



## 追加の要件

- [ハイ アベイラビリティ ログイン プロファイル \(1 ページ\)](#)
- [単一クラスタ コンフィギュレーション \(4 ページ\)](#)
- [XMPP 標準への準拠 \(12 ページ\)](#)
- [設定変更通知およびサービス再起動通知 \(13 ページ\)](#)

## ハイ アベイラビリティ ログイン プロファイル

### ハイ アベイラビリティ ログイン プロファイルに関する重要事項

- この項のハイ アベイラビリティ ログイン プロファイル テーブルを使用して、プレゼンス冗長グループのクライアント再ログインの上限値と下限値を設定できます。**[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [システム (System)] > [サービス パラメータ (Service Parameters)]** を選択し、[サービス (Service)] メニューから **[Cisco Server Recovery Manager]** を選択して、クライアント ログインの上限値と下限値を設定します。
- ハイ アベイラビリティ クライアント ログイン プロファイルは、単一クラスタの展開でのみ適用されます。複数のクラスタが存在する場合、ハイ アベイラビリティ クライアント ログイン プロファイルには、冗長グループの上位および下位のクライアントの再ログイン値を設定することはできません。複数のクラスタ展開でハイ アベイラビリティ クライアント ログイン プロファイルを検出するには、さらにテストを実行する必要があります。
- Cisco XCP ルータ サービスに対してデバッグロギングが有効になっている場合は、IM and Presence サービスに対して現在サポートされているロギングレベルの CPU 使用率の増加と減少が予想されます。
- ここに示すテーブルに基づいてプレゼンス冗長グループのクライアント再ログインの上限と下限を設定することで、展開のパフォーマンスの問題および高 CPU スパイクを回避できます。

- 各 IM and Presence Service ノードのメモリ サイズおよび各ハイアベイラビリティ展開タイプ（アクティブ/アクティブまたはアクティブ/スタンバイ）用にハイアベイラビリティログインプロファイルを提供します。
- ハイアベイラビリティログインプロファイルテーブルは、次の入力に基づいて計算されます。
  - クライアント再ログインの下限は、Server Recovery Manager のサービスパラメータ「重要なサービス停止遅延（Critical Service Down Delay）」に基づいており、デフォルトは90秒です。重要なサービス停止遅延（Critical Service Down Delay）が変更されると、下限も必ず変わります。
  - アクティブ/スタンバイ展開のプレゼンス冗長グループ内のユーザ合計数、またはアクティブ/アクティブ展開のユーザが最も多いノード。
- プレゼンス冗長グループ内の両方のノードで、クライアント再ログインの上限値と下限値を設定する必要があります。プレゼンス冗長グループの両方のノードでこれらの値をすべて手動で設定する必要があります。
- クライアント再ログインの上限値と下限値は、プレゼンス冗長グループの各ノードで同じである必要があります。
- ユーザを再平衡化する場合は、ハイアベイラビリティログインプロファイルテーブルに基づくクライアント再ログインの上限値と下限値を再設定する必要があります。

## ハイアベイラビリティログインプロファイルテーブルの使用

ハイアベイラビリティログインプロファイルテーブルを使用して、次の値を取得します。

- [クライアント再ログインの下限（Client Re-Login Lower Limit）] サービスパラメータ値
- [クライアント再ログインの上限（Client Re-Login Upper Limit）] サービスパラメータ値

### 手順

- ステップ 1** 仮想ハードウェア設定およびハイアベイラビリティ展開タイプに基づいてプロファイルテーブルを選択します。
- ステップ 2** プロファイルテーブルで、展開内のユーザ数を選択します（最も近い値に切り上げ）。アクティブ/スタンバイ展開を使用している場合、ユーザが最も多いノードを使用します。
- ステップ 3** プレゼンス冗長グループの[ユーザ数（Number of Users）]の値に基づいて、プロファイルテーブル内の対応する再試行の下限値と上限値を取得します。
- ステップ 4** [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]> [システム（System）]> [サービスパラメータ（Service Parameters）]を選択し、[サービス（Service）]メニューから [Cisco Server Recovery Manager] を選択して、IM and Presence Service の再試行の下限値と上限値を設定します。

