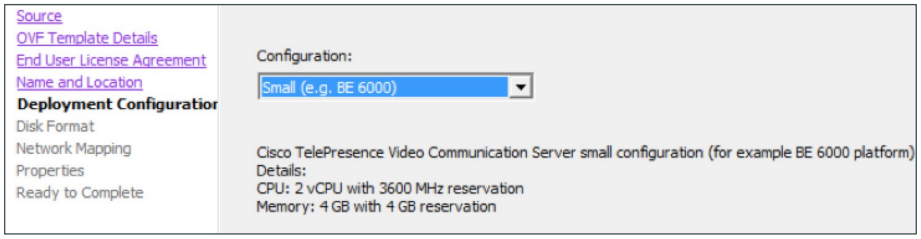
ステップ 6：[End User License Agreement（エンドユーザ ライセンス契約）] ページが表示されたら、EULA を読んで、[Accept（同意する）] をクリックし、[Next（次へ）] をクリックします。

ステップ 7：[Name and Location（名前と場所）] ページで、**EXPc1** と入力し、仮想マシンを配置するインベントリの場所を指定します。

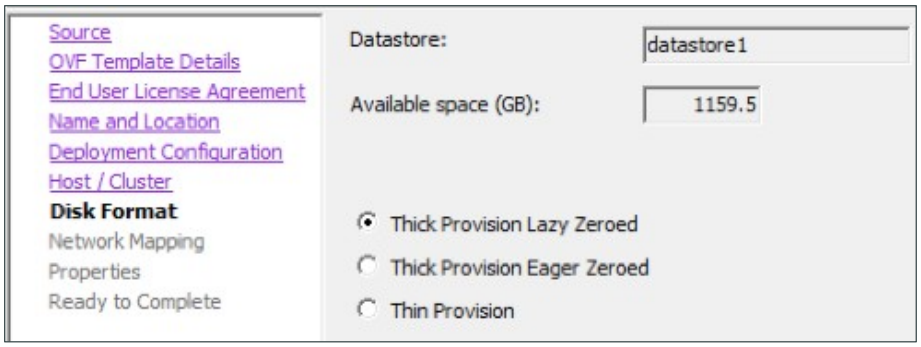


ステップ 8:[Storage(ストレージ)] ページで、Expressway-C VM ゲストを導入するデータストアを選択し、[Next(次へ)] をクリックします。

ステップ 9:[Deployment Configuration(導入の構成)] ページで、構成オプションとして [Small(e.g. BE 6000)(小規模(例:BE 6000))] を選択します。



ステップ 10:[Disk Format(ディスクのフォーマット)] ページで、デフォルトのディスク フォーマット [Thick Provision Lazy Zeroed(シック プロビジョニング(Lazy Zeroed))] が選択されていることを確認し、[Next(次へ)] をクリックします。



技術的なヒント

パーティション サイズの変更中に VM のパフォーマンスが低下する可能性があるため、Thin Provision は推奨されません。

ステップ 11:[Network Mapping(ネットワークのマッピング)] が表示されている場合は、それを設定し、使用するインフラストラクチャに適用するネットワーク マッピング(デフォルトは VM Network)を選択して、[Next(次へ)] をクリックします。

ステップ 12:[Ready to Complete(終了準備の完了)] ページで、導入設定を確認します。

ステップ 13:[Power on after deployment(展開後に起動)] を選択し、[Finish(終了)] をクリックします。これで、Expressway-C OVA が VM ホスト上のゲストとして導入されます。

手順 2 VM ゲストの設定

ステップ 1:VM ゲストを右クリックし、[Open Console(コンソールを開く)] をクリックします。VM ゲストの起動には少し時間がかかります。

ステップ 2:2 つ目のハード ディスク パーティションを作成してリブートします。ログイン プロンプトが表示されます。

ステップ 3:ログイン プロンプトで、ユーザ名 admin とパスワード TANDBERG を入力します。

ステップ 4：インストール ウィザードのプロンプトで y を入力し、Enter を押します。

ステップ 5：インストール ウィザードで、以下の情報を入力します。その他のエントリは必要に応じて設定します。

- Run install wizard（インストール ウィザードの実行）：y
- Do you wish to change the system password（システム パスワードを変更しますか）：y
- Password（パスワード）：**[パスワード]**
- IP Protocol（IP プロトコル）：**IPv4**
- IP Address LAN1（IP アドレス LAN1）：**192.168.1.29**
- Subnet Mask LAN1（サブネット マスク LAN1）：**255.255.255.0**
- Default Gateway Address（デフォルト ゲートウェイのアドレス）：**192.168.1.1**
- Ethernet Speed（イーサネット速度）：auto（自動）
- Run ssh daemon（ssh デーモンの実行）：y

設定が適用され、Expressway-C からログアウトされます。

ステップ 6：Expressway-C に admin としてログインし、以下のコマンドを入力して、VM ゲストをリブートします。

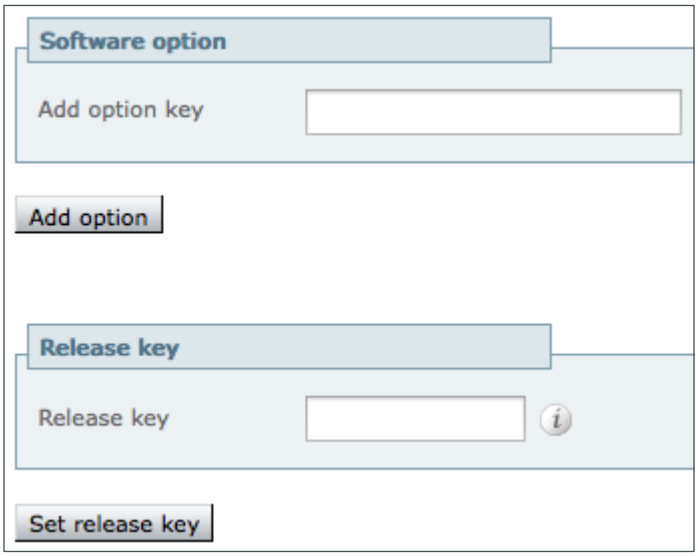
```
Xcommand boot
```

Expressway-C に Web ブラウザを使用してアクセスできるようになります。

手順 3　ライセンスの適用

ステップ 1：[Maintenance（メンテナンス）] > [Option keys（オプション キー）] に移動し、提供されたリリース キーを入力して、[Set release key（リリース キーの設定）] をクリックします。

ステップ 2：提供されたオプション キーごとに、[Add option key（オプション キーの追加）] にオプション キーの値を入力し、[Add option（オプションを追加する）] をクリックします。



ステップ 3：[Maintenance（メンテナンス）] > [Restart options（オプションの再起動）] に移動し、[Restart（再起動）] をクリックします。

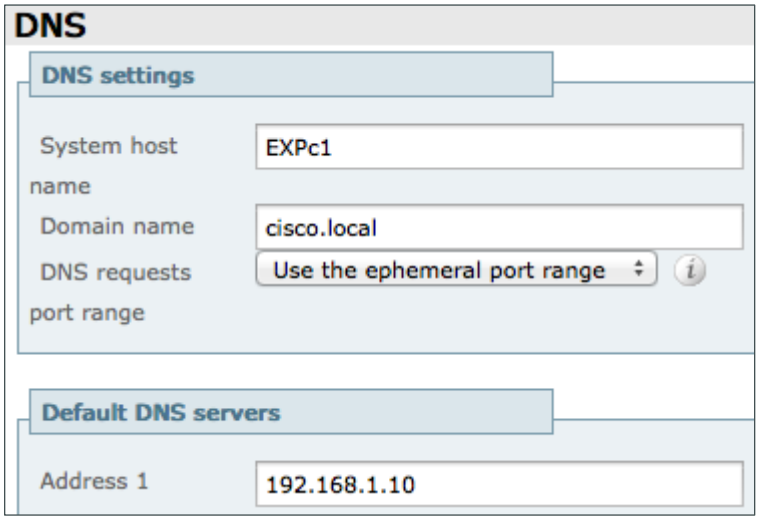
手順 4　システム名、DNS、および NTP の設定

ステップ 1:[System(**システム**)] > [DNS] に移動し、[DNS settings(DNS **設定**)] セクションで、以下の値を入力します。その他のフィールドは、そのデフォルト値のままにします。

- System host name(システム ホスト名):**EXPc1**
- Domain name(ドメイン名):**cisco.local**

ステップ 2:[Default DNS servers(**デフォルト** DNS **サーバ**)] セクションで、以下の値を入力します。その他のフィールドは、そのデフォルト値のままにします。

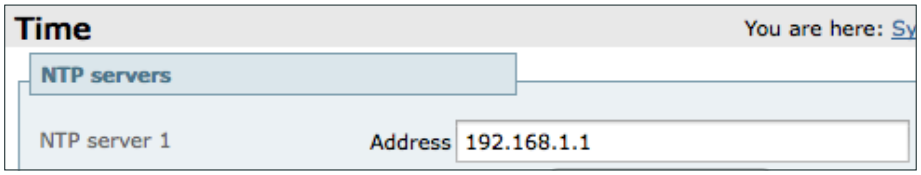
- Address 1(アドレス 1):**192.168.1.10**

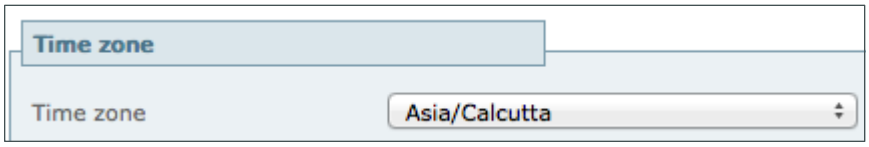


ステップ 3:[Save(**保存**)] をクリックします。

ステップ 4:[System(**システム**)] > [Time(**時間**)] に移動し、以下を入力します。

- NTP server 1(NTP **サーバ** 1):**192.168.1.1**





ステップ 5:[Save(**保存**)] をクリックします。

プロセス

Cisco Expressway-E の設置

1. ホストへの OVA 導入
2. VM ゲストの設定
3. ライセンスの適用
4. システム名、DNS、および NTP の設定
5. スタティック NAT の設定

手順を開始する前に、構築するサイトに固有の情報を予め用意する必要があります。以下の表を埋めてください。

Expressway-E は、DMZ ネットワーク内に配置され、パブリックにルーティング可能な IP に NAT 変換されます。Expressway-E に NAT が設定されると、Expressway-E との間のすべての通信で NAT 変換済み IP が使用されます。

Expressway-E は、インターネット上のパブリック DNS サーバ設定に向けられます。以下の手順では例として以下の表の CVD 設定の値を入力値として記載しています。

表 2 :Cisco Expressway-E を設定するのに必要な情報

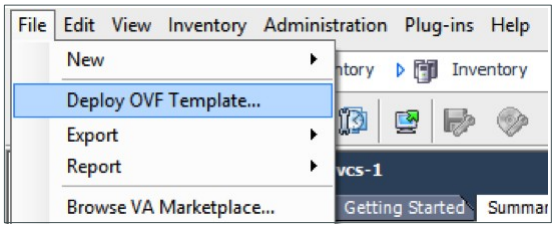
項目	CVD 設定	サイト固有の詳細情報
IPV4 アドレス	192.168.4.18	
IPV4 NAT 変換済み IP	192.168.6.18	
IPV4 サブネット	255.255.255.252	
IPV4 デフォルト ゲートウェイ	192.168.4.17	
システム名	EXPe1	
DNS サーバ アドレス	192.168.6.5	
DNS ローカル ホスト名	EXPe1	
DNS ドメイン名	cisco.local	
NTP サーバのアドレス	192.168.1.1	
タイムゾーン	アジア/コルカタ	

手順 1　ホストへの OVA 導入

標準的なインストール手順を示します。[Deploy OVF Template（OVF テンプレートの展開）] は、ホストの設定を反映して動的に変化します。

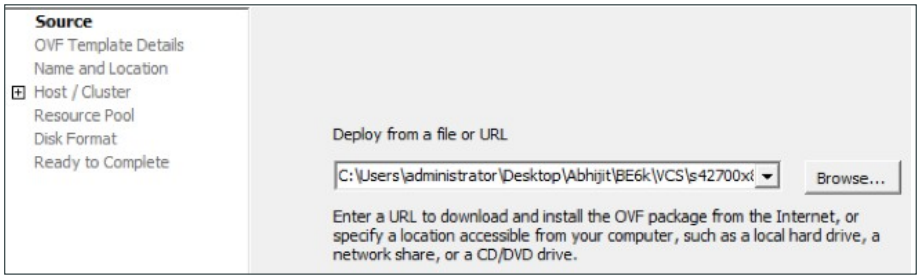
ステップ 1：vSphere にログインし、ESXi ホストにアクセスします。

ステップ 2:[File(ファイル)] > [Deploy OVF Template(OVF テンプレートの展開)] の順に選択します。



ステップ 3:[Browse(参照)] をクリックして .ova ファイルを探し、[Open(開く)] をクリックしてから [Next(次へ)] をクリックします。

