Cisco TelePresence Server Media 310/320

印刷可能なオンライン ヘルプ

ソフトウェア バージョン：4.2

はじめに

このドキュメントには、Cisco TelePresence Server バージョン 4.2 の Web ユーザ インターフェイスについてのオンライン ヘルプの内容が含まれています。このドキュメントを使用して、ヘルプのすべての内容を単一のドキュメントとして表示および印刷できます。

このドキュメントは TelePresence Server ソフトウェアのバージョン 4.2 に付属しています。このソフトウェアは、次の Cisco Multiparty ハードウェア上で使用できます。

- Cisco Multiparty Media 310
- Cisco Multiparty Media 320

このドキュメントの内容は製品のユーザ インターフェイスに対応して編成されており、内容は製品のオンライン ヘルプと同じです。

各章はインターフェイスの各ページに対応しており、各章の冒頭にその章のトピック一覧を掲載しています。

その他の情報

この製品のソフトウェア ライセンスの詳細については、オンライン ヘルプを参照してください。

Web インターフェイスへのログイン

Web インターフェイスにログインしなければならないのはなぜですか。

TelePresence Server には、事前設定のすべてのアカウントが保持されています。それ以外のアカウントを使用するユーザのアクセスは拒否され、これによりユーザ アクセスが制限されます。各アカウントにはユーザ名とパスワードがあり、これを使用することでそのアカウントの所有者は自分の権限にアクセスできるようになります。

ユーザ アカウントには次の 3 つの権限レベルがあります。

- *Administrator*：この権限レベルのユーザは、すべての機能にアクセスできます。
- *API access*：この特権レベルのユーザがアクセスできるのは API だけで、Web インターフェイスにはアクセスできません。
- *None*：この権限レベルのユーザは、TelePresence Server にアクセスできません。このレベルは、アカウントを無効にするときに使用します。

タスク

Web インターフェイスへのログイン：

1. Web ブラウザのアドレス バーに、TelePresence Server のホスト名または IP アドレスを入力します。

   ログイン ページが表示されます。
2. 割り当てられた [Username] と [Password] を入力します。
3. [OK] をクリックします。

Web インターフェイスへのログインが失敗する

[Access denied] ページが表示されますが原因は何でしょうか。

ログインできないのは、次のいずれかの理由によります。

- **無効なユーザ名/パスワード**：間違ったユーザ名またはパスワードが入力されました。
- **空きセッションがない**：TelePresence Server で同時に許可される最大セッション数に到達しています。
- **IP アドレスが指定したブラウザ Cookie のものと一致しない**：Cookie を削除してから再ログインしてください。
- **そのページを表示するアクセス権がない**：そのページを表示するために必要なアクセス権がありません。
- **ページが期限切れになった**：TelePresence Server にパスワードの変更を要求したユーザとそのパスワード変更要求の送信ユーザが異なると判断された場合、[Change password] ページが期限切れになることがあります （新しいブラウザ タブを開いて要求を送信すると、この問題が発生する場合があります）。

システム ステータス

システム ステータスの表示

[Status] ページには、TelePresence Server のステータスの概要が表示されます。この情報にアクセスするには、[Status] に移動します。

注：TelePresence Server を制御するには外部アプリケーションが必要です。Cisco TelePresence Conductor などの外部アプリケーションは、TelePresence Server の API を使用して会議や参加者の作成および管理を行います。詳細については、Cisco TelePresence Server API のマニュアルを参照してください。

表示される情報の詳細については、次の表を参照してください。

表 1　システム ステータス

フィールド	フィールドの説明	使用方法のヒント
Model	TelePresence Server のモデル。	
Serial number	TelePresence Server に固有のシリアル番号。	カスタマー サポートに問い合わせる場合に、この情報を提供する必要があります。
Software version	インストールされているソフトウェアのバージョン。	
Build	インストールされているソフトウェアのビルド情報。	
Uptime	TelePresence Server を最後に再起動してからの経過時間。	
Host name	TelePresence Server に割り当てられているホスト名。	
IP address	TelePresence Server に割り当てられている IP アドレス。	
IPv6 address	TelePresence Server の IPv6 アドレス。	
License mode	TelePresence Server が Screen Licensed モード（デフォルト）と Multiparty Licensed モードのどちらで動作しているかを示します。	Multiparty Licensed モードを使用するには、TelePresence Server がリモート管理モードで動作しており、アクティブなコールが存在せず、Multiparty Licensed モードが有効な TelePresence Conductor に接続されている必要があります。

表 2　機能キー

フィールド	フィールドの説明	使用方法のヒント
Media 310 activation または Media 320 activation	ユニットが有効になっているかどうか。	TelePresence Server は、有効にしないと動作しません。この機能キーは出荷前にインストールされます。
Media encryption	メディア暗号化機能が有効になっているかどうか。	*メディア暗号化*機能キーにより、その TelePresence Server 上の会議が暗号化されます。機能キーは、[Configuration] > [Upgrade] ページでインストールします。「TelePresence Server のバックアップとアップグレード」を参照してください。
Screen licenses	TelePresence Server に割り当てられているスクリーン ライセンスの数。クラスタの場合、クラスタ全体に割り当てられたスクリーン ライセンスの数になります。 割り当てられるスクリーン ライセンスの数は、システムでサポート可能な最大数より少ない場合があります。	スクリーン ライセンスを有効にするには、スクリーン ライセンス キーをインストールする必要があります。ライセンスの詳細については、「TelePresence Server の会議容量について」（76 ページ）を参照してください。

表 3　会議ステータス

フィールド	フィールドの説明	使用方法のヒント
Active conferences	TelePresence Server でアクティブな会議の数。	会議がアクティブになるのは、参加者がいる場合です。
Active participants	TelePresence Server で現在会議をしている参加者（すべてのタイプ）の数。	
Previous participants	会議に参加していた参加者の数（TelePresence Server が最後に再起動して以降）。	

表 4　システム ログ

フィールド	フィールドの説明	使用方法のヒント
	システム ログには、シャットダウンおよびアップグレードの最新のイベントが表示されます。最後に行われたものが最初に表示されます。	

表 5　診断情報

フィールド	フィールドの説明	使用方法のヒント
Diagnostic information	診断ファイルは、テキスト ドキュメントを含んだ **.zip** アーカイブ形式で提供されます。診断ファイルをダウンロードするには、[Download file] をクリックします。	診断情報は、TelePresence Server で発生した問題のトラブルシューティングを支援するために提供されます。 TelePresence Server で問題が発生した場合は、このファイルを Cisco Technical Assistance Center（TAC）に提出してください。必要に応じて診断テストが実施されます。
Network capture file	ネットワーク キャプチャをダウンロードするには、[Download file] をクリックします。	また、[Delete network capture] リンクも表示されます。このリンクは、TelePresence Server が再び正常に動作するようになってからクリックしてください。
System logs	ログ ファイルをダウンロードするには、[Download file] をクリックします。	アーカイブには有用なログ ファイルが複数含まれています。

ハードウェア ヘルス ステータスの表示

[Health status] ページ（[Status] > [Health status]）には、TelePresence Server のハードウェア コンポーネントに関する情報が表示されます。

注：[Worst status seen] には、TelePresence Server の最後の再起動以降の情報が表示されます。

これらの値をリセットするには、[Clear] をクリックします。表示される情報の意味については、次の表を参照してください。

表 6　デバイス ヘルスの詳細

フィールド	フィールドの説明	使用方法のヒント
Fans **Voltages** **RTC battery**	以下のいずれかの状態が表示されます。 • OK • Out of spec [Current status] と [Worst status seen] の両方の状態が表示されます。	これらの状態の意味は次のとおりです。 • *OK*：コンポーネントが正常に機能しています。 • *Out of spec*：サポート プロバイダーに確認してください。コンポーネントを修理しなければならない場合があります。 [Worst status seen] 列に [Out of spec] と表示されていても [Current status] が [OK] の場合は、ステータスを定期的にモニタしてそれが一時的な状態かどうかを確認してください。
Temperature	以下のいずれかの状態が表示されます。 • OK • Out of spec • Critical [Current status] と [Worst status seen] の両方の状態が表示されます。	これらの状態の意味は次のとおりです。 • *OK*：TelePresence Server の温度が適切な範囲内に収まっています。 • *Out of spec*：周囲温度が 34 °C 以上になっていないかどうか、および通気口が塞がれていないかどうかを確認してください。 • *Critical*：TelePresence Server の温度が高すぎます。状態が変わらない場合にシステムが 60 秒でシャットダウンすることを示すエラーもイベント ログに記録されます。 [Worst status seen] 列に [Out of spec] と表示されていても [Current status] が [OK] の場合は、ステータスを定期的にモニタしてそれが一時的な状態かどうかを確認してください。

マスター TelePresence Server 上のクラスタ ステータスの表示

クラスタ ステータスを表示するには、[Status] > [Cluster] に移動します。

ここに表示されるのは、クラスタを構成する Media 310/320 ユニットのクラスタ ステータスのみです。クラスタリングの詳細については、「クラスタリングについて」を参照してください。

次の表は、[Status] > [Cluster] ページに表示される、クラスタ内のマスター TelePresence Server に関する情報を示しています。スレーブ ブレードの詳細については、「スレーブ TelePresence Server 上のクラスタ ステータスの表示」（9 ページ）を参照してください。

表 7　クラスタ ステータス

フィールド	フィールドの説明	使用方法のヒント
IP	スレーブの IP アドレス。または、マスターの場合は [Master] 。	IP アドレスをクリックすると、スレーブのクラスタ ページに移動します。 [Master] をクリックすると、 マスター上のクラスタ設定ページに移動します。
Status	マスターのステータスは、[OK] にしかなりません。これはマスターがクラスタ内で正常に動作していることを示します。 スレーブでは、以下のいずれかのステータスが表示されます。 • *OK*：マスターとスレーブが正常に通信しています。 • *OK (last seen <number> seconds ago)*：マスターがスレーブとの接続を失いました。スレーブは自動的に再起動して、クラスタに再参加します。数分待ってから、[Status] > [Cluster] ページを更新してください。 • *Still starting up*：スレーブが起動中です。数分待ってから、[Status] > [Cluster] ページを更新してください。 • *Lost contact <number> secs ago*：マスターがスレーブとの接続を失いました。スレーブは自動的に再起動して、クラスタに再参加します。数分待ってから、[Status] > [Cluster] ページを更新してください。 • *Failed, version mismatch*：クラスタ内のすべての TelePresence Server が同じソフトウェアのバージョンを実行している必要があります。このステータス メッセージは、このスレーブがマスターとは異なるソフトウェアを実行していること、つまりこの Telepresence Server がクラスタに属していないことを示します。ソフトウェアを更新して、クラスタ内のすべてのユニットのソフトウェアが同じバージョンになるようにしてください。 • *Clustered unit not configured as slave*：スレーブにすべきユニットがスレーブとして明示的に設定されていません。この問題は、スレーブ アプライアンスを置き換えた後、新しいアプライアンスがまだ*スレーブ*として設定されていない場合に発生する可能性があります。	スレーブのステータスが [OK] の場合は、クラスタ内で正しく機能していることを示します。それ以外のステータスの場合、そのスレーブはクラスタの一部として機能していません。 1 台のスレーブがクラスタ内で正しく動作していなくても、クラスタはそのスレーブなしで動作を継続できます。 スレーブで障害が発生しても、会議の参加者の接続が解除されることはありません。クラスタ内に十分なリソースがあれば、クラスタは音声とビデオの受信を継続します。最悪の場合は、参加者にビデオが表示されなくなることがあります。音声はすべてマスターによって処理されるので、音声が中断されることはありません。 マスターとスレーブ間の接続が失われると、スレーブが自動的に再起動します。これにより、スレーブはクラスタに再参加できます。

フィールド	フィールドの説明	使用方法のヒント
	• *Clustered unit of incorrect type*：スレーブがマスターと互換性がありません。この問題は、MCU 5300 シリーズ アプライアンスがスタッキング ケーブルで接続されている場合に、そのケーブルで接続されている反対側のアプライアンスで TelePresence Server ソフトウェアが実行されており、なおかつそれが マスターとして設定されていると発生します。	
Software version	クラスタ内の各 TelePresence Server 上のソフトウェア バージョン。	
Media processing load	クラスタ内の各 TelePresence Server の現在のメディア負荷の概要。会議の使用がピークになる時間帯は負荷が増加する可能性があります。	会議はクラスタ内の TelePresence Server 間で分散されます。各サーバの負荷は、サーバ上で実行されている会議の数とサイズによって異なります。
Screen licenses	このクラスタ内の各 TelePresence Server 上のスクリーン ライセンスの数。	スレーブ上のすべてのスクリーン ライセンスがマスターによって制御されます。スクリーン ライセンスの割り当て方法はクラスタにとってはさほど重要なことではありません。マスターがすべてのスクリーン ライセンスを制御します。スレーブで障害が発生した場合でも、マスターはそのスレーブに割り当てられたすべてのスクリーン ライセンスにアクセスできます。

スレーブ TelePresence Server 上のクラスタ ステータスの表示

クラスタ ステータスを表示するには、[Status] > [Cluster] に移動します。スレーブ TelePresence Server 上で [Status] > [Cluster] ページを開くと、マスターのステータスが表示されます。

次の表に、クラスタ内のスレーブ TelePresence Server に関して表示される [Status] > [Cluster] ページの説明を示します。マスター TelePresence Server については、未解決の相互参照「マスター TelePresence Server 上のクラスタ ステータスの表示」（7 ページ）を参照してください。

スレーブ ユニットではユーザ インターフェイスが制限されており、すべての設定を使用できるわけではありません。専用の Web インターフェイスを介して各 TelePresence Server のクラスタ モードを設定する必要があります。

表 8　クラスタ ステータス

フィールド	フィールドの説明	使用方法のヒント
Status	マスター ユニットには、次のステータスがあります。 • *Still starting up*：マスターが起動中です。数分後に、[Status] > [Cluster] ページを更新してください。 • *OK*：マスターとスレーブが正常に通信しています。 • *Lost contact*：スレーブがマスターとの接続を失いました。この場合は、スレーブがすぐに自動的に再起動するため、このステータスが表示されるのは少しの間だけです。	スレーブ TelePresence Server がマスターとの接続を失った場合は、自動的に再起動します。これが、スレーブがクラスタに正しく再参加できる唯一の方法です。 スレーブがマスターとの接続を失う一般的な理由は、マスターが再起動したためです。
Last seen	このフィールドは、マスターが検出されなくなってから最長で 11 秒間だけ表示されます。スレーブは、マスターとの接続を失うと、すぐに自動的に再起動します。	
IP address	マスター TelePresence Server の IP アドレス。	

ネットワーク設定

ネットワーク設定の構成

TelePresence Server 上でネットワーク設定を構成して、ネットワーク ステータスをチェックするには、[Network] > [Network settings] に移動します。

このページの内容

IP 構成の設定

これらの設定によって、TelePresence Server の適切なイーサネット ポートの IP 設定が決定されます。完了したら、[Update IP Configuration] をクリックします。

表 9　IPv4 設定

フィールド	フィールドの説明	使用方法のヒント
IP configuration	ポートを手動と自動のどちらで設定するかを指定します。[Automatic via DHCP] に設定した場合、TelePresence Server はこのポート用の固有の IP アドレスを DHCP（Dynamic Host Configuration Protocol）経由で自動的に取得します。[Manual] に設定した場合、TelePresence Server は後述する手動設定フィールドで指定された値を使用します。	TelePresence Server ポートで IPv4 を無効にすることは可能ですが、それができるのは IPv6 を使用してログインしている場合に限られます。
IP address	このポートのドット区切りの IPv4 アドレス（192.168.4.45 など）。	このオプションは、上記の [Manual] IP 設定を選択した場合にだけ指定する必要があります。 ポート A では、IP 設定が [Automatic by DHCP] に設定されている場合、この設定は無視されます。
Subnet mask	使用する IP アドレスに必要なサブネット マスク（255.255.255.0 など）	
Default gateway	このサブネット上のデフォルト ゲートウェイの IP アドレス（192.168.4.1 など）	

表 10　IPv6 設定

フィールド	フィールドの説明	使用方法のヒント
IP configuration	[Disabled]、[Automatic via SLAAC/DHCPv6]、または [Manual] を選択します。 [Manual] を選択した場合は、IPv6 アドレス、プレフィックス長、およびデフォルト ゲートウェイも入力する必要があります。 [Automatic via SLAAC/DHCPv6] を選択した場合は、TelePresence Server が自動的に IPv6 アドレスを取得します。サーバは、ICMPv6 ルータ アドバタイズメント（RA）メッセージに応じて、SLAAC、ステートフル DHCPv6、またはステートレス DHCPv6 を使用します（後述する自動 IPv6 アドレス設定を参照してください）。	ネットワークが IPv6 をサポートしていない場合は、ポートで IPv6 を無効にします。 TelePresence Server ポート上の IPv6 を無効にすることができますが、IPv4 を使用してログインしている場合に限られます。
IPv6 address	[Manual] 設定を選択した場合は、IPv6 アドレスを CIDR 形式で入力します（`fe80::202:b3ff:fe1e:8329` など）。	[Manual] IP 設定を選択した場合にのみアドレスを入力する必要があります。[Automatic via SLAAC/DHCPv6] を選択した場合は、手動で入力された設定は無視されます。
Prefix length	[Manual] 設定を選択した場合は、プレフィックス長を入力します。	プレフィックス長は、このアドレスの固定のビット数（10 進数）です。
Default gateway	（オプション）このサブネット上のデフォルト ゲートウェイの IPv6 アドレスを入力します。	アドレスは、グローバルにもリンクローカルにもできます。

