



## **Cisco Unified Communications Manager の IM and Presence サービスのパーティションイントラドメインフェデレーション、リリース 11.0(1)**

初版：2015年06月08日

### **シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリック ドメイン バージョンの一部として、UCB が開発したプログラムを最適化したものです。 All rights reserved. Copyright © 1981, Regents of the University of California.

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。

Cisco および Cisco ロゴは、シスコや米国および他の国の関連会社の商標です。シスコの商標の一覧は、<http://www.cisco.com/go/trademarks> で参照できます。本書に記載されているサードパーティの商標は、それぞれの所有者の財産です。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません (1110R)。

© 2016 Cisco Systems, Inc. All rights reserved.



## 目次

### 統合の概要 1

パーティションイントラドメインフェデレーション 1

パーティションフェデレーション配置の概要 2

単一ドメインの例 3

複数のドメインの例 4

複数ドメインの設定ミスの例 5

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 6

アベイラビリティ 9

アベイラビリティの登録およびポリシー 9

IM and Presence サービス ユーザへのサブスクリプション 10

Microsoft Lync または Microsoft Office Communicator ユーザへのサブスクリプション 10

アベイラビリティ マッピング状態 11

インスタントメッセージ 13

要求のルーティング 14

IM and Presence から Microsoft サーバへの要求のルーティング 14

パーティションイントラドメインフェデレーションの基本的なルーティングモード 14

パーティションイントラドメインフェデレーションの高度なルーティングモード 16

IM and Presence サービスの要求ルーティングへの Microsoft サーバ 16

クラスタ間展開とマルチノード展開 18

ドメイン間フェデレーション 18

ドメイン内フェデレーションのハイ アベイラビリティ 19

Microsoft サーバ要求ルーティングへの IM and Presence サービスのハイアベイラビリティ 19

Microsoft サーバから IM and Presence サービスへの要求のルーティングのハイア ベイルビリティ	21
連絡先の検索	22
ユーザの移行	22
IM アドレスの例	23
ユーザ移行ツール	24
<b>統合の計画</b>	<b>27</b>
サポート対象のパーティションイントラドメイン フェデレーションの統合	27
Presence Web Service の API サポート	28
Microsoft Lync の統合に関する制約事項	28
ハードウェア要件	29
ソフトウェア要件	30
サーバソフトウェア	30
クライアントソフトウェア	31
IM and Presence サービス対応クライアント	31
Microsoft サーバ対応クライアント	31
統合の準備	32
プレゼンス ドメイン	32
ユーザの移行	33
DNS の設定	33
認証権限サーバ	33
高可用性	33
IM and Presence サービスの前提条件の設定	34
IM and Presence サービス ノードのルーティングの追加構成	34
IM and Presence サービス機能サービスの開始	35
オフピーク期間中のサービス再起動の計画	36
<b>ユーザの移行計画</b>	<b>37</b>
移行中のユーザ ID の保守	37
移行前のタスク	38
Microsoft サーバ SIP URI 変更	40
IM and Presence サービス ユーザの連絡先の名前変更	40
詳細なユーザ移行計画	41

1000 ユーザ OVA	42
5000 ユーザ OVA	43
ユーザ移行ツールの時間に関するガイドライン	43
連絡先リスト エクスポート ツール	43
アカウント無効化ツール	44
アカウント削除ツール	44
一括管理ツールの連絡先リストのインポート	45
一括管理ツールの連絡先の名前変更	46
<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ワークフロー</b>	<b>47</b>
Lync を使用した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ワークフロー	47
OCS を使用した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ワークフロー	49
Microsoft サーバから IM and Presence サービスへのユーザの移行のための設定ワークフロー	51
IM and Presence と Microsoft サーバドメイン間フェデレーションフェデレーション機能との統合の設定ワークフロー	52
<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 IM and Presence サービス ノードの設定</b>	<b>53</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ドメイン設定	53
IM アドレス ドメインの表示	54
パーティションイントラドメイン フェデレーション オプションの設定	54
スタティック ルートの設定	56
着信アクセス コントロール リストの設定	58
TLS 暗号化の設定	59
アプリケーション リスナー ポートを設定します。	60
TLS ピア サブジェクトの設定	61
ピア認証 TLS コンテキストの設定	62
認証局のルート証明書のインポート	63
IM and Presence サービスの証明書署名要求の生成	64
認証局からの署名付き証明書のインポート	65
ルーティング IM and Presence サービス ノードでの機能サービスの非アクティブ化	66