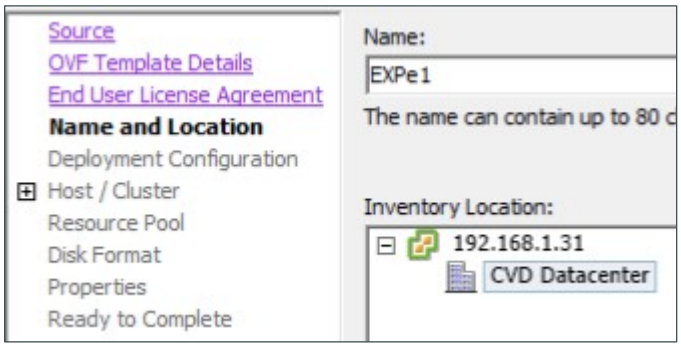
ステップ 4:[Next(次へ)] をクリックします。



ステップ 5:[OVF Template Details(OVF テンプレートの詳細)] ページで、[Next(次へ)] をクリックします。

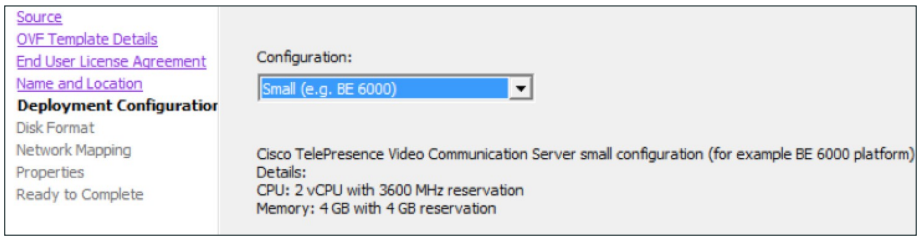
ステップ 6:[End User License Agreement(エンド ユーザ ライセンス契約)] ページが表示されたら、EULA を読んで、[Accept(同意する)] をクリックし、[Next(次へ)] をクリックします。

ステップ 7:[Name and Location(名前と場所)] ページで、名前として **EXPe1** と入力し、仮想マシンを配置するインベントリの場所を指定します。

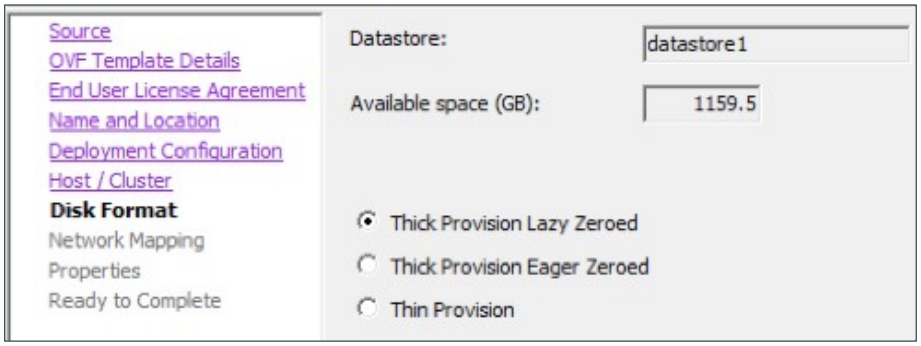


ステップ 8:[Storage(ストレージ)] ページで、Expressway-E VM ゲストを導入するデータストアを選択し、[Next(次へ)] をクリックします。

ステップ 9:[Deployment Configuration(導入の構成)] ページで、構成オプションとして [Small(e.g. BE 6000)(小規模(例:BE 6000))] を選択します。



ステップ 10:[Disk Format(ディスクのフォーマット)] ページで、デフォルトのディスク フォーマット [Thick Provision Lazy Zeroed(シック プロビジョニング(Lazy Zeroed))] が選択されていることを確認し、[Next(次へ)] をクリックします。



技術的なヒント

パーティション サイズの変更中に VM のパフォーマンスが低下する可能性があるため、Thin Provision は推奨されません。

ステップ 11:[Network Mapping(ネットワークのマッピング)] が表示されている場合は、それを設定し、使用するインフラストラクチャに適用するネットワーク マッピング(デフォルトは VM Network)を選択して、[Next(次へ)] をクリックします。

ステップ 12:[Ready to Complete(終了準備の完了)] ページで、導入設定を確認します。

ステップ 13:[Power on after deployment(展開後に起動)] を選択します。

ステップ 14:[Finish(終了)] をクリックします。

これで、Expressway-E OVA が VM ホスト上のゲストとして導入されます。

手順 2 VM ゲストの設定

ステップ 1:VM ゲストを右クリックし、[Open Console(コンソールを開く)] をクリックします。VM ゲストの起動には少し時間がかかります。

ステップ 2:2 つ目のハード ディスク パーティションを作成してリブートします。ログイン プロンプトが表示されます。

ステップ 3:ログイン プロンプトで、ユーザ名 admin とパスワード TANDBERG を入力します。

ステップ 4：インストール ウィザードのプロンプトで y を入力し、Enter を押します。

ステップ 5：インストール ウィザードに従って、IP 情報を入力します。該当するフィールドに次のように入力します。その他のエントリは必要に応じて設定します。

- Run install wizard（インストール ウィザードの実行）：y
- Do you wish to change the system password（システム パスワードを変更しますか）：y
- Password（パスワード）：**[パスワード]**
- IP Protocol（IP プロトコル）：**IPv4**
- IP Address LAN1（IP アドレス LAN1）：**192.168.4.18**
- Subnet Mask LAN1（サブネット マスク LAN1）：**255.255.255.252**
- Default Gateway Address（デフォルト ゲートウェイのアドレス）：**192.168.4.17**
- Ethernet Speed（イーサネット速度）：auto（自動）
- Run ssh daemon（ssh デーモンの実行）：y

設定が適用され、Expressway-E からログアウトされます。

ステップ 6：Expressway-E に admin としてログインし、以下のコマンドを入力して、VM ゲストをリブートします。

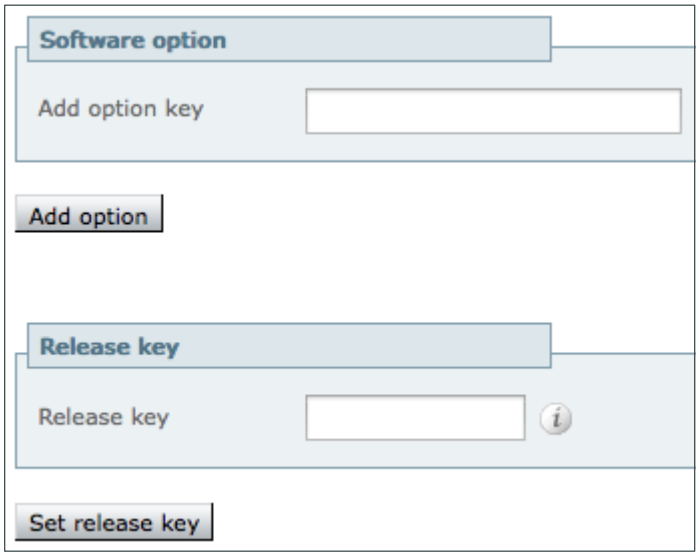
```
Xcommand boot
```

Expressway-E に Web ブラウザを使用してアクセスできるようになります。

手順 3　ライセンスの適用

ステップ 1：[Maintenance（メンテナンス）] > [Option keys（オプション キー）] に移動し、提供されたリリース キーを入力して、[Set release key（リリース キーの設定）] をクリックします。

ステップ 2：提供されたオプション キーごとに、[Add option key（オプション キーの追加）] フィールドにオプション キーの値を入力し、[Add option（オプションを追加する）] をクリックします。



ステップ 3：[Maintenance（メンテナンス）] > [Restart options（オプションの再起動）] に移動し、[Reboot（リブート）] をクリックします。

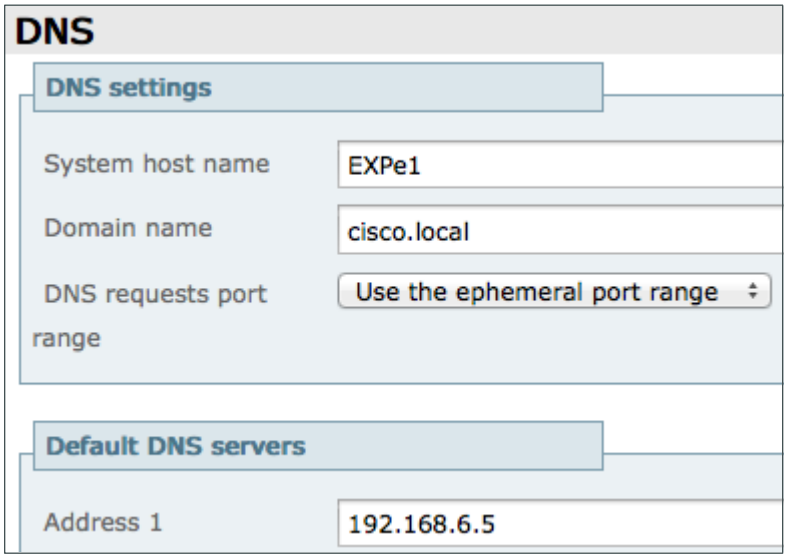
手順 4　システム名、DNS、および NTP の設定

ステップ 1:[System(**システム**)] > [DNS] に移動し、[DNS settings(DNS **設定**)] セクションで、以下を入力します。その他のフィールドは、そのデフォルト値のままにします。

- System host name(システム ホスト名):**EXPe1**
- Domain name(ドメイン名):**cisco.local**

ステップ 2:[Default DNS servers(**デフォルト** DNS **サーバ**)] セクションで、以下を入力します。その他のフィールドは、そのデフォルト値のままにします。

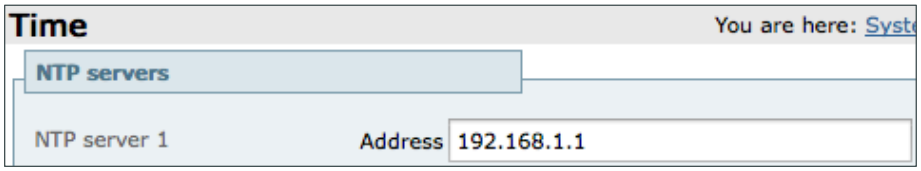
- Address 1(アドレス 1):**192.168.6.5**

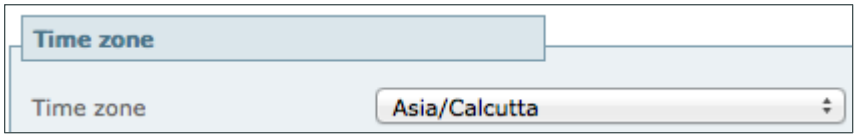


ステップ 3:[Save(**保存**)] をクリックします。

ステップ 4:[System(**システム**)] > [Time(**時間**)] に移動し、以下を入力します。

- NTP server 1(NTP **サーバ** 1):**192.168.1.1**





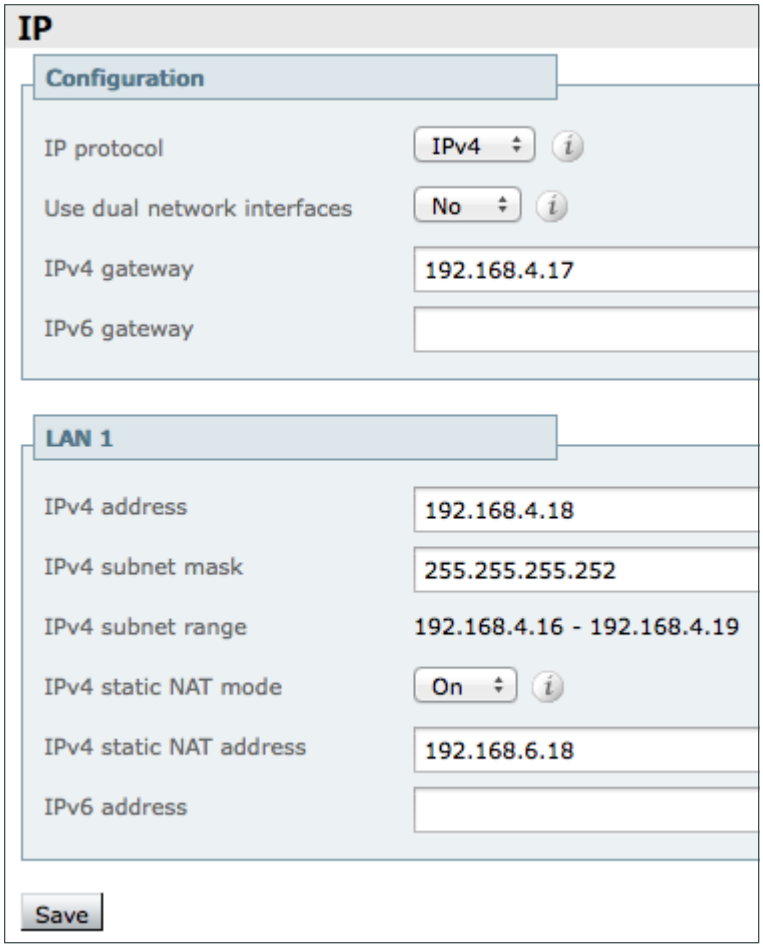
ステップ 5:[Save(**保存**)] をクリックします。

手順 5　スタティック NAT の設定

Expressway-E で NAT 機能を有効にするには、高度なネットワーク キーが必要です。

ステップ 1：[System（**システム**）] > [IP] に移動し、該当するフィールドに以下を入力します。その他のフィールドは、そのデフォルト値のままにします。

- Use Dual Network Interfaces（デュアル ネットワーク インターフェイスを使用する）：**No**
- IPv4 static NAT mode（IPv4 スタティック NAT モード）：**On（有効）**
- IPv4 static NAT address（IPv4 スタティック NAT アドレス）：**192.168.6.18**



ステップ 2：[Save（**保存**）] をクリックします。

プロセス

CUCM の設定

1. ビデオのリージョンを設定する
2. CUCM でビデオ用のデバイス プールを設定し、ビデオのリージョンを追加する
3. すべてのビデオ エンドポイントに対して上記のデバイス プールを選択する

Cisco Unified Communications Manager（CUCM）のインストールと基本設定については、『Unified Communications Using Cisco BE6000 Technology Design Guide（Cisco BE6000 を使用したユニファイド コミュニケーション テクノロジー設計ガイド）』を参照してください。

このプロセスは、Mobile & Remote Access または Business-to-Business（B2B）コミュニケーションの設定を開始するために CUCM で必要となる前提条件の設定を示しています。

