Cisco Unified SIP Proxy の概要

Cisco Unified Session Initiation Protocol（SIP）Proxy Release 8.5 のオンライン ヘルプへようこそ。

- このファイルでヘルプ トピックを検索するには、このページの右上にある [Search] フィールドに用語を入力します。
- [Contents] タブまたは [Index] タブの下の左側にある、トピックのリストをスクロールすることもできます。
- このオンライン ヘルプ システムのすべての内容の PDF を参照するには、[View PDF] をクリックします。

Cisco Unified SIP Proxy Release 8.5 の詳細については、次の URL から入手できる Cisco Unified SIP Proxy のマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps10475/tsd_products_support_series_home.html

ヒント Cisco Unified SIP Proxy を使用する場合、ブラウザの [Back] ボタンおよび [Forward] ボタンを使用して別のウィンドウの情報を表示できますが、そのウィンドウで変更を行い、変更を送信すると、エラーを受け取り、その変更は保存され**ません**。**ブラウザのナビゲーション ツールを使用して別のウィンドウに移動した後で、情報を送信しないでください**。該当するボタンまたはメニューをクリックして、情報を入力するウィンドウに到達します。

- 「設定タスクの概要」
- 「Cisco Unified SIP Proxy グラフィカル ユーザ インターフェイス（GUI）へのログイン」
- 「ダッシュボードについて」

設定タスクの概要

次に、Cisco Unified SIP Proxy システムを使用する前に必要なタスクの概要を示します。

タスク	情報の入手先
始める前に	
Cisco Unified SIP Proxy システムをインストールします。	『*Installation Guide for Cisco Unified SIP Proxy Release 8.5*』
設定	
SIP スタックを設定します。	「SIP スタックの設定」
ネットワーク パラメータを設定します。	「ネットワークの設定」

タスク	情報の入手先
システムのトリガーを設定します。	「トリガーの設定」
サーバ グループを編集します。	「サーバ グループの設定」
ルート グループを設定します。	「ルート グループの設定」
ルート テーブルを設定します。	「ルート テーブルの設定」
ルート ポリシーを設定します。	「ルート ポリシーの設定」
正規化ポリシーを設定します。	「正規化ポリシーの設定」
時間ポリシーを設定します。	「時間ポリシーの設定」
ルーティング トリガーを設定します。	「ルーティング トリガーの設定」
正規化トリガーを設定します。	「正規化トリガーの設定」
Lite モードをイネーブル化またはディセーブル化します。	「Cisco Unified SIP Proxy モジュールのリロードおよび、Lite モードのイネーブル化とディセーブル化」
モニタリング	
システム情報を表示します。	「システム情報の表示」
Cisco Unified SIP Proxy システムのステータスをモニタします。	「Cisco Unified SIP Proxy システムのモニタリング」
ライセンス情報を表示します。	「ライセンス情報の表示」
メンテナンス	
定期的に Cisco Unified SIP Proxy システムをバックアップします。必要に応じて、復元します。	「バックアップと復元の設定」
トラブルシューティング	
必要に応じて Cisco Unified SIP Proxy システムをトラブルシューティングします。	「トラブルシューティング」

Cisco Unified SIP Proxy グラフィカル ユーザ インターフェイス（GUI）へのログイン

制約事項

Cisco Unified SIP Proxy GUI だけが次の Web ブラウザをサポートします。

- Internet Explorer Release 7 および 8
- Mozilla Firefox Release 3

始める前に

- Cisco Unified SIP Proxy Release 8.5 をインストールします。詳細については、『Installation Guide for Cisco Unified SIP Proxy Release 8.5』を参照してください。
- インストレーション中に入力した、管理者のユーザ名およびパスワードを用意します。

手順

ステップ 1 Web ブラウザを開始します。

ステップ 2 Cisco Unified SIP Proxy システムの IP アドレスを入力します。

ログイン画面が表示されます。

ステップ 3 管理者名を入力します。

ステップ 4 管理者パスワードを入力します。

ステップ 5 [Log In] をクリックします。

Cisco Unified SIP Proxy の GUI 内に Cisco Unified SIP Proxy ダッシュボードが表示されます。

ダッシュボードについて

ダッシュボードには、システムの健全性およびステータスに関する一般情報が含まれます。

- サーバ グループ ステータスの下に、サーバ グループの動作ステータスが表示されます。ステータスはアップまたはダウンです。
- コール ルーティング サマリー（最近 72 時間）の下に、次の数値が表示されます。
  - 処理された総コール数
  - ドロップされたコール数
  - ピーク CPS
  - 平均 CPS

いずれかのヘッダーをクリックすると、[Monitoring] ページに移動します。「Cisco Unified SIP Proxy システムのモニタリング」を参照してください。

商用オープン ソース ライセンシング

Cisco Unified SIP Proxy Release 8.5 用に作成されたソフトウェアのコンポーネントの一部は、オープン ソース ライセンシングまたは商用ライセンシングを通じて提供されています。これらのコンポーネントおよび関連する著作権宣言文については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps10475/products_licensing_information_listing.html

Cisco Unified SIP Proxy Release 8.5 マニュアルのロードマップ

主なマニュアル リスト

- 『*Release Notes for Cisco Unified SIP Proxy Release 8.5*』
- 『*Open Source Licensing for Cisco Unified SIP Proxy Release 8.5*』
- 『*Install Guide for Cisco Unified SIP Proxy Release 8.5*』
- 『*CLI Configuration Guide for Cisco Unified SIP Proxy Release 8.5*』
- 『*CLI Command Reference for Cisco Unified SIP Proxy Release 8.5*』
- 『*GUI Administration Guide for Cisco Unified SIP Proxy Release 8.5*』

リリースおよび一般的な情報

ライセンス情報

『*Open Source Licensing for Cisco Unified SIP Proxy Release 8.5*』

この製品で使用されているオープン ソース ソフトウェアに関する情報が含まれています。

この資料は、http://www.cisco.com/en/US/products/ps10475/products_licensing_information_listing.html から入手できます。

リリース ノート

『*Release Notes for Cisco Unified SIP Proxy Release 8.5*』

システム要件、ライセンス情報、新しい機能、制限事項、参考資料が記載されています。

この資料は、http://www.cisco.com/en/US/products/ps10475/prod_release_notes_list.html から入手できます。

リファレンス ガイド

コマンド リファレンス

『*Command Reference for Cisco Unified SIP Proxy Release 8.5*』

Command-Line Interface（CLI; コマンドライン インターフェイス）を使用した Cisco Unified SIP Proxy Release 8.5 ソフトウェアの設定に関するヒントが記載されています。使用できる CLI コマンドおよび構文の一覧です。

この資料は、http://www.cisco.com/en/US/products/ps10475/prod_command_reference_list.html から入手できます。

インストールおよびアップグレード

インストールおよびアップグレード ガイド

『*Installation Guide for Cisco Unified SIP Proxy Release 8.5*』

Cisco Unified SIP Proxy Release 8.5 のインストール方法およびライセンスのインストールに関する情報が記載されています。

この資料は、http://www.cisco.com/en/US/products/ps10475/prod_installation_guides_list.html から入手できます。

維持および操作

維持および操作ガイド

『*CLI Configuration Guide for Cisco Unified SIP Proxy Release 8.5*』

Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、Cisco Unified SIP Proxy システムのセットアップ、設定、操作、維持を行う方法を説明します。

この資料は、
http://www.cisco.com/en/US/products/ps10475/products_installation_and_configuration_guides_list.html
から入手できます。

『*GUI Administration Guide for Cisco Unified SIP Proxy Release 8.5*』

このマニュアルは、Cisco Unified SIP Proxy の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）にあるオンライン ヘルプと同一です。GUI を使用して、Cisco Unified SIP Proxy システムのセットアップ、設定、操作、維持を行う方法に関する情報が含まれています。

この資料は、
http://www.cisco.com/en/US/products/ps10475/products_installation_and_configuration_guides_list.html
から入手できます。

Cisco DocWiki 上のトラブルシューティング情報

Cisco Unified SIP Proxy のトラブルシューティング情報は、http://docwiki.cisco.com/wiki/Cisco_Unified_SIP_Proxy の Cisco DocWiki から入手できます。

DocWiki の情報は、Cisco.com ユーザ ID とパスワードを持つ人は誰でも更新できます。このように、トラブルシューティング情報は、Cisco とお客様との共同作業です。

販売資料

http://www.cisco.com/en/US/products/ps10140/index.html から入手可能な、Cisco Unified SIP Proxy Release 8.5 の販売資料（データ シートを含む）を参照してください。

ソフトウェアのダウンロード

Cisco Unified SIP Proxy Release 8.5 ソフトウェアをダウンロードするには、http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=282713225 にナビゲートします。

SIP スタックの設定

SIP スタックの一般的な設定の参照と編集

手順

ステップ 1 [Configure] > [SIP Stack] > [General Settings] を選択します。

一般的な SIP 設定の一覧が示された、[SIP Stack Settings] ページが表示されます。

ステップ 2 表 1 の説明のように、値を更新します。

表 1　SIP スタックの一般的な設定

パラメータ	説明
SIP メッセージ	
SIP Header Compaction	SIP ヘッダー圧縮をイネーブルにするかどうか。 イネーブルの場合、次の SIP ヘッダーに対して圧縮ヘッダー形式が使用されます。 • Call-ID • Contact • Content-Encoding • Content-Length • Content-Type • From • Subject • To • Via ヘッダー圧縮がディセーブルの場合、ヘッダー形式にかかわらず、すべての発信メッセージで SIP ヘッダー全体が使用されます。
SIP Message Logging	すべての着信および発信 SIP メッセージのロギングをイネーブルにするかどうか。 **（注）** SIP ロギングをオンにすると、Cisco Unified SIP Proxy のパフォーマンスに大きな影響を与えます。
SIP Statistics	アクティブな SIP キューの統計情報を表示するかどうか。
Period Time	（オプション。[SIP Statistics] をオンにした場合にのみ使用可能）peg-logging 統計情報を収集する頻度を決定します。
Reset Time	（オプション。[SIP Statistics] をオンにした場合にのみ使用可能）peg-logging 統計情報をリセットする頻度を決定します。
Max Forwards	要求が別のサーバに転送できる最大回数を指定します。要求がサーバによって受信されるたびに、この値が 1 減ります（要求に Max Forwards ヘッダーがない場合は、値に 1 が追加されます）。値が 0 になると、サーバは 483（Too Many Hops）応答で応答し、トランザクションを終了します。 Max Forwards ヘッダー フィールドを使用して、ネットワーク内の転送ループを検出できます。 指定できる値は 0 ～ 255 です。デフォルト値は 70 です。 **（注）** このコマンドの値は 10 以上 100 以下に設定することを推奨します。

表 1　SIP スタックの一般的な設定 （続き）

パラメータ	説明
過負荷	
Reject	サーバが過負荷状態になったときに 503 （Server Unavailable）応答を送信するようにサーバを設定します。
Retry After	（オプション。[Reject] を選択した場合にのみ使用可能） 送信者がトランザクションを再度試行できる場合に指定する、503（Server Unavailable）応答の SIP Retry-After ヘッダー フィールドの送信秒数。このオプションを指定しない場合、503 （Server Unavailable）応答に Retry-After ヘッダー フィールドが含まれません。指定できる最小値は 0 です。デフォルト値は 0 です。
Redirect	サーバが過負荷状態になったときに 300 （Redirect）応答を送信するようにサーバを設定します。
IP Address	（オプション。[Redirect] を選択した場合にのみ使用可能） SIP Contact ヘッダー フィールドで送信されるリダイレクト インターフェイス ホスト名または IP アドレスです。以降の要求はこのアドレスでサーバにリダイレクトされます。
Port	（オプション。[Redirect] を選択した場合にのみ使用可能） リダイレクト ホストのポート。有効な範囲は 1024 ～ 65535 です。デフォルトは 5060 です。
Transport Type	（オプション。[Redirect] を選択した場合にのみ使用可能）リダイレクト ホストにより使用される転送プロトコルです。UDP、TCP、または TLS の場合があります。
DNS 設定	
DNS SRV Lookups	SIP DNS SRV ルックアップ コマンドを設定します。
DNS NAPTR Lookups	ドメイン ホスト名 /IP アドレス マッピングの、DNS NAPTR の使用をイネーブルにします。
TCP 設定	
Idle Connection Timeout	キープアライブ プローブの送信前に渡すことができる、アイドル時間の長さを設定します。
Maximum Connections	TCP/TLS 接続の最大数を設定します。TCP/TLS 接続が最大数に達した場合、パッシブ（着信）接続は受け入れられず、追加のアクティブ（発信）接続は行うことができます。

表 1　SIP スタックの一般的な設定 （続き）

パラメータ	説明
TLS 設定	
TLS Settings	他の SIP エンティティとの SIP Transport Layer Security（TLS; トランスポート層セキュリティ）接続の使用をイネーブルにします。これによって、インターネット経由のセキュアな通信が実現されます。 イネーブルまたはディセーブルのいずれかに設定できます。

ステップ 3　[Update] をクリックします。

関連項目

「SIP スタックの設定」の目次ページに戻る

エイリアス FQDN の追加と削除

手順

ステップ 1　[Configure] > [SIP Stack] > [Alias FQDNs] を選択します。

[Alias FQDNs] ページが表示されます。

ステップ 2　エイリアス FQDN を追加するには、次の操作を実行します。

a.　名前を入力します。

b.　[Add Alias] をクリックします。

ステップ 3　エイリアス FQDN を削除するには、次の操作を実行します。

a.　削除するエイリアス FQDN の名前の横にあるボックスをオンにします。

b.　[Remove] をクリックします。

関連項目

「SIP スタックの設定」の目次ページに戻る

信頼できるピアの追加と削除

この手順では、1 つまたは複数の SIP TLS の信頼できるピアが作成されます。リモート側の ID と、信頼できる設定済みのピアの ID が一致しない限り、TLS 接続の確立は失敗します。信頼できるピアが設定されていない場合、TLS ハンドシェイクが成功すれば、接続は受け入れられます。

手順

ステップ 1 [Configure] > [SIP Stack] > [TLS Trusted Peers] を選択します。

[TLS Trusted Peers] ページが表示されます。

ステップ 2 TLS の信頼できるピアを追加するには、次の操作を実行します。

a. 名前を入力します。

b. [Add Trusted Peer] をクリックします。

ステップ 3 TLS の信頼できるピアを削除するには、次の操作を実行します。

a. 削除する TLS の信頼できるピアの名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

関連項目

「SIP スタックの設定」の目次ページに戻る

ネットワークの設定

ネットワークのリストの表示

SIP ネットワークは、一般的なルーティング目的のものと同様と見なせるローカル インターフェイスの論理集合です。

手順

ステップ 1 [Configure] > [Networks] を選択します。

[Networks] ページに、現在のすべてのネットワークの一覧が表示されます。

関連項目

「ネットワークの設定」の目次ページに戻る

ネットワークの追加

制約事項

SIP ネットワークの作成後は、SIP ネットワークを削除できません。

手順

ステップ 1 [Configure] > [Networks] を選択します。

[Networks] ページが表示されます。

ステップ 2 [Add] をクリックします。

[Networks] ページが表示されます。

ステップ 3 次のネットワークに関する情報を入力します。

パラメータ	説明
Name	このネットワークの名前です。ネットワークの名前には、英数字、ピリオド、ダッシュ、およびアンダースコアを使用できます。 **ヒント** ネットワークの名前は変更できないため、慎重に名前を選択します。
Type	次のいずれかを指定できます。 • [standard] : 標準 SIP を使用するためのネットワーク インターフェイスを設定します。ネットワークは UDP に完全に対応しています。ネットワーク インターフェイスは、ICMP、および各エンドポイントで使用できるさまざまなソケットに対応しています。 • [icmp] : Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）を使用するためのネットワーク インターフェイスを設定します。 • [noicmp] : 各エンドポイントで別のソケットを使用しないようにネットワーク インターフェイスを指定します。この設定によって、ICMP 以外のエラーがサポートされます。 • [nat] : Network Address Translation（NAT）を使用するためのネットワーク インターフェイスを設定します。
Allow Outbound Connections	このネットワークに発信 TCP/TLS クライアント接続のイネーブル化またはディセーブル化をさせるかどうかを指定します。 イネーブルまたはディセーブルのいずれかに設定できます。デフォルト値はイネーブルです。
SIP Header Hiding	ダウン ストリーム要素がメッセージ パスを認識できないように、システムに VIA ヘッダーを除去させる場合に、このチェックボックスをオンにします。
UDP Settings: Maximum packet size	このネットワークの UDP データグラムの最大サイズを設定します。値は 1500 ～ 16,000 であることが必要です。

ステップ 4 [Add] をクリックします。

[Networks] ページに、今追加したネットワークを含め、すべてのネットワークの一覧が表示されます。

ステップ 5 SIP リッスン ポイントを追加するには、次の手順を実行します。

a. [SIP Listen Points] 列見出しの下にある、このネットワークの行の [click here] をクリックします。

b. [Add] をクリックします。

c. 次の必須の値を入力します。

- SIP リッスン ポイントの IP アドレス
- SIP リッスン ポイントのポート
- SIP リッスン ポイントのトランスポート タイプ（UDP、TCP、または TLS）

d. [Add] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ネットワークの設定」の目次ページに戻る

ネットワークの一般設定の編集

制約事項

ネットワークの名前は編集できません。

手順

ステップ 1 [Configure] > [Networks] を選択します。

[Networks] ページが表示されます。

ステップ 2 ネットワークの下線付きの名前をクリックします。

[Network: < *ネットワーク名* >] ページにネットワークの情報が表示されます。ページの最上部には、[General Settings]、[SIP Retransmissions]、[SIP Listen Points]、および [SIP Record-Route] の 4 つのタブがあります。

ステップ 3 [General Settings] タブをクリックします。

ステップ 4 値を更新します。

ステップ 5 [Update] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ネットワークの設定」の目次ページに戻る

ネットワークの SIP 再送信設定の編集

手順

ステップ 1 [Configure] > [Networks] を選択します。

[Networks] ページが表示されます。

ステップ 2 ネットワークの下線付きの名前をクリックします。

[Network: < *ネットワーク名* >] ページにネットワークの情報が表示されます。

ステップ 3 [SIP Retransmissions] タブをクリックします。

SIP 再送信フィールドおよびタイマー フィールドに自動的に値が代入されます。

表 2　　SIP 再送信

フィールド	説明
T1	最初の要求の再送信間隔を設定します。
T2	要求の再送信の最大値を設定します。
T4	要求または応答の再送信を処理するために、完了後に NONINVITE クライアント トランザクションまたは INVITE サーバ トランザクションがアクティブのままになる時間を設定します。
TU1	応答の再送信を処理するために、2xx 応答の完了後に INVITE トランザクションがアクティブのままになる時間を設定します。
TU2	トランザクションがタイムアウトしたと見なされてから、サーバが INVITE クライアント トランザクションまたは NONINVITE サーバ トランザクションの暫定応答または最終応答を待機する時間を設定します。
clientTn	クライアント トランザクションの最大有効期間を設定します。
serverTn	サーバ トランザクションの最大有効期間を設定します。
Provisional (TU3)	（オプション）TU3 送信タイプだけを使用して SIP ネットワークを設定します。
INVITE client transaction	INVITE 要求の再送信回数を指定します。
INVITE server transaction	INVITE 要求の最終応答の再送信回数を指定します。
Client transaction	INVITE 以外の要求の再送信回数を指定します。

ステップ 4 値を更新します。

ステップ 5 [Update] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ネットワークの設定」の目次ページに戻る

SIP リッスン ポイント

SIP リッスン ポイントまたはリスナーは、特定の SIP ネットワーク、ホスト、およびポート上の SIP トラフィックをリッスンします。単一のネットワークに複数の SIP リッスン ポイントを設定できますが、サーバが SIP トラフィックを受け付ける前に少なくとも 1 個作成する必要があります。

（注）
- ネットワークの設定の変更を行う場合に、ネットワーク上のリスナーをディセーブルにする必要はありません。
- TCP リスナーおよび TLS リスナーを同じポート上で実行することはできません。

手順

ステップ 1 [Configure] > [Networks] を選択します。

[Networks] ページに、現在のすべてのネットワークの一覧が表示されます。

ステップ 2 ネットワークに関連付けられた SIP リッスン ポイントを表示するには、[SIP Listen Points] ヘッダーの下にある [click here] をクリックします。