IP ステータス

[IP status] セクションには、自動と手動のどちらで設定されたかに関係なく、次のように、TelePresence Server のこのイーサネット ポートの現在の IP 設定が表示されます。

IPv4 の設定：

- DHCP
- IP アドレス
- サブネット マスク
- デフォルト ゲートウェイ

IPv6 の設定：

- DHCPv6
- IPv6 アドレス
- IPv6 デフォルト ゲートウェイ
- IPv6 リンクローカル アドレス

イーサネットの設定

TelePresence Server のこのポートのイーサネット設定を構成してから、[Update Ethernet configuration] をクリックします。

表 11　イーサネット設定

フィールド	フィールドの説明	使用方法のヒント
Ethernet settings	[Automatic] または [Manual] を選択します。 [Manual] を選択した場合は、速度とデュプレックスの設定を入力する必要もあります。このイーサネットポートで自動的に接続先のデバイスとイーサネット設定をネゴシエートする場合は、[Automatic] を選択します。	イーサネット接続の両端のデバイスが同じ設定になっていることが重要です。つまり、両方のデバイスを自動ネゴシエーションを使用するように設定するか、両方のデバイスを同じ固定の速度とデュプレックスの設定で構成します。 [1000 Mbit/s] の接続速度が必要な場合は、[Automatic] ネゴシエーションを選択します。
Speed	（[Manual] 設定の場合のみ）接続速度を、使用可能なオプションのいずれかに設定します。	接続速度の設定は、この接続の両端のポートで同じにする必要があります。
Duplex	（[Manual] 設定の場合のみ）接続のデュプレックスモードを [Full duplex] または [Half duplex] に設定します。	接続のデュプレックス設定は、この接続の両端のポートで同じにする必要があります。 全二重モードでは同時双方向伝送が可能ですが、半二重モードでは同時ではない双方向伝送のみが可能です。

イーサネットのステータス

表 12　イーサネット ステータス

フィールド	フィールドの説明	使用方法のヒント
Link status	このイーサネット リンクが接続されているかどうかを示します。	
Speed	このイーサネット リンクの速度。	この値は、このポートが接続されているデバイスとネゴシエートされた値か、または手動設定に基づく値となります。
Duplex	このポートへのネットワーク接続のデュプレックス モード（[Full duplex] または [Half duplex]）。	この値は、このポートが接続されているデバイスとネゴシエートされた値か、または上で選択された手動設定に基づく値となります。
MAC address	このポートの固定のハードウェア MAC（Media Access Control）アドレス。	この値は情報提供のために表示されるだけで、変更はできません。
Packets sent	このポートから送信されたパケットの総数（すべての TCP トラフィックと UDP トラフィック）。	この情報は、TelePresence Server がネットワークにパケットを送信していることの確認に使用できます。
Packets received	このポートで受信されたパケットの総数（すべての TCP トラフィックと UDP トラフィック）。	この情報は、TelePresence Server がネットワークからパケットを受信していることの確認に使用できます。
Statistics:	このポートの詳細な統計情報。 • Multicast packets sent • Multicast packets received • Total bytes sent • Total bytes received • Receive queue drops • Collisions • Transmit errors • Receive errors	この情報は、リンク速度やデュプレックス ネゴシエーションの問題などのネットワークの問題の診断に役立ちます。

DNS 設定の構成

[Network] > [DNS] に移動し、TelePresence Server の DNS 設定をチェックして変更します。

[Update DNS Configuration] をクリックして、新しい設定を適用します。

表 13　DNS 設定

フィールド	フィールドの説明	使用方法のヒント
DNS configuration	TelePresence Server にそのネーム サーバ アドレスを取得させる方法を選択します。 たとえば、[Via Port A DHCPv6] を選択した場合は、デバイスが自動的にイーサネット ポート A に接続された IPv6 ネットワーク経由で DHCP を使用してネーム サーバ アドレスを取得します。 [Manual] を選択した場合は、ネーム サーバ アドレスを入力する必要があります。セカンダリ ネーム サーバまたはドメイン名（DNS サフィックス）を入力することもできます。	選択されたインターフェイスに対して静的 IP アドレスが設定されている場合は、TelePresence Server でネーム サーバ アドレスを自動設定することはできません。 たとえば、ここで [Via Port A DHCPv4] を選択しても、[Port A settings] ページの [IPv4 configuration] セクションで [Manual] を選択しているなら、TelePresence Server により、DNS サーバが設定されないことが警告されます。
Host name	TelePresence Server の名前を指定します。	ホスト名は最大 63 文字にすることができます。 ネットワーク設定によっては、TelePresence Server の IP アドレスを知らなくても、このホスト名を使用して TelePresence Server と通信することができます。
Name server	ネーム サーバの IP アドレス	[DNS configuration] が [Manual] の場合は必須です。
Secondary name server	オプションの 2 台目のネーム サーバを識別します。	オプションの 2 台目のネーム サーバが設定されている場合は、TelePresence Server はどちらのネーム サーバにも DNS クエリを送信できます。
Domain name (DNS suffix)	DNS ルックアップの実行時に追加するオプションのサフィックスを指定します。	非修飾ホスト名を使用して（IP アドレスを使用する代わりに）デバイスを参照する場合に、サフィックスを追加します。 たとえば、ドメイン名（サフィックス）が *cisco.com* に設定されている場合、ホスト *endpoint* の IP アドレスの検索要求がネーム サーバに対して行われると、実際には *endpoint.cisco.com* が検索されます。

DNS ステータスの表示

DNS ステータス フィールドを使用して、次のような TelePresence Server の現在の DNS 設定を確認します。

- ホスト名
- ネーム サーバ
- セカンダリ ネーム サーバ
- ドメイン ネーム (DNS suffix)

IP ルート設定の構成

IP トラフィックが TelePresence Server を出入りする方法を制御するために 1 つ以上のルートをセットアップしなければならない場合があります。

このルートは正しく作成することが重要です。そうしないと、電話の発信や Web へのアクセスができなくなる可能性があります。

ルート設定を構成するには、[Network] > [Routes] に移動します。

このページの内容

IP ルート設定

このセクションでは、TelePresence Server から IP パケットを転送する方法を制御できます。この設定を変更する場合は、TelePresence Server が接続されているネットワークのトポロジを十分理解している必要があります。

新しい IP ルートの追加

新しい IP ルートを追加するには：

1. ターゲット ネットワークの IP アドレスと、アドレスの範囲を定義するマスク長を入力します。
2. これらのアドレスへのトラフィックを、ポート A のデフォルト ゲートウェイ（[Port A]）と、指定したゲートウェイ（[Gateway]）のどちらを経由してルーティングするかを選択します。

3. [Add IP route] をクリックします。

   新しいルートがリストに追加されます。ルートがすでに存在する場合、または、既存のルートをエイリアス（オーバーラップ）する場合は、インターフェイスからルートを修正するように要求されます。

次の表を参考にしてください。

表 14　IP ルートの設定

フィールド	フィールドの説明	使用方法のヒント
IP address / mask length	これらのフィールドを使用して、このルートを適用する IP アドレスの範囲を定義します。 IPv4 アドレッシング：ターゲット ネットワークの IP アドレスを、アドレスの可変ビットを 0 に設定したドット区切りの 4 つの数字列の形式で入力します。[mask length] フィールドを使用して、固定ビット数（これで、可変ビット数が決まり、アドレスの範囲が指定される）を指定します。 IPv6 アドレッシング：ターゲット ネットワークの IP アドレスを、アドレスの可変ビットを 0 に設定した CIDR 形式で入力します。[mask length] フィールドを使用して、固定にするビット数（および可変にするビット数、つまり、アドレスの範囲を意味する）を指定します。	IPv4 の場合：たとえば、192.168.4.128 ～ 192.168.4.255 の範囲のすべての IPv4 アドレスをルーティングするには、IP アドレスを 192.168.4.128 に指定して、マスク長を 25 に指定します。最初の 25 ビットが固定です。これは、最後の 7 ビットでアドレスの範囲が決定されることを意味します。 IPv6 の場合：たとえば、2001:db8::0000 ～ 2001:db8::ffff の範囲のすべての IPv6 アドレスをルーティングするには、IP アドレスを 2001:db8:: に指定して、マスク長を 112 に指定します。最初の 112 ビットが固定です。これは、最後の 16 ビットでアドレスの範囲が決定されることを意味します。
Route	このフィールドを使用して、指定されたパターンと一致するアドレス宛てのパケットのルーティング方法を制御します。	[Port A] または [Gateway] を選択できます。[Gateway] を選択した場合は、パケットを転送するゲートウェイの IP アドレスを入力します。 [Port A] を選択した場合は、一致するパケットがポート A のデフォルト ゲートウェイにルーティングされます（ネットワーク設定の構成を参照）。

既存の IP ルートを表示または削除するには

ページに、各ルートに関する次の詳細情報が表示されます。

- IP アドレス パターンとマスク

- 一致したパケットのルーティング先。これは次のいずれかになります。
- Port A：ポート A に対して設定されたデフォルト ゲートウェイを意味します
- **<** IP アドレス**>**：特定のアドレスが選択されています
- そのルートが他の設定の結果として自動的に設定されたものなのか、手動で追加されたものか

デフォルト ルートは、IPv4 と IPv6 の [Default gateway preference] の選択に応じて自動的に設定され（ネットワーク設定の構成を参照）、削除することができません。手動で設定されたルートと一致しないアドレス宛てのパケットは、デフォルト ゲートウェイ経由でルーティングされます。

手動で設定されたルートは削除できます。ルートの横にあるチェックボックスをオンにしてから、[Delete selected] をクリックします。

現在のルート テーブル

各テーブルに、TelePresence Server のイーサネット ポートに対して IPv4 と IPv6 用に設定されたすべてのルート（手動と自動の両方）が表示されます。イーサネット ポートの IP 設定を変更する場合は、[Network] > [Network settings] に移動します。

IP サービスの設定

[Network] > [Services] に移動して、TelePresence Server 上の Web サービスへのアクセスを制御します。

TelePresence Server は、Web インターフェイスのための HTTP や、電話の発信および受信のための SIP などの Web サービスを提供します。ユニットのイーサネット インターフェイス上でサービスにアクセスできるかどうかと、それらのサービスが利用可能な TCP/UDP ポートを制御できます。

TCP/UDP サービスの有効化

[Network] > [Network settings] ページでどの IP バージョンが有効になっているかに応じて、IPv4 または IPv6 サービスを制御するオプションが表示されます。

1. 有効にするサービス名の横にあるボックスをオンにするか、サービスを無効にする場合はそのボックスをオフにします。
2. 必要に応じて、サービスのポート番号を編集します

   （よく使用されるポート値がデフォルトで入力されています）。
3. [Apply Changes] をクリックします。

エフェメラル ポート範囲の定義

注：最小のエフェメラル ポートを、設定された最大の TCP または UDP サービス ポートより大きくする必要があります。たとえば、HTTPS がポート 20000 に設定されている場合は、許容される最小のエフェメラル ポートは 20001 です。

1. 優先エフェメラル ポート範囲内で最小のポート番号を入力します。

   デフォルト値は 49152 です。最小ポートを 10000 未満に設定することはできません。

2. 優先エフェメラル ポート範囲内で最大のポート番号を入力します。

   デフォルトは、最大可能設定の 65535 で、約 15000 ポートのデフォルト範囲を意味します。TelePresence Server では、範囲を 5000 ポート未満にすることができません。これは、会議機能に悪影響が及ぶ可能性があるためです。

3. [Apply Changes] をクリックします。
4. 値をデフォルト設定にリセットする場合は、[Reset to default] をクリックしてから、[Apply changes] をクリックします。

デフォルト設定へのリセット

1. [Reset to default] をクリックします。

   TelePresence Server が、変更された設定をそのページのデフォルトに置き換えます。この変更はすぐには有効になりません。

2. [Apply Changes] をクリックします。

   デフォルト設定が有効になります。

表 15　[Network] > [Services] フィールドの説明

フィールド	フィールドの説明	使用方法のヒント
HTTP	該当するポート上の Web アクセスを有効/無効にします。	TelePresence Server の Web ページを表示して変更したり、オンライン ヘルプ ファイルを読んだりするには、Web アクセスが必要です。
HTTPS	指定したインターフェイスでセキュアな（HTTPS）Web アクセスを有効/無効にするか、このサービスに使用するポートを変更します。	デフォルトで、TelePresence Server には専用の SSL 証明書と秘密キーが割り当てられます。ただし、必要に応じて新しい秘密キーと証明書をアップロードできます。SSL 証明書の詳細については、「SSL 証明書の設定」を参照してください。

フィールド	フィールドの説明	使用方法のヒント
SIP (TCP)	SIP over TCP を使用する TelePresence Server への着信コールを許可/拒否するか、このサービスに使用するポートを変更します。	
Encrypted SIP (TLS)	SIP over TLS を使用する TelePresence Server への着信暗号化 SIP コールを許可/拒否するか、このサービスに使用するポートを変更します。	
SIP (UDP)	SIP over UDP を使用する TelePresence Server への着信コールと発信コールを許可/拒否するか、このサービスに使用するポートを変更します。	このオプションを無効にすると、SIP over UDP を使用するコールが禁止されます。
Minimum	エフェメラル ポート範囲の下限。	デフォルトで 49152 に設定されますが、10000 ～ 60535 の範囲内で設定できます。
Maximum	エフェメラル ポート範囲の上限。	デフォルトで 65535 に設定されますが、15000 以上に設定できます。最小範囲は 5000 ポートに制限されます。

QoS 設定の構成

TelePresence Server 上の Quality of Service（QoS）を音声とビデオ用に設定するには、[Network] > [QoS] に移動します。

QoS は、特定のデータ クラスの処理をカスタマイズするネットワークの能力を表す用語です。たとえば、QoS は、HTTP トラフィックよりも音声伝送とビデオ伝送を優先するために使用することができます。これらの設定は、すべての出力音声パケットと出力ビデオ パケットに影響します。他のパケットはすべて 0 の QoS で送信されます。

TelePresence Server ではタイプ オブ サービス（IPv4）やトラフィック クラス（IPv6）に対して 6 ビット値を設定できますが、これはネットワークではタイプ オブ サービス（ToS）か差別化サービス（DiffServ）として解釈される可能性があります。IPv6 QoS は機能的に IPv4 QoS と同じであることに注意してください。

注意：必要がなければ、QoS 設定を変更しないでください。

QoS 設定を構成するには、6 ビットのバイナリ値を入力する必要があります。

ToS と DiffServ の値を含む QoS に関する詳細は、Internet Engineering Task Force の Web サイト（www.ietf.org）にある次の RFC に記載されています。

- RFC 791
- RFC 2474
- RFC 2597
- RFC 3246

このページの内容

QoS 構成の設定について

次の表に、[Network] > [QoS] ページでの設定に関する説明を示します。

変更後に [Update QoS settings] をクリックします。

表 16　IPv4 設定

フィールド	フィールドの説明	使用方法のヒント
Audio	ネットワーク上の音声データ パケットに優先順位を付けるための 6 ビットのバイナリ フィールド。	必要がなければ、この設定を変更しないでください。
Video	ネットワーク上のビデオ データ パケットに優先順位を付けるための 6 ビットのバイナリ フィールド。	必要がなければ、この設定を変更しないでください。

表 17　IPv6 設定

フィールド	フィールドの説明	使用方法のヒント
Audio	ネットワーク上の音声データ パケットに優先順位を付けるための 6 ビットのバイナリ フィールド。	必要がなければ、この設定を変更しないでください。
Video	ネットワーク上のビデオ データ パケットに優先順位を付けるための 6 ビットのバイナリ フィールド。	必要がなければ、この設定を変更しないでください。

ToS 設定

ToS 設定は、プレシデンス、遅延、スループット、および信頼性という抽象的なパラメータの間のトレードオフを意味します。

ToS では、使用可能な 8 ビットのうちの 6 ビットが使用されます。TelePresence Server では、ビット 0 ～ 5 を設定できますが、ビット 6 と 7 は 0 に設定されます。

- ビット 0 ～ 2 には IP プレシデンス（パケットの優先順位）を設定します。
- ビット 3 には遅延（0 = 標準遅延、1 = 低遅延）を設定します。
- ビット 4 にはスループット（0 = 標準スループット、1 = 高スループット）を設定します。
- ビット 5 には信頼性（0 = 標準信頼性、1 = 高信頼性）を設定します。
- ビット 6 ～ 7 は将来使用するために予約されており、TelePresence Server インターフェイスを使用して設定できません。

音声パケットとビデオ パケットに優先順位を付けることにより、ただしその一方でネットワーク上の他のパケットに過度の遅延を生じさせないようにすることにより、バランスをとる必要があります。たとえば、すべての値を 1 に設定しないでください。