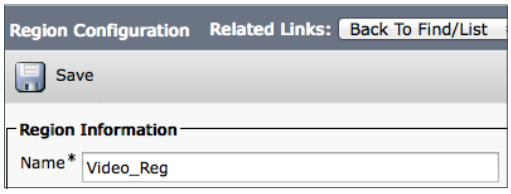
手順 1　ビデオのリージョンを設定する

まず、[Cisco Unified Communications Manager Administration（Cisco Unified Communications Manager の管理）] ページにログインし、リージョン内コールやリージョン間コールの帯域幅を多く確保できるようにビデオ トラフィック用のリージョンを作成します。

ステップ 1：[System（システム）] > [Region Information（リージョン情報）] > [Region（リージョン）] に移動し、[Add New（新規に追加）] をクリックします。

ステップ 2：以下を入力します。

- Name（名前）：**Video_Reg**

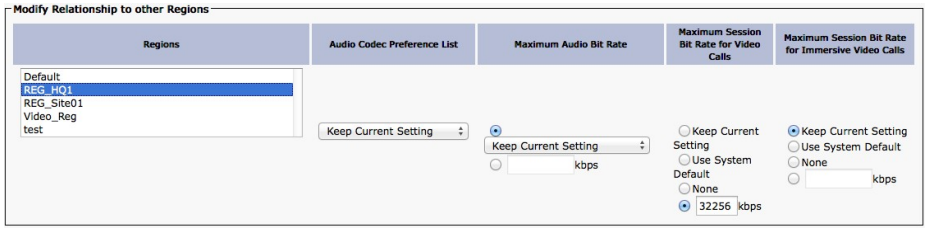


ステップ 3：[Save（保存）] をクリックします。

ステップ 4：[Region（リージョン）] で [REG_HQ1] を選択します。

ステップ 5：以下を入力します。

- Maximum Session Bit Rate for Video Calls（ビデオ コールの最大セッション ビット レート）：**32256**

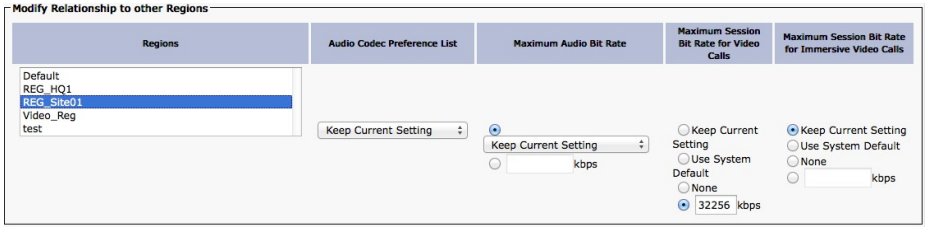


ステップ 6：[Save（保存）] をクリックします。

ステップ 7：[Region（リージョン）] で [REG_Site01] を選択します。

ステップ 8：以下を入力します。

- Maximum Session Bit Rate for Video Calls（ビデオ コールの最大セッション ビット レート）：**32256**



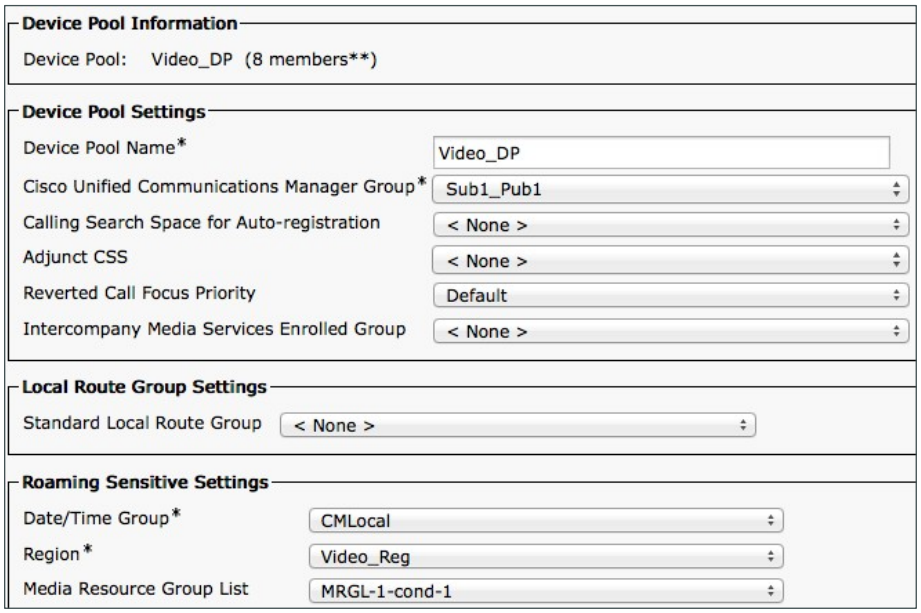
ステップ 9：[Save（保存）] をクリックします。

手順 2　CUCM でビデオ用のデバイス プールを設定し、ビデオのリージョンを追加する

ステップ 1：[System（システム）] > [Device Pool（デバイス プール）] に移動し、[Add New（新規に追加）] をクリックします。

ステップ 2：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Device Pool Name（デバイス プール名）：**Video_DP**
- Date/Time Group（日付/時間グループ）：CMLocal
- Region（リージョン）：Video_Reg

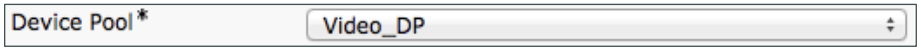


ステップ 3：[Save（保存）] をクリックします。

手順 3　すべてのビデオ エンドポイントに対して上記のデバイス プールを選択する

ステップ 1：[Device（デバイス）] > [Phone（電話）] に移動し、[Find（検索）] をクリックして、ビデオ エンドポイントを選択します。

ステップ 2：[Device Pool（デバイス プール）] で [Video_DP] を選択します。



ステップ 3：[Save（保存）] をクリックします。

ステップ 4：[Apply Config（設定を適用）] をクリックします。

プロセス

Mobile & Remote Access の導入

1. 関連する SRV レコードと A レコードを使用して社内 DNS サーバを設定する
2. 関連する SRV レコードと A レコードを使用してパブリック DNS サーバを設定する
3. ファイアウォールを設定する
4. CUCM 用に Expressway-C を設定する
5. Expressway-C で Unified CM と IM&P サーバを検出する
6. Unified CM 用に Expressway-E を設定する
7. サーバ証明書と CA 証明書を設定する
8. Expressway-C でトラバーサル クライアント ゾーンを設定する
9. Expressway-E で Expressway-C クレデンシャルを設定する
10. Expressway-E でトラバーサル サーバ ゾーンを設定する

シスコ ユニファイド コミュニケーションの Mobile & Remote Access を利用することで、Cisco Jabber などのエンドポイントが企業ネットワーク外にある場合に、Cisco Unified Communications Manager への登録、呼制御、プロビジョニング、メッセージング、およびプレゼンスの機能を使用することができるようになります。Expressway-C および Expressway-E は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。以下の手順で示す入力項目値は入力例となります。

技術的なヒント

VPN ベースのリモート アクセスについては、『Cisco Validated Designs for Enterprise WAN（エンタープライズ WAN 向けの Cisco Validated Designs）』CVD で VPN 関連の適切な設定を参照できます。

手順 1　関連する SRV レコードと A レコードを使用して社内 DNS サーバを設定する

Mobile & Remote Access エンドポイントでは、クライアントが社内と社外のどちらにあるかを判断するにあたり、ドメイン ネーム サーバを使用します。エンドポイントが社内にある場合は内部ネーム サーバを、社外にある場合は外部ネーム サーバを検索します。これらのネーム サーバに対して、エンドポイントは、SRV レコードを問い合わせて、利用できるサービスを特定します。エンドポイントが社内にある場合は、*_cisco-uds.* サービスを検索して、CUCM および IM&P サーバを検出します。

エンドポイントが CUCM を検出するためには、ローカル DNS サーバに以下の例のように SRV レコードと A レコードが設定されている必要があります。

```
_cisco-uds._tcp.cisco.local.  SRV    10    10    8443    CUCM-Pub.cisco.local
_cuplogin._tcp.cisco.local.  SRV    10    10    8443    CUCM-IMP1.cisco.local
CUCM-Pub.cisco.local.    IN     A    192.168.1.16
CUCM-IMP1.cisco.local.   IN     A    192.168.1.27
```

手順 2　関連する SRV レコードと A レコードを使用してパブリック DNS サーバを設定する

エンドポイントが社外にある場合は、*_collab-edge.* サービスを検索して、リモート アクセス用の Expressway-E を検出します。

エンドポイントが Mobile & Remote Access 用に Expressway-E を検出するためには、パブリック DNS サーバに以下の例のように SRV レコードと A レコードが設定されている必要があります。

```
_collab-edge._tls.cisco.local. SRV 10 10 8443 EXPe1.cisco.local
EXPe1.cisco.local.    IN     A   192.168.6.18
```

手順 3　ファイアウォールを設定する

内部ネットワーク（Expressway-C がある場所）と DMZ（Expressway-E がある場所）間、および DMZ とパブリック インターネット間の以下のポートでトラフィックを許可するようにファイアウォールを設定します。

表 3 :Expressway-C（内部）から Expressway-E（DMZ）への送信

目的	プロトコル	Expressway-C（送信元）	Expressway-E（リスニング）
XMPP（IM およびプレゼンス）	TCP	7400	7400
SSH（HTTP/S トンネル）	TCP	エフェメラル ポート	2222
トラバーサル ゾーン SIP シグナリング	TLS	25000 ～ 29999	7001
トラバーサル ゾーン SIP メディア	UDP	36012 ～ 59999	36000 ～ 36011

表 4 :Expressway-E (DMZ) からパブリック インターネットへの送信

目的	プロトコル	Expressway-C (送信元)	Expressway-E (リスニング)
SIP メディア	UDP	36012 ～ 59999	UDP ポート
SIP シグナリング	TLS	25000 ～ 29999	TLS リスニング ポート

表 5 :パブリック インターネットから Expressway-E (DMZ) への受信

目的	プロトコル	Expressway-C (送信元)	Expressway-E (リスニング)
XMPP (IM およびプレゼンス)	TCP	TCP 送信元ポート	5222
UDS (プロビジョニング/電話帳)	TCP	TCP 送信元ポート	8443
メディア	UDP	UDP 送信元ポート	36012 ～ 59999
SIP シグナリング	TLS	TLS 送信元ポート	5061
HTTPS (管理アクセス)	TCP	TCP 送信元ポート	443

技術的なヒント

デフォルトのメディア ポート レンジの 36000 ～ 59999 は、新たにインストールされる X8.0 以降に適用されます。レンジ内の最初の 2 つのポートは、多重化トラフィック専用として使用されます (大規模な VM 展開環境では、レンジ内の最初の 12 個のポート 36000 ～ 36011 が使用されます)。X8.0 以前の場合、デフォルトのレンジは 50000 ～ 54999 です。

技術的なヒント

ポート 8191/8192 TCP および 8883/8884 TCP は、VCS アプリケーションの内部で、VCS Control と VCS Expressway 間の通信に使用されます。ファイアウォールに関する要件はありませんが、これらのポートを他の目的に割り当てることはできません。

手順 4　CUCM 用に Expressway-C を設定する

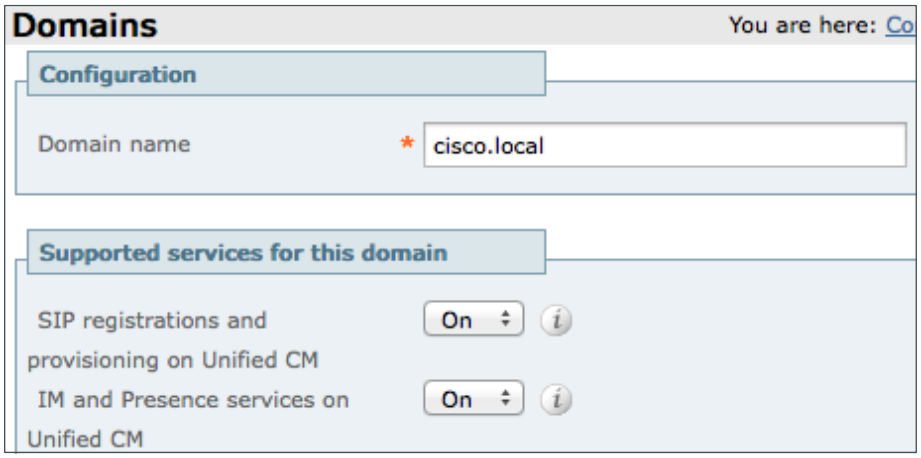
ステップ 1:[Configuration (設定)] > [Unified Communications (ユニファイド コミュニケーション)] > [Configuration (設定)] に移動し、[Mobile and Remote Access] を [On (有効)] に設定します。

ステップ 2:[Save (保存)] をクリックします。

ステップ 3:[Configuration (設定)] > [Domains (ドメイン)] に移動し、[New (新規)] をクリックします。

ステップ 4：該当するフィールドに、以下の値を入力します。

- Domain name（ドメイン名）：**cisco.local**
- SIP registrations and provisioning on Unified CM（Unified CM の SIP 登録とプロビジョニング）：On（有効）
- IM and Presence services on Unified CM（Unified CM の IM およびプレゼンス サービス）：On（有効）



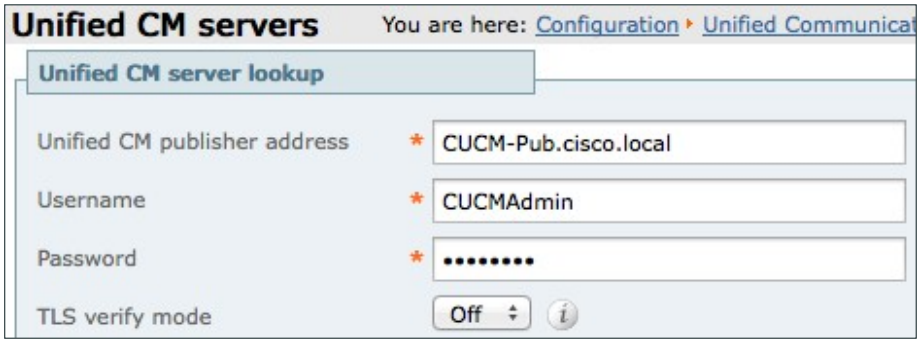
ステップ 5：[Create Domain（ドメインの作成）] をクリックします。