[Network: < *ネットワーク名* >] ページが表示され、[SIP Listen Point] タブが強調表示されます。

（注） 他の数の SIP リッスン ポイントを各ページに表示するには、右上にあるドロップダウン ボックスで他の数を選択し、[Go] をクリックします。10、25、50、100、またはすべての SIP リッスン ポイントの表示を選択できます。他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 3 SIP リッスン ポイントを削除するには、次の手順を実行します。

a. 削除する SIP リッスン ポイントの名前の隣にあるチェックボックスをオンにします。

b. [Remove] をクリックします。

関連項目

「ネットワークの設定」の目次ページに戻る

SIP リッスン ポイントの追加

手順

ステップ 1 [Configure] > [Networks] を選択します。

[Networks] ページに、現在のすべてのネットワークの一覧が表示されます。

ステップ 2 ネットワークに関連付けられた SIP リッスン ポイントを表示するには、[SIP Listen Points] ヘッダーの下にある [click here] をクリックします。

[Network: < *ネットワーク名* >] ページが表示され、[SIP Listen Point] タブが強調表示されます。

ステップ 3 SIP リッスン ポイントを追加するには、次の手順を実行します。

a. [Add] をクリックします。

a. SIP リッスン ポイントの IP アドレス、ポート、およびトランスポート タイプを入力します。

b. [Add] をクリックします。

ステップ 4 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ネットワークの設定」の目次ページに戻る

ネットワークの SIP レコードルートの編集

制約事項

システムで Lite モードをイネーブルにすると、レコードルート コンフィギュレーションが削除され、[SIP Record-Route] タブにアクセスできなくなります。Lite モードをイネーブルまたはディセーブルにするには、「Administration Control Panel の使用」を参照してください。

手順

ステップ 1 [Configure] > [Networks] を選択します。

[Networks] ページが表示されます。

ステップ 2 ネットワークの下線付きの名前をクリックします。

[Network: < *ネットワーク名* >] ページにネットワークの情報が表示されます。

ステップ 3 [SIP Record-Route] タブをクリックします。

ステップ 4 イネーブルまたはディセーブルのいずれかを選択します。

ステップ 5 イネーブルを選択した場合、次の情報を入力します。

- SIP レコードルートのホスト
- SIP レコードルートのポート
- SIP レコードルートのトランスポート タイプ（UDP、TCP、または TLS）

ステップ 6 [Update] をクリックします。

ステップ 7 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ネットワークの設定」の目次ページに戻る

トリガーの設定

トリガーの参照と削除

手順

ステップ 1 [Configure] > [Triggers] を選択します。

[Triggers] ページが表示され、すべてのトリガーが表示されます。

ステップ 2 このトリガーに関連付けられている条件ケースを参照するには、強調表示されているトリガーの名前をクリックします。

ステップ 3 トリガーを削除するには、次の操作を実行します。

a. 削除するトリガーの名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「トリガーについて」
- 「トリガーの例」
- 「使用可能なトリガー条件とケース」
- 「システム設定の管理」
- 「トリガーの設定」の目次ページに戻る

トリガーについて

トリガーは、ルーティングと正規化のロジックの指令に使用できる、条件のセットです。特定のイベント（または条件ケース）に対する応答として、自動的に実行されます。条件には、複数のケースがあります。

次の構造に注意してください。

- トリガーは、1 つまたは複数のルールで構成されています。
- ルールは、1 つまたは複数の条件で構成されています。
- 条件は、1 つまたは複数のケースで構成されています。

関連項目

- 「トリガーの設定」の目次ページに戻る
- 次の項目：「トリガーの例」
- 前の項目：「使用可能なトリガー条件とケース」

トリガーの例

たとえば、New_Trigger という名前のトリガーがあるとします。New_Trigger には、1、2、および 3 の番号が付いた 3 つのルールがあります。各ルールには、少なくとも 1 つの条件があり、各条件には 1 つのケースがあります。

表 3　New_Trigger という名前のトリガーの構造

トリガー ルール			
	ロジック	条件	
1		Inbound Network is exactly '100'	AND
		Local IP Address is exactly '100.10.10.101'	AND
		SIP Message request	
2	OR	Time Of Day is exactly '200'	AND
		Mid-Dialog	AND
		SIP Method UPDATE	
3	OR	Outbound Network is exactly '300'	AND
		Transport Protocol tcp	

前述の表で、トリガーの名前は New_Trigger です。New_Trigger には、3 つのルールがあります。「OR」ロジックのため、トリガーが起動される前に 3 つのルールの 1 つのみが真になる必要があります。

ルール 1 には、次の 3 つの条件があります。

- Inbound Network is exactly '100'
- Local IP Address is exactly '100.10.10.101'
- SIP Message request

「AND」ロジックのため、ルールが真になる前に 3 つのすべての条件が真になる必要があります。

「Inbound Network is exactly '100'」という条件では、条件が「Inbound Network」で、ケースが「is exactly '100'」です。

関連項目

- 「トリガーの設定」の目次ページに戻る
- 次の項目：「使用可能なトリガー条件とケース」
- 前の項目：「トリガーについて」

使用可能なトリガー条件とケース

表 4 に、使用可能なトリガー条件およびケースの一覧を示します。

表 4　使用可能なトリガー条件とケース

トリガー名	トリガーの説明	トリガー条件ケース
Inbound Network	サーバ側トランザクションについて、トリガー条件の着信ネットワークを設定します。	次のケースを入力します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP
Outbound Network	クライアント側トランザクションについて、トリガー条件の発信ネットワークを設定します。	次のケースを入力します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP
Local IP Address	着信要求を受け入れるローカルリッスン IP アドレスをトリガー条件に割り当てます。	次のケースを入力します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP

表 4　使用可能なトリガー条件とケース （続き）

トリガー名	トリガーの説明	トリガー条件ケース
Local Port	ローカル リッスン ポートをトリガー条件に割り当てます。	次のケースを入力します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP
Remote IP Address	トリガー条件のリモート IP ネットワークを設定します。	次のケースを入力します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP
Remote Port	トリガー条件のリモート ポートを設定します。	次のケースを入力します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP
SIP Message	SIP メッセージのヘッダーが要求ヘッダーまたは応答ヘッダーのいずれであるかに基づいて、トリガー条件を発生させるかどうかを決定します。	次のケースを入力します。 • request（デフォルト） • response

表 4　使用可能なトリガー条件とケース （続き）

トリガー名	トリガーの説明	トリガー条件ケース
SIP Method	要求の特定の SIP 方式名でトリガーが発生する、トリガー条件を設定します。	• INVITE（デフォルト） • ACK • PRACK • UPDATE • BYE • REFER • INFO • MESSAGE • OPTIONS • SUBSCRIBE • NOTIFY • REGISTER • PUBLISH • 正規表現
SIP Response Code	特定の応答で発生するトリガー条件を設定します。	次のケースを入力します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP
SIP Header	このヘッダーの正規表現と一致する場合に発生するトリガーを設定します。	SIP ヘッダー名を設定します。 次の SIP ヘッダー インデックスから選択します。 • first（デフォルト） • last • all 次の一致タイプから選択します。 • is exactly（デフォルト） • contains • starts with • ends with • regex
Mid-Dialog	ダイアログ中の応答で発生するトリガーを設定します。	none

表 4　使用可能なトリガー条件とケース （続き）

トリガー名	トリガーの説明	トリガー条件ケース
Time Of Day	指定された時間ポリシーを満たす場合に発生するトリガーを設定します。	次のケースを入力します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP
Transport Protocol	トリガー条件にトランスポート プロトコルを割り当てます。	次のケースを入力します。 • none（デフォルト） • udp • tcp • tls
Proxy Route	プロキシ ルート ルールを設定します。	次のパラメータから選択します。 • uri（デフォルト） • uri-user • uri-host • uri-port • uri-scheme • uri-parameter • header-parameter 次の一致タイプから選択します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP

表 4　使用可能なトリガー条件とケース （続き）

トリガー名	トリガーの説明	トリガー条件ケース
Request URI	指定された Uniform Resource Identifier (URI; ユニフォーム リソース識別子）パラメータの正規表現と一致する場合に発生するトリガーを設定します。	次のパラメータから選択します。 • uri（デフォルト） • uri-user • uri-host • uri-port • uri-scheme • uri-parameter • header-parameter 次の一致タイプから選択します。 • is exactly（デフォルト） • contains • starts with • ends with • regex 次の条件を入力します。 • リモート IP アドレスの IP

関連項目

- 「トリガーの設定」の目次ページに戻る
- 次の項目：「トリガーについて」
- 前の項目：「トリガーの例」

トリガーの追加

制約事項

既存のトリガーの名前を変更することはできないため、名前は注意深く選択してください。

手順

ステップ 1　[Configure] > [Triggers] を選択します。

[Triggers] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Trigger: New] ページが表示されます。

ステップ 3　このトリガーの名前を入力します。

ステップ 4　トリガーの起動前にルールを 1 つのみ適用する（つまり、「OR」ロジックを適用）には、[Logic] ボックスをオンにして、ロジックをルールに追加します。

ステップ 5 [Add] をクリックします。

[Trigger Conditions < *トリガー名* >] ページが表示されます。

ステップ 6 ルールをトリガーに追加します。「トリガーのルールの参照、追加、移動、および削除」を参照してください。

ステップ 7 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「トリガーの設定」の目次ページに戻る

トリガーのルールの参照、追加、移動、および削除

始める前に

トリガーを追加します。「トリガーの追加」を参照してください。

手順

ステップ 1 [Configure] > [Triggers] を選択します。

[Triggers] ページが表示されます。

ステップ 2 トリガーのルールを参照するには、強調表示されているトリガーの名前をクリックします。

[Trigger Rules < *トリガー名* >] ページが表示されます。

ステップ 3 トリガーのルールを追加するには、次の操作を実行します。

a. [Add] をクリックします。

[Trigger Conditions < *トリガー名* >] ページが表示されます。

b. 条件を追加します。「トリガー ルールの条件の追加、編集、および削除」を参照してください。

ステップ 4 トリガーのルールを削除するには、次の操作を実行します。

a. 削除するルールの横にあるボックスをオンにします。

b. [Remove] をクリックします。

ステップ 5 トリガーに複数のルールがある場合、次の操作を行うことによって、命令を再実行できます。

ヒント ルールが一致すると、トリガーがただちに実行されます。システムを最適化するには、リストの最も上で一致するよう、ルールを設定することを推奨します。

a. ルールを選択します。

b. 上矢印または下矢印をクリックします。

c. [Update] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「トリガーの設定」の目次ページに戻る

トリガー ルールの条件の追加、編集、および削除

始める前に

トリガーおよびトリガーのルールを追加します。「トリガーの追加」および「トリガーのルールの参照、追加、移動、および削除」を参照してください。

制約事項

- 既存のルールには条件ケースを追加できません。最初にルールと作成するときにのみ、条件ケースを追加できます。
- ルールに添付されている既存の条件は編集できません。
- 条件ケースはルールから削除できません。

手順

ステップ 1 [Configure] > [Triggers] を選択します。

[Triggers] ページが表示されます。

ステップ 2 強調表示されているトリガーの名前をクリックします。

[Trigger Rules < *トリガー名* >] ページが表示されます。

ステップ 3 ここでルールを追加するには、[Add] をクリックします。

[Trigger Conditions < *トリガー名* >] ページが表示されます。このページを表示することによって、新しいルールを自動的に追加していることになります。このページは、新しいルールに条件を追加するページです。

ステップ 4 条件を追加するには、次の操作を実行します。

a. [Trigger Condition] ドロップダウン メニューから、条件を選択します。表 4 を参照してください。

b. 必要な場合、条件ケースを選択します。

c. 必要な場合、一致させる条件を入力します。

d. [Add] をクリックします。

新しい条件を使用して、[Trigger Conditions < *トリガー名* >] ページが表示されます。

ステップ 5 必要に応じて、このルールに追加条件を追加します。

関連項目

- 「システム設定の管理」
- 「トリガーの設定」の目次ページに戻る

サーバ グループの設定

サーバ グループの一覧の参照

サーバ グループでは、Cisco Unified SIP Proxy システムが各ネットワークで交信する要素が定義されます。

手順

ステップ 1 [Configure] > [Server Groups] > [Groups] を選択します。

表 5 に説明されているフィールドが含まれる、[Groups] タブが強調表示された状態で、[Server Groups] ページが表示されます。

表 5　[Server Groups]（[Groups] タブ）フィールド

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	このサーバ グループの名前。 （注）　サーバ グループ名は、発信要求の SIP URI に挿入されます。Cisco Unified Communications Manager などの一部のデバイスでは、処理前に要求の URI が検証されますので、この機能を使用できるようにするため、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用してエンド デバイスを設定する必要があります。
Load Balancing Scheme	すべての SIP サーバ グループのロード バランス アルゴリズムを設定します。 次のいずれかを指定できます。 • [global]（デフォルト） • [call-id]：call-id によるハッシュ アルゴリズムを実行して要素を選択するよう指定します。 • [request-uri]：要求 URI によるハッシュ アルゴリズムを実行して要素を選択するよう指定します。 • [to-uri]：To ヘッダー URI によるハッシュ アルゴリズムを実行して要素を選択するよう指定します。 • [weight]：同じ q-value を持つ他の要素の重みに対して、その重みに比例して要素が選択されるよう指定します。この値を適用できるのは、重み付けに基づくルーティングが実装されている場合だけです。 • [highest-q]：使用可能な要素のリストで、同一の最も高い q-value を持つ最初の要素を選択するよう指定します。
Network	このサーバ グループに関連付けられるネットワークの名前。
Elements	このサーバ グループに関連付けられる要素。
Pinging Allowed	ping が使用可能か使用不能か。true または false のいずれかです。
Failover Response Codes	ネクストホップ サーバが要求を処理できないことを示す応答コード。有効な値は、500 ～ 599 までの範囲の数字です。 複数のフェールオーバー応答コードを追加するには、個々のコードをカンマで区切り、ダッシュ記号を使用して範囲を指定します。カンマとダッシュの後にスペースを入力する必要があります。

ステップ 2 サーバ グループを削除するには、次の操作を実行します。

a. 削除するサーバ グループの横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 3 この変更内容を、最後にコミットしたときの状態に戻すには、次の手順を実行します。

a. 元に戻す変更があるサーバ グループの名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

サーバ グループの追加

始める前に

サーバ グループを追加する前に、少なくとも 1 つのネットワークを作成し、設定する必要があります。「ネットワークの設定」を参照してください。

手順

ステップ 1 [Configure] > [Server Groups] > [Groups] を選択します。

[Groups] タブが強調表示された状態で、[Server Groups] ページが表示されます。

ステップ 2 [Add] をクリックします。

[Server Group (New)] ページが表示されます。

ステップ 3 情報を入力します。表 5 を参照してください。

ステップ 4 [Add] をクリックします。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

サーバ グループの編集

手順

ステップ 1 [Configure] > [Server Groups] > [Groups] を選択します。

[Groups] タブが強調表示された状態で、[Server Groups] ページが表示されます。

ステップ 2 強調表示されている、編集するサーバ グループの名前をクリックします。

[Group Settings] タブが強調表示されて、[Server Group: **< サーバ グループ名 >**] ページが表示されます。

ステップ 3 情報を編集します。表 5 を参照してください。

ステップ 4 [Update] をクリックします。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

すべてのサーバ グループの一般的な設定の参照と編集

次の手順を実行して、すべてのサーバ グループに影響を及ぼす一般的な設定を参照および編集します。

手順

ステップ 1 [Configure] > [Server Groups] > [General Settings] を選択します。

表 5 に説明されているフィールドが含まれる、[General Settings] タブが強調表示された状態で、[Server Groups] ページが表示されます。

表 6 [Server Groups]（[General Settings] タブ）フィールド

パラメータ	説明
サーバ グループ要素の再試行	
UDP	要素がダウンしたと見なされるまでに、指定されたプロトコルを通じてサーバ グループ要素に要求を送信した場合の、連続して失敗した試行の最大回数。試行が失敗する原因は、タイムアウト、ICMP エラー、または障害応答の受信が考えられます。有効な範囲は 0 ～ 65535 です。
TCP	
TLS	

表 6　[Server Groups]（[General Settings] タブ）フィールド （続き）

パラメータ	説明
グローバル ロード バランシング スキーム	
Load Balancing Scheme	すべての SIP サーバ グループのロード バランス アルゴリズムを設定します。 次のいずれかを指定できます。 • [call-id]（デフォルト）：call-id によるハッシュ アルゴリズムを実行して要素を選択するよう指定します。 • [request-uri]：要求 URI によるハッシュ アルゴリズムを実行して要素を選択するよう指定します。 • [to-uri]：To ヘッダー URI によるハッシュ アルゴリズムを実行して要素を選択するよう指定します。 • [weight]：同じ q-value を持つ他の要素の重みに対して、その重みに比例して要素が選択されるよう指定します。この値を適用できるのは、重み付けに基づくルーティングが実装されている場合だけです。 • [highest-q]：使用可能な要素のリストで、同一の最も高い q-value を持つ最初の要素を選択するよう指定します。
グローバル ping	
Pinging Allowed	ping が使用可能か使用不能か。イネーブルまたはディセーブルのいずれかに設定できます。
経過時間後のデフォルトの障害要素の再試行（ミリ秒単位）	
Failover Response Codes	ネクストホップ サーバが要求を処理できないことを示す応答コード。有効な値は、500 ～ 599 までの範囲の数字です。 複数のフェールオーバー応答コードを追加するには、個々のコードをカンマで区切り、ダッシュ記号を使用して範囲を指定します。カンマとダッシュの後にスペースを入力する必要があります。

ステップ 2　設定を編集するには、値を変更します。

ステップ 3　[Update] をクリックします。

ステップ 4　[Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

サーバ グループ要素の参照と削除

各サーバ グループには、複数の要素がある場合があります。

手順

ステップ 1 [Configure] > [Server Groups] > [Groups] を選択します。

[Groups] タブが強調表示された状態で、[Server Groups] ページが表示されます。

ステップ 2 このサーバ グループに関連付けられている要素を参照するには、[Elements] の見出しで、[click here] をクリックします。

[Elements] タブが強調表示されて、[Server Group: **< サーバ グループ名 >**] ページが表示されます。表 7 に説明されているフィールドが含まれるページが表示されます。

表 7 [Server Group]（[Elements] タブ）フィールド

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
IP Address	サーバ グループ要素のインターフェイス ホスト名または IP アドレスを指定します。
Port	サーバ グループ要素で使用されるポートを指定します。有効な値は 1024 ～ 65535 です。デフォルトは 5060 です。
Transport	サーバ グループ要素の転送タイプを指定します。次のいずれかを指定できます。 • [UDP]（デフォルト） • [TCP] • [TLS]
Nested Server Group	このグループに別のサーバ グループを含めることができるかどうか。
Q-Value	サーバ グループ内の他の要素に対する、サーバ グループ要素のプライオリティを指定する実数を指定します。 有効な値は 0.0 ～ 1.0 です。デフォルト値は 1.0 です。
Weight	重み付けに基づくルーティングを実装する場合に、サーバ グループの IP 要素に割り当てられる割合を指定します。 有効な範囲は 0 ～ 100 です。デフォルトの重みは 0 です。