**パーティションイントラドメイン フェデレーション用 Microsoft Lync の設定 69**

Lync サーバのドメインの確認 70

Microsoft Lync サーバ コンフィギュレーション タスク リストにフェデレーション リンク 70

フェデレーション用の Microsoft Lync のスタティック ルートを設定 73

Enterprise Edition Lync Server での IM and Presence サービスに対するホスト認証の追加 76

IM and Presence サービスのホスト認証をスタンダード エディションの Lync サーバに追加 78

トポロジのパブリッシュ 80

Lync への認証局のルート証明書のインストール 81

既存の Lync 署名付き証明書の検証 83

Lync の認証局から署名付き証明書を要求 84

CA サーバから証明書をダウンロード 86

Lync の署名付き証明書をインポート 86

Lync への証明書の割り当て 87

Lync サーバでのサービスの再起動 88

**Microsoft Office Communications Server for Partitioned Intradomain Federation の設定 91**

OCS サーバのドメインの確認 91

OCS サーバでのポート 5060/5061 の有効化 92

Microsoft OCS サーバ コンフィギュレーション タスク リストへのフェデレーテッド リンク 93

IM and Presence サービスをポイントする OCS のスタティック ルートの設定 96

OCS での IM and Presence サービスのホスト認証の追加 97

OCS フロント エンド サーバでのサービスの再起動 98

TLS 暗号化の設定 99

連邦情報処理標準コンプライアンスを OCS で有効にする 99

TLS 相互認証の OCS での設定 100

認証局ルート証明書の OCS へのインストール 101

既存の OCS 署名付き証明書の検証 103

OCS サーバの認証局から署名付き証明書の要求 104

OCS サーバで署名付き証明書をインストールします。 106

TLS ネゴシエーション用にインストールされた証明書の選択	107
<b>ユーザの移行</b>	<b>109</b>
シスコのユーザ移行ツール	109
移行前の推奨事項	110
無制限の連絡先リストとウォッチャの設定	111
サブスクリプション要求の自動許可の有効化	111
サブスクライバ通知ポップアップ	112
Microsoft Lync ポップアップの無効化	113
リストアの Microsoft Lync のポップアップ動作	113
移行するユーザ用の Microsoft サーバ SIP URI 形式の確認	114
Lync SIP URI の変更	115
OCS SIP URI の変更	115
IM and Presence サービスの連絡先リスト内のコンタクト ID の変更	116
コンタクト ID のジョブの名前変更結果	118
Cisco Unified Communications Manager の Microsoft サーバのユーザ プロビジョニング	118
ユーザの Microsoft サーバの連絡先リスト情報のバックアップ	119
ユーザを移行するための連絡先リストのエクスポート	119
ログ ファイル	120
実行モード	121
入力ファイルの形式	121
Microsoft サーバのユーザの無効化	125
移行するユーザの Microsoft サーバ アカウントの無効化	125
Active Directory の更新が Microsoft サーバと同期していることの確認	126
ユーザを移行するためのデータベースからのユーザ データの削除	128
IM and Presence にユーザを移行するための連絡先リストのインポート	130
BAT を使用した CSV ファイルのアップロード	131
新しい一括管理ジョブの作成	132
一括管理ジョブの結果	132
ユーザ... への IM and Presence サービスでサポートされているクライアントの導入	132
連絡先リストと最大ウォッチャの最大サイズのリセット	133
<b>ドメイン間フェデレーションとイントラドメイン フェデレーション導入の統合</b>	<b>135</b>

Microsoft サーバのドメイン間フェデレーション機能の IM and Presence サービスの統合	135
連携動作と制限事項	136
Microsoft サーバのドメイン間フェデレーション機能の IM and Presence サービスの統合	136
Microsoft サーバのドメイン内フェデレーション接続を介したドメイン間フェデレーションのリモートドメインのセットアップ	137
リモートドメインへのスタティックルートの設定	138
Microsoft サーバのドメイン間フェデレーション機能と IM and Presence サービス統合の削除	140
リモートドメイン用のスタティックルートの削除	140
SIP フェデレーションドメインの削除	140
統合のトラブルシューティング	143
IM and Presence サービスのトレース	143
IM and Presence サービスのトレースの設定	145
Microsoft サーバ SIP トレース	146
Lync での SIP トレースの有効化	146
OCS 上での SIP トレースの有効化	147
統合の一般的な問題	148
Lync の 2013 クライアントが、IM and Presence サービス ユーザを連絡先リストに追加した後、繰り返しログアウトおよびログインする	148
Microsoft サーバのユーザを IM and Presence サービス連絡先リストに追加すると、ポップアップを受信しない	148
Microsoft サーバのユーザを IM and Presence サービスの連絡先リストに追加すると、ポップアップを受信するが、承認後のアベイラビリティがない	149
Microsoft Lync または Microsoft Office Communicator ユーザが連絡先リストにユーザを追加した場合に IM and Presence サービス ユーザにポップアップが表示されない	150
IM and Presence サービスのユーザが送信した IM を Microsoft サーバのユーザが受信しない	151
Microsoft サーバユーザによって送信された IM を IM and Presence ユーザが受信しない	152