手順 5　Expressway-C で Unified CM と IM&P サーバを検出する

ステップ 1：[Configuration（設定）] > [Unified Communications（ユニファイド コミュニケーション）] > [Unified CM Servers（Unified CM サーバ）] に移動し、[New（新規）] をクリックします。

ステップ 2：該当するフィールドに、以下の値を入力します。

- Unified CM publisher address（Unified CM パブリッシャ アドレス）：**CUCM-Pub.cisco.local**
- Username（ユーザ名）：**CUCMAdmin**
- Password（パスワード）：**[パスワード]**
- TLS verify mode（TLS 検証モード）：Off（無効）



ステップ 3：[Add Address（アドレスの追加）] をクリックします。

次に、リモート アクセス用に IM&P サーバを設定します。

ステップ 4：[Configuration（設定）] > [Unified Communications（ユニファイド コミュニケーション）] > [IM and Presence servers（IM およびプレゼンス サーバ）] に移動し、[New（新規）] をクリックします。

ステップ 5：該当するフィールドに、以下の値を入力します。

- IM and Presence publisher address（IM およびプレゼンスのパブリッシャ アドレス）：**CUCM-IMP1.cisco.local**
- Username（ユーザ名）：**CUCMAdmin**
- Password（パスワード）：**[パスワード]**
- TLS verify mode（TLS 検証モード）：**Off（無効）**

ステップ 6：[Add Address（アドレスの追加）] をクリックします。

読者へのヒント

IM&P の詳細については、『Unified Communications Using Cisco BE6000 Technology Design Guide（Cisco BE6000 を使用したユニファイド コミュニケーション テクノロジー設計ガイド）』を参照してください。

手順 6　Unified CM 用に Expressway-E を設定する

ステップ 1：[Configuration（設定）] > [Unified Communications（ユニファイド コミュニケーション）] > [Configuration（設定）] に移動し、[Mobile and Remote Access] を [On（有効）] に設定します。

ステップ 2：[Save（保存）] をクリックします。

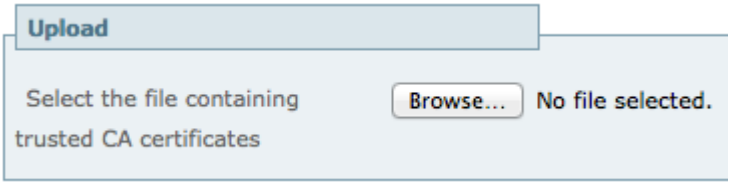
手順 7　サーバ証明書と CA 証明書を設定する

リモート クライアントとモバイル クライアントは、接続先の Expressway-E のアイデンティティを（サーバ証明書の検証によって）確認する必要があります。そのためには、Expressway-E のサーバ証明書に署名する際に使用された認証局が、クライアントの信頼された CA のリストに含まれている必要があります。

この設計では、Expressway-C と Expressway-E の間に加えて、Expressway-E と社外にあるエンドポイント間にもセキュアな通信が必要です。

ステップ 1：CSR の生成や Expressway-C/E へのサーバ証明書のアップロードを実行するには、[Maintenance（**メンテナンス**）] > [Security certificates（**セキュリティ証明書**）] に移動し、[Generate CSR（CSR **の生成**）] をクリックします。

ステップ 2：信頼された認証局（CA）証明書を Expressway-C/E にアップロードするには、[Maintenance（**メンテナンス**）] > [Security certificates（**セキュリティ証明書**）] > [Trusted CA certificate（**信頼された** CA **証明書**）] に移動します。



読者へのヒント

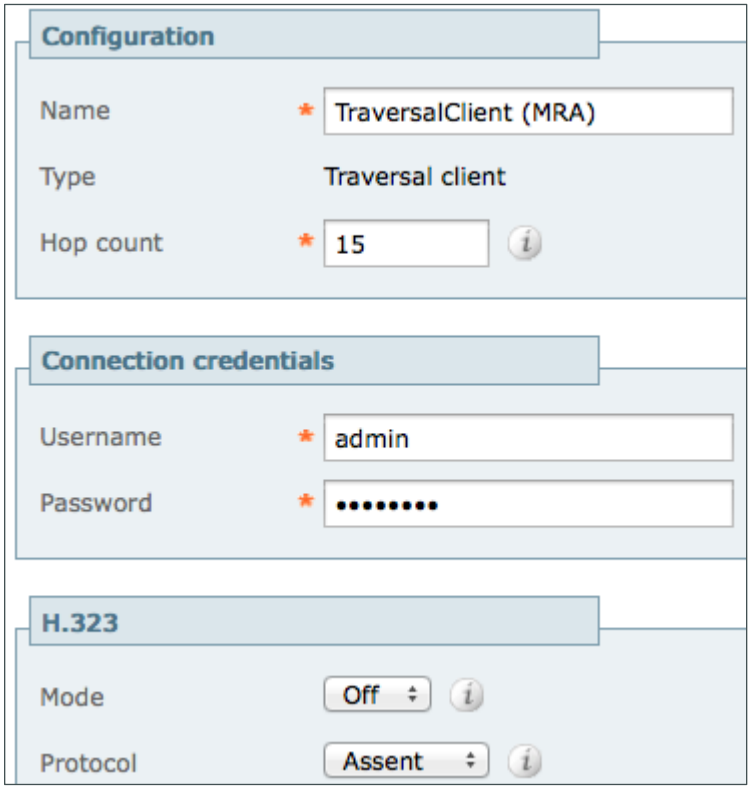
詳細については、『Cisco Expressway Certificate Creation and Use Deployment Guide（Cisco Expressway **の証明書の作成と使用に関する導入ガイド**）』を参照してください。

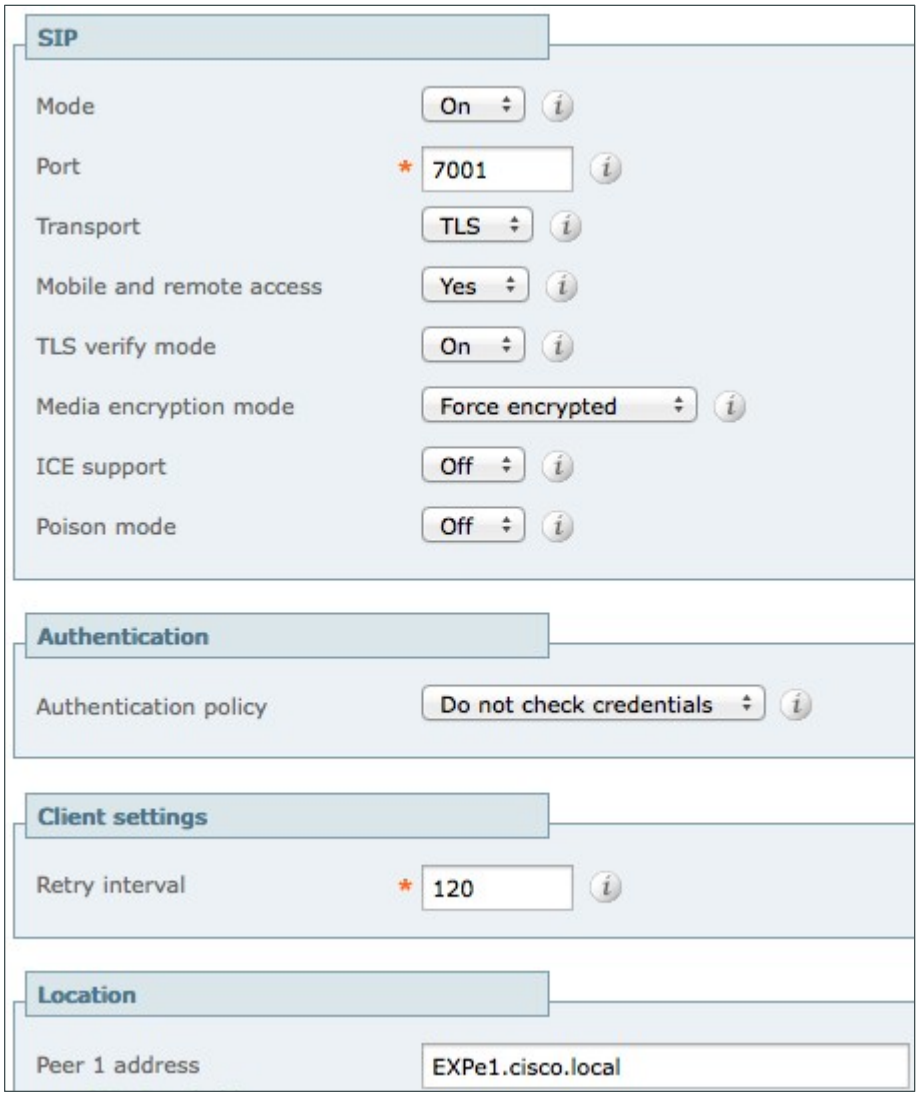
手順 8　Expressway-C でトラバーサル クライアント ゾーンを設定する

ステップ 1：[Configuration（**設定**）] > [Zones（**ゾーン**）] > [Zones（**ゾーン**）] に移動し、[New（**新規**）] をクリックします。

ステップ 2：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- [Configuration（設定）] セクション：
  - Name（名前）：**TraversalClient（MRA）**
  - Type（タイプ）：Traversal Client（トラバーサル クライアント）
- [Connection credentials（接続クレデンシャル）] セクション
  - Username（ユーザ名）：**admin**
  - Password（パスワード）：**[パスワード]**
- [H.323] セクション
  - Mode（モード）：Off（無効）
- [SIP] セクション
  - Mode（モード）：On（有効）
  - Port（ポート）：**7001**
  - Transport（トランスポート）：TLS
  - Mobile and remote access：Yes（はい）
  - TLS verify mode（TLS 検証モード）：On（有効）
  - Media encryption mode（メディア暗号化モード）：Force Encrypted（強制暗号化）
  - ICE support（ICE サポート）：Off（無効）
  - Poison mode（Poison モード）：Off（無効）
- [Location（場所）] セクション
  - Peer 1 address（ピア 1 アドレス）：**EXPe1.cisco.local**





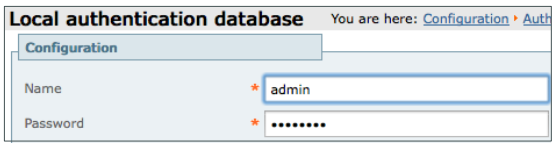
ステップ 3:[Create zone(ゾーンの作成)] をクリックします。

手順 9 Expressway-E で Expressway-C クレデンシャルを設定する

ステップ 1:[Configuration(**設定**)] > [Authentication(**認証**)] > [Local database(**ローカル データベース**)] に移動し、[New(**新規**)] をクリックします。

ステップ 2:該当するフィールドに、以下の値を入力します。

- Name(名前):**admin**
- Password(パスワード):**[EXPc1.cisco.local のパスワード]**



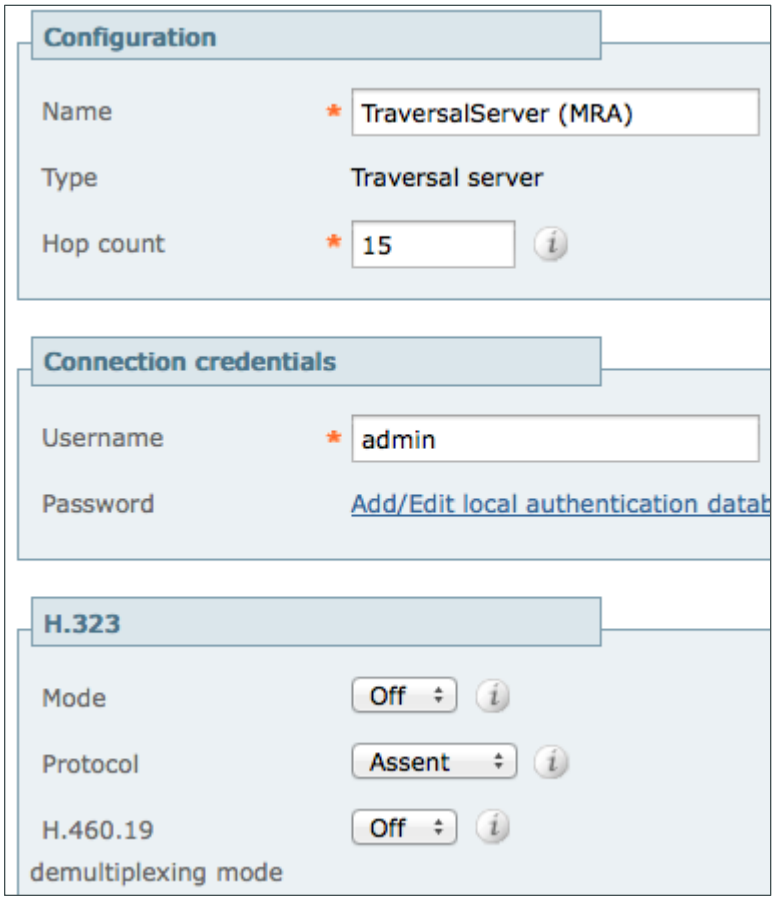
ステップ 3：[Create credential（クレデンシャルの作成）] をクリックします。