ステップ 3 サーバ グループ要素を削除するには、次の操作を実行します。

a. 要素の名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 4 この変更内容を、最後にコミットしたときの状態に戻すには、次の手順を実行します。

a. 元に戻す変更があるサーバ グループ要素の名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

サーバ グループ要素の追加と編集

手順

ステップ 1 [Configure] > [Server Groups] > [Groups] を選択します。

[Groups] タブが強調表示された状態で、[Server Groups] ページが表示されます。

ステップ 2 要素を追加するサーバ グループに対応する [Elements] 見出しの下で、[click here] をクリックします。

[Elements] タブが強調表示されて、[Server Group: **<サーバ グループ名>**] ページが表示されます。

ステップ 3 要素を追加するには、次の操作を実行します。

a. [Add] をクリックします。[Server Group: **<サーバ グループ名>**] > [Element (New)] ページが表示されます。

b. この要素が、エンドポイントか、サーバ グループかを、選択します。

c. 表 7 の説明のように、要素に関する情報を入力します。

d. [Add] をクリックします。

ステップ 4 要素を編集するには、次の操作を実行します。

a. 強調表示されている、編集する要素の IP アドレスをクリックします。[Server Group: **<サーバ グループ名>**] > [Element] ページが表示されます。

b. 値を変更します。

c. [Update] をクリックします。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

SIP ping ネットワーク接続の一覧の参照

始める前に

少なくとも 1 つのネットワークを作成しておく必要があります。「ネットワークの設定」を参照してください。

手順

ステップ 1 [Configure] > [Server Groups] > [SIP Ping] を選択します。

表 8 に説明されているフィールドが含まれる、[SIP Ping] ページが表示されます。

表 8 [SIP Ping] フィールド

パラメータ	説明
Network	この SIP ping ネットワーク接続の名前。
IP Address	SIP ping への応答をリッスンする、インターフェイス ホスト名または IP アドレスを指定します。 **（注）** ホスト名を指定する場合、サーバでは DNS lookup を実行してホストを名前解決できることを確認します。その後、設定の保存時には、IP アドレスが使用されます。ホスト名を解決できない場合、「IP Address validation failed」エラーが表示されます。
Port	SIP ping に対する応答をリッスンする UDP ポート。有効な範囲は 1024 ～ 65535 です。デフォルト値は 4000 です。 **（注）** このポート番号は、サーバの SIP リッスン ポイントに対して指定されたポート番号とは異なることを確認してください。
SIP Method	SIP ping の要求方式です。次のいずれかを指定できます。 • [OPTIONS]（デフォルト） • [PING] • [INFO]
Ping Timeout	ping が失敗したと見なされるまでの、ping と応答の間隔の最大時間数（ミリ秒）を指定します。指定できる最小値は 0 です。デフォルト値は 500 です。

表 8　[SIP Ping] フィールド （続き）

パラメータ	説明
Ping Type	SIP ping の ping タイプ。次のいずれかを指定できます。 • [Proactive] : up 要素と down 要素の両方に対して ping が実行され、この両方が同じ間隔で ping されるよう指定します。 • [Reactive] : ping が down 要素でだけ実行されるように指定します。これはデフォルト値です。 • [Adaptive] : up 要素と down 要素の両方に対して ping が実行され、この両方が異なる間隔で ping されるよう指定します。
Up Element Ping Interval	（オプション。[「Ping Type」] で [Adaptive] を選択した場合にのみ使用可能）up 要素の連続的な ping 間隔を指定します。
Down Element Ping Interval	連続的な ping 間隔をミリ秒単位で指定します。アダプティブな ping の場合、この値は down 要素 ping 間隔を設定します。デフォルト値は 1,000 ミリ秒です。

ステップ 2　SIP ping ネットワーク接続を削除するには、次の操作を実行します。

a. 削除する SIP ping ネットワーク接続の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

SIP ping 設定の追加

制約事項

- 各ネットワークには、1 つの SIP ping 設定のみを定義できます。複数の SIP 設定を作成するには、複数のネットワークを作成し、設定する必要があります。
- サーバ グループ要素の SIP ping は、UDP の転送タイプでのみ追加できます。

始める前に

SIP ping 設定を追加する前に、少なくとも 1 つのネットワークを作成し、設定する必要があります。「ネットワークの設定」を参照してください。

手順

ステップ 1　[Configure] > [Server Groups] > [SIP Ping] を選択します。

[SIP Ping] ページが表示されます。

ステップ 2　[Add] をクリックします。

[SIP Ping Configuration (New)] ページが表示されます。

ステップ 3 情報を入力します。表 8 を参照してください。

ステップ 4 [Add] をクリックします。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

SIP ping 設定の編集

手順

ステップ 1 [Configure] > [Server Groups] > [SIP Ping] を選択します。

[SIP Ping] ページが表示されます。

ステップ 2 編集する SIP ping ネットワーク設定の横にあるボックスをオンにします。

ステップ 3 [Edit] をクリックします。

[SIP Ping Configuration: **< ネットワーク名 >**] ページが表示されます。

ステップ 4 情報を編集します。表 8 を参照してください。

ステップ 5 [Update] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「サーバ グループの設定」の目次ページに戻る

ルート グループの設定

ルート グループと対応する要素の一覧の参照

手順

ステップ 1 [Configure] > [Route Groups] を選択します。

表 9 に説明されているフィールドが含まれる、[Route Groups] ページが表示されます。

ステップ 2 ルート グループには、複数の要素がある場合があります。このルート グループに関連付けられている要素を参照するには、[click here] をクリックします。

表 10 に説明されているフィールドが含まれる、[Route Group Elements] ページが表示されます。

ステップ 3 ルート グループを削除するには、次の操作を実行します。

a. 削除するルート グループの名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 4 この変更内容を、最後にコミットしたときの状態に戻すには、次の手順を実行します。

a. 元に戻す変更があるルート グループの名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ルート グループについて

ルート グループを使用すると、ゲートウェイおよびトランクが選択される順序を指定できます。発信トランクの選択について、ゲートウェイとポートのリストの優先順位を決めることができます。

たとえば、2 つの長距離通信会社を使用する場合、長距離コールで、費用がより低い通信会社の優先度が高くなるよう、ルート グループを追加できます。最初のトランクが使用不能な場合にのみ、費用がより高いルートがコールに使用されます。

[Route Group] ページでは、ルート グループを追加、更新、または削除することができます。また、要素を追加、更新、または削除することもできます。

ルート グループ フィールド

表 9 に、[Route Groups] ページのフィールドの一覧を示します。

表 9　　ルート グループ パラメータ

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	このルート グループの名前。
Elements	このルート グループに属する要素。
Time of Day Routing	このルート グループで、時間ポリシー ベースのルーティングを許可するかどうかを指定します。 True または False のいずれかです。デフォルト値は False です。
Weight Based Routing	このルート グループで、重みベースのルーティングを許可するかどうかを指定します。 True または False のいずれかです。デフォルト値は False です。

要素フィールド

表 10 に、[Elements] タブが強調表示されたときの、[Route Group] ページのフィールドの一覧が表示されます。

表 10　ルート グループ要素のパラメータ

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
宛先	
Host	ルート グループ要素のインターフェイス ホスト名または IP アドレスを指定します。
Port	ルート グループ要素で使用されるポートを指定します。有効な値は 1024 ～ 65535 です。デフォルトは 5060 です。
Transport	ルート グループ要素の転送タイプを指定します。 次のいずれかを指定できます。 • [none]（デフォルト） • [UDP] • [TCP] • [TLS]
ネクスト ホップ	
SIP URI	ネクスト ホップの URI。
オプション	
Network	このルート グループが関連付けられるネットワークの名前。
Q-Value	（オプション）ルート グループ内の他の要素に対する、ルート グループ要素のプライオリティを指定する実数を指定します。 有効な値は 0.0 ～ 1.0 です。デフォルト値は 1.0 です。
Weight	（オプション）重み付けに基づくルーティングを実装する場合に、ルート グループの IP 要素に割り当てられる割合を指定します。 有効な範囲は 0 ～ 100 です。デフォルトの重みは 0 です。
Time Policy	時間ベースのルーティングが使用されている場合に、時間ポリシーを指定します。
Failover Response Codes	ネクストホップ サーバが要求を処理できないことを示す応答コード。有効な値は、500 ～ 599 までの範囲の数字です。 複数のフェールオーバー応答コードを追加するには、個々のコードをカンマで区切り、ダッシュ記号を使用して範囲を指定します。カンマとダッシュの後にスペースを入力する必要があります。

関連項目

- 「システム設定の管理」
- 「ルート グループの設定」の目次ページに戻る

ルート グループの追加

手順

ステップ 1 [Configure] > [Route Groups] を選択します。

[Route Groups] ページが表示されます。

ステップ 2 [Add] をクリックします。

[Route Group (New)] ページが表示されます。

ステップ 3 このルート グループの名前を入力します。時間に基づくルーティングまたは重みに基づくルーティングをイネーブルにするには、これらのチェックボックスをオンにします。

ステップ 4 [Add] をクリックします。

表に一覧が表示されている新しいルート グループが含まれる、[Route Groups] ページが表示されます。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート グループの設定」の目次ページに戻る

ルート グループ要素の参照と削除

手順

ステップ 1 [Configure] > [Route Groups] を選択します。

[Route Groups] ページが表示されます。

ステップ 2 [Elements] というタイトルの下の、削除する要素があるルート グループの回線で、[click here] をクリックします。

[Elements] タブが強調表示されて、[Route Group: **< ルート グループ名 >**] ページが表示されます。

ステップ 3 ルート グループ要素を削除するには、次の操作を実行します。

a. 要素の名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 4 この変更内容を、最後にコミットしたときの状態に戻すには、次の手順を実行します。

a. 元に戻す変更があるルート グループ要素の名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート グループの設定」の目次ページに戻る

ルート グループ要素の追加と編集

手順

ステップ 1 [Configure] > [Route Groups] を選択します。

[Route Groups] ページが表示されます。

ステップ 2 [Elements] で、要素を追加するルート グループの行にある [click here] をクリックします。

[Elements] タブが強調表示されて、[Route Group: **<ルート グループ名>**] ページが表示されます。

ステップ 3 要素を追加するには、次の操作を実行します。

a. [Add] をクリックします。[Route Group : **<ルート グループ名>**] > [Element (New)] ページが表示されます。

b. この要素が宛先かネクスト ホップかを選択します。

c. 表 10 の説明のように、要素に関する情報を入力します。

d. [Add] をクリックします。

ステップ 4 要素を編集するには、次の操作を実行します。

a. 強調表示されている要素のネクスト ホップをクリックします。[Route Group : **<ルート グループ名>**] > [Element (New)] ページが表示されます。

b. 表 10 の説明のように、要素に関する情報を変更します。

c. [Update] をクリックします。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート グループの設定」の目次ページに戻る

ルート グループの編集

手順

ステップ 1 [Configure] > [Route Groups] を選択します。

[Route Groups] ページが表示されます。

ステップ 2 強調表示されている、編集するルート グループの名前をクリックします。

[Group Settings] タブが強調表示されて、[Route Group < **ルート グループ名** >] ページが表示されます。

ステップ 3 このルート グループで、時間に基づくルーティングをイネーブルにするか、重みに基づくルーティングをイネーブルにするかを、変更できます。

ステップ 4 [Update] をクリックします。

ステップ 5 ルート グループの要素を編集するには、「ルート グループ要素の追加と編集」に説明されている手順に従って操作します。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート グループの設定」の目次ページに戻る

ルート テーブルの設定

ルート テーブルの一覧の参照

手順

ステップ 1 [Configure] > [Route Tables] を選択します。

表 11 に説明されているフィールドが含まれる、[Route Tables] ページが表示されます。

ステップ 2 ルート テーブルを削除するには、次の操作を実行します。

a. 削除するルート テーブルの名前の横にあるボックスを選択します。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 3 この変更内容を、最後にコミットしたときの状態に戻すには、次の手順を実行します。

a. 元に戻す変更があるルート テーブルの名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ルート テーブルについて

SIP 要求を適切な宛先へ送るには、ルート テーブルを設定します。各ルート テーブルは、ルックアップ ポリシーに基づいて照合するキーのセットで構成されています。

たとえば、1 つのテーブルで、各キーはダイヤルされた電話番号の市外局番を表す場合があります。テーブルでは、ダイヤルされた市外局番によって、タスクが実行されます。この例では、テーブルは、ダイヤルされた電話番号が 510 で始まっている場合を除き、呼び出しに 404 メッセージ（not found）で応答する設計になっています。別のテーブルは、ダイヤルされた電話番号がエスケープ シーケンス（91）で始まっている場合を除き、呼び出しに 404 メッセージ（not found）で応答する設計になっています。

[Route Tables] ページでは、ルート テーブルを追加、更新、または削除できます。また、ルートを追加、更新、または削除することもできます。

ルート テーブル フィールド

表 11 に、[Route Tables] ページのフィールドの一覧を示します。

表 11　ルート テーブル パラメータ

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	このルート テーブルの名前。有効な文字は、英数文字、ダッシュ、ピリオド、および下線です。
Routes	このルート テーブルに属するルート。

ルート フィールド

表 12 に、[Route Table: <*ルート名*>] ページのフィールドの一覧を示します。

（注）　選択したルート タイプにより、これらのパラメータの一部またはすべてが表示されます。

表 12　ルート テーブルのルート パラメータ

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。

表 12　ルート テーブルのルート パラメータ （続き）

パラメータ	説明
候補値	
Key	ルート テーブルの検索キー番号を指定します。検索キーは、一致している SIP メッセージの一部を表します。また、ルーティング テーブルに対して一意である必要があります。
Route Type	次のいずれかを指定できます。 • [destination] • [route-group] • [route-policy] • [response] • [default-sip]
宛先ルート タイプ（オプション。[Route Type] で destination または default-sip を選択した場合のみ使用可能）	
Destination Route Type	ルートのタイプ。宛先、ネクスト ホップ、またはその両方のいずれかを指定できます。
Network	SIP ネットワーク名を指定します。
宛先（オプション。[Destination Route Type] で宛先または両方を選択した場合のみ使用可能）	
Host	宛先のホスト名または IP アドレス。
Port	宛先のポート。値は 1024 ～ 65535 です。
Transport Type	次のいずれかを指定できます。 • [none] • [UDP] • [TCP] • [TLS]
ネクスト ホップ（オプション。[Destination Route Type] でネクスト ホップまたは両方を選択した場合のみ使用可能）	
SIP URI	ネクスト ホップの URI。
ルート グループのルート タイプ（オプション。[Route Type] で route-group を選択した場合のみ使用可能）	
Route Group	ルート グループの名前。
応答ルート タイプ（オプション。[Route Type] で response を選択した場合のみ使用可能）	
Response	ルーティング テーブル内のルックアップ キーに対して応答コードを指定します。
ルート ポリシーのルート タイプ（オプション。[Route Type] で route-policy を選択した場合のみ使用可能）	
Lookup Route Policy	ルーティング テーブルで使用するルート検索ポリシーを指定します。
Default SIP Route	RFC 3263 に準拠した簡易ルーティング。

関連項目

- 「システム設定の管理」
- 「ルート テーブルの設定」の目次ページに戻る

ルート テーブルの追加

手順

ステップ 1 [Configure] > [Route Tables] を選択します。

[Route Tables] ページが表示されます。

ステップ 2 [Add] をクリックします。

[Route Tables] ページが表示されます。

ステップ 3 このルート テーブルの名前を入力します。

ステップ 4 [Add] をクリックします。

新しいルート テーブルの一覧が含まれる、[Route Tables] ページが表示されます。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート テーブルの設定」の目次ページに戻る

ルート テーブル ルートの一覧の参照

手順

ステップ 1 [Configure] > [Route Tables] を選択します。

表 11 に説明されているフィールドが含まれる、[Route Tables] ページが表示されます。

ステップ 2 見出し [Routes] の下で、ルート テーブルに関連付けられているルートを参照するには、[click here] をクリックします。

表 12 に説明されている一部またはすべてのフィールドが含まれる、[Route Table: **<ルート テーブル名>**] ページが表示されます。

ステップ 3 各ページで異なるルート番号を参照するには、右上のドロップダウン ボックスから別の番号を選択し、[Go] をクリックします。10、25、50、100、またはすべてのルートを参照するよう、選択できます。

ステップ 4 他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 5 ルートを削除するには、次の操作を実行します。

a. 削除するルートの名前の横にあるボックスを選択します。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 6 この変更内容を、最後にコミットしたときの状態に戻すには、次の手順を実行します。

a. 元に戻す変更があるルート テーブルの名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート テーブルの設定」の目次ページに戻る

ルート テーブルへのルートの追加

始める前に

ファイルから 1 つまたは複数のルートをインポートする場合、ファイルを pfs:/cusp/routes/ ディレクトリに置きます。

手順

ステップ 1 [Configure] > [Route Tables] を選択します。

[Route Tables] ページが表示されます。

ステップ 2 強調表示されている、ルートを追加するルート テーブルの名前をクリックします。

[Route Table: **< ルート テーブル名 >**] ページが表示されます。

ステップ 3 [Add] をクリックします。

[Route Table: **< ルート テーブル名 >**] > [Route (New)] ページが表示されます。

ステップ 4 表 12 の説明のように、ルートに関する情報を入力します。

ステップ 5 [Add] をクリックします。

ステップ 6 ファイルからルート テーブルのルートをロードするには、[Import] をクリックします。

ステップ 7 ファイルの名前を入力します。

（注） ファイルは、ディレクトリ pfs:/cusp/routes/ にある必要があります。

ステップ 8 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート テーブルの設定」の目次ページに戻る

ルート テーブルに関連付けられているルートの編集

手順

ステップ 1 [Configure] > [Route Tables] を選択します。

[Route Tables] ページが表示されます。

ステップ 2 強調表示されている、編集するルートが含まれているルート テーブルの名前をクリックします。

[Route Table: **< ルート テーブル名 >**] ページが表示されます。

ステップ 3 強調表示されている、編集するルートのキーの名前をクリックします。

[Route Table: **< ルート テーブル名 >**] > [Route] ページが表示されます。

ステップ 4 値を変更します。

ステップ 5 [Update] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート テーブルの設定」の目次ページに戻る

ルート ポリシーの設定

ルート ポリシーの一覧の参照

ルート ポリシーには、ルートの動作が定義されます。

（注） ルート ポリシーは、CLI のルックアップ ポリシーとも呼ばれます。

手順

ステップ 1 [Configure] > [Route Policies] を選択します。

表 13 に説明されているフィールドが含まれる、[Route Policies] ページが表示されます。

ステップ 2 ルート ポリシーを削除するには、次の操作を実行します。

a. 削除するルート ポリシーの名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 3 ルート ポリシーを、最後にコミットされた時間の設定まで戻すには、次の操作を実行します。

a. 元に戻す設定があるルート ポリシーの名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

[Route Policy] フィールド

表 13 に、[Route Policies] ページのフィールドの一覧を示します。

表 13　[Route Policy] フィールド

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	このルート ポリシーの名前。

[Route Policy Step] フィールド

表 14 に、[Route Policy Step] ページのフィールドの一覧を示します。

表 14　[Route Policy Step] フィールド

パラメータ	説明
ルート テーブル	
Name	このルート ポリシーが添付されるルート テーブルの名前。
Lookup Key Matches:	次のいずれかを指定できます。 • [Exactly]（デフォルト）：指定したテーブルのキーの完全一致を検索ポリシーで検索することを指定します。 • [Prefix-Longest-Match]：最も長いプレフィクスの一致を検索ポリシーで検索することを指定します。 • [Subdomain]：テーブルのキーの最も長いサブドメインを検索ポリシーで検索することを指定します。ドメイン名の一致では大文字と小文字が区別され、最も詳細な一致が優先されます。IP アドレスの一致は完全一致である必要があります。要求に non-SIP request-URI が含まれる場合、この検索は失敗します。このエラーを回避するには、[Case Sensitive] の横にあるチェックボックスをオンにします。 • [Subnet]：テーブルのキーの最も長い IP アドレスを検索ポリシーで検索することを指定します。 • [Prefix-Fixed-Length]：キー全体ではなく、キーの文字の固定数が検索されることを指定します。
Case Sensitive	ルート テーブルのルックアップ ポリシーで、大文字と小文字が区別されるように設定する場合は、このボックスをオンにします。

表 14　[Route Policy Step] フィールド （続き）

パラメータ	説明
ルート テーブル ルックアップ キー	
Lookup Key	ドロップダウン メニューから、宛先を選択します。値は次のとおりです。 • [Request URI] : Request-URI ヘッダーに適用する検索ポリシーを指定します。 • [Field] • [SIP Header] : 検索ポリシーを適用できるヘッダーを指定します。 ドロップダウン メニューから、URI コンポーネントを選択します。値は次のとおりです。 • [URI] : URI 全体に適用する検索ポリシーを指定します。 • [User] : user URI コンポーネントに適用する検索ポリシーを指定します。 • [Phone] : phone URI コンポーネントに適用する検索ポリシーを指定します。 • [Host] : host URI コンポーネントに適用する検索ポリシーを指定します。 • [Host-Port] : host-port URI コンポーネントに適用する検索ポリシーを指定します。 • [Param] : URI コンポーネント パラメータ名を指定します。
ルックアップ キー修飾子	
Regular Expression Match	正規表現に一致するキー修飾子を指定します。
Regular Expression Replace	正規表現を置き換えるキー修飾子を指定します。

関連項目

- 「システム設定の管理」
- 「ルート ポリシーの設定」の目次ページに戻る

ルート ポリシーの追加

始める前に

ルート ポリシーを追加する前に、少なくとも 1 つのルート テーブルを作成し、設定する必要があります。「ルート テーブルの設定」を参照してください。

手順

ステップ 1　[Configure] > [Route Policies] を選択します。

[Route Policies] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Route Policy Steps: (New)] ページが表示されます。

