Cisco TelePresence Server on Multiparty Media 820

印刷可能なオンライン ヘルプ

2015 年 8 月

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、Cisco TelePresence Server on Multiparty Media 820 にインストールして使用する 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. 次に、[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 820 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 Media 820 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。	最大 2 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 ライセンスを有効化するには、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」（74 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
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 ℃ 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。

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
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。

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 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。	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。
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。

フィールド	フィールドの説明	使用方法のヒント
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。クラスタの場合、スクリーン ライセンスの割り当て方法は重要ではありません。これは、マスターがすべてのスクリーン ライセンスを制御するためで、スレーブに障害が発生しても、マスターはそのスレーブに割り当てられてい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 の [Status] > [Cluster] ページには、マスターのステータスが表示されます。

次の表は、[Status] > [Cluster] ページに表示される、クラスタ内のスレーブ TelePresence Server に関する情報を示しています。マスター TelePresence Server の情報については、「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、一部の設定は使用できません。

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。数分待ってから、[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、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 は、マスターとの接続が切断されると自動的に再起動します。これは、スレーブがクラスタに正常に再接続できる唯一の方法です。 スレーブとマスターの接続が切断される一般的な理由は、マスターの再起動です。

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、最大で 11 秒間マスターが検出されなかった場合にのみ表示されます。スレーブはマスターとの接続が切断されるとすぐに再起動します。	
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 でネットワーク設定を行って、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 configuration] 設定

これらの設定によって、TelePresence Server の該当するイーサネット ポートの IP 設定が決まります。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 はこのポートの独自の IP アドレスを DHCP（Dynamic Host Configuration Protocol）経由で自動的に取得します。[Manual] に設定すると、TelePresence Server は、以下の [Manual configuration] のフィールドに指定した値を使用します。	IPv6 を使用してログインした場合にのみ TelePresence Server ポートの IPv4 を無効にできます。
IP address	このポートのドット区切りの IPv4 アドレス（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のみ指定する必要があります。 ポート A については、IP 設定を [Automatic by DHCP] に設定した場合、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] を選択する場合は、IPv6 アドレス、プレフィックス長、およびデフォルト ゲートウェイも指定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。これには、ICMPv6 ルータ アドバタイズメント（RA）メッセージの指定に応じて、SLAAC、ステートフル DHCPv6 またはステートレス DHCPv6 が使用されます（下記の IPv6 アドレス自動設定を参照）。	ネットワークで IPv6 がサポートされていない場合は、ポートの IPv6 を無効にします。 IPv4 を使用してログインした場合にのみ TelePresence Server ポートの IPv6 を無効にできます。
IPv6 address	[Manual] 設定を選択した場合は、CIDR 形式で IPv6 アドレスを指定します（`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] を選択すると、手動で入力し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、このアドレスに対して固定された（10 進数）ビット数です。
Default gateway	（任意）このサブネット上のデフォルト ゲートウェイの IPv6 アドレスを指定します。	アドレスは、グローバルの場合とリンクローカルの場合があります。

IP status

[IP status] セクションには、自動設定か手動設定かにかかわらず、TelePresence Server のこのイーサネット ポートに関する現在の IP 設定が表示されます。内容は次のとおりです。

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 のこのポートに対してイーサネット設定を行って、[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] を選択する場合は、速度およびデュプレックスの設定も指定する必要があります。接続されたデバイスとのイーサネット設定のネゴシエーションをこのイーサネット ポートで自動的に行う場合は、[Automatic] を選択します。	イーサネット接続している両方のデバイスの設定が同じである必要があります。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、同じ固定速度およびデュプレックスを両方のデバイスに設定します。 接続速度を [1000 Mbit/s] にする必要がある場合は、[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 [100 Mbit/s] 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すが、半二重モードでは双方向伝送のみ可能で、同時には伝送できません。

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。	

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、このポートが接続しているデバイスとの間で行われるネゴシエーション、または手動設定によって決まります。
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、このポートが接続しているデバイスとの間で行われるネゴシエーション、または上記で選択した [Manual] 設定によって決まります。
MAC address	このポートの固定ハードウェア MAC（メディア アクセス コントロール）アドレス。	この値は情報として表示されるだけで、変更することはできません。
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 および UDP トラフィック）。	この情報によって、TelePresence Server がネットワークにパケットを送信していることを確認できます。
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）。	この情報によって、TelePresence Server がネットワークからパケットを受信していることを確認できます。
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、ネットワークの問題を診断する際に役立ちます。

DNS の設定

TelePresence Server の DNS 設定を確認および変更するには、[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 によるネーム サーバ アドレスの取得方法を選択します。 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 ネットワーク経由で DHCP を使用して自動的にネーム 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 アドレスを指定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）を指定することもできます。	選択したインターフェイスでスタティック IP アドレスを設定している場合、TelePresence Server で自動的にネーム サーバ アドレスを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、さらに [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 には、DNS サーバが設定されないことを示す警告が表示されます。
Host name	TelePresence Server の名前を指定します。	ホスト名には最大で 63 文字まで使用できます。 ネットワーク設定によっては、IP アドレスを把握していなくても、このホスト名を使用して 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] の場合は必須です。
Secondary name server	オプションで 2 番目のネーム サーバを指定します。	2 番目のネーム サーバを設定した場合、TelePresence Server はいずれか一方のネーム サーバに DNS クエリを送信する場合があります。
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。	デバイスの参照に（IP アドレスではなく）非修飾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。 ドメイン名（サフィックス）を *cisco.com* に設定した場合、ネーム サーバに対してホスト *endpoint* の IP アドレスを検索する要求を行うと、実際には *endpoint.cisco.com* が検索されます。

DNS ステータスの表示

TelePresence Server の現在の DNS 設定を確認するには、次を含む DNS ステータスのフィールドを使用します。

- Host name
- Name server

- Secondary name server
- Domain name (DNS suffix)

IP ルートの設定

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 つ以上のルートの設定が必要な場合があります。

これらのルートを正確に作成することが重要です。ルートに誤りがあると、コールを発信したり、Web にアクセスしたりすることができなくなる可能性があります。

ルートを設定するには、[Network] > [Routes] に移動します。

このページの内容

IP ルートの設定

このセクションでは、IP パケットが TelePresence Server から転送される方法を制御できます。この設定は、TelePresence Server が接続されているネットワーク トポロジを十分理解している場合にのみ変更してください。

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、および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、[Port A] のデフォルト ゲートウェイ経由または指定した [Gateway] 経由のどちらで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か、既存のルートのエイリアス（オーバーラップ）である場合、ルートの修正を求めるプロンプトが表示されます。

参考として、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：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。アドレスの固定されていないビットはすべて 0 に設定します。[mask length] フィールドを使用して、固定されたビット数を指定します（これにより、固定されていないビット数で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。アドレスの固定されていないビットはすべて 0 に設定します。[mask length] フィールドを使用して、固定されたビット数を指定します（これにより、固定されていないビット数で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、マスク長を 25 に指定します。最初の 25 ビットが固定されており、最後の 7 ビットによってアドレス範囲が決ま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 アドレスに 2001:db8::、マスク長に 112 を入力します。最初の 112 ビットが固定されており、最後の 16 ビットによってアドレス範囲が決ま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のルーティング方法を制御する場合に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、パケットの送信先となるゲートウェイの IP アドレスを入力します。 [Port A] を選択すると、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 ルートの表示または削除について

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およびマスク
- 一致するパケットのルーティング先として、次のように表示されます。
  - [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。
- ルートが、他の設定に応じて自動的に設定されたか、手動で追加されたか。

デフォルト ルートは、IPv4 および IPv6 の [Default gateway] 設定の選択内容（「ネットワークの設定」を参照）によって自動的に設定されます。削除することはできません。手動で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。

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

現在のルートのテーブル

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 に対して設定された（手動と自動の両方）すべてのルートが表示されます。イーサネット ポートの IP 設定は、[Network] > [Network settings] から変更できます。

IP サービスの設定

TelePresence Server で 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 インターフェイス用の HTTP やコールの発信および受信用の SIP などの Web サービスを提供します。サービスがユニットのイーサネット インターフェイスでアクセス可能かどうか、またこれらのサービスの利用に使用される 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] ページには、有効化された IP バージョンに応じて IPv4 または IPv6 サービス（または両方）を制御するオプションがあります。

1. 有効化するサービス名の隣にあるチェックボックスをオンにします。サービスを無効化する場合は、チェック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

   （一般的に使用されるポートの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：最小エフェメラル ポートは、設定された TCP または UDP の最大サービス ポートよりも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、指定できる最小エフェメラル ポートは 20001 です。

1. 希望するエフェメラル ポート範囲の最小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. 希望するエフェメラル ポート範囲の最大ポート番号を入力します。

   デフォルトは 65535（設定可能な最大値）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はできません。5000 ポート未満の場合、会議機能がブロックさ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 によって、変更された設定がページのデフォルトに置き換えられます。これはすぐには適用されません。

2. [Apply changes] をクリックします。

   デフォルト設定が適用されます。

表 15 [Network] > [Services] **のフィールドの説明**

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 ページを表示および変更し、オンライン ヘルプ ファイルを読み取るには、Web アクセスが必要です。
HTTPS	指定したインターフェイスでのセキュア（HTTPS）Web アクセスを有効または無効にします。または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 には独自の SSL 証明書と秘密キーがあります。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。
SIP (TCP)	SIP over TCP を使用した TelePresence Server への着信コールを許可または拒否します。 または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ます。または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
SIP (UDP)	SIP over UDP を使用した TelePresence Server への着信および発信コールを許可または拒否します。または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 を使用したコールはできなくなります。
Minimum	エフェメラル ポート範囲の下限。	デフォルトでは 49152 に設定されていますが、10000 ～ 60535 の値を設定できます。
Maximum	エフェメラル ポート範囲の上限。	デフォルトは 65535 です。設定可能な最小値は 15000 です。最小範囲は 5000 ポートに制限されています。

QoS の設定

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

QoS とは、特定クラスのデータの処理をカスタマイズするネットワークの機能を指す用語です。たとえば QoS を使用して、HTTP トラフィックでの音声伝送およびビデオ伝送に優先度を指定することができます。これらの設定は、発信音声および発信ビデオのすべてのパケットに影響します。他のすべてのパケットは QoS が 0 で送信されます。