ステップ 5 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] > [システム (System)] > [サービス パラメータ (Service Parameters)] を選択し、[サービス (Service)] メニューから [Cisco Server Recovery Manager] を選択して [重要なサービス停止 (Critical Service Down Delay)] の値を確認します。デフォルト値は 90 秒です。再試行下限値はこの値に設定してください。

## 高可用性 ログイン設定の例

### 例 1 : ユーザ数 15,000 のフル UC プロファイル - アクティブ/アクティブ展開

プレゼンス冗長グループ内のユーザが 3,000 人で、あるノードに 2,000 人、2 台目のノードに 1,000 人のユーザがいます。非平衡型のアクティブ/アクティブ展開の場合、シスコはユーザが最も多いノード（この場合は、2,000 人のユーザが割り当てられているノード）を使用することを推奨します。ユーザ数 15,000 のフル米国（4 vCPU 8 GB）アクティブ/アクティブプロファイルを使用して、次の再試行の下限値と上限値を取得します。

アクティブ ユーザの予想数	再試行下限値	再試行上限値
2000	120	253



(注) 再試行上限値は、フェールオーバー発生後にすべてのクライアントがバックアップノードにログインするまでのおおよその時間（秒）です。



(注) 120 の下限値は、[重要なサービス停止遅延 (Critical Service Down Delay)] サービスパラメータが 120 に設定されていることを前提としています。

### 例 2 : ユーザ数 5000 のフル UC プロファイル - アクティブ/アクティブ展開

プレゼンス冗長グループ内の各ノードに 4,700 人のユーザがいます。シスコは、最も近い値に切り上げ、ユーザ数 5,000 のフル米国（4 vCPU 8 GB）アクティブ/アクティブプロファイルを使用して、ユーザ数 5,000 に基づいて、再試行の下限値と上限値を取得することを推奨します。

アクティブ ユーザの予想数	再試行下限値	再試行上限値
5,000	120	953

## 単一クラスタ コンフィギュレーション

### 500 ユーザ フル UC (1vCPU 700MHz 2GB) のアクティブ/アクティブ プロファイル

表 1: 標準展開 (500 ユーザ フル UC のアクティブ/アクティブ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	187
250	120	287

### 500 ユーザ フル UC (1vCPU 700MHz 2GB) のアクティブ/スタンバイ プロファイル

表 2: 標準展開 (500 ユーザ フル UC のアクティブ/スタンバイ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	187
250	120	287
500	120	453

### 1000 ユーザ フル UC (1vCPU 1500MHz 2GB) のアクティブ/アクティブ プロファイル

表 3: 標準展開 (1000 ユーザ フル UC のアクティブ/アクティブ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153

アクティブ ユーザの予想数	再試行下限値	再試行上限値
250	120	203
500	120	287

## 1000 ユーザフル UC (1vCPU 1500MHz 2GB) のアクティブ/スタンバイ プロファイル

表 4: 標準展開 (1000 ユーザフル UC のアクティブ/スタンバイ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453

## 2000 ユーザフル UC (1vCPU 1500Mhz 4GB) のアクティブ/アクティブ プロファイル

表 5: 標準展開 (2000 ユーザフル UC のアクティブ/アクティブ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
500	120	287
1000	120	453

## 2000 ユーザ フル UC (1vCPU 1500Mhz 4GB) のアクティブ/スタンバイ プロファイル

表 6: 標準展開 (2000 ユーザ フル UC のアクティブ/スタンバイ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453
1250	120	537
1,500	120	620
1750	120	703
2000	120	787

## 5000 ユーザ フル UC (4 GB 2vCPU) のアクティブ/アクティブ プロファイル

表 7: 標準展開 (5000 ユーザ フル UC のアクティブ/アクティブ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	137
500	120	203
1000	120	287
1,500	120	370
2000	120	453
2500	120	537

