



# システムとエンタープライズパラメータを設定

- [初期システムおよびエンタープライズパラメータの概要, 1 ページ](#)
- [システムとエンタープライズの初期設定タスクフロー, 2 ページ](#)

## 初期システムおよびエンタープライズパラメータの概要

初めて Cisco Unified Communications Manager ノードを設定する場合は、次のシステム全体のパラメータを考慮します。必要に応じて、導入におけるシステム全体のパラメータを変更できますが、ほとんどの場合、推奨されるデフォルト設定で動作します。

- IP フォンのフォールバック接続モニタ期間を設定します。
- すべてのユーザに対して社内ディレクトリの検索を許可します。
- クラスタの完全修飾電話番号 (FQDN) と組織のトップレベルドメインを設定します。
- ビデオ対応の Cisco Jabber 開始条件を設定します。
- (オプション) クラスタが MLPP を使用している場合は、Multilevel Precedence and Preemption (MLPP) を有効にします。
- (オプション) ネットワークが IPv6 を使用している場合は、IPv6 を有効にします。
- (オプション) リモート syslog サーバ名前を入力します。
- (オプション) 導入をトラブルシューティングするためのコールトレースログを設定します。
- (オプション) 依存関係レコードを有効にします。

# システムとエンタープライズの初期設定タスク フロー

はじめる前に

Cisco Unified Communications Manager ノードとポートの設定をセットアップします。

手順

	コマンドまたはアクション	目的
ステップ 1	<a href="#">初期システム パラメータとエンタープライズ パラメータの設定, (2 ページ)</a>	Cisco Unified Communications Manager ノードの初期セットアップに必要なシステム全体のパラメータを設定します。推奨されるシステム設定のリストについては、 <a href="#">システムおよびエンタープライズの初期設定, (5 ページ)</a> を参照してください。
ステップ 2	<a href="#">iOS Cisco Jabber の SSO ログインの動作設定, (10 ページ)</a>	制御されたモバイルデバイス管理 (MDM) の環境で IdP による証明書ベースの認証を Cisco Jabber で実行するために必要なエンタープライズパラメータを設定します。
ステップ 3	<a href="#">RTMT への SSO の設定, (11 ページ)</a>	Cisco Unified Communications Manager を介してエンタープライズ パラメータを設定し、Real-Time Monitoring Tool (RTMT) の SAML SSO を有効にします。

次の作業

Cisco Unified Communications Manager クラスタで設定されているすべてのデバイスに適用する共通設定を確立する目的で、デバイスプールに対してコア設定を設定するためには、[デバイスプールのタスク フローのコア設定](#)を参照します。

## 初期システム パラメータとエンタープライズ パラメータの設定

Cisco Unified Communications Manager Administration を使用して、特定の導入環境でシステムおよびエンタープライズパラメータを設定できます。システムの初期セットアップに重要であるパラメータを記載していますが、推奨するデフォルト設定は、ほとんどの導入環境で問題なく動作します。

コールドトレースログの有効化など、トラブルシューティングに役立つパラメータは、ネットワークのパフォーマンスに影響があるため、問題が解決した後は無効にする必要があります。

ほとんどのパラメータは、変更を有効にするためにすべてのデバイスをリセットする必要があります。すべての設定手順を完了してから、すべてのデバイスをリセットしてください。すべてのデバイスをリセットするのは、稼働率の低い時間帯に実行することを推奨します。



- (注) リリース 10.0(1) から、Cisco Unified Communications Manager および IM and Presence サービスに同じエンタープライズパラメータを使用します。IM and Presence サービスのエンタープライズパラメータの値を変更する場合、変更した値は Cisco Unified Communications Manager に自動で反映されます。