ステップ 3 このルート ポリシーの名前を入力します。

[Add] をクリックします。

[Route Policy Step: Add] ページが表示されます。

ステップ 4 ルート ポリシーの手順を入力します。「ルート ポリシー手順の追加と編集」を参照してください。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート ポリシーの設定」の目次ページに戻る

ルート ポリシー手順の参照

手順

ステップ 1 [Configure] > [Route Policies] を選択します。

[Route Policies] ページが表示されます。

ステップ 2 強調表示されている、ルート ポリシーの手順を参照するルート ポリシーの名前をクリックします。

[Route Policy Steps: **<ルート ポリシー名>**] ページが表示され、このルート ポリシーに関連付けられているすべての手順が示されます。

ステップ 3 ルート ポリシーの手順を削除するには、次の操作を実行します。

a. 削除するルート ポリシーの手順の名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 4 ルート ポリシーの手順を、最後にコミットされた時間の設定まで戻すには、次の操作を実行します。

a. 元に戻す設定があるルート ポリシーの手順の名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ルート ポリシー手順の追加と編集

（注） ルート ポリシーの編集時には、それに関連付けられている手順のみを編集できます。

手順

ステップ 1 [Configure] > [Route Policies] を選択します。

[Route Policies] ページが表示されます。

ステップ 2 強調表示されている、ルート ポリシーの手順を追加または編集するルート ポリシーの名前をクリックします。

[Route Policy Steps: **<ルート ポリシー名>**] ページが表示され、このルート ポリシーに関連付けられているすべての手順が示されます。

ステップ 3 ルート ポリシーの手順を追加するには、次の操作を実行します。

a. [Add] をクリックします。

[Route Policy Step: ***Add***] ページが表示されます。

b. 表 14 の説明のように、ルート ポリシーの手順に関する情報を入力します。

c. [Add] をクリックします。

ステップ 4 ルート ポリシーの手順を編集するには、次の操作を実行します。

a. 強調表示されているルート ポリシーの手順の名前をクリックします。

[Route Policy Step: ***Edit***] ページが表示されます。

b. 表 14 の説明のように、ルート ポリシーの手順の値を変更します。

c. [Update] をクリックします。

ステップ 5 ルート ポリシーの手順を移動するには、その横にあるボックスをオンにし、上矢印または下矢印をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルート ポリシーの設定」の目次ページに戻る

正規化ポリシーの設定

正規化ポリシーのリストの表示

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、表 15 で説明したフィールドを含む [Normalization Policies] ページが表示されます。

ステップ 2 正規化ポリシーを削除するには、次の手順を実行します。

a. 削除する正規化ポリシー名の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 3 この変更内容を、最後にコミットしたときの状態に戻すには、次の手順を実行します。

a. 元の状態に戻したい正規化ポリシー名の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

正規化ポリシーの概要

正規化ポリシーは、互換性がないネットワークを考慮して SIP メッセージを変更します。

正規化ポリシーのフィールド

表 15 に [Normalization Policies] ページのフィールドを一覧で示します。

表 15　正規化ポリシーのパラメータ

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	正規化ポリシーの名前

[Request URI]、[URI Component] フィールド

表 16 に、[Request URI] タブ、および [URI Component] タブを表示した場合の、[Normalization Policy: **<正規化ポリシー名>**] ページのフィールドを一覧で示します。

表 16　[Request URI]、[URI Component] のフィールド

パラメータ	説明
Category	このページには、次に示すパラメータごとに 1 つずつ、合計 5 個のボックスがあります。 • [User] : user URI コンポーネントに適用する正規化ポリシーを指定します。 • [Phone] : phone URI コンポーネントに適用する正規化ポリシーを指定します。 • [Host] : host URI コンポーネントに適用する正規化ポリシーを指定します。 • [Host and Port] : host-port URI コンポーネントに適用する正規化ポリシーを指定します。 • [URI] : URI 全体に適用する正規化ポリシーを指定します。 各ボックスに一致パターンを入力し、値を置換します。
Match Pattern	一致する URI コンポーネントの正規表現文字列を指定します。**all** と入力すると、ヘッダー全体が置き換えられます。
Replace Value	一致する文字列を置き換える URI コンポーネントの正規表現文字列を指定します。

[Request URI]、[URI Conversion] のフィールド

表 17 に、[Request URI] タブ、および [URI Conversion] タブを表示した場合の、[Normalization Policy: <正規化ポリシー名>] ページのフィールドを一覧で示します。

表 17　[Request URI]、[URI Conversion] のフィールド

パラメータ	説明
SIP URI から TEL URI への変換	
Conversion	この変換をイネーブルにするかディセーブルにするかを指定します。デフォルトではディセーブルです。
TEL URI から SIP URI への変換	
Conversion	この変換をイネーブルにするかディセーブルにするかを指定します。デフォルトではディセーブルです。
Host	URI のホストを入力します。
Port	URI のポートを入力します。

[Request URI]、[URI Parameter] のフィールド

表 18 に、[Request URI] タブ、および [URI Parameter] タブを表示した場合の、[Normalization Policy: <正規化ポリシー名>] ページのフィールドを一覧で示します。

表 18　[Request URI]、[URI Parameter] のフィールド

パラメータ	説明
URI パラメータの追加	
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	正規化ルールが適用される URI パラメータ名を指定します。
Value	URI パラメータに追加する値を指定します。
URI パラメータの削除	
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	URI パラメータ名を指定します。

表 18　[Request URI]、[URI Parameter] のフィールド （続き）

パラメータ	説明
URI パラメータの更新	
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	ヘッダー パラメータ名を指定します。
Match Pattern	一致する URI パラメータの正規表現文字列を指定します。**all** と入力すると、ヘッダー全体が置き換えられます。
Replace Value	一致する文字列を置き換える URI パラメータの正規表現文字列を指定します。

SIP ヘッダーのフィールド

表 19 に、[SIP Header] タブを表示した場合の、[Normalization Policy: **<正規化ポリシー名>**] ページのフィールドを一覧で示します。

表 19　SIP ヘッダーのパラメータ フィールド

パラメータ	説明
SIP ヘッダーの追加	
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Instances	追加する SIP ヘッダー インスタンス。

表 19　SIP ヘッダーのパラメータ フィールド （続き）

パラメータ	説明
SIP ヘッダーの削除	
State	次のいずれかを指定できます。 • [New] : 新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified] : 変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted] : 削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active] : アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
Total Number of Header Instances	削除される SIP ヘッダー インスタンスの合計数。
SIP ヘッダーの更新	
State	次のいずれかを指定できます。 • [New] : 新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified] : 変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted] : 削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active] : アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first] : 特定のヘッダー パラメータが複数ある場合、この正規化手順は最初のパラメータにだけ適用されることを指定します。 • [last] : 特定のヘッダー パラメータが複数ある場合、この正規化手順は最後のパラメータにだけ適用されることを指定します。 • [all] : 特定のヘッダー パラメータが複数ある場合、この正規化手順はすべてのパラメータに適用されることを指定します。
Match Pattern	一致するヘッダー パラメータの正規表現文字列を指定します。**all** と入力すると、ヘッダー全体が置き換えられます。
Replace Value	一致する文字列を置き換えるヘッダー パラメータの正規表現文字列を指定します。

[SIP Header]、[URI Component] のフィールド

表 20 に、[SIP Header] タブ、および [URI Component] タブを表示した場合の、[Normalization Policy: <正規化ポリシー名>] ページのフィールドを一覧で示します。

表 20　[SIP Header]、[URI Component] のフィールド

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first]：特定の URI コンポーネントが複数ある場合、この正規化手順は最初のコンポーネントにだけ適用されることを指定します。 • [last]：特定の URI コンポーネントが複数ある場合、この正規化手順は最後のコンポーネントにだけ適用されることを指定します。 • [all]：特定の URI コンポーネントが複数ある場合、この正規化手順はすべてのコンポーネントに適用されることを指定します。
URI Component Type	次のいずれかを指定できます。 • [URI]：URI 全体に適用する検索ポリシーを指定します。 • [User (default)]：user URI コンポーネントに適用する検索ポリシーを指定します。 • [Phone]：phone URI コンポーネントに適用する検索ポリシーを指定します。 • [Host]：host URI コンポーネントに適用する検索ポリシーを指定します。 • [Host-Port]：host-port URI コンポーネントに適用する検索ポリシーを指定します。
Match Pattern	一致する URI コンポーネントの正規表現文字列を指定します。**all** と入力すると、ヘッダー全体が置き換えられます。
Replace Value	一致する文字列を置き換える URI コンポーネントの正規表現文字列を指定します。

[SIP Header]、[URI Conversion] のフィールド

表 21 に、[SIP Header] タブ、および [URI Conversion] タブを表示した場合の、[Normalization Policy: <正規化ポリシー名>] ページのフィールドを一覧で示します。

表 21　[SIP Header]、[URI Conversion] のフィールド

パラメータ	説明
TEL URI から SIP URI への変換	
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first]：特定の TEL URI が複数ある場合、この正規化手順は最初のコンポーネントにだけ適用されることを指定します。 • [last]：特定の TEL URI が複数ある場合、この正規化手順は最後のコンポーネントにだけ適用されることを指定します。 • [all]：特定の TEL URI が複数ある場合、この正規化手順はすべてのコンポーネントに適用されることを指定します。
Host	URI のホストを入力します。
Port	URI のポートを入力します。
SIP URI から TEL URI への変換	
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。

表 21　[SIP Header]、[URI Conversion] のフィールド （続き）

パラメータ	説明
SIP Header Index	次のいずれかを指定できます。 • [first]：特定の SIP URI が複数ある場合、この正規化手順は最初のコンポーネントにだけ適用されることを指定します。 • [last]：特定の SIP URI が複数ある場合、この正規化手順は最後のコンポーネントにだけ適用されることを指定します。 • [all]：特定の SIP URI が複数ある場合、この正規化手順はすべてのコンポーネントに適用されることを指定します。

[SIP Header]、[URI Parameter] のフィールド

表 22 に、[SIP Header] タブ、および [URI Parameter] タブを表示した場合の、[Normalization Policy: <正規化ポリシー名>] ページのフィールドを一覧で示します。

表 22　[SIP Header]、[URI Parameter] のフィールド

パラメータ	説明
URI パラメータの追加	
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first]：特定の URI パラメータが複数ある場合、この正規化手順は最初のコンポーネントにだけ適用されることを指定します。 • [last]：特定の URI パラメータが複数ある場合、この正規化手順は最後のコンポーネントにだけ適用されることを指定します。 • [all]：特定の URI パラメータが複数ある場合、この正規化手順はすべてのコンポーネントに適用されることを指定します。
Parameter Name	正規化ルールが適用される URI パラメータ名を指定します。
Value	追加する値を指定します。

表 22　[SIP Header]、[URI Parameter] のフィールド （続き）

パラメータ	説明
URI パラメータの削除	
State	次のいずれかを指定できます。 • [New] : 新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified] : 変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted] : 削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active] : アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first] : 特定の URI パラメータが複数ある場合、この正規化手順は最初のコンポーネントにだけ適用されることを指定します。 • [last] : 特定の URI パラメータが複数ある場合、この正規化手順は最後のコンポーネントにだけ適用されることを指定します。 • [all] : 特定の URI パラメータが複数ある場合、この正規化手順はすべてのコンポーネントに適用されることを指定します。
Parameter Name	URI パラメータ名を指定します。
URI パラメータの更新	
State	次のいずれかを指定できます。 • [New] : 新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified] : 変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted] : 削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active] : アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first] : 特定の URI パラメータが複数ある場合、この正規化手順は最初のコンポーネントにだけ適用されることを指定します。 • [last] : 特定の URI パラメータが複数ある場合、この正規化手順は最後のコンポーネントにだけ適用されることを指定します。 • [all] : 特定の URI パラメータが複数ある場合、この正規化手順はすべてのコンポーネントに適用されることを指定します。
Parameter Name	ヘッダー パラメータ名を指定します。

表 22　[SIP Header]、[URI Parameter] のフィールド （続き）

パラメータ	説明
Match Pattern	一致する URI パラメータの正規表現文字列を指定します。**all** と入力すると、ヘッダー全体が置き換えられます。
Replace Value	一致する文字列を置き換える URI パラメータの正規表現文字列を指定します。

[SIP Header]、[Header Parameter] のフィールド

表 23 に、[SIP Header] タブ、および [Header Parameter] タブを表示した場合の、[Normalization Policy: <正規化ポリシー名>] ページのフィールドを一覧で示します。

表 23　[SIP Header]、[Header Parameter] のフィールド

パラメータ	説明
ヘッダー パラメータの追加	
State	次のいずれかを指定できます。 • [New] : 新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified] : 変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted] : 削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active] : アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first] : 特定のヘッダー パラメータが複数ある場合、この正規化手順は最初のパラメータにだけ適用されることを指定します。 • [last] : 特定のヘッダー パラメータが複数ある場合、この正規化手順は最後のパラメータにだけ適用されることを指定します。 • [all] : 特定のヘッダー パラメータが複数ある場合、この正規化手順はすべてのパラメータに適用されることを指定します。
Parameter Name	この追加 URI パラメータの名前。
Value	この追加 URI パラメータの値。
ヘッダー パラメータの削除	
State	次のいずれかを指定できます。 • [New] : 新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified] : 変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted] : 削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active] : アクティブなレコードとアクティブな設定。

表 23　[SIP Header]、[Header Parameter] のフィールド （続き）

パラメータ	説明
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first] : 特定のヘッダー パラメータが複数ある場合、この正規化手順は最初のパラメータにだけ適用されることを指定します。 • [last] : 特定のヘッダー パラメータが複数ある場合、この正規化手順は最後のパラメータにだけ適用されることを指定します。 • [all] : 特定のヘッダー パラメータが複数ある場合、この正規化手順はすべてのパラメータに適用されることを指定します。
Parameter Name	この削除 URI パラメータの名前。
ヘッダー パラメータの更新	
State	次のいずれかを指定できます。 • [New] : 新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified] : 変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted] : 削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active] : アクティブなレコードとアクティブな設定。
SIP Header Name	正規化手順を適用できる SIP メッセージ ヘッダーを指定します。たとえば、From、To、Record-Route、Diversion、Request-URI、P-Asserted-Identity が含まれます。
SIP Header Index	次のいずれかを指定できます。 • [first] : 特定のヘッダー パラメータが複数ある場合、この正規化手順は最初のパラメータにだけ適用されることを指定します。 • [last] : 特定のヘッダー パラメータが複数ある場合、この正規化手順は最後のパラメータにだけ適用されることを指定します。 • [all] : 特定のヘッダー パラメータが複数ある場合、この正規化手順はすべてのパラメータに適用されることを指定します。
Parameter Name	この更新 URI パラメータの名前。
Match Pattern	一致する URI コンポーネントの正規表現文字列を指定します。**all** と入力すると、ヘッダー全体が置き換えられます。
Replace Value	一致する文字列を置き換える URI コンポーネントの正規表現文字列を指定します。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

正規化ポリシーの追加

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 [Add] をクリックします。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 3 この正規化ポリシーの名前を入力します。

[Add] をクリックします。

システムにより、新しい正規化ポリシーが一覧表示された [Normalization Policies] ページが表示されます。

ステップ 4 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

要求 URI の URI コンポーネントの使用

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 下線が引かれた、使用する正規化ポリシーの名前をクリックします。

システムにより、[URI Component] タブが選択された [Normalization Policy: **< 正規化ポリシー名 >**] ページが表示されます。

ステップ 3 URI コンポーネントを追加または編集するには、次の手順を実行します。

a. 値を追加または編集するコンポーネントのチェックボックスをオンにします。

b. 値を入力または変更します。表 16 を参照してください。

c. [Update] をクリックします。

ステップ 4 URI コンポーネントを削除するには、次の手順を実行します。

a. 削除するコンポーネントのチェックボックスをオフにします。

b. [Update] をクリックします。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

要求 URI の URI 変換パラメータの使用

宛先の TEL URI を特定の host-port 値が指定された SIP URI に変換する正規化ポリシー手順を設定するには、次の手順を実行します。

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 下線が引かれた、使用する正規化ポリシーの名前をクリックします。

システムにより、[Normalization Policy: **< 正規化ポリシー名 >**] ページが表示されます。

ステップ 3 [URI Conversion] タブをクリックします。

ステップ 4 値を入力または更新します。表 17 を参照してください。

ステップ 5 [Update] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

要求 URI の URI パラメータの使用

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 下線が引かれた、使用する正規化ポリシーの名前をクリックします。

システムにより、[Normalization Policy: **< 正規化ポリシー名 >**] ページが表示されます。

ステップ 3 [URI Parameter] タブをクリックします。

ステップ 4 URI パラメータを要求 URI に追加するには、次の手順を実行します。

a. 見出し [Add URI Parameters] の下の [New] をクリックします。

b. パラメータの名前と値を入力します。

c. [Add] をクリックします。

ステップ 5 URI からパラメータを削除するには、次の手順を実行します。

a. 見出し [Remove URI Parameters] の下の [New] をクリックします。

b. 削除するパラメータの名前を入力します。

c. [Add] をクリックします。

ステップ 6 URI のパラメータを更新するには、次の手順を実行します。

a. 見出し [Update URI Parameters] の下の [New] をクリックします。

b. 更新するパラメータの名前と、一致するパターンを入力します。オプションで、パターンと置き換える値を入力することもできます。

c. [Add] をクリックします。

ステップ 7 ステップ 4 から ステップ 6 で追加したパラメータを削除するには、パラメータの横のボックスをオンにし、[Remove] をクリックします。

ステップ 8 ステップ 4 から ステップ 6 で追加したパラメータを以前の設定に戻すには、パラメータの横のボックスをオンにし、[Revert] をクリックします。

ステップ 9 ステップ 4 または ステップ 6 で追加したパラメータを編集、追加、または更新するには、パラメータ名をクリックし、変更を加えます。

ステップ 10 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

SIP ヘッダーの使用

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 下線が引かれた、SIP ヘッダーを追加する正規化ポリシーの名前をクリックします。

システムにより、[Normalization Policy: **< 正規化ポリシー名 >**] ページが表示されます。

ステップ 3 [SIP Header] タブをクリックします。

システムにより、[SIP Header] タブが表示された [Normalization Policy: **< 正規化ポリシー名 >**] ページが開かれます。

ステップ 4 SIP ヘッダーを追加するには、次の手順を実行します。

a. 見出し [Add SIP Headers] の下の [New] をクリックします。

b. パラメータの名前を入力します。

c. [Add] をクリックします。

d. SIP ヘッダーのインデックスと値を入力します。

e. [Add] をクリックします。

f. [SIP Header] タブが表示された [Normalization Policy: **<正規化ポリシー名>**] ページに戻るには、[Cancel] をクリックします。

ステップ 5 SIP ヘッダーを削除するには、次の手順を実行します。

a. 見出し [Remove SIP Headers] の下の [New] をクリックします。

b. 削除する SIP ヘッダーの名前を入力します。ヘッダー インスタンスの最上部から削除する数と、最下部から削除する数を入力します。

c. [Add] をクリックします。

ステップ 6 SIP ヘッダーを更新するには、次の手順を実行します。

a. 見出し [Update SIP Headers] の下の [New] をクリックします。

b. 更新する SIP ヘッダーの名前と、一致するパターンを入力します。オプションで、パターンと置き換える SIP ヘッダー インデックスおよび値を入力することもできます。

c. [Add] をクリックします。

ステップ 7 ステップ 4 から ステップ 6 で追加した SIP ヘッダーを削除するには、パラメータの横のボックスをオンにし、[Remove] をクリックします。

ステップ 8 ステップ 4 から ステップ 6 で追加した SIP ヘッダーを以前の設定に戻すには、SIP ヘッダーの横のボックスをオンにし、[Revert] をクリックします。

ステップ 9 ステップ 4 または ステップ 6 で追加したパラメータを編集、追加、または更新するには、SIP ヘッダー名をクリックし、変更を加えます。

ステップ 10 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

SIP ヘッダーの URI コンポーネントの使用

ソース メッセージのヘッダーに含まれる URI コンポーネント フィールドを更新する正規化ポリシー手順を設定するには、次の手順を実行します。

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 下線が引かれた、使用する正規化ポリシーの名前をクリックします。

