



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」](#)
- [「エイリアス FQDN の追加と削除」](#)
- [「信頼できるピアの追加と削除」](#)

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	<p>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。</p> <ul style="list-style-type: none"> • Call-ID • Contact • Content-Encoding • Content-Length • Content-Type • From • Subject • To • Via <p>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。</p>
SIP Message Logging	<p>すべての着信および発信 SIP メッセージのログギングをイネーブルにするかどうか。</p> <p>(注) SIP ログ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。</p>
SIP Statistics	<p>アクティブな SIP キューの統計情報を表示するかどうか。</p>
Period Time	<p>(オプション。[SIP Statistics] をオンにした場合にのみ使用可能) <code>peg-logging</code> 統計情報を収集する頻度を決定します。</p>
Reset Time	<p>(オプション。[SIP Statistics] をオンにした場合にのみ使用可能) <code>peg-logging</code> 統計情報をリセットする頻度を決定します。</p>
Max Forwards	<p>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。</p> <p>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。</p> <p>指定できる値は 0 ~ 255 です。デフォルト値は 70 です。</p> <p>(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。</p>

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。
- 名前を入力します。
 - [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。
- 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。
 - [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。
- 名前を入力します。
 - [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。
- 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。
 - [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