## 手順

- ステップ 1** Cisco Unified CM の管理で、[システム (System) ] > [エンタープライズパラメータ (Enterprise Parameters) ] を選択します。
- ステップ 2** クラスタの IP フォンが、TCP 接続が使用可能になったときに、プライマリ ノードに戻るまでの時間を、[エンタープライズパラメータの設定 (Enterprise Parameters Configuration) ] セクションの [接続モニタ間隔 (Connection Monitor Duration) ] フィールドに秒数を入力してから、[保存 (Save) ] をクリックします。デフォルト値は 120 秒です。  
ヒント すべてのデバイスをリセットしないで、クラスタ内の影響を受けるデバイスに変更を適用するには、[設定の適用 (Apply Config) ] をクリックしてからし、[OK (OK) ] をクリックします。
- ステップ 3** [ユーザ データ サービス パラメータ (User Data Service Parameters) ] セクションの [ユーザ検索をすべて有効にする (Enable All User Search) ] セクションで、[True (True) ] を選択して、姓、名、または電話番号が指定されていないときに、すべてのユーザを組織内名簿で検索することを許可します。
- ステップ 4** [クラスタ全体のドメイン設定 (Clusterwide Domain Configuration) ] セクションで、クラスタ全体のドメインをセットアップします。
- [組織の最上位ドメイン (Organization Top Level Domain) ] フィールドで組織の最上位ドメインを入力します。255 文字まで指定できます。
  - [クラスタの完全修飾ドメイン名 (Cluster Fully Qualified Domain Name) ] フィールドに、クラスタの完全修飾ドメイン名 (FQDN) を入力します。255 文字まで指定できます。  
複数の FQDN はスペースで区切る必要があります。アスタリスク (\*) を使用して、FQDN 内でワイルドカードを指定することができます。たとえば、cluster-1.cisco.com\*.cisco.com です。
- ステップ 5** [Cisco Jabber (Cisco Jabber) ] セクションで、[ビデオありコールを開始しない (Never Start Call with Video) ] フィールドから [False (False) ] を選択します。
- ステップ 6** (任意) [MLPP および機密アクセス レベルパラメータ (MLPP and Confidential Access Level Parameters) ] セクションで、Multilevel Precedence and Preemption (MLPP) ドメインを入力し、デバイスで MLPP の使用を有効にします。
- [MLPP ドメイン ID (MLPP Domain Identifier) ] フィールドに MLPP サービスのドメインを入力します。このパラメータには 16 進値 (0x で始まる値) を指定します。

- b) [MLPP 通知ステータス (MLPP Indication Status) ] フィールドで、[MLPP 通知をオンにする (MLPP indication turned on) ] を選択します。
- ステップ 7** (任意) [IPv6 (IPv6) ] セクションで、[IPv6 を有効にする (Enable IPv6) ] フィールドに [True (True) ] を設定します。
- ステップ 8** (任意) [Cisco Syslog エージェント (Cisco Syslog Agent) ] セクションでは、[リモート syslog サーバ名 1 (Remote Syslog Server Name 1) ] に、リモート syslog サーバの名前または IP アドレスを入力します。サーバ名が指定されていない場合、Cisco Unified Serviceability は syslog メッセージを送信しません。
- ステップ 9** (任意) [セッション トレース用コール トレース ログの設定 (Call Trace Log Configuration for Session Trace) ] セクションで、セッション トレースの SIP コール情報を収集するコール トレース ログをセットアップします。
- Real-Time Monitoring Tool (RTMT) のセッション トレース機能は、トラブルシューティングに利用できるコールのフロー図を生成するためにこの情報を使用します。
- a) [コール トレース ログを有効にする (Enable Call Trace Log) ] フィールドに [True (True) ] を設定します。
- b) Cisco Unified Communications Manager が生成できる SIP コール トレース ログ ファイルの最大数を [コール トレース ログ ファイルの最大数 (Max Number of Call Trace Log Files) ] フィールドに入力します。  
デフォルト値は 2000 です。有効な範囲は 5 ~ 4000 です。
- c) [コール トレース ログ (Call Trace Log) ] フィールドに SIP コール トレース ログ ファイルの最大サイズ (MB) を入力します。  
デフォルト値は 2 です。有効な範囲は 1 ~ 10 です。
- (注) SIP コール トラフィックが多い時間帯では、パフォーマンスが低下することがあります。システム パフォーマンスへの影響を低減するために、Cisco CallManager サービスパラメータの [セッション トレースのコール関連 REFER/NOTIFY/SUBSCRIBE SIP メッセージのログ (Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace) ] に False を設定します。これにより、SIP コール トレースから REFER/NOTIFY/SUBSCRIBE メッセージを除外します。
- ステップ 10** [CCMAdmin パラメータ (CCMAdmin Parameters) ] セクションの [依存関係レコードを有効化 (Enable Dependency Records) ] フィールドで [True (True) ] を選択します。
- ステップ 11** [保存 (Save) ] をクリックします。
- ステップ 12** [リセット (Reset) ] をクリックし、[OK] をクリックしてすべてのデバイスをリセットします。すべてのデバイスをリセットするのは、稼働率の低い時間帯に実行することを推奨します。
- ヒント** すべてのデバイスをリセットするために、システム内の全デバイス プールをリセットできます。