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 6 ビット値を設定できます。ネットワークは、この値をタイプ オブ サービス（ToS）または差別化サービス（DiffServ）として解釈します。機能の点では、IPv6 QoS と IPv4 QoS は同じであることに注意してください。

注意：必要がない限り、QoS 設定は変更しないでください。

QoS 設定を変更する場合は、6 ビット バイナリ値を入力する必要があります。

ToS および DiffServ の値を含む QoS の詳細は、Internet Engineering Task Force の Web サイト（www.ietf.org）で利用可能な次の 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 設定について

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

変更を行った後は、[Update QoS settings] をクリックしてください。

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 パケットに優先度を指定するための 6 ビット バイナリのフィールド。	必要がない限り、この設定は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 パケットに優先度を指定するための 6 ビット バイナリのフィールド。	必要がない限り、この設定は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 パケットに優先度を指定するための 6 ビット バイナリのフィールド。	必要がない限り、この設定は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 パケットに優先度を指定するための 6 ビット バイナリのフィールド。	必要がない限り、この設定は変更しないでください。

ToS 設定

ToS 設定は、優先度、遅延、スループット、および信頼性といった抽象パラメータ間のトレードオフを表します。

ToS では、使用可能な 8 ビットの内 6 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 と 7 にはゼロが入ります。

- ビット 0 ～ 2 で IP Precedence（パケットの優先度）を設定します。
- ビット 3 で遅延を設定します（0：通常の遅延、1：低遅延）。
- ビット 4 でスループットを設定します（0：通常のスループット、1：高スループット）。
- ビット 5 で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 と 7 は今後の使用に備えて予約されており、TelePresence Server インターフェイスを使用して設定することはできません。

音声パケットおよびビデオ パケットに優先度を割り当てることで調整し、ネットワーク上の他のパケットに大きな遅延が発生しないようにする必要があります。たとえば、すべての値を 1 に設定することは避けてください。

DiffServ 設定

DiffServ では、使用可能な 8 ビットの内 6 ビットを使用してコードポイントを設定します（64 のコードポイントを使用できます）。TelePresence Server ではビット 0 ～ 5 を設定でき、ビット 6 と 7 にはゼロが入ります。DiffServ ノードによってコードポイントが解釈され、パケットの処理方法が決まります。

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 の場合、これは IP Precedence が 5 に設定され、優先度が比較的高いことを意味します。遅延は低、スループットは高、信頼性は通常に設定されています。
  - DiffServ の場合は、Expedited Forwarding（EF; 完全優先転送）を意味します。
- [Video]： *100010*:
  - ToS の場合、これは IP Precedence が 4 に設定され、優先度がかなり高い（ただし音声の優先度ほど高くはない）ことを意味します。遅延は通常、スループットは高、信頼性は通常に設定されています。
  - 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。

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 を有効にすると（デフォルトで有効になっています）、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 にはローカル証明書と秘密キーが事前にインストールされており、HTTPS を使用したユニットへのアクセス時にブラウザに対する認証に使用されます。ただし、すべての Cisco TelePresence Server に同じデフォルト証明書および秘密キーがインストールされているため、独自の証明書とキーをアップロードしてセキュリティを確保することを推奨します。推奨されるキー長は 2048 ～ 8192 ビットです。

TelePresence Server では、TIP エンドポイントとの暗号化パラメータのネゴシエーションに DTLS を使用します。この際に証明書が必要です。TelePresence Server に実装された DTLS は、ユーザ指定の証明書を次のように処理します。

- Opportunistic DTLS では、ユーザ指定の証明書がアップロードされても、DTLS ネゴシエーションに必ず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ユーザ指定の証明書が使用されます（推奨処理）。

エンドポイントが RFC 5763 をサポートしている場合は Negotiated DTLS が使用されます。サポートしていない場合は、TIP コールで Opportunistic 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：TelePresence Server に*メディア暗号化*機能キーがある場合にのみ、DTLS のネゴシエーションが実行されます。

次の表を参考にしてフィールドに入力し、[Upload certificate and key] をクリックします。証明書とキーは同時にアップロードする必要があります。新しい証明書とキーをアップロードした後は、Cisco TelePresence Server を再起動してください。

注：証明書および秘密キーは PEM 形式にする必要があります。

ストアでは複数の証明書を保持することができます。これは、通常の BEGIN および END 証明書タグ内に連続して複数の PEM エンコード形式の CA 証明書を含む、単一の信頼ストア ファイルをアップロードすることで実現できます。

[Delete custom certificate and key] をクリックすれば、必要に応じて独自の証明書とキーを削除できます。証明書の削除後は、TelePresence Server を再起動する必要があります。

次の表で、[Network] > [SSL certificates] ページのフィールドについて説明します。

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都道府県。 • [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]：証明書の共通名、またはドメイン名。	
Issuer	証明書の発行元の詳細。	自身で発行した証明書の場合、これらの詳細は [Subject] の情報と同じです。
Issued	ローカル証明書の発行日。	
Expires	ローカル証明書の有効期日。	
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、Cisco TelePresence Server に返送するデータの暗号化に SSL 証明書の公開キーを使用します。Cisco TelePresence Server では秘密キーを使用してそのデータを復号化します。[Private key] フィールドに「Key matches certificate」と表示されている場合、データは双方向で安全に暗号化されます。

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た場合、または自身で証明書を生成できる場合は、その証明書をアップロードできます。[Choose File] をクリックし、証明書ファイルを見つけて選択します。	証明書および秘密キーは PEM 形式にする必要があります。
Private key	[Choose File] をクリックし、証明書に付属する秘密キー ファイルを見つけて選択します。	証明書および秘密キーは PEM 形式に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
Private key encryption password	秘密キーが暗号化形式で保存されている場合は、ここにパスワードを入力すると、Cisco TelePresence Server にキーをアップロードできるようになります。	

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	信頼ストアの証明書の詳細。通常は、ローカル証明書の確認に使用される機関によって発行された証明書です。	
Issuer	信頼ストアの証明書の発行元の詳細。	これらは信頼できる証明機関の詳細情報です。
Issued	信頼ストアの証明書の発行日。	
Expires	信頼ストアの証明書の有効期日。	

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	次の 2 つの理由により、信頼ストアが必要です。 • SIP TLS 接続のリモート エンドの ID を検証するため（着信または発信コール、または登録）。 • 発信 HTTPS 接続のリモート エンドの ID を検証するため（フィードバック レシーバ、`flex.participant.requestDiagnostics` を呼び出す API アプリケーションなど）。	信頼ストアの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。 ストアでは複数の証明書を保持することができます。 検証が必要な場合（次の設定を参照）、リモート側の証明書が信頼ストアに対して検証されます。リモート証明書は、いずれかの証明書の信頼ストアまたは信頼チェーンに存在する必要があります。 証明書を削除したり、更新したファイルに置き換えたりする場合は、[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。	次のいずれかのドロップダウン オプションを選択して [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に対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]：

フィールド	フィールドの説明	使用方法のヒント
		TelePresence Server は、SIP TLS および HTTPS のすべての発信接続に対して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 接続に対して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、最大 12 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 とリモートのビデオ会議デバイス（ホスト）間で発生したネットワークの問題のトラブルシューティングを実行できます。

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追跡できます。結果には、TelePresence Server とリモート ホストがネットワーク接続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。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テキスト ボックスに入力し、[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およびリモート ホストの IP アドレスが表示されます。

ping の結果に、エコー応答のラウンドトリップ時間（ミリ秒単位）と存続可能時間（TTL）の値が表示されます。

TelePresence Server とリモート ホストの間にある各中間ホスト（通常はルータ）については、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場合があります（無効な ICMP チェックサムを含む場合など）。TelePresence Server では無効な ICMP 応答も認識されないため、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 にそのホストへの IP ルートがあると、ping は成功します。この機能により、セキュリティに影響を与えずに TelePresence Server の IP ルーティング設定をテストできます。

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

ネットワーク統計情報（netstat）の表示

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確認するには、[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。または [Refresh] をクリックするか、[Resolve names] チェックボックスをオンまたはオフにすると更新されます。

表 22 [Netstat] のフィールドの説明

フィールド	説明
Resolve names	アドレスに対する DNS ルックアップを実行して、ホスト名（可能な場合）を表示するには、チェック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チェックボックスをオフにします。チェックボックスのオンとオフを切り替えるとデータが更新されます。
Protocol	接続で使用されているインターネット プロトコルおよびアドレッシング方式を示す *[tcp4]*、*[tcp6]*、*[udp4]*、または *[udp6]*。
Recv-Q	TelePresence Server でまだ処理されていないため、キューイングされているこの接続のバイト数。
Send-Q	リモート側でまだ確認応答されないため、キューイングされているこの接続のバイト数。
Local Address	この接続の TelePresence Server のアドレス。[Resolve names] をオフにした場合、このフィールドにローカル ソケットが **`address:port`** の形式で表示されます。[Resolve names] をオンにした場合、ソケットが **`hostname:servicename`** の形式で表示されます（可能な場合）。 例： **`ts.example.com:http`** または **`127.0.0.1:80`**
Foreign Address	この接続のリモート側のアドレス。[Resolve names] をオフにした場合、このフィールドに外部ソケットが **`address:port`** の形式で表示されます。[Resolve names] をオンにした場合、ソケットが **`hostname:servicename`** の形式で表示されます（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おり、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。