DiffServ 設定

DiffServ では、使用可能な 8 ビットのうちの 6 ビットを使用してコードポイントが設定されます（使用可能な 64 個のコードポイントがあります）。TelePresence Server では、ビット 0 ～ 5 を設定できますが、ビット 6 と 7 は 0 に設定されます。コード ポイントが DiffServ ノードによって解釈され、パケットの処理方法が決定されます。

デフォルト設定

QoS のデフォルト設定は次のとおりです。

- **Audio** *101110*：
  - ToS では、IP プレシデンスが、比較的高い優先順位を示す 5 に設定されることを意味します。遅延は低に設定され、スループットは高に設定され、信頼性は標準に設定されます。
  - Diff Serv では、完全優先転送を意味します。
- **Video** *100010*：
  - ToS では、IP プレシデンスが、かなり高い（ただし、音声プレシデンスほどではない）優先順位を示す 4 に設定されることを意味します。遅延は標準に設定され、スループットは高に設定され、信頼性は標準に設定されます。
  - DiffServ では、相対的優先転送（コードポイント 41）を意味します。

設定をデフォルト設定に戻すには、[Reset to default] をクリックします。

SSL 証明書の設定

[Network] > [Services] ページで HTTPS を有効にした場合（デフォルトで有効になっている）は、HTTPS を使用して TelePresence Server の Web インターフェイスにアクセスできます。

注：[Network] > [Services] で [Encrypted SIP (TLS)] サービスを使用するように選択した場合は、証明書とキーも必要です。

Cisco TelePresence Server にはローカル証明書と秘密キーが事前にインストールされています。HTTPS を使用してユニットにアクセスするときには、それらがブラウザに対する TelePresence Server の認証に使用されます。ただし、すべての Cisco TelePresence Server に同じデフォルトの証明書とキーがインストールされているので、セキュリティを確かなものにするためにも、独自の証明書と秘密キーをアップロードすることをお勧めします。また、キー長は 2048 ～ 8192 ビットにすることをお勧めします。

TelePresence Server は、DTLS を使用して TIP エンドポイントと暗号化パラメータをネゴシエートします。これには、証明書の使用が必要です。TelePresence Server の DTLS の実装は、顧客支給の証明書を次のように処理します。

- Opportunistic DTLS では、顧客支給の証明書がアップロードされた場合でも、DTLS ネゴシエーションにデフォルトの証明書が使用されます。
- Negotiated DTLS では、アップロードされた顧客支給の証明書が使用されます（これが推奨される処理です）。

Negotiated DTLS は、エンドポイントが RFC 5763 をサポートしている場合に使用されますが、そうでない場合、TIP コールでは、Opportunistic DTLS が試行されます。

独自の証明書とキーをアップロードするには、[Network] > [SSL certificates] に移動します。

注：DTLS は、TelePresence Server に*メディア暗号化*機能キーがインストールされている場合にのみネゴシエートされます。

次の表を参照しながらフィールドに値を入力して、[Upload certificate and key] をクリックします。証明書とキーを同時にアップロードする必要があることに注意してください。新しい証明書とキーをアップロードしたら、Cisco TelePresence Server を再起動する必要があります。

注：証明書と秘密キーは PEM 形式にする必要があります。

ストアには複数の証明書を含めることができます。これは、通常の証明書の BEGIN タグと END タグの間に PEM エンコードの複数の証明機関証明書が順番に含まれた単一の信頼ストア ファイルをアップロードすることによって実現できます。

必要に応じて、独自の証明書とキーを削除する場合は、[Delete custom certificate and key] をクリックします。証明書の削除後は、TelePresence Server を再起動する必要があります。

次の表に、[Network] > [SSL certificate] ページのフィールドの詳細を示します。

表 18　ローカル証明書

フィールド	フィールドの説明	使用方法のヒント
Subject	証明書が発行された企業の詳細： • **C**：企業が登録されている国。 • **ST**：企業が所在する州または県。 • **L**：企業が所在する地域または都市。 • **O**：企業の正式名称。 • **OU**：組織単位または部署。 • **CN**：証明書の一般名、または、ドメイン名。	
Issuer	証明書の発行者の詳細。	証明書が自己発行されたものであれば、詳細は [Subject] の詳細と同一になります。
Issued	ローカル証明書が発行された日付。	
Expires	ローカル証明書が期限切れになる日付。	
Private key	秘密キーが証明書と一致するかどうか。	Web ブラウザは、SSL 証明書の公開キーを使用して、Cisco TelePresence Server に戻すデータを暗号化します。Cisco TelePresence Server ではそのデータを復号化するために秘密キーが使用されます。[Private key] フィールドに「Key matches certificate」と表示されている場合は、データが双方向で確実に暗号化されます。

表 19　ローカル証明書の設定

フィールド	フィールドの説明	使用方法のヒント
Certificate	組織で証明書を購入済みである場合や、独自の方法で証明書を生成する場合は、それをアップロードできます。[Choose File] をクリックし、証明書ファイルを探して選択します。	証明書と秘密キーは PEM 形式にする必要があります。
Private key	[Choose File] をクリックして、証明書に付随する秘密キー ファイルを探して選択します。	証明書と秘密キーは PEM 形式にする必要があります。
Private key encryption password	秘密キーが暗号化形式で保存されている場合、Cisco TelePresence Server にキーをアップロードするためには、ここでパスワードを入力しなければなりません。	

表 20　信頼ストア

フィールド	フィールドの説明	使用方法のヒント
Subject	信頼ストア証明書（通常は、ローカル証明書を確認するために使用される、機関によって発行された証明書）の詳細。	
Issuer	信頼ストア証明書の発行者の詳細。	これは、信頼できる証明機関の詳細です。
Issued	信頼ストア証明書が発行された日付。	
Expires	信頼ストア証明書が期限切れになる日付。	

表 21　信頼ストアの設定

フィールド	フィールドの説明	使用方法のヒント
Trust store	信頼ストアは次の 2 つの理由で必要です。 • SIP TLS 接続のリモート エンドの ID を確認するため（着信コール、発信コール、または登録） • 発信 HTTPS 接続のリモート エンドの ID を確認するため（`flex.participant.requestDiagnostics` を呼び出すフィードバック レシーバや API アプリケーションなど）	信頼ストア証明書を参照して選択し、[Upload trust store] をクリックします。 ストアには複数の証明書を含めることができます。 検証が必要な場合（次の設定を参照）は、リモート パーティの証明書が信頼ストアに照らして検証されます。リモート証明書は、信頼ストアか、信頼ストアの証明書の 1 つの信頼チェーン内に含める必要があります。 信頼ストアを削除する、または、それを更新されたファイルに置き換える必要がある場合は、[Delete trust store] をクリックします。

フィールド	フィールドの説明	使用方法のヒント
Certificate verification settings	リモート証明書を信頼ストアを使って検証する必要がある状況を特定します。	次のドロップダウン オプションの 1 つを選択して、[Apply changes] をクリックします。 • *No verification*：リモート証明書が信頼ストアに照らして検証されません（リモート エンドが常に信頼されます）。 • *Outgoing connections only*：TelePresence Server は、すべての発信 SIP TLS および HTTPS 接続に対してリモート証明書を検証しようとします。 • *Outgoing connections and incoming calls*：TelePresence Server は、すべての着信および発信 SIP TLS 接続と発信 HTTPS 接続に対してリモート証明書を検証しようとします。 **注**：証明書の検証が有効になっている場合は、最大 12 個の subjectAltName がサポートされます。

ネットワーク接続のテスト

[Network connectivity] ページを使用して、TelePresence Server とリモート ビデオ会議デバイス（ホスト）間のネットワーク問題をトラブルシューティングすることができます。

このページでは、TelePresence Server の Web インターフェイスから別のデバイスを ping して、そのデバイスへのルートを追跡することができます。結果には、TelePresence Server とリモート ホスト間でネットワーク接続が確立されているかどうかが表示されます。

リモート デバイスとの接続をテストするには、[Network] > [Connectivity] に移動します。テキスト ボックスに、接続をテストするデバイスの IP アドレスまたはホスト名を入力して、[Test connectivity] をクリックします。

結果には、クエリの発信インターフェイスとリモート ホストの IP アドレスが表示されます。

ping の結果には、ミリ秒単位のラウンドトリップ時間とエコー応答時の TTL（パケット存続時間）の値が表示されます。

TelePresence Server とリモート ホスト間の中間ホスト（通常はルータ）ごとに、ホストの IP アドレスと応答時間が表示されます。

すべてのデバイスが TelePresence Server からのメッセージに応答するわけではありません。応答しないデバイスのルーティング エントリは [<unknown>] と表示されます。無効な ICMP 応答パケット（無効な ICMP チェックサム付きなど）を送信するデバイスがあることがわかっています。無効な ICMP 応答も TelePresence Server で認識されないため、この場合も [<unknown>] と表示されます。

注：ping メッセージは、TelePresence Server からリモート ホストの IP アドレスに送信されます。したがって、TelePresence Server に特定のホストへの IP ルートが設定されている場合は、ping が成功します。この機能を使用すれば、TelePresence Server の IP ルーティング設定をテストすることができます。またこの方法なら、セキュリティへの影響もありません。

注：リモート ホストを ping できない場合は、ネットワーク設定、特に、NAT を使用しているファイアウォールをチェックしてください。

ネットワーク統計情報（netstat）の表示

[Network] > [Netstat] に移動して、TelePresence Server へのすべての TCP 接続と UDP 接続の現在のステータスを表示します。

netstat データは、UI ページをロードまたは更新するたびに更新されるほか、[Refresh] をクリックしたときや、[Resolve names] チェックボックスをオンまたはオフにしたときにも更新されます。

表 22　Netstat フィールドの説明

フィールド	説明
Resolve names	アドレスに対して DNS ルックアップを実行し、可能であればホスト名を表示する場合は、このボックスをオンにします。代わりに IP アドレスを表示する場合は、このボックスをオフにします。データは、チェックボックスのオン/オフで更新されます。
Protocol	[tcp4]、[tcp6]、[udp4]、または [udp6]。これらは、接続で使用されているインターネット プロトコルとアドレッシング スキームを表します。
Recv-Q	TelePresence Server でまだ処理されていないために、この接続上でキューイングされているバイト数。
Send-Q	リモート パーティでまだ確認されていないために、この接続上でキューイングされているバイト数。
Local Address	この接続上の TelePresence Server のアドレス。[Resolve names] がオンになっていない場合は、このフィールドにローカル ソケットが [address:port] として表示されます。[Resolve names] がオンになっている場合は、可能であれば、ソケットが [hostname:servicename] として表示されます。 例：**`ts.example.com:http`** または **`127.0.0.1:80`**
Foreign Address	この接続上のリモート パーティのアドレス。[Resolve names] がオンになっていない場合は、このフィールドに外部ソケットが [address:port] として表示されます。[Resolve names] がオンになっている場合は、可能であれば、ソケットが [hostname:servicename] として表示されます。 例：**`browser.example.com:http`** または **`192.168.3.1:80`**

フィールド	説明
状態	接続の状態。詳細については、http://tools.ietf.org/html/rfc793#section-3.2 を参照してください。
サービス	TelePresence Server がこの接続上で提供するサービスの名前。サービス名は、[Network] > [Services] ページにハイパーリンクされているため、必要に応じてサービス設定を変更できます。

設定

システム設定の構成

システム設定を変更するには、[Configuration] > [System settings] に移動して、フィールドを編集してから（詳細は表を参照）、[Apply changes] をクリックします。

TelePresence Server が Multiparty Media 310/320 プラットフォーム上で実行中は、[System settings] ページが大きく制限されます。ほとんどの会議設定のデフォルトが TelePresence Conductor などの管理システムを使用して作成されます。

表 23　設定済みのすべての会議に関する設定

フィールド	フィールドの説明	使用方法のヒント
Display video preview images	オンの場合は、会議参加者のビデオ ストリームのサムネイル プレビュー画像が TelePresence Server ユーザ インターフェイスに表示されます。	デフォルトは有効（オン）です。
Show event log messages on	このボックスをオンにすると、シリアル コンソールへのイベント ログの出力が有効になり、このボ	チェックボックスはデフォルトでオフになっています。これは、イベント ログのシリアル出力が

フィールド	フィールドの説明	使用方法のヒント
console	ックスをオフにすると、シリアル コンソールへのイベント ログの出力が無効になります。 TelePresence Server の再起動後も選択が保持されます。 このチェックボックスがオフになっている場合でも、TelePresence Server は、電源が入ってからメディア リソースが使用可能になるまではイベント ログ メッセージをシリアル コンソールに出力します。その後は、TelePresence Server がコンソールへのイベント ログ メッセージの送信を停止します。	無効になっていることを意味します。このデフォルトは TelePresence Server のパフォーマンスの向上に役立っています。つまり、この設定を有効にするとパフォーマンスに影響が出る可能性があります。 syslog サーバを使用して、イベント ログ メッセージを収集することをお勧めします。 「syslog を使用したロギング」（57 ページ）を参照してください。
Disable serial console input during startup	このボックスをオンにすると、TelePresence Server が起動中にコンソールからの入力に反応しなくなります。	このボックスをオンにして、コンソール ユーザによって通常のブート シーケンスが中断されないようにすることをお勧めします。
Require administrator login for serial console commands	このボックスをオンにすると、ユーザが識別されていない場合には、TelePresence Server でコンソール コマンドが解釈されなくなります。	このボックスをオンにして、物理アクセスを取得した未承認ユーザからシリアル コンソールを保護することをお勧めします。 **注：**TelePresence Server のコンソールはすべての Unicode 文字を受け入れることができるわけではありません。コンソール アクセスに使用されるアカウントの場合、ユーザ名とパスワードに使用できるのは ASCII 文字のみに限定されます。
Idle serial console session timeout	TelePresence Server が最後の入力以降に公開コンソール セッションを維持する分数。	短期間の値を使用することにより、無人のコンソール セッションが未承認ユーザに対して開いたままにならないようにすることをお勧めします。

SIP 設定の構成

[SIP setting] ページでは、TelePresence Server の SIP 設定を管理することができます。

この情報にアクセスするには、[Configuration] > [SIP settings] に移動します。

デフォルトを更新する場合や、いつでも設定を変更する場合には、次の表で詳細を参照しながらフィールドを編集し、[Apply changes] をクリックします。

表 24　SIP

フィールド	フィールドの説明	使用方法のヒント
Outbound call configuration	この設定は、発信 SIP コールに影響します。 [Use trunk] の場合、VCS や CUCM などのトランク宛先に発信コールをルーティングします。 [Call direct] の場合、発信 SIP コールを直接（トランクを経由せずに）ルーティングします。	*Use trunk*： • 発信 SIP コールを指定された SIP サーバ アドレスにトランク経由で転送します。 • SIP サーバ（Cisco Video Communication Server（VCS）や Cisco Unified Call Manager（CUCM）など）は、TelePresence Server からの発信 SIP コールの前方ルーティングを担当します。 *Call direct*： • TelePresence Server は、可能な場合に、SIP コールを直接接続します。[Outbound address] パラメータや [Outbound domain] パラメータは使用しません。 • TelePresence Server は、トランクを使用しようとしません。
Outbound address	SIP レジストラまたはトランク宛先のホスト名または IP アドレス。	[Outbound call configuration] が [Call direct] に設定されている場合は、TelePresence Server はこのフィールドを無視します。
Outbound domain	トランク宛先のドメイン。	[Outbound call configuration] が [Call direct] に設定されている場合は、TelePresence Server がこのフィールドを無視します。 TelePresence Server は、入力されたアドレスに @ 記号が含まれていないすべての発信 SIP コールに対してこの値を使用します。 発信ドメインが指定されなかった場合は、TelePresence Server は代わりに発信アドレスを使用します。
Username	TelePresence Server は、SIP デバイス（トランク宛先またはエンドポイント）が認証を要求する場合、この名前を使ってそのデバイスとの認証を行います。	

フィールド	フィールドの説明	使用方法のヒント
Password	TelePresence Server は、SIP デバイス（トランク宛先またはエンドポイント）が認証を要求する場合、このパスワードを使ってそのデバイスとの認証を行います。	SIP 宛先は認証を必要としない場合もあります。その場合は、このユーザ名とパスワードの組み合わせでのログインを受け入れるように設定する必要があります。
Outbound transport	TelePresence Server が発信コールに使用するプロトコルを選択します。 [TCP]、[UDP]、または [TLS] のいずれか。	TelePresence Server は、トランク宛先との通信にこのプロトコルを使用します。 暗号化機能キーをインストールしてある場合、シグナリングを暗号化するには、[TLS] を選択します。 TelePresence Server は、この [Outbound transport] の設定に関係なく、接続に使用されるプロトコル（TCP、UDP、または TLS）が何であっても着信接続を受け入れ、同じプロトコルを使用して応答を返します。[Network] > [Services] ページでこれらのサービスが有効になっていることを確認してください。
Advertise Dual IPv4/IPv6	TelePresence Server で IPv4 と IPv6 の混合ネットワークで SIP コールをサポートする場合は、[Use ANAT] を選択します。	デフォルトは、[Disabled] です。ANAT（代替ネットワーク アドレス タイプ）を使用するように設定されたデバイスは、セッションの説明内の ANAT 構文をサポートします。詳細については、http://tools.ietf.org/html/rfc4091 を参照してください。
Negotiate SRTP using SDES	TelePresence Server が SDES を使用して SRTP をネゴシエートするオプションを次の中から選択します。 • *For secure transports (TLS) only* • *For all transports*。 （注：このパラメータは、*メディア暗号化*機能キーがある場合にのみ表示されます）。	TelePresence Server は、SIP との暗号化の併用をサポートします。暗号化が SIP と一緒に使用されている場合は、音声メディアとビデオ メディアが Secure Real-time Transport Protocol（SRTP）を使用して暗号化されます。SRTP を使用している場合は、キー交換のデフォルト メカニズムが Session Description Protocol Security Description（SDES）になります。SDES はクリア テキストでキーを交換するため、呼制御メッセージ用のセキュアなトランスポートと組み合わせて SRTP を使用することをお勧めします。さらに、SIP コール制御メッセージに使用可能なセキュアなトランスポート メカニズムである Transport Layer Security（TLS）を使用するように TelePresence Server を設定することができます。 デフォルト設定は、[For secure transports (TLS) only] です。