システムにより、[Normalization Policy: **<正規化ポリシー名>**] ページが表示されます。

ステップ 3 [SIP Header] タブをクリックします。

ステップ 4 [URI Component] タブをクリックします。

ステップ 5 URI コンポーネントを SIP ヘッダーに追加するには、次の手順を実行します。

a. [New] をクリックします。

b. 値を入力します。表 20 を参照してください。

c. [Add] をクリックします。

ステップ 6 SIP ヘッダーの URI コンポーネントを編集するには、次の手順を実行します。

a. 下線が引かれた SIP ヘッダーの名前をクリックします。

b. 一致パターンを更新するか、値を置き換えます。表 20 を参照してください。

c. [Update] をクリックします。

ステップ 7 SIP ヘッダーの URI コンポーネントを削除するには、URI コンポーネントの横のボックスをオンにし、[Remove] をクリックします。

ステップ 8 SIP ヘッダーの URI コンポーネントを元の設定に戻すには、URI コンポーネントの横のボックスをオンにし、[Revert] をクリックします。

ステップ 9 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

SIP ヘッダーの URI 変換パラメータの使用

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 下線が引かれた、使用する正規化ポリシーの名前をクリックします。

システムにより、[Normalization Policy: **< 正規化ポリシー名 >**] ページが表示されます。

ステップ 3 [SIP Header] タブをクリックします。

ステップ 4 [URI Conversion] タブをクリックします。

ステップ 5 新しい変換パラメータを追加するには、次の手順を実行します。

a. [TEL URI to SIP URI Conversions] ヘッダー、または [SIP URI to TEL URI Conversions] ヘッダーの下の [New] をクリックします。

b. 値を入力します。表 21 を参照してください。

c. [Add] をクリックします。

ステップ 6 TEL URI から SIP URI への変換パラメータを編集するには、次の手順を実行します。

a. 下線が引かれた SIP ヘッダーの名前をクリックします。

b. 値を更新します。表 21 を参照してください。

c. [Update] をクリックします。

ステップ 7 URI 変換パラメータを削除するには、URI 変換パラメータの横のボックスをオンにし、[Remove] をクリックします。

ステップ 8 URI 変換パラメータを元の設定に戻すには、URI 変換パラメータの横のボックスをオンにし、[Revert] をクリックします。

ステップ 9 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

SIP ヘッダーの URI パラメータの使用

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 下線が引かれた、使用する正規化ポリシーの名前をクリックします。

システムにより、[Normalization Policy: **< 正規化ポリシー名 >**] ページが表示されます。

ステップ 3 [SIP Header] タブをクリックします。

ステップ 4 [URI Parameter] タブをクリックします。

ステップ 5 URI パラメータを SIP ヘッダーに追加するには、次の手順を実行します。

a. 見出し [Add URI Parameters] の下の [New] をクリックします。

b. 値を入力します。表 22 を参照してください。

c. [Add] をクリックします。

ステップ 6 URI パラメータを SIP ヘッダーから削除するには、次の手順を実行します。

a. 見出し [Remove URI Parameters] の下の [New] をクリックします。

b. 値を入力します。表 22 を参照してください。

c. [Add] をクリックします。

ステップ 7 SIP ヘッダーの URI パラメータを更新するには、次の手順を実行します。

a. 見出し [Update URI Parameters] の下の [New] をクリックします。

b. 値を入力します。表 22 を参照してください。

c. [Add] をクリックします。

ステップ 8 ステップ 5 から ステップ 7 で追加したパラメータを削除するには、パラメータの横のボックスをオンにし、[Remove] をクリックします。

ステップ 9 ステップ 5 から ステップ 7 で追加したパラメータを以前の設定に戻すには、パラメータの横のボックスをオンにし、[Revert] をクリックします。

ステップ 10 ステップ 5 または ステップ 7 で追加したパラメータを編集、追加、または更新するには、パラメータ名をクリックし、変更を加えます。

ステップ 11 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

SIP ヘッダーのヘッダー パラメータの使用

手順

ステップ 1 [Configure] > [Normalization Policies] を選択します。

システムにより、[Normalization Policies] ページが表示されます。

ステップ 2 下線が引かれた、使用する正規化ポリシーの名前をクリックします。

システムにより、[Normalization Policy: **< 正規化ポリシー名 >**] ページが表示されます。

ステップ 3 [SIP Header] タブをクリックします。

ステップ 4 [Header Parameter] タブをクリックします。

ステップ 5 ヘッダー パラメータを SIP ヘッダーに追加するには、次の手順を実行します。

a. 見出し [Add Header Parameters] の下の [New] をクリックします。

b. 値を入力します。表 23 を参照してください。

c. [Add] をクリックします。

ステップ 6 ヘッダー パラメータを SIP ヘッダーから削除するには、次の手順を実行します。

a. 見出し [Remove Header Parameters] の下の [New] をクリックします。

b. 値を入力します。表 23 を参照してください。

c. [Add] をクリックします。

ステップ 7 SIP ヘッダーのヘッダー パラメータを更新するには、次の手順を実行します。

a. 見出し [Update Header Parameters] の下の [New] をクリックします。

b. 値を入力します。表 23 を参照してください。

c. [Add] をクリックします。

ステップ 8 ステップ 5 から ステップ 7 で追加したパラメータを削除するには、パラメータの横のボックスをオンにし、[Remove] をクリックします。

ステップ 9 ステップ 5 から ステップ 7 で追加したパラメータを以前の設定に戻すには、パラメータの横のボックスをオンにし、[Revert] をクリックします。

ステップ 10 ステップ 5 または ステップ 7 で追加したパラメータを編集、追加、または更新するには、パラメータ名をクリックし、変更を加えます。

ステップ 11 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化ポリシーの設定」の目次ページに戻る

時間ポリシーの設定

時間ポリシーの参照

手順

ステップ 1 [Configure] > [Time Policies] を選択します。

[Time Policies] ページが表示され、表 24 のフィールドに時間ポリシーが示されます。

ステップ 2 時間ポリシーを削除するには、次の操作を実行します。

a. 削除する時間ポリシーの名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

ステップ 3 この変更内容を、最後にコミットしたときの状態に戻すには、次の手順を実行します。

a. 元に戻す変更がある時間ポリシーの名前の横にあるボックスをオンにします。

b. [Revert] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

時間ポリシーについて

時間ポリシーは、時間ベースのルーティングを実装する場合に、ルート グループによって使用される時間ベースのルーティング設定です。

時間ベース フィールド

表 24 に、[Time Policies] ページのフィールドの一覧を示します。

表 24　　時間ポリシーのパラメータ

パラメータ	説明
State	次のいずれかを指定できます。 • [New]：新しいレコード。コミット時に、アクティブな設定に追加されます。 • [Modified]：変更されたレコード。コミット時に、アクティブな設定になります。 • [Deleted]：削除されたレコード。コミット時に、アクティブな設定から削除されます。 • [Active]：アクティブなレコードとアクティブな設定。
Name	この時間ポリシーの名前。

関連項目

- 「システム設定の管理」
- 「時間ポリシーの設定」の目次ページに戻る

時間ポリシーの追加

手順

ステップ 1　[Configure] > [Time Policies] を選択します。

[Time Policies] ページが表示されます。

ステップ 2　[Add] をクリックします。

[*Time Policy (New)*] ページが表示されます。

ステップ 3　この時間ポリシーの名前を入力します。

[Add] をクリックします。

新しい時間ポリシーの一覧が示された [Time Policy Step : < *時間ポリシー名* >] > [Add] ページが表示されます。

ステップ 4　手順が時間ポリシーに追加されます。「時間ポリシー手順の追加と編集」を参照してください。

ステップ 5　[Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「時間ポリシーの設定」の目次ページに戻る

時間ポリシー手順の参照

手順

ステップ 1 [Configure] > [Time Policies] を選択します。

[Time Policies] ページが表示されます。

ステップ 2 強調表示されている時間ポリシーの名前をクリックします。

[Time Policy Steps: < *時間ポリシー名* >] ページが表示されます。

関連項目

「時間ポリシーの設定」の目次ページに戻る

時間ポリシー手順の追加と編集

手順

ステップ 1 [Configure] > [Time Policies] を選択します。

[Time Policies] ページが表示されます。

ステップ 2 強調表示されている時間ポリシーの名前をクリックします。

[Time Policy Steps: < *時間ポリシー名* >] ページが表示されます。

ステップ 3 時間ポリシーの手順を追加するには、次の操作を実行します。

a. [Add] をクリックします。

新しい時間ポリシーの一覧が示された [Time Policy Step : < *時間ポリシー名* >] > [Add] ページが表示されます。

b. フィールドに値を入力します。表 25 を参照してください。

表 25 時間ポリシーの手順

パラメータ	説明
アクティブな日付	
Start Date & Time	この時間ポリシーを開始する日付と時刻。 日付、時刻、分、および AM または PM のいずれかを入力します。
End Date & Time	この時間ポリシーを終了する日付と時刻。 このチェックボックスをオンにし、[Update] をクリックすると、日付の入力を求めるプロンプトが表示されます。

表 25　時間ポリシーの手順 （続き）

パラメータ	説明
スケジュールの制約事項	
Weekdays/Dates	時間ポリシーに制約事項がある場合に、平日または日付の制約事項を定義します。 このチェックボックスをオンにし、[Update] をクリックすると、[Days of the Week] または [Days of the Month] の選択を求めるプロンプトが表示されます。 • [Days of the Week] のチェックボックスをオンにすると、このポリシーが発生する曜日のチェックボックスをオンにすることを求めるプロンプトが表示されます。 • [Days of the Month] のチェックボックスをオンにすると、このポリシーが発生する日付のチェックボックスをオンにすることを求めるプロンプトが表示されます。
Months	時間ポリシーに制約事項がある場合に、月ごとの制約事項を定義します。 このチェックボックスをオンにし、[Update] をクリックすると、ポリシーが実行される日付の入力を求めるプロンプトが表示されます。
Times of Day	時間ポリシーに制約事項がある場合に、時刻の制約事項を定義します。 このチェックボックスをオンにし、[Update] をクリックすると、時刻の入力を求めるプロンプトが表示されます。時刻を入力したら、[Add] をクリックします。さらに追加の時刻を入力することができます。

c. [Update] をクリックします。

ステップ 4　時間ポリシーの手順を編集するには、次の操作を実行します。

a. 強調表示されている時間ポリシー手順の名前をクリックします。

時間ポリシーの値の一覧が示された [Time Policy Step : < *時間ポリシー名* >] > [Edit] ページが表示されます。

b. フィールドの値を更新します。

c. [Update] をクリックします。

ステップ 5　[Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「時間ポリシーの設定」の目次ページに戻る

ルーティング トリガーの設定

ルーティング トリガーのリストの参照

ルーティング トリガーによって、トリガー条件がトリガー ポリシー（ルックアップ ポリシーとも呼ばれる）と関連付けられます。照合される対応条件によって、単一のポリシーが選択されます。条件はシーケンス番号の昇順で評価されます。

ルーティング トリガーは、ルーティング ロジックの指令に使用できる、条件のセットです。特定のイベント（または条件ケース）に対する応答として、自動的に実行されます。条件には、複数のケースがあります。

手順

ステップ 1 [Configure] > [Routing Triggers] を選択します。

[Routing Triggers] ページが表示され、すべてのルーティング トリガーが表示されます。

ステップ 2 ルーティング トリガーを削除するには、次の操作を実行します。

a. 削除するルーティング トリガーの名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

「ルーティング トリガーの設定」の目次ページに戻る

ルーティング トリガーの追加と編集

始める前に

システムには、少なくとも 1 つのトリガーが存在する必要があります。「トリガーの設定」を参照してください。

手順

ステップ 1 [Configure] > [Routing Triggers] を選択します。

[Routing Triggers] ページが表示されます。

ステップ 2 ルーティング トリガーを追加するには、次の操作を実行します。

a. [Add] をクリックします。

b. [Routing Trigger (New)] ページが表示されます。

c. ドロップダウンボックスから、ルーティング ポリシーを選択します。

d. ドロップダウンボックスから、トリガー条件を選択します。

e. [Add] をクリックします。

新しいルーティング トリガーが示された [Routing Triggers] ページが表示されます。

ステップ 3 既存のルーティング トリガーを編集するには、次の操作を実行します。

a. 編集するルーティング トリガーの名前の横にあるボックスをオンにします。

b. [Edit] をクリックします。

c. 異なるルーティング ポリシーまたはトリガー条件を選択します。いずれか一方または両方を変更できます。

d. [Update] をクリックします。

ステップ 4 既存のルーティング トリガーを移動するには、次の操作を実行します。

a. 移動するルーティング トリガーの名前の横にあるボックスをオンにします。

b. 上矢印または下矢印をクリックします。

ステップ 5 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「ルーティング トリガーの設定」の目次ページに戻る

正規化トリガーの設定

正規化前トリガーのリストの参照

手順

ステップ 1 [Configure] > [Normalization Triggers] > [Pre-Normalization] を選択します。

[Pre-Normalization] ページが表示され、すべての正規化前トリガーが表示されます。

ステップ 2 正規化前トリガーを削除するには、次の操作を実行します。

a. 削除する正規化前トリガーの名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化トリガーの設定」の目次ページに戻る

正規化後トリガーのリストの参照

手順

ステップ 1 [Configure] > [Normalization Triggers] > [Post-Normalization] を選択します。

[Post-Normalization] ページが表示され、すべての正規化後トリガーが表示されます。

ステップ 2 正規化後トリガーを削除するには、次の操作を実行します。

a. 削除する正規化後トリガーの名前の横にあるボックスをオンにします。

b. [Remove] をクリックします。

c. [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

正規化トリガーについて

正規化トリガーは、トリガー条件を正規化ポリシーと相互に関連付けます。正規化トリガーには、次の 2 つのタイプがあります。

- ルーティング前に発生する、正規化前トリガー
- ルーティング後に発生する、正規化後トリガー

特殊なポリシーでは、mid-dialog メッセージでの正規化がバイパスされます。

[Pre-Normalization Triggers] ページおよび [Post-Normalization Triggers] ページから、正規化トリガーを追加、更新、または削除できます。

関連項目

- 「システム設定の管理」
- 「正規化トリガーの設定」の目次ページに戻る

正規化前トリガーの追加と編集

手順

ステップ 1 [Configure] > [Normalization Triggers] > [Pre-Normalization] を選択します。

[Pre-Normalization Triggers] ページが表示されます。

ステップ 2 正規化前トリガーを追加するには、次の操作を実行します。

a. [Add] をクリックします。[Pre-Normalization Trigger: *New*] ページが表示されます。

b. ドロップダウン メニューから、正規化ポリシーを選択します。

c. ドロップダウン メニューから、トリガー条件を選択します。

d. [Add] をクリックします。

[Pre-Normalization Triggers] ページが表示され、すべてのトリガーが表示されます。

ステップ 3 正規化前トリガーのルールを追加、編集、または削除するには、「トリガーのルールの参照、追加、移動、および削除」の手順に従います。

ステップ 4 正規化前トリガーを編集するには、次の操作を実行します。

a. 編集する正規化前トリガーの名前の横にあるチェックボックスをオンにします。

b. [Edit] をクリックします。[Pre-Normalization Trigger] ページが表示されます。

c. ドロップダウン メニューから、正規化ポリシーを選択します。

d. ドロップダウン メニューから、トリガー条件を選択します。

e. [Update] をクリックします。[Pre-Normalization Triggers] ページが表示され、すべてのトリガーが表示されます。

ステップ 5 複数の正規化前トリガーがある場合、次の操作を行うことによって、命令を再実行できます。

ヒント 1 つの正規化前トリガーが一致すると、その他のすべてのトリガーが無視されます。システムを最適化するには、リストの最も上で一致するよう、正規化前トリガーを設定することを推奨します。

a. 正規化前トリガーを選択します。
b. 上矢印または下矢印をクリックします。
c. [Update] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化トリガーの設定」の目次ページに戻る

正規化後トリガーの追加と編集

手順

ステップ 1 [Configure] > [Normalization Triggers] > [Post-Normalization] を選択します。

[Post-Normalization Triggers] ページが表示されます。

ステップ 2 正規化後トリガーを追加するには、次の操作を実行します。

a. [Add] をクリックします。[Post-Normalization Trigger: *New*] ページが表示されます。
b. ドロップダウン メニューから、正規化ポリシーを選択します。
c. ドロップダウン メニューから、トリガー条件を選択します。
d. [Add] をクリックします。

[Post-Normalization Triggers] ページが表示され、すべてのトリガーが表示されます。

ステップ 3 正規化後トリガーのルールを追加、編集、または削除するには、「トリガーのルールの参照、追加、移動、および削除」の手順に従います。

ステップ 4 正規化後トリガーを編集するには、次の操作を実行します。

a. 編集する正規化後トリガーの名前の横にあるチェックボックスをオンにします。
b. [Edit] をクリックします。[Post-Normalization Trigger] ページが表示されます。
c. ドロップダウン メニューから、正規化ポリシーを選択します。
d. ドロップダウン メニューから、トリガー条件を選択します。
e. [Update] をクリックします。[Post-Normalization Triggers] ページが表示され、すべてのトリガーが表示されます。

ステップ 5 複数の正規化後トリガーがある場合、次の操作を行うことによって、命令を再実行できます。

ヒント 1 つの正規化後トリガーが一致すると、その他のすべてのトリガーが無視されます。システムを最適化するには、リストの最も上で一致するよう、正規化後トリガーを設定することを推奨します。

a. 正規化後トリガーを選択します。

b. 上矢印または下矢印をクリックします。

c. [Update] をクリックします。

ステップ 6 [Cisco Unified SIP Proxy] ヘッダーで、[Commit Candidate Configuration] をクリックして、変更をコミットします。

関連項目

- 「システム設定の管理」
- 「正規化トリガーの設定」の目次ページに戻る

ユーザの設定

ユーザのリストの表示

手順

ステップ 1 [Configure] > [Users] を選択します。

[Configure Users] ページに次のフィールドが表示されます。

- [User ID] : デフォルトで、ユーザがユーザ ID のアルファベット順に表示されます。
- [Display Name]
- [Primary Extension]

ステップ 2 異なる人数のユーザを各ページに表示するには、右上にあるドロップダウン ボックスで別の人数を選択し、[Go] をクリックします。10、25、50、100、またはすべてのユーザの表示が選択できます。

ステップ 3 他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 4 ユーザを並べ替えるには、該当するヘッダーをクリックします。

ステップ 5 Cisco Unified SIP Proxy システムからユーザを削除する（ユーザのメールボックスも削除されます）には、次の手順を行います。

a. 削除するユーザ ID の隣のチェックボックスをオンにします。

b. [Delete] をクリックします。

c. [OK] をクリックして削除を確認します。

ユーザ プロフィール フィールド

表 26 に、[User Profile] ページのフィールドを示します。

表 26　　ユーザ プロフィール パラメータ

パラメータ	説明
User ID	英数字のユーザ ID です。
First Name	ユーザの名です。発信者はこの名前を使用して内線番号にアクセスすることで、名前によるダイヤル機能を使用します。このフィールドに特殊文字、スペース、数字は使用できません。
Last Name	ユーザの姓です。発信者はこの名前を使用して内線番号にアクセスすることで、名前によるダイヤル機能を使用します。このフィールドに特殊文字、スペース、数字は使用できません。
Nick Name	ユーザのニックネームでオプションです。
Display Name	Cisco Unified SIP Proxy アプリケーションに表示されるユーザ名です。
Primary E.164 Number	市外局番を含む、ユーザのプライマリ電話番号です。
Fax Number	このユーザのファクス番号です。
Language	ボイスメール ユーザに対して話される応答の言語です。使用できる言語は、インストールした Cisco Unified SIP Proxy のバージョンによって異なります。
Password Login	ログインがパスワード対応であるかどうかです。
Password options	ユーザが GUI へのアクセスに使用するパスワードの場合、次のうちのいずれかを選択します。 • [Generate a Random Password]：システムによってランダムなパスワードを生成します。 • [Blank Password]：パスワードを空白のままにします。 • [Password Specified Below]：このユーザのパスワードを指定します。
Password	パスワードは文字と数字から構成され、その長さは 3 文字以上で、32 文字以下です。
PIN Login	ログインが PIN 対応であるかどうかです。
PIN options	**（注）** PIN を設定する領域がありますが、Cisco Unified SIP Proxy システムは PIN を使用しません。このフィールドに値を設定しても使用されません。
PIN	使用しません。