会議の設定のほとんどのデフォルトは、管理システム（TelePresence Conductor など）を使用して作成されます。

表 23 すべての設定済み会議の設定

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。	デフォルトでは有効（オン）になっています。
Show event log messages on console	チェックボックスをオンにしてシリアル コンソールへのイベント ログ出力を有効にするか、チェックボックスをオフにしてシリアル コンソールへのイベント ログ出力を無効にします。 選択内容は TelePresence Server を再起動しても保持されます。 このチェックボックスをオフにすると、TelePresence Server は、電源投入後からメディア リソースが使用可能になるまでの間、引き続きシリアル コンソールにイベント ログ メッセージを出力します。この期間を過ぎる	デフォルトではチェックボックスがオフになっているため、イベント ログのシリアル出力は無効です。このデフォルトは TelePresence Server のパフォーマンスを向上させます。したがって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 メッセージのキャプチャには 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」（55 ページ）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
	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。	
Disable serial console input during startup	起動中に TelePresence Server がコンソールからの情報を処理しないようにするには、チェックボックスをオンにします。	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、このチェックボックスをオンにすることを推奨します。
Require administrator login for serial console commands	ユーザが特定されない限り、TelePresence Server がコンソール コマンドを解釈しないようにするには、チェックボックスをオンにします。	このチェックボックスをオンにして、権限がなくても物理的にアクセスできるユーザからシリアル コンソールを保護することを推奨します。 **注：**TelePresence Server のコンソールでは、一部の Unicode 文字を使用できません。コンソール アクセスに使用するアカウントは、ユーザ名およびパスワードの ASCII 文字に限定されます。
Idle serial console session timeout	最後の入力後、TelePresence Server が開いているコンソール セッションを維持する分数。	権限のないユーザに対して無人のコンソール セッションが開いたままになることを避けるため、小さ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 の SIP 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、任意の時点で設定を変更したりする場合は、次の表で詳細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		*Use trunk*： • 指定した SIP サーバ アドレスにトランクを使用して発信 SIP コールを転送します。 • 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 コールのオンワード ルーティングを実行します。 *Call direct*： • 可能であれば、TelePresence Server は SIP コールを直接接続します。この場合、[Outbound address] および [Outbound domain] のパラメータは使用されません。 • 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、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、TelePresence Server はこのフィールドを無視します。 TelePresence Server は、指定されたアドレスに @ 記号が含まれていない発信 SIP コールに対してこの値を使用します。 発信ドメインを指定しない場合、TelePresence Server は代わりに発信アドレスを使用します。
Username	TelePresence Server は、デバイスが認証を必要とする場合、SIP デバイス（トランク宛先またはエンドポイント）での認証にこの名前を使用します。	
Password	TelePresence Server は、デバイスが認証を必要とする場合、SIP デバイス（トランク宛先またはエンドポイント）での認証にこのパスワードを使用します。	SIP 宛先では認証を要求できません。認証を行う場合は、このユーザ名とパスワードの組み合わせによる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]*、*[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。 接続でどのプロトコル（TCP、UDP、または TLS）が使用されていても、TelePresence Server は着信接続を受け入れて、この [Outbound transport] の設定に関係なく、同じプロトコルを使用して応答します。[Network] > [Services] ページでこれらのサービスを有効にする必要があります。
Advertise Dual IPv4/IPv6	TelePresence Server が IPv4 と IPv6 の混合ネットワークで SIP コールに対応できるようにする場合は、[Use ANAT] を選択します。	デフォルトは [Disabled] です。ANAT（Alternative Network Address Types）を使用するように設定すると、デバイスでセッション記述の ANAT 構文がサポートされます。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	次のいずれのオプションに対して、TelePresence Server が SRTP のネゴシエーションに SDES を使用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*機能キーがある場合にのみ表示されます）	TelePresence Server は、SIP による暗号化の使用をサポートします。SIP による暗号化が使用されている場合、音声およびビデオ メディアは Secure Real-time Transport Protocol（SRTP）を使用して暗号化されます。SRTP 使用時のキー交換のデフォルト メカニズムは、Session Description Protocol Security Description（SDES）です。SDES ではクリア テキストでキーを交換するため、コール制御メッセージには安全な転送とともに SRTP を使用することを推奨します。Transport Layer Security（TLS）も使用するように TelePresence Server を設定できます。これは SIP コール制御メッセージに使用できる安全な転送メカニズムです。 デフォルト設定は [For secure transports (TLS) only] です。

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

システム時間

表示される現在の時刻は、TelePresence Server による時刻です。

NTP

TelePresence Server は NTP プロトコルをサポートします。TelePresence Server を NTP サーバと自動同期させる場合は、NTP 設定を入力して [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 の有効なイーサネット インターフェイスのいずれかに対してローカルである場合、TelePresence Server と NTP サーバの通信に自動的にそのポートが使用されます。

NTP サーバがローカルでない場合、TelePresence Server と NTP サーバの通信にはデフォルト ゲートウェイとして設定されたポートが使用されます。ただし、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る場合（[Network] > [Routes] を参照）を除きます。

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 25 デバイスの時刻設定

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、チェックボックスをオンにします。	
UTC offset	使用するタイムゾーンの UTC からのオフセット。	英国夏時間やその他の夏時間方式など、タイム ゾーンの局地的な変更に関しては、手動でこのオフセットを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。	

ネットワーク アドレス変換（NAT）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、追加設定は不要です。

NTP サーバのローカル ネットワークで NAT を使用する場合、NAT 転送テーブルを設定して、TelePresence Server から NTP サーバの UDP ポート 123 に NTP データを転送する必要があります。

TelePresence Server のバックアップと復元

このページの内容

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

アップグレードが必要な TelePresence Server のメイン ソフトウェア イメージは、ファームウェア コンポーネントのみです。

TelePresence Server のメイン 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. メイン ソフトウェア イメージの [Current version] で、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. また、サポート ページにログオンして、最新のイメージが使用可能であるかどうかを特定します。
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オンします。
7. [Configuration] > [Upgrade] に移動します。
8. ハード ドライブにある解凍済みファイルを見つけます。

   [Browse...] や [Choose File] など、ボタンはブラウザによって異なります。
9. [Upload software image] をクリックします。TelePresence Server へのファイルのアップロードが開始され、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 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。以前の設定に戻したり、設定を別のユニットにコピーすることで実質的にユニットをクローニングしたりすることが可能です。

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。

後で設定を復元する場合は、次の手順を実行します。

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

   [Browse...] や [Choose File] など、ボタンはブラウザによって異なります。
3. 保存済みの設定で上書きする対象として、現在の [Network settings]、[User settings]、または両方を選択します。

   デフォルトで上書きの制御は選択されていません。ソフトウェアでは、既存のネットワーク設定およびユーザ アカウントの維持が想定されています。
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、上書きの対象となる設定を制御できます。

- [Network settings] をオンにすると、ネットワーク設定は指定し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 からバックアップしたファイルで復元する場合、またはアウト オブ サービス状態の 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て、競合が存在すると（両方のデバイスが同じ固定 IP アドレスを使用するように設定されてしまった場合など）、デバイスのいずれかまたは両方に IP を介し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、復元操作によって、既存のネットワーク設定が上書きされることはありません（QoS 設定のみ例外です）。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] をオンにすると、現在のユーザ アカウントとパスワードは指定したファイルの内容で上書きされます。
- ユーザ設定を上書きして、復元されたファイルのユーザ アカウントが現在のログインに対応していない場合は、ファイルのアップロード後に再びログインする必要があります。

TelePresence Server 機能の有効化

TelePresence Server の機能の多くは、使用する前にアクティブ化する必要があります（TelePresence Server がアクティブ化されていない場合、Web インターフェイス上部のバナーに警告が明示されます。それ以外、Web インターフェイスは通常どおりに表示され、機能します）。

新しい TelePresence Server ではすでにアクティブ化されています。アクティブ化されていない場合や、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有効化する場合は、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。

それぞれのキーは、特定の TelePresence Server に固有のものです。サプライヤが有効なキーを提供できるよう、キーを要求する際はデバイスのシリアル番号を確認してください。

TelePresence Server をアクティブ化する場合も、拡張機能を有効化する場合も、キーを適用するプロセスは同じです。

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

1. [Feature management] リストを参照して、機能がアクティブ化されてい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表示されます。
2. サプライヤから提供されたキーを、ダッシュも含めて*取得時と同じ状態で* [Add key] フィールドに入力します。
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に表示されます。

   キーが無効な場合は、再入力を求められます。

   キーは期間が限定されている場合があります。この場合は、有効期日が表示されるか、機能がすでに期限切れであ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もそのままリストに表示されます。
4. 後日再入力が必要になる場合に備えてキーを記録します。

TelePresence Server または機能が正常にアクティブ化されると、即座に適用され、その状態は TelePresence Server を再起動しても保持されます。

一部の機能は削除することができます。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 のシャットダウンと再起動

アップグレードの一環として、または電源をオフにするために、TelePresence Server のシャットダウンおよび再起動が必要になることがあります。

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、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。

   このボタンが [Confirm TelePresence Server shutdown] に変わります。
3. 再度ボタンをクリックして確定します。

   TelePresence Server のシャットダウンが開始されます。ページ上部のバナーが、シャットダウンに関する表示に変わります。

   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. 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する管理者パスワードを変更できます。これは、現在のユーザが「管理者」である場合にのみ該当します。このページにアクセスするには、[Configuration] > [Change password] に移動します。

定期的に管理者パスワードを変更することを推奨します。パスワードをメモして、安全な場所に保管してください。

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、この TelePresence Server に設定されている会議が、ステータス（[Active] や [Inactive] など）に関係なくすべて表示されます。

このリストにアクセスするには、[Conferences] に移動します。

デフォルトでは、会議は名前のアルファベット順にソートされます。ソート順序を変更したり、ステータスまたは URI でリストをソートしたりするには、該当するカラム見出しをクリックします。

このページで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、各会議に関する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	設定済みの会議の名前。	会議名をクリックすると、会議の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ている URI。	リモート管理モードの TelePresence Server は、個々の会議の URI をゲートキーパーに登録しません。 参加者がダイヤルできる URI を 2 つまで会議に指定できます。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。 URI は複数の PIN をサポートできるため、ゲスト/チェアーの PIN を個別に設定できます。 個々の参加者がダイヤルするそれぞれの 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	会議のステータスは次のとおりです。 • *Scheduled* • *Active* • *Inactive* • *Ending*	会議には次のものがあります。 • [Scheduled] の会議では、会議開始までの時間が表示されます。 • [Active] の会議では、[(<X> endpoints, <N> screens)] が表示されます。すべてのエンドポイントが音声専用の場合は、[Active (<X>