## 5000 ユーザフル UC (4 GB 2vCPU) のアクティブ/スタンバイ プロファイル



注目 5000 ユーザシステムで最大のクライアント ログインスループットを実現するために、シスコでは、少なくとも 2.6 GHz の CPU クロック速度を推奨しています。

表 8: 標準展開 (5000 ユーザフル UC のアクティブ/スタンバイ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	154
500	120	287
1000	120	453
1,500	120	620
2000	120	787
2500	120	953
3,000	120	1120
3500	120	1287
4000	120	1453
4500	120	1620
5,000	120	1787

## 15000 ユーザフル UC (4 vCPU 8GB) のアクティブ/アクティブ プロファイル

注目 15000 ユーザシステムで最大のクライアント ログインスループットを実現するために、シスコでは、少なくとも 2.5GHz の CPU クロック速度を推奨しています。

表 9: 標準展開 (15000 ユーザフル UC のアクティブ/アクティブ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		

アクティブ ユーザの予想数	再試行下限値	再試行上限値
100	120	127
500	120	153
1000	120	187
1,500	120	220
2000	120	253
2,500	120	287
3,000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
7500	120	620

## 15000 ユーザ フル UC (4 vCPU 8GB) のアクティブ/スタンバイ プロファイル

注目 15000 ユーザシステムで最大のクライアントログインスループットを実現するために、シスコでは、少なくとも 2.6GHz の CPU クロック速度を推奨しています。

表 10: 標準展開 (15000 ユーザ フル UC のアクティブ/スタンバイ) のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	137
500	120	203
1000	120	287
1,500	120	370

アクティブ ユーザの予想数	再試行下限値	再試行上限値
2000	120	453
2,500	120	537
3,000	120	620
3500	120	703
4000	120	787
4500	120	870
5000	120	953
6000	120	1120
7000	120	1287
8000	120	1453
9000	120	1620
10,000	120	1787
11000	120	1953
12000	120	2120
13,000	120	2287
14000	120	2453
15000	120	2620

## 25000 ユーザフル UC (6vCPU16GB) のアクティブ/アクティブ プロファイル



注目 25000 ユーザ システムで最大のクライアント ログイン スループットを実現するために、シスコでは、少なくとも 2.8GHz の CPU クロック速度を推奨しています。

表 11: アクティブ/アクティブプロファイルのログインレート: 9 は 45% CPU を使用します。

アクティブ ユーザの予想数	再試行下限値	再試行上限値
100	120	131
500	120	176

アクティブユーザの予想数	再試行下限値	再試行上限値
1000	120	231
1,500	120	287
2000	120	342
2,500	120	398
3,000	120	453
3500	120	509
4000	120	564
4500	120	620
5,000	120	676
6000	120	787
7000	120	898
7500	120	953
8000	120	1009
9000	120	1120
10,000	120	1231
11000	120	1342
12000	120	1453
12500	120	1509

## 25000ユーザフル UC (6 vCPU 16 GB) アクティブ/スタンバイプロファイル



注目 25000ユーザシステムで最大のクライアントログインスループットを実現するために、シスコでは、少なくとも 2.6GHz の CPU クロック速度を推奨しています。

表 12: アクティブ/スタンバイプロファイルのログイン率 : 16ユーザが 80% の CPU を使用

アクティブユーザの予想数	再試行下限値	再試行上限値
100	120	133
500	120	183

アクティブユーザの予想数	再試行下限値	再試行上限値
1000	120	245
1,500	120	308
2000	120	370
2,500	120	433
3,000	120	495
3500	120	558
4000	120	620
4500	120	683
5,000	120	745
6000	120	870
7000	120	995
8000	120	1058
9000	120	1120
10,000	120	1245
11000	120	1370
12000	120	1495
13,000	120	1620
14000	120	1870
15000	120	1995
16000	120	2120
17000	120	2245
18000	120	2370
19000	120	2495
20000	120	2620
21000	120	2745
22000	120	2870
23000	120	2995
24000	120	3120