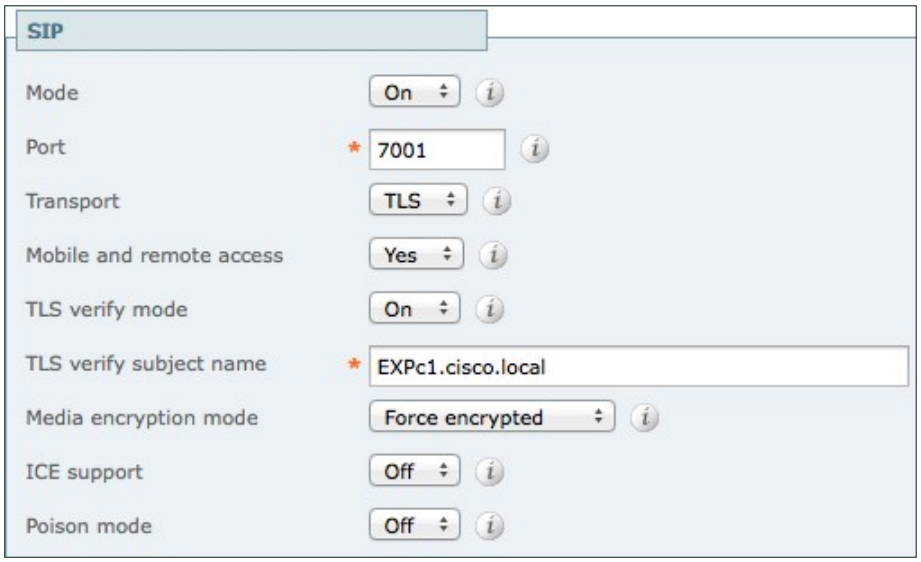
手順 10　Expressway-E でトラバーサル サーバ ゾーンを設定する

ステップ 1：[Configuration（設定）] > [Zones（ゾーン）] > [Zones（ゾーン）] に移動し、[New（新規）] をクリックします。

ステップ 2：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- [Configuration（設定）] セクション：
  - Name（名前）：**TraversalServer（MRA）**
  - Type（タイプ）：Traversal Server（トラバーサル サーバ）
- [Connection credentials（接続クレデンシャル）] セクション
  - Username（ユーザ名）：**admin**
- [H.323] セクション
  - Mode（モード）：Off（無効）
- [SIP] セクション
  - Mode（モード）：On（有効）
  - Port（ポート）：**7001**
  - Transport（トランスポート）：TLS
  - Mobile and remote access：Yes（はい）
  - TLS verify mode（TLS 検証モード）：On（有効）
  - TLS verify subject name（TLS 検証サブジェクト名）：**EXPc1.cisco.local**
  - Media encryption mode（メディア暗号化モード）：Force Encrypted（強制暗号化）
  - ICE support（ICE サポート）：Off（無効）
  - Poison mode（Poison モード）：Off（無効）





ステップ 3:[Create zone(ゾーンの作成)] をクリックします。

読者へのヒント

複数の Expressway によるクラスタを設定して、フェールオーバー（冗長性）サポートを提供し、拡張性を向上できます。Expressway クラスタの設定に関する詳細については、『Cisco Expressway cluster creation and maintenance deployment guide（Cisco Expressway クラスタの作成とメンテナンスに関する導入ガイド）』を参照してください。

Jabber エンドポイントおよび DNS の設定の詳細については、『Configure DNS for Cisco Jabber（Cisco Jabber 向けの DNS の設定）』を参照してください。

これで、Mobile & Remote Access が設定されました。VPN を使用せずに、Jabber エンドポイントを CUCM に登録できます。

プロセス

B2B の導入

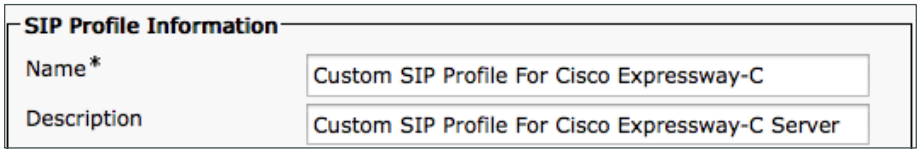
1. CUCM で Cisco Expressway-C 用に SIP プロファイルを設定する
2. CUCM で Cisco Expressway-C 用に SIP トランク セキュリティ プロファイルを設定する
3. CUCM で Expressway-C に SIP トランクを設定する
4. CUCM で B2B 用に SIP ルート パターンを設定する
5. ファイアウォールを設定する
6. Expressway-C で CUCM 用にネイバー ゾーンを設定する
7. Expressway-C で Expressway-E 用にトラバーサル クライアント ゾーンを設定する
8. Expressway-C で検索ルールを設定する
9. Expressway-C でトランスフォームを設定する
10. Expressway-E で Expressway-C 用にトラバーサル サーバ ゾーンを設定する
11. Expressway-E で DNS ゾーンを設定する
12. Expressway-E で検索ルールを設定する
13. Expressway-E でトランスフォームを設定する
14. パブリック DNS サーバで SRV レコードを設定する

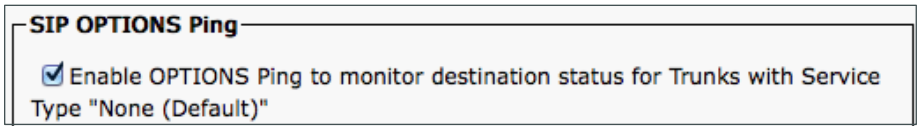
手順 1　CUCM で Cisco Expressway-C 用に SIP プロファイルを設定する

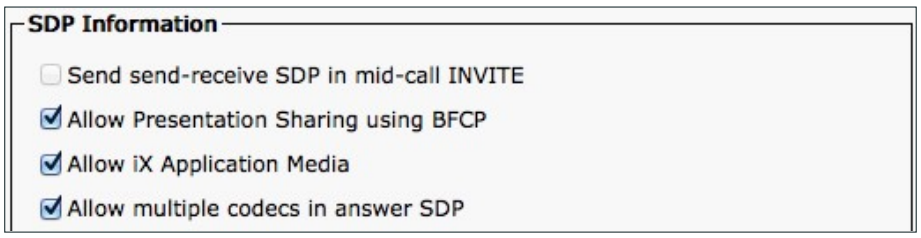
ステップ 1：[Device（デバイス）] > [Device Settings（デバイス設定）] > [SIP Profile（SIP プロファイル）] に移動し、[Add New（新規に追加）] をクリックします。

ステップ 2：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Name（名前）：**Custom SIP Profile For Cisco Expressway-C（Cisco Expressway-C 用のカスタム SIP プロファイル）**
- Description（説明）：**Custom SIP Profile For Cisco Expressway-C Server（Cisco Expressway-C サーバ用のカスタム SIP プロファイル）**
- Enable OPTIONS Ping to monitor destination status for Trunks with Service Type " None（Default）"（サービスタイプ「なし（デフォルト）」のトランクの接続先ステータスをモニタするために OPTIONS Ping を有効にする）：選択する
- Allow Presentation Sharing using BFCP（BFCP を使用するプレゼンテーション共有を許可）：選択する
- Allow iX Application Media（iX アプリケーション メディアを許可）：選択する
- Allow multiple codecs in answer SDP（応答 SDP で複数のコーデックを許可）：選択する







ステップ 3：[Save（保存）] をクリックします。

手順 2　CUCM で Cisco Expressway-C 用に SIP トランク セキュリティ プロファイルを設定する

B2B コールをルーティングする場合、CUCM と Expressway-C の間に SIP トランクを作成する必要があります。

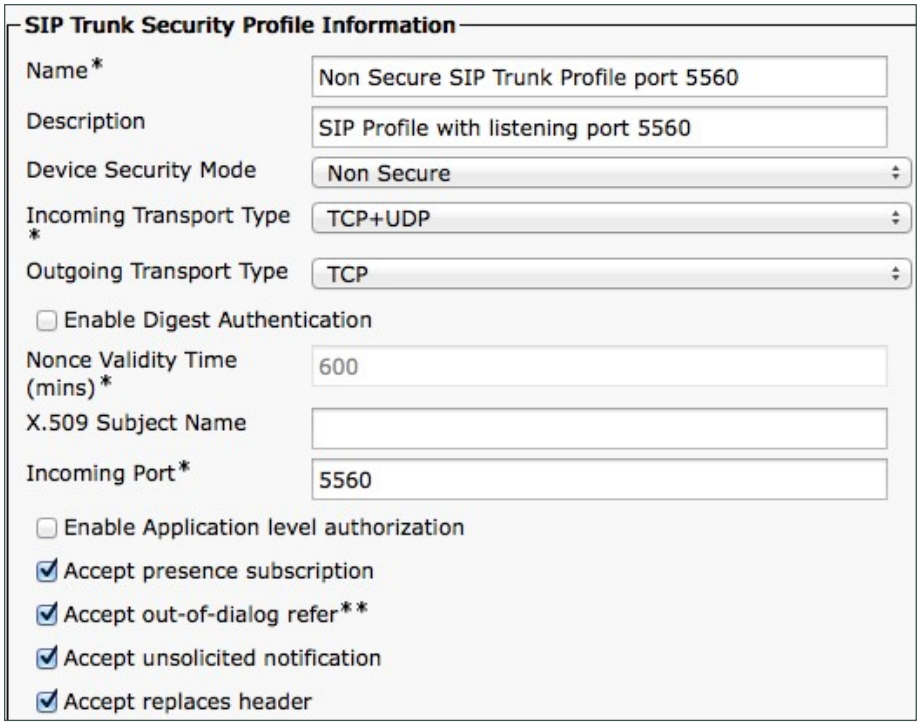
この設計では、Expressway-C はすでに Mobile & Remote Access 用の設定が済んでいます。Mobile & Remote Access シナリオでは、ポート 5060 がエンドポイントの回線側の登録に使用されます。CUCM では同じデバイスの同じポートを使用した回線側通信とトランク側通信を受け付けないので、Expressway-C と CUCM の間で 5060 を使用して SIP トランク形成することはできません。

そのため、Expressway-C から CUCM への SIP トランクでは、CUCM の受信側に別の SIP ポートを使用する必要があります。この設計では、SIP トランクの受信ポートとして **5560** を使用します。SIP 受信ポートを変更するには、新しい SIP トランク セキュリティ プロファイルを作成し、CUCM と Expressway-C の間に作成した SIP トランクにこのプロファイルを割り当てます。

ステップ 1：[System（システム）] > [Security（セキュリティ）] > [SIP Trunk Security Profile（SIP トランク セキュリティ プロファイル）] に移動し、[Add New（新規に追加）] をクリックします。

ステップ 2：該当するフィールドに、以下の値を入力します。

- Name（名前）：**Non Secure SIP Trunk Profile port 5560（セキュリティ保護されていない SIP トランク プロファイル ポート 5560）**
- Description（説明）：**SIP Profile with listening port 5560（リスニング ポートが 5560 の SIP プロファイル）**
- Incoming Port（受信ポート）：**5560**
- Accept presence subscription（プレゼンスの SUBSCRIBE の許可）：選択する
- Accept out-of-dialog refer（Out-of-Dialog REFER の許可）：選択する
- Accept unsolicited notification（Unsolicited NOTIFY の許可）：選択する
- Accept replaces header（Replaces ヘッダーの許可）：選択する



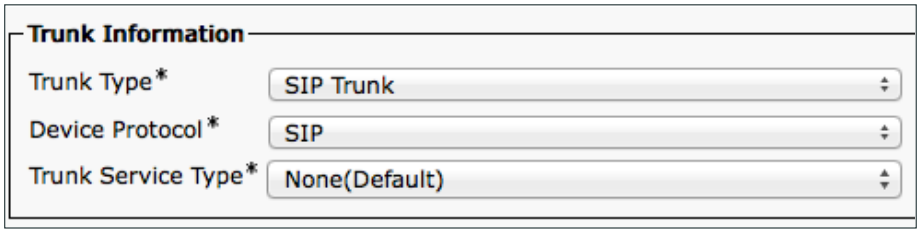
ステップ 3：[Save（保存）] をクリックします。

手順 3　CUCM で Expressway-C に SIP トランクを設定する

ステップ 1：[Device（デバイス）] > [Trunk（トランク）] に移動し、[Add New（新規追加）] をクリックします。

ステップ 2：該当するフィールドに、以下の値を入力します。

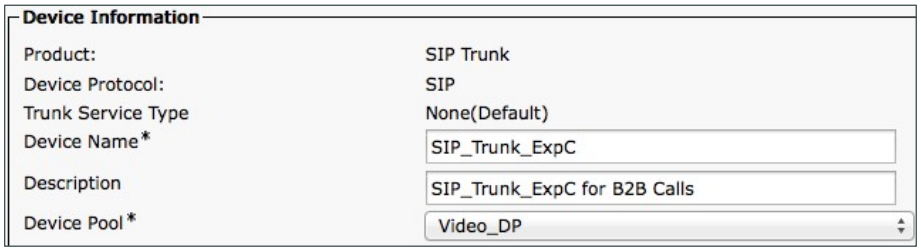
- Trunk Type（トランク タイプ）：SIP Trunk（SIP トランク）
- Device Protocol（デバイス プロトコル）：SIP
- Trunk Service Type（トランク サービス タイプ）：None(Default)（なし（デフォルト））

