リモート管理モードの Cisco TelePresence Server 7010 および MSE 8710

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、リモート管理モードで動作する 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 TelePresence ハードウェア上で使用できます。

- Cisco TelePresence Server 7010
- Cisco TelePresence Server MSE 8710 ブレード

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*：この権限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。	
H.323 gatekeeper status	TelePresence Server が H.323 ゲートキーパーに登録されているかどうか、およびその登録がプライマリまたは代替のゲートキーパーに行われたかどうか。	このフィールドは、TelePresence Server クラスタのマスター ブレードでのみ表示されます。
SIP registrar status	TelePresence Server が SIP レジストラに登録されているかどうか。	このフィールドは、TelePresence Server クラスタのマスター ブレードでのみ表示されます。

フィールド	フィールドの説明	使用方法のヒント
Operation mode	TelePresence Server がローカル管理モードとリモート管理モードのどちらで動作しているかを示します。	
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
TelePresence Server 8710 activation または TelePresence Server 7010 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。
Cluster support	この機能では、同じ Cisco TelePresence MSE 8000 シャーシに設定された複数の MSE 8710 ブレードをリンクして単一ユニットとして機能させることができます。 7010 プラットフォームのアプライアンスはクラスタ化できないため、このキーは適用されません。	最大 4 つのブレードで 1 つのクラスタを構成できます。「クラスタリングについて」を参照してください。 ブレードをクラスタリングする場合は、各ブレードに *クラスタ サポート*機能キーがインストールされている必要があります。 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」（79 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。	予期しない再起動または電源障害が起きた場合、またはアップグレードの後には、ログに「unknown」と表示されます。これが頻繁に発生する場合は、カスタマー サポートに問題を報告してください。

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。 **注：**8710 にはファンがないため、[Fans] フィールドは表示されません。
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 ℃ 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。

注：このクラスタ関連ページは、TelePresence Server がクラスタ内で動作している場合にのみ使用可能です。

クラスタのステータスは、Cisco TelePresence Supervisor MSE 8050 上でクラスタの一部として設定されたブレードでのみ使用可能です。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」（10 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
Slot	テーブルのこの行に対応する Cisco TelePresence MSE 8000 シャーシのスロット数。	ブレードをクラスタ内のマスターまたはスレーブとして設定するには、Supervisor にログインします。
IP	スレーブの IP アドレス。または、マスターの場合は [Master blade]。	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。
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	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
	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。 • *Cluster support not enabled*：この TelePresence Server にクラスタ サポートの機能キーがありません。 • *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。 • *Blade not configured as slave*：Supervisor でスレーブとして認識されているブレードが、マスターではスレーブとして認識されていません。スレーブ ブレードが置き換えられた可能性があります。 • *Blade incorrect type*：クラスタの設定後にスレーブ ブレードが別のブレード タイプに置き換えられた可能性があります。	
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。 スレーブ ブレード上の音声負荷は常に 0 です。マスターがすべての音声を処理します。
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 ライセンスはマスターによって制御されます。MSE シャーシでブレードをどのように使用するかによって、マスター ブレードを収納す

フィールド	フィールドの説明	使用方法のヒント
		るスロットにすべてのスクリーン ライセンスを割り当てるか、またはクラスタ内のスロット間でスクリーン ライセンスを分散させることを推奨します。スクリーン ライセンスをどのように割り当てるかはクラスタに関係ありません。マスターはすべてスクリーン ライセンスを制御し、スレーブに障害が発生しても、マスターは障害が発生したスレーブに割り当てられているすべてのスクリーン ライセンスに引き続きアクセスできます。

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

クラスタの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 で [Status] > [Cluster] ページを見ると、マスターのステータスが表示されます。

注：このクラスタ関連ページは、TelePresence Server がクラスタ内にある場合にのみ使用できます。

次の表では、クラスタ内のスレーブ TelePresence Server に表示される [Status] > [Cluster] ページについて説明します。マスター TelePresence Server については、「マスター TelePresence Server のクラスタ ステータスの表示（8 ページ）」を参照してください。

スレーブ ユニットはユーザ インターフェイスを制限しています。すべての設定が使用できるわけではありません。Cisco TelePresence Supervisor MSE 8050 からクラスタを設定する必要があります。

表 8　クラスタのステータス

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 ユニットのステータスは次のとおりです。 • [Still starting up]：マスターが起動中です。数分間待ってから、[Status] > [Cluster] ページを更新します。 • [OK]：マスターおよびスレーブが正しく通信しています。 • [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、スレーブが自動ですぐに再起動されるため、このステータスは一瞬しか表示されません。	スレーブ TelePresence Server はマスターとの接続を失うと、自動で再起動します。これは、スレーブが正しくクラスタに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なう一般的な理由として、マスターが再起動していることなどが考えられます。

フィールド	フィールドの説明	使用方法のヒント
Last seen	このフィールドは、マスターが最大 11 秒間見られなかった場合のみ表示されます。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

ネットワークの設定

TelePresence Server のネットワーク設定を行い、ネットワーク ステータスを確認するには、[Network] > [Network settings] に移動します。

このページの内容

IP 構成時の設定

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 設定が決定します。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	ポートを手動で設定するか自動で設定するかを指定します。[Automatic via DHCP] に設定すると、TelePresence Server は DHCP（Dynamic Host Configuration Protocol）を介してこのポートに対するそれ自体の IP アドレスを自動的に取得します。[Manual] に設定すると、TelePresence Server は次のフィールドでユーザが指定した値を使用します。	IPv6 を使用してログインしている場合のみ、TelePresence Server ポートで IPv4 をディセーブルにできます。
IP address	このポートのドット区切りの IPv4 アドレス（例：192.168.4.45）。	このオプションを指定する必要があるのは、前述のように IP 設定を [Manual] に設定した場合のみです。 ポート A の場合、IP 設定が [Automatic by DHCP] に設定されていれば、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（例：255.255.255.0）。	
Default gateway	このサブネットのデフォルト ゲートウェイの IP アドレス（例：192.168.4.1）。	

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] を選択すると、TelePresence Server は自動的に IPv6 アドレスを取得します。TelePresence Server は、ICMPv6 ルータ アドバタイズメント（RA）メッセージによって示される SLAAC、ステートフル DHCPv6 または ステートレス DHCPv6 を使用します（次の自動 IPv6 アドレス設定を参照）。	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 をディセーブルにします。 IPv4 を使用してログインしている場合のみ、TelePresence Server ポートで IPv6 をディセーブルにできます。
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（例：`fe80::202:b3ff:fe1e:8329`）。	アドレスを入力する必要があるのは、IP 設定を [Manual] に設定した場合のみです。[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指定します。	プレフィックス長はこのアドレスに固定されるビット数（10 進数）です。
Default gateway	（任意）このサブネットのデフォルト 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またはリンクローカルにできます。

IP ステータス

[IP status] セクションには、TelePresence Server のこのイーサネット ポートの現在の IP 設定が、自動で設定されたか手動で設定されたかどうかにかかわらず、次のように表示されます。

IPv4 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 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設定し、[Update Ethernet configuration] をクリックします。

表 11 イーサネットの構成

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も指定する必要があります。このイーサネット ポートのイーサネット設定を接続されたデバイスと自動的にネゴシエートするようにするには、[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を持つことが重要です。つまり、自動ネゴシエーションを使用するように両方のデバイスを設定するか、または同じ固定速度およびデュプレックスの設定で両方を設定します。 *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である必要があります。
Duplex	（[Manual] 設定のみ）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。	接続デュプレックスの設定は、この接続の両端のポートで同じである必要があります。 全二重モードでは同時双方向伝送が可能であるのに対し、半二重モードは同時ではない双方向伝送のみ可能です。

イーサネットのステータス

表 12 イーサネットのステータス

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。	

フィールド	フィールドの説明	使用方法のヒント
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るデバイス、またはユーザによる手動の設定に基づくデバイスにネゴシエートされます。
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るデバイス、または上記で選択した手動の設定に基づくデバイスにネゴシエートされます。
MAC address	このポートの固定ハードウェア MAC（Media Access Control）アドレス。	この値は単なる情報なので変更できません。
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 および UDP トラフィック）。	この情報を使用して、TelePresence Server がネットワークにパケットを送信しているかを確認できます。
Packets received	このポートが受信したパケットの総数（すべての TCP および UDP トラフィック）。	この情報を使用して、TelePresence Server がネットワークからパケットを受信しているかを確認できます。
Statistics:	このポートの詳細な統計情報。 • 送信されたマルチキャスト パケット • 受信されたマルチキャスト パケット • 送信されたバイトの総数 • 受信されたバイトの総数 • 受信キューのドロップ • コリジョン • 送信エラー • 受信エラー	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、ネットワーク問題の診断に役立ちます。

DNS 定義の設定

TelePresence Server の DNS 設定を確認し変更するには、[Network] > [DNS] に移動します。

新しい設定を適用するには、[Update DNS Configuration] をクリックします。

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 がそのネーム サーバ アドレスを取得する方法を選択します。 たとえば、[Via Port A DHCPv6] を選択した場合、デバイスはイーサネット ポート A に接続された IPv6 ネットワークで DHCP を使用してネーム サーバ アドレスを自動的に取得します。 [Manual] を選択した場合は、ネーム サーバ アドレスを指定する必要があります。また、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）を指定することもできます。	TelePresence Server では、選択したインターフェイスで静的 IP アドレスを設定すると、ネーム サーバ アドレスを自動的に設定することはできません。 たとえば、ここでは [Via Port A DHCPv4] を選択し、[Port A settings] ページの [IPv4 configuration] セクションで [Manual] を選択している場合、TelePresence Server によって 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。	ホスト名には最大 63 文字を使用できます。 ネットワーク設定によっては、このホスト名を使用して、IP アドレスが分からなくても TelePresence Server と通信できる場合があります。
Name server	ネーム サーバの IP アドレス	[DNS configuration] が [Manual] の場合に必要です。
Secondary name server	オプションの 2 番目のネーム サーバを識別します。	オプションの 2 番目のネーム サーバが設定されている場合、TelePresence Server はどちらかのネーム サーバに DNS クエリを送信することができます。
Domain name (DNS suffix)	DNS ルックアップの実行時に追加する任意のサフィックスを指定します。	デバイスの参照に未認定のホスト名を使用する場合は、サフィックスを追加します（IP アドレスを使用する代わりに）。 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 *エンドポイント*の IP アドレスを検索する要求をネーム サーバに行うと、実際には *endpoint.cisco.com* で検索が行われます。

DNS ステータスの表示

以下のような TelePresence Server の現在の DNS 設定を確認するには、DNS ステータス フィールドを使用します。

- ホスト名
- ネーム サーバ
- セカンダリ ネーム サーバ
- ドメイン名（DNS サフィックス）

IP ルートの設定

TelePresence Server への IP トラフィックの出入りを制御するには、1 つ以上のルートをセットアップする必要がある場合があります。

これらのルートを正しく作成することが重要です。そうしないと、コールを開始したり Web にアクセスしたりできなくなる場合があります。

ルート設定を行うには、[Network] > [Routes] に移動します。

このページの内容

IP ルートの設定

ここでは、IP パケットを TelePresence Server からどのように経路指定するかを制御できます。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場合にのみ、この設定を変更してください。

新しい IP ルートの追加

新しいルートを追加するには、次の手順を実行します。

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. それらのアドレスへのトラフィックが**ポート A** のデフォルト ゲートウェイ経由でルーティングされるか、またはユーザが指定した**ゲートウェイ**経由でルーティングされるかを選択します。
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のエイリアスである（重複する）場合は、インターフェイスによってルートを修正するよう指示されます。

参照用に次の表を使用してください。

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	このルートを適用する IP アドレスの範囲を定義する場合は、これらのフィールドを使用します。 IPv4 アドレッシング：ドット区切りの 4 つの数字列形式でターゲット ネットワークの IP アドレスを入力します。アドレスの非固定ビットは 0 に設定します。固定するビット数を指定するには [mask length] フィールドを使用します（これによって固定されないビット数が決まり、アドレスの範囲が指定されます）。 IPv6 アドレッシング：CIDR 形式でターゲット ネットワークの IP アドレスを入力します。アドレスの非固定ビットは 0 に設定します。固定するビット数を指定するには [mask length] フィールドを使用します（これによって固定されないビット数が決まり、アドレスの範囲が指定されます）。	IPv4 の例：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、マスク長を 25 に指定します。最初の 25 ビットが固定されます。これは、最後の 7 ビットによってアドレスの範囲が決定することを意味します。 IPv6 の例：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:: と入力し、マスク長を 112 と入力します。最初の 112 ビットが固定されます。これは、最後の 16 ビットによってアドレスの範囲が決定することを意味します。
Route	指定したパターンに一致するアドレス宛のパケットがどのようにルーティングされるかを制御するには、このフィールドを使用します。	[Port A] または [Gateway] を選択できます。[Gateway] を選択した場合は、パケットの宛先となるゲートウェイの IP アドレスを入力します。 [Port A] を選択した場合、一致するパケットはポート A のデフォルト ゲートウェイにルーティングされます（「ネットワークの設定」を参照）。