フィールド	フィールドの説明	使用方法のヒント
	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。	endpoints)] が表示されます。 • [Inactive] の会議は、実質的には [Active] 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、および期間は表示されます。 • [Ending] は会議が破棄中であることを示します。この間は、残っている参加者に終了ロビーが表示されます。 会議の期間、およびロックされているかどうかに関する追加情報がステータスに含まれている場合があります (例：Inactive - Ends in 5 hours and 27 minutes [Locked])。 会議の設定に関する警告が表示される場合があります（例：[No participants allowed - limited to 0 participants]）。

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。[Status] ページを表示するには、[Conferences] に移動して会議名をクリックします。

このページで会議の次の情報を確認できます。

- アクティブであるかどうか、および会議の参加エンドポイント数。
- 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。
- 以前に参加者がいたかどうか、およびその参加者名。
- 会議に URI が割り当てられているかどうか。

[Conference] > *会議名* > [Status] ページで可能な操作

- 参加者を選択して接続を解除（[Disconnect selected]）する。
- すべての参加者の接続を解除（[Disconnect all]）して、効率的に会議を終了する。
- 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。

- [More...] をクリックして参加エンドポイントに関する詳細なステータス情報を表示するか、[Expand all] をクリックしてすべてのアクティブ エンドポイントに関する情報を表示する（詳細は次の表を参照）。

会議ステータスの参照

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	会議のステータスは次のとおりです。 • *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] の会議では、会議開始までの時間が表示されます。 • [Active] の会議では、[(<X> endpoints, <N> screens)] が表示されます。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] の会議は、実質的には [Active] 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、および期間は表示されます。 • [Ending] は会議が破棄中であることを示します。この間は、残っている参加者に終了ロビーが表示されます。 会議の期間、およびロックされているかどうかに関する追加情報がステータスに含まれている場合があります (例：Inactive - Ends in 5 hours and 27 minutes [Locked])。 会議の設定に関する警告が表示される場合があります（例：[No participants allowed - limited to 0 participants]）。
URIs	会議に割り当てられている URI。	参加者がダイヤルできる URI を 2 つまで会議に指定できます。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。 URI は複数の PIN をサポートできるため、ゲスト/チェアーの PIN を個別に設定できます。 個々の参加者がダイヤルするそれぞれの 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されているかどうか。	次のいずれかになります。 • [No current presentation]：会議でコンテンツ共有が有効になっていますが、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 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	アクティブな会議に現在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すると、[Status] ページに移動します。
Type	エンドポイント タイプ。	
Authority	会議の参加者のロール（および関連付けられている権限）を示します（[Chair] または [Guest]）。	管理システムでこの会議にゲスト/チェアー制御レベルが明示的に適用されている場合を除き、デフォルトですべての参加者に対して [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]：エンドポイントはこの会議に参加します。 • [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]：エンドポイントが使用中のため、再試行が実行されています。 [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]（音声についても同様）、[important]、および [audio-only] などの追加ステータス情報が表示される場合があります。 事前設定されたエンドポイントが会議の開始時に使用中であった場合、TelePresence Server は会議中に 5 回までエンドポイントを再試行し、使

フィールド	フィールドの説明	使用方法のヒント
		用可能になると接続します。再試行の間隔は 5、15、30、60、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。会議へのエンドポイントの関与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  およびミュート  解除 ビデオのミュート  およびミュート  解除 参加者に対する「重要」（送信ストリームのみ）  または「重要でない」の設定 

表 29 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	以前この会議に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、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すると、[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に参加していない理由。	TelePresence Server がエンドポイントの接続を解除する理由には、次のようなものがあります。 • [requested by administrator]：管理者によってエンドポイントの接続が解除されました。 • [call rejected]：遠端側によってコールが拒否されました。 • [left conference]：会議の終了時にエンドポイントの接続が解除されました。 • [requested via API]：API によってエンドポイントの接続が解除されました。 • [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、これ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
		• [destination unreachable]：エンドポイントは到達不能でした。 • [Encryption not supported by far end]：コールに必要な暗号化を遠端側がサポートしていないか、暗号化が禁止されているコールで遠端側が暗号化を必要としています。 • [timeout]：接続がタイムアウトしました。 • [insufficient free ports]：空きポートが不足しているためにエンドポイントの接続が解除されました。 • [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の接続が解除されました。 • [Conference locked]：会議がロックされているためコールが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、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の接続が解除されました。 • [Network error]：ネットワーク エラーが原因でエンドポイントの接続が解除されました。 • [Unavailable]：エンドポイントを使用できません。 • [Capability negotiation error]：エンドポイントおよび TelePresence Server が、相互に互換性のあるコール設定のネゴシエーションを実行できません。 • [Insufficient token allocation]：TIP/MUX コールに対するトークンの指定/割り当てが十分ではありません。 • [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、エンドポイントの接続が解除されました。 • [No media received]：メディアの送信が予期せず停止してから 30 秒以上経過したため、TelePresence Server はこのエンドポイントの接続を解除しました。 • [unspecified error]：TelePresence Server ではエンドポイントが接続解除した理由を認識していません。

エンドポイントおよびグループ 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に参加している場合にのみ表示できます。このページでエンドポイントをある程度まで制御できます。

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. 次の表を参照して、エンドポイントを確認または制御します。
4. ブラウザのページを更新すると、最新のステータスが表示されます。

表 30 エンドポイントから提供される情報

フィールド	フィールドの説明	使用方法のヒント
Country code/extension	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。詳細情報の内容は、各メーカーによって異なる場合があります。	この情報はエンドポイントの初回接続後に表示されます。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	現在エンドポイントが会議に参加中であるかどうか、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、接続されている場合は着信または発信のどちらのコールか。	
Protocol	このコールで使用されるプロトコル（SIP など）。	
Endpoint advertised capabilities	コールのネゴシエーション時にエンドポイントがアドバタイズした機能。	[Audio]、[Video]、[Video content]、[Encrypted traffic]、[Unencrypted traffic] など。
Audio channels	Cisco TelePresence Server と遠端の間で送受信音声チャネルが開いているかどうか。	
Video channels	Cisco TelePresence Server と遠端の間で送受信ビデオ チャネルが開いているかどうか。	
Extended video channels	Cisco TelePresence Server と遠端の間で送受信拡張ビデオ チャネルが開いているかどうか。	

フィールド	フィールドの説明	使用方法のヒント
Received audio gain mode	TelePresence Server から受信する音声用にエンドポイントで設定されているオーディオ ゲイン モード。したがって、*[<use default>]*、*[Automatic]*、*[Fixed]*、*[Disabled]* のいずれかになります。	[<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対して無効になっています。 [Fixed]：TelePresence Server はエンドポイントが受信する音声を固定比率で調整します。固定比率は、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、統合した総帯域幅ではなく各コール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画像。	プレビューには、適切な方向と帯域幅を使用した画像を基に調整された、受信ストリームと送信ストリームの両方の各画面の画像が表示されます。プレビューをクリックして更新できます。
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	エンドポイントまたはエンドポイント グループがこの会議に参加していた時間。	
Disconnect	会議からエンドポイントまたはエンドポイント グループの接続を解除するには、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の音声をミュートまたはミュート解除するには、このコントロールを使用します。これにより、他の会議参加者がこのエンドポイントの音声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をミュートまたはミュート解除するには、このコントロールを使用します。エンドポイントへの音声をミュートすると、そのエンドポイントでは音声が聞こえなくなります。	

フィールド	フィールドの説明	使用方法のヒント
Mute video from / Unmute video from	このエンドポイントからのビデオをミュートまたはミュート解除するには、このコントロールを使用します。これにより、他の会議参加者にこのエンドポイントが表示さ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をミュートまたはミュート解除するには、このコントロールを使用します。エンドポイントへのビデオをミュートすると、そのエンドポイントには何も映っていない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（画像内の画像）を自動的に中央に配置し、PiP を可能な限り大きく表示できるように画面に応じて PiP を移動します。これは、参加者が会議に参加および退席すると同時に動的に行われます。 このエンドポイントに送信されるレイアウトの参加者の PiP を手動でリセットおよび中央配置する必要がある場合に、[Tidy view] オプションを使用してください。
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 エンドポイントでの表示位置を選択し、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。	

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、[Audio]、[Auxiliary audio]、[Video]、および [Content channel] の最大 4 つのセクションに表示されます。

各チャネルの統計情報は、[Receive stream] 統計情報と [Transmit stream] 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。または、ブラウザ ページの更新によって手動でデータを更新するか、[Refresh] をクリックすれば、最新の統計情報を取得できます。

複数画面のエンドポイントの場合、[Multiscreen Stream Selection] ページが表示されます。目的の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のデータが表示されます。

表 32 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たコーデック。ビデオおよびコンテンツ チャネルの場合は、ビデオ ストリームのサイズも表示されます。
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に使用できるネゴシエーション済みの帯域幅。
Receive bit rate	このフィールドは、ビデオおよびコンテンツ チャネルの受信ストリームにのみ適用されます。Cisco TelePresence Server がエンドポイントに送信を要求したビット レート（ビット/秒単位）。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	このチャネルのパケットが Cisco TelePresence Server に到達する、パケット間でのタイミングの変動を表します。数値が小さいほど、パケットがより適切に到達していることを意味します。
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、音声信号強度の基準となります。単位はミリデシベルです。-34000 などの大きな負の数値の場合は音量が非常に小さく、負の数値がゼロに近づくほど音量は大きくなります。
Packets received / errors	Cisco TelePresence Server が受信した音声/ビデオ/コンテンツのパケット数。2 番目の数値は、シーケンスの中断や誤った RTP 情報など、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。これは、ビデオ（実際のビデオ データ）に何らかのエラーがあるパケットとは異なります。
Packets total / missing	このエンドポイントから Cisco TelePresence Server 宛の音声パケットの数。2 番目の数値は、受信した破損しているパケットの数を示します。
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 ストリームのフレーム レート、および受信した音声/ビデオ/コンテンツ フレームの総数に対してエラーがあるフレームの数。
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 間で送受信されたストリームの 1 秒あたりのフレーム数です。