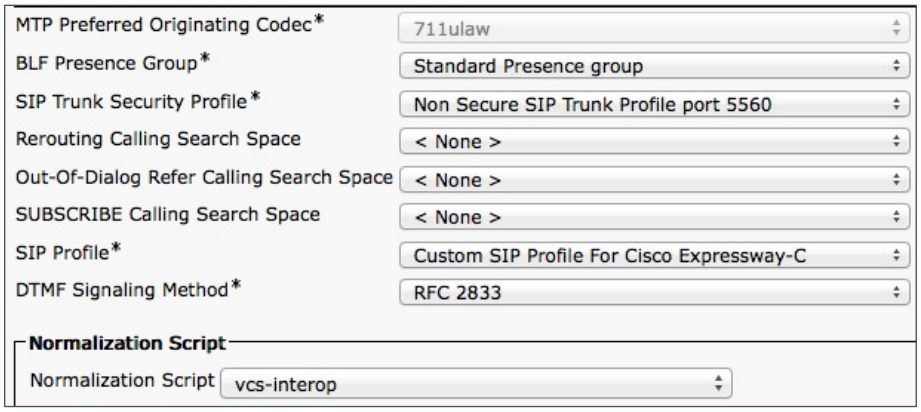


ステップ 3：[Next（次へ）] をクリックします。

ステップ 4：該当するフィールドに、以下の値を入力します。その他のフィールドは、そのデフォルト値のままにします。

- Device Name（デバイス名）：**SIP_Trunk_ExpC**
- Description（説明）：**SIP_Trunk_ExpC for B2B Calls（B2B コール用の SIP_Trunk_ExpC）**
- Device Pool（デバイス プール）：Video_DP
- Calling and Connected Party Info Format（発呼側および接続側情報形式）：Deliver URI only in connected party, if available（接続側にのみ URI を配信(使用可能な場合)）
- Destination Address（宛先アドレス）：**192.168.1.29**
- SIP Trunk Security Profile（SIP トランク セキュリティ プロファイル）：Non Secure SIP Trunk Profile port 5560（セキュリティ保護されていない SIP トランク プロファイル ポート 5560）
- SIP Profile（SIP プロファイル）：Custom SIP Profile For Cisco Expressway-C（Cisco Expressway-C 用のカスタム SIP プロファイル）
- DTMF Signaling Method（DTMF 信号方式）：RFC 2833
- Normalization Script（正規化スクリプト）：vcs-interop





ステップ 5:[Save(保存)] をクリックします。

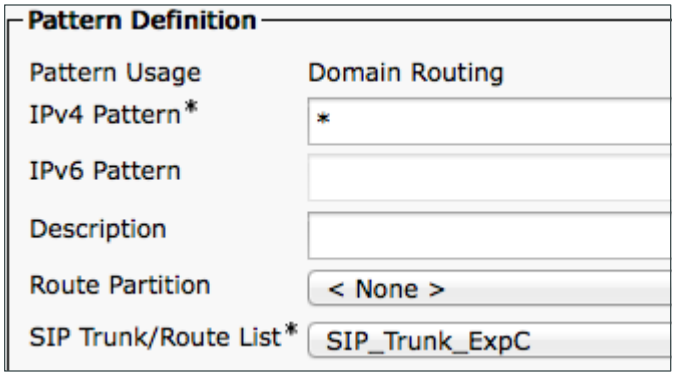
手順 4　CUCM で B2B 用に SIP ルート パターンを設定する

すべての B2B コールを Expressway-C にルーティングするため、以下の SIP ルート パターンが設定されますが、既存のルート パターンとは一致しません。

ステップ 1:[Call Routing(コール ルーティング)] > [SIP Route Pattern(SIP ルート パターン)] に移動し、[Add New(新規追加)] をクリックします。

ステップ 2:該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Pattern Usage(パターンの使用方法):Domain Routing(ドメイン ルーティング)
- IPv4 Pattern(IPv4 パターン):*
- SIP Trunk/Route List(SIP トランク/ルート リスト):SIP_Trunk_ExpC



ステップ 3:[Save(保存)] をクリックします。

手順 5　ファイアウォールを設定する

内部ネットワーク（Expressway-C がある場所）と DMZ（Expressway-E がある場所）間、および DMZ とパブリック インターネット間の以下のポートでトラフィックを許可するようにファイアウォールを設定する必要があります。

表 6 :Expressway-C（内部）から Expressway-E（DMZ）への送信

目的	トランスポート プロトコル	送信元ポート	宛先ポート
管理	TCP	>=1024	80/443/22/23
SNMP モニタリング	UDP	>=1024	161
RTP Assent	UDP	36002 ～ 59999	36000
RTCP Assent	UDP	36002 ～ 59999	36001
SIP TCP/TLS	TCP	25000 ～ 29999	7011
H.323 RAS Assent	UDP	1719	6011
Q.931/H.225 および H.245	TCP	15000 ～ 19999	2776

技術的なヒント

メディア ポート範囲の 36000 ～ 59999 のうち、最初の 2 つのポートは、多重化トラフィック専用として使用されます（大規模な VM 展開環境では、範囲内の最初の 12 個のポート 36000 ～ 36011 が使用されます）。

表 7 :Expressway-E（DMZ）から Expressway-C（内部）への送信

目的	トランスポート プロトコル	送信元ポート	宛先ポート
ロギング	UDP	30000 ～ 35999	514
管理	TCP	>=1024	80/443
LDAP（ログイン用、必要な場合）	TCP	30000 ～ 35999	389/636
NTP（時間の同期）	UDP	123	123
DNS	UDP	>=1024	53

表 8 :Expressway-E（DMZ）からパブリック インターネットへの送信

目的	トランスポート プロトコル	送信元ポート	宛先ポート
SIP TCP および TLS	TCP	25000 ～ 29999	>=1024
SIP UDP	UDP	5060	>=1024
RTP および RTCP	UDP	36000 ～ 59999	>=1024
DNS	UDP	>=1024	53
NTP（時間の同期）	UDP	123	123

表 9：パブリック インターネットから Expressway-E（DMZ）への受信

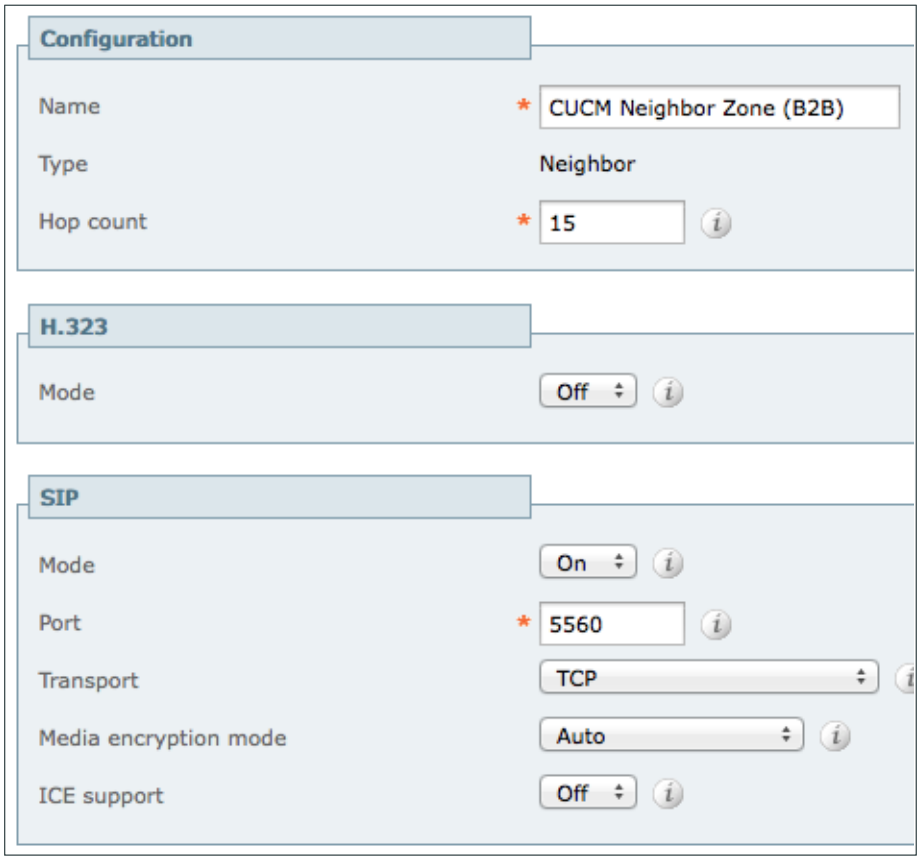
目的	トランスポート プロトコル	送信元ポート	宛先ポート
SIP UDP	UDP	>=1024	5060
SIP TLS	TCP	>=1024	5061
RTP および RTCP	UDP	>=1024	36002 ～ 59999

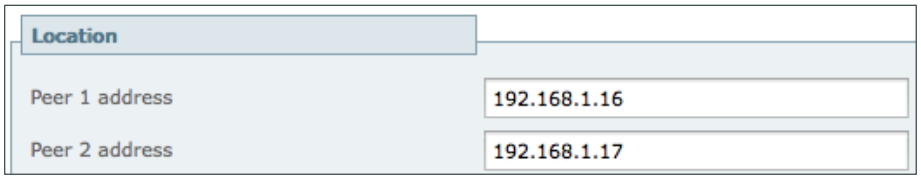
手順 6　Expressway-C で CUCM 用にネイバー ゾーンを設定する

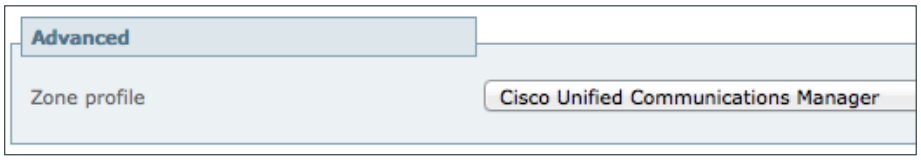
ステップ 1：[Configuration（設定）] > [Zones（ゾーン）] > [Zones（ゾーン）] に移動し、[New（新規）] をクリックします。

ステップ 2：該当するフィールドに、以下の値を入力します。

- Name（名前）：**CUCM Neighbor Zone（B2B）（CUCM ネイバー ゾーン（B2B））**
- Type（タイプ）：Neighbor（ネイバー）
- H.323 Mode（H.323 モード）：Off（無効）
- SIP Mode（SIP モード）：On（有効）
- Port（ポート）–**5560**
- Transport（トランスポート）：TCP
- Peer 1 Address（ピア 1 アドレス）：**192.168.1.16**
- Peer 2 Address（ピア 1 アドレス）：**192.168.1.17**
- Zone Profile（ゾーン プロファイル）：Cisco Unified Communications Manager







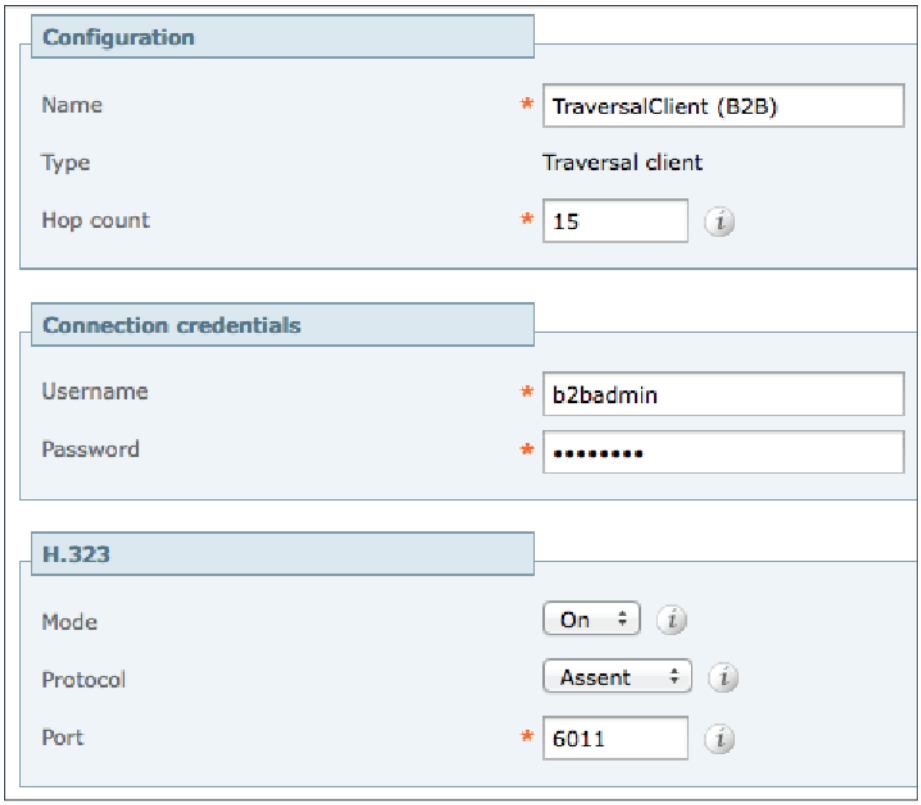
ステップ 3:[Create zone(ゾーンの作成)] をクリックします。

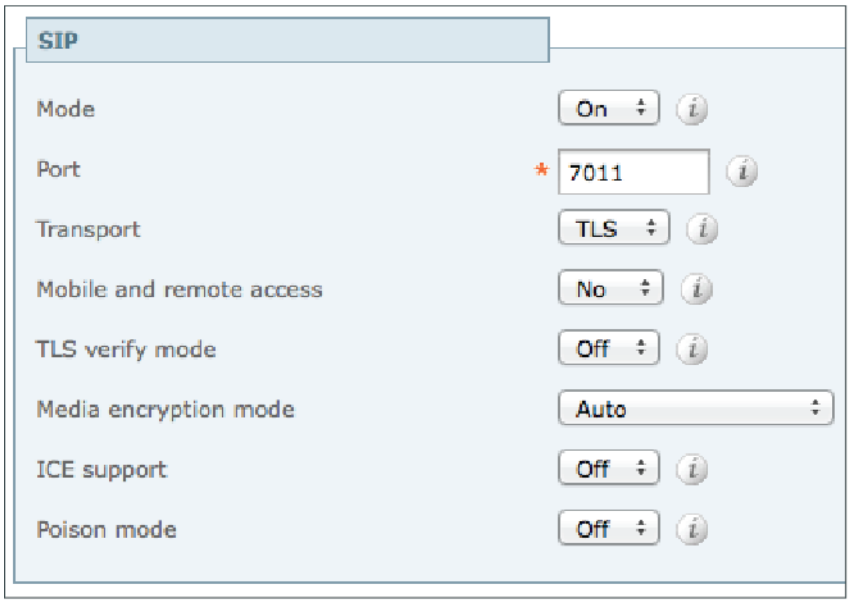
手順 7 Expressway-C で Expressway-E 用にトラバーサル クライアント ゾーンを設定する