Microsoft サーバの更新と IM の表示に最大 40 秒かかる	153
高度なルーティングがイネーブルの場合にアベイラビリティが IM and Presence サービスと Microsoft サーバの間で交換されない	154
IM and Presence サービス ユーザが Microsoft サーバ アドレス帳に表示されない	154
IM and Presence サービスがドメイン間フェデレーション要求を Microsoft サーバの配置経路でルーティングできない	155
IM and Presence サービスおよび Microsoft サーバ間の TLS ハンドシェイク エラー	155
Microsoft Lync ユーザまたは Microsoft Office Communicator ユーザが Cisco Unified Personal Communicator の連絡先リストに追加されると、不正な SIP URI がそのユーザに指定される	156
Cisco Unified Personal Communicator 上の Microsoft Lync または Microsoft Office Communicator の連絡先に表示名が表示されない	156
ユーザ移行のトラブルシューティング	156
ユーザ移行のトレース	156
連絡先リスト エクスポート ツール	156
アカウント無効化ツール	158
アカウント削除ツール	159
IM and Presence サービス BAT による連絡先リストのインポート	161
IM and Presence サービスでの一括プロビジョニング サービス ログの設定	161
IM and Presence サービス一括管理ツールの連絡先の名前変更	162
ユーザ移行の一般的な問題	163
アプリケーションが正しく初期化できない：ユーザ移行ツールのいずれかを実行しているときにエラーが発生する	163
連絡先リスト エクスポート ツールが Lync ユーザ用の出力ファイルを生成しない	164
連絡先リスト エクスポート ツールのログに getAndPrintContactsForUsers エラーが表示される	164
連絡先リスト エクスポート ツール - ログの概要にいくつかのユーザが見つからないと表示される	164

- 連絡先リストエクスポート ツール - 通常モードで実行すると、ツールは経過表示バーを表示せず、エクスポートされた連絡先の出力ファイルを生成しない **165**
- アカウント無効化ツール - ログには、IP/FQDN/ホスト名を使用して LDAP に接続できないことが記載されている **165**
- アカウント削除ツール - Microsoft サーバデータベースまたはサーバインスタンスが見つからない **166**
- アカウント削除ツール - SQL Server への接続中にログにエラーが表示される **166**
- BAT 連絡先リストの更新 : アップロードされた連絡先リスト ファイルがドロップダウンリストに表示されない **167**
- BAT 連絡先リストの更新 : BAT ジョブの後にログ ファイルが結果ページ上に存在しない **167**
- BAT 連絡先リストの更新 : ユーザの連絡先が BAT ジョブ中にインポートされない **167**
- BAT 連絡先リストの更新 : ユーザの連絡先が BAT ジョブ中に部分的にインポートされる **167**
- BAT 連絡先リストの更新 - 連絡先が BAT ジョブ中にインポートされない **168**
- ユーザ ステータスの移行は、移行プロセス中に Microsoft サーバユーザに対して「ステータスが不明 (Status Unknown) 」または「プレゼンスが不明 (Presence Unknown) 」と表示される **168**



## 第 1 章

# 統合の概要

- [パーティションイントラドメインフェデレーション, 1 ページ](#)
- [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, 6 ページ](#)
- [アベイラビリティ, 9 ページ](#)
- [インスタントメッセージ, 13 ページ](#)
- [要求のルーティング, 14 ページ](#)
- [クラスタ間展開とマルチノード展開, 18 ページ](#)
- [ドメイン間フェデレーション, 18 ページ](#)
- [ドメイン内フェデレーションのハイアベイラビリティ, 19 ページ](#)
- [連絡先の検索, 22 ページ](#)
- [ユーザの移行, 22 ページ](#)