システム時刻の表示とリセット

TelePresence Server のシステム日時を手動で設定することも、Network Time Protocol（NTP）を使用して時刻を同期させることもできます。

時刻設定を構成するには、[Configuration] > [Time] に移動します。

システム時間

現在の時刻には、TelePresence Server に従った時刻が表示されます。

システム日時を手動で設定するには、新しい値を入力して、[Change system time] をクリックします。

NTP

TelePresence Server は NTP プロトコルをサポートします。TelePresence Server を自動的に NTP サーバと同期させる場合は、NTP 設定を入力してから、[Update NTP settings] をクリックします。

TelePresence Server は 1 時間ごとに NTP サーバと同期します。

NTP サーバが TelePresence Server 上で有効になっているイーサネット インターフェイスのいずれかに対してローカルな場合は、TelePresence Server が自動的にそのポートを使用して NTP サーバと通信します。

NTP サーバがローカルでない場合、NTP サーバのネットワーク/IP アドレスへの IP ルートが指定されていなければ、TelePresence Server は、デフォルト ゲートウェイとして設定されたポートを使用して NTP サーバと通信します（[Network] > [Routes] を参照してください）。

TelePresence Server と NTP サーバ間にファイアウォールが設置されている場合は、UDP ポート 123 への NTP トラフィックを許可するようにファイアウォールを設定します。

表 25　デバイス時刻の設定

フィールド	フィールドの説明	使用方法のヒント
Enable NTP	このボックスをオンにすると、TelePresence Server 上の NTP プロトコルが有効になります。	
UTC offset	UTC からの現在のタイム ゾーンのオフセット。	英国夏時間やその他の夏時間調整方式などのタイム ゾーンに対する地域の変更を考慮するようにこのオフセットを手動で更新する必要があります。
NTP host	ネットワークのタイム キーパーとして機能するサーバの IP アドレスまたはホスト名。	

NTP over NAT（ネットワーク アドレス変換）の使用

NAT が TelePresence Server のネットワークに対してローカルな場合は、追加設定は必要ありません。

NAT が NTP サーバのローカル ネットワーク上で使用されている場合は、TelePresence Server から NTP サーバ上の UDP ポート 123 に NTP データを転送するように NAT 転送テーブルを設定する必要があります。

クラスタの設定

Media 310/320 ハードウェア上で TelePresence Server のクラスタを設定するには、[Configuration] > [Cluster] に移動します。

ドロップダウンから [Cluster mode] を選択してから、[Apply changes] をクリックします

注：Media 310 と Media 320 をクラスタ化する場合は、より容量の大きなユニット（Media 320）をマスターとして設定する必要があります。

フィールド	説明
Cluster mode	[Master]、[Slave]、または [Unclustered] のいずれか。 Media 300 ボックス同士をスタッキング ケーブルで初めて接続するときは、クラスタは自動的に設定されません。ユニットのそれぞれに順番にログインして、1 台を [Master] として設定し、それ以外を [Slave] として設定する必要があります。 設定が不完全または間違っているクラスタでは、[Master] や [Unclustered] の TelePresence Server はコールを受信できますが、[Slave] は（マスターがないと）コールを受信できません。

TelePresence Server のバックアップとアップグレード

このページの内容

メイン TelePresence Server ソフトウェア イメージのアップグレード

メイン TelePresence Server ソフトウェア イメージは、アップグレードする必要がある唯一のファームウェア コンポーネントです。

メイン TelePresence Server ソフトウェア イメージをアップグレードするには：

1. [Configuration] > [Upgrade] に移動します。
2. メイン ソフトウェア イメージの [Current version] をチェックして、現在インストールされているバージョンを確認します。
3. サポート ページにログオンして、新しいイメージが入手可能かどうかを確認します。
4. 入手可能な最新のイメージをダウンロードして、ローカル ハード ドライブに保存します。
5. イメージ ファイルを解凍します。
6. TelePresence Server の Web ブラウザ インターフェイスにログオンします。
7. [Configuration] > [Upgrade] に移動します。
8. ハード ドライブ上で解凍したファイルを探します。

   [Browse...] や [Choose File] などのボタン（このボタンはブラウザによって異なります）を使用します。
9. [Upload software image] をクリックします。ブラウザが TelePresence Server へのファイルのアップロードを開始し、新しいブラウザ ウィンドウが開いてアップロードの進捗状況が表示されます。完了すると、ブラウザ ウィンドウが更新され、「Main image upgrade completed」と表示されます。
10. アップグレードのステータスが [TelePresence Server software upgrade status] フィールドに表示されます。
11. TelePresence Server をシャットダウンして再起動します。

設定のバックアップと復元

[Configuration] > [Upgrade] ページの [Back up and restore] セクションを使用すれば、Web インターフェイスを使用して TelePresence Server の設定をバックアップまたは復元することができます。これにより、以前の設定に戻したり、今の設定を別の設定にコピーすることによってユニットを効率的にコピーしたりすることができます。

設定をバックアップするには、[Save backup file] をクリックして、生成された configuration.xml ファイルを安全な場所に保存します。

後日に設定を復元するには：

1. [Configuration] > [Upgrade] に移動します。
2. 以前保存した configuration.xml ファイルを探して選択します。

   ボタンはブラウザによって違う場合があります（[Browse...] や [Choose File] など）。
3. 保存した設定で上書きする現在の設定として、[Network settings] と [User settings] のどちらかまたはその両方を選択します。

   上書きコントロールはデフォルトでは選択されていません。ソフトウェアは、デフォルトでは既存のネットワーク設定とユーザ アカウントを維持する設定になっています。
4. [Restore backup file] をクリックします。

新しい設定ファイルを TelePresence Server に復元するときは、設定のどの部分を上書きするかを制御できます。

- [Network settings] をオンにした場合は、指定されたファイルのネットワーク設定でネットワーク設定が上書きされます。

  通常は、同じ TelePresence Server からバックアップされたファイルから復元する場合や、使われていない TelePresence Server を交換する場合にのみ、このチェックボックスをオンにします。

  別のアクティブな TelePresence Server からネットワーク設定をコピーするときにクラッシュが発生すると（たとえば、両方が同じ固定の IP アドレスを使用するように設定された場合など）、どちらかまたは両方のデバイスが IP 経由で到達不能になります。[Network settings] をオンにしなかった場合は、復元操作で既存のネットワーク設定は上書きされません。ただし、1 つの例外があります。それは QoS 設定です。QoS 設定は、[Network settings] チェックボックスに関係なく、上書きされます。
- [User settings] をオンにした場合は、現在のユーザ アカウントとパスワードが、指定されたファイル内のユーザ アカウントとパスワードで上書きされます。
- ユーザ設定を上書きする場合、復元されたファイル内に、現在のログインに対応するユーザ アカウントが存在しなければ、ファイルのアップロード後に再度ログインする必要があります。

TelePresence Server 機能の有効化

TelePresence Server はアクティブにしないと、その機能のほとんどを使用できません（TelePresence Server がアクティブになっていない場合は、Web インターフェイスの上部のバナーに人目を引く警告が表示されます。それ以外の点では、Web インターフェイスの表示と動作は通常と変わりません）。

これが新しい TelePresence Server の場合は、すでにアクティブになっているはずです。そうでない場合、または、新しいファームウェア バージョンにアップグレードした場合や、新しい機能を有効にしようとしている場合は、販売店に問い合わせて適切なアクティベーション キーを取得してください。

キーは TelePresence Server ごとに異なります。販売店が有効なキーを提供できるように、キーを要求するときはデバイスのシリアル番号を伝えられるようにしておいてください。

キーの適用手順は、TelePresence Server をアクティブにする場合も高度な機能を有効にする場合も同じです。

キーを TelePresence Server に適用するには：

1. [Feature management] リストを参照して、機能がアクティブになっているかどうかをチェックします。

   製品アクティベーション キーもこのリスト内にあります。

2. [Add key] フィールドに、販売店から渡されたキーを、ダッシュも含めて*受け取ったものをそのとおり*入力します。
3. [Add Key] をクリックします。

   ブラウザ ウィンドウが更新され、新しく追加された機能と入力されたキーが一覧に表示されます。

   キーが有効でない場合は、再入力するように要求されます。

   キーには有効期限がある場合があります。その場合は、失効日、または、機能が期限切れになっているという警告が表示されます。期限切れになったキーは、対応する機能が無効になっていてもリストに表示されます。

4. 後で再入力しなければならない場合に備えて、キーをメモしておきます。

TelePresence Server または機能のアクティベーションが成功すると、すぐに有効になり、TelePresence Server の再起動後も保持されます。

一部のタイプの機能を削除できることに注意してください。機能を削除するには、キーの横にある [remove] をクリックします。

スクリーン ライセンスの適用

スクリーン ライセンス キーは、TelePresence Server のハードウェア シリアル番号に関連付けられます。スクリーン ライセンス キーは、機能キーを追加するとき（上で詳述した手順）と同様に、TelePresence Server 上で直接入力します。

TelePresence Server のシャットダウンと再起動

アップグレードの一環で再起動する場合や、電源をオフにする場合に、TelePresence Server をシャットダウンしなければならないことがあります。

注意：TelePresence Server をシャットダウンすると、すべてのアクティブ コールが切断されます。

TelePresence Server をシャットダウンするには：

1. [Configuration] > [Shutdown] に移動します。
2. [Shut down TelePresence Server] をクリックします。

   ボタンが [Confirm TelePresence Server shutdown] に変化します。
3. このボタンをもう一度クリックして確定します。

   TelePresence Server がシャットダウンを開始します。ページの上部にあるバナーが変化してそのことを示します。

   シャットダウンが完了すると、ボタンが [Restart TelePresence Server] に変化します。
4. 最後にもう一度このボタンをクリックして TelePresence Server を再起動します。

管理者パスワードの変更

このページでは、この TelePresence Server へのログインに使用される管理者パスワードを変更することができます。これは、管理者になる必要のある現在のユーザに適用されます。このページにアクセスするには、[Configuration] > [Change password] に移動します。

管理者パスワードは定期的に変更することをお勧めします。パスワードはメモして安全な場所に保管しておくことができます。

パスワードを変更するには、新しいパスワードを 2 回入力して、[Change Password] をクリックします。

会議

会議リストの表示

[Conferences] ページには、そのステータス（[Active] または [Inactive]）に関係なく、この TelePresence Server 上で設定されているすべての会議が一覧表示されます。

[Conferences] に移動してこのリストにアクセスします。

会議はデフォルトで名前のアルファベット順にソートされます。ソート順序を変更するには、あるいは、ステータスか URI でリストをソートするには、関連する列ヘッダーをクリックします。

このページでは、次の操作を実行できます。

- 会議を削除する。
- 会議名をクリックして、そのステータスを表示する。

リストには、会議ごとに次の情報が表示されます。

表 26　会議リストの詳細

フィールド	フィールドの説明	使用方法のヒント
Name	事前に設定された会議の名前。	会議名をクリックすると、会議ステータスと参加者が表示されます。
URIs	会議に割り当てられた URI。	リモート管理モードでは、TelePresence Server はゲートキーパーに個別の会議 URI を登録しません。 会議には、参加者がダイヤル可能な最大 2 つの多用途 URI を割り当てることができます。URI が PIN で保護されている場合は、そのステータスが表示されます。 1 つの URI で複数の PIN をサポートできるため、ゲスト/議長の PIN を個々に設定することができます。 参加者ごとに、彼らがダイヤルする個人用の URI を割り当てることができます。これらはこのリストに表示されません。
Status	次のような会議のステータス。 • *Scheduled* • *Active* • *Inactive* • *Ending* このフィールドには、会議の設定に関する警告も表示される場合があります。	会議の種類は次のとおりです。 • [Scheduled] 会議には、会議の開始までの時間が表示されます。 • [Active] 会議には、[(<X> endpoints, <N> screens)] またはすべてのエンドポイントが音声専用の場合は [Active (<X> endpoints)] が表示されます。 • [Inactive] 会議は、事実上、[Active] 会議と同じですが、参加者がいません。ただし、URI、開始までの時間、および期間を指定することはできます。 • [Ending] は、会議が終了中であることを示します。この間に、残りのすべての参加者に終了ロビーが表示されます。 ステータスで、会議の継続期間と会議がロックされているかどうかに関する追加情報が表示される場合があります。たとえば、[Inactive - Ends in 5 hours and 27 minutes [Locked]] のように表示されます。 会議設定警告（[No participants allowed - limited to 0 participants] など）が表示される場合があります。

会議ステータスの表示

会議の [Status] ページには、会議のリアルタイムのステータスが表示されます。[Conferences] に移動してから、会議名をクリックし、[Status] ページを表示します。

このページから、会議の状態について以下のことを把握できます。

- アクティブかどうか。また、いくつのエンドポイントが会議に参加しているか
- ロックされているかどうか
- コンテンツ チャネルがあるかどうか
- 参加者がいるかどうか。またそれぞれの参加者のステータス
- それまでにどんな参加者がいたか
- 会議に割り当てられた URI があるか

[Conference] > [Conference Name] > [Status] ページでは、次の操作を実行できます。

- 参加者を選択してから、[Disconnect selected] で選択した参加者の接続を解除する
- [Disconnect all] ですべての参加者の接続を解除して、事実上、会議を終了する
- 1 つまたはすべてのエンドポイントにメッセージを送信する
- 参加しているエンドポイントに関する追加のステータス情報を表示するには、[More...] をクリックします。[Expand all] をクリックすると、すべてのアクティブなエンドポイントに関する追加のステータス情報が表示されます（詳細については、次の表を参照してください）。

会議ステータス リファレンス

表 27　ステータス

フィールド	フィールドの説明	使用方法のヒント
Status	次のような会議のステータス。 • *Scheduled* • *Active* • *Inactive* • *Ending* このフィールドに、会議の設定に関する警告が表示される場合があります。	会議の種類は次のとおりです。 • [Scheduled] 会議には、会議の開始までの時間が表示されます。 • [Active] 会議には、[(<X> endpoints, <N> screens)] またはすべてのエンドポイントが音声専用の場合は [Active (<X> endpoints)] が表示されます。 • [Inactive] 会議は、事実上、[Active] 会議と同じですが、参加者がいません。ただし、URI、開始までの時間、および期間を指定できます。 • [Ending] は、会議が破壊中であることを示します。この間に、残りのすべての参加者に終了ロビーが表示されます。 ステータスに、会議の継続期間と会議がロックされているかどうかに関する追加情報が表示される場合があります。たとえば、[Inactive - Ends in 5 hours and 27 minutes [Locked]] のように表示されます。 会議設定警告（[No participants allowed - limited to 0 participants] など）が表示される場合があります。
URIs	会議に割り当てられた URI。	会議には、参加者がダイヤル可能な最大 2 つの多用途 URI を割り当てることができます。URI が PIN で保護されている場合は、そのステータスが表示されます。 1 つの URI で複数の PIN をサポートできるため、ゲスト/議長の PIN を個々に設定することができます。 参加者ごとに、彼らがダイヤルする独自の URI を割り当てることができます。これらはこのリストに表示されません。
Conference lock status	会議がロックされているかどうかを示します。	

フィールド	フィールドの説明	使用方法のヒント
Content	コンテンツ チャネルが使用中かどうか。	次のいずれかになります。 • *No current presentation*：コンテンツ共有が会議に対して有効になっていますが、アクティブなコントリビュータが存在しません。 • *Presentation from <endpoint display name>*：コンテンツのアクティブなコントリビュータが存在します。 詳細については、「コンテンツ チャネル サポート」を参照してください。

表 28　すべての参加者

フィールド	フィールドの説明	使用方法のヒント
Endpoint	現在アクティブな会議に参加しているエンドポイントの名前。	会議がアクティブでない場合は、このセクションに [No endpoints] と表示されます。 会議から参加者を削除するには、該当するチェックボックスをオンにして、[Disconnect selected] を選択します。 エンドポイントの名前をクリックして、[Status] ページに移動します。
Type	エンドポイント タイプ。	
Authority	[Chair] または [Guest] のどちらか。会議における参加者の役割（および関連する権限）を示します。	管理しているシステムがこの会議に議長/ゲストの制御レベルを明示的に適用していない場合は、デフォルトですべての参加者が [Chair] に設定されます。
Status	エンドポイントのステータス。	次のいずれかになります。 • *Joining conference*：エンドポイントはこの会議に参加しようとしています。 • *In conference*：エンドポイントは現在この会議に参加しています。 • *Attempting to re-establish call*：エンドポイントはビジーで、再試行が行われています。 [xx failed to join]（グループ分けされたエンドポイント）、[packet loss detected]、[video to muted]、[video from muted]、[video muted]（および音声に関する同様の情報）、[important]、[audio-only] などの追加のステータス情報が表示される場合があります。