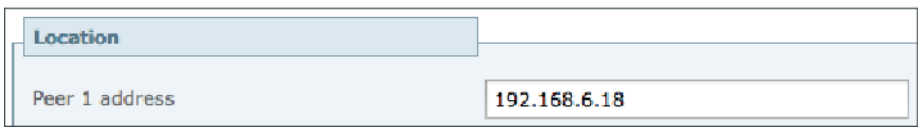
ステップ 1:[Configuration(設定)] > [Zones(ゾーン)] > [Zones(ゾーン)] に移動し、[New(新規)] をクリックします。

ステップ 2:該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Name(名前):**TraversalClient(B2B)**
- Type(タイプ):Traversal Client(トラバーサル クライアント)
- Username(ユーザ名):**b2badmin**
- Password(パスワード):**[パスワード]**
- H.323 Port(H.323 ポート):**6011**
- SIP Port(SIP ポート):**7011**
- Mobile and remote access:No(いいえ)
- Transport(トランスポート):TLS
- Peer 1 Address(ピア 1 アドレス):**192.168.6.18**


Configuration
Name
TraversalClient (B2B)
Type
Traversal client
Hop count
15
Connection credentials
Username
b2badmin
Password
H.323
Mode
On
Protocol
Assent
Port
6011


SIP
Mode
On
Port
7011
Transport
TLS
Mobile and remote access
No
TLS verify mode
Off
Media encryption mode
Auto
ICE support
Off
Poison mode
Off


Location
Peer 1 address
192.168.6.18

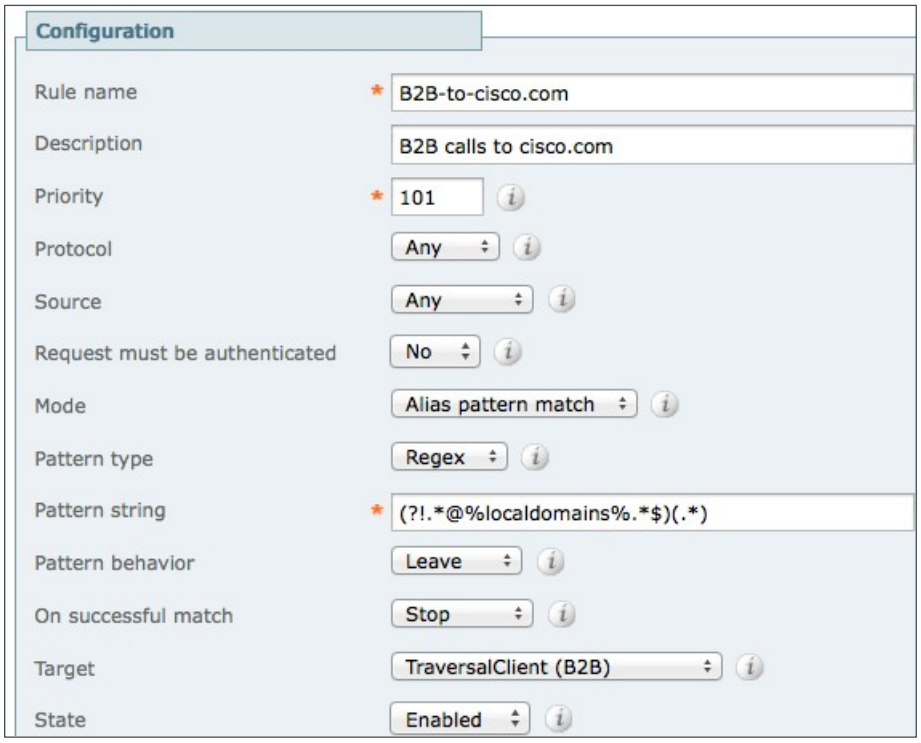
ステップ 3:[Create zone(ゾーンの作成)] をクリックします。

手順 8 Expressway-C で検索ルールを設定する

ステップ 1:[Configuration(設定)] > [Dial Plan(ダイヤル プラン)] > [Search Rules(検索ルール)] に移動し、[New(新規)] をクリックします。

ステップ 2:該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Rule Name(ルール名):**B2B-to-cisco.com**
- Description(説明):**cisco.com への B2B コール**
- Priority(プライオリティ):**101**
- Mode(モード):Alias Pattern Match(エイリアスのパターン マッチ)
- Pattern type(パターン タイプ):Regex(正規表現)
- Pattern String(パターン文字列):**(?!.*@%localdomains%.*$)(.*)**
- Pattern Behavior(パターン動作):Leave(変更なし)
- On Successful Match(正常に一致する場合):Stop(停止)
- Target(ターゲット):TraversalClient(B2B)
- State(状態):Enabled(有効)

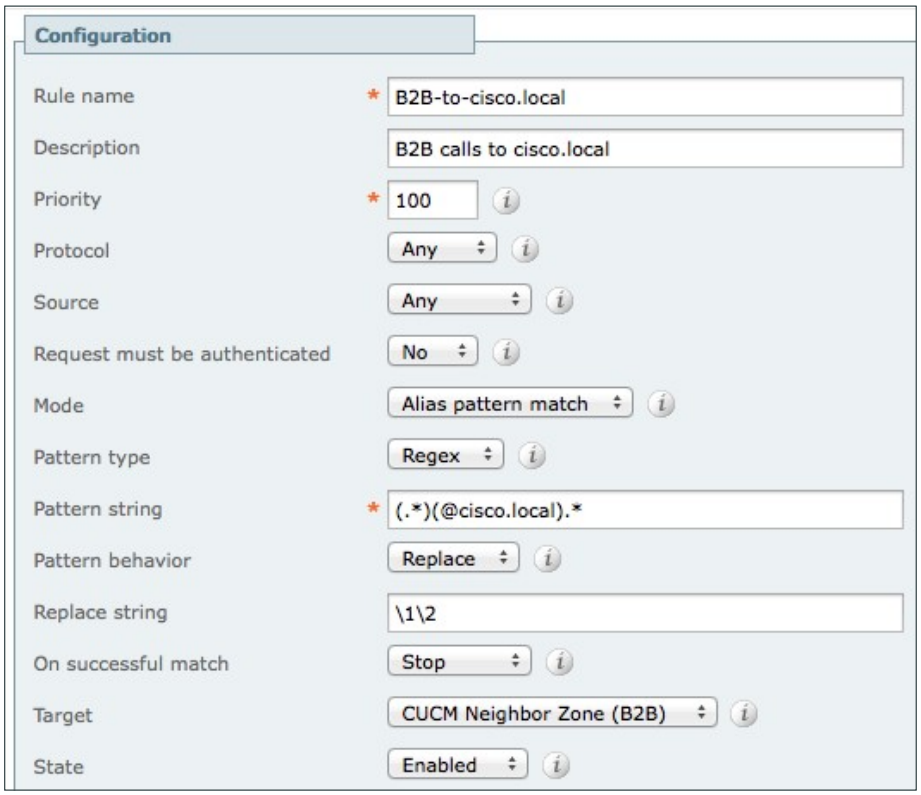


ステップ 3:[Create Search Rule(検索ルールの作成)] をクリックします。

ステップ 4:[New(新規)] をクリックします。

ステップ 5：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Rule Name（ルール名）：**B2B-to-cisco.local**
- Description（説明）：**cisco.local への B2B コール**
- Priority（プライオリティ）：**100**
- Mode（モード）：Alias Pattern Match（エイリアスのパターン マッチ）
- Pattern type（パターン タイプ）：Regex（正規表現）
- Pattern String（パターン文字列）：**(.*)(@cisco.local).***
- Pattern Behavior（パターン動作）：Replace（置換）
- Replace String（置換文字列）：**\1\2**
- On Successful Match（正常に一致する場合）：Stop（停止）
- Target（ターゲット）：CUCM Neighbor Zone（B2B）（CUCM ネイバー ゾーン（B2B））
- State（状態）：Enabled（有効）



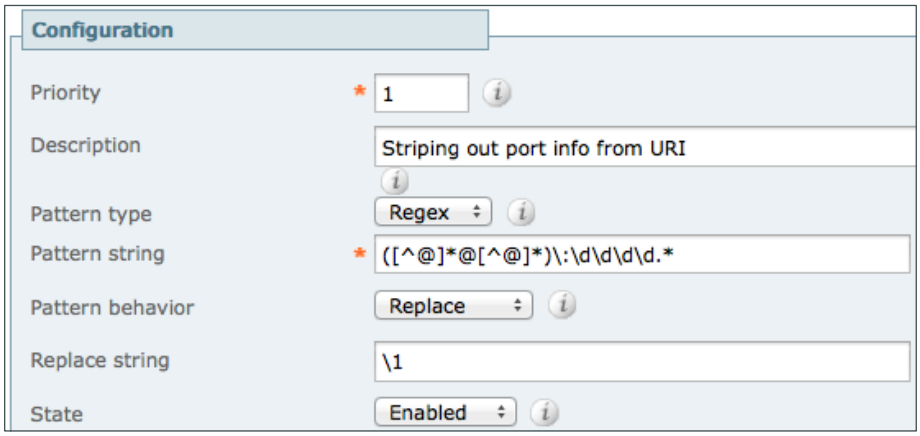
ステップ 6：[Create Search Rule（検索ルールの作成）] をクリックします。

手順 9　Expressway-C でトランスフォームを設定する

ステップ 1：[Configuration（設定）] > [Dial Plan（ダイヤル プラン）] > [Transforms（トランスフォーム）] に移動し、[New（新規）] をクリックします。

ステップ 2：該当するフィールドに、以下の値を入力します。

- Priority（優先度）：**1**
- Description（説明）：**Striping out port info from URI（URI からポート情報を除去）**
- Pattern type（パターン タイプ）：Regex（正規表現）
- Pattern string（パターン文字列）：**([^@]*@[^@]*)\:\d\d\d\d.***
- Pattern Behavior（パターン動作）：Replace（置換）
- Replace String（置換文字列）：**\1**
- State（状態）：Enabled（有効）



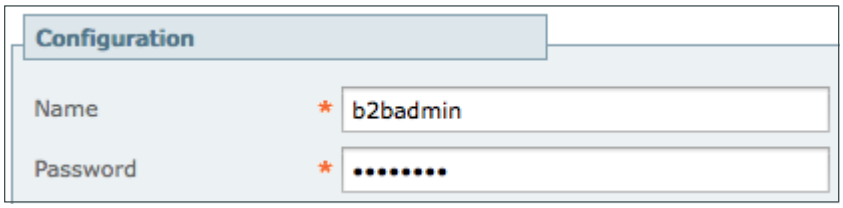
ステップ 3：[Create Transform（トランスフォームの作成）] をクリックします。

手順 10　Expressway-E で Expressway-C 用にトラバーサル サーバ ゾーンを設定する

ステップ 1：[Configuration（設定）] > [Authentication（認証）] > [Local Database（ローカル データベース）] に移動し、[New（新規）] をクリックします。

ステップ 2：該当するフィールドに、以下の値を入力します。

- Name（名前）：**b2badmin**
- Password（パスワード）：**[パスワード]**

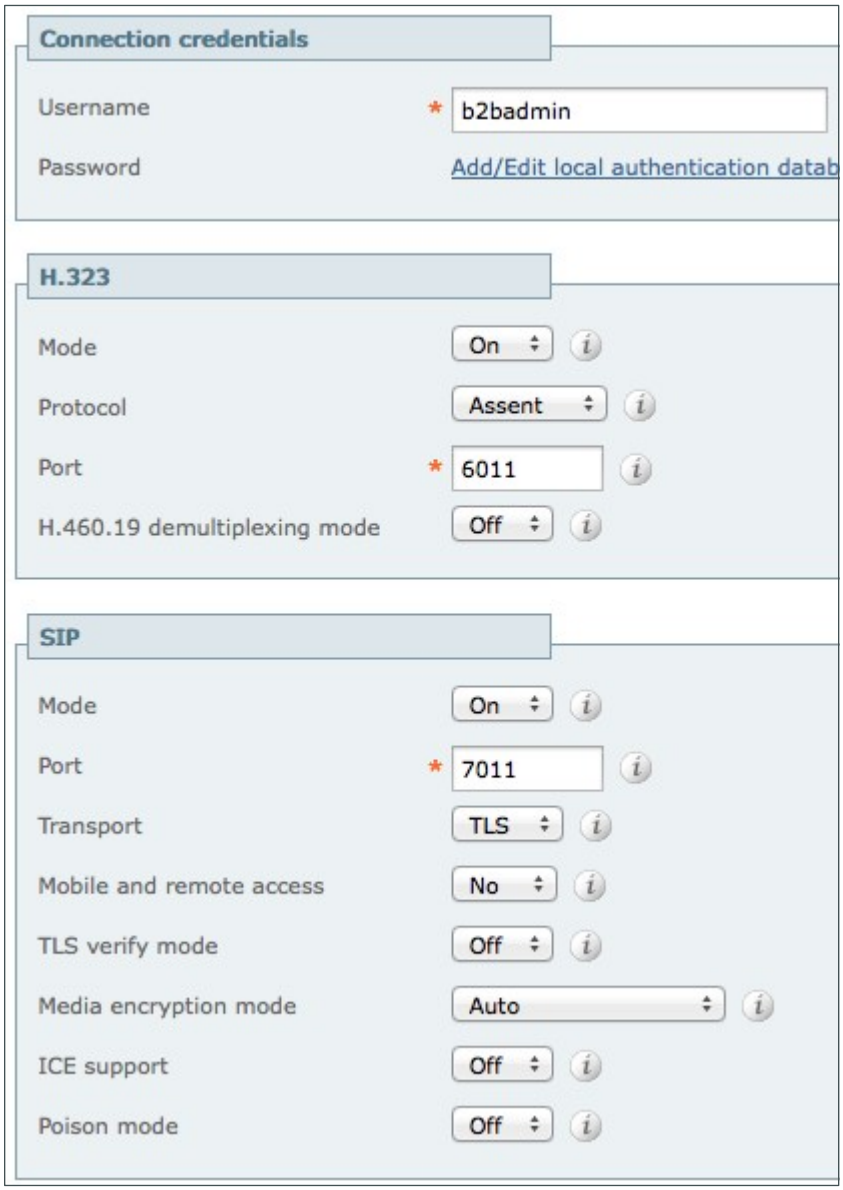


ステップ 3：[Create credential（クレデンシャルの作成）] をクリックします。

ステップ 4：[Configuration（設定）] > [Zones（ゾーン）] > [Zones（ゾーン）] に移動し、[New（新規）] をクリックします。