フィールド	フィールドの説明
Fast update requests sent	このチャネルで TelePresence Server が送信したクイック更新要求（FUR）の数。たとえばパケットが失われた場合に、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 TelePresence Server との間で ActiveControl のネゴシエーションを実行できない場合、値は [Not supported] です。 他には、オーバーヘッド率および復元されたパケット数の 2 つの統計情報があります。 オーバーヘッド率と元のストリームを比較して、挿入される FEC パケットの数を測定します。エンドポイントがストリームに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 つに 1 つ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 %、4 つに 1 つのパケットなら 25 % です。リアルタイム統計情報は、カウンティング間隔と RTCP レポートのタイミングにより、常にこれらのレベルと完全に一致するわけではありません。 復元されたパケット数とは、元のパケットが失われたために、TelePresence Server がエンドポイントの FEC パケットから復元したパケットの単純な総数です。
ClearPath LTRF	LTRF（Long Term Reference Frames）が有効な場合に、[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たコーデック。ビデオおよびコンテンツ チャネルの場合は、ビデオ ストリームのサイズも表示されます。
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に使用できるネゴシエーション済みの帯域幅。
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にのみ適用されます。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。Cisco TelePresence Server から送信されるビデオ データを単純に測定した実際のビット レートは、カッコ内に表示されます。
Packets sent / reported lost	エンドポイント宛の音声/ビデオ/コンテンツ パケットの数。2 番目の数値は、エンドポイントによって報告された、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およびコンテンツ 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 間で送受信されたストリームの 1 秒あたりのフレーム数です。

フィールド	フィールドの説明
Fast update requests received	このチャネルで TelePresence Server がエンドポイントから受信したクイック更新要求（FUR）の数。
ClearPath FEC	このストリームで使用された前方誤り訂正の統計情報。 オーバーヘッド率および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。 オーバーヘッド率と元のストリームを比較して、挿入される FEC パケットの数を測定します。TelePresence Server がストリームに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 つに 1 つ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 %、4 つに 1 つのパケットなら 25 % です。TelePresence Server が現在このストリームに FEC を適用していない場合、オーバーヘッドは 0 % です。 表示される数値は、元のパケットが失われたために、エンドポイントが TelePresence Server の FEC パケットから復元した報告済みパケットの数です。
ClearPath LTRF	Long Term Reference Frames 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 TelePresence Server との間で ActiveControl のネゴシエーションを実行できない場合、値は [Not supported] です。それ以外の場合、この値は [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 に存在するすべてのユーザ アカウントの概要が示されます。

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 インターフェイスへのアクセスに必要なユーザ名。必要に応じてどの文字セットのテキストでも入力できますが、一部のクライアントでは Unicode 文字がサポートされないことに注意してください。
Name	ユーザの名前（任意のため表示されない場合があります）。

フィールド	フィールドの説明
Access rights	このユーザに付与されているロールおよび関連付けられた権限。[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 アクセスおよび管理アクセスが可能です。

ユーザの削除

ユーザを選択して [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

TelePresence Server でユーザ アカウントを追加、編集、および削除するには、ユーザのリストにアクセス（[Users] に移動）します。

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。相違点については次の参照表で説明します。

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 35 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 番号を指定します。 この値は、TelePresence Server へのアクセスに必要なユーザ名です。	必要に応じて、どの文字セットのテキストでも入力できますが、一部のクライアントでは Unicode 文字がサポートされないことに注意してください。 **注：**TelePresence Server のコンソールでは、一部の Unicode 文字を使用できません。コンソール アクセスに使用するアカウントは、ユーザ名およびパスワードの ASCII 文字に限定されます。
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。	必要に応じて、どの文字セットのテキストでも入力できますが、一部のクライアントでは Unicode 文字がサポートされ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、新規ユーザを追加するときにの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] をクリックすると、これらのフィールドが編集可能になります。
Access rights	ドロップダウンからユーザのロールを選択します。ロールに応じて、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 アクセスおよび管理アクセスが可能です。	

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 ログからの情報収集が必要になる場合があります。通常は、カスタマー サポートを利用してこれらのログを取得します。

イベント ログ

TelePresence Server では、サブシステムによって生成された直近 2000 件のキャプチャ済みメッセージが保存されます。これらは [Event log] ページ([Logs] > [Event log])に表示されます。一般的に、これらのメッセージは情報提供を目的としています。また、[Event log] には [Warnings] または [Errors] が表示される場合があります。

TelePresence Server の操作またはパフォーマンスに特定の問題が発生した場合、カスタマー サポートではログに記録されたメッセージとその意味を解釈することができます。

次の作業を実行できます。

- カラム ヘッダーをクリックしてイベントをソートする。
- ページ番号をクリックして、表示されるログを 100 イベント刻みで切り替える。

- すべてのシステム ログを 1 つの zip ファイルとしてダウンロードする（[Download system logs] をクリックします）。
- テキスト形式でイベント ログをダウンロードする（[Logs] > [Event log] に移動して [Download event log] をクリックします）。
- 表示されるパラメータを変更して、情報を目的の範囲に制限する（[Logs] > [Event display filter]）。
- [Logs] > [Event capture filter] ページを編集して、トレースに収集される詳細のレベルを変更する。

注：イベント キャプチャ 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。

- 保管または分析のため、ネットワーク上の 1 つ以上の syslog サーバにイベント ログを送信する （サーバは [Logs] > [Syslog] ページで定義されています）。
- [Clear event log] をクリックしてログを空にする。

イベント キャプチャ フィルタ

イベント キャプチャ フィルタでは、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、TelePresence Server のすべてのサブシステムから*エラー*、*警告*、*および情報*をキャプチャするようにこのフィルタが設定されています。

注：このフィルタは、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。

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求められた場合は、次の手順を実行します。

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、パフォーマンスが影響を受け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（一時的に詳細のレベルを上げるだけで、問題が解決したら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、他のすべてのサブシステムのデフォルト情報に加えて、ビデオ サブシステムからは詳細なトレース情報をキャプチャします。

イベント表示フィルタ

イベント表示フィルタを使用すると、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ことができます。このフィルタは保存されたエントリに対して機能し、どのイベントがキャプチャされるかには影響しません。

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 フィルタリング

1. 特定の文字列を含む保存済みイベントのみを表示するには、[Filter string] に入力します。
2. フィルタリングされた結果内で特定の文字列を見分けやすくするには、[Highlight string] に入力します。
3. [Update display] をクリックします。

   TelePresence Server に、フィルタリングおよび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あり、そのどれもがイベントをログに記録できます。サブシステムごとまたはすべてのサブシステムについて、表示する詳細のレベルを変更できます。

たとえば SIP エラーのみを対象とする場合は、次の手順を実行します。

1. ページ下部の [Set all to:] ボタンとその横のドロップダウンが表示されるまでスクロールします。
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が [None] に変更されます。
4. SIP サブシステムの横のドロップダウン 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 エラーのみが表示されます。

プロトコル メッセージのロギング

[Protocols log] ページには、TelePresence Server で送受信したさまざまなプロトコルの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 ロギングはデフォルトで無効になっています。ただし、トラブルシューティングの一環としてカスタマー サポートからこれを有効にするよう求めら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には、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] をクリックすると、これらのプロトコル メッセージの記録が開始されます。
3. 解決しようとしている問題の再現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 ファイルとして取得し、サポートに送信します。

問題が解決したことを確認できたら、今後ユニットのパフォーマンスに影響しないように、[Disable protocols logging] および [Clear log] をクリックします。

フィールド	説明
Current status	[Enabled] または [Disabled]。デフォルトは [Disabled] です。
Messages logged	ログに記録されるメッセージの数。
Protocol filters	• *BFCP* • *SIP* • *XCCP* キャプチャするプロトコル メッセージのチェックボックスをオンにします。これらは表示フィルタではなくキャプチャ フィルタです。プロトコルを選択せずにプロトコル ロギングを有効にした場合、TelePresence Server では、選択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状態では、ログに記録するプロトコルを変更できません。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てチェックボックスの選択を変更してから、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 ログは HTTP または HTTPS を介して利用可能なため、リモート デバイスにログを記録できます。プロトコル ロギングの有効化または無効化の設定によって、リモート デバイスへのログの送信が無効になることはありません。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には、次の手順を実行します。

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、有効なユーザおよびパスワードのパラメータ（**authenticationUser=***username*&*authentication***Password=***password***）を含める必要があります。

   wget を使用した例を次に示します（Linux システムの場合）：
   wget https://<*IP address*>/protocols_log_stream --post-data=authenticationUser=*username*&*authentication*Password=*password*

   （API 専用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 ログの内容全体が、この TCP 接続を使用したストリームでリモート デバイスに戻されます。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

保管または分析用に、ネットワーク上の 1 つ以上の syslog サーバにイベント ログを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 設定を行う際の参考として、次の表を参照してください。

Table 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。	設定した各ホストに送信されるパケット数は、それぞれの 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 メッセージ* • *[2]：メール システム* • *[3]：システム デーモン*	Cisco TelePresence Server の値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およびプロセスで、類似するセキュリティ/認証、監査、およびアラート メッセージにファシリティ 4、10、13、および 14 が使用されます。 **注 2：**さまざまなオペレーティング システムでクロック（cron/at）メッセージにファシリティ 9 と 15 の両方が使用されます。

フィールド	フィールドの説明	使用方法のヒント
	• *[4]：セキュリティ/認証メッセージ（注 1 を参照）* • *[5]：syslogd によって内部で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）* • *[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）*	ファシリティ値が明示的に割り当てられていないプロセスおよびデーモンでは、「ローカル使用」ファシリティ（16 ～ 21）または「ユーザレベル」ファシリティ（1）が使用される場合があります。そこで、これらのいずれかの値を選択することを推奨します。

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 キャプチャ フィルタによって制御します。

syslog サーバを定義するには、その IP アドレスを入力して [Update syslog settings] をクリックします。設定した各ホストに送信されるパケット数は、それぞれの IP アドレスの横に表示されます。