フィールド	フィールドの説明	使用方法のヒント
		会議の開始時に事前に設定されたエンドポイントがビジーだった場合は、TelePresence Server が会議中に最大 5 回そのエンドポイントへの接続を再試行し、ビジーでなくなっていれば接続します。再試行間隔は 5、15、30、60、および 120 秒です。
More...	[More...] をクリックすると、送受信ストリームのプレビューが表示されます。会議に対するエンドポイントの貢献度を制御することもできます。 [Expand/Collapse All] をクリックして、リスト内のすべてのエンドポイントの詳細なステータス情報を表示します。	次の作業を実行できます。 音声のミュート  とミュート解除  ビデオのミュート  とミュート解除  参加者を重要（ストリームのみを送信）  にするか、重要でないにするか  ビデオ ストリームがトランスコードされていない場合は、送信/受信ビデオ ストリームのプレビューを使用できません。この場合は、[No preview] メッセージが表示されます。 加えて、[All participants] ペインの下部に [* Preview Panes are not available for non-transcoded (SVC) video streams] と表示され、プレビュー ペインが表示されない理由が明らかにされます。

表 29　過去の参加者

フィールド	フィールドの説明	使用方法のヒント
Endpoint	この会議に過去に参加していたエンドポイントの名前。	参加者を会議に再接続するには、該当するチェックボックスをオンにして、[Retry connection] を選択します。 エンドポイントの名前をクリックして、[Status] ページに移動します。
Type	エンドポイント タイプ。	
Reason for disconnection	エンドポイントが会議から離脱した理由。	TelePresence Server は、次のような理由でエンドポイントを接続解除することがあります。 • *requested by administrator*：エンドポイントが管理者によって接続解除されました。 • *call rejected*：相手先がコールを拒否しました。 • *left conference*：エンドポイントが会議の終了時に接続解除されました。 • *requested via API*：エンドポイントが API 経由で接続解除されました。

フィールド	フィールドの説明	使用方法のヒント
		• *no answer*：エンドポイントがコールに応答しませんでした。 • *busy*：エンドポイントがビジーだったために接続に失敗しました（SIP コールの場合は、エンドポイントがコールを拒否した可能性もあります）。 • *destination unreachable*：エンドポイントが到達不能でした。 • *DNS failure*：DNS ルックアップが失敗しました。 • *Encryption not supported by far end*：コールに暗号化が必要ですが、相手先が暗号化をサポートしていません。あるいは、このコールで暗号化が禁止されていますが、相手先は暗号化を要求しています。 • *timeout*：接続がタイムアウトしました。 • *insufficient free ports*：空きポートが足りないために、エンドポイントが接続解除されました。 • *conference port limit reached*：会議ポートの制限に達したために、エンドポイントが接続解除されました。 • *Conference locked*：会議がロックされていたため、コールを接続できませんでした。 • *Product not activated*：TelePresence Server にアクティベーション キーがインストールされていないために、コールを発信/受信できませんでした。 • *Protocol error*：プロトコル エラーが原因でエンドポイントが接続解除されました。 • *Network error*：ネットワーク エラーが原因でエンドポイントが接続解除されました。 • *Unavailable*：エンドポイントが使用できません。 • *Capability negotiation error*：エンドポイントと TelePresence Server で相互に互換性のあるコール セットアップをネゴシエートできません。 • *Insufficient token allocation*：TIP/MUX コールに対するトークン指定/割り当てが十分ではありませんでした。 • *TIP/MUX negotiation failure*：TIP/MUX ネゴシエーションが正常に完了しなかったために、エンドポイントが接続解除されました。 • *No media received*：エンドポイントが突然メディアの送信を停止してから 30 秒が経過したために、TelePresence Server がそのエンドポイントを接続解除しました。 • *unspecified error*：エンドポイントが接続解除されましたが、TelePresence Server がその理由を認識していません。

エンドポイントとグループのステータスの表示

エンドポイント ステータスは、エンドポイントがリモート管理モードでアクティブな会議に参加している場合にのみ使用できます。ここからエンドポイントをある程度制御することができます。

1. [Conference] に移動して、[Status] ページを選択します。
2. エンドポイントまたはグループ名をクリックします。
3. 次の表を参照しながら、エンドポイントを確認または制御します。
4. ブラウザでページを更新して最新のステータスを表示します。

表 30　エンドポイント提供情報

フィールド	フィールドの説明	使用方法のヒント
Country code/ extension	これらのフィールドには、エンドポイントから返された情報が表示されます。詳細は、メーカーによって異なります。	この情報は、エンドポイントが初めて接続されるときに表示されます（現在接続されているかどうかは関係ありません）。
Manufacturer code		
Product		
Version		

表 31　ステータス

フィールド	フィールドの説明	使用方法のヒント
Connected to conference	エンドポイントが現在会議に参加しているかどうかと、参加している場合はその会議の名前。	会議名をクリックすると、その会議のステータス ページに移動します。
Call status	コールが接続されているかどうかと、接続されている場合はそれが着信コールか発信コールか。	
Protocol	このコールで使用されるプロトコル（SIP など）。	
Endpoint advertised capabilities	エンドポイントがコールのネゴシエート中にアドバタイズした機能。	たとえば、音声、ビデオ、ビデオ コンテンツ、暗号化されたトラフィック、暗号化されていないトラフィックなどがあります。

フィールド	フィールドの説明	使用方法のヒント
Audio channels	Cisco TelePresence Server と相手先の間で音声受信チャネルと音声送信チャネルが開いているかどうか。	
Video channels	Cisco TelePresence Server と相手先の間でビデオ受信チャネルとビデオ送信チャネルが開いているかどうか。 [Single-stream] または [Multi-stream] は、現在のビデオ チャネルの動作モードを示します。	最初、エンドポイントは、マルチストリーム ネゴシエーションが完了するまでシングルストリーム エンドポイントとして会議に参加します。エンドポイントがそのコール内の最初のエンドポイントで、他のエンドポイントが参加するのを待っているときにも、[single-stream] として表示されます。
Extended video channels	Cisco TelePresence Server と相手先の間で拡張ビデオ受信チャネルと拡張ビデオ送信チャネルが開いているかどうか。	
Received audio gain mode	エンドポイント上で TelePresence Server から受信された音声に対して設定された音声ゲイン モード。[<use default>]、[Automatic]、[Fixed]、または [Disabled] のいずれか。	*<use default>*：このエンドポイントは、会議のオートゲイン コントロール設定を継承しています。 *Automatic*：TelePresence Server は、このエンドポイントが受信する音声のゲインを、他の参加者が受信するレベルに近づくよう動的に調整します。 *Disabled*：このエンドポイントが受信する音声に対してゲイン コントロールが無効になっています。 *Fixed*：TelePresence Server はエンドポイントの受信音声を一定比率で調整します。これは、エンドポイントの設定ページの [Received audio gain] フィールドで設定します。
Bandwidth	各方向でこのコールのメディアに使用されるネットワーク帯域幅の容量。	エンドポイント グループの場合は、合計帯域幅ではなく、コールごとの帯域幅が表示されます。
Preview	ビデオ ストリームのサンプル スチール。	プレビューには、受信ストリームと送信ストリームの両方の各画面のスチールが、該当する方向と帯域幅使用量の下に表示されます。クリックするとプレビューを更新できます。 ビデオ ストリームがトランスコードされていない場合は、送信/受信ビデオ ストリームのプレビューを使用できません。この場合は、[No preview] メッセージが表示されます。

フィールド	フィールドの説明	使用方法のヒント
Endpoint *X*	（エンドポイント グループのみ）エンドポイント グループ内の各エンドポイントの接続ステータス。	
Duration	エンドポイント/エンドポイント グループがこの会議に参加していた時間。	
Disconnect	このコントロールは、会議からエンドポイントまたはエンドポイント グループを接続解除するために使用します。	
Mute audio from / Unmute audio from	このコントロールは、このエンドポイントからの音声のミューティングを開始または停止するために使用します。これは、他の会議参加者がこのエンドポイントを視聴できるかどうかに影響します。	
Mute audio to / Unmute audio to	このコントロールは、このエンドポイントへの音声のミューティングを開始または停止するために使用します。エンドポイントへの音声をミュートすると、そのエンドポイントに音声が流れなくなります。	
Mute video from / Unmute video from	このコントロールは、このエンドポイントからのビデオのミューティングを開始または停止するために使用します。これは、他の会議参加者がこのエンドポイントを視聴できるかどうかに影響します。	
Mute video to / Unmute video to	このコントロールは、このエンドポイントへのビデオのミューティングを開始または停止するために使用します。エンドポイントへのビデオをミュートすると、そのエンドポイントに空白のビデオが送信されます。	

フィールド	フィールドの説明	使用方法のヒント
Tidy view	このコントロールは、このエンドポイントまたはエンドポイント グループに送信されるビュー レイアウトを整理するために使用します。 マルチストリーム エンドポイントの場合は、このボタンが無効になります。	TelePresence Server は、自動的に、他の参加者のビデオ ストリームを表示する PiP（ピクチャ イン ピクチャ）を中央に配置し、少しでも大きく表示できる場合は PiP を画面間で移動します。これは、参加者が会議に参加したり、会議から離脱したりするのに応じて動的に行われます。 必要に応じて、ビューの整理オプションを使用して、このエンドポイントに送信されたレイアウト内の参加者の PiP を手動でリセットして中央に配置できます。
Send message	エンドポイントにメッセージを送信する場合にクリックします。 [Send message] ページには以下が表示されます。 1. メッセージを入力して、ターゲット エンドポイント上のその位置を選択し、メッセージの表示期間（秒単位）を入力します。 2. [Send message] をクリックします。	このボタンは、次の状況下でマルチストリーム エンドポイントに対してのみ有効になります。 • エンドポイントは ActiveControl に対応している必要があります。 • エンドポイントはメッセージにサブスクライブする必要があります。 • 会議でメッセージングが有効になっている必要があります。

エンドポイントまたはエンドポイント グループの統計情報の表示

1. [Conference] に移動して、[Status] ページを選択します。
2. エンドポイントまたはグループ名をクリックします。エンドポイントの [Status] ページが表示されます。
3. [Statistics] をクリックして、[Endpoint Statistics] ページを表示します。

   情報は最大 4 つのセクション（[Audio]、[Auxiliary audio]、[Video]、および [Content channel]）に表示されます。

   各チャネルの統計情報は、2 つのリスト（[Receive stream] 統計情報と [Transmit stream] 統計情報）にグループ分けされます。
4. データは 3 秒ごとに自動的に更新されます。ただし、ブラウザでページを再表示することによって手動でデータを更新することも、[Refresh] をクリックして最新の統計情報を取得することもできます。

マルチスクリーン エンドポイントの場合は、[Multiscreen Stream Selection] ページに誘導されます。必要なストリームを選択して [Endpoint Statistics] ページに移動します。このページには、そのチャネルに関連付けられたすべてのストリームに関するデータが表示されます。

マルチストリーム エンドポイントは、最大 4 本の受信ビデオ ストリームと最大 16 本の送信ビデオ ストリームを持ちます。マルチストリーム エンドポイントの個々のビデオ、音声、およびコンテンツ ストリームは、[Rx Audio]、[Tx Audio]、[Rx Video]、[Tx Video]、および [Content] として表示されます。[Multistream Stream Selection] ページでストリームを選択すると、選択したストリームのみの [Statistics] ページが表示されます。

注：マルチスクリーン チャネルを選択すると、そのチャネルに関連付けられたすべてのストリームに関するデータが表示されます。一方、マルチストリーム エンドポイントの場合は、ストリーム同士が独立しているうえに、数も多いため、個別のストリームを選択する必要があります。選択すると、[Endpoint Statistics] ページにそのストリームに関するデータだけが表示されます。

表 32　受信ストリーム統計情報

フィールド	フィールドの説明
Receive stream	受信ストリームに使用されるコーデック。ビデオ チャネルとコンテンツ チャネルの場合は、ビデオ ストリームの次元も表示されます。
Encryption	このストリームが暗号化されているかどうか。
Channel bit rate	エンドポイントが Cisco TelePresence Server に音声/ビデオ/コンテンツを送信するためのネゴシエートされた利用可能な帯域幅。
Receive bit rate	このフィールドは、ビデオ チャネル受信ストリームとコンテンツ チャネル受信ストリームにのみ適用されます。Cisco TelePresence Server が要求したエンドポイントの送信ビット レート（ビット/秒）を表します。最近測定されたビット レートがカッコ内に表示されます。
Received jitter	このチャネルを介してパケットが Cisco TelePresence Server に到着するタイミングの変動を表します。数値が小さいほど、パケットがより予想どおりに到着していることを示します。
Receive energy	このフィールドは、音声受信ストリームにのみ適用され、音声信号強度の尺度として使用されます。単位はミリデシベルで、-34000 などの大きな負の数値は声が非常に小さいことを意味し、0 に近い負の数値は声が大きいことを意味します。
Packets received / errors	Cisco TelePresence Server によって受信された音声/ビデオ/コンテンツ パケットの数。2 つ目の数値は、シーケンスの中断や不正な RTP 詳細などの音声/ビデオ/コンテンツ パケット レベルのエラー数を示します。ビデオ（実際のビデオ データ）で何らかのエラーが発生したパケット数とは違います。
Packets total / missing	このエンドポイントから Cisco TelePresence Server 宛ての音声パケットの数。2 つ目の数値は、受信したが、破損していたパケットの数を示します。

フィールド	フィールドの説明
Frames received / errors	エンドポイントに送信される音声/ビデオ/コンテンツ ストリームのフレーム レート、および、受信された音声/ビデオ/データ フレームに対する、エラーを伴うフレーム数の比較。
Frame rate	このフィールドは、ビデオ受信ストリームとコンテンツ受信ストリームに適用されます。エンドポイントと TelePresence Server の間で送信/受信されたストリームの 1 秒あたりのフレーム数です。
Fast update requests sent	このチャネルを介して TelePresence Server から送信された Fast Update Request（FUR）の数。たとえば、パケットが失われた場合、TelePresence Server はエンドポイントに FUR を送信します。
ClearPath FEC	このストリームで使用された前方誤り訂正（FEC）に関する統計情報。エンドポイントがストリームに FEC を適用できない場合、または、TelePresence Server と ActiveControl をネゴシエートできない場合は、値が [Not supported] になります。 そうでない場合は、2 つの統計情報（パーセンテージ オーバーヘッドと回復されたパケットの数）が表示されます。 パーセンテージ オーバーヘッドは、オリジナルのストリームに対する、挿入される FEC パケットの数の比率を表します。エンドポイントがストリーム内のすべてのパケットのコピーを挿入する場合、オーバーヘッドは 100% になります。エンドポイントがパケット 2 つにつき 1 つの割合でパケットのコピーを挿入する場合は、オーバーヘッドは 50% になり、4 つにつき 1 つの割合ならば、25% になります。実際の統計情報がいつもこれらのレベルと完全に一致するとは限りません。これは、カウントの間隔と RTCP レポートのタイミングに依存します。 回復されたパケットの数は、オリジナルが失われたため、TelePresence Server によってエンドポイントの FEC パケットから回復されたパケットの単純なカウント数となります。
ClearPath LTRF	LTRF（Long Term Reference Frames）が有効になっている場合は、[N repair frames received] を報告します。これは、LTRF がストリームで使用された回数を示します。

表 33　送信ストリーム統計情報

フィールド	フィールドの説明
Transmit stream	送信ストリームで使用されるコーデック。ビデオ チャネルとコンテンツ チャネルの場合は、ビデオ ストリームの次元も表示されます。
Encryption	このストリームが暗号化されているかどうか。
Channel bit rate	Cisco TelePresence Server がエンドポイントに音声/ビデオ/コンテンツを送信するためのネゴシエートされた利用可能な帯域幅。

フィールド	フィールドの説明
Transmit bit rate	このフィールドは、ビデオ送信ストリームとコンテンツ送信ストリームにのみ適用され、Cisco TelePresence Server がその時点で送信しようとしているビット レートを表します。Cisco TelePresence Server から送信されるビデオ データを単純に測定したレートである実ビット レートがカッコ内に表示されます。
Packets sent / reported lost	エンドポイント宛ての音声/ビデオ/コンテンツ パケットの数。2 つ目の数値は、エンドポイントから報告された、エンドポイントで受信されなかったパケットの数です。
Frame rate	このフィールドは、ビデオ ストリームとコンテンツ ストリームに適用されます。エンドポイントと TelePresence Server の間で送信/受信されたストリームの 1 秒あたりのフレーム数です。
Fast update requests received	エンドポイントからこのチャネルを介して TelePresence Server で受信された Fast Update Request（FUR）の数。
ClearPath FEC	このストリームで使用された前方誤り訂正に関する統計情報。 2 つの統計情報（パーセンテージ オーバーヘッドと回復されたパケットの数）が表示されます。 パーセンテージ オーバーヘッドは、オリジナルのストリームに対する、挿入される FEC パケットの数の比率を表します。TelePresence Server がストリーム内のすべてのパケットのコピーを挿入する場合、オーバーヘッドは 100% になります。TelePresence Server がパケット 2 つにつき 1 つの割合でパケットのコピーを挿入する場合は、オーバーヘッドは 50% になり、4 つにつき 1 つの割合ならば、25% になります。TelePresence Server がこのストリームに現在 FEC を適用していない場合は、オーバーヘッドは 0% になります。 数字は、オリジナルが失われたため、エンドポイントによって TelePresence Server の FEC パケットから回復されたと報告されたパケットの数です。
ClearPath LTRF	長期参照フレームがこのストリームで使用されているかどうか。エンドポイントが TelePresence Server と ActiveControl をネゴシエートできない場合は、値が [Not supported] になります。そうでない場合は、この値が [Enabled] になり、LTRF がエンドポイントに送信され、必要に応じて使用できることを意味します。