アクティブユーザの予想数	再試行下限値	再試行上限値
25000	120	3245

## XMPP 標準への準拠

IM and Presence サービスは次の XMPP 標準に準拠しています。

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
  - XEP-0004 Data Forms
  - XEP-0012 Last Activity
  - XEP-0013 Flexible Offline Message Retrieval
  - XEP-0016 Privacy Lists
  - XEP-0030 Service Discovery
  - XEP-0045 Multi-User Chat
  - XEP-0054 Vcard-temp
  - XEP-0055 Jabber Search
  - XEP-0060 Publish-Subscribe
  - XEP-0065 SOCKS5 Bystreams
  - XEP-0066 Out of Band Data Archive OOB requests
  - XEP-0068 Field Standardization for Data Forms
  - XEP-0071 XHTML-IM
  - XEP-0082 XMPP Date and Time Profiles
  - XEP-0092 Software Version
  - XEP-0106 JID Escaping
  - XEP-0114 Jabber Component Protocol
  - XEP-0115 Entity Capabilities
  - XEP-0124 Bidirectional Streams over Synchronous HTTP (BOSH)
  - XEP-0126 Invisibility
  - XEP-0128 Service Discovery Extensions
  - XEP-0160 Best Practices for Handling Offline Messages
  - XEP-0163 Personal Eventing Via PubSub
  - XEP-0170 Recommended Order of Stream Feature Negotiation

- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT (Stanza Interception and Filtering Technology)

## 設定変更通知およびサービス再起動通知

サービスを再起動する必要がある場合は常に、**アクティブな通知**ポップアップが表示されます。Cisco ユニファイド CM IM and プレゼンス管理 GUI ヘッダーの右上に、**アクティブな通知の概要**が表示されます。

さらに、Cisco ユニファイド CM IM and プレゼンス管理インターフェイスから [システム > 通知(System notification)] を選択して、アクティブな通知リストにアクセスすることもできます。

### 再起動が必要な設定変更

多くの IM およびプレゼンス設定の変更と更新については、Cisco XCP ルータ、Cisco SIP プロキシ、または Cisco Presence エンジンを再起動する必要があります。

次の表に、これらのサービスの再起動が必要な設定変更を示します。このリストには設定の変更が含まれていますが、インストールやアップグレードなどのプラットフォームの変更は含まれていません。

再起動が必要な設定	再起動するサービス
<b>アプリケーション リスナーの設定</b> ([システム (System)] > [アプリケーションリスナー (Application Listeners)]) アプリケーション リスナーの編集	Cisco SIP Proxy
<b>コンプライアンス プロファイルの設定</b> (Messaging > コンプライアンス > コンプライアンス設定) (Messaging > コンプライアンス > コンプライアンスプロファイル サードパーティコンプライアンスサーバに割り当てられているイベントの設定を編集する場合)	Cisco XCP Router
<b>グループ チャットのシステム管理者</b> ([メッセージング (Messaging)] > [グループチャットのシステム管理者 (Group Chat System Administrators)]) この設定を有効または無効にすると、	Cisco XCP Router

再起動が必要な設定	再起動するサービス
<b>外部ファイル サーバの設定</b> ([メッセージング (Messaging)] > [外部サーバの設定 (External Server Setup)] > [外部ファイルサーバ (External File Servers)]) [ホスト/Ip アドレス (Host/IP Address)] 設定を編集する場合 外部ファイルサーバの公開キーを再生成する場合	Cisco XCP Router
<b>グループ チャットと持続チャットの設定</b> ([メッセージング (Messaging)] > [グループチャットと持続チャット (Group Chat and Persistent Chat)]) 起動時にチャットノードが外部データベースに到達できない場合は、Cisco XCP Text 会議マネージャサービスが実行されていません。	Cisco XCP Router
<b>グループ チャット サーバエイリアス マッピング</b> ([メッセージング (Messaging)] > [グループチャットサーバエイリアスマッピング (Group Chat Server Alias Mapping)]) チャットエイリアスの追加	Cisco XCP Router
<b>ACL 設定</b> ([システム (System)] > [セキュリティ (Security)] > [着信ACL (Incoming ACL)]) ([システム (System)] > [セキュリティ (Security)] > [発信ACL (Outgoing ACL)]) 着信または発信 ACL の設定の編集	Cisco SIP Proxy
<b>コンプライアンス設定</b> メッセージアーカイバ: 設定を編集します。	Cisco XCP Router
<b>LDAP サーバ (LDAP Server)</b> (アプリケーション > サードパーティ製クライアント > サードパーティの LDAP 設定) LDAP 検索: LDAP 検索の編集 LDAP からのビルド Vcard の編集 VCard FN に使用する LDAP 属性の編集	Cisco XCP Router