## 関連トピック

システムおよびエンタープライズの初期設定、(5 ページ)

## システムおよびエンタープライズの初期設定

表 1: Cisco Unified Communications Manager の初期設定のシステムおよびエンタープライズパラメータ

カテゴリ (Category)	パラメータ名	説明
エンタープライズ パラメータ	接続モニタ間隔 (Connection Monitor Duration)	<p>クラスタ内の IP フォンがセカンダリ ノードに登録された場合に、このパラメータを使用して、プライマリ ノードが使用可能になった後、それがフォールバックして再登録される前に、IP フォンが待機する時間を設定します。このパラメータは、特定のセキュア Survivable Remote Site Telephony (SRST) ルータに対応するすべてのセキュアなデバイスに影響します。</p> <p>詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』 (<a href="http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html">http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html</a>) を参照してください。</p> <p>デフォルトは 120 秒です。</p> <p>変更内容を反映するには、すべてのサービスを再起動してください。</p>
CCMAdmin パラ メータ	[依存性レコー ドを有効化 (Enable Dependency Records) ]	<p>このパラメータは、トラブルシューティングに必要な依存関係レコードを表示するために使用されます。依存関係レコードを表示すると、初期システム設定時に役立つ場合があります。</p> <p>依存関係レコードを表示すると、CPU 使用率が急増し、コール処理に影響する可能性があります。考えられるパフォーマンス問題を回避するために、システム設定の完了後は、このパラメータを無効にします。負荷の低い時間帯またはメンテナンス ウィンドウの間だけに依存関係レコードを表示することを推奨します。</p> <p>有効にするには、Cisco Unified Communications Manager の管理を使用して大半の設定ウィンドウからアクセスできる [関連リンク (Related Links) ] ドロップダウンリストから [依存関係レコード (Dependency Records) ] を選択できます。</p> <p>デフォルト: [いいえ (False) ]</p>

カテゴリ (Category)	パラメータ名	説明
MLPP および機密 アクセス レベル パラメータ	MLPP Domain Identifier	<p>この Multilevel Precedence and Preemption (MLPP) パラメータは、MLPP サービスのドメインを指定します。MLPP ドメイン内の MLPP サブスクリバからのコールには優先度レベルが割り当てられます。同じ MLPP ドメイン内のより優先度の高いコールのみをプリエンプション処理できます。</p> <p>このパラメータには16進値 (0x で始まる値) を指定できます。</p> <p>デフォルト : 000000</p> <p>変更内容を反映するには、すべてのデバイスを再起動してください。すべてのデバイスをリセットするには、システム内の全デバイス プールをリセットします。</p>
	MLPP 表示ス テータス (MLPP Indication Status)	<p>MLPP ドメイン内のデバイスが MLPP サービスを使用できるように、このパラメータを有効にします。MLPP サービスには、トーン、特殊な表示、MLPP 情報要素 (IE) /信号 IE/原因 IE の送信が含まれます。</p> <p>デフォルト : MLPP 表示はオフ</p> <p>変更内容を反映するには、すべてのデバイスを再起動してください。すべてのデバイスをリセットするには、システム内の全デバイス プールをリセットします。</p>
ユーザ データ サービスパラメ ータ	Enable All User Search	<p>このパラメータを使用して、ユーザは、名、姓、電話番号が指定されていない場合でも、社内ディレクトリですべてのユーザを検索できます。このパラメータは、[Cisco CallManager セルフ ケア (Cisco CallManager Self Care) ] (CCMUser) ウィンドウでのディレクトリ検索にも適用されます。</p> <p>デフォルト : [はい (True) ]</p>