既存の IP ルートを表示または削除する場合

このページには、各ルートに関する次の詳細情報が表示されます。

- IP アドレスのパターンとマスク
- 一致するパケットのルーティング先（可能性を含む）
  - [Port A]：ポート A に設定されたデフォルト ゲートウェイを意味します

  - **[<IP address>]**：特定のアドレスが選択されています
- 他の設定の結果としてルートが自動的に設定されているか、またはユーザによって手動で追加されたかどうか。

*デフォルト*のルートは IPv4 および IPv6 の*デフォルト ゲートウェイの設定*で選択した内容によって自動的に設定され（「ネットワークの設定」を参照）、削除できません。手動設定したルートに一致しないアドレス宛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。

手動設定し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選択し、[Delete selected] をクリックします。

現在のルート テーブル

各テーブルには、TelePresence Server のイーサネット ポートの IPv4 および IPv6 に設定されたすべてのルート（手動および自動の両方）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

TelePresence Server の Web サービスへのアクセスを制御するには、[Network] > [Services] に移動します。

TelePresence Server は Web サービスを提供します（Web インターフェイスの場合は HTTP、コールの開始および受信の場合は SIP など）。ユニットのイーサネット インターフェイスでこれらのサービスにアクセスできるか、また TCP/UDP ポート経由でこれらのサービスを利用できるかについて管理できます。

TCP/UDP サービスのイネーブル化

どの IP バージョンが [Network] > [Network settings] ページで有効になっているかによって、IPv4 および/または IPv6 サービスを制御するオプションがあります。

1. 有効にするサービス名の隣にあるボックスをオンにするか、またはサービスを無効にするには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。

   （一般に使用されるポートの値はデフォルトで入力されます）。
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 ポートは、設定されている TCP または UDP サービス ポートの最大値よりも大きくなければなりません。たとえば、HTTPS がポート 20000 に設定されている場合、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 ポート範囲に最小のポート番号を入力します。

   デフォルト値は 49152 です。最小ポートは 10000 未満に設定できません。

2. 優先エフェメラル ポート範囲に最大のポート番号を入力します。

   デフォルトは 65535 です。これは設定可能な最大値で、デフォルトの範囲が約 15000 ポートであることを示します。TelePresence Server では、範囲を 5000 ポート未満に減らすことはできません。会議の機能が妨げられる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 で、変更された設定がページのデフォルトと置き換えられます。これら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	適切なポートでの Web アクセスを有効または無効にします。	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 ファイルを読むには、Web アクセスが必要です。
HTTPS	指定したインターフェイスでのセキュアな（HTTPS）Web アクセスを有効または無効にしたり、このサービスに使用するポートを変更します。	デフォルトでは、TelePresence Server には独自の SSL 証明書と秘密キーがあります。ただし、新しい秘密キーと証明書を必要に応じて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。
Incoming H.323	H.323 を使用して TelePresence Server への着信コールを受信する機能を有効または無効にしたり、このサービスに使用するポートを変更します。	このオプションをディセーブルにしても、TelePresence Server によって行われる H.323 デバイスへの発信コールは回避できません。
SIP (TCP)	TCP を介した SIP を使用した TelePresence Server への着信コールを許可または拒否したり、このサービスに使用するポートを変更します。	

フィールド	フィールドの説明	使用方法のヒント
Encrypted SIP (TLS)	TCP を介した SIP を使用した TelePresence Server への暗号化された着信 SIP コールを許可または拒否したり、このサービスに使用するポートを変更します。	
FTP	指定したインターフェイスでの FTP アクセスを有効または無効にしたり、このサービスに使用するポートを変更します。	FTP は、TelePresence Server の設定をアップロードおよびダウンロードするために使用できます。 組織のファイアウォール外にあるポートで FTP アクセスを無効にすることを検討する必要があります。 TelePresence Server に高度なセキュリティが必要な場合は、FTP アクセスを無効にします。
SIP (UDP)	UDP を介した SIP を使用した TelePresence Server への着信コールおよび発信コールを許可または拒否したり、このサービスに使用するポートを変更します。	このオプションをディセーブルにすると、UDP を介した SIP を使用したコールが回避されます。
Minimum	エフェメラル ポート範囲の下限。	デフォルトは 49152 ですが、最小で 10000、最大で 60535 に設定できます。
Maximum	エフェメラル ポート範囲の上限。	デフォルトは 65535 ですが、最小で 15000 に設定できます。最小範囲は 5000 ポートに制限されます。

QoS の設定

音声およびビデオ用に TelePresence Server で Quality of Service（QoS）を設定するには、[Network] > [QoS] に移動します。

QoS とは、データの特定のクラスの処理をカスタマイズするネットワークの機能を示す用語です。たとえば、QoS を使用して、HTTP トラフィックを介して音声送信およびビデオ伝送を優先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およびビデオ パケットに影響します。他のパケットはすべて QoS 0 として送信されます。

TelePresence Server では、タイプ オブ サービス（IPv4）またはトラフィック クラス（IPv6）に対し 6 ビットの値を設定でき、その値はネットワークによってタイプ オブ サービス（ToS）または差別化サービス（DiffServ）として解釈される場合があります。機能面では、IPv6 QoS は 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 設定を行うには、6 ビットの 2 進値を入力する必要があります。

ToS および DiffServ に対する値などの QoS の詳細については、Internet Engineering Task Force の Web サイト www.ietf.org で入手可能な次の RFC で確認できます。

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

このページの内容

QoS の設定について

次の表では、[Network] > [QoS] ページでの設定について説明します。

変更を行った後に、[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	ネットワークで音声データ パケットを優先するための 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	ネットワークでビデオ データ パケットを優先するための 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	ネットワークで音声データ パケットを優先するための 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	ネットワークでビデオ データ パケットを優先するための 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 の設定

ToS の設定は、優先順位、遅延、スループットおよび信頼性の抽象的なパラメータ間のトレードオフを表します。

ToS は使用可能な 8 つのビットのうち 6 つのビットを使用します。TelePresence Server では、ビット 0 ～ 5 を設定でき、ビット 6 および 7 にはゼロが配置されます。

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

ネットワーク上の他のパケットに過度の遅延を引き起こすことなく、音声パケットおよびビデオ パケットにプライオリティを割り当てることで、バランスを作成する必要があります。たとえば、すべての値を 1 に設定しないでください。

DiffServ の設定

DiffServ は、コードポイントの設定に使用可能な 8 つのビットのうち 6 つのビットを使用します。（考えられるコードポイントは 64 個あります。）TelePresence Server では、ビット 0 ～ 5 を設定でき、ビット 6 および 7 にはゼロが配置されます。コードポイントは DiffServ ノードによって解釈され、パケットの処理方法が決定します。

デフォルト設定

QoS のデフォルト設定は次のとおりです。

- **音声** *101110*:
  - ToS の場合は、IP プレシデンスが 5 に設定され、比較的高いプライオリティが与えられることを意味します。遅延は [low] に設定され、スループットは [high] に設定され、信頼性は [normal] に設定されます。
  - Diff Serv の場合は、Expedited Forwarding（EF; 完全優先転送）を意味します。

- **ビデオ** *100010*：
  - ToS の場合は、IP プレシデンスが 4 に設定され、極めて高いプライオリティが与えられることを意味します（しかし音声の優先順位よりは高くありません）。遅延は [normal] に設定され、スループットは [high] に設定され、信頼性は [normal] に設定されます。
  - DiffServ の場合は、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 をイネーブルにすると（デフォルトでイネーブルになっています）、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)] サービスの使用を選択した場合は、証明書とキーも必要です。

Cisco TelePresence Server にはローカルの証明書と秘密キーが事前にインストールされており、ユーザが HTTPS を使用してユニットにアクセスするときに、その Server はそれらを使用してブラウザに対し自身を認証します。ただし、デフォルトの証明書とキーはすべての Cisco TelePresence Server で同じであるため、セキュリティを確保するには独自の証明書と秘密キーをアップロードすることを推奨します。キーの長さは 2048 ～ 8192 ビットの間にすることを推奨します。

TelePresence Server は、暗号化パラメータを TIP エンドポイントとネゴシエートするために DTLS を使用します。これには、証明書を使用する必要があります。TelePresence Server の DTLS の実装によって、カスタマーから提供された証明書が次のように処理されます。

- カスタマーから提供された証明書がアップロードされても、状況対応型の DTLS は DTLS のネゴシエーションにデフォルトの証明書を常に使用します。
- ネゴシエートされた DTLS は、カスタマーから提供された証明書がアップロードされている場合はその証明書を使用します（これは、優先される手順です）。

ネゴシエートされた 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。それ以外の場合、TIP コールでは、状況対応型の DTLS が試行されます。

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

注：DTLS がネゴシエートされるのは、TelePresence Server に*メディア暗号化*機能キーがある場合のみです。

次の表を参考にしてフィールドに値を入力し、[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。複数の PEM エンコードされた証明機関の証明書を含む単一の信頼ストアファイルを正常な BEGIN および END 証明書タグ内に順々にアップロードすることでこれをアーカイブできます。

必要に応じて、[Delete custom certificate and key] をクリックすることで、独自の証明書およびキーを削除できます。証明書を削除した後に TelePresence Server を再起動する必要があります。

次の表に、[Network] > [SSL certificates] 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ビジネスの詳細。 • [C]：ビジネスが登録されている国。 • [ST]：ビジネスが所在する州や県。 • [L]：ビジネスが所在する地域または町。 • [O]：ビジネスの正式名称。 • [OU]：組織単位または部署。 • [CN]：証明書の共通名、またはドメイン名。	
Issuer	証明書の発行元の詳細。	証明書が自己発行された場合は、これらの詳細は [Subject] の場合と同じです。
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。	

フィールド	フィールドの説明	使用方法のヒント
Private key	秘密キーが証明書と一致するかどうか。	Web ブラウザでは、Cisco TelePresence Server に送り返すデータを暗号化するために SSL 証明書の公開キーを使用します。秘密キーは、Cisco TelePresence Server でデータを復号化するのに使用されます。[Private key] フィールドに「Key matches certificate」と表示されている場合、データは両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している場合、または証明書を生成する独自の方法がある場合は、それをアップロードできます。証明書ファイルを検索して選択するには、[Choose File] をクリックします。	証明書と秘密キーは PEM 形式にする必要があります。
Private key	証明書に付随する秘密キー ファイルを検索して選択するには、[Choose File] をクリックします。	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	秘密キーを暗号化形式で保存する場合は、Cisco TelePresence Server にキーをアップロードできるようにここにパスワードを入力する必要があります。	

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	信頼ストア証明書の詳細。通常は、ローカル証明書を確認するために使用される認証局によって発行された証明書です。	
Issuer	信頼ストア証明書の発行者の詳細。	これら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 つの理由により必要となります。 • SIP TLS 接続のリモート エンドの ID を確認するため（着信コールまたは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（たとえば、フィードバックの受信者または **`flex.participant.requestDiagnostics`** を呼び出す API アプリケーション）	信頼ストア証明書ファイルを参照して選択し、[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、リモート側の証明書が信頼ストアと対照して検証されます。リモート証明書は、信頼ストア内またはその証明書のいずれかの信頼チェーン内にある必要があります。 削除したり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。
Certificate verification settings	リモート証明書を信頼ストアで検証する必要がある状況を決定します。	次のドロップダウン オプションのいずれかを選択して、[Apply changes] をクリックします。 • [No verification]：リモート証明書は信頼ストアと対照して検証されません（リモート エンドは常に信頼されます）。 • [Outgoing connections only]：TelePresence Server は、すべての発信 SIP TLS および HTTPS 接続のリモート証明書の検証を試行します。 • [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 接続のリモート証明書の検証を試行します。 **注**：証明書の検証が有効になっている場合は、最大 12 の subjectAltNames がサポートされます。

ネットワーク接続のテスト

TelePresence Server とリモートのビデオ会議デバイス（ホスト）間のネットワークの問題をトラブルシューティングするには、[Network connectivity] ページを使用できます。

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に ping を実行し、そのデバイスへのルートをトレースできます。結果には、TelePresence Server とリモート ホスト間にネットワーク接続があるかどうかが示されます。

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、接続性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、[Test connectivity] をクリックします。

結果には、クエリに対する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の TTL（パケット存続時間）値が示されます。

TelePresence Server とリモート ホスト間の各中間ホスト（通常、ルータ）では、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。一部のデバイスは無効な ICMP 応答パケットを送信することで知られています（たとえば、無効な ICMP チェックサムによって）。無効な ICMP 応答は TelePresence Server によっても認識されていないため、これらの応答も <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 ルートがあれば、ping は成功します。この機能を使用して、TelePresence Server の IP ルーティング設定をテストでき、セキュリティには影響しません。

注：リモート ホストに ping できない場合は、ネットワーク設定を確認してください（特に NAT を使用しているファイアウォール）。

ネットワーク統計情報の表示（netstat）

TelePresence Server へのすべての TCP および UDP 接続の現在のステータスを表示するには、[Network] > [Netstat] に移動します。