関連項目

「ユーザの設定」の目次ページに戻る

新しいユーザの追加

手順

ステップ 1 [Configure] > [Users] を選択します。

[Configure Users] ページが表示されます。

ステップ 2 [Add] をクリックします。

ステップ 3 フィールドに情報を入力します。表 26 を参照してください。

ステップ 4 [Add] をクリックします。

（注） ランダムなパスワードを選択した場合、新しいパスワードを示すメッセージが表示されます。値を安全な場所に書き記し、ユーザに伝えます。値は、ユーザ プロファイル ページにも表示されます（「ユーザ プロファイルの表示または変更」を参照）。

関連項目

「ユーザの設定」の目次ページに戻る

ユーザ プロファイルの表示または変更

手順

ステップ 1 [Configure] > [Users] を選択します。

[Configure Users] ページが表示されます。

ステップ 2 表示するユーザの下線付きのユーザ ID をクリックします。

（注） 探しているユーザが表示されない場合は、[Find] をクリックします （「ユーザの検索」を参照）。

[User Profile] ページに表 26 のフィールドが表示されます。

関連項目

「ユーザの設定」の目次ページに戻る

グループ登録の表示または変更

ユーザが割り当てられるグループを変更するには、次の手順を使用します。

手順

ステップ 1 [Configure] > [Users] を選択します。

[Configure Users] ページが表示されます。

ステップ 2 グループへの登録を表示または変更するユーザの下線付きの名前をクリックします。

[User Profile] ページが表示されます。

ステップ 3 [Groups] タブをクリックします。次のフィールドが表示されます。

- [Group ID]
- [Rights]：ユーザがグループのメンバーであるかどうか、またはオーナーであるかどうかです。
- [Description]
- [Primary extension]：グループに割り当てられる共有メールボックスのプライマリ内線番号です。

ステップ 4 ユーザを他のグループのオーナーとして登録するには、[Subscribe as owner] をクリックします。ユーザを他のグループのメンバーとして登録するには、[Subscribe as member] をクリックします。

[Find] ページが表示されます。

ステップ 5 グループ ID、説明、または内線番号を入力し、[Find] をクリックします。

ステップ 6 このユーザを追加するグループの隣にあるチェックボックスをオンにし、[Select Rows] をクリックします。

ステップ 7 （オプション）ユーザをグループから登録解除するには、グループ名の隣にあるチェックボックスをオンにし、[Unsubscribe] をクリックします。

関連項目

- 「ユーザの設定」の目次ページに戻る
- 「グループの設定」

ユーザの検索

手順

ステップ 1 [Configure] > [Users] を選択します。

[Configure Users] ウィンドウが表示されます。

ステップ 2 [Find] をクリックします。

次のフィールドが表示されます。

- [User ID]
- [Name]
- [Extension]

ステップ 3 1 つまたは複数のフィールドに検索条件を入力し、[Find] をクリックします。
検索結果が表示されます。

関連項目
「ユーザの設定」の目次ページに戻る

パスワードの変更

制約事項

- パスワードは長さが 3 文字以上 32 文字以下で、英数字である必要があります。
- 大文字と小文字および数字を組み合わせて使用します。
- スペースは使用できません。

手順

ステップ 1 [Configure] > [Users] を選択します。
[Configure Users] ページが表示されます。
ステップ 2 ユーザのリストで、ユーザの名前をクリックします。
ステップ 3 [Password options] フィールドで、[Password specified below] が選択されていることを確認します。
ステップ 4 新しいパスワードを入力します。
ステップ 5 確認のため、新しいパスワードをもう一度入力します。
ステップ 6 [Apply] をクリックします。

関連項目
「ユーザの設定」の目次ページに戻る

ユーザ デフォルトの設定

ユーザを作成するとき、[Configure User] ウィンドウに設定されるデフォルトが有効です。すべてのユーザのデフォルト グローバル パスワード ポリシー設定を指定するには、次の手順を使用します。このパラメータのデフォルト設定は、新しいユーザの作成時に適用されます。

（注） このウィンドウでデフォルトを設定した後でも、個別のユーザのパスワード ポリシーを変更できます。「パスワードの変更」を参照してください。

- 「パスワード オプションの設定」
- 「アカウント ロックアウト ポリシーの設定」

パスワード オプションの設定

ユーザのパスワードの自動生成を選択する場合、次の手順で設定します。

手順

ステップ 1 [Configure] > [User Defaults] を選択します。

[Configure User Defaults] ページが表示されます。

ステップ 2 [Password] カラムで次の手順を実行することで、パスワード オプションを設定します。

（注） PIN を設定する領域がありますが、Cisco Unified SIP Proxy システムは PIN を使用しません。このフィールドに値を設定しても使用されません。

a. 自動生成ポリシーは、ランダム、または空白を選択します。

b. （オプション）[Enable expiry (days):] をチェックして、パスワードの有効期限を設定します。範囲は 3 ～ 365 です。

c. 履歴数を設定します。範囲は 1 ～ 10 です。

d. パスワードの最小の長さを選択します。パスワードの範囲は、3 ～ 32 です。

ステップ 3 [Apply] をクリックします。

関連項目

「ユーザ デフォルトの設定」の目次ページに戻る

アカウント ロックアウト ポリシーの設定

アカウント ロックアウト ポリシーは、ユーザがログインを試みて失敗したときのシステム動作を規定します。

手順

ステップ 1 [Configure] > [User Defaults] を選択します。

[Configure User Defaults] ページが表示されます。

ステップ 2 次のロックアウト ポリシー タイプのうちのいずれかを [Password] フィールドで選択します。

（注） PIN を設定する領域がありますが、Cisco Unified SIP Proxy システムは PIN を使用しません。このフィールドに値を設定しても使用されません。

- [Disable lockout]：ユーザは、失敗による影響なしにログインの試行を継続できます。
- [Permanent]：ユーザは、特定回数のログイン試行の失敗の後で、永続的にロックアウトされます。試行失敗の最大数を入力します。範囲は 1 ～ 200 です。
- [Temporary]：ユーザは一時的にシステムからロックアウトされます。次の値を入力します。
  - 試行が可能な回数。範囲は 1 ～ 200 です。
  - 一時的ロックアウト期間。任意の数（分単位）を選択します。
  - 試行失敗の最大数。範囲は 1 ～ 200 です。

ステップ 3 [Apply] をクリックして設定を保存します。

関連項目

「ユーザ デフォルトの設定」の目次ページに戻る

グループの設定

グループのリストの表示

手順

ステップ 1 [Configure] > [Groups] を選択します。

次のフィールドのある [Configure Groups] ページが表示されます。

- [Group ID]
- [Display Name]
- [Primary Extension]
- [Privileges]

ステップ 2 異なる数のグループを各ページに表示するには、右上にあるドロップダウン ボックスで別の数を選択し、[Go] をクリックします。10、25、50、100、またはすべてのグループの表示が選択できます。

ステップ 3 他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 4 グループを並べ替えるには、該当するヘッダーをクリックします。

グループ フィールド

表 27 には、ページのフィールドの一覧が示されています。

表 27　　グループ パラメータ

パラメータ	説明
Group ID	英数字のユーザ ID です。
Full name	電話機に表示されるグループの長い名前です。
Description	グループの説明です。Group ID エントリに単語「group」が自動的に追加されます。
Primary Extension	グループの共用メールボックスのプライマリ内線番号です。
Primary E.164 Number	このグループに、完全な電話番号と市外局番を割り当てます。
Fax Number	このグループに、ファクス番号を割り当てます。

関連項目

「グループの設定」の目次ページに戻る

新しいユーザ グループの追加

1 つまたは複数のグループの設定はオプションです。多くの企業で、共用メールボックスと呼ばれるグループのためのメールボックスを用意すると便利であることがわかっています。グループのメンバーは、共用メールボックスにあるボイスメッセージを取得できます。たとえば、Customer Service メールボックスを顧客からのメールの受信用に設定すると、Customer Service グループに割り当てられたユーザは誰でもそのメッセージを取得できます。共用メールボックスのメンバーは、個々のユーザまたは他のグループです。個々のユーザは、それぞれのメールボックスも所有できます。別のグループのメンバーであるグループも、固有のメールボックスを所有できます。

始める前に

グループに割り当てるプライマリ内線番号を決定します。この内線番号がアクティブであることを確認します。

手順

ステップ 1　[Configure] > [Groups] を選択します。

[Configure Groups] ページが表示されます。

ステップ 2　[Add] をクリックします。

[Add a New Group] ページが表示されます。

ステップ 3　次に示されるフィールドに情報を入力します。

- [Group ID]
- [Full name]
- [Description]：Group ID エントリに単語「group」が自動的に追加されます。この説明にテキストを追加できます。
- [Primary Extension]：グループの共用メールボックスのプライマリ内線番号です。
- [Primary E.164 Number]
- [Fax Number]

ステップ 4 このグループが保有する機能の隣のチェックボックスをオンにします。「機能について」を参照してください。

ステップ 5 [Add] をクリックします。

[Configure Groups] ページの表に新しいグループが表示されます。

関連項目

「グループの設定」の目次ページに戻る

グループへのメンバーまたはオーナーの登録

グループにメンバーを追加する場合、各メンバーはグループのメールボックスに格納されたボイスメッセージにアクセスできます。

グループ オーナーはグループのメールボックスを制御できますが、グループのメッセージにはアクセスできません。メッセージにアクセスするには、グループ オーナーがグループのメンバーでもあることが必要です。

手順

ステップ 1 [Configure] > [Groups] を選択します。

[Configure Groups] ページが表示されます。

ステップ 2 新しいメンバーまたはオーナーを追加するグループの下線付きの名前をクリックします。

そのグループの [Group Profile] ページが表示されます。

ステップ 3 [Owners/Members] タブをクリックします。

グループのすべてのオーナーとメンバーが表示されます。

ステップ 4 新しいメンバーを追加するには、[Subscribe Member] をクリックします。新しいオーナーを追加するには、[Subscribe Owner] をクリックします。

[Find] ページが表示されます。

ステップ 5 [type] の下で、[users] または [groups] を選択します。このグループに追加する人またはグループのユーザ ID またはグループ ID、名前または説明、または内線番号を入力します。

ステップ 6 [Find] をクリックします。

検索条件に一致するすべてのユーザまたはグループが表示されます。

ステップ 7 次のいずれかを実行します。

- 選択されたメンバーまたはオーナーの名前の隣にあるチェックボックスをオンにして、[Select Rows] をクリックすることで、1 人または複数のメンバーまたはオーナーをグループに追加します。[Group] ページに、追加された新しいメンバーまたはオーナーが表示されます。
- 名前の隣にあるチェックボックスをオンにせずに [Back to Find] をクリックして、追加する他の人を探します。[Find] ページが表示されます。ステップ 5 に戻って続行します。

ステップ 8 さらにメンバーまたはオーナーをグループに追加するには、ステップ 4 からステップ 7 を繰り返します。

関連項目

「グループの設定」の目次ページに戻る

グループへのメンバーまたはオーナーの登録解除

制約事項

グループ オーナーだけが、メンバーおよびオーナーを削除できます。

手順

ステップ 1 [Configure] > [Groups] を選択します。

[Configure Groups] ページが表示されます。

ステップ 2 対象となるグループの下線付きの名前をクリックします。

そのグループの [Group Profile] ページが表示されます。

ステップ 3 [Owners/Members] タブをクリックします。

グループのすべてのオーナーとメンバーが表示されます。

ステップ 4 このグループから登録を解除する削除するメンバーまたはオーナーの名前の隣にあるチェックボックスをオンにします。

ステップ 5 [Unsubscribe] をクリックします。

[Group Members] ページが、メンバーまたはオーナーが削除された状態で表示されます。

関連項目

「グループの設定」の目次ページに戻る

グループ パラメータの表示または変更

手順

ステップ 1 [Configure] > [Groups] を選択します。

[Configure Groups] ページが表示されます。

ステップ 2 表示または変更するグループの下線付きの名前をクリックします。

そのグループの [Group Profile] ページに次のフィールドが表示されます。

- [Group ID]
- [Full name]
- [Description]
- [Primary Extension]
- [Primary E.164 Number]
- [Fax Number]
- [Capabilities] 機能については、「機能について」を参照してください。

ステップ 3 これらのフィールドを編集するには、新しい情報を入力し、[Apply] をクリックします。

関連項目

「グループの設定」の目次ページに戻る

グループのオーナーおよびメンバーの表示

手順

ステップ 1 [Configure] > [Groups] を選択します。

[Configure Groups] ページが表示されます。

ステップ 2 表示するグループの下線付きの名前をクリックします。

そのグループの [Group Profile] ページが表示されます。

ステップ 3 [Owners/Members] タブをクリックして、このグループのオーナーまたはメンバーであるユーザを表示します。

[Owners/Members] ページが表示されます。

ステップ 4 列見出し行をクリックして、その項目で並べ替えます。

関連項目

「グループの設定」の目次ページに戻る

他のグループのグループ オーナーおよびメンバーの変更

グループは、1 組のメンバーを保有しますが、1 つまたは複数の他のグループのメンバーまたはオーナーとして割り当てることもできます。あるグループが別のグループのオーナーとして割り当てられている場合、オーナーのグループの各メンバーは、所有するグループのオーナーとしての特権を保持します。たとえば、Administrator グループが Technical Support グループのオーナーとして追加された場合、Administrator グループの各メンバーは、Technical Support グループのメンバーの追加、変更、削除ができます。さらに、一方のグループの所属していないユーザは、Technical Support グループのオーナーとして追加できます。

手順

ステップ 1 [Configure] > [Groups] を選択します。

[Configure Groups] ページが表示されます。

ステップ 2 メンバーを変更するグループの名前をクリックします。

そのグループの [Group Profile] ページが表示されます。

ステップ 3 [Owner/Member of Groups] タブをクリックします。

[Owner/Member of Groups] ページが表示されます。

ステップ 4 異なる数のグループを各ページに表示するには、右上にあるドロップダウン ボックスで別の数を選択し、[Go] をクリックします。10、25、50、100、500 のグループの表示が選択できます。

ステップ 5 他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 6 グループを並べ替えるには、該当するヘッダーをクリックします。

ステップ 7 グループを他のグループのオーナーとして指定するには、[Subscribe as owner] をクリックします。グループを他のグループのメンバーとして登録するには、[Subscribe as member] をクリックします。

[Find] ページが表示されます。

ステップ 8 検索するグループのグループ ID、説明、または内線番号を入力します。

ステップ 9 [Find] をクリックします。

検索条件に一致するすべてのグループが表示されます。

ステップ 10 1 つまたは複数のグループを選択するには、グループ名の隣にあるチェックボックスをオンにして、[Select Rows] をクリックします。

新しいグループが [Owner/Member of Groups] ページのグループのリストに追加されます。

関連項目

「グループの設定」の目次ページに戻る

グループの削除

グループの削除によって、グループのメールボックスが削除されますが、グループのメンバーは削除されません。

手順

ステップ 1 [Configure] > [Groups] を選択します。

[Configure Groups] ページが表示されます。

ステップ 2 削除するグループの名前の隣にあるチェックボックスを選択し、[Delete] をクリックします。

ステップ 3 プロンプトで [OK] をクリックして、グループを削除します。

関連項目

「グループの設定」の目次ページに戻る

グループの検索

グループを検索するには次の手順を使用します。

手順

ステップ 1 [Configure] > [Groups] を選択します。
[Configure Groups] ページが表示されます。

ステップ 2 [Find] をクリックします。[Find Groups] ウィンドウに次のフィールドが表示されます。

- [Group ID]
- [Description]
- [Extension]：グループの共用メールボックスの内線番号

ステップ 3 1 つまたは複数のフィールドに検索条件を入力し、[Find] をクリックします。
[Configure Groups] ページに検索結果が表示されます。

関連項目

「グループの設定」の目次ページに戻る

機能について

グループに機能を割り当てることができます。

Cisco Unified SIP Proxy には 3 つの機能があります。

- pfsread：ユーザは Public File System（PFS）から読み込むことができます。
- pfsreadwrite：ユーザは PFS の読み書きができます。
- superuser：このグループのユーザに管理者特権を与えます。

関連項目

「グループの設定」の目次ページに戻る

特権の設定

特権の表示

手順

ステップ 1 [Configure] > [Privileges] を選択します。

[Configure Privileges] ページが表示されます。

ステップ 2 異なる数の特権を各ページに表示するには、右上にあるドロップダウン ボックスで別の数を選択し、[Go] をクリックします。10、25、50、100、またはすべての特権の表示が選択できます。

ステップ 3 他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 4 特権を並べ替えるには、該当するヘッダーをクリックします。

ステップ 5 特権を削除するには、次の手順を行います。

a. 削除する特権を選択します。

b. [Delete] をクリックします。

ヒント pfsread、pfsreadwrite、またはスーパーユーザの各特権は削除できません。

特権の概要

Cisco Unified SIP Proxy では、グループに割り当てられる事前定義の特権が 3 つあります。独自の特権を作成することも、事前定義の特権を変更することもできます。

特権をグループに割り当てた場合、すべてのグループ メンバーに特権が付与されます。管理者として指定され、インポートされた加入者から、ソフトウェアのインストール プロセスによって管理者グループが自動的に作成されます。

特権を作成または変更する場合、その特権に許可された操作を追加または削除します。操作は、許可される CLI コマンドおよび GUI 機能を定義します。多くの操作は、CLI コマンドおよび GUI 機能を 1 つだけ含みます。特権に操作を追加することに加えて、特権が別の特権をネストして保持するように設定できます。ネストした特権を保持するように設定された特権は、ネストした特権に設定されたすべての操作を含みます。

表 28 に、特権に追加できる、使用可能なすべての操作を示しています。

（注） ユーザには自分のデータにアクセスする特権は必要ありません。ユーザのデータは、主にボイスメール アプリケーションおよび次の項目と関係があります。

- 言語（ユーザのボイス メールボックスに設定されている）
- パスワード
- ユーザが所有するグループに対するメンバーシップ
- ユーザが所有するグループのオーナーシップ
- プロファイルの通知
- カスケード設定
- 個人ボイスメールのゼロ出力数
- ボイスメールのグリーティングの種類
- ボイスメール チュートリアル再生フラグ
- ユーザが所有するパブリック同報リスト
- プライベート同報リスト

表 28　　操作のリスト

操作	説明
group.configuration	グループを作成、変更および削除します。
security.aaa	AAA サービス設定を設定および変更します。
security.access	データの暗号化に関するシステム レベルのセキュリティを設定します（暗号キーの定義を含む）。 **（注）** システムのリロードの許可も含まれます。
security.password	次のような、システム パスワードおよびポリシーの設定を設定します。 • 有効期限 • ロックアウト（一時的または永続的） • 履歴 • 長さ

表 28　操作のリスト （続き）

操作	説明
security.pin	次のような、PIN およびポリシーを設定します。 • 有効期限 • ロックアウト（一時的または永続的） • 履歴 • 長さ
services.configuration	システム サービスの設定：DNS、NTP/クロック、SMTP、SNMP、Fax Gateway、Cisco UMG、ホスト名、ドメイン、インターフェイス（カウンタ）、およびシステムのデフォルト言語。 **（注）**　システムのリロードの許可も含まれます。
services.manage	DNS キャッシュのクリアや ping などの、設定とは関係ないシステム レベル サービス コマンド。
software.install	システム ソフトウェアまたは言語やライセンスなどのアドオンをインストール、アップグレード、または検査します。 **（注）**　システムのリロードの許可も含まれます。
system.backup	バックアップを設定します。
system.configuration	クロック、ホスト名、ドメイン名、デフォルト言語、インターフェイス（カウンタ）などのシステム設定を設定します。
system.debug	トレース データおよびデバッグ データを収集、および設定します。コア ファイルやログ ファイルなどのデータのコピーも含まれます。
system.view	システム設定およびコンフィギュレーションを表示します。
user.configuration	ユーザおよびグループを作成、変更、削除し、次の項目の設定を行います。 • 姓名 • ニックネーム • 表示名 • 言語
user.password	他のユーザのパスワードの作成、設定、削除を行います。
user.pin	他のユーザの PIN の作成、設定、削除を行います。

関連項目

「特権の設定」の目次ページに戻る

特権の作成

手順

ステップ 1 [Configure] > [Privileges] を選択します。
[Configure Privileges] ページが表示されます。
ステップ 2 [Add] をクリックします。
ステップ 3 特権の名前と説明を入力します。
ステップ 4 特権に追加する操作をチェックします。表 28 を参照してください。
ステップ 5 [Add] をクリックします。