カテゴリ (Category)	パラメータ名	説明
クラスタ全体のドメイン設定	[組織の最上位ドメイン (Organization Top Level Domain) ]	<p>このパラメータは、組織のトップレベルドメインを定義します。例：cisco.com</p> <p>最大長：255 文字</p> <p>有効な値：大文字と小文字、数字 (0-9)、ハイフン、ドット (ドメインラベル区切り記号として) を使用した有効なドメイン。ドメインラベルの先頭文字をハイフンにすることはできません。最後のラベルの先頭文字を数字にすることはできません。たとえば、cisco.lom といったドメインは無効です。</p>
	[クラスタの完全修飾ドメイン名 (Cluster Fully Qualified Domain Name) ]	<p>このパラメータに、このクラスタの1つまたは複数の完全修飾ドメイン名 (FQDN) を定義します。複数の FQDN はスペースで区切る必要があります。アスタリスク (*) を使用して、FQDN 内でワイルドカードを指定することができます。例：cluster-1.cisco.com *.cisco.com</p> <p>このパラメータのいずれかの FQDN に一致するホスト部分がある URL を含む要求 (SIP コールなど) は、クラスタと接続されたデバイスにルーティングされます。</p> <p>最大長：255 文字</p> <p>有効な値：FQDN または * ワイルドカードを使用した部分的な FQDN。大文字と小文字、数字 (0-9)、ハイフン、ドット (ドメインラベル区切り記号として)。ドメインラベルの先頭文字をハイフンにすることはできません。最後のラベルの先頭文字を数字にすることはできません。たとえば、cisco.lom といったドメインは無効です。</p>

カテゴリ (Category)	パラメータ名	説明
IPv6	IPv6を有効化 (Enable IPv6)	<p>このパラメータは、Cisco Unified Communications Manager がインターネットプロトコルバージョン 6 (IPv6) をネゴシエートできるかどうか、電話で IPv6 機能をアダプタイズできるかどうかを指定します。</p> <p>このパラメータを有効にする前に、すべてのノードのプラットフォームに含まれている他のすべてのネットワークコンポーネントで IPv6 を有効にする必要があります。それ以外の場合、システムは引き続き IPv4 専用モードで稼働します。</p> <p>必須フィールドです。</p> <p>デフォルト : False (IPv6 は無効です)</p> <p>IPv6 パラメータの変更を反映するため以下のサービスを再起動し、さらに IM およびプレゼンスサービスクラスタ内の影響を受けるサービスも再起動する必要があります。</p> <ul style="list-style-type: none"> <li>• Cisco CallManager</li> <li>• Cisco IP Voice Media Streaming App</li> <li>• Cisco CTIManager</li> <li>• Cisco Certificate Authority Proxy Function</li> </ul>
Cisco Syslog Agent	リモート Syslog サーバ名 1 (Remote Syslog Server Name 1)	<p>リモート Syslog サーバの名前または IP アドレスを入力します。サーバ名が指定されていない場合、Cisco Unified Serviceability は Syslog メッセージを送信しません。このパラメータは、ログ用に Syslog サーバを使用している場合にのみ必須です。</p> <p>最大長 : 255 文字</p> <p>有効な値 : 大文字と小文字、数字 (0-9)、ハイフン、およびドットを使用した有効なリモート Syslog サーバ名。</p> <p>接続先として別の Cisco Unified Communications Manager ノードを指定しないでください。</p>



カテゴリ (Category)	パラメータ名	説明
セッショントレースのコールレースログの設定	コールトレースログを有効にする (Enable Call Trace Log)	<p>このパラメータは、Cisco Unified Communications Manager が、デバイス名、IP ドレス、およびコール中に使用される SIP 方式を含む、SIP コールの情報を収集できるようにします。Real-Time Monitoring Tool (RTMT) のセッショントレース機能は、トラブルシューティングに役立つコールフロー図を生成するためにこの情報を使用します。</p> <p>SIP コールトラフィック量が多い期間は、ある程度のパフォーマンスの低下が生じることがあります。システムパフォーマンスの影響を低減するには、[セッショントレースのコール関連の REFER/NOTIFY/SUBSCRIBE SIP メッセージをログに記録する (Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace) ] という Cisco CallManager サービスパラメータを [False] に設定します。これによって、SIP コールトレースから REFER、NOTIFY、および SUBSCRIBE メッセージが除外されます。</p> <p>デフォルト : True (SIP コールトレースのロギングは有効)</p>
	コールトレースログファイルの最大数 (Max Number of Call Trace Log Files)	<p>このパラメータは、Cisco Unified Communications Manager が生成できる SIP コールトレースログファイルの最大数を指定します。Real-Time Monitoring Tool (RTMT) のセッショントレース機能は、トラブルシューティングに役立つコールフロー図を生成するためにその情報を使用します。</p> <p>コールトレースログファイルのサイズは、[コールトレースログファイルのサイズ (MB) (Call Trace Log File Size (MB))] パラメータを使用して設定されます。</p> <p>コールトレースログファイルは、ラウンドロビン形式で上書きされます。たとえば、コールトレースログファイルの数として 10 を指定し、コールトレースログファイルのサイズを 5 MB に設定した場合、最初のコールトレースログファイルのデータが 5 MB に達すると、Cisco Unified Communications Manager は 2 番目のコールトレースログファイルを作成するといった具合になります。10 個のファイルが上書きされた後は、最も古いコールトレースログファイルが最新の情報で上書きされます。</p> <p>デフォルト : 2000</p> <p>最小値 : 5</p> <p>最大値 : 4000</p>