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ます。また、[Refresh] をクリックした場合や、[Resolve names] チェックボックスをオンまたはオフにした場合も更新されます。

表 22 Netstat フィールドの説明

フィールド	説明
Resolve names	アドレスで DNS ルックアップを実行し、可能な場合にホスト名を表示するにはボックスをオンにし、代わりに IP アドレスを表示するにはボックスをオフにします。チェックボックスを切り替えるとデータが更新されます。
Protocol	[tcp4]、[tcp6]、[udp4] または [udp6]。その接続が使用しているインターネット プロトコルとアドレッシング方式を示します。
Recv-Q	TelePresence Server でまだ処理されていないためこの接続でキューイングされているバイト数。
Send-Q	リモート側でまだ認識されていないためこの接続でキューイングされているバイト数。
Local Address	この接続での TelePresence Server のアドレス。[Resolve names] がオンになっていない場合、このフィールドにはローカル ソケットが **address:port** と表示されます。[Resolve names] がオンになっている場合、このフィールドにはソケットが **hostname:servicename** と表示されます（可能な場合）。 例： **ts.example.com:http** または **127.0.0.1:80**
Foreign Address	この接続でのリモート側のアドレス。[Resolve names] がオンになっていない場合、このフィールドには外部ソケットが **address:port** と表示されます。[Resolve names] がオンになっている場合、このフィールドにはソケットが **hostname:servicename** と表示されます（可能な場合）。 例： **browser.example.com:http** または **192.168.3.1:80**
State	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。
Service	TelePresence Server がこの接続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ので、必要に応じてサービス設定を変更できます。

設定

システムの設定

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（詳細については表を参照）、[Apply changes] をクリックします。

[System settings] ページは、TelePresence Server がリモート管理モードで動作している場合は厳しく制限されます。ほとんどの会議のデフォルト設定は、TelePresence Conductor などの管理システムを使用して行われます。

表 23　すべての設定済み会議に対する設定

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	オンにすると、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 のユーザ インターフェイスに表示されます。	デフォルトでイネーブル（オン）になっています。
Show event log messages on console	シリアル コンソールに出力されるイベント ログを有効にするにはボックスをオンにし、シリアル コンソールに出力されるイベント ログを無効にするにはボックスをオフにします。 選択は、TelePresence Server を再起動しても保持されます。 チェックボックスがクリアされた場合、TelePresence Server は、電源投入時からメディア リソースが使用可能になるまでシリアル コンソールにイベント ログ メッセージを出力し続けます。この時間が経過すると、TelePresence Server は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。	このチェックボックスはデフォルトでクリアされています。つまり、イベント ログのシリアル出力は無効になっています。このデフォルト設定によって TelePresence Server のパフォーマンスが向上しているので、この設定を有効にするとパフォーマンスに影響する可能性があります。 イベント ログ メッセージをキャプチャするには syslog サーバを使用することを推奨します。 「Syslog を使用したロギング」（60 ページ）を参照してください。
Disable serial console input during startup	起動中に TelePresence Server がコンソールから何も解釈しないようにするにはボックスをオンにします。	コンソール ユーザが通常のブート シーケンスを中断しないように、このボックスをオンにすることを推奨します。

フィールド	フィールドの説明	使用方法のヒント
Require administrator login for serial console commands	ユーザが特定されていない場合は TelePresence Server がコンソール コマンドを解釈しないようにするためにボックスをオンにします。	物理アクセスを取得している承認されていないユーザからシリアル コンソールを保護するために、このボックスをオンにすることを推奨します。 **注：**TelePresence Server のコンソールは、一部の Unicode 文字を受け入れることができません。コンソール アクセスに使用するアカウントは、ユーザ名とパスワードの場合 ASCII 文字に制限されています。
Idle serial console session timeout	最後の入力後に TelePresence Server がオープン コンソール セッションを維持する分数。	無人のコンソール セッションが承認されていないユーザに開かれたままにならないよう、短い値を使用することを推奨します。

SIP の設定

[SIP settings] ページでは、TelePresence Server SIP の設定を制御できます。

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

デフォルトを更新したり、設定を変更するには、次の表を参照して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 コールおよび登録に影響します。 [Use trunk] を選択すると、SIP 登録が無効になり、既存の登録が切断されます。発信コールがトランクの接続先（たとえば VCS や CUCM）にルーティングされます。 [Call direct] を選択すると、SIP 登録が無効になり、既存の登録が切断されます。発信 SIP コールは直接転送されます（トランク経由ではなく）。	[Use trunk]： • 発信 SIP コールがトランク経由で指定した SIP サーバ アドレスに転送されます。 • Cisco Video Communication Server（VCS）や Cisco Unified Call Manager（CUCM）などの SIP サーバは、TelePresence Server からの発信 SIP コールの前進ルーティングを行います。 [Call direct]： • TelePresence Server は SIP コールを直接接続します（可能な場合）。これは**発信アドレス** パラメータまたは**発信ドメイン** パラメータを使用しません。 • TelePresence Server はトランクの使用を試行しません。
Outbound address	SIP レジストラまたはトランク接続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、TelePresence Server はこのフィールドを無視します。
Outbound domain	トランク接続先のドメイン。	[Outbound call configuration] が [Call direct] に設定されている場合、TelePresence Server はこのフィールドを無視します。 指定されたアドレスに @ 記号が含まれていない場合、TelePresence Server はこの値を発信 SIP コールに使用します。 発信ドメインを指定しない場合、TelePresence Server は発信アドレスを代わりに使用します。
[Username]	SIP デバイス（トランク接続先またはエンドポイント）で認証が必要な場合、TelePresence Server はこの名前を使用してそのデバイスで認証を行います。	
Password	SIP デバイス（トランク接続先またはエンドポイント）で認証が必要な場合、TelePresence Server はこのパスワードを使用してそのデバイスで認証を行います。	SIP 接続先は認証を必要としない場合があります。その場合は、このユーザ名とパスワードの組み合わせから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。

フィールド	フィールドの説明	使用方法のヒント
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] のいずれかです。	TelePresence Server は、トランク接続先との通信にこのプロトコルを使用します。 暗号化機能キーがインストールされていて、シグナリングを暗号化する場合は、[TLS] を選択します。 TelePresence Server は、接続が使用するすべてのプロトコル（TCP、UDP、または TLS）上で着信接続を受け入れ、この [Outbound transport] 設定に関係なく同じプロトコルを使用して応答します。[Network] > [Services] ページでそれらのサービスを必ずイネーブルにしてください。
Advertise Dual IPv4/IPv6	TelePresence Server が IPv4 および IPv6 の混合ネットワークで SIP コールをサポートするようにするには、[Use ANAT] を選択します。	デフォルトは [Disabled] になっています。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した場合は、デバイスがセッションの説明で 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 が次のどのオプションの SDES を使用して SRTP をネゴシエートするかを選択します。 • *For secure transports (TLS) only* • *For all transports* （注：このパラメータは、*メディア暗号化*機能キーでのみ表示されます。）	TelePresence Server は、SIP での暗号化の使用をサポートします。暗号化が SIP で使用されている場合、音声およびビデオのメディアは Secure Real-time Transport Protocol（SRTP）を使用して暗号化されます。SRTP を使用すると、キーを交換するデフォルト メカニズムは Session Description Protocol Security Description（SDES）です。SDES はクリア テキストでキーを交換するので、コール制御メッセージのセキュア トランスポートで SRTP を使用することを推奨します。また、SIP コール制御メッセージに使用できるセキュア 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 を設定できます。 デフォルト設定は [For secure transports (TLS) only] です。
Use local certificate for outgoing connections and registrations	発信 TLS コールを開始するときに TelePresence Server がローカル証明書を提示できるようにするには、このオプションをオンにします。このオプションがオフになっていると、TelePresence Server は要求されてもローカル証明書を提示しません。	このオプションは、TLS が使用中の場合はオンにする必要があります。

動作モード

[Operation mode] ページで、TelePresence Server をローカルで管理するかリモートで（Cisco TelePresence Conductor などのデバイスによって）管理するかを設定できます。

TelePresence Server がリモート管理モードに設定されている場合、そのリソースを動的に最適化できます。これは、コールが接続でき、必要なリソースのみを使用できることを意味します。これによって、さまざまな参加者の異なるメディア タイプ（音声、ビデオ、コンテンツなど）で最も効率的にブレード リソースを使用することができます。

動作モードを設定するには、[Configuration] > [Operation mode] に移動します。

動作モードを追加または変更するには、次の表を参照してフィールドを編集し、[Apply changes] をクリックします。

注意：

- 動作モードを変更すると、TelePresence Server を再起動する必要があります。
- リモート管理モードでは、設定されているエンドポイントと会議は使用できません。
- リモート管理モードの TelePresence Server で設定された会議は、ユニットの再起動時になくなります。

2 つの動作モードは 2 つの別個の API によってサポートされます。リモート管理モードを使用すると、柔軟な API が操作可能になり、ローカル管理モードを使用すると、スタンドアロン API が操作可能になります。

API の使用の詳細については、Cisco TelePresence Server API のマニュアルを参照してください。

表 25　動作モードの設定

フィールド	フィールドの説明	使用方法のヒント
Operation mode	この選択によって、TelePresence Server の動作モードが決まります。次のオプションがあります。 • *Locally managed* • *Remotely managed*	ローカル管理モードでは、TelePresence Server はすべての会議を管理します。 リモート管理モードでは、すべての会議の作成と参加者の管理が Cisco TelePresence Conductor などのデバイスによって TelePresence Server の外部で行われ、リソースは動的に最適化されます。 デフォルトでは、ローカル管理モードになっています。

システム時刻の表示およびリセット

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

時間を設定するには、[Configuration] > [Time] に移動します。

システム時間

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

手動でシステムの日時を設定するには、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ています。TelePresence Server が NTP サーバと自動的に同期するようにするには、NTP 設定を入力し、[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 の対応イーサネット インターフェイスのいずれかにローカルの場合、TelePresence Server は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はない場合、NTP サーバのネットワーク/IP アドレスへの特定の 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ているポートを使用して NTP サーバと通信します（[Network] > [Routes] を参照）。

TelePresence Server と NTP サーバの間にファイアウォールがある場合は、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 26　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	TelePresence Server で NTP プロトコルを有効にするにはボックスをオンにします。	
UTC offset	UTC から取得したタイム ゾーンのオフセット。	英国夏時間や他のサマータイム方式など、タイム ゾーンの地域による変化を構成するには、手動でこのオフセットを更新する必要があります。

フィールド	フィールドの説明	使用方法のヒント
NTP host	ネットワークの時間記録係として機能しているサーバの IP アドレスまたはホスト名。	

NAT（ネットワーク アドレス変換）による NTP の使用

NAT が TelePresence Server のネットワークに対してローカルである場合は、追加の設定は不要です。

NAT が NTP サーバのローカル ネットワークで使用される場合は、TelePresence Server から NTP サーバの 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。

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 のソフトウェア イメージのアップグレード

メイン TelePresence Server のソフトウェア 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 のソフトウェア イメージをアップグレードするには、次の手順を実行します。

1. [Configuration] > [Upgrade] に移動します。
2. 現在インストールされているバージョンを確認するために、メイン ソフトウェア イメージの [Current version] を確認します。
3. 最新のイメージが使用可能であるかどうかを確認するには、サポート ページにログインします。
4. 使用可能な最新のイメージをダウンロードし、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インします。

7. [Configuration] > [Upgrade] に移動します。
8. ハード ドライブで解凍したファイルを見つけます。

   ボタンはブラウザによって [Browse...] または [Choose File] などとなります。
9. [Upload software image] をクリックします。ブラウザが TelePresence Server に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、ブラウザの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は、[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、再起動します。

ローダー ソフトウェア イメージのアップグレード

通常、ローダ ソフトウェア イメージのアップグレードは、メイン ソフトウェア イメージのアップグレードと同様利用できません。

注：カスタマー サポートから指示された場合以外は行わないでください。

ローダ ソフトウェア イメージをアップグレードするには、次の手順を実行します。

1. [Configuration] > [Upgrade] に移動します。
2. 現在インストールされているバージョンを確認するために、ローダー ソフトウェアの [Current version] を確認します。
3. Web サイトのソフトウェア ダウンロード ページに移動して、最新のイメージが使用可能であるかどうかを確認します。
4. 使用可能な最新のイメージをダウンロードし、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. ハード ドライブで解凍したファイルを見つけて選択します。

   ボタンはブラウザによって [Browse...] または [Choose File] などとなります。
7. [Upload software image] をクリックします。ブラウザが TelePresence Server に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、ブラウザのウィンドウが更新され、「Loader image upgrade completed」と表示されます。
8. アップグレードのステータスは、[Loader upgrade status] フィールドに表示されます。
9. TelePresence Server をシャットダウンし、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] セクションでは、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および復元できます。これによって、以前の設定に戻したり、設定をコピーすることでユニットを効率的に複製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。

後日設定を復元するには、次の手順を実行します。

1. [Configuration] > [Upgrade] に移動します。
2. 前に保存した configuration.xml ファイルを見つけて選択します。