ユーザ

ユーザ リストの表示

[Users] ページには、TelePresence Server 上に存在するすべてのユーザ アカウントの概要が表示されます。

表 34　ユーザ リストの詳細

フィールド	フィールドの説明
User ID	TelePresence Server の Web インターフェイスにアクセスするために必要なユーザ名。テキストは任意の文字セットで入力できますが、クライアントによっては Unicode 文字をサポートしていない場合があることに注意してください。
Name	ユーザの名前（省略可能なため、存在しない場合があります）。
Access rights	このユーザに付与された役割と関連する権限。3 つのレベル（[Administrator]、[API access]、および [None]）があります。 *None*：このユーザは TelePresence Server からロックアウトされています。 *API access*：このユーザはこの TelePresence Server の XML-RPC インターフェイスで API コマンドを実行できます。 *Administrator*：Web インターフェイスへの API アクセスと管理アクセスができます。

ユーザの削除

ユーザを選択してから、[Delete selected users] をクリックします。*admin* ユーザは削除できません。

ユーザの追加と更新

ユーザのリストにアクセスする（[Users] に移動する）ことによって、TelePresence Server 上でユーザ アカウントを追加、編集、および削除できます。

ユーザ アカウントを追加または編集するときに使用する情報はほとんど同じです。異なる点については、次の参照テーブルで説明します。

ユーザの追加

1. [Users] に移動します。
2. [Add new user] をクリックします。
3. 必要に応じて次の表を参照しながら、ユーザ アカウントの詳細を入力します。
4. [Add User] をクリックします。

ユーザの更新

1. [Users] に移動します。
2. ユーザ ID をクリックします。
3. 必要に応じて次の表を参照しながら、ユーザ アカウントの詳細を変更します。
4. [Modify user] をクリックします。
5. パスワードを変更する必要がある場合は、[Change password] をクリックします。

ユーザ詳細リファレンス

表 35　ユーザ詳細

フィールド	フィールドの説明	詳細情報
User ID	ユーザのログイン名または ID 番号を識別します。 この値は、TelePresence Server にアクセスするために必要なユーザ名です。	テキストは任意の文字セットで入力できますが、クライアントによっては Unicode 文字をサポートしていない場合があることに注意してください。 **注：**TelePresence Server のコンソールはすべての Unicode 文字を受け入れることができるわけではありません。コンソール アクセスに使用されるアカウントは、ASCII 文字のユーザ名とパスワードに制限されます。
Name	ユーザの名前。	オプション。
Password	このユーザのパスワードを入力します。	テキストは任意の文字セットで入力できますが、クライアントによっては Unicode 文字をサポートしていない場合があることに注意してください。
Re-enter	パスワードを再入力します。	パスワード入力フィールドは、新しいユーザを追加したときにの

フィールド	フィールドの説明	詳細情報
password		みデフォルトでアクティブになります。既存のユーザを更新する場合は、[Change password] をクリックして、次のフィールドの編集を可能にします。
Access rights	ドロップダウンからユーザの役割を選択します。役割によって次のような権限が付与されます。 *None*：このユーザは TelePresence Server からロックアウトされています。 *API access*：このユーザはこの TelePresence Server の XML-RPC インターフェイスで API コマンドを実行できます。 *Administrator*：Web インターフェイスへの API アクセスと管理アクセスができます。	

ログ

イベント ログの操作

高度なトラブルシューティングを必要とする複雑な問題が発生した場合は、TelePresence Server のログから情報を収集する必要があります。通常は、カスタマー サポートがこれらのログの収集をお手伝いします。

イベント ログ

TelePresence Server は、そのサブシステムで生成され、最近収集されたメッセージを 2000 件保存しています。これらは [Event log] ページ（[Logs] > [Event log]）に表示されます。通常は、これらのメッセージが情報として提供され、場合によって、[Warnings] または [Errors] がイベント ログに表示されます。

カスタマー サポートは、TelePresence Server の運用またはパフォーマンスに伴う特定の問題が発生した場合に、記録されたメッセージとそれらの意味をご説明いたします。

次の作業を実行できます。

- 列ヘッダーをクリックすると、イベントがソートされます。
- ページ番号をクリックすると、表示されたログが 100 イベント単位で先に進みます。
- すべてのシステム ログを単一の zip ファイルにダウンロードする：[Download system logs] をクリックします。
- イベント ログをテキストとしてダウンロードする：[Logs] > [Event log] に移動して、[Download event log] をクリックします。
- 情報を関心領域に限定するように表示のパラメータを変更します（[Logs] > [Event display filter]）。
- [Logs] > [Event capture filter] ページを編集することによって、トレースで収集する詳細のレベルを変更します。

注：イベント収集フィルタは、カスタマー サポートから指示された場合にのみ変更してください。これらの設定を変更すると、TelePresence Server のパフォーマンスが低下する可能性があります。

- イベント ログを保存または分析のためにネットワーク上の 1 つ以上の Syslog サーバに送信します。サーバは [Logs] > [Syslog] ページで定義します。
- [Clear event log] をクリックすることによってログを空にします。

イベント収集フィルタ

イベント収集フィルタは、TelePresence Server がログに保持するイベントを定義します。デフォルトで、このフィルタは、すべての TelePresence Server サブシステムから [Errors, warnings and information] を収集するように設定されます。

注：このフィルタは、カスタマー サポートからアドバイスされた場合にのみ変更してください。

たとえば、TelePresence Server の問題をトラブルシューティングするときに、サポート担当者がビデオ サブシステムの詳細なトレースを収集するように要請する場合があります:

1. [Logs] > [Event capture filter] に移動します。
2. [VIDEO] ドロップダウン リストから [Detailed trace] を選択します。

   TelePresence Server に、パフォーマンスに影響が出る可能性があることを示す警告が表示されます。
3. [OK] をクリックします（これは、問題の解決後に元に戻すことが可能な詳細情報の一時的な昇格です）。
4. [Update settings] をクリックします。

   TelePresence Server が、ビデオ サブシステムからの詳細なトレース情報に加えて、他のすべてのサブシステムに関するデフォルト情報を収集します。

イベント表示フィルタ

イベント表示フィルタは、イベント ログのサブセットを表示したり、特定のエントリを強調表示したりするために使用できます。このフィルタは保存されたエントリに適用され、収集するイベントには影響を与えません。

イベント表示フィルタを変更するには、[Logs] > [Event display filter] に移動します。

メッセージ テキストのフィルタリング

1. その文字列を含む保存されたイベントだけを表示するには、[Filter string] を入力します。
2. フィルタリング結果内の文字列の確認を容易にしたい場合は、[Highlight string] を入力します。
3. [Update display] をクリックします。

   TelePresence Server に、フィルタリングされたイベント ログと強調表示されたイベント ログが表示されます。

現在の表示レベル

TelePresence Server には多数のサブシステムが存在し、そのすべてでイベントのロギングが可能です。サブシステムごと、または、すべてのサブシステムに関して、表示する詳細情報のレベルを変更できます。

たとえば、SIP エラーにしか興味がないとします。

1. [Set all to:] ボタンとその横にあるドロップダウンが表示されるまで下にスクロールします。

2. ドロップダウンで [None] を選択します。
3. [Set all to:] をクリックします。

   すべてのサブシステムの表示レベルを [None] に変更します。
4. SIP サブシステムの横にあるドロップダウン リストから、[Errors only] を選択します。
5. [Update settings] をクリックします。

   TelePresence Server に、SIP だけが表示されます。

プロトコル メッセージのロギング

[Protocols log] ページでは、さまざまなプロトコルに関して TelePresence Server との間で送受信されるメッセージが記録されます。

メッセージの容量がパフォーマンスに影響するため、プロトコル ロギングはデフォルトで無効になっていますが、カスタマー サポートがそれを有効にしてトラブルシューティングに役立てるように要請する場合があります。

プロトコル メッセージのロギングを開始するには：

1. 記録するプロトコルを選択します。
2. [Enable protocols logging] をクリックして、それらのプロトコル メッセージの記録を開始します。
3. 解決しようとしている問題を再現するために必要なテストを実行します。
4. [Download as XML] をクリックして、ログを XML ファイルとしてサポートに送信します。

問題の解決が確認されたら、[Disable protocols logging] をクリックしてから、[Clear log] をクリックして、それ以降のユニットのパフォーマンスに対する影響を回避します。

フィールド	説明
Current status	[Enabled] と [Disabled] があります。デフォルトは [Disabled] です。
Messages logged	記録されたメッセージの数。

フィールド	説明
Protocol filters	• *BFCP* • *SIP* • *XCCP* 収集するプロトコル メッセージに対応するボックスをオンにします。これらは収集フィルタで、表示フィルタではありません。プロトコルをオフにしてからプロトコル ロギングを有効にした場合は、TelePresence Server はオフにされたプロトコルのメッセージを収集しません。 ロギングが有効になっている間は、記録するプロトコルを変更できません。収集フィルタを変更するには、ロギングを無効にして、チェックボックスを変更してから、再度ログインを有効にします。

プロトコル メッセージのリモート ロギング

プロトコル ログは、HTTP または HTTPS 経由で使用できるため、ログをリモート デバイスに記録することができます。プロトコル ロギングを有効または無効に設定しても、リモート デバイスへのログの送信は無効になりません。いつでも、最大 2 つの同時ログ ストリームを使用できます。

リモート デバイスへのプロトコル メッセージのロギングを開始するには：

1. リモート デバイスから **`http[s]://`***<ip address>*`/protocols_log_stream`** に HTTP POST 要求を送信します。この POST 要求には、有効なユーザ パラメータとパスワード パラメータ（**`authenticationUser=`***username*`&authentication`**`Password=`***password*）を含める必要があります。

   wget（Linux システムの場合）を使用した例を以下に示します。

   `Wget https://`*<IP address>*`/protocols_log_stream --post-data=authenticationUser=`***username**&authentication*`Password=`***password***

   （API のみの権限を持っているユーザが有効と見なされます）。

2. プロトコル ログの内容全体がこの TCP 接続を通してリモート デバイスに転送されます。このログ ストリームは、リモート デバイスが TCP 接続を解除するまで続きます。

syslog を使用したロギング

イベント ログは、保存または分析のためにネットワーク上の 1 つ以上の Syslog サーバに送信することができます。

syslog ファシリティを設定するには、[Logs] > [Syslog] に移動します。

Syslog 設定

Syslog 設定を構成する場合は、次の表を参照しながら行ってください。

表 36　Syslog 設定

フィールド	フィールドの説明	使用方法のヒント
Host address 1 to 4	最大 4 つの Syslog レシーバ ホストの IP アドレスを入力します。	設定済みの各ホストに送信されたパケットの数がその IP アドレスの横に表示されます。
Facility value	Syslog ホスト上の Cisco TelePresence Server からのイベントを識別するために設定可能な値。次のオプションから選択します。 • *0 - カーネル メッセージ* • *1 - ユーザ レベルのメッセージ* • *2 - メール システム* • *3 - システム デーモン* • *4 - セキュリティ/認可メッセージ（注 1 を参照）* • *5 - syslogd によって内部的に生成されるメッセージ* • *6 - ライン プリンタ サブシステム* • *7 - ネットワーク ニュース サブシステム* • *8 - UUCP サブシステム* • *9 - クロック デーモン（注 2 を参照）* • *10 - セキュリティ/認可メッセージ（注 1 を参照）* • *11 - FTP デーモン* • *12 - NTP サブシステム* • *13 - ログ監査（注 1 を参照）* • *14 - ログ アラート（注 1 を参照）* • *15 - クロック デーモン（注 2 を参照）* • *16 - ローカル使用 0（local0）* • *17 - ローカル使用 1（local1）* • *18 - ローカル使用 2（local2）* • *19 - ローカル使用 3（local3）* • *20 - ローカル使用 4（local4）*	Cisco TelePresence Server として記憶しておく値を選択します。 **注 1：**さまざまなオペレーティング システム デーモンとプロセスが、同様と見なされているセキュリティ/認可、監査、およびアラートの各メッセージにファシリティ 4、10、13、および 14 を使用しています。 **注 2：**さまざまなオペレーティング システムが、クロック（cron/at）メッセージにファシリティ 9 と 15 の両方を使用しています。 明示的にファシリティ値が割り当てられていないプロセスとデーモンは、"ローカル使用" ファシリティ（16 または 21）のどちらかを使用する場合と "ユーザ レベル" ファシリティ（1）を使用する場合があります。これらの値のいずれかを選択することをお勧めします。

フィールド	フィールドの説明	使用方法のヒント
	• *21 - ローカル使用 5（local5）* • *22 - ローカル使用 6（local6）* • *23 - ローカル使用 7（local7）*	

syslog の使用

syslog レシーバ ホストに転送されるイベントは、イベント ログ収集フィルタによって制御されます。

syslog サーバを定義するには、その IP アドレスを入力してから、[Update syslog settings] をクリックします。設定済みの各ホストに送信されたパケットの数がその IP アドレスの横に表示されます。

注：イベントごとに次のような重大度指標が設定されます。

- 0 - 緊急：システムが使用不能（Cisco TelePresence Server では未使用）
- 1 - アラート：すぐに対処すべき（Cisco TelePresence Server では未使用）
- 2 - 重大：危機的状態（Cisco TelePresence Server では未使用）
- 3 - エラー：エラー状態（Cisco TelePresence Server の*エラー*イベントで使用）
- 4 - 警告：警告状態（Cisco TelePresence Server の*警告*イベントで使用）
- 5 - 通知：正常だが有意状態（Cisco TelePresence Server の*情報*イベントで使用）
- 6 - 情報：情報メッセージ（Cisco TelePresence Server の*トレース*イベントで使用）
- 7 - デバッグ：デバッグ レベルのメッセージ（Cisco TelePresence Server の*詳細トレース*イベントで使用）

呼詳細レコードの操作

TelePresence Server は、最大 2000 件の呼詳細レコードを表示できます。ただし、TelePresence Server は呼詳細レコードを長期保存するように設計されていません。CDR ログを保持する場合は、それをダウンロードして別の場所に保存する必要があります。

CDR ログがいっぱいになると、最も古いログが上書きされます。

CDR ログを表示して管理するには、[Logs] > [CDR log] に移動します。使用可能なオプションの詳細と表示される情報の説明については、次の表を参照してください。

- 呼詳細レコード ログの管理
- 呼詳細レコード ログ

呼詳細レコード ログの管理

CDR ログには大量の情報を書き込むことができます。このセクション内のコントロールは、表示する各自にとって最も有益な情報を選択するのに役立ちます。変更を終了したら、[Update display] をクリックして、変更を有効にします。オプションの説明については、次の表を参照してください。

表 37　ステータスと表示

フィールド	フィールドの説明	使用方法のヒント
Messages logged	ログ内の現在の CDR の数。	
Filter records	TelePresence Server で記録された CDR レコード タイプのリスト。	このボックスをオフのままにすると、すべてのレコードが表示されます。または、興味のあるレコード タイプのボックスをオンにします。
Filter string	このフィールドは、表示する呼詳細レコードの範囲を制限する場合に使用します。フィルタ文字列は大文字と小文字が区別されません。	フィルタ文字列は、ログ表示の [Message] フィールドに適用されます。特定のレコードの詳細が展開されていた場合は、フィルタ文字列がそれらにも適用されます。
Expand details	デフォルトで、CDR ログには各イベントの簡単な説明しか表示されません。利用可能な場合は、詳細を表示するためのオプションをリストの中から選択します。	[All] を選択すると、その他のオプションが選択されているかどうかに関係なく、すべてのメッセージの詳細が最も多く表示されます。

呼詳細レコード ログ

呼詳細レコード ログは、複数ページにまたがる長い表として表示され、最大 2000 行で構成されます。上記のフィルタリングに加えて、次のような方法でもログをナビゲートできます。

- 特定の列で昇順または降順にソートするには、その列ヘッダーをクリックします。

- 特定の会議または参加者 GUID に関連したすべてのレコードのログをフィルタリングするには、その GUID をクリックします（[Show all] をクリックすると、このフィルタが元に戻ります）。
- 表示されたレコードのリスト内の特定のページにジャンプするには、そのページ番号をクリックします。

ログをテキスト エディタで編集したり、将来の参照用としてアーカイブしたりするには、[Download as XML] をクリックします。このボタンは、現在保存されている*すべてのレコードをダウンロード*します。Web ページで設定された表示フィルタは無視されます。