カテゴリ (Category)	パラメータ名	説明
	コールトレースログファイルのサイズ (MB) (Call Trace Log File Size (MB))	このパラメータは、SIP コールトレースログファイルの最大ファイルサイズをメガバイト単位で指定します。Real-Time Monitoring Tool (RTMT) のセッショントレース機能は、トラブルシューティングに役立つコールフロー図を生成するためにこの情報を使用します。[コールトレースログファイルパラメータの最大数 (Max Number of Call Trace Log Files)]パラメータが大きな数値に設定されている場合は、ディスク容量をより適切に使用できるように、このパラメータの値を小さくすることを検討してください。  デフォルト：2  最小値：1  最大値：10
Cisco Jabber	ビデオとともにコールを開始しない (Never Start Call with Video)	このパラメータは、ビデオ コールの開始時に、ビデオを送信するかどうかを決定します。すぐにビデオを送信せずにビデオ コールを開始するには、[True] を選択します。ビデオ コール中はいつでも、ビデオの送信開始を選択できます。  このパラメータは、IMおよびプレゼンスサービスの優先度をオーバーライドします。False に設定すると、IMおよびプレゼンス サービスに設定されている優先度に従ってビデオコールが開始します。  デフォルト：[いいえ (False)]

## iOS Cisco Jabber の SSO ログインの動作設定

### 手順

- 
- ステップ 1** Cisco Unified CM の管理から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。
- ステップ 2** オプトイン制御を設定するには、[SSO の設定 (SSO Configuration)] セクションで、[iOS 向け SSO ログイン動作 (SSO Login Behavior for iOS)] パラメータで、[ネイティブブラウザの使用 (Use Native Browser)] オプションを選択します。

(注) [iOS 向け SSO ログイン動作 (SSO Login Behavior for iOS)] パラメータには次のオプションが含まれます。

- [組み込みブラウザの使用 (Use Embedded Browser)] : このオプションを有効にすると、Cisco Jabber は SSO の認証に、組み込みブラウザを使用します。このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。このオプションは、デフォルトで有効です。
- [ネイティブブラウザの使用 (Use Native Browser)] : このオプションを有効にすると、Cisco Jabber は、iOS デバイスで Apple Safari フレームワークを使用し、MDM の導入で、ID プロバイダー (IdP) を利用する証明書ベースの認証を実行します。

(注) ネイティブブラウザの使用は組み込みブラウザの使用ほど安全ではないため、制御された MDM の導入での利用を除いては、このオプションの設定を推奨しません。

ステップ 3 [保存 (Save)] をクリックします。

---

## RTMT への SSO の設定

### 手順

---

ステップ 1 Cisco Unified CM の管理から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] の順に選択します。

ステップ 2 RTMT に SSO を設定するには、[SSO の設定 (SSO Configuration)] セクションで、[RTMT での SSO の使用 (Use SSO for RTMT)] パラメータに [True] を選択します。

(注) [RTMT での SSO の使用 (Use SSO for RTMT)] パラメータには、次のオプションが含まれます。

- [True] : このオプションを選択すると、RTMT は、SAML SSO ベースの IdP ログイン ウィンドウを表示します。

(注) 新規インストール時には、[RTMT での SSO の使用 (Use SSO for RTMT)] パラメータのデフォルト値は [True] になっています。
- [False] : このオプションを選択すると、RTMT は、基本認証のログイン ウィンドウを表示します。

(注) [RTMT での SSO の使用 (Use SSO for RTMT)] パラメータがない Cisco Unified Communications Manager のバージョンからアップグレードする場合、新しいバージョンに表示されるこのパラメータのデフォルト値は [False] です。

ステップ 3 [保存 (Save)] をクリックします。

---