   ボタンはブラウザによって [Browse...] または [Choose File] などとなります。
3. 保存した設定で現在の [Network settings]、[User settings] またはその両方を上書きするかどうかを選択します。

   上書き制御はデフォルトで選択されていません。ソフトウェアは、既存のネットワーク設定およびユーザ アカウントを維持することを前提としています。
4. [Restore backup file] をクリックします。

新しいコンフィギュレーション ファイルを TelePresence Server に復元する場合は、設定のどの部分を上書きするかを制御できます。

- [Network settings] をオンにすると、ネットワーク設定が指定されたファイルのネットワーク設定で上書きされます。

  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、またはアウトオブサービスの 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したときに衝突が発生した場合（たとえば、両方が同じ固定 IP アドレスを使用するように設定されている場合）、一方または両方のデバイスが IP を通じて到達できなくなる可能性があります。[Network settings] をオフにすると、QoS 設定を除き、復元操作で既存のネットワークの設定が上書きされません。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] をオンにすると、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のものと上書きされます。
- ユーザ設定を上書きし、復元されたファイルに現在のログインに対応するユーザ アカウントがない場合は、ファイルがアップロードされた後に再びログインする必要があります。

TelePresence Server 機能のイネーブル化

TelePresence Server では、ほとんどの機能を使用する前にアクティブ化する必要があります。（TelePresence Server がアクティブになっていないと、Web インターフェイスの上部のバナーに警告が目立つように表示されます。他のすべての点で Web インターフェイスは正常に表示され機能します。）

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、または新しい機能をイネーブルにしている場合は、サプライヤに連絡して適切なアクティベーション キーを取得してください。

各キーは特定の TelePresence Server に固有です。サプライヤが有効なキーを提供できるように、キーを依頼するときはデバイスのシリアル番号を確認してください。

キーの適用プロセスは、TelePresence Server をアクティブにしている場合も拡張機能をイネーブルにしている場合も同じです。

キーを TelePresence Server に適用するには、次の手順を実行します。

1. [Feature management] リストを確認し、機能がすでにアクティブであるかどうかを確認します。

   製品アクティベーション キーもこのリストにあります。
2. サプライヤから受け取ったキーを [Add key] フィールドに入力します。入力時は*受け取った通り正確に*ダッシュも含めて入力します。
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したキーがリストされます。

   キーが無効の場合は、再入力するように求められます。

   キーには時間制限がある場合があります。この場合、失効日が表示されるか、または機能の期限がすでに切れていることを示す警告が表示されます。期限切れのキーは、対応する機能が無効になっていてもリスト内に残ります。
4. あとで再入力する場合に備えてキーを記録します。

正常な TelePresence Server または機能のアクティベーションは即座に有効になり、TelePresence Server を再起動しても保持されます。

一部の機能は削除できます。機能を削除するには、キーの横の [remove] をクリックします。

スクリーン ライセンスの適用

TelePresence Server MSE 8710 をライセンス化するには、スーパーバイザにログインし、ブレード スロットにスクリーン ライセンスを割り当てる必要があります。スクリーン ライセンスはシャーシのシリアル番号にリンクされます。詳細については、スーパバイザのマニュアルを参照してください。

TelePresence Server 7010 の場合、スクリーン ライセンス キーは TelePresence Server のハードウェア シリアル番号にリンクされます。機能キーを追加する方法（手順は上記に記載）と同様に、ライセンス キーを TelePresence Server に直接入力します。

TelePresence Server のシャットダウンと再起動

アップグレードの一部として TelePresence Server を再起動したり、電源をオフにするには、TelePresence Server をシャットダウンする必要がある場合があります。

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、次の手順を実行します。

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] に変わります。
3. ボタンを再度クリックして確認します。

   TelePresence Server がシャットダウンを開始します。ページ上部のバナーがその旨を示すように変化します。

   シャットダウンが完了すると、ボタンは [Restart TelePresence Server] に変わります。
4. このボタンをクリックすると TelePresence Server が再起動します。

管理者パスワードの変更

このページでは、この TelePresence Server にログインするときに使用する管理者パスワードを変更できます。これは「管理者」である必要が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推奨します。パスワードをメモして、この情報を安全な場所に保管することを推奨します。

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、[Change password] をクリックします。

FTP 経由の設定のバックアップと復元

TelePresence Server の Web インターフェイスまたは File Transfer Protocol（FTP）経由で設定をバックアップおよび復元できます。FTP を使用して TelePresence Server に接続するには、TelePresence Server で FTP サービスをイネーブルにしておく必要があります（[Network] > [Services] ページ）。

FTP 経由で設定をバックアップするには、次の手順を実行します。

1. FTP クライアントと、Web インターフェイスにログインするのに使用する管理者クレデンシャルを使用して、TelePresence Server に接続します。

   TelePresence Server の設定を含む **configuration.xml** というファイルが表示されます。
2. このファイルをダウンロードし、安全な場所に保存します。

FTP を使用して設定を復元するには、次の手順を実行します。

1. 復元する **configuration.xml** のコピーを検索します。
2. FTP クライアントと、Web インターフェイスにログインするのに使用する管理者クレデンシャルを使用して、TelePresence Server に接続します。
3. TelePresence Server に **configuration.xml** ファイルをアップロードします。それによって既存のバージョンのファイルが上書きされます。

注：同じプロセスを使用して、ある TelePresence Server ブレードから別のブレードに設定を転送できます。ただし、これを行う前に、設定を交換するブレードから元の機能キーのコピーを必ずとっておいてください。

コンフィギュレーション ファイルを使用して重複するブレードを設定する場合は、重複するブレードで静的 IP アドレスを再設定する必要があることに注意してください。

会議

会議リストの表示

[Conferences] ページには、この TelePresence Server に設定されているすべての会議がそのステータス（たとえば [Active] または [Inactive]）に関係なく一覧表示されます。

このリストにアクセスするには、[Conferences] に移動します。

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ています。ソート順序を変更する場合、またはステータスや URI でリストをソートするには、該当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。

- 会議の削除。
- 会議名をクリックすることで、そのステータスを表示。

リストには、各会議に関する次の情報が含まれています。

表 27 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	事前設定されている会議の名前。	会議のステータスと参加者を表示するには会議の名前をクリックします。
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々の会議 URI を登録しません。 会議には、参加者がダイヤルできる最大 2 つの多用途 URI を指定できます。URI が PIN で保護されている場合、このステータスが表示されます。 URI は複数の PIN をサポートできるので、個別のゲスト/chair PIN を設定できます。 個々の参加者は、自身がダイヤルする自分の URI を指定できます。これらはこのリストに表示されません。
Status	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。	会議には次のものがあります。 • [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)] と表示されます。または、すべてのエンドポイントが音声のみの場合は [Active (<X> endpoints)] と表示されます。 • [Inactive] 会議は事実上 [Active] 会議と同じですが、参加者がいません。しかし、URI と、開始および期間までの時間を指定できます。

フィールド	フィールドの説明	使用方法のヒント
		• [Ending] は、会議が終了過程にあることを示します。この間に、残りの参加者には終了のロビーが表示されます。 ステータスには、会議の期間とその会議がロックされているかどうかに関する追加情報が含まれている場合があります。たとえば、[Inactive - Ends in 5 hours and 27 minutes [Locked]] などのように表示されます。 会議の設定に関する警告が表示される場合があります。たとえば、[No participants allowed - limited to 0 participants] などのように表示されます。

会議ステータスの表示

会議の [Status] ページには、会議のライブ ステータスが表示されます。[Status] ページを表示するには、[Conferences] に移動して、会議の名前をクリックします。

このページから、会議の次の内容について確認できます。

- アクティブかどうか、および会議にいるエンドポイントの数
- ロックされているかどうか
- コンテンツ チャネルが含まれているかどうか
- 参加者がいるかどうか、およびそれぞれのステータス
- 以前参加者がいたかどうか、およびその人物について
- URI が会議に割り当てられているかどうか

[Conference] > [Conference Name] > [Status] ページで、次のことを実行できます。

- 参加者を選択し、選択した参加者の切断
- 効率的に会議を終了させるための**すべての参加者の切断**
- 1 つまたはすべてのエンドポイントへのメッセージの送信
- 参加している 1 つの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、すべてのアクティブ エンドポイントに関してこの情報を表示するには、[Expand all] をクリックします（詳細については次の表を参照）。

会議ステータスの参照

表 28 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	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。	会議には次のものがあります。 • [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)] と表示されます。または、すべてのエンドポイントが音声のみの場合は [Active (<X> endpoints)] と表示されます。 • [Inactive] 会議は事実上 [Active] 会議と同じですが、参加者がいません。しかし、URI と、開始および期間までの時間を指定できます。 • [Ending] は、会議が終了過程にあることを示します。この間に、残りの参加者には終了のロビーが表示されます。 ステータスには、会議の期間とその会議がロックされているかどうかに関する追加情報が含まれている場合があります。たとえば、[Inactive - Ends in 5 hours and 27 minutes [Locked]] などのように表示されます。 会議の設定に関する警告が表示される場合があります。たとえば、[No participants allowed - limited to 0 participants] などのように表示されます。
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々の会議 URI を登録しません。 会議には、参加者がダイヤルできる最大 2 つの多用途 URI を指定できます。URI が PIN で保護されている場合、このステータスが表示されます。 URI は複数の PIN をサポートできるので、個別のゲスト/chair PIN を設定できます。 個々の参加者は、自身がダイヤルする自分の URI を指定できます。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 チャネルが現在使用中かどうか。	次のいずれかになります。 • [No current presentation]：コンテンツ共有は会議でイネーブルになっていますが、アクティブな共同作成者がいません。 • [Presentation from <endpoint display name>]：コンテンツのアクティブな共同作成者がいます。 詳細については、「コンテンツ チャネルのサポート」を参照してください。

表 29　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、このセクションには [No endpoints] と表示されます。 会議から参加者を削除するには、適切なチェックボックスを選択して、[Disconnect selected] を選択します。 エンドポイントの [Status] ページに移動するには、エンドポイントの名前をクリックします。
Type	エンドポイントのタイプ。	
Authority	[Chair] または [Guest]。会議での参加者のロール（および関連する権限）を示します。	管理システムがこの会議に chair/guest 制御レベルを明示的に適用している場合を除き、デフォルトではすべての参加者に対し [Chair] が設定されています。
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]：エンドポイントがこの会議に参加しています • [In conference]：エンドポイントがこの会議に現在参加しています。 • [Attempting to re-establish call]：エンドポイントが使用中であり、再試行が発生しています。 追加のステータス情報が表示される場合があります。たとえば、[xx failed to join]（グループ化されたエンドポイント）、[packet loss detected]、[video to muted]、[video from muted]、[video muted]（および音声相当）、[important]、および [audio-only] 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
		会議の開始時に事前設定されたエンドポイントが使用中の場合、TelePresence Server は会議中に 5 回までエンドポイントを再試行し、空いた場合は接続します。再試行間隔は 5、15、30、60 および 120 秒です。
More...	送受信ストリームのプレビューを表示するには、[More...] をクリックします。また、会議へのエンドポイントの貢献を制御することもできます。 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するには、[Expand / Collapse All] をクリックします。	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 参加者を重要扱いにする（送信ストリームのみ）  または重要ではない扱いとする 

表 30　以前の参加者

フィールド	フィールドの説明	使用方法のヒント
Endpoint	この会議に以前参加していたエンドポイントの名前。	会議に参加者を再接続するには、適切なチェックボックスを選択して、[Retry connection] を選択します。 エンドポイントの [Status] ページに移動するには、エンドポイントの名前をクリックします。
Type	エンドポイントのタイプ。	
Reason for disconnection	エンドポイントが会議から除外された理由。	TelePresence Server は次の理由のいずれかにより、エンドポイントを切断した可能性があります。 • [requested by administrator]：エンドポイントは、管理者によって切断されました。 • [call rejected]：相手先がコールを拒否しました。 • [left conference]：エンドポイントは会議の終了時に切断されました。 • [requested via API]：エンドポイントは API 経由で切断されました。 • [no answer]：エンドポイントがコールに応答しませんでした。 • [busy]：エンドポイントが使用中であったため、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ことを意味する場合があります）。

フィールド	フィールドの説明	使用方法のヒント
		• [gatekeeper error]：コールを確立している間にゲートキーパーのエラーが発生しました。 • [destination unreachable]：エンドポイントは到達不能でした。 • [DNS failure]：DNS ルックアップが失敗したか、または H.323 ゲートキーパーが要求されたエイリアスを見つけることができませんでした。 • [Encryption not supported by far end]：コールには暗号化が必要だが相手先で暗号化をサポートしていない、またはこのコールでは暗号化が禁止されているが相手先が暗号化を要求している場合。 • [timeout]：接続がタイム アウトしました。 • [insufficient free ports]：十分な空きポートがなかったためエンドポイントは切断されました。 • [conference port limit reached]：会議ポートの制限に達したためエンドポイントは切断されました。 • [Conference locked]：ロックされていたためコールが会議に接続できませんでした。 • [Product not activated]：アクティベーション キーが TelePresence Server にインストールされていなかったため、コールを発信/受信できませんでした。 • [Protocol error]：プロトコル エラーによりエンドポイントは切断されました。 • [Network error]：ネットワーク エラーによりエンドポイントは切断されました。 • [Unavailable]：エンドポイントは使用できません。 • [Capability negotiation error]：エンドポイントおよび TelePresence Server は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]：トークンの仕様/割り当てが TIP/MUX コールに十分でありませんでした。 • [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、エンドポイントは切断されました。