関連項目

「特権の設定」の目次ページに戻る

特権の編集

制約事項

- pfsread、pfsreadwrite、またはスーパーユーザ特権は変更できません。
- 一部の操作は必須であり、削除できません。

始める前に

- 特権を作成します。「特権の作成」を参照してください。

手順

ステップ 1 [Configure] > [Privileges] を選択します。
[Configure Privileges] ページが表示されます。
ステップ 2 カスタマイズする特権の下線付きの名前をクリックします。
ステップ 3 特権と追加する操作を選択するか、または削除する操作の選択を解除します。
ステップ 4 [Apply] をクリックします。
ステップ 5 [OK] をクリックして、変更を保存します。

関連項目

「特権の設定」の目次ページに戻る

認証、認可、アカウンティングの設定

AAA 認証サーバの設定

関連項目

「認証、認可、アカウンティングの設定」の目次ページに戻る

認証の順序について

AAA ポリシーでは、認証サーバにオプションで設定できるフェールオーバー機能を指定できます。2 つのフェールオーバー機能は、別々に、または組み合わせて、使用できます。

- 認証フェールオーバー
- 到達不能フェールオーバー

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA 認証サーバの設定」の目次ページに戻る
- 次の項目：「認証フェールオーバーについて」

認証フェールオーバーについて

認証フェールオーバー機能を使用すると、ユーザ ログイン認証のために、ローカル データベースに加え、オプションでリモート RADIUS サーバを使用できるようになります。この項の手順では、認証が解決される順序が設定されます。次のシステムを使用するよう、認証を設定できます。

- ローカル データベースのみ
- リモート サーバのみ
- 最初にローカル データベース、次にリモート サーバ
- 最初にリモート サーバ、次にローカル データベース

ローカル認証とリモート認証の両方を使用する場合、リモート RADIUS AAA サーバから取得されるユーザ属性を、同じユーザ名のローカル ユーザ データベースで見つかった属性にマージするかどうかも、設定できます。

（注） 認証フェールオーバー機能には、次の制限があります。

- RADIUS サーバでの認証は、GUI または CLI インターフェイスへのアクセス時にのみ使用可能で、ユーザ ID およびパスワードのみが必要です。自動受付インターフェイスは、ユーザに依存しないため、認証は不要です。
- ログイン情報は、ローカル システムとリモート サーバとの間では同期がとられません。したがって、次のとおりになります。
  - パスワードの期限切れなどのセキュリティ機能は、Cisco Unified SIP Proxy と RADIUS サーバで別々に設定する必要があります。
  - パスワードの期限切れまたはアカウントのロックアウトなどのセキュリティ イベントが、RADIUS サーバで発生した場合、Cisco Unified SIP Proxy ユーザに対しては、プロンプトは表示されません。
  - パスワードの期限切れまたはアカウントのロックアウトなどのセキュリティ イベントが、Cisco Unified SIP Proxy で発生した場合、RADIUS サーバのユーザに対しては、プロンプトは表示されません。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA 認証サーバの設定」の目次ページに戻る
- 次の項目：「到達不能フェールオーバーについて」

到達不能フェールオーバーについて

到達不能フェールオーバー機能は、RADIUS サーバでのみ使用されます。この機能を使用すると、RADIUS サーバへのアクセスに使用できる最大 2 つまでのアドレスを設定できます。

Cisco Unified SIP Proxy によって、RADIUS サーバでユーザの認証が試行されると、RADIUS サーバが、ユーザの認証に到達できないか、失敗したかを通知するメッセージが、ユーザに送信されます。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る

- 「AAA 認証サーバの設定」の目次ページに戻る
- 次の項目：「認証シーケンスの例」

認証シーケンスの例

この例では、認証は、まず、リモート サーバによって実行され、次に、ローカル データベースによって実行されます。また、2 つのアドレスが、リモート RADIUS サーバに対して設定されます。

イベントのこのシーケンスは、次の例の認証中に発生する可能性があります。

1. Cisco Unified SIP Proxy では、まず、リモート RADIUS サーバへの通信が試行されます。
2. 1 台目の RADIUS サーバで、応答がないか、ユーザの認証クレデンシャルが受け付けられない場合、Cisco Unified SIP Proxy では、2 台目のリモート RADIUS サーバへの通信が試行されます。
3. 2 台目の RADIUS サーバで、応答がないか、ユーザの認証クレデンシャルが受け付けられない場合、ユーザは該当するエラー メッセージを受信し、Cisco Unified SIP Proxy では、ローカル データベースへの通信が試行されます。
4. ローカル データベースで、ユーザの認証クレデンシャルが受け付けられない場合、ユーザはエラー メッセージを受信します。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA 認証サーバの設定」の目次ページに戻る
- 次の項目：「AAA 認証サーバの接続パラメータの設定」

AAA 認証サーバの接続パラメータの設定

手順

ステップ 1 [Configure] > [AAA] > [Authentication] を選択します。

[Configure AAA Authentication] ページが表示されます。

ステップ 2 プライマリ サーバの適切なフィールドに、次の情報を入力し、オプションで、セカンダリ サーバの適切なフィールドにも入力します。

- 認証順序
- ログイン再試行の回数
- ログイン タイムアウトの長さ
- ホスト名
- ポート
- パスワード

ステップ 3 [Apply] をクリックします。

ステップ 4 [OK] をクリックして、変更を保存します。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA 認証サーバの設定」の目次ページに戻る

認証と認可の動作を制御するポリシーの指定

手順

ステップ 1 [Configure] > [AAA] > [Authorization] を選択します。

[Configure AAA Authorization] ページが表示されます。

ステップ 2 リモート AAA サーバの属性を、ローカル データベースの属性とマージするかどうかを、選択するか、選択を解除します。

ステップ 3 [Apply] をクリックします。

ステップ 4 [OK] をクリックして、変更を保存します。

関連項目

「認証、認可、アカウンティングの設定」の目次ページに戻る

AAA アカウンティング サーバの設定

- 「概要」
- 「AAA アカウンティング イベント ロギング」
- 「AAA アカウンティング サーバとイベント ロギングの設定」

関連項目

「認証、認可、アカウンティングの設定」の目次ページに戻る

概要

最大で 2 台の AAA アカウンティング サーバを設定できます。アカウンティング サーバを 2 台設定すると、自動フェールオーバー機能を使用できます。1 台目のサーバが到達不能の場合、アカウンティング情報が 2 台目のサーバに送信されます。両方のアカウンティング サーバが到達不能の場合、サーバが使用可能になるまで、アカウンティング レコードがキャッシュ保存されます。キャッシュがいっぱいになるまでにサーバに到達できない場合、最も古いアカウンティング パケットがドロップされ、新しいパケットのための容量が確保されます。

AAA アカウンティング サーバの設定は、AAA 認証サーバの設定から完全に独立しているため、AAA アカウンティング サーバは、AAA 認証サーバと同じマシンまたは異なるマシンに設定できます。

Syslog サーバを使用する場合、AAA 設定には影響を受けず、既存のユーザ インターフェイスが使用し続けられます。RADIUS サーバから Syslog サーバに AAA アカウンティング情報が送信される場合、記録される前に 1 つの文字列に正規化されます。Syslog サーバが定義されていない場合、Cisco Unity Express でローカルに実行されている Syslog サーバによって、AAA アカウンティング ログが記録されます。

（注） RADIUS サーバのみがサポートされます。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA アカウンティング サーバの設定」の目次ページに戻る
- 次の項目：「AAA アカウンティング イベント ロギング」

AAA アカウンティング イベント ロギング

AAA アカウンティング ログには、次の操作を簡単に実行できる情報が含まれています。

- 設定の変更を監査する。
- セキュリティを管理する。
- 正確にリソースを割り当てる。
- リソースの使用を課金する必要があるかどうかを決定する。

AAA アカウンティングを設定し、次のタイプのイベントのログを記録することができます。

ログ名	説明
login	ログインが必要な場合のすべての形式のシステム アクセス。
logout	ログアウト前にログインが必要な場合のすべての形式のシステム アクセス。
login-fail	ログインが必要な場合のすべての形式のシステム アクセスの、失敗したログイン試行。
config-commands	任意のインターフェイスを使用してシステム設定に行われた変更。
exec-commands	任意のインターフェイスを使用して EXEC モードで入力されたすべてのコマンド。
system-startup	システムのソフトウェア バージョン、インストールされているライセンス、インストールされているパッケージ、インストールされている言語などに関する情報が含まれる、システムの起動。
system-shutdown	システムのソフトウェア バージョン、インストールされているライセンス、インストールされているパッケージ、インストールされている言語などに関する情報が含まれる、システムのシャットダウン。

実行されるアクションのタイプ固有の情報に加え、次の情報を示すアカウンティング ログも示されます。

- アクションを認可したユーザ
- アクションが実行された時刻
- アカウンティング レコードがサーバに送信された時刻

（注） スタートアップ コンフィギュレーションのシステム電源投入時の再実行中には、アカウント ロギングは実行されません。システムの起動時には、startup-config コマンドは記録されません。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA アカウンティング サーバの設定」の目次ページに戻る
- 次の項目：「AAA アカウンティング サーバとイベント ロギングの設定」

AAA アカウンティング サーバとイベント ロギングの設定

この手順を使用して、アカウンティング サーバへのログインに使用される情報を設定します。

手順

ステップ 1 [Configure] > [AAA] > [Accounting] を選択します。

[Configure AAA Accounting] ページが表示されます。

ステップ 2 適切なフィールドに、次の情報を入力します。

- アカウンティングがイネーブルか
- ログイン再試行の回数
- ログイン タイムアウトの長さ（秒単位）
- プライマリ サーバのサーバ IP アドレスまたは DNS 名
- プライマリ サーバに使用されるポート番号
- プライマリ サーバのパスワード
- セカンダリ サーバのサーバ IP アドレスまたは DNS 名
- セカンダリ サーバに使用されるポート番号
- セカンダリ サーバのパスワード

ステップ 3 ログに含めるログ イベントを選択し、含めないイベントの選択を解除します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [OK] をクリックして、変更を保存します。

関連項目

- 「認証、認可、アカウンティングの設定」の目次ページに戻る
- 「AAA アカウンティング サーバの設定」の目次ページに戻る

システム情報の表示

Cisco Unified SIP Proxy のライセンス情報を参照するには、[System] > [System Information] を選択します。

[System Information] ページが表示され、次の情報が示されます。

パラメータ	説明
Module SKU	Cisco Unified SIP Proxy モジュールの一意識別名です。
Module Serial Number	Cisco Unified SIP Proxy モジュールのシリアル番号です。
Chassis Type	Cisco Unified SIP Proxy モジュールのシャーシのタイプです。
Chassis Serial Number	シャーシのシリアル番号です。
Software Version	このシステムで実行中の Cisco Unified SIP Proxy ソフトウェアのバージョンです。
Uptime	Cisco Unified SIP Proxy システムが実行されている時間の長さです。

ドメイン ネーム設定の設定

[System Domain Name Settings] ページで次の作業を実行します。

- Cisco Unified SIP Proxy があるドメインとホスト名を指定します。「DNS サーバの変更」を参照してください。
- Domain Name Settings（DNS）サーバを追加します。「DNS サーバの追加」を参照してください。
- DNS サーバを削除します。「DNS サーバの削除」を参照してください。

DNS サーバの変更

DNS サーバの名前または IP アドレスが変更になった場合に DNS サーバを変更するには、次の手順を使用します。

始める前に

次の情報を用意します。

- Cisco Unified SIP Proxy システムのホスト名。
- DNS サーバのドメイン名と IP アドレス。

手順

ステップ 1 [System] > [Domain Name Settings] を選択します。

[Domain Name Settings] ページが表示されます。

ステップ 2 アプリケーション ファイルに格納された、サーバのホスト名またはドメイン名を変更します。

ステップ 3 [Apply] をクリックします。

次の作業

設定を保存し、リロードします。「Administration Control Panel の使用」を参照してください。

関連項目

「ドメイン ネーム設定の設定」の目次ページに戻る

DNS サーバの追加

システムがプライマリ ドメイン ネーム サーバにアクセスできない場合に使用される代替宛先サーバとして、追加の DNS サーバを入力します。

制約事項

最大 4 個の DNS サーバを持つことができます。

手順

ステップ 1 [System] > [Domain Name Settings] を選択します。

[Domain Name Settings] ページが表示されます。

ステップ 2 [Domain Name Service (DNS) Servers] の下にある [Add] をクリックします。

[Add a DNS server] ページが表示されます。

ステップ 3 サーバの IP アドレスを入力します。

ステップ 4 [Add] をクリックします。

次の作業

設定を保存し、リロードします。「Administration Control Panel の使用」を参照してください。

関連項目

「ドメイン ネーム設定の設定」の目次ページに戻る

DNS サーバの削除

手順

ステップ 1 [System] > [Domain Name Settings] を選択します。

[Domain Name Settings] ページが表示されます。

ステップ 2 削除する DNS サーバの隣のチェックボックスをオンにします。

ステップ 3 [Delete] をクリックします。

ステップ 4 プロンプトで [OK] をクリックします。

次の作業

設定を保存し、リロードします。「Administration Control Panel の使用」を参照してください。

関連項目

「ドメイン ネーム設定の設定」の目次ページに戻る

ネットワーク時刻および時間帯の設定

ボイスメールおよびシステムプロセスが関連する正しい日付と時刻を取得できるようにするために、NTP サーバを Cisco Unified SIP Proxy システムに追加し、時間帯を設定する必要があります。

- 「NTP サーバの追加」
- 「RemovingNTP サーバの削除」
- 「優先サーバとしての NTP サーバの設定」
- 「時間帯の変更」

NTP サーバの追加

制約事項

最大 3 個の NTP サーバを持つことができます。

手順

ステップ 1 [System] > [Network Time & Time Zone Settings] を選択します。

[Network Time & Time Zone Settings] ページが表示されます。

ステップ 2 [Add] をクリックします。

[Add a NTP Server] ページが表示されます。

ステップ 3 NTP サーバのホスト名または IP アドレスを入力します。プライマリ NTP サーバにするには、[Preferred] チェックボックスをオンにします。

ステップ 4 [Add] をクリックします。

[Network Time and Time Zone Settings] の表に新しいサーバが表示されます。

次の作業

設定を保存し、リロードします。「Administration Control Panel の使用」を参照してください。

関連項目

「ネットワーク時刻および時間帯の設定」の目次ページに戻る

RemovingNTP サーバの削除

手順

ステップ 1 [System] > [Network Time & Time Zone Settings] を選択します。
[Network Time & Time Zone Settings] ページが表示されます。

ステップ 2 削除する NTP サーバの隣のチェックボックスをオンにし、[Delete] をクリックします。

ステップ 3 プロンプトで [OK] をクリックします。

次の作業

設定を保存し、リロードします。「Administration Control Panel の使用」を参照してください。

関連項目

「ネットワーク時刻および時間帯の設定」の目次ページに戻る

優先サーバとしての NTP サーバの設定

制約事項

少なくとも 2 個の NTP サーバが必要です。

手順

ステップ 1 [System] > [Network Time & Time Zone Settings] を選択します。
[Network Time & Time Zone Settings] ページが表示されます。

ステップ 2 優先サーバとして設定する NTP サーバの隣のチェックボックスをオンにし、[Preferred] をクリックします。

ステップ 3 [OK] をクリックします。

次の作業

設定を保存し、リロードします。「Administration Control Panel の使用」を参照してください。

関連項目

「ネットワーク時刻および時間帯の設定」の目次ページに戻る

時間帯の変更

手順

ステップ 1 [System] > [Network Time & Time Zone Settings] を選択します。
[Network Time & Time Zone Settings] ページが表示されます。

ステップ 2 ドロップダウン メニューを使用して、正しい国を選択します。

ステップ 3 ドロップダウン メニューを使用して、正しい時間帯を選択します。

ステップ 4 [Apply] をクリックします。

ステップ 5 情報プロンプトで [OK] をクリックします。

次の作業

設定を保存し、リロードします。「Administration Control Panel の使用」を参照してください。

関連項目

「ネットワーク時刻および時間帯の設定」の目次ページに戻る

システム ログイン バナーの設定

ユーザが CLI にログインしたときに表示されるログイン バナーのテキストを変更するには、次の手順を使用します。

手順

ステップ 1 [System] > [Login Banner] を選択します。

[Login Banner] ページが表示されます。

ステップ 2 ログイン バナーのテキストを入力します。

ステップ 3 [Apply] をクリックして設定を保存します。

Cisco Unified SIP Proxy システムのモニタリング

1 秒当たりのコール数のモニタリング

システムが処理する Calls Per Second（CPS; 1 秒当たりのコール）数は、システムのキャパシティを判断する 1 つの方法です。キャパシティは、ネットワークが処理するように設計されたトラフィック量の測定方法です。ボイス ネットワークは一般に、ターゲット ピークロード キャパシティを処理するように設計されており、一般に CPS で測定されます。

ライセンシングのために CPS 数をモニタリングする必要があります。CPS 数を超える、つまりライセンスの数を超えると、システムはコールをドロップします。トラフィック パターンを決定するために、CPS をモニタリングする必要があることがあります。

システムには、CPS 数および次の情報を表示する 2 つのグラフが用意されています。

- 最近 1 時間の受信 CPS 数
- 最近 72 時間の受信 CPS 数

手順

ステップ 1 [Monitor] > [Calls-Per-Second] をクリックします。

2 組のグラフが含まれるページが表示されます。1 組のグラフは、最近 1 時間の受信 CPS 数を表示し、もう 1 組は、最近 72 時間の受信 CPS 数を表示します。

ヒント 2 組のグラフが表示されない場合は、下へスクロールします。

ステップ 2 1 秒当たりのコール（最近 60 分）のデータの右上にある、[Series Selector] をクリックし、次のうちから表示するデータを選択します。

- [5-minute CPS]
- [Incoming CPS]
- [License Limit CPS]

ステップ 3 選択後に [Series Selector] をもう一度クリックして、データを表示します。

要求したデータが 2 つのグラフに表示されます。上のグラフでは、縦方向の目盛りで CPS が表示され、横方向の目盛りで最新 1 時間が表示されます。

下のグラフでは、縦方向の目盛りで実際のコール数が表示され、横方向の目盛りで最新 1 時間が表示されます。

ステップ 4 1 秒当たりのコール（最近 72 時間）のデータの右上にある、[Series Selector] をクリックし、次のうちから表示するデータを選択します。

- [Incoming Peak]
- [Incoming Average]
- [5-Minute Peak]
- [5-Minute Average]
- [License Limit CPS]

ステップ 5 選択後に [Series Selector] をもう一度クリックして、データを表示します。

要求したデータが 2 つのグラフに表示されます。上のグラフでは、縦方向の目盛りで CPS が表示され、横方向の目盛りで最新 72 時間が表示されます。

下のグラフでは、縦方向の目盛りで実際のコール数が表示され、横方向の目盛りで最新 72 時間が表示されます。

ステップ 6 4 つのグラフの任意の時点に関する詳細情報を表示するには、データの線上にマウス ポインタを乗せます。情報を表示するポップアップ ボックスが 1 つまたは複数表示されます。表示される情報は、[Series Selector] メニューでチェックしたデータによって異なります。

たとえば、下のグラフの緑色の「ルーティング」ライン上にマウス ポインタを合わせると、マウス ポインタを合わせている時点の正確な日付と時刻、さらに、その瞬間のルーティングされたコール数とドロップされたコール数を示すボックスが表示されます。

関連項目

- 「ライセンス情報の表示」
- 「Cisco Unified SIP Proxy システムのモニタリング」の目次ページに戻る

サーバ グループ ステータスのモニタリング

サーバ グループと要素のステータスをモニタし、動作を停止していないことを確認します。

ヒント サーバ グループまたは要素がダウンしている場合、サーバ グループまたはエレメントがアップ状態に戻ったときにプロキシが認識できるように SIP ping が設定されていることを確認します。

手順

ステップ 1 [Monitor] > [Server Group Status] を選択します。

次の情報を含む [Server Group Element Status] ページが表示されます。

フィールド	説明
[Server Group/Element]	SIP サーバ グループの名前を表示します。
[Status]	SIP サーバ グループの動作ステータスを表示します。
[Q-Value]	サーバ グループ内の他の要素に対する、サーバ グループ要素のプライオリティを指定する実数を表示します。 **（注）** サーバ グループに複数の要素があり、すべての要素が見られるように表示が展開されない場合、これらの値は空白になります。
[Weight]	重み付けに基づくルーティングを実装する場合に、ルート グループの request-URI または route-URI 要素に割り当てられる割合を表示します。 **（注）** サーバ グループに複数の要素があり、すべての要素が見られるように表示が展開されない場合、これらの値は空白になります。