ステップ 5：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Name（名前）：**TraversalServer（B2B）**
- Type（タイプ）：Traversal Server（トラバーサル サーバ）
- Username（ユーザ名）：**b2badmin**
- H.323 Port（H.323 ポート）：**6011**
- SIP Port（SIP ポート）：**7011**
- Mobile and remote access：No（いいえ）
- Transport（トランスポート）：TLS



ステップ 6：[Create zone（ゾーンの作成）] をクリックします。

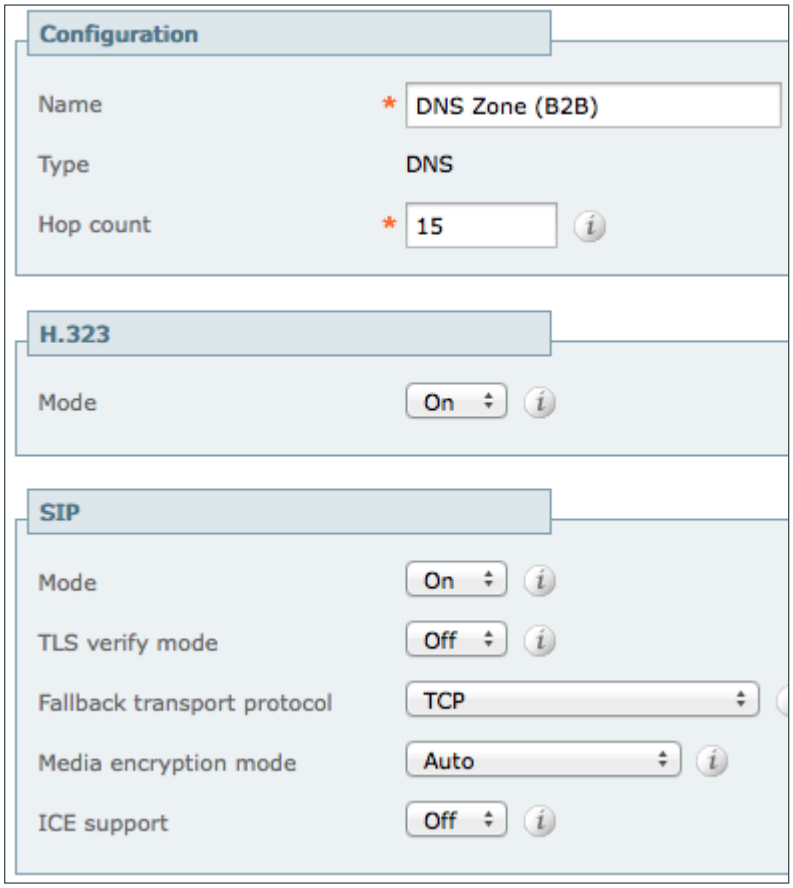
手順 11　Expressway-E で DNS ゾーンを設定する

B2B コールの場合、Expressway-E は異なるドメインに対するコールのルーティング先がわかりません。Expressway-E では、そのドメイン用にネイバーが作成されません。そのため、Expressway-E はすべてのコールをパブリック DNS サーバにルーティングします。

ステップ 1：[Configuration（設定）] > [Zones（ゾーン）] > [Zones（ゾーン）] に移動し、[New（新規）] をクリックします。

ステップ 2：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Name（名前）：**DNS Zone（B2B）（DNS ゾーン（B2B））**
- Type（タイプ）：DNS
- H.323 Mode（H.323 モード）：On（有効）
- SIP Mode（SIP モード）：On（有効）
- Fallback Transport Protocol（フォールバック トランスポート プロトコル）：TCP



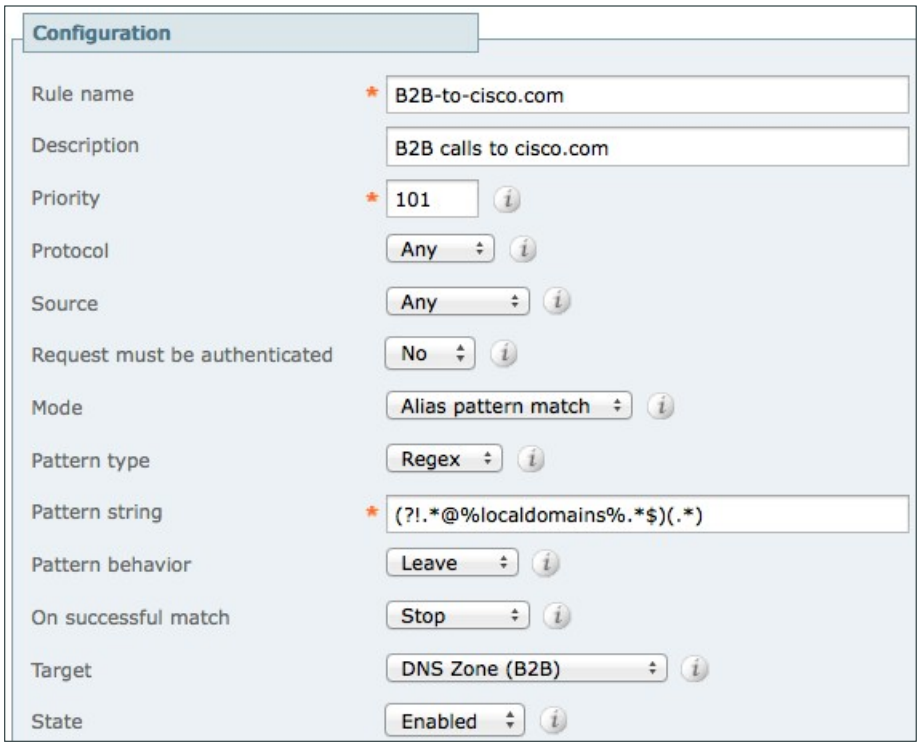
ステップ 3：[Create zone（ゾーンの作成）] をクリックします。

手順 12　Expressway-E で検索ルールを設定する

ステップ 1：[Configuration（設定）] > [Dial Plan（ダイヤル プラン）] > [Search Rules（検索ルール）] に移動し、[New（新規）] をクリックします。

ステップ 2：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Rule Name（ルール名）：**B2B-to-cisco.com**
- Description（説明）：**cisco.com への B2B コール**
- Priority（プライオリティ）：**101**
- Mode（モード）：Alias Pattern Match（エイリアスのパターン マッチ）
- Pattern type（パターン タイプ）：Regex（正規表現）
- Pattern String（パターン文字列）：**(?!.*@%localdomains%.*$)(.*)**
- Pattern Behavior（パターン動作）：Leave（変更なし）
- On Successful Match（正常に一致する場合）：Stop（停止）
- Target（ターゲット）：DNS Zone（B2B）（DNS ゾーン（B2B））
- State（状態）：Enabled（有効）

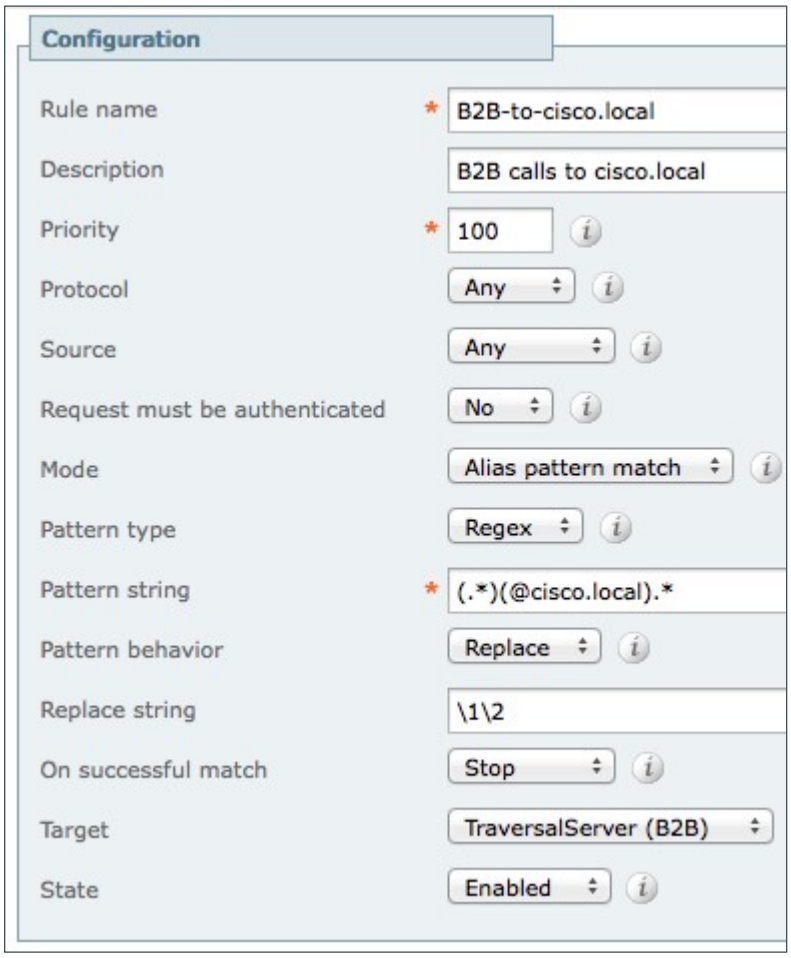


ステップ 3：[Create Search Rule（検索ルールの作成）] をクリックします。

ステップ 4：[New（新規）] をクリックします。

ステップ 5：該当するフィールドに以下を入力し、その他のフィールドはデフォルト値のままにします。

- Rule Name（ルール名）：**B2B-to-cisco.local**
- Description（説明）：**cisco.local への B2B コール**
- Priority（プライオリティ）：**100**
- Mode（モード）：Alias Pattern Match（エイリアスのパターン マッチ）
- Pattern type（パターン タイプ）：Regex（正規表現）
- Pattern String（パターン文字列）：**(.*)(@cisco.local).***
- Pattern Behavior（パターン動作）：Replace（置換）
- Replace String（置換文字列）：**\1\2**
- On Successful Match（正常に一致する場合）：Stop（停止）
- Target（ターゲット）：TraversalServer（B2B）
- State（状態）：Enabled（有効）



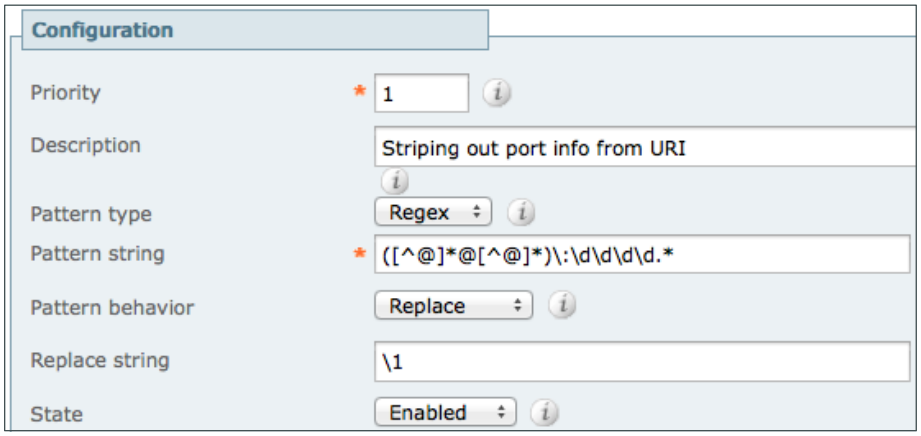
ステップ 6：[Create Search Rule（検索ルールの作成）] をクリックします。

手順 13　Expressway-E でトランスフォームを設定する

ステップ 1：[Configuration（設定）] > [Dial Plan（ダイヤル プラン）] > [Transforms（トランスフォーム）] に移動し、[New（新規）] をクリックします。

ステップ 2：該当するフィールドに、以下の値を入力します。

- Priority（優先度）：**1**
- Description（説明）：**Striping out port info from URI（URI からポート情報を除去）**
- Pattern type（パターン タイプ）：Regex（正規表現）
- Pattern string（パターン文字列）：**([^@]*@[^@]*)\:\d\d\d\d.***
- Pattern Behavior（パターン動作）：Replace（置換）
- Replace String（置換文字列）：**\1**
- State（状態）：Enabled（有効）



ステップ 3：[Create Transform（トランスフォームの作成）] をクリックします。

手順 14　パブリック DNS サーバで SRV レコードを設定する

エンドポイントが Expressway-E を検出して Business-to-Business（B2B）コールをルーティングできるように、パブリック DNS サーバに以下の SRV レコードと A レコードが設定されていることを確認します。

```
_sip._tcp.cisco.local. SRV 10 10 5060 expe1.cisco.local
_sip._udp.cisco.local. SRV 10 10 5060 expe1.cisco.local
expe1.cisco.local.    IN     A   192.168.6.18
```

付録 A: 製品リスト

コンポーネント	製品説明	部品番号	ソフトウェア
コール制御	Cisco Business Edition 6000（最大 1000 ユーザ）	BE6K-SW-10.0	10.0
Cisco Collaboration Edge	Cisco Expressway-C	EXPWY-VE-C-K9	s42700x8_1_0
	Cisco Expressway-E	EXPWY-VE-E-K9	
ソフト クライアント	Cisco Jabber for Windows	JAB9-DSK-K9	9.6（試験用）
	Cisco Jabber for IOS		9.6

フィードバック

このガイドに関するコメントや提案を送信する場合は、フィードバック フォームをご利用ください。

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間: 平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

14.06

B-470-COL-1 04/14