フィールド	フィールドの説明	使用方法のヒント
		• [No media received]：エンドポイントが予期せずにメディアの送信を停止してから 30 秒以上経過したため、TelePresence Server はこのエンドポイントを切断しました。 • [unspecified error]：エンドポイントが切断されましたが、TelePresence Server は原因を把握していません。

エンドポイントとグループのステータスの表示

エンドポイントのステータスは、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の一部であ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一定の範囲まで制御できます。

1. [Conference] に移動し、[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. 次の表を参照して、エンドポイントを確認するか、または制御します
4. 最新のステータスを表示するには、ブラウザでページを更新します。

表 31 エンドポイントにより提供される情報

フィールド	フィールドの説明	使用方法のヒント
Country code/extension **Manufacturer code** **Product** **Version**	これらのフィールドには、エンドポイントによって返される情報が表示されます。詳細は、製造業者間の一貫した方法で提供されない場合があります。	この情報は、（現在接続されているかどうかにかかわらず）エンドポイントが初めて接続された後に表示されます。

表 32 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あるかどうか、およびある場合はその会議の名前。	その会議のステータス ページに移動するには、会議の名前をクリックします。
Call status	コールが接続されているかどうか、および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。	

フィールド	フィールドの説明	使用方法のヒント
Protocol	このコールで使用されるプロトコル（SIP など）。	
Endpoint advertised capabilities	コールをネゴシエートするときにエンドポイントがアドバタイズした機能。	例：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。
Audio channels	送受信音声チャネルが Cisco TelePresence Server と相手先との間で開いているかどうか。	
Video channels	送受信ビデオ チャネルが Cisco TelePresence Server と相手先との間で開いているかどうか。	
Extended video channels	送受信拡張ビデオ チャネルが Cisco TelePresence Server と相手先との間で開いているかどうか。	
Received audio gain mode	エンドポイントで、TelePresence Server から受信した音声に対し設定されている音声ゲイン 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動的に調整し、他の参加者が受信するレベルを概算します。 [Disabled]：ゲイン コントロールはこのエンドポイントが受信する音声についてはディセーブルになっています。 [Fixed]：TelePresence Server は固定比率によってエンドポイントの受信音声を調整します。これは、エンドポイントの設定ページの [Received audio gain] フィールドで設定されます。
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量。	エンドポイント グループの場合は、複合帯域幅の合計ではなく各コールの帯域幅を示します。
Preview	ビデオ ストリームのサンプル スチール。	このプレビューには、受信ストリームと送信ストリームの両方について各画面からのスチールが適切な方向と帯域幅によって使用される図の下に並べて表示されます。クリックしてプレビューを更新できます。
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いる時間。	

フィールド	フィールドの説明	使用方法のヒント
Disconnect	会議からエンドポイントまたはエンドポイント グループを切断するには、このコントロールを使用します。	
Mute audio from / Unmute audio from	このエンドポイントから音声のミュートを開始または停止するには、このコントロールを使用します。これによって、他の会議参加者がこのエンドポイントを聞けるかどうかが変わります。	
Mute audio to / Unmute audio to	このエンドポイントへの音声のミュートを開始または停止するには、このコントロールを使用します。エンドポイント*に対し*音声をミュートにすると、エンドポイントでは何も聞こえません。	
Mute video from / Unmute video from	このエンドポイントからビデオのミュートを開始または停止するには、このコントロールを使用します。これによって、他の会議参加者がこのエンドポイントを見れるかどうかが変わります。	
Mute video to / Unmute video to	このエンドポイントへのビデオのミュートを開始または停止するには、このコントロールを使用します。エンドポイント*に対し*ビデオをミュートにすると、そのエンドポイントにはブランクのビデオが送信されます。	
Tidy view	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には、このコントロールを使用します。	TelePresence Server は、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）を自動的に中心に配置し、画面間の PiP を移動します。これが行われることで PiP が若干大きく表示されます。これは、参加者が会議に出入りするときに動的に行われます。 このエンドポイントに送信されたレイアウトで参加者の PiP を手動でリセットし中央に配置する必要がある場合は、[tidy view] オプションを使用します。

フィールド	フィールドの説明	使用方法のヒント
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] ページには次の内容が表示されます。 1. メッセージを入力し、ターゲット エンドポイントの位置を選択し、表示するメッセージの時間（秒単位）を入力します。 2. [Send message] をクリックします。	

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、[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、[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、**受信ストリーム**統計情報と**送信ストリーム**統計情報の 2 つのリストにグループ化されます。
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更新することでデータを手動で更新したり、[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。

複数画面のエンドポイントの場合は、[Multiscreen Stream Selection] ページに移動します。目的のストリームを選択して [Endpoint Statistics] ページに移動すると、そのチャネルに関連付けられたすべてのストリームのデータが表示されます。

表 33　受信ストリームの統計情報

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。ビデオとコンテンツ チャネルでは、ビデオ ストリームの寸法も表示されます。
Encryption	このストリームを暗号化するかどうか。
Channel bit rate	Cisco TelePresence Server に音声/ビデオ/コンテンツを送信するエンドポイントのネゴシエートされた使用可能な帯域幅。

フィールド	フィールドの説明
Receive bit rate	このフィールドは、ビデオおよびコンテンツのチャネル受信ストリームのみに適用されます。Cisco TelePresence Server がエンドポイントの送信を要求したビット レート（1 秒あたりのビット数）。最後に測定されたビット レートがカッコ内に表示されます。
Received jitter	パケットが Cisco TelePresence Server に到達したときのこのチャネルでのパケット間のタイミングの変動を表します。数値が小さほどパケットがより予想通りに到達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のみに適用され、音声信号強度の尺度となります。単位はミリデシベルで、-34000 などの大きい負の数だと非常に静かで、負の数がゼロに近づくにつれて大きくなります。
Packets received / errors	Cisco TelePresence Server によって受信された音声/ビデオ/コンテンツのパケット数。2 番目の数値は音声/ビデオ/コンテンツのパケットレベルのエラーを示します。たとえば、シーケンスの中断や不正な RTP の詳細などです。これは、ビデオ（実際のビデオ データ）が何らかの理由でエラーになるパケットと同じではありません。
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 番目の数値は、受信されたが破損しているパケット数を示します。
Frames received / errors	現在エンドポイントに送信されている音声/ビデオ/コンテンツのストリームのフレーム レートと、受信した音声/ビデオ/コンテンツのフレームの総数に対するエラーを伴うフレーム数。
Frame rate	このフィールドは、ビデオおよびコンテンツの受信ストリームに適用されます。これは、エンドポイントと TelePresence Server 間の送信/受信ストリームの 1 秒あたりのフレーム数です。
Fast update requests sent	このチャネルで TelePresence Server から送信された高速更新要求（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る前方誤り訂正（FEC）の統計情報。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 ActiveControl を TelePresence Server とネゴシエーションできない場合は、この値は *サポートされません*。 そうでなければ、オーバーヘッド率と復元されたパケット数の 2 つの統計情報があります。 オーバーヘッド率は、元のストリームと比較してどのくらいの FEC パケットが挿入されるかを測定します。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 % です。エンドポイントが 2 番目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 50 % で、4 番目のすべてのパケットのコピーを挿入する場合は 25 % です。リアル統計情報は、RTCP レポートのカウント間隔とタイミングにより、これらのレベルと常に完全に一致するとは限りません。 復元されたパケット数は、オリジナルが失われたため、エンドポイントの FEC パケットから TelePresence Server によって復元されたパケットの数にすぎません。
ClearPath LTRF	LTRF（長期参照フレーム）がイネーブルの場合、*受信した N 修正フレーム*をレポートします。これは、LTRF がストリームで使用された回数を示します。

表 34　送信ストリームの統計情報

フィールド	フィールドの説明
Transmit stream	送信ストリームに使用されるコーデック。ビデオとコンテンツ チャネルでは、ビデオ ストリームの寸法も表示されます。
Encryption	このストリームを暗号化するかどうか。
Channel bit rate	エンドポイントに音声/ビデオ/コンテンツを送信する Cisco TelePresence Server のネゴシエートされた使用可能な帯域幅。
Transmit bit rate	このフィールドは、ビデオおよびコンテンツの送信ストリームのみに適用され、Cisco TelePresence Server が現時点で送信しようとしているビット レートです。実際のビット レート（これは単に Cisco TelePresence Server から発信されるビデオ データの測定レートです）は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/コンテンツのパケット数。2 番目の数字は、エンドポイントにより報告される、エンドポイントが受信しなかったパケットの数です。
Frame rate	このフィールドは、ビデオとコンテンツのストリームに適用されます。これは、エンドポイントと TelePresence Server 間の送信/受信ストリームの 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で TelePresence Server によって受信された高速更新要求(FUR)の数。
ClearPath FEC	このストリームで使用される前方誤り訂正の統計情報。 オーバーヘッド率と報告された復元済みパケット数の 2 つの統計情報があります。 オーバーヘッド率は、元のストリームと比較してどのくらいの FEC パケットが挿入されるかを測定します。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 % です。TelePresence Server が 2 番目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 50 % で、4 番目のすべてのパケットのコピーを挿入する場合は 25 % です。TelePresence Server がこのストリームに現在 FEC を適用していない場合、オーバーヘッドは 0 % です。 この数字は、元のパケットが失われたために TelePresence Server の FEC パケットからエンドポイントによって復元されたと報告されているパケットの数です。
ClearPath LTRF	長期参照フレームがこのストリームで使用されるかどうか。エンドポイントが ActiveControl を TelePresence Server とネゴシエーションできない場合は、この値は *サポートされません*。それ以外の場合、この値は [Enabled] となっており、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 に存在するすべてのユーザ アカウントの概要が提示されます。

表 35 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。任意の文字セットでテキストを入力できますが、一部のクライアントは Unicode 文字をサポートしていないことに注意してください。
Name	ユーザの名前（任意、したがってなくても可）。
Access rights	このユーザに許可されるロールと関連する権限。[Administrator]、[API access]、および [None] の 3 つのレベルがあります。 [None]：このユーザは TelePresence Server からロックアウトされます。 [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 アクセス権および管理アクセス権があります。

ユーザの削除

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

ユーザの追加および更新

ユーザのリスト（[Users] に移動）にアクセスすることで、TelePresence Server のユーザ 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際に使用する情報の大部分は同じですが、違いを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、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、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場合は、[Change password] をクリックします。

ユーザの詳細の参照

表 36 ユーザの詳細

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。	任意の文字セットでテキストを入力できますが、一部のクライアントは Unicode 文字をサポートしていないことに注意してください。 **注：**TelePresence Server のコンソールは、一部の Unicode 文字を受け入れることができません。コンソール アクセスに使用するアカウントは、ユーザ名とパスワードの場合 ASCII 文字に制限されています。
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。	任意の文字セットでテキストを入力できますが、一部のクライアントは Unicode 文字をサポートしていないことに注意してください。
Re-enter password	パスワードを再入力します。	パスワードの入力フィールドは、新規ユーザの追加時にデフォルトでのみアクティブになっています。既存のユーザを更新する場合は、[Change password] をクリックしてこれらのフィールドの編集を有効にします。

フィールド	フィールドの説明	詳細情報
Access rights	ドロップダウンからユーザのロールを選択します。ロールによって次のように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 アクセス権および管理アクセス権があります。	

ログ

イベント ログの使用

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、TelePresence Server のログから情報を収集する必要がある場合があります。通常は、これらのログの取得を手助けしてくれるカスタマー サポートと一緒に作業を行います。

イベント ログ

TelePresence Server は、そのサブシステムによって生成された直近にキャプチャされた 2000 のメッセージを保存します。これらは [Event log] ページ（[Logs] > [Event log]）に表示されます。一般に、これらのメッセージは情報として提供され、場合によっては、*警告*または*エラー*がイベント ログに表示されます。

TelePresence Server の操作またはパフォーマンスで特定の問題が発生した場合、カスタマー サポートはログに記録されたメッセージとユーザに対するその重要性を解釈できます。

次の作業を実行できます。

- イベントをソートするには、列ヘッダーをクリックします。
- 100 イベントずつ表示されたログを移動するには、ページ番号をクリックします。
- すべてのシステム ログを 1 つの zip ファイルにダウンロードするには、[Download system logs] をクリックします。
- テキストとしてイベント ログをダウンロードするには、[Logs] > [Event log] に移動し、[Download event log] をクリックします。
- 特定の領域に情報を制限するには、ディスプレイ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で、トレースに収集された詳細のレベルを変更します。