再起動が必要な設定	再起動するサービス
<p><b>メッセージ設定の構成</b></p> <p>([メッセージング (Messaging) ]&gt;[設定 (Settings) ])</p> <p>[インスタントメッセージの有効化 (Enable instant message)] の編集</p> <p>オフライン中の相手へのインスタントメッセージの送信を無効にする</p>	Cisco XCP Router
<p><b>Microsoft RCC の設定</b></p> <p>([アプリケーション (Application) ]&gt;[Microsoft RCC]&gt;[設定 (Settings) ])</p> <p>このページの設定の編集</p>	Cisco SIP Proxy
<p><b>プレゼンス ゲートウェイ (Presence Gateway)</b></p> <p>([プレゼンス (Presence) ]&gt;[ゲートウェイ (Gateways) ])</p> <p>プレゼンス ゲートウェイの追加、編集、削除</p> <p>MS Exchange 証明書をアップロードした後</p>	Cisco Presence Engine
<p><b>プレゼンス設定の構成</b></p> <p>([プレゼンス (Presence) ]&gt;[設定 (Settings) ]&gt;[標準設定 (Standard Configuration) ])</p> <p>[プレゼンスステータスの共有を有効にする (Enable Availability Sharing) ] 設定の編集</p> <p>確認プロンプトなしで、ユーザが他のユーザのプレゼンスステータスを表示できるようにする</p> <p>連絡先リストの最大サイズ (ユーザごと) (Maximum Contact List Size (per user))</p> <p>最大数のウォッチャー</p>	Cisco Presence Engine Cisco XCP Router
<p><b>プレゼンス設定の構成</b></p> <p>([プレゼンス (Presence) ]&gt;[設定 (Settings) ]&gt;[標準設定 (Standard Configuration) ])</p> <p>[ <b>Enable user Of Email address For ドメイン間フェデレーション</b> ] フィールドの編集</p>	Cisco XCP Router

再起動が必要な設定	再起動するサービス
<p><b>パーティションイントラドメイン フェデレーションの設定</b></p> <p>[プレゼンス (Presence) ]&gt;[設定 (Settings) ]&gt;[標準設定 (Standard Configuration) ] (チェックボックス)</p> <p>プレゼンス&gt;イントラドメインフェデレーションのセットアップ(ウィザード)</p> <p>チェックボックスを使用するか、またはウィザードを使用して、LC/OCS/Lync とのパーティションイントラドメインフェデレーションを有効にします。</p> <p>パーティション分割されたイントラドメインルーティングモード: [Standard Configuration] ウィンドウまたはウィザードを使用して設定します。</p>	<p>これらの設定を編集すると、Cisco SIP プロキシが自動的に再起動します</p> <p>さらに、XCP ルータを再起動する必要があります。</p>
<p><b>プロキシ設定</b></p> <p>([プレゼンス (Presence) ]&gt;[ルーティング (Routing) ]&gt;[設定 (Settings) ])</p> <p>プロキシ設定に対するすべての編集</p>	Cisco SIP Proxy
<p><b>セキュリティ設定 (Security Settings)</b></p> <p>([システム (System) ]&gt;[セキュリティ (Security) ]&gt;[設定 (Settings) ])</p> <p>Sip クラスタ内プロキシからプロキシトランスポートプロトコルなどの SIP セキュリティ設定の編集</p> <p>XMPP セキュリティ設定の編集</p>	<p>Cisco SIP プロキシ (SIP セキュリティの編集用)</p> <p>Cisco XCP ルータ (XCP セキュリティの編集用)</p>
<p><b>SIP フェデレーテッドドメイン</b></p> <p>([プレゼンス (Presence) ]&gt;[ドメイン間フェデレーション (Interdomain Federation) ]&gt;[SIP フェデレーション (SIP Federation) ])</p> <p>この設定の追加、編集、削除</p>	Cisco XCP Router
<p><b>サードパーティ製コンプライアンス サービス</b></p> <p>(アプリケーション&gt;サードパーティ製クライアント&gt;サードパーティ製 LDAP サーバ)</p> <p>[Hostname/IP Address]、[Port]、[Password]、[Confirm Password] の各フィールドを編集します。</p>	Cisco XCP Router