注：各イベントの重大度インジケータは次のとおりです。

- [0]（緊急）：システムが使用不能（Cisco TelePresence Server で未使用）
- [1]（アラート）：即時対処が必要（Cisco TelePresence Server で未使用）
- [2]（クリティカル）：深刻な状態（Cisco TelePresence Server で未使用）
- [3]（エラー）：エラー状態（Cisco TelePresence Server *エラー* イベントで使用）
- [4]（警告）：警告状態（Cisco TelePresence Server *警告*イベントで使用）
- [5]（通知）：正常だが注意を要する状態（Cisco TelePresence Server *情報*イベントで使用）
- [6]（情報）：情報メッセージ（Cisco TelePresence Server *トレース* イベントで使用）
- [7]（デバッグ）：デバッグレベル メッセージ（Cisco TelePresence Server *詳細トレース* イベントで使用）

呼詳細レコードの使用

TelePresence Server では、最大 2000 の呼詳細レコードを表示できます。ただし、TelePresence Server は呼詳細レコードの長期ストレージを目的としたものではありません。CDR ログを残す場合は、ダウンロードして別の場所に保存してください。

CDR ログが最大数に達すると、最も古いログが上書きされます。

CDR ログを表示および制御するには、[Logs] > [CDR log] に移動します。使用可能なオプションおよび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。

- 呼詳細レコード ログ コントロール
- 呼詳細レコード ログ

呼詳細レコード ログ コントロール

CDR ログには多くの情報が含まれている可能性があります。このセクションのコントロールを使用すると、最も有用な情報を選択して表示できます。変更を終えたら、[Update display] をクリックすると変更が適用されます。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 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。	チェック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。または目的のレコード タイプのチェックボックスをオンにします。
Filter string	このフィールドを使用して、表示される呼詳細レコードの範囲を制限します。フィルタ文字列は大文字と小文字が区別されません。	このフィルタ文字列は、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を展開すると、これらにもフィルタ文字列が適用されます。
Expand details	デフォルトでは、CDR ログに各イベントの簡単な説明のみが表示されます。該当する場合は、表示されるオプションから選択して詳細を表示します。	[All] を選択すると、その他の選択されているオプションに関係なくすべてのメッセージの詳細が最大量表示されます。

呼詳細レコード ログ

呼詳細レコード ログは、複数のページにまたがった最大 2000 行を含む長いテーブルとして表示されます。上記のフィルタリングに加えて、次の方法でログを操作できます。

- 特定のカラムで昇順または降順にソートするには、そのカラム ヘッダーをクリックします。
- 特定の会議または参加者の 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（このフィルタを元に戻すには、[Show all] をクリックします）。
- 表示されたレコード リスト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したりする場合は、[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*。つまり、Web ページで設定した表示フィルタは無視されます。

注：ユニットに負荷がかかった状態で 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場合があります。

ログの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] を使用すると、TelePresence Server から *すべてのレコードが完全に削除されます*。クリアしたレコードを取得することはできません。

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 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。 着信 CDR のログ イベントは（UTC ではなく）ローカル タイムスタンプで保存されます。 システム時刻の変更または NTP の更新によって時刻を変更すると、CDR ログの新しいイベントには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。	新しい会議はそれぞれ、グローバル一意識別子(GUID)で作成されます。特定の会議に関連するすべてのレコードにこの識別子が表示されるため、会議イベントをより簡単に監査できます。 GUID をクリックすると、その会議に関連するレコードのみが表示されます。
Participant	このレコードが適用される参加者の GUID。	各参加者はグローバル一意識別子によって表されるため、レコードの管理を簡素化できます。 GUID をクリックすると、その参加者に関連するレコードのみが表示されます。
Message	呼詳細レコードのタイプ、および簡単な説明（該当する場合）。	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] をクリックすれば、すべてのメッセージを対象にこの操作を実行できます。メッセージに特定の単語が含まれるレコードを検索する場合に、[Filter string] と組み合わせて使用すると便利です。

API クライアント

TelePresence Server は、ユニットに要求を送信した直近 10 の API クライアントをログに記録します。このリストを表示するには、[Logs] > [API clients] をクリックします。

5 分以上 API 要求を送信していないクライアントはグレーで表示されます。

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と、このリストに再度表示されます。

デフォルトで、ページは [Time since last request] カラムでソートされています。

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	クライアントが最後に要求を送信してから経過した時間。	
Last request method	API クライアントが送信した最後の API 要求メソッド。	
Last request user	クライアントが API 要求で使用したユーザ名。	ここでは、最後の API 要求の認証が失敗したクライアントに [(authentication failed)] のフラグが表示されます。
Requests received since last reset	最後にリセットされてから受信した要求の数。	1 秒間に複数の要求が受信された場合、1 秒あたり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 秒あたり 1.8 要求です。 「過活動」クライアントには、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。 最後のリセットからの経過時間がテーブル下部のボタンの横に表示されます。

フィードバック レシーバ

TelePresence Server がフィードバック イベントをパブリッシュすることで、これをリスニングするレシーバは変更が行われた場合に対処できます。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] をクリックします。

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

リスト内の各レシーバについて、次の詳細情報が表示されます。

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 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、Cisco Telepresence Management Suite（適切な API コールを使用してフィードバック イベントに応答し、フィードバック送信元から変更内容のリストを取得できます）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ます。

Call Home の使用

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

TelePresence Server は、そのステータスと発生した障害に関するレポートを Cisco Call Home サービスに送信できます。TelePresence Server では、Call Home へのレポートの送信に常にセキュア接続（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）、[Call Home mode] でいずれかを選択しないと、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か、自動的に送信する機能を設定できます。

[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することはできません。これらのレポートはシスコのエンジニアのみが利用可能で、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 モードの [anonymous] を選択した後、TelePresence Server によって自動的にレポートが送信されるようにする場合は、[Automatic Call Home enabled] をオンにします。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。その後は、予期しない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、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。このレポートが存在しても、特殊な状態または障害を意味しているわけではありません。自動 Call Home が有効になっていると、TelePresence Server は起動時に毎回これらのレポートを送信します。

Call Home の設定方法は次のとおりです。

1. [Logs] > [Call Home] に移動します。
   [Status] セクションには、この機能が有効になっているかどうか、および現在使用できるレポートが表示されます。

2. [Call Home mode] で [Anonymous Call Home] を選択します。
3. （任意）手動による介入なしで TelePresence Server に自動的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。
   ダイアログに「Are you sure you want to apply configuration changes?」と表示されます。
5. [OK] をクリックして続行するか、[Cancel] をクリックして設定変更を破棄します。
   自動 Call Home が有効になっている場合、TelePresence Server は保留中のレポートをすぐに送信します。
6. （任意）[Current reports] 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 41 ステータスのフィールド

フィールド	説明
Call Home status	Call Home のステータスとして次のいずれかを示します。 • *[Automatic – Anonymous Call Home]*：[Call Home mode] が有効で、[Automatic Call Home enabled] がオンになっています。 • *[Enabled – Anonymous Call Home]*：[Call Home mode] が有効で、[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] が無効になっている場合、TelePresence Server は起動中のイベント ログにその情報を記録します。[Call Home mode] が有効（[Anonymous Call Home]）でも、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。
Submission status	日時を含む、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のステータスは [Not sent] です。
Last submitted report reference	このフィールドは、[Unexpected media resource restart diagnostics] レポートまたは [Unexpected device restart diagnostics] レポートが送信された場合にのみ表示されます。Cisco TAC では、この参照番号が提供されるとレポートを分析できます。
Call Home now	[Current reports] 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場合や、自動レポート送信を有効化する場合は、データがシスコに送信されることを示す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 回目の試行で送信が失敗すると、Web インターフェイスにバナーが表示されます。

表 42 設定のフィールド

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、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るようになります。また、起動時に TelePresence Server がインベントリ レポートを送信できるようになります。

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）を使用できます。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 BFCP と呼ばれるプロトコルをコンテンツに使用します。
- Cisco CTS システムなどの TIP システムでは、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で、2番目のビデオ チャネルを使用できないエンドポイントに対応します。この機能を有効にすると、TelePresence Server はこ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間、コンテンツ チャネルは通常のビデオで構成されます（コンテンツが最大ペインに表示され、他の参加者のビデオ ストリームはディスプレイの下部に沿った連続表示ペインの中央に配置されます）。

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、これらのオプションを TelePresence Server のユーザ インターフェイスから設定することはできません。

このページの内容

会議のレイアウト

システムに対して TelePresence Server が選択するレイアウトは、システムの画面数と他の会議参加者の特性によって異なります。エンドポイントでも、遠端カメラ制御または DTMF キー 2 および 8 によってレイアウトを選択したり、下記の選択肢のいずれかを事前設定したりすることができます。TelePresence Server では、1 画面、2 画面、3 画面、および 4 画面の標準およびイマーシブ エンドポイントを使用できます。また、会議に参加している複数のシステムを組み合わせて、会議の他のタイプのシステムに表示できます。

TelePresence Server の通常の動作では、最も目立つレイアウト ペインに「最大音量」の参加者が表示されます。使用可能なペインより参加者が多い場合、「最小音量」の参加者は表示されません。

1 画面の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、ボックス幅または参加者ごとに設定できます。このデフォルト設定は、参加者が遠端カメラ制御または DTMF キー 2 および 8 を使用してレイアウトの選択を変更することで上書きされる場合があります。

ActivePresence レイアウトでは、最大音量の参加者が全画面表示され、その他の参加者は画面下部の最大 6 つの同一サイズのオーバーレイ ペインに表示されます。それ以外の参加者は [Participant Overflow] アイコンで示されます。

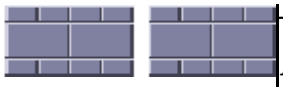
TelePresence Server は、[Default layout type for single-screen endpoints] の設定に従って、1 画面のエンドポイントのレイアウトを構成します。

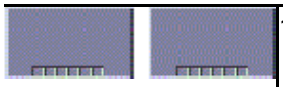
表 43 1 画面のエンドポイントに送信されるレイアウト

	[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、その他の参加者は画面下部の最大 6 つの同一サイズのオーバーレイ ペインに表示されます。それ以外の参加者は、表示されていない参加者の数とともに右下隅の [Participant Overflow] アイコンで示されます。
	[Prominent]：エンドポイントは 1 つの大きなペインに表示され、その他の参加者は画面下部の最大 6 つの同一サイズのペインに表示されます。それ以外の参加者は、表示されていない参加者の数とともに右下隅の [Participant Overflow] アイコンで示されます。
	[Equal]：エンドポイントは、画面上でグリッド パターンの同一サイズのペインに表示されます（4 X 4 まで）。 ペインの各行に、複数画面のリモート システムの画面、または画面数が少ない複数のリモート システムの組み合わせを表示できます。