注：イベント キャプチャ フィルタを変更するのは、カスタマー サポートから指示された場合のみにしてください。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場合があります。

- 保存または分析のためにイベント ログをネットワークの 1 つ以上の Syslog サーバに送信します。サーバは [Logs] > [Syslog] ページで定義されます。
- [Clear event log] をクリックしてログを空にします。

イベント キャプチャ フィルタ

イベント キャプチャ 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。デフォルトでは、このフィルタはすべての TelePresence Server のサブシステムからの*エラー*、*警告*、*および情報*を取得するように設定されています。

注：このフィルタを変更するのは、カスタマー サポートから指示された場合のみにしてください。

たとえば、TelePresence Server の問題のトラブルシューティング時に、サポートの担当者からビデオ サブシステムの詳細なトレースをキャプチャするように指示される場合があります。

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 によって、パフォーマンスが影響を受ける可能性があることが警告されます。
3. [OK] をクリックします（これは詳しくは一時的な昇格で、問題が解決した後で元に戻すことができます。）
4. [Update settings] をクリックします。

   TelePresence Server はビデオ サブシステムからの詳細なトレース情報だけでなく、他のすべてのサブシステムのデフォルト情報もキャプチャします。

イベント表示フィルタ

イベント表示フィルタを使用して、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することができます。このフィルタは保存されたエントリで機能し、どのイベントがキャプチャされるかについては影響しません。

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. 特定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**フィルタ文字列**を入力します。
2. フィルタリングされた結果内の文字列を簡単に見つけるには、**強調表示文字列**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 のサブシステムは多くあり、それらはすべてログ イベントにできます。各サブシステムまたはすべてのサブシステムについて、表示する詳細レベルを変更できます。

たとえば、SIP エラーのみに関心がある場合は、次の手順を実行します。

1. ページの下部までスクロールし、[Set all to:] ボタンとその横にあるドロップダウンを表示します。
2. ドロップダウンから [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が [None] に変わります。
4. SIP サブシステムの横のドロップダウンから [Errors only] を選択します。

5. [Update settings] をクリックします。

   TelePresence Server に SIP エラー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] ページには、さまざまなプロトコルについて、TelePresence Server が受信したメッセージまたは TelePresence Server から送信されたメッセージが記録されます。

メッセージの量がパフォーマンスに影響するためプロトコルのロギングはデフォルトで無効になっていますが、トラブルシューティング時にカスタマー サポートによって有効にするように指示される場合があります。

プロトコル メッセージのロギングを開始する場合は、次の手順を実行します。

1. ログに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、これらのプロトコル 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、XML ファイルとしてログを取得し、サポートに送信します。

問題が解決したら、[Disable protocols logging] をクリックしてから [Clear log] をクリックし、以後のユニットのパフォーマンスに影響しないようにする必要があります。

フィールド	説明
Current status	[Enabled] または [Disabled] です。デフォルトでは [Disabled] になっています。
Messages logged	ロギングするメッセージの数。
Protocol filters	• *BFCP* • *H.323* • *SIP* • *XCCP* キャプチャするプロトコル メッセージのボックスをオンにします。これらはキャプチャ フィルタであり表示フィルタではありません。プロトコルのチェックを外しプロトコルのロギングを有効にすると、TelePresence Server はチェックされていないプロトコルのメッセージをキャプチャしません。 ロギングが有効になっている間は、どのプロトコルをロギングするかを変更できません。キャプチャ フィルタを変更する場合は、ロギングを無効にし、チェックボックスを変更してから、ロギングを再度有効にします。

プロトコル メッセージのリモート ロギング

プロトコルのログは HTTP または HTTPS を介して使用できるので、ログをリモート デバイスに記録できます。プロトコルのロギングを有効または無効にする設定によって、リモート デバイスへのログの送信は無効になりません。最大 2 つの同時ログ ストリームをいつでも使用できます。

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場合は、次の手順を実行します。

1. リモート デバイスから HTTP POST 要求を **http[s]://***<ip address>***/protocols_log_stream** に送信します。この POST 要求には次の有効なユーザとパスワードのパラメータが含まれている必要があります。
   authenticationUser=*username***&authentication****Password=***password***

   以下は wget を使用した例です（Linux システムの場合）。
   wget https://*<IP address>***/protocols_log_stream --post-data=authenticationUser=***username***&authentication****Password=***password***

   （API のみの権限を持つユーザが有効と見なされます。）

2. プロトコル ログのコンテンツ全体はその後、この TCP 接続を使用してリモート デバイスに戻ります。ログのストリームは、リモート デバイスが TCP 接続を中断するまで続きます。

Syslog を使用したロギング

保存または分析のためにイベント ログをネットワークの 1 つ以上の Syslog サーバに送信できます。

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

Syslog の設定

Syslog の設定時は、次の表を参照してください。

表 37　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 つまでの syslog レシーバ ホストの IP アドレスを入力します。	各設定されたホストに送信されたパケット数は、その IP アドレスの横に表示されます。
Facility value	Syslog ホストで Cisco TelePresence Server からイベントを識別するための	Cisco TelePresence Server として覚え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 システムのデーモンとプロセスは、同じ

フィールド	フィールドの説明	使用方法のヒント
	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 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/認証メッセージ（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/認証メッセージ（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）*	ように見えるセキュリティ/認証、監査およびアラートのメッセージに対し、ファシリティ 4、10、13、および 14 を使用します。 **注 2：**さまざまなオペレーティング システムは、クロック（cron/at）メッセージに対し、ファシリティ 9 および 15 の両方を使用します。 ファシリティ値が明示的に割り当てられているプロセスとデーモンは「ローカル使用」ファシリティ（16 ～ 21）のいずれかを使用でき、または、「ユーザレベルの」ファシリティ（1）を使用することができます。シスコではこれらの値のいずれかを選択することを推奨します。

フィールド	フィールドの説明	使用方法のヒント
	• *[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）* • *[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 ログのキャプチャ 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、IP アドレスを入力し、[Update syslog settings] をクリックします。各設定されたホストに送信されたパケット数は、その IP アドレスの横に表示されます。

注：次のように、各イベントには重大度の指標があります。

- [0 - Emergency]：システムが使用不能（Cisco TelePresence Server によって使用されていない）
- [1 - Alert]：アクションをすぐに実行する必要があります（Cisco TelePresence Server によって使用されていない）
- [2 - Critical]：クリティカルな状態（Cisco TelePresence Server によって使用されていない）
- [3 - Error]：エラー状態（Cisco TelePresence Server の*エラー*イベントで使用されている）
- [4 - Warning]：警告状態（Cisco TelePresence Server の*警告*イベントで使用されている）
- [5 - Notice]：正常だが顕著な状態（Cisco TelePresence Server の*情報*イベントで使用されている）
- [6 - Informational]：情報メッセージ（Cisco TelePresence Server の*トレース*イベントで使用されている）
- [7 - Debug]：デバッグ レベルのメッセージ（Cisco TelePresence Server の*詳細トレース*イベントで使用されている）

コール詳細レコードの使用

TelePresence Server は、最大 2000 のコール詳細レコードを表示できます。ただし、TelePresence Server はコール詳細レコードの長期ストレージを目的として作られていません。CDR ログを保存する場合は、それら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 ログを表示して制御するには、[Logs] > [CDR log] に移動します。使用可能なオプションの詳細および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。

- コール詳細レコードのログのコントロール
- コール詳細レコードのログ

コール詳細レコードのログのコントロール

CDR ログには多くの情報を含めることができます。このセクションのコントロールは、最も役立つ情報を表示するのに役立ちます。変更を終えたら、[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 38 ステータスおよび表示

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 がログに記録する CDR レコード タイプのリスト。	すべてのレコードを表示するにはボックスを空白のままにします。または、該当するレコード タイプのボックスをオンにします。
Filter string	表示されるコール詳細レコードの範囲を制限するには、このフィールドを使用します。フィルタ文字列では、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。特定のレコードに拡張された詳細がある場合、フィルタ文字列はそれらにも適用されます。
Expand details	デフォルトでは、CDR ログには各イベントの簡単な説明のみが表示されます。利用可能な場合は、リストされたオプションから選択してさらに詳細を表示します。	[All] を選択すると、他に選択されているオプションにかかわらず、すべてのメッセージの最大量の詳細が表示されます。

コール詳細レコードのログ

コール詳細レコードのログは、長い表として表示され、複数のページにまたがっている場合があり、最大 2000 の行から成ります。上記のフィルタリングに加えて、次の方法でログに移動できます。

- 任意の列で昇順または降順に並べ替えるには、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 に関連するすべてのレコードのログをフィルタリングするには、GUID をクリックします（このフィルタを戻すには [Show all] をクリックします）。

- 表示されたレコードのリスト内の特定のページに移動するには、ページ番号をクリックします。

ログをテキスト エディタで処理したり、今後の参照用にアーカイブするには、[Download as XML] をクリックします。このボタンを使用すると、現在保存されている *すべてのレコードがダウンロードされます*。Web ページで設定した表示フィルタは無視されます。

注：ユニットに大きな負荷がかかっている場合は 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] をクリックすると、TelePresence Server から *すべてのレコードが完全に削除されます*。クリアされたレコードは回収できません。

CDR ログの参照

次の表では、CDR ログのフィールドについて説明します。

表 39　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)	このコール詳細レコードの一意のインデックス番号。	
Time	コール詳細レコードが作成された時刻。	レコードはさまざまな会議イベントが発生したときに作成されます。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。 着信 CDR ログ イベントはローカル タイムスタンプで（UTC ではなく）保存されます。 時刻を変更すると（システム時刻を変更するかまたは NTP 更新によって）、CDR ログ内の新しいイベントが新しい時刻を表示するようになります。既存のレコードのタイムスタンプへの変更は行われません。
Conference	このレコードが適用される会議の GUID。	各新しい会議はグローバル一意識別子(GUID)で作成されます。特定の会議に関するすべてのレコードにこの ID が表示され、会議イベントの監査をより簡単に行うことができます。 この会議に関連しているレコードだけを表示するには、GUID をクリックします。
Participant	このレコードを適用する参加者の GUID。	各参加者はグローバル一意識別子（GUID）によって表され、レコード管理を簡略化できます。 この参加者に関係しているレコードだけを表示するには、GUID 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
Message	コール詳細レコードのタイプ、および簡単な詳細（使用可能な場合）。	このタイプのすべてのメッセージの詳細を展開するには [>>] をクリックします。 [All] を選択して [Update display] をクリックすることで、すべてのメッセージに対しこれを実行できます。これは、**フィルタ文字列**と組み合わせることによって、メッセージに特定の単語を含むレコードを検索する際に役立ちます。

API クライアント

TelePresence Server は、直近でユニットに要求を行った 10 の API クライアントのログを記録します。このリストを表示するには、[Logs] > [API clients] の順にクリックします。

5 分を超えて API 要求をしていないクライアントはグレーアウトで表示されます。

API クライアントのリストを更新するには、[Refresh] をクリックします。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。これによって、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と、このリストに再表示されます。

デフォルトでは、このページは [Time since last request] 列でソートされています。

表 40　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	最後の要求がそのクライアントによって送信されてからの時間。	
Last request method	その API クライアントによって送信された最後の API 要求メソッド。	
Last request user	クライアントが API 要求に使用したユーザ名。	最後の API 要求の認証が失敗したクライアントにはここで *(authentication failed)* というフラグが付けられます。
Requests received since last reset	最後にリセットから受信した要求の数。	1 秒あたりに複数の要求が受信される場合、1 秒あたりの平均要求数が () に表示されます。 現在のしきい値は、1 秒あたり 1.8 の要求です。 「過剰にアクティブな」クライアントは、TelePresence Server と現在通信している場合にのみフラグが付けられます。 最後にリセットしてからの経過時間がテーブルの下、ボタンの横に表示されます。

フィードバックの受信者

何らかの変更が行われたときに、それを受信している受信者が処置を実行できるように、TelePresence Server はフィードバック イベントを発行します。フィードバック受信者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] をクリックすることで、すべての設定されたフィードバック受信者をクリアできます。この操作は取り消すことができません。

リスト内の各受信者には次の詳細があります。

表 41 フィードバック受信者の詳細

フィールド	フィールドの説明	使用方法のヒント
Index	受信者リスト内のその受信者の位置。	
Receiver URI	受信者の完全修飾 URI。	受信者は Cisco TelePresence Management Suite などのソフトウェア アプリケーションである場合があり、適切な API コールでフィードバック イベントに応答し、フィードバックの送信元から変更のリストを取得することができます。

Call Home の使用

注：TelePresence Server は現在 Anonymous Reporting のみをサポートしています。

TelePresence Server は、そのステータスと Cisco Call Home サービスに発生した障害に関するレポートを送信できます。TelePresence Server は、Call Home にレポートを送信する際は常にセキュア接続（HTTPS）を使用します。

Call Home が無効になっている場合（デフォルト設定）は、**Call Home モード**が選択されるまで、デバイスはいずれのタイプのレポートも送信しません。Call Home をイネーブルにしている場合は、手動でレポートを送信するか、または自動的に機能するように設定できます。