再起動が必要な設定	再起動するサービス
<b>TLS ピア サブジェクトの設定</b> ([システム (System)] > [セキュリティ (Security)] > [TLSピアサブジェクト (TLS Peer Subjects)]) このページでの編集	Cisco SIP Proxy
<b>TLS コンテキスト</b> ([システム (System)] > [セキュリティ (Security)] > [TLSコンテキスト設定 (TLS Context Configuration)]) このページでのいずれかの編集	関連付けられているチャットサーバの再起動が必要になる場合があります
<b>XMPP フェデレーション</b> ([プレゼンス (Presence)] > [ドメイン間フェデレーション (Interdomain Federation)] > [XMPPフェデレーション (XMPP Federation)] > [設定 (Settings)]) ([プレゼンス (Presence)] > [ドメイン間フェデレーション (Interdomain Federation)] > [XMPPフェデレーション (XMPP Federation)] > [ポリシー (Policy)]) XMPP フェデレーションに対するすべての編集	Cisco XCP Router
<b>クラスタ間ピアリング</b> (プレゼンス クラスタ間設定) クラスタ間ピア設定の編集	場合によっては、Cisco XCPルータを再起動するように求められる場合があります (右上のウィンドウに通知が表示されます)。
<b>イーサネット設定</b> ([Cisco Unified IM and PresenceのOSの管理 (Cisco Unified IM and Presence OS Administration)] から、[設定 (Settings)] > [IP] > [イーサネット/イーサネットIPv6 (Ethernet/Ethernet IPv6)]) いずれかのイーサネット設定の編集	システムがすぐに再起動される
<b>IPv6 設定</b> ([システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)]) [IPv6を有効化] エンタープライズパラメータの有効化の編集	Cisco XCP Router Cisco SIP Proxy Cisco Presence Engine

再起動が必要な設定	再起動するサービス
<b>トラブルシューティング</b> サブスクライバがオフラインのときに IM およびプレゼンスパブリッシャが変更された場合 サブスクライバから > IP > パブリッシャの設定を編集します。	サブスクライバノードの再起動
IM and プレゼンスのアップグレード中に、以前のバージョンに切り替える必要があります	システムを再起動します。
cup 証明書の再生成	Cisco SIP Proxy Cisco Presence Engine
カップの再生成-xmpp	Cisco XCP Router
cup-xmpp-s2s 証明書の再生成	Cisco XCP Router
新しい証明書のアップロード	その証明書に関連するサービスを再起動します。  カップ信頼証明書の場合は、Cisco SIP プロキシを再起動します。
リモート監査ログの転送プロトコル  任意のユーティリティ <code>remotesyslog set protocol *</code> CLI コマンドを実行する場合	ノードの再起動
次のいずれかのアラートが表示された場合: <ul style="list-style-type: none"> <li>• PEIDSQueryError</li> <li>• PEIDStoIMDBDatabaseSyncError</li> <li>• PEIDSSubscribeError</li> <li>• PEWebDAVInitializationFailure</li> </ul>	Cisco Presence エンジン を再起動することをお勧めします。
次のアラートのいずれかを受け取った場合 <ul style="list-style-type: none"> <li>•</li> <li>• XCPCConfigMgrJabberRestartRequired</li> <li>• XCPCConfigMgrR2RPasswordEncryptionFailed</li> <li>• XCPCConfigMgrR2RRequestTimedOut</li> <li>• XCPCConfigMgrHostNameResolutionFailed</li> </ul>	Cisco XCP ルータを再起動することをお勧めします。