注：ユニットに高い負荷がかかっている間は CDR ログをダウンロードしないでください。パフォーマンスが低下する可能性があります。

ログ メモリを空にするには、[Clear all records] をクリックします。

注意：[Clear all records] は、TelePresence Server から*すべてのレコードを完全に削除します*。クリアしたレコードを回復することはできません。

CDR ログ リファレンス

次の表に、CDR ログ内のフィールドの説明を示します。

表 38　CDR ログの詳細

フィールド	フィールドの説明	使用方法のヒント
# (record number)	この呼詳細レコードの一意のインデックス番号。	
Time	呼詳細レコードが作成された時刻。	レコードは会議イベントが発生するたびに作成されます。レコードが作成された時刻は、イベントが発生した時刻です。 入力 CDR ログ イベントは、現地のタイムスタンプ（UTC ではない）と一緒に保存されます。 時刻を変更する（システム時刻を変更するか、NTP 更新を介して）と、CDR ログ内の新しいイベントに新しい時刻が表示されます。既存のレコードのタイムスタンプは変更されません。
Conference	このレコードが適用される会議の GUID。	新しい会議は、グローバル一意識別子（GUID）を使って作成されます。特定の会議に関連したすべてのレコードにこの ID が表示されるため、会議イベントの監査を大幅に簡素化することができます。 GUID をクリックすると、その会議に関連したレコードだけが表示されます。

フィールド	フィールドの説明	使用方法のヒント
Participant	このレコードが適用される参加者の GUID。	参加者はグローバル一意識別子（GUID）別に表示されるため、レコード管理が容易になります。 GUID をクリックすると、その参加者に関連したレコードだけが表示されます。
Message	呼詳細レコードのタイプと、入手可能な場合の簡単な説明。	[>>] をクリックすると、そのタイプのすべてのメッセージの詳細が展開されます。これをすべてのメッセージに対して実行するには、[All] を選択して [Update display] をクリックします。これは、[Filter string] と組み合わせて、メッセージに特定の単語が含まれているレコードを見つけるのに役立ちます。

API クライアント

TelePresence Server は、ユニットに要求を発行した最新の 10 台の API クライアントを記録します。このリストを表示するには、[Logs] > [API clients] をクリックします。

5 分を超える期間 API 要求を発行していないクライアントは灰色表示されます。

[Refresh] をクリックして、API クライアントのリストを更新します。すべてのデータをクリアするには、[Reset statistics] をクリックします。これにより、API クライアントの現在のリストがクリアされます。クライアントが新しいコマンドを送信するたびに、それらがこのリスト内に再表示されます。

デフォルトで、ページは [Time since last request] 列でソートされます。

表 39　API クライアントの詳細

フィールド	フィールドの説明	使用方法のヒント
Client IP	要求を送信するクライアントの IP アドレス。	
Time since last request	そのクライアントから最後の要求が送信された以降の時間。	
Last request method	その API クライアントから送信された最後の API 要求メソッド。	
Last request user	クライアントが API 要求内で使用したユーザ名。	最後の API 要求で認証に失敗したクライアントは、ここで [*(authentication failed)*] によって注意喚起されます。

フィールド	フィールドの説明	使用方法のヒント
Requests received since last reset	最後のリセット以降に受信された要求の数。	1 秒間に複数の要求が受信された場合は、秒単位の平均要求数がカッコ内に表示されます。 現在のしきい値は、1.8 要求/秒です。 「活動過剰な」クライアントは、TelePresence Server と通信している場合にのみ警告されます。 最後のリセット以降の経過時間がボタンの横の表の下に表示されます。

フィードバック レシーバ

TelePresence Server は、フィードバック イベントを公開して、それをリッスンしているレシーバが変化に対応できるようにします。フィードバック レシーバのリストを表示するには、[Logs] > [Feedback receivers] の順にクリックします。

[Delete all] をクリックすれば、設定されたすべてのフィードバック レシーバをクリアすることができます。この操作は取り消すことができません。

リスト内のレシーバごとに次の詳細が表示されます。

表 40　フィードバック レシーバの詳細

フィールド	フィールドの説明	使用方法のヒント
Index	レシーバのリスト内のレシーバの位置。	
Receiver URI	レシーバの完全修飾 URI。	レシーバは、適切な API コールでフィードバック イベントに応答してフィードバック送信元から変更のリストを取得可能な Cisco TelePresence Management Suite などのソフトウェア アプリケーションです。

Call Home の使用

注：TelePresence Server は、現時点で、匿名レポートしかサポートしていません。

TelePresence Server は、そのステータスと Cisco Call Home サービスで発生した障害に関するレポートを送信できます。TelePresence Server は、必ず、セキュア接続（HTTPS）を使用して、Call Home にレポートを送信します。

Call Home が無効（デフォルト設定）になっている場合は、[Call Home mode] が選択されるまで、デバイスはどのタイプのレポートも送信しません。Call Home を有効にした場合は、手動でレポートを送信することも、その機能を自動起動に設定することもできます。

Anonymous Call Home を使用している場合、匿名で送信されたレポートは表示できません。このようなレポートは、シスコのエンジニアしか使用することができず、潜在的な問題を診断する目的でのみ使用されます。

注：Call Home レポートに関する質問は、Cisco TAC までお問い合わせください。

Call Home モードとして [anonymous] を選択した場合は、[Automatic Call Home enabled] をオンにすれば、TelePresence Server から自動的にレポートを送信することができます。この変更を適用した直後に、デバイスから保留中のレポートが送信されます。その後は、自動的に、予期せぬデバイスの再起動やメディア リソースの再起動に関する診断レポートが送信されます。手動による介在は必要ありません。

Automatic Call Home を使用しない場合は、[Call Home] をクリックすれば、いつでもレポートを手動で送信できるようになります。

[Device inventory] レポートは常に使用できます。その存在が特殊な状態や障害を示しているわけではありません。Automatic Call Home が有効になっている場合は、TelePresence Server が起動時に必ずこのレポートを送信します。

Call Home を設定するには：

1. [Logs] > [Call Home] に移動します。

   [Status] セクションに、この機能が有効になっているかどうかと、現在使用可能なレポートが表示されます。
2. [Call Home mode]、[Anonymous Call Home] の順に選択します。
3. （オプション）手動の介在なしで TelePresence Server にレポートを送信させる場合は、[Automatic Call Home enabled] をオンにします。
4. [Apply changes] をクリックします。

   ダイアログが開いて、[Are you sure you want to apply configuration changes?] と表示されます。
5. [OK] をクリックして先に進むか、[Cancel] をクリックして設定の変更を破棄します。

   Automatic Call Home が有効になっている場合は、TelePresence Server が保留中のレポートを直ちに送信します。
6. （オプション）現在のレポートを手動で送信する場合は、[Call Home now] をクリックします。

表 41　ステータス フィールド

フィールド	説明
Call Home status	次のいずれかとして Call Home ステータスを示します。 • *Automatic – Anonymous Call Home*：**Call Home モード**が有効になっており、[Automatic Call Home enabled] がオンになっています。 • *Enabled – Anonymous Call Home*：**Call Home モード**が有効になっており、[Automatic Call Home enabled] がオフになっています。 • *Disabled*（デフォルト） 起動時に **Call Home モード**が無効になっている場合は、TelePresence Server が起動中にイベント ログにこれを記録します。TelePresence Server は、**Call Home モード**が有効になっている（*Anonymous Call Home*）が、自動的にレポートを送信するように設定されていない場合は、メッセージも記録します。
Current reports	使用可能なレポートのリスト。
Submission status	日付と時刻を含む、最新のレポート送信のステータスを示します。 レポートが送信されていない場合は、ステータスが [Not sent] になります。
Last submitted report reference	このフィールドは、[Unexpected media resource restart diagnostics] または [Unexpected device restart diagnostics] レポートが送信されたことがある場合にのみ表示されます。この参照番号を Cisco TAC に提出すれば、レポートの分析が可能になります。
Call Home now	手動で**現在のレポート**を送信します。 手動でレポートを送信するか、自動レポートを有効にすると、そのデータがシスコに送信されることを伝える確認ポップアップが表示されます。 レポートの送信は 3 回試行されます。3 回目の送信が失敗したら、Web インターフェイス上にバナーが表示されます。

表 42　設定フィールド

フィールド	説明
Call Home mode	*Anonymous Call Home* を有効にします （デフォルトは [Disabled] で、どのレポートも送信できません）。
Automatic Call Home enabled	必要に応じて、TelePresence Server に診断レポートの送信を許可します。また、TelePresence Server に起動中のインベントリ レポートの送信を許可します。

参照先

コンテンツ チャネル サポート

ほとんどの TelePresence エンドポイントが 2 つ目のビデオ チャネル（コンテンツ チャネル）の使用をサポートしています。通常、これはライブ ビデオと同時に実行するプレゼンテーションで使用されます。

- SIP システムは、コンテンツに BFCP というプロトコルを使用します。
- Cisco CTS システムなどの TIP システムは、TIP を使用してコンテンツ共有を制御します。

TelePresence Server は、メイン ビデオ内のコンテンツを許可することによって、2 つ目のビデオ チャネルをサポートしていないエンドポイントに対処します。この機能が有効になっている場合は、TelePresence Server がこのようなエンドポイントにメイン ビデオ チャネルでコンテンツを送信します。コンテンツ チャネルがアクティブの間は、コンテンツ チャネルが標準のビデオで構成されます（コンテンツが一番大きいペインに表示され、他の参加者のビデオ ストリームがディスプレイの下部にある連続表示ペインに配置されます）。

レイアウト ビューでの参加者の表示方法について

注：TelePresence Server がリモート管理モードで動作している場合は、TelePresence Server のユーザ インターフェイスからこれらのオプションを設定することができません。

このページの内容

会議のレイアウト

TelePresence Server によって選択されるシステム用のレイアウトは、システム内の画面の数と他の会議参加者の特性によって異なります。エンドポイントは、遠端カメラ制御または DTMF キーの 2 と 8 を使用してレイアウトを選択することも、次の選択肢の中から事前に設定することもできます。TelePresence Server は、1、2、3、および 4 画面の標準エンドポイントと没入型エンドポイントを操作して、会議に参加しているこれらのシステムの組み合わせをその会議内の他のタイプのシステムに表示することができます。

TelePresence Server の通常の動作は、「最も声の大きい」参加者を最も人目を引くレイアウトのペインに表示することです。使用可能なペインの数よりコントリビュータの数の方が多い場合は、「最も声の小さい」参加者が表示されなくなります。

1 画面システムに送信されるレイアウト

デフォルト レイアウトは、ボックス幅と参加者単位のどちらかで設定できます。このデフォルト設定は、参加者が遠端カメラ制御を使用して、または、DTMF キー の 2 と 8 を介して、レイアウト選択を変更することによって上書きされます。

ActivePresence レイアウトでは、最も声の大きい参加者が全画面で表示され、その他の参加者が画面下部にある最大 6 つの同じ大きさのオーバーレイ ペインに表示されます。その他の参加者は参加者オーバーフロー アイコンで示されます。

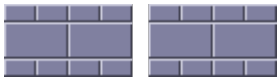
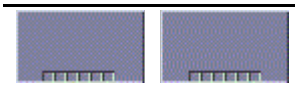
TelePresence Server は、[Default layout type for single-screen endpoints] の設定に従って、1 画面エンドポイント用のレイアウトを表示します。

表 43　1 画面エンドポイントに送信されるレイアウト

	*Single*：エンドポイントが 1 つの全画面ペインに表示されます。
	*ActivePresence*：エンドポイントが 1 つの全画面ペインに表示され、その他の参加者が画面下部にある最大 6 つの同じ大きさのオーバーレイ ペインに表示されます。その他の参加者は、表示されていない参加者の数と一緒に、右下の参加者オーバーフロー アイコンで示されます。
	*Prominent*：エンドポイントが 1 つの大きなペインに表示され、その他の参加者が画面下部にある最大 6 つの同じ大きさのオーバーレイ ペインに表示されます。その他の参加者は、表示されていない参加者の数と一緒に、右下の参加者オーバーフロー アイコンで示されます。
	*Equal*：エンドポイントが同じ大きさのペインのグリッド パターン（最大 4X4）で表示されます。 ペインの行ごとに、リモート マルチスクリーン システムの画面またはリモート システムと一部の画面の組み合わせを表示できます。

2 画面システムに送信されるレイアウト

表 44　2 画面システムに送信されるレイアウト

	TelePresence Server が部屋切り替え表示モードの場合は、3 または 4 画面の TelePresence システムが会議に参加していれば、TelePresence Server がこのレイアウトをその会議に参加している 2 画面システムに送信します。 4 つのペインの行ごとに、リモート 4 画面システムの 4 つの画面またはシステムと一部の画面の組み合わせを表示できます。
	1 または 2 画面システムしか会議に参加していない場合は、TelePresence Server がこのレイアウトを使用します（すべてのビデオ ストリームの表示が使用可能なペインに収まる場合）。可能な場合は、オーバーレイ ペイン（最大 6 つ）が自動的に中央に表示されます。

3 画面システムに送信されるレイアウト

表 45　3 画面システムに送信されるレイアウト

	PiP を含まないレイアウトが使用できます。つまり、PiP の使用が禁止されます。DTMF 2 および 8/FECC を使用してそれを選択できます。
	TelePresence Server が部屋切り替え表示モードの場合は、4 画面の TelePresence システムが会議に参加していれば、TelePresence Server がこのレイアウトをその会議に参加している 3 画面システムに送信します。 4 つの大きなペインの中央の行に、リモート 4 画面システムの 4 つの画面または 1、2、および 3 画面の会議参加者の組み合わせを表示できます。この行を正確に中央に配置するために、TelePresence Server は、3 つの画面の中央にペインを表示し、左端の画面の左側または右端の画面の右側を使用しません。
	4 画面の TelePresence システムが会議に参加していない場合は、TelePresence Server がこのレイアウトをその会議に参加している 3 画面システムに使用します。

4 画面システムに送信されるレイアウト

TelePresence Server は、このレイアウトを会議に参加している 4 画面システムに送信します。

4 つのペインの行（4 つの全画面、または、6 つの小さなオーバーレイ ペインの行の 1 つで構成された行）ごとに、4 画面システムまたはリモート システムと一部の画面の組み合わせを表示できます。可能な場合は、オーバーレイ ペインが自動的に中央に配置されます。

ビューのレイアウトに影響するエンドポイント設定オプション

セルフ ビュー設定

エンドポイントの [Self view] 設定では、TelePresence Server がそのエンドポイント上でそれ自体のビデオ ストリームを表示するかどうか、つまり、参加者が自分自身を表示できるかどうかが決定されます。この設定が選択されなかった場合は、エンドポイントにそれ自体のビデオ ストリームが表示されません。

エンドポイントにそれ自体のビデオの表示を許可した場合は、TelePresence Server が使用可能なビュー ペインに参加者を配置するときに、その参加者がコール内で最も声が大きい参加者であっても（つまり、他の会議参加者から目立つ場所に表示されていても）、必ずセルフ ビューの最後に配置します。

1 画面エンドポイントの全画面ビューの表示

参加者をレイアウト ペイン内に配置するときに、TelePresence Server は、「最も声の大きい」人物を最も人目を引くペインに配置してから、「最も声の小さい」人物をより小さいペインに配置します。ただし、TelePresence システム（大型の高解像度ディスプレイを使用することが多い）と低品質のビデオに対応したシステム（ビデオ対応携帯電話など）を組み合わせた会議では、低解像度参加者を大きな全画面ペインに表示することはお勧めできません。

1 画面システムの場合は、[Show full screen view of single-screen endpoints] 設定によって、エンドポイントを大きな全画面ペインに表示するかどうかまたはその方法が決定されます。使用可能な設定は、[Always]、[Dynamic]、および [Disabled] です。

- *Always*：1 画面エンドポイントが常にマルチスクリーン エンドポイントのメイン ペインの占有を許可されます。
- *Dynamic*：1 画面エンドポイントが、他のマルチスクリーン エンドポイントが会議に参加していない場合に、マルチスクリーン エンドポイントのメイン ページに表示されます。マルチスクリーン エンドポイントが会議に参加している場合は、1 画面エンドポイントが PiP ストリップに格下げされます。
- *Disabled*：1 画面エンドポイントがマルチスクリーン エンドポイントのメイン ペインに表示されることはありません。

この設定は、マルチスクリーン エンドポイントとエンドポイント グループでは表示されません。

メイン ビデオ内のコンテンツの許可

この機能を使用すれば、TelePresence Server から、追加チャネルをサポートしておらず、それ以外の方法ではコンテンツを参照できないエンドポイントのメイン ビデオ チャネルで会議のコンテンツを送信することができます。

コンテンツ チャネル ストリームには、メイン ビデオ チャネルで表示される、この編成済みのレイアウトの一番大きいペインが与えられます。最大 6 人の他の参加者の連続表示ペインは、コンテンツ ストリームの下のレイアウトの一番下に表示されます。連続表示ペインが中央に配置されます。

エンドポイント設定の周りの境界線の表示

[Show borders around endpoints] が有効になっている場合は、小さいペインに表示された参加者の周りに境界線が表示されます。全画面ペインに表示された参加者の周りには境界線が表示されません。