ステップ 2 一覧を展開するには、[Expand All] をクリックします。一覧を折りたたむには、[Collapse All] をクリックします。

関連項目

「Cisco Unified SIP Proxy システムのモニタリング」の目次ページに戻る

システム リソースのモニタリング：CPU

このグラフには、システムが使用している CPU リソースの割合が表示されます。この情報は、システムの問題の診断および予防に役立ちます。一般に、CPU は、システム リソースの 80 % を超えて使用してはなりません。

ヒント システムの使用する CPU が多すぎる場合、トレース ログを小さくするか、オフにする（「トレース設定の指定」を参照）、または、CLI を開始して、SIP メッセージ ログまたはペグ カウント ログを小さくするか、オフにします。

制約事項

グラフを表示するには、Adobe Flash Player Release 9 以降がインストールされている必要があります。

手順

ステップ 1 [Monitor] > [System Resources] > [CPU] を選択します。

[System Resource Utilizations] ページに、次の項目を示す 3 つのグラフが表示されます。

- 過去 60 秒の CPU 使用（1 秒当たりの割合）
- 過去 60 分の CPU 使用（1 分当たりの割合）
- 過去 72 時間の CPU 使用（1 時間当たりの割合）

ヒント グラフがすべて表示されない場合は、下へスクロールします。

それぞれのグラフには、縦方向の目盛りで CPU 使用割合が表示され、横方向の目盛りで時間が表示されます。

2 番目および 3 番目のグラフでは、平均 CPU 使用も表示されます。

関連項目

「Cisco Unified SIP Proxy システムのモニタリング」の目次ページに戻る

システム リソースのモニタリング：メモリ

このグラフには、システムが使用しているメモリの量が表示されます。

制約事項

グラフを表示するには、Adobe Flash Player Release 9 以降がインストールされている必要があります。

手順

ステップ 1 [Monitor] > [System Resources] > [Memory] を選択します。

[System Memory Utilizations] ページに、次の項目を示す 3 つのグラフが表示されます。

- 過去 60 秒のメモリ使用
- 過去 60 分のメモリ使用
- 過去 72 時間のメモリ使用

ヒント グラフがすべて表示されない場合は、下へスクロールします。

それぞれのグラフには、縦方向の目盛りでメモリ使用量（KB 単位）が表示され、横方向の目盛りで時間が表示されます。

関連項目

「Cisco Unified SIP Proxy システムのモニタリング」の目次ページに戻る

レポートの表示

バックアップ履歴レポートの表示

手順

ステップ 1 [Reports] > [Backup History] を選択します。

レポートするバックアップ履歴がある場合、バックアップ履歴レポートには次のフィールドが含まれます。

- [ID]：バックアップの ID です。
- [Server URL]：バックアップ履歴が格納されているサーバです。
- [Backup Time and Date]：システムが最後にバックアップされた日付と時刻です。
- [Version]：インストールされている Cisco Unified SIP Proxy ソフトウェアのバージョンです。
- [Description]：バックアップの説明です。
- [Result]：最終バックアップ手順のステータスです。[Result] は成功（Success）または失敗（Fail）を示します。

ステップ 2 異なる数のバックアップレポートを各ページに表示するには、右上にあるドロップダウン ボックスで別の数を選択し、[Go] をクリックします。10、25、50、100、またはすべてのバックアップ レポートの表示が選択できます。

ステップ 3 他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 4 バックアップ レポートを並べ替えるには、該当するヘッダーをクリックします。

関連項目

「レポートの表示」の目次ページに戻る

復元履歴レポートの表示

手順

ステップ 1 [Reports] > [Restore History] を選択します。

レポートする復元履歴がある場合、復元履歴レポートには次のフィールドが含まれます。

- [ID]：復元の ID です。
- [Server URL]：復元履歴が格納されているサーバです。
- [Restore Time and Date]：システムが最後にバックアップされた日付と時刻です。
- [Version]：インストールされている Cisco Unified SIP Proxy ソフトウェアのバージョンです。
- [Result]：最終復元手順のステータスです。[Result] は、復元されたコンポーネントの成功（Success）または失敗（Fail）を示します。

ステップ 2 異なる数の復元レポートを各ページに表示するには、右上にあるドロップダウン ボックスで別の数を選択し、[Go] をクリックします。10、25、50、100、またはすべての復元レポートの表示が選択できます。

ステップ 3 他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 4 復元レポートを並べ替えるには、該当するヘッダーをクリックします。

関連項目

「レポートの表示」の目次ページに戻る

ネットワーク タイム プロトコル レポートの表示

手順

ステップ 1 [Reports] > [Network Time Protocol] を選択します。

レポートには次のフィールドが表示されます。

- [#] : NTP サーバの優先番号です。システムは、システムの時間の同期を NTP サーバ番号 1 から試みます。
- [NTP Server] : NTP サーバの IP アドレスまたはホスト名です。
- [Status] : NTP サーバが Cisco Unified SIP Proxy と接続されたか、または拒絶されたかを示します。
- [Time Difference (secs)] : NTP サーバとクライアントとの間のタイム オフセットです。
- [Time Jitter (secs)] : RMS の時差の移動平均として測定される、システム クロックの推定誤差時間です。

関連項目

「レポートの表示」の目次ページに戻る

バックアップと復元の設定

バックアップ サーバの設定

バックアップ処理を開始する前に、バックアップ設定パラメータを設定します。

始める前に

次の値を集めます。

表 29　　バックアップ設定パラメータ

パラメータ	説明
Server URL	バックアップ ファイルが保存されているネットワーク上のサーバの URL。 形式は ftp://<*server/directory*>/ で、<*server/directory*> は、バックアップ サーバの IP アドレスまたはホスト名です。
User ID	バックアップ サーバのユーザ ID。 データをバックアップするサーバ上には、ユーザのアカウントが必要です。匿名のユーザ ID は使用しないでください。
Password	バックアップ サーバのユーザ ID のパスワード。
Maximum revisions	バックアップ サーバに保存するバックアップ データのリビジョンの最大番号。 最大番号は 50 です。デフォルト値は 5 です。

手順

ステップ 1　[Administration] > [Backup / Restore] > [Configuration] を選択します。

[Backup / Restore Configuration] ページが表示されます。

ステップ 2　表 29 に示された情報を入力します。

ステップ 3 [Apply] をクリックして、情報を保存します。

関連項目

「バックアップと復元の設定」の目次ページに戻る

スケジュール バックアップの参照

手順

ステップ 1 [Administration] > [Backup / Restore] > [Scheduled Backups] を選択します。

次の情報が示された [Backup / Restore Configuration] ページが表示されます。

- 名前
- 説明
- スケジュール
- 次の実行
- 保存するバックアップのカテゴリまたはデータのタイプ

ステップ 2 各ページで異なる数のスケジュール バックアップを参照するには、右上のドロップダウン ボックスから別の数を選択し、[Go] をクリックします。10、25、50、100、またはすべてのスケジュール バックアップを参照するよう、選択できます。

ステップ 3 他のページに移動するには、右下にある左右矢印ボタンを使用するか、または他のページ番号を入力して Enter を押します。

ステップ 4 スケジュール バックアップを並べ替えるには、任意の見出しをクリックします。

関連項目

「バックアップと復元の設定」の目次ページに戻る

スケジュール バックアップの追加

ジョブを一度または次の頻度で繰り返すよう、スケジュール バックアップを設定できます。

- N 日ごとの特定の時刻
- N 週ごとの特定の日付と時刻
- N か月ごとの月の特定の日付と時刻
- N 年ごとの特定の日付と時刻

始める前に

- データのバックアップに使用されるサーバを設定します。「バックアップ サーバの設定」を参照してください。
- システム設定を保存します。「システム設定の管理」を参照してください。

手順

ステップ 1 [Administration] > [Backup / Restore] > [Scheduled Backups] を選択します。

[Backup / Restore Scheduled Backup] ページが表示されます。

ステップ 2 [Schedule Backup] をクリックします。

[Backup / Restore Scheduled Backups] ページが表示されます。

ステップ 3 スケジュール バックアップの名前と説明を入力します。

ステップ 4 保存するデータのタイプのチェックボックスをオンにします。次のいずれか一方または両方を選択できます。

- [Configuration]：システムとアプリケーションの設定を保存します。
- [Data]：アプリケーション データと音声メッセージを保存します。

ステップ 5 [Schedule] タブから、スケジュール バックアップの頻度を選択します。

- [Once]
- [Daily]
- [Weekly]
- [Monthly]
- [Yearly]

ステップ 6 スケジュール バックアップを開始するかどうかを選択します。

- [Immediately]
- 特定の日付または時刻

ステップ 7 [Add] をクリックします。

関連項目

「バックアップと復元の設定」の目次ページに戻る

手動でのバックアップの開始

始める前に

- データのバックアップに使用されるサーバを設定します。「バックアップ サーバの設定」を参照してください。
- 設定を保存します。「システム設定の管理」を参照してください。

手順

ステップ 1 [Administration] > [Backup / Restore] > [Start Backup] をクリックします。

[Backup / Restore Start Backup] ページが表示され、バックアップ ID が自動的に生成されます。サーバをバックアップするたびに、バックアップ ID が 1 増加します。

ステップ 2 たとえば「backupdata6-2-04」などの、バックアップ ファイルの説明を入力します。

ステップ 3 保存するデータのタイプのチェックボックスをオンにします。次のいずれか一方または両方を選択できます。

- [Configuration]：システムとアプリケーションの設定を保存します。
- [Data]：アプリケーション データと音声メッセージを保存します。

ステップ 4 [Start Backup] をクリックします。

ステップ 5 確認メッセージで、[OK] をクリックします。

関連項目

「バックアップと復元の設定」の目次ページに戻る

復元の開始

設定データのバックアップ後は、新たなインストールまたはアップグレードごとに復元できます。

始める前に

バックアップ サーバを設定します。「バックアップ サーバの設定」を参照してください。

手順

ステップ 1 [Administration] > [Backup / Restore] > [Start Restore] を選択します。

次のフィールドが示された [Backup / Restore Start Restore] ページが表示されます。

- [Backup ID]：前のバックアップのバックアップ ID。
- [Version]：バージョン。
- [Description]：このバックアップの名前。
- [Backup Time and Date]：このバックアップが行われた日付と時刻。
- [Categories]：復元するデータのタイプ。

ステップ 2 復元する設定が含まれる行を選択します。

ステップ 3 保存するデータのタイプのチェックボックスをオンにします。次のいずれか一方または両方を選択できます。

- [Configuration]：システムとアプリケーションの設定を保存します。
- [Data]：アプリケーション データと音声メッセージを保存します。

ステップ 4 [Start Restore] をクリックします。

関連項目

「バックアップと復元の設定」の目次ページに戻る

Administration Control Panel の使用

Cisco Unified SIP Proxy モジュールのリロードおよび、Lite モードのイネーブル化とディセーブル化

制約事項

- モジュールのリロードによって、すべてのユーザ セッションが終了され、すべての未保存のデータが失われます。
- Lite モードをイネーブルにすると、レコードルート コンフィギュレーションが削除され、[SIP Record-Route] タブにアクセスできなくなります。[SIP Record-Route] タブの詳細については、「ネットワークの SIP レコードルートの編集」を参照してください。

手順

ステップ 1 [Administration] > [Control Panel] を選択します。

[Control Panel] ページが表示されます。

ステップ 2 次のいずれかを実行します。

- モジュールをリロードするには、[Reload Module] をクリックします。ダイアログボックスが表示され、システムのリロードによって、すべてのエンドユーザ セッションが終了され、すべての未保存のデータが失われることが警告されます。
- Lite モードをイネーブルにするには、[enable (0 CPS)] を選択します。ダイアログボックスが表示され、Lite モードをイネーブルにするとレコード ルーティングがディセーブルになることが警告されます。
- Lite モードをディセーブルにするには、[disable (0 CPS)] を選択します。ダイアログボックスが表示され、Lite モードをディセーブルにすると、ライセンスされた制限にパフォーマンスがリセットされることが警告されます。

ステップ 3 プロンプトで [OK] をクリックします。

ステップ 4 [OK] をクリックします。

ライセンス情報の表示

Cisco Unified SIP Proxy のライセンス情報を表示するには、[Administration] > [Licenses] を選択します。[Administration Licenses] ページに次の情報が表示されます。

パラメータ	説明
モジュール情報	
Product ID	Cisco Unified SIP Proxy モジュールの一意識別名です。
Serial Number	Cisco Unified SIP Proxy モジュールのシリアル番号です。
ライセンス情報	
Feature	ライセンスを取得した機能の名前です。
Description	ライセンスの説明です。
Type	ライセンスのタイプです。Permanent（恒久）または Evaluation（評価）のいずれかです。
State	アクティブかどうか、使用中か、使用中でないか、EULA が同意されなかったかなどの、このライセンスの状態です。
Priority	このライセンスの優先順位です。Low（低い）、Medium（中程度）、または High（高い）です。
Usage	コール数です。
Validity Left	このライセンスに残された時間です。

システム設定の管理

システム デフォルトの復元

手順

ステップ 1 [Administration] > [Manage Configuration] > [Restore Defaults / Rollback] を選択します。

[Manage Configuration] ページが表示されます。

ステップ 2 コンフィギュレーションを保存またはコミットする（このコンフィギュレーションを新しいスタートアップ コンフィギュレーションにする）には、次の作業を行います。

a. [Save/Commit Configuration] をクリックします。

b. 確認ウィンドウで、[OK] をクリックします。

ステップ 3 工場出荷時の状態にコンフィギュレーションを復元するには、次の手順を実行します。これは、実施した変更がすべて失われ、モジュールがリロードされることを意味します。

a. [Restore Factory Defaults] をクリックします。

b. 確認ウィンドウで、[OK] をクリックします。

ステップ 4 最新のコンフィギュレーションにシステムをロールバックするには次の手順を実行します。これは現在のコンフィギュレーションを置き換え、モジュールをリロードします。

a. [Rollback Active Configuration] をクリックします。

b. 確認ウィンドウで、[OK] をクリックします。

関連項目

「システム設定の管理」の目次ページに戻る

候補コンフィギュレーションのプレビュー

候補コンフィギュレーションのコードが表示されます。

（注） まったく変更がなければ、そのことを示すメッセージが表示されます。

手順

ステップ 1 [Administration] > [Manage Configuration] > [Candidate Preview] を選択します。

[Candidate Configuration Preview] ページが表示されます。

ステップ 2 コンフィギュレーションを保存またはコミットする（このコンフィギュレーションを新しいスタートアップ コンフィギュレーションにする）には、次の作業を行います。

a. [Save/Commit Configuration] をクリックします。

b. 確認ウィンドウで、[OK] をクリックします。

ステップ 3 候補コンフィギュレーションのシステムをクリアする（コミットされていないすべての変更が破棄される）には、次の作業を実行します。

a. [Clear Candidate Configuration] をクリックします。

b. 確認ウィンドウで、[OK] をクリックします。

関連項目

「システム設定の管理」の目次ページに戻る

トラブルシューティング

CUSP トレースのイネーブル化

手順

ステップ 1 [Troubleshoot] > [CUSP Traces] を選択します。

[CUSP Tracing] ページが表示されます。

ステップ 2 システム上でトレースをイネーブルにするには、[Enable Tracing] チェックボックスをオンにします。

ステップ 3 次の要素について、トレース コンポーネントを設定します。

- Base Tracing
- Routing
- Proxy-Core
- SIP-Wire-Log
- Normalization
- Proxy-Transactions
- SIP-Ping
- License-Mgmt
- Trigger-Conditions
- Accounting
- SIP-Search
- Config-Mgmt

各コンポーネントについて、次のレベルの 1 つを選択できます。

レベル	説明
default	親のトレース レベルを使用します。
debug	重大度がデバッグまたはそれ以上のメッセージをログに記録します。
info	重大度が情報またはそれ以上のメッセージをログに記録します。
warn	重大度が警告またはそれ以上のメッセージをログに記録します。
error	重大度がエラーまたはそれ以上のメッセージをログに記録します。
fatal	重大度が重大またはそれ以上のメッセージをログに記録します。
off	メッセージをログに記録しません。

ステップ 4 [Update] をクリックして、変更を保存します。

関連項目

「トラブルシューティング」の目次ページに戻る

CUSP トレース ログ ファイルの参照

手順

ステップ 1 [Troubleshoot] > [View CUSP Trace Log File] を選択します。

[CUSP Trace Log File] ページが表示され、CUSP トレース ログ ファイルの内容が示されます。

ステップ 2 別のページに移動するには、右矢印ボタンおよび左矢印ボタンを使用するか、または、別のページ番号を入力して Enter を押します。

ステップ 3 トレース ログ ファイルの情報を保存するには、次の操作を実行します。

a. [Download CUSP Trace Log File] をクリックします。

b. 適切な場所にファイルを保存します。

c. 終了したら、[Close] をクリックします。

関連項目

「トラブルシューティング」の目次ページに戻る

トレース設定の指定

次の手順を使用して、Cisco Unified SIP Proxy システムのコンポーネントで、トレースをイネーブルにするか、メッセージ出力をデバッグします。コンポーネントは、システムにあるモジュール、エンティティ、およびアクティビティです。[Troubleshoot] > [View] > [Trace Buffer] を選択すると、出力を確認することができます。「トレース バッファの参照」を参照してください。

制約事項

イネーブルにするトレースが多すぎると、システムのパフォーマンスに悪影響を及ぼす可能性があります。

手順

ステップ 1 [Troubleshoot] > [Traces] を選択します。

システム コンポーネントの階層の一覧が示された、[Traces] ページが表示されます。

ステップ 2 システム コンポーネントでトレースをイネーブルにするには、コンポーネントの名前の横にあるチェックボックスをオンにします。

- コンポーネントの一覧を展開するには、任意の上位レベル コンポーネントの横にある [+] 記号をクリックします。コンポーネントの一覧を折りたたむには、任意の上位レベル コンポーネントの横にある [-] 記号をクリックします。
- 任意の上位レベルのコンポーネントの横にあるチェックボックスをオンにすると、そのコンポーネントの下にあるすべてのコンポーネントのトレースがイネーブルになります。任意の上位レベルのコンポーネントの横にあるチェックボックスをオフにすると、そのコンポーネントの下にあるすべてのコンポーネントのトレースがディセーブルになります。

ステップ 3 [Apply] をクリックして、変更を保存します。

ステップ 4 確認ウィンドウで、[OK] をクリックします。

関連項目

「トラブルシューティング」の目次ページに戻る

技術サポート情報の参照

手順

ステップ 1 [Troubleshoot] > [View] > [Tech Support] を選択します。

[Tech Support] ページが表示され、設定データの集まりが示されます。

ステップ 2 技術サポート情報を保存するには、[Download Tech Support] をクリックします。

ステップ 3 適切な場所にファイルを保存します。

ステップ 4 終了したら、[Close] をクリックします。

関連項目

「トラブルシューティング」の目次ページに戻る

トレース バッファの参照

手順

ステップ 1 [Troubleshoot] > [View] > [Trace Buffer] を選択します。

[Trace Buffer] ページが表示され、トレース バッファの内容が示されます。

ステップ 2 別のページに移動するには、右矢印ボタンおよび左矢印ボタンを使用するか、または、別のページ番号を入力して Enter を押します。

ステップ 3 トレース バッファの情報を保存するには、次の操作を実行します。

a. [Download Trace Buffer] をクリックします。

b. 適切な場所にファイルを保存します。

c. 終了したら、[Close] をクリックします。

ステップ 4 トレース バッファをクリアするには、次の操作を実行します。

a. [Clear Trace Buffer] をクリックします。

b. 確認プロンプトで、[OK] をクリックします。

関連項目

「トラブルシューティング」の目次ページに戻る

ログ ファイルの参照

手順

ステップ 1 [Troubleshoot] > [View] > [Log File] を選択します。

[Log File] ページが表示され、ログ ファイルの内容が示されます。

ステップ 2 別のページに移動するには、右矢印ボタンおよび左矢印ボタンを使用するか、または、別のページ番号を入力して Enter を押します。

ステップ 3 ログ ファイルを保存するには、次の操作を実行します。

a. [Download Log File] をクリックします。

b. 適切な場所にファイルを保存します。

c. 終了したら、[Close] をクリックします。

関連項目

「トラブルシューティング」の目次ページに戻る