[Anonymous Call Home] を使用する場合、匿名で送信されたレポートを表示できません。それらのレポートはシスコのエンジニアのみが表示でき、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 レポートについて質問がある場合は、Cisco TAC までご連絡ください。

Call Home モードを [anonymous] に選択すると、[Automatic Call Home enabled] をオンにすることで、TelePresence Server が自動的にレポートを送信するように設定できます。この変更を適用するとすぐに、デバイスは保留中のレポートを送信します。

その後、予期しないデバイスの再起動またはメディア リソースの再起動に関する診断レポートが追加の手動による介入なしで自動的に送信されます。

自動 Call Home を使用しない場合は、[Call Home now] をクリックして、いつでも手動でレポートを送信できます。

デバイス インベントリ レポートは常に使用可能です。このレポートの存在は特別な状態や障害を示すものではありません。自動 Call Home がイネーブルの場合、TelePresence Server は常に起動時にこれらのレポートを送信します。

Call Home を設定するには、次の手順を実行します。

1. [Logs] > [Call Home] に移動します。
   [Status] セクションには、この機能がイネーブルかどうかと、現在使用可能なレポートが表示されます。
2. **Call Home モード**で [Anonymous Call Home] を選択します。
3. （任意）TelePresence Server が手動による介入なしでレポートを送信するようにするには、[Automatic Call Home enabled] をオンにします。
4. [Apply changes] をクリックします。
   [Are you sure you want to apply configuration changes?] と尋ねるダイアログが表示されます。
5. 続行するには [OK] をクリックし、設定変更を破棄するには [Cancel] をクリックします。
   自動 Call Home がイネーブルになると、TelePresence Server によって保留中のレポートがただちに送信されます。
6. （任意）**現在のレポート**を手動で送信するには、[Call Home now] をクリックします。

表 42 ステータス フィールド

フィールド	説明
Call Home status	Call Home のステータスを次のいずれかとして示します。 • [Automatic – Anonymous Call Home]：[Call Home mode] がイネーブルで、[Automatic Call Home enabled] がオンになっています。 • [Enabled – Anonymous Call Home]：[Call Home mode] がイネーブルで、[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 mode] がディセーブルになっている場合、TelePresence Server は起動時にイベントログにこれを記録します。また、[Call Home mode] がイネーブル（[Anonymous Call Home]）になっているが、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、TelePresence Server はメッセージもログに記録します。
Current reports	使用可能なレポートのリスト。

フィールド	説明
Submission status	日付と時刻を含む、最近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、ステータスは [Not sent] となります。
Last submitted report reference	このフィールドは、**予期しないメディア リソースの再起動の診断**レポートまたは**予期しないデバイスの再起動の診断**レポートが送信された場合にのみ表示されます。この参照番号は、レポートの分析のために Cisco TAC に提示できます。
Call Home now	**現在のレポート**を手動で送信します。 手動でレポートを送信するか、または自動レポートをイネーブルにすると、データがシスコに送信されることを示す確認の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 回目の試行後に送信が失敗すると、バナーが Web インターフェイスに表示されます。

表 43　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。（デフォルトの [Disabled] では、レポートを送信することはできません。）
Automatic Call Home enabled	必要に応じて TelePresence Server が診断レポートを送信できます。また、起動時に、TelePresence Server がインベントリ レポートを送信できます。

参照先

コンテンツ チャネル サポート

ほとんどの TelePresence エンドポイントでは、2 番目のビデオ 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。

- H.323 システムは H.239 というプロトコルを使用して、コンテンツ チャネルのビデオの送受信します。
- SIP システムは、コンテンツに対し BFCP というプロトコルを使用します。
- Cisco CTS システムや他の 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 ビデオのコンテンツを許可することによって、2 番目のビデオ チャネルをサポートしていないエンドポイントの要求を満たします。この機能がイネーブルの場合、TelePresence Server は、それらのエンドポイントにメイン ビデオ チャネルの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な一方でコンテンツ チャネルは正常なビデオで構成されます（コンテンツは最大のペインに表示され、他の参加者のビデオ ストリームはディスプレイの下部で連続表示ペインで中央に配置されます）。

レイアウト ビューで参加者を表示する方法について

注：これらのオプションは、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設定できません。

このページの内容

- メイン ビデオでのコンテンツの許可
- エンドポイントを囲む境界線表示の設定
- 参加者を「重要」としてマーク
- ミュートされた参加者

会議のレイアウト

システムの TelePresence Server によって選択されるレイアウトは、システムが持つ画面数と他の会議参加者の特性によって異なります。また、エンドポイントは、遠端カメラ制御や DTMF キー 2 および 8 を持つレイアウトを選択したり、または次の選択肢の 1 つに事前設定したりすることもできます。TelePresence Server は、1、2、3、および 4 画面の標準およびイマーシブ エンドポイントで動作し、会議内の他のタイプのシステムに会議に参加しているシステムの組み合わせを表示できます。

一般に、TelePresence Server の動作は、最も顕著なレイアウト ペインで「最も音量が大きい」参加者を表示することです。使用可能なペインより多くの共同作成者がいる場合、「最も音量が小さい」参加者は表示されません。

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規模または参加者 1 人あたりで設定できます。このデフォルト設定は、参加者によって遠端カメラ制御または DTMF キー 2 および 8 を使用してレイアウト選択を変更することで上書きできます。

ActivePresence レイアウトでは、最も音量が大きい参加者は全画面に表示され、他の参加者は画面の下部の最大 6 つの均等にサイズ分けされたオーバーレイ ペインに表示されます。追加の参加者は [Participant Overflow] アイコンで示されます。

TelePresence Server は、**1 画面エンドポイントのデフォルト レイアウト タイプ**の設定に従って、1 画面エンドポイントのレイアウトを構成します。

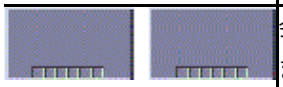
表 44　1 画面エンドポイントに送信されるレイアウト

	*シングル*：エンドポイントは、1 つの全画面ペインに表示されます。
	*ActivePresence*：エンドポイントは 1 つの全画面ペインに表示され、他の参加者は画面の下部の最大 6 つの均等にサイズ分けされたオーバーレイ ペインに表示されます。追加の参加者は、表示されていない参加者の数とともに右下隅に [Participant Overflow] アイコンで示されます。
	*対象拡大表示*：エンドポイントは 1 つの大きなペインに表示され、他の参加者は画面の下部の最大 6 つの均等にサイズ分けされたペインに表示されます。追加の参加者は、表示されていない参加者の数とともに右下隅に [Participant Overflow] アイコンで示されます。

	*均等*：エンドポイントは 4 X 4 までの画面に均等にサイズ分けされたペインのグリッド パターンで表示されます。 ペインの各行は、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。

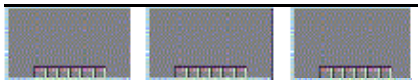
2 画面システムに送信されるレイアウト

表 45　2 画面システムに送信されるレイアウト

	TelePresence Server が会議室スイッチド表示モードの場合に、会議に 3 画面または 4 画面の TelePresence システムがある場合、TelePresence Server はその会議の 2 画面システムにこのレイアウトを送信します。 4 つのペインの各行は、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。
	会議に 1 画面および 2 画面システムしかない場合、TelePresence Server はこのレイアウトを使用します（すべてのビデオ ストリームが使用可能なペインに適合する場合）。可能な場合、オーバーレイ ペイン（最大 6 つ）が自動的に中央に配置されます。

3 画面システムに送信されるレイアウト

表 46　3 画面システムに送信されるレイアウト

	pip のないレイアウトが使用可能です。つまり pip なしにする必要があります。DTMF 2 および 8/ FECC を使用して選択できます。
	TelePresence Server が会議室スイッチド表示モードの場合に、会議に 4 画面の TelePresence システムがある場合、TelePresence Server はその会議の 3 画面システムにこのレイアウトを送信します。 4 つの大きいペインの中央の行は、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。この行を正しく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。
	会議に 4 画面の TelePresence システムがない場合、TelePresence Server はその会議の 3 画面システムにこのレイアウトを使用します。

4 画面システムに送信されるレイアウト

TelePresence Server は会議の 4 画面システムにこのレイアウトを送信します。

4 つのペインの各行（4 つのフルスクリーン ペインから構成される行または 6 つの小さいオーバーレイ ペインの行の 1 つ）は、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、オーバーレイ ペインが自動的に中央に配置されます。

OneTable モード

OneTable モードの TelePresence Server は、コール参加者の 3 つの異なるビデオ ストリームに関与し、それ故、TelePresence Server はこれらのシステムから受信した 3 つのストリームを 3 つの隣接するペインに並べて表示できなくなりました。

OneTable モードを有効にするには、会議の設定ページに移動し、[Use OneTable mode when appropriate] を [4 person mode] に設定します。

[4 person mode]：TelePresence Server は、物理的な場所に関係なく、テーブルの片側に 4 人が隣り合わせで座っているかのように参加者のビデオ ストリームを構成します。

会議には、OneTable 機能をサポートする少なくとも 3 人の参加者が存在する必要があります。

接続されたシステムに送信される会議のレイアウトは、次のように、そのシステムが持つ画面の数に応じて異なります。

表 47　OneTable モードのレイアウト

	1 画面システムに送信されるレイアウト可能な場合、オーバーレイ ペインが自動的に中央に配置されます。
	2 画面システムに送信されるレイアウト
	3 画面システムに送信されるレイアウト可能な場合、オーバーレイ ペインが自動的に中央に配置されます。
	4 画面システムに送信されるレイアウト可能な場合、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**セルフ ビュー**設定によって、TelePresence Server がそのエンドポイント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します。この設定がオフの場合、エンドポイントにはそれ自体のビデオ ストリームが表示されません。

エンドポイントがそれ自体のビデオを表示することを許可すると、参加者がコール内の最も音量が大きい人の 1 人だった場合でも（すなわち、その参加者が他の会議参加者より目立って表示される場合でも）、TelePresence Server は参加者を使用可能なビュー ペインに配置するときに常にセルフ ビューを最後に配置します。

1 画面エンドポイントのフルスクリーン ビューの表示

参加者をレイアウト ペイン内に配置する際、TelePresence Server は、「最も音量が大きい」人を最初に最も目立つペインに配置し、最も音量が小さい人を小さいペインに配置します。ただし、TelePresence システム（通常は大きい高解像度のディスプレイを使用）と低品質のビデオ（たとえば、ビデオ対応携帯電話）に対応できるシステムを組み合わせた会議では、低解像度の参加者を大きな全画面ペインに表示することが望ましくない場合があります。

1 画面システムの場合、[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できるか（およびその方法）が決定します。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は、マルチスクリーン エンドポイントのメイン ペインを常に占有できます。
- [Dynamic]：1 画面エンドポイントは、他のマルチスクリーン エンドポイントがその会議にいない場合に、マルチスクリーン エンドポイントのメイン ペインに表示されます。マルチスクリーン エンドポイントが会議に参加すると、1 画面エンドポイントは PiP ストリップに降格されます。
- [Disabled]：1 画面エンドポイントは、マルチスクリーン エンドポイントのメイン ペインには表示されません。

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

メイン ビデオでのコンテンツの許可

この機能によって、TelePresence Server は、追加チャネルをサポートしないエンドポイントのメイン ビデオ チャネルの会議コンテンツを送信できます。そうでなければコンテンツを表示できません。

コンテンツ チャネルのストリームは、この構成されたレイアウトの最も大きいペインを付与され、それはメイン ビデオ チャネルに表示されます。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下に構成されます。連続表示ペインは中央に配置されます。

エンドポイントを囲む境界線表示の設定

[Show borders around endpoints] がイネーブルの場合、TelePresence Server は、小さいペインに表示される参加者を囲む境界線を引きます。全画面ペインに表示されている参加者を囲む境界線は引かれません。

TelePresence Server は会議のアクティブなスピーカーを囲む青色の境界線を引き、他のすべてのケースでは灰色の境界線を引きます。たとえば、全員がミュートになっている場合や誰も話していない場合など、会議で強調表示されるのはいつもアクティブなスピーカーとは限りません。

エンドポイントにこの設定をイネーブルにすると、そのエンドポイントに送信されたビデオ レイアウトが境界線を使用することを意味します。これは、この参加者が他の参加者への境界線内に常に表示されることを意味するものではありません。これらの他の参加者のビューは、それ自体の [Show borders around endpoints] 設定を使用します。

参加者を「重要」としてマーク

各会議では、1 人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 がどの共同作成者をどのレイアウト ペインに表示するかを決定する際に、通話する声の大きさによって設定されているリスト内の位置よりも、この参加者を最初に考慮することを意味します。「会議ステータスの表示」のエンドポイントの管理設定を参照してください。

ミュートされた参加者

オーディオ ミュート

Web インターフェイスから音声がミュートされた参加者は会議に音声を提供しません。また、ミュートされた参加者は、TelePresence Server がビューのレイアウト ペインに参加者を配置するときに、ミュートされていない参加者の後と見なされます。