会議で発言中の参加者の周りには青色の境界線が、それ以外は灰色の境界線が表示されます。たとえば、全員がミュートされている場合や誰も発言していない場合は、会議で強調表示されるアクティブ スピーカーはいません。

エンドポイントに対してこの設定を有効にすると、そのエンドポイントに送信されたビデオ レイアウトで境界線が使用されます。ただし、この参加者が常に他の参加者との境界線内に表示されるとは限りません。これらの他の参加者のビューでは、個別の [Show borders around endpoints] 設定が使用されます。

参加者を「重要」としてマーキングする

会議ごとに 1 人ずつのアクティブな参加者を「重要」として設定できます。これは、TelePresence Server が、どのレイアウト ペインにどのコントリビュータを表示するかを決定するときに、声の大きさ順に設定されたリストの位置ではなく、その参加者を優先することを意味します。会議ステータスの表示でエンドポイント制御設定を参照してください。

ミュートした参加者

音声ミュート

Web インターフェイスから自分の音声をミュートしている参加者は会議に音声を出力しません。加えて、ミュートした参加者は、TelePresence Server がビュー レイアウト ペインに参加者を配置するときに、ミュートしていない参加者のあとに考慮されます。

その参加者がミュートしていることを他の参加者は認識しないことに注意してください。その参加者の話声が聞こえないだけです。

ビデオ ミュート

Web インターフェイスから自分のビデオをミュートしている参加者は会議にビデオを出力しません。音声は通常どおりに出力します（別にミュートされていなければ）。

高度なレイアウト エクスペリエンス

TelePresence Server は、デフォルトで、マルチストリーム ビデオをサポートします。

これは、マルチストリーム対応エンドポイントがビデオ ストリームを会議レイアウトにローカルに組み込むことによって、ユーザ エクスペリエンスが向上することを意味します。ただし、すべてのエンドポイントが可能な限り最良のエクスペリエンスでサポートされます。

これを実現するために、TelePresence Server は、複数のストリームを送信可能なことをアドバタイズして、マルチストリーム対応エンドポイントが必要なストリームにサブスクライブできるようにします。

TelePresence Server は、同じビデオ ソースのマルチストリーム対応エンドポイントから最大 4 本のメイン ビデオ ストリームを別々の解像度とフレーム レートで受信することができます。たとえば、エンドポイントは 1080p30 と 720p60 の両方または 720p30 と 480p30 の両方を送信できます。

TelePresence Server は、最大 16 本のビデオ ストリームを別々の解像度とフレーム レートでエンドポイントに送信できます。その後で、マルチストリーム対応エンドポイントがそのビデオ ストリームを会議レイアウトにローカルに組み込みます。

この機能に関する留意点を以下に示します。

- Cisco TelePresence Server on Virtual Machine と Cisco Multiparty Media 310/320 上のリモート管理モードでしかサポートされません。
- TelePresence Server は、マルチストリーム エンドポイントとシングルストリーム エンドポイントの両方を使用した会議をサポートします。
- スイッチド メディア ストリームの暗号化を提供します。
- 前方誤り訂正とレート制御を使用したマルチストリーム コールの復元が可能です。
- マルチストリームは SIP 経由でのみサポートされます（H.323 や TIP 経由ではサポートされません）。
- デフォルトではイネーブルです。ただし、これは API `multistreamMode` パラメータを使用して無効にすることができます。
- TelePresence Server は、マルチストリーム対応エンドポイントとの間でビデオ ストリームを送受信するための H.264 SVC チャネルの使用をサポートします。
- マルチストリームは、カスケード リンク経由ではサポートされません。
- マルチストリームは、すべてのトークン レベルに対してサポートされます。ただし、メイン ビデオ ビット レートは 500 kbps 以上にする必要があります。

注：

- TIP エンドポイントは、アクティブ スピーカー セグメントのみを表示することによって、マルチストリーム対応エンドポイント上に表示されます。
- グループ化されたエンドポイントが会議に参加している場合は、すべてのエンドポイントがトランスコード モードに切り替えられます。

エンドポイント タイプ

表 46　エンドポイント タイプ

エンドポイント タイプ（UI に表示される）	ハードウェア名/モデル番号
規格	標準のビデオ エンドポイント、以下に例を示します。 • EX60 / EX90 • C シリーズ コーデック（C20、C40、C60、C90） • Cisco Jabber • Microsoft Lync[MicrosoftLync] • その他の非 TIP サードパーティ エンドポイント TelePresence Server でエンドポイント タイプが不明な場合にも表示されます。
カスケード	別の TelePresence Server（Media 310/320、MSE 8710、または Cisco TelePresence Server on Virtual Machine）へのカスケード コール
N 個のエンドポイントのグループ	エンドポイントのグループ。リストには個別のグループ メンバーは含まれません。

レガシー TIP エンドポイント	• レガシー ソフトウェア（CTS 1.6/1.7 ～ 1.7.3）を実行している Cisco CTS システムの不明なタイプ
	• レガシー ソフトウェア（CTS 1.6/1.7 ～ 1.7.3）を実行している Cisco CTS 1 画面システム
	  • CTS 500
	  • CTS 1000
	  • CTS 1100
	• 次のような、レガシー ソフトウェア（CTS 1.6/1.7 ～ 1.7.3）を実行している Cisco CTS 3 画面システム
	  • Cisco TelePresence System 3000 シリーズ（CTS 30x0）
	  • Cisco TelePresence System 3200 シリーズ（CTS 32x0）

SIP テレプレゼンス	CTS 1.7.4 以降を実行している Cisco CTS またはその他の TIP 対応システムの不明なタイプ
SIP 1 画面テレプレゼンス	次のような、CTS 1.7.4 以降を実行している Cisco CTS またはその他の TIP 対応 1 画面システム • CTS 500 • CTS 1000 • CTS 1100

エンドポイント タイプ（UI に表示される）	ハードウェア名/モデル番号
SIP 3 画面テレプレゼンス	次のような、CTS 1.7.4 以降を実行している Cisco CTS またはその他の TIP 対応 3 画面システム • Cisco TelePresence System 3000 シリーズ（CTS 30x0） • Cisco TelePresence System 3200 シリーズ（CTS 32x0） • Cisco TelePresence TX9000 • Cisco TelePresence TX9200
マルチストリーム	シスコがサポートするマルチストリーム対応エンドポイント。

エンドポイントの相互運用性

表 47　エンドポイント機能のサポート

機能	この機能をサポートするエンドポイント	注意
パネル切り替えレイアウトの最も声の大きい参加者の特定	T3、CTS 3200、CTS 3000、TX9000、TX9200	CTS 1300 とエンドポイント グループは、最も声の大きい参加者を特定しません。 **注**：T3 システムによっては、位置オーディオ（つまり、T3 Custom）を提供できない場合があります。
レガシー TIP エンドポイントの追加	• CTS 500 • CTS 1000 • CTS 1100 • CTS 1300 • CTS 3000 • CTS 3010 • CTS 3200 • CTS 3210	CTS ソフトウェアのバージョン 1.6.x または 1.7.x（1.7.3 以前）を実行しているエンドポイントは [Add legacy TIP endpoint] を使用して追加する必要があります。 CTS ソフトウェアのバージョン 1.7.4 以降を実行しているエンドポイントは [Add new endpoint] を使用して追加することができます。 **注**：エンドポイントは、ローカル管理モードでしか追加することができません。これは、リモート管理モードでは事前に設定されたエンドポイントが許可されないためです。

機能	この機能をサポートするエンドポイント	注意
会議終了通知	• CTS 500 • CTS 1000 • CTS 1100 • CTS 1300 • CTS 3000 • CTS 3010 • CTS 3200 • CTS 3210 • TX9000 • TX9200	これらのエンドポイントは、TelePresence Server から通知を受け取ると独自の会議終了警告を生成します。また、他のタイプのエンドポイントと同様に、オーバーレイ メッセージの代わりにアイコンを表示します。

クラスタリングについて

クラスタは、スタックとも呼ばれる 2 台の Media 310/320 アプライアンスのグループであり、ケーブル（MCU 5300 シリーズ スタッキング ケーブル）で接続することにより、単体のユニットとして動作できます。

クラスタは、クラスタ内の両方のアプライアンスの総合スクリーン ライセンス カウントを提供します。この多めのスクリーン カウントは、参加者を増やした会議や複数の小規模会議をセットアップする柔軟性を提供します。

TelePresence Server Media 310/320 クラスタの概要

TelePresence Server ソフトウェアを実行している Cisco Multiparty Media 310/320 プラットフォームはクラスタリングをサポートします。最大 2 台の Media 310/320 アプライアンス（一方がマスターで、もう一方がスレーブ）をクラスタ化できます。

これらのアプライアンスを使用してクラスタを作成する場合に同じハードウェアを使用する必要はありません。Media 310 と Media 320 をクラスタ化できます。この場合は、Media 320 をマスターに設定することをお勧めします。

マスター TelePresence Server

クラスタ内の TelePresence Server ごとに割り当てられるスクリーン ライセンスは、マスターによって「継承」されます。クラスタ内のすべての容量がマスターによって制御されます。マスター経由で Web インターフェイスと API のどちらかを使用してクラスタの機能を制御する必要があります。

クラスタとエンドポイント間のすべてのコールがマスターから発信されます。

スレーブ TelePresence Server

スレーブ TelePresence Server には、完全な Web インターフェイスが表示されません。ネットワーク設定やロギング設定を構成するページや、ソフトウェアをアップグレードするページなどの一部の設定ページが使用できます。

同様に、スレーブ TelePresence Server は、API コマンドのフルセットに対応していません。詳細については、関連する API マニュアルを参照してください。

クラスタ化された TelePresence Server のアップグレード

クラスタ内のすべてのユニット上の TelePresence Server ソフトウェアをアップグレードする必要がある場合は、クラスタ内のユニットごとに新しいソフトウェア イメージをアップロードしてから、マスターを再起動します。スレーブは、自動的に再起動して、アップグレードが完了します。

一般的な留意点

クラスタリングに関して注意すべきポイントを以下に示します。

- Media 310/320 アプライアンスをクラスタ化する場合は、*クラスタ サポート*機能キーが必要ありません。
- TelePresence Server on Media 310/320 と MCU 5300 シリーズをクラスタ化するには、5300 シリーズ アプライアンス上の MCU ソフトウェアを Media 310/320 上で実行している TelePresence Server の同じビルドに置き換える必要があります。MCU 5300 シリーズ上の MCU ソフトウェアの交換に関するガイドを入手するには、TelePresence Server インストレーション ガイドのサイトにアクセスしてください。
- クラスタ内の Media 310/320 アプライアンスのそれぞれにクラスタの役割（*マスター/スレーブ*）をその Web インターフェイス（[Configuration] > [Cluster configuration]）を介して割り当てる必要があります。1 台のアプライアンスで障害が発生した場合は、それを交換すれば、クラスタ設定が継承されますが、アクティブ コールと会議は次のような影響を受けます。
  - マスターを再起動または削除すると、スレーブも再起動します。その結果、すべてのコールと会議が終了します。
  - スレーブで障害が発生した場合は、コールがドロップされるか、音声のみの参加に制限されます。

TelePresence Server の会議容量について

このトピックには、Cisco TelePresence Server のすべてのタイプに関する情報が含まれています。特定のモデルに関連した情報を探してください。

ライセンス キーとスクリーン ライセンス

TelePresence Server のライセンス供与モデルは、ライセンス アクティベーション キーの形で購入され提供される「スクリーン ライセンス」に基づきます。スクリーン ライセンスは、TelePresence Server の会議容量を使用可能にします。最大数のライセンスを適用することによって、TelePresence Server の最大容量が使用可能になります。この最大数は、次のように、ハードウェア プラットフォームによって異なります。

ハードウェア プラットフォーム	スクリーン ライセンスの最大数
TelePresence Server MSE 8710	12
2、3、または 4 台の TelePresence Server MSE 8710 のクラスタ	それぞれ、24、36、または 48
TelePresence Server 7010	12
TelePresence Server on Media 310	6
2 台の TelePresence Servers on Media 310 のクラスタ	12
TelePresence Server on Media 320	12
TelePresence Servers on Media 310 および Media 320 の混合クラスタ	18
2 台の TelePresence Servers on Media 320 のクラスタ	24
TelePresence Server on Virtual Machine（8 コア）	4
TelePresence Server on Virtual Machine（8 コア、HD）	5
TelePresence Server on Virtual Machine（30 vCPU/高密度 VM）	10
TelePresence Server on Media 400v	18
TelePresence Server on Media 410v	27

TelePresence Server MSE 8710 をライセンスする場合は、スーパーバイザの Web インターフェイスを介してライセンス キーをシャーシに適用してから、それらのブレードを収容しているスロットにスクリーン ライセンスを割り当てます。

その他のプラットフォームをライセンスする場合は、TelePresence Server の独自の Web インターフェイス（[Configuration] > [Upgrade] ページ）を介してライセンス キーを適用します。

クラスタのライセンス

TelePresence Server MSE 8710 ブレードのクラスタをライセンスする場合は、ブレードのスロットごとにライセンスを割り当てることをお勧めします。実際には、アクティブにされたスクリーン ライセンスは、使用可能なスクリーン ライセンスの数がクラスタ内のブレードに割り当てられたスクリーン ライセンスの合計になるように、効率的にプールされ、クラスタ内のマスター ブレードに割り当てられます。

TelePresence Servers on Media 310/320 プラットフォームのクラスタをライセンスする場合は、ユニットごとにライセンス キーを適用することをお勧めします。実際には、スレーブがダウンしてもマスターがすべてのライセンスを管理しますが、将来的にユニットを分離する必要がある場合やいずれかのユニットで重大な障害が発生した場合は、クラスタの分離後のユニットをカバーする個別のライセンスを持つことになります。

動作モード

TelePresence Server 7010 と MSE 8710 用の 2 つの動作モード（リモート管理モードとローカル管理モード）があります。動作モードは、同時コールをホストするためにスクリーン ライセンスをどのように容量に転換するかに影響します。

注：TelePresence Server on Media 310/320 と Cisco TelePresence Server on Virtual Machine はローカル管理モードをサポートしません。また、これらのプラットフォームでは、TelePresence Server を Cisco TelePresence Conductor や Cisco TelePresence Exchange System などのシステムで管理する必要があります。

リモート管理モードに関して提供される情報は、インストールされたソフトウェアにローカル/リモート管理モードの概念がない場合でも、Media 310/320 プラットフォームと Virtual Machine プラットフォームに関係します。

ローカル管理モード（7010 と MSE 8710 のみ）

各スクリーン ライセンスは、TelePresence Server とエンドポイント間の一定のコール数に転換されます。これは、HD モードに応じて、スクリーン ライセンスあたり 1 コールまたは 2 コールにすることができます。

- 「フル HD」モードのライセンスを使用すれば、音声チャネルとコンテンツ チャネルが関連付けられた 1 コール（最大 1080p30 または 720p60 のビデオ）が使用できます。
- 「HD」モードのライセンスを使用すれば、音声チャネルとコンテンツ チャネルが関連付けられた 2 コール（最大 720p30 または w448p60 のビデオ）が使用できます。

たとえば、6 スクリーン ライセンスを持つローカル管理モードの TelePresence Server 7010 は、最大 6 コール（最大 1080p30）または最大 12 コール（最大 720p30）をホストできます。

TelePresence Server ユニットごとに、ビデオ ポート、音声専用ポート、およびコンテンツ ポートの数が制限されます。各ビデオ ポートには、コンテンツが使用されているかどうかに関係なく、対応するコンテンツ ポートが割り当てられます。

次の同時コール制限表に、これらのポートがローカル管理モードの TelePresence Server で使用可能な 2 つの HD モードに対してどのように割り当てられるかを示します。

リモート管理モード（すべてのモデル）

リモート管理モードでは、スクリーン ライセンスがよりきめ細かくコールに割り当てられます。スクリーン ライセンスごとに、1 つのフル HD コール（ローカル管理モードなど）または複数の低解像度コールに十分な容量が解放されます。

たとえば、1 つのスクリーン ライセンスは、1 つの 1080 コール、2 つの 720 コール、4 つの 448 コール、または 8 つの 360 コールに十分な容量を提供します。

コール制限

次の表に、上で説明した動作モードのそれぞれにおける TelePresence Server のコール容量を示します。

ローカル管理モードでの同時コール制限（7010 と MSE 8710 のみ）

表 48　HD モードでのハードウェア タイプ別のポート割り当て

ハードウェアの構成	ビデオ ポート	コンテンツ ポート	音声専用ポート
7010	24	24	10
8710	24	24	10
2 台の 8710 のクラスタ	48	48	20
3 台の 8710 のクラスタ	72	72	30
4 台の 8710 のクラスタ	96	96	40

表 49　フル HD モードでのハードウェア タイプ別のポート割り当て

ハードウェアの構成	ビデオ ポート	コンテンツ ポート	音声専用ポート
7010	12	12	10
8710	12	12	10
2 台の 8710 のクラスタ	24	24	20
3 台の 8710 のクラスタ	36	36	30
4 台の 8710 のクラスタ	48	48	40

リモート管理モードでの同時コール制限

マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool（BST）の使用方法、サービス要求の送信および追加情報の収集方法については、『Cisco 製品マニュアルの最新情報（www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html）』を参照してください。

『What's New in Cisco Product Documentation』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

シスコの法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

シスコの商標または登録商標