2 画面のシステムに送信されるレイアウト

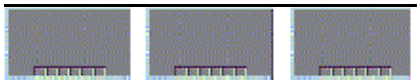
表 44 2 画面のシステムに送信されるレイアウト

	TelePresence Server が会議室スイッチド表示モードで、3 画面または 4 画面の TelePresence システムが会議に参加している場合、TelePresence Server は、このレイアウトを会議の 2 画面のシステムに送信します。 4 つのペインの各行に、4 画面のリモート システムの 4 つの画面、または画面数が少ない複数のシステムの組み合わせを表示できます。

	1 画面および 2 画面のシステムのみが会議に参加している場合、TelePresence Server はこのレイアウトを使用します（表示するすべてのビデオ ストリーム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）が自動的に中央に配置されます。

3 画面のシステムに送信されるレイアウト

表 45 3 画面のシステムに送信されるレイアウト

	PiP のないレイアウトを利用できます（強制的に PIP なしのレイアウトになります）。DTMF 2 および 8 または 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で、4 画面の TelePresence システムが会議に参加している場合、TelePresence Server は、このレイアウトを会議の 3 画面のシステムに送信します。 4 つの大きいペインの中央行に、4 画面のリモート システムの 4 つの画面、または 1 画面、2 画面、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。この行を適切に中央に配置するため、TelePresence Server は 3 つの画面の中央にペインを表示し、左端の画面の左側および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、TelePresence Server は、会議の 3 画面のシステムに対してこのレイアウトを使用します。

4 画面のシステムに送信されるレイアウト

TelePresence Server は、会議の 4 画面の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 つの全画面ペインで構成される行または 6 つの小さいオーバーレイ ペインのいずれかの行）に、4 画面のシステムまたは画面数が少ない複数のリモート システム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 レイアウトに影響するエンドポイントの設定オプション

セルフ ビュー設定

エンドポイントの [Self view] 設定によって、そのエンドポイントの TelePresence Server が自身のビデオ ストリームを表示するかどうか、つまり、参加者に自分自身が表示されるかどうかが決まります。この設定がオフの場合、エンドポイントは自身のビデオ ストリームを表示しません。

エンドポイントが自身のビデオを表示できるようにした場合、TelePresence Server は、使用可能なビュー ペインに参加者を配置するときに、自身の参加者がコール内で最も音量が大きい場合（つまり、他の会議参加者には顕著に表示されている場合）でも、常にセルフ ビューを最後に配置します。

1 画面のエンドポイントの全画面ビューの表示

レイアウト ペイン内に参加者を配置する際、TelePresence Server は、最初に「最大音量」の参加者を最も目立つペインに配置し、より小さいペインに最小音量の参加者を配置します。ただし、TelePresence システム（通常、高解像度の大きなディスプレイを使用）と、かなり低品質のビデオに対応したシステム（ビデオ対応の携帯電話など）が混在する会議では、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は適切でない場合があります。

1 画面のシステムの場合、大きな全画面ペインにエンドポイントを表示できるか、およびその表示方法は、[Show full screen view of single-screen endpoints] 設定によって決まります。使用可能な設定は [Always]、[Dynamic] および [Disabled] です。

- [Always]：1 画面のエンドポイントを複数画面のエンドポイントのメイン ペインに常に表示できます。
- [Dynamic]：会議に複数画面のエンドポイントが 1 つだけ参加している場合は、そのメイン ペインに 1 画面のエンドポイントを表示できます。複数画面のエンドポイントが会議に参加すると、1 画面のエンドポイントは PiP ストリップに降格されます。
- [Disabled]：1 画面のエンドポイントは複数画面のエンドポイントのメイン ペインに表示されません。

この設定は、複数画面の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 ビデオのコンテンツの許可

この機能を使用すると、TelePresence Server は追加チャネルに対応していないエンドポイントのメイン ビデオ チャネルに会議のコンテンツを送信できます。使用しない場合はこれらのエンドポイントで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には、この構成済みレイアウトの最大ペイン（メイン ビデオ チャネルに表示される）が割り当てられます。最大 6 人の他の参加者の連続表示ペインが、コンテンツ ストリームの下のレイアウト下部に沿って表示されます。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枠の表示の設定

[Show borders around endpoints] を有効にすると、TelePresence Server は小さいペインに表示される参加者を囲む枠線を表示します。全画面ペインでは参加者を囲む枠線が表示されません。

TelePresence Server は、会議のアクティブ スピーカーの周囲に青色の枠線を表示し、それ以外の場合はグレーの枠線を表示します。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など、会議で強調表示されるアクティブ スピーカーが存在しないこともあります。

エンドポイントの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 レイアウトでは枠線が使用されます。この参加者が他の参加者に対して常に枠線内に表示されるわけではありません。他の参加者のビューでは、それぞれの [Show borders around endpoints] 設定が使用されます。

参加者の「重要」マーク付け

会議ごとに 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 がどの参加者をどのレイアウト ペインに表示するかを決定するときに、それぞれの音量によって設定されるリスト内の位置に関係なく、この参加者が優先されることを意味します。「会議ステータスの表示」のエンドポイント制御設定を参照してください。

ミュートされた参加者

音声ミュート

Web インターフェイスから自身の音声をミュートした参加者は会議に音声を提供しません。また、TelePresence Server がビュー レイアウトのペインに参加者を配置する際、ミュートしていない参加者がミュート中の参加者より優先されます。

参加者がミュート中であることは、他の参加者に示されないことに注意してください。他の参加者にはその参加者の音声が聞こえなくなるだけです。

ビデオ ミュート

Web インターフェイスから自身のビデオをミュートした参加者は会議にビデオを提供しません。別途音声をミュートしない限り、通常どおり音声は引き続き提供されます。

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 ビデオに対応しています。

つまり、マルチストリーム対応のエンドポイントは会議レイアウトにビデオ ストリームをローカルに構成することができるため、ユーザ エクスペリエンスの向上につながります。ただし、すべてのエンドポイントは利用できる最適なエクスペリエンスで引き続きサポートされます。

これを実現するため、TelePresence Server は複数のストリームを送信する機能をアドバタイズし、マルチストリーム対応のエンドポイントが必要なストリームをサブスクライブできるようにします。

TelePresence Server は、マルチストリーム対応のエンドポイントから、異なる解像度およびフレーム レートで同じビデオ ソースのメイン ビデオ ストリームを最大 4 つ受信できます。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、同じく異なる解像度とフレーム レートで最大 16 のビデオ ストリームをエンドポイントに送信できます。その後、マルチストリーム対応のエンドポイントは会議レイアウトにビデオ ストリームをローカルに構成します。

この機能に関して注意すべき重要事項は次のとおりです。

- Cisco TelePresence Server on Virtual Machine および Cisco Multiparty Media 310/320 でのリモート管理モードの場合にのみサポートされます。
- TelePresence Server は、マルチストリームとシングル ストリームの両方のエンドポイントを使用する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。
- 前方誤り訂正およびレート制御を使用してマルチストリーム コールを復元できます。
- マルチストリームは、H.323 または TIP ではなく SIP を介した場合にのみサポートされます。
- デフォルトではイネーブルです。ただし、API の **`multistreamMode`** パラメータを使用して無効にできます。
- TelePresence Server は H.264 SVC チャネルを使用してサポートを提供し、マルチストリーム対応のエンドポイントとの間でビデオ ストリームを送受信します。
- カスケード リンクによるマルチストリーム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 レベルでサポートされます。ただし、メイン ビデオのビット レートが 500 kbps 以上である必要があります。

注：

- アクティブ スピーカー セグメントのみを表示することで、TIP エンドポイントがマルチストリーム対応のエンドポイントに表示されます。
- 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、すべてのエンドポイントはトランスコード 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）	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。例： • EX60 / EX90 • C シリーズ コーデック（C20、C40、C60、C90） • Cisco Jabber • Microsoft Lync • 他の非 TIP のサードパーティ エンドポイント TelePresence Server でエンドポイント タイプが不明である場合も表示されます。
Cascade	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
Group of N endpoints	エンドポイントのグループリストには個々のグループ メンバは含まれません

Legacy TIP endpoint	• 従来のソフトウェア（CTS 1.6/1.7 ～ 1.7.3）を実行している、タイプが不明な Cisco CTS システム
	• 従来のソフトウェア（CTS 1.6/1.7 ～ 1.7.3）を実行している、1 画面の Cisco CTS システム。例：
	  • CTS 500
	  • CTS 1000
	  • CTS 1100
	• 従来のソフトウェア（CTS 1.6/1.7 ～ 1.7.3）を実行している、3 画面の Cisco CTS システム。例：
	  • 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）	ハードウェア名/モデル番号
SIP telepresence	CTS 1.7.4 以降を実行している、タイプが不明な Cisco CTS システムまたは他の TIP 対応システム
SIP single screen telepresence	CTS 1.7.4 以降を実行している、1 画面の Cisco CTS システムまたは他の TIP 対応システム。例： • CTS 500 • CTS 1000 • CTS 1100
SIP three screen telepresence	CTS 1.7.4 以降を実行している、3 画面の Cisco CTS システムまたは他の TIP 対応システム。例： • 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
Multistream	シスコがサポートするマルチストリーム対応のエンドポイント。

エンドポイントの相互運用性

表 47 エンドポイントの機能サポート

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 スイッチド レイアウトでの最大音量の参加者の表示	T3、CTS 3200、CTS 3000、TX9000、TX9200	CTS 1300 およびエンドポイント グループは最大音量の参加者を表示しません。 **注**：一部の T3 システムは位置音声（T3 カスタム）を提供できません。
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。他のタイプのエンドポイントに示すため、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

クラスタとは、同じ Cisco TelePresence MSE 8000 シャーシにホストされたブレードのグループです。複数のブレードが 1 つのユニットとして機能するように相互にリンクされています。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。