ある参加者がミュートされたことは他の参加者には示されないことに注意してください。単にその参加者の通話が聞こえなくなります。

ビデオ ミュート

Web インターフェイスからビデオがミュートされた参加者は会議にビデオを提供しません。彼らは個別にミュートされない限り、通常どおり音声を提供し続けます。

エンドポイント タイプ

表 48 エンドポイント タイプ

エンドポイント タイプ（UI に表示されます）	ハードウェアの名前と型番
規格	標準のビデオ エンドポイント。次に例を示します。 • EX60 / EX90 • C シリーズ コーデック（C20、C40、C60、C90） • Cisco Jabber • Microsoft Lync • その他の非 TIP サードパーティ エンドポイント また、エンドポイント タイプが TelePresence Server で不明の場合にも表示されます。
TANDBERG T1 または TANDBERG 1 画面 TelePresence	Cisco TelePresence System T1（旧称 TANDBERG telepresence T1）
TANDBERG T3 または TANDBERG 3 画面 TelePresence	Cisco TelePresence System T3（旧称 TANDBERG Telepresence T3）
カスケード	別の TelePresence Server（メディア 310/320、MSE 8710、または仮想マシンでの Cisco TelePresence Server）へのカスケード コール
N 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 ソフトウェアを実行中の Cisco CTS システムの不明なタイプ（CTS 1.6 / 1.7 ～ 1.7.3 まで）
	• レガシー ソフトウェアを実行中の Cisco CTS 単一画面システム（CTS 1.6 / 1.7 ～ 1.7.3 まで）。次に例を示します。
	  • CTS 500
	  • CTS 1000
	  • CTS 1100
	• レガシー ソフトウェアを実行中の Cisco CTS 3 画面システム（CTS 1.6 / 1.7 ～ 1.7.3 まで）。次に例を示します。
	  • Cisco TelePresence System 3000 シリーズ（CTS 30x0）
	  • Cisco TelePresence System 3200 シリーズ（CTS 32x0）

エンドポイント タイプ（UI に表示されます）	ハードウェアの名前と型番
SIP テレプレゼンス	CTS 1.7.4 以降を実行中の Cisco CTS または他の TIP 対応システムの不明なタイプ
SIP 1 画面 TelePresence	CTS 1.7.4 以降を実行中の Cisco CTS または他の TIP 対応 1 画面システム。次に例を示します。 • CTS 500 • CTS 1000 • CTS 1100
SIP 3 画面 TelePresence	CTS 1.7.4 以降を実行中の Cisco CTS または他の TIP 対応 3 画面システム。次に例を示します。 • 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

エンドポイントの相互運用性

表 49　エンドポイントの機能サポート

機能	これをサポートするエンドポイント	注意
パネル スイッチド レイアウトへの最も音量が大きい参加者の公開	T3、CTS 3200、CTS 3000、TX9000、および TX9200	CTS 1300 およびエンドポイント グループは最も音量が大きい参加者を公開しません。 **注**：一部の T3 システムは位置オーディオ（つまり T3 カスタム）を提供できません。
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	エンドポイントが 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）を実行している場合は、[Add legacy TIP endpoint] を使用してこれらのエンドポイントを追加する必要があります。 エンドポイントが CTS ソフトウェア バージョン 1.7.4 以降を実行している場合は、[Add new endpoint] を使用してこれらのエンドポイントを追加することができます。 **注**：リモート管理モードは設定済みのエンドポイントを許可しないので、エンドポイントはローカル管理モードでのみ追加できます。

機能	これ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。これらは、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示します。
OneTable モード	T3	会議の一部の参加者がこれらのエンドポイントを使用していて、OneTable モードがイネーブルの場合、TelePresence Server は OneTable レイアウト モードを使用します。

クラスタリングについて

クラスタは、同じ Cisco TelePresence MSE 8000 シャーシでホストされる、1 つのユニットとして機能するようにリンクされたブレードのグループです。Cisco TelePresence Supervisor MSE 8050 を使用してクラスタを設定および管理できます。

クラスタは、クラスタ内のすべてのブレードの組み合わせたスクリーン ライセンス数を提供します。この画面の数値が大きいと、追加の参加者を含む会議や複数の小さな会議を柔軟に設定できます。

Cisco TelePresence Server MSE 8710 クラスタの概要

ソフトウェア バージョン 2 以降を実行している Cisco TelePresence Server MSE 8710 ブレードはクラスタリングをサポートしています。現在は、最大 4 つのブレードをクラスタ化でき、1 つのブレードをマスターに、他のブレードをスレーブにします。

マスターは、必要に応じてクラスタのライセンスを割り当てることができます。たとえば、すべてを 1 つの大規模な会議に割り当てたり、複数の小さな会議に分散したりできます。詳細については、79 ページの「TelePresence Server の会議容量について」を参照してください。

マスター TelePresence Server

クラスタ内の各 TelePresence Server 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キャパシティはマスターによって制御されます。Web インターフェイスまたは API を使用して、マスター経由で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で作成されます。

スレーブ TelePresence Server

スレーブ TelePresence Server では、完全な Web インターフェイスが表示されません。ネットワークおよびロギングの設定を構成したり、ソフトウェアをアップグレードするなどの、一部の設定ページを使用できます。

同様に、スレーブ TelePresence Server は API コマンドの完全な補完に応答しません。詳細については、関連する API の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で 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、最初に新しいソフトウェア イメージをクラスタ内の各ユニットにアップロードし、それからマスターを再起動します。スレーブが自動的に再起動し、アップグレードが完了します。

概要ポイント

次は、クラスタリングに関する注意すべきポイントです。

- スーパーバイザは、クラスタリングを設定するにはソフトウェア バージョンが 2.1 以降を実行している必要があります。
- クラスタ内のすべての TelePresence Server が同一のソフトウェア ビルドを実行している必要があります。
- クラスタ内の各ブレードに *クラスタ サポート*の機能キーが必要です。
- 8710 ブレード上で実行している TelePresence Server の同一ビルドで 8510 ブレード上の MCU ソフトウェアを交換していれば、MCU MSE 8510 番台で TelePresence Server MSE 8710 番台をクラスタ化できます。MCU MSE 8510で MCU ソフトウェアを交換するための適切なガイドを取得するには、TelePresence Server インストール ガイドのサイトを参照してください。
- シャーシには複数のクラスタを含めることができ、シャーシは異なるタイプのクラスタをホストできます。
- クラスタリングをサポートしていないブレードをクラスタとともに MSE 8000 シャーシに設置できます。

- シャーシ内のスロットにクラスタ ロール（マスター/スレーブ）を割り当てる必要があります（スーパーバイザ経由で）。ブレードに障害が発生した場合は、そのブレードを交換でき、クラスタの設定が持続しますが、アクティブなコールおよび会議が次のように影響を受けます。
  - 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。すべてのコールおよび会議が終了します。
  - スレーブ ブレードに障害が発生すると、スーパーバイザおよびブレードのクラスタリング設定が合わなくなる可能性があります。この場合、スーパーバイザがブレードにクラスタリング設定をプッシュします。クラスタリング設定にはクラスタリング情報のみが含まれています。これによってブレードのネットワーク設定やその他の設定は行われません。スーパーバイザがブレードに設定変更をプッシュすると、スーパーバイザからブレードを再起動するように求められます。
  - スーパーバイザが再起動または削除されると、クラスタは機能を継続し、会議は継続され、スーパーバイザが再表示されたときにクラスタは再起動しません。
- スーパーバイザの最新のバックアップを常に保持してください。

TelePresence Server の会議容量について

ここでは、すべてのタイプの Cisco TelePresence Server について説明します。ご自身の特定のモデルに関連する情報を検索してください。

ライセンス キーおよびスクリーン ライセンス

TelePresence Server のライセンス モデルは「スクリーン ライセンス」に基づいています。そのライセンスは、ライセンス アクティベーション キーの形式で購入および提供されます。スクリーン ライセンスは、TelePresence Server の会議容量をアクティブにします。TelePresence Server の全容量は、最大ライセンス数を適用することでアクティブ化されます。その数は、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 つの TelePresence Server MSE 8710 番台のクラスタ	それぞれ 24、36、または 48
TelePresence Server 7010	12
Media 310 の TelePresence Server	6
Media 310 の 2 つの TelePresence Server のクラスタ	12
Media 320 の TelePresence Server	12
Media 310 および Media 320 の TelePresence Server の混在クラスタ	18
Media 320 の 2 つの TelePresence Server のクラスタ	24
仮想マシンの TelePresence Server（8 コア）	4
仮想マシンの TelePresence Server（8 コア、HD）	5

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
仮想マシンの TelePresence Server（30 vCPU / 高密度 VM）	10
Media 400v の TelePresence Server	18
Media 410v の TelePresence Server	27

TelePresence Server MSE 8710 番台にライセンスを供与する場合は、スーパーバイザの Web インターフェイスを介してシャーシにライセンス キーを適用してから、それらのブレードを格納するスロットにスクリーン ライセンスを割り当てます。

他のプラットフォームにライセンスを供与する場合は、[Configuration] > [Upgrade] ページで、TelePresence Server の Web インターフェイス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供与

TelePresence Server MSE 8710 ブレードのクラスタにライセンスを供与する場合は、各ブレードのスロットにライセンスを割り当てることを推奨します。実際には、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ているスクリーン ライセンスの合計になるように、有効なスクリーン ライセンスがクラスタ内のマスター ブレードに効果的にプールされ割り当てられます。

Media 310/320 プラットフォームで TelePresence Server のクラスタにライセンスを供与する場合は、各ユニットにライセンス キーを適用することを推奨します。実際には、スレーブがダウンしてもマスターはすべてのライセンスを制御します。しかし、今後ユニットを分離させる場合、またはユニットの 1 つに壊滅的な障害が発生した場合は、クラスタが分割された後にユニットをカバーする独立したライセンスが必要です。

動作モード

TelePresence Server 7010 および MSE 8710 の動作モードには、リモート管理モードとローカル管理モードの 2 つがあります。動作モードは、スクリーン ライセンスが同時発生コールをホストする容量にどのように変換するかに影響します。

注：Media 310/320 の TelePresence Server および仮想マシンの Cisco TelePresence Server は、ローカル管理モードをサポートしていません。これらのプラットフォームでは、TelePresence Server は 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提示される情報は、ソフトウェアにローカルまたはリモートの管理モードの概念がない場合でも、Media 310/320、および仮想マシンのプラットフォームに関連します。

ローカル管理モード（7010 および 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コールの固定数に変換します。これは、HD モードに応じて、スクリーン ライセンス 1 つにつき 1 コールまたは 2 コールにできます。

- 「フル HD」モードのライセンスでは、関連付けられた音声とコンテンツのチャネルを含む、最大 1080p30 または 720p60 ビデオのコールが 1 つ許可されます。
- 「HD」モードのライセンスでは、関連付けられた音声とコンテンツのチャネルを含む、最大 720p30 または w448p60 ビデオのコールが 2 つ許可されます。

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

各 TelePresence Server ユニットでは、ビデオ ポート、音声専用ポート、およびコンテンツ ポートの数は限られています。各ビデオ ポートには、コンテンツが使用されるかどうかにかかわらず、対応するコンテンツ ポートが割り当てられます。

同時コールの制限数を示した次の表では、これらのポートがローカル管理モードの TelePresence Server に使用可能な 2 つの HD モードにどのように割り当てられるかについて示しています。

リモート管理モード（全モデル）

リモート管理モードでは、スクリーン ライセンスはより細かな方法でコールに割り当てられます。各スクリーン ライセンスは、1 つのフル HD コール（ローカル管理モードでの）または多数のリソースが少ないコールに対する十分な容量をロック解除します。

たとえば、1 つのスクリーン ライセンスでは、1 つの 1080 コール、または 2 つの 720 コール、あるいは 4 つの 448 コール、または 8 つの 360 コールに対する十分な容量が提供されます。

コールの制限数

次の表に、上で説明した動作の各モードにおける TelePresence Server のコール容量を示します。

ローカル管理モードの同時コールの制限数（7010 および MSE 8710 のみ）

表 50　HD モードのハードウェア タイプごとのポート割り当て

ハードウェアの配置	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 つの 8710 番台のクラスタ	48	48	20

ハードウェアの配置	ビデオ ポート	コンテンツ ポート	音声専用ポート
3 つの 8710 番台のクラスタ	72	72	30
4 つの 8710 番台のクラスタ	96	96	40

表 51　フル HD モードのハードウェア タイプごとのポート割り当て

ハードウェアの配置	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 つの 8710 番台のクラスタ	24	24	20
3 つの 8710 番台のクラスタ	36	36	30
4 つの 8710 番台のクラスタ	48	48	40

リモート管理モードでの同時コールの制限数

マニュアルの入手とサービス要求の送信

マニュアルの入手方法、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、『What's New in Cisco Product Documentation』（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』に配信登録すると、新しい（または改訂された）シスコ技術情報のリストが RSS フィードとして提供され、リーダー アプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。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