再起動が必要な設定	再起動するサービス
PWSSCBInitFailed	Cisco SIP プロキシを再起動することをお勧めします。
Exchange サービスパラメータの編集 <ul style="list-style-type: none"> <li>• Microsoft Exchange 通知ポート (Microsoft Exchange Notification Port)</li> <li>• カレンダーの拡散</li> <li>• Exchange タイムアウト (秒) (Exchange Timeout (seconds))</li> <li>• Exchange キュー (Exchange Queue)</li> <li>• スレッドの交換</li> <li>• EWS ステータスの頻度</li> </ul>	Cisco Presence Engine
Exchange 証明書のアップロード	Cisco SIP Proxy Cisco Presence Engine
ロケールのインストール	IM and Presence サービスの再起動
新しい MSSQL 外部データベースの作成	Cisco XCP Router
外部データベース設定の編集	Cisco XCP Router
外部データベースのマージ	Cisco XCP Router
TLS ピア サブジェクトの設定	Cisco SIP Proxy
ピア認証 TLS コンテキストの設定	Cisco SIP Proxy

再起動が必要な設定	再起動するサービス
<p>次の Cisco SIP プロキシサービスパラメータを編集します。</p> <ul style="list-style-type: none"> <li>• CUCM ドメイン</li> <li>• サーバ名 (補足)</li> <li>• HTTP ポート (HTTP Port)</li> <li>• ステートフルサーバ (トランザクションステートフル)</li> <li>• TCP 接続の永続化</li> <li>• 共有メモリサイズ (バイト) (Shared memory size (bytes))</li> <li>• フェデレーションルーティング IM/P FQDN</li> <li>• Microsoft フェデレーションのユーザエージェントヘッダー (カンマ区切り)</li> </ul>	Cisco SIP Proxy
ルーティング通信タイプのサービスパラメータの編集	Cisco XCP Router
IM アドレススキームの編集	Cisco XCP Router
デフォルトドメインの割り当て	Cisco XCP Router
クラスタからのノードの削除または削除	Cisco XCP Router
Cisco XCP ルータに影響を与えるパラメータを編集するには、Cisco XCP ルータを再起動する必要があります。	Cisco XCP Router
ルーティング通信タイプサービスパラメータ	Cisco XCP Router
<p>Cisco XCP File Transfer Manager サービスパラメータのいずれかを編集します。</p> <ul style="list-style-type: none"> <li>• 外部ファイルサーバの使用可能なスペースの下限しきい値</li> <li>• 外部ファイルサーバの使用可能領域の上限しきい値</li> </ul>	Cisco XCP Router
[マルチデバイスメッセージングの有効化 (Enable 複数 Device Messaging)] サービスパラメータの編集	Cisco XCP Router
[ Maximum number of logon sessions per user ] サービスパラメータの編集	Cisco XCP Router
外部データベース上の install_dir/data/pg_hba.conf または install_dir/data/postgresql.conf config ファイルの更新	Cisco XCP Router

再起動が必要な設定	再起動するサービス
移行ユーティリティ： <ul style="list-style-type: none"><li>• [プレゼンスの設定 (Presence Settings) ] ウィンドウでの [確認プロンプトなしで、ユーザが他のユーザのプレゼンスステータスを表示できるようにする (Allow users to view the availability of other users without being prompted for approval) ] 設定の編集。</li><li>• [プレゼンス設定の構成 (プレゼンス設定の設定)] ウィンドウで、<b>連絡先リストの最大サイズ(ユーザ単位)と最大数のウォッチャー(ユーザごと)</b>の設定を編集します。</li></ul>	Cisco XCP Router
クラスタからのノードの削除または削除	Cisco XCP Router



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。