クラスタでは、クラスタ内の両方のアプライアンスのスクリーン ライセンス数を統合できます。画面数が増えることで、より多くの参加者または複数の小規模な会議を含む会議を状況に応じて設定できます。

Cisco TelePresence Server on Media 820 クラスタの概要

TelePresence Server ソフトウェア バージョン 4.2 以降を実行する Cisco Multiparty Media 820 ブレードはクラスタリングをサポートします。現在は、1 つをマスター、もう 1 つをスレーブとして、最大 2 つのブレードをクラスタ化できます。

マスターはクラスタのライセンスを必要に応じて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、複数の小規模な会議に分散して割り当てたりすることができます。

詳細については、「TelePresence Server の会議容量について」（74 ページ）を参照してください。

マスター TelePresence Server

クラスタ内の各 TelePresence Server に割り当てられたスクリーン ライセンスはマスターによって「継承」され、クラスタ内のすべての容量はマスターが制御します。クラスタの機能は、マスターでその Web インターフェイスまたは API を使用して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はマスターによって実行されます。

スレーブ TelePresence Server

スレーブ TelePresence Server には、一部の Web インターフェイスのみが表示されます。ネットワークおよびロギングの設定やソフトウェアのアップグレードを行う設定ページなどは使用可能です。

同様に、スレーブ TelePresence Server はすべての API コマンドに応答するわけではありません。詳細については、該当する 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の TelePresence Server ソフトウェアをアップグレードするには、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てから、マスターを再起動します。スレーブが自動的に再起動されてアップグレードが完了します。

一般事項

クラスタリングに関する注意事項は次のとおりです。

- クラスタリングを設定するには、スーパーバイザで 2.3(1.38) より**後**のソフトウェア バージョン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 で、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。
- Media 820 のクラスタリングではシャーシのどのスロットでも使用できます。
- Media 820 とほかのタイプのブレード間でクロスクラスタを実行することはできません。
- 1 つのシャーシに複数のクラスタを含めることができ、シャーシはさまざまな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。
- スーパーバイザを使用してシャーシ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。ブレードに障害が発生した場合は交換でき、クラスタ設定は継続されます。ただし、アクティブ コールおよび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、スレーブも再起動されてすべてのコールおよび会議は終了します。
  - 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一致しない場合があります。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おり、ネットワーク設定またはブレード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した場合、スーパーバイザによってブレードの再起動を求められます。
  - スーパーバイザが再起動または削除された場合、クラスタは動作を継続し、会議は続行されます。スーパーバイザが再表示されてもクラスタは再起動されません。
- スーパーバイザの最新バックアップを常に保存しておいてください。

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。お使いのモデルに関連する情報を確認してください。

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、購入した「スクリーン ライセンス」（ライセンス アクティベーション キーの形式で提供されます）で決まります。スクリーン ライセンスは TelePresence Server の会議容量をアクティブ化します。最大数のライセンスを適用すると、TelePresence Server の全容量がアクティブ化されます。次のようにハードウェア プラットフォームによって最大数は異なります。

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	上記の順に 24、36、48
TelePresence Server 7010	12
TelePresence Server on Media 310	6
2 台の TelePresence Server on Media 310 のクラスタ	12
TelePresence Server on Media 320	12
TelePresence Server on Media 310 と TelePresence Server on Media 320 の混在クラスタ	18
2 台の TelePresence Server on Media 320 のクラスタ	24
TelePresence Server on Multiparty Media 820	30
2 台の TelePresence Server on Multiparty Media 820 のクラスタ	60
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 または TelePresence Server on Multiparty Media 820 にライセンスを適用する場合、スーパーバイザの Web インターフェイスを使用してシャーシにライセンス キーを適用し、これらのブレードが挿入され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。

他のプラットフォームにライセンスを適用する場合は、[Configuration] > [Upgrade] ページで、TelePresence Server の Web インターフェイスを使用してライセンス キーを適用します。

クラスタへのライセンス適用

TelePresence Server MSE 8710 ブレードまたは TelePresence Server on Multiparty Media 820 のクラスタにライセンスを適用する場合は、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、アクティブ化されたスクリーン ライセンスは、クラスタ内のマスター ブレードに効率的にプールおよび割り当てられます。したがって使用可能なスクリーン ライセンス数は、クラスタ内のブレードに割り当てられたスクリーン ライセンスの合計となります。

TelePresence Server on Media 310 および 320 プラットフォームのクラスタにライセンスを適用する場合は、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がすべてのライセンスを制御します。ただし、ユニットを分離する予定がある場合や一方に壊滅的な障害が発生した場合、クラスタの分割後は各ユニットをカバーする独立したライセンスを持つことになります。

動作モード

TelePresence Server 7010 および MSE 8710 には、リモート管理モードとローカル管理モードの 2 つの動作モードがあります。動作モードは、スクリーン ライセンスを容量に変換して同時コールをホストする方法に影響します。

注：TelePresence Server on Media 310/320、TelePresence Server on Multiparty Media 820、および 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。これらのプラットフォームでは、Cisco TelePresence Conductor や Cisco TelePresence Exchange System などのシステムで TelePresence Server を管理する必要があります。

リモート管理モードの場合に表示される情報は、Media 310/320、TelePresence Server on Multiparty Media 820、および TelePresence Server on Virtual Machine プラットフォームに関連しています。ただし、それぞれのソフトウェアにはローカルまたはリモート管理モードの概念はありません。

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一定数のコールに変換されます。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 または 2 コールになります。

- 「フル HD」モードでは、1 つのライセンスで音声およびコンテンツ チャネルが関連付けられた最大 1080p30 または 720p60 のビデオ コールを 1 つ利用できます。
- 「HD」モードでは、1 つのライセンスで音声およびコンテンツ チャネルが関連付けられた最大 720p30 または w448p60 のビデオ コールを 2 つ利用できます。

たとえば、スクリーン ライセンスが 6 つあるローカル管理モードの TelePresence Server 7010 は、最大 1080p30 のコールを 6、または最大 720p30 のコールを 12 までホストできます。

各 TelePresence Server ユニットのビデオ 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 ポートは、使用されるコンテンツに関係なく対応するコンテンツ ポートに割り当てられます。

以下の同時発生コール制限の表では、ローカル管理モードの TelePresence Server で使用できる 2 つの HD モードごとに、これらのポートの割り当てについて説明します。

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 ライセンスがより細かく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と同様）または多くの低リソース コールに対して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 ライセンスは、1080 では 1 コール、720 では 2 コール、448 では 4 コール、360 では 8 コールに対して十分な容量を提供します。

コール制限

次の表に、上記で説明した各動作モードでの 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発生コール制限（7010 および MSE 8710 のみ）

表 48 HD モードでのハードウェア 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 タイプごとのポート割り当て

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発生コール制限

表 50 コール タイプ別の 1 コールあたりの TelePresence Server スクリーン ライセンス

コール タイプの説明			コールあたりに必要なスクリーン ライセンス
メイン ビデオ	Audio	内容	
-	モノ	-	1/52
360p30 †	モノ	メイン ビデオ内	⅛
360p30 †	ステレオ	720p5	¼
480p30	ステレオ	メイン ビデオ内	¼
480p30	ステレオ	720p5	⅓
720p30	ステレオ	720p5	½
720p30	ステレオ	720p30	1
1080p30	ステレオ	720p15	1
720p60	ステレオ	720p15	1
1080p30	ステレオ	720p30	1½
3 画面 720p30	マルチチャネル	720p5	1½
3 画面 720p30	マルチチャネル	720p30	2
1080p30	ステレオ	1080p30	2
2 画面 1080p30	ステレオ	720p30	2
3 画面 1080p	マルチチャネル	720p30	3
3 画面 1080p	マルチチャネル	1080p30	4
4 画面 1080p	ステレオ	1080p30	4

† TelePresence Conductor XC2.2 以降が必要です。

表 51 現在の製品のさまざまなプラットフォームでの TelePresence Server の会議容量

コールあたりに必要なスクリーン ライセンス	ハードウェア タイプ別の最大コール数（100 % の容量を提供するライセンス）								
	8 コア VM（8 vCPU）	Media 310 または MCU 5310	30 vCPU VM ‡	Media 320 または MCU 5320	アプライアンス 2 つのクラスタ	Media 410v ‡ (46 vCPU)	Media 820	8710/8510 の 4 ブレード クラスタ	Media 820 の 2 ブレード クラスタ
	5 スクリーン ライセンス	6 スクリーン ライセンス	10 スクリーン ライセンス	12 スクリーン ライセンス	24 スクリーン ライセンス	27 スクリーン ライセンス	30 スクリーン ライセンス	48 スクリーン ライセンス	60 スクリーン ライセンス
1/52	200*	200*	200*	200*	200*	200*	200*	200*	200*
⅛	41	49	81	97	195	145 †	200*	200*	200*
¼	20	24	40	48	97	108	120	195	200*
⅓	15	18	30	36	73	81	90	146	180
½	10	12	20	24	48	54	60	97	120
1	5	6	10	12	24	27	30	48	60
1½	3	4	6	8	16	18	20	32	40
2	2	3	5	6	12	13	15	24	30
3	1	2	3	4	8	9	10	16	20
4	1	1	2	3	6	6	7	12	15

* 200 は TelePresence Server での最大コール数です。Cisco TelePresence Conductor XC2.3 以降が必要です。

† デバイスでこのスクリーン ライセンス分割の 145 を超えるコールが発信されると、パフォーマンスの低下を招く場合があります。

‡最大コール数を実現するには、Cisco TelePresence Server on Virtual Machine 以外の VM を、Multiparty Media 400v、410v、または 30 vCPU VM でホストしないでください。他の UC アプリケーションとは共存できません（2.4 GHz 以上で実行される共存可能な 8 コア オプションとは異なります）。

注：上記の表では、1 種類のコールを使用してこれらの最大値に到達することを想定しています。さまざまな同時発生コールに必要な総ライセンス数を計算するには、それぞれの同時発生コールに必要なスクリーン ライセンスを合計します。

マニュアルの入手方法およびテクニカル サポート

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（Cisco 製品資料の更新情報）』（http://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（Cisco 製品資料の更新情報）』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。

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