## パーティションイントラドメインフェデレーション

IM およびアベイラビリティプラットフォームとして Cisco Unified Communication Manager IM and Presence サービスを選択する企業はますます増えています。これらの企業にすでに Microsoft Lync または配置された Microsoft Office Communications Server (OCS) があり、IM and Presence サービス対応クライアントにユーザを移行するようにします。

この移行中、IM and Presence サービス対応クライアントに移行するユーザは、Microsoft サーバをまだ使用しているユーザとアベイラビリティおよびインスタントメッセージを引き続き共有できることが重要です。対応している IM and Presence サービスクライアントの詳細については、「ソフトウェア要件」の項を参照してください。

パーティションイントラドメインフェデレーションでは、同一企業内の IM and Presence サービスクライアントユーザと Microsoft Lync または Microsoft Office Communicator のユーザが、プレゼンスアベイラビリティとインスタントメッセージ (IM) を交換できます。

この統合により、IM and Presence サービスと Microsoft サーバの両方で共通ドメインまたはドメインのセットをホストできます。それらのドメイン内の各ユーザは IM and Presence サービスまたは Microsoft サーバでイネーブルになります。



(注) パーティションイントラドメインフェデレーションでは、ユーザは1つのシステムでのみで有効である必要があります。この統合は、IM and Presence サービスと Microsoft サーバで、同時にユーザをサポートしません。

IM and Presence サービスは、標準 Session Initiation Protocol (SIP RFC 3261) を使用して、次の Microsoft サーバプラットフォームにパーティションイントラドメインフェデレーションのサポートを提供します。

- Microsoft Lync Server 2010、Standard Edition および Enterprise Edition
- Microsoft Lync Server 2013、Standard Edition および Enterprise Edition
- Microsoft Office Communications Server 2007 R2 Standard Edition および Enterprise Edition



(注) このマニュアルで使用されている Microsoft サーバという用語は、サポートされているすべての Lync および OCS プラットフォームのタイプを示しています。特定のプラットフォームに固有の情報が識別されます。

#### 関連トピック

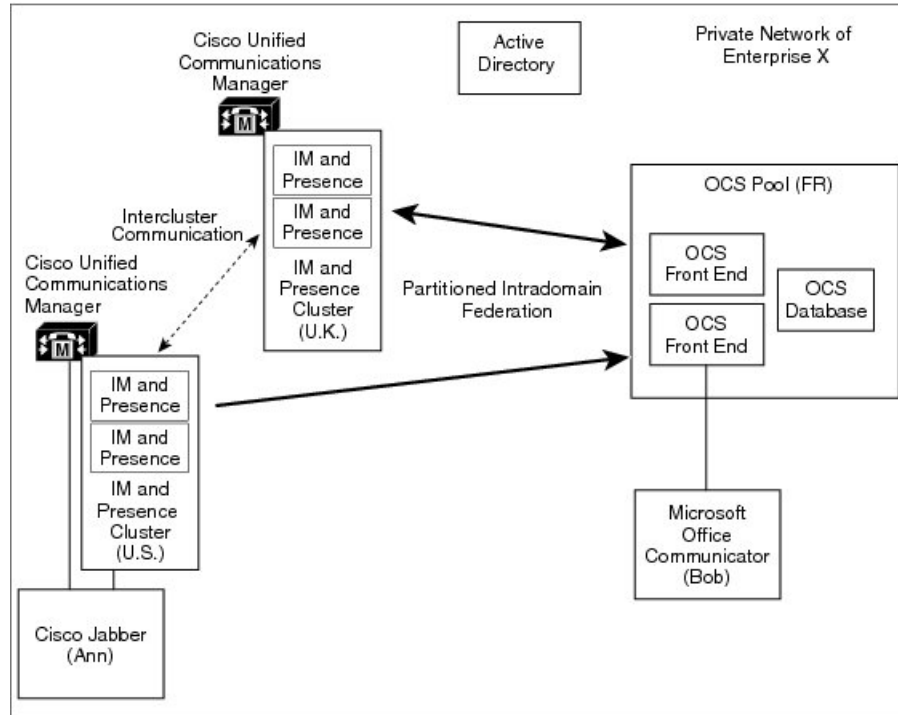
[ソフトウェア要件, \(30 ページ\)](#)

## パーティションフェデレーション配置の概要

次の図は、IM and Presence サービス と Microsoft OCS を同じドメイン内に配置したハイレベルサンプルを示します。次に、OCS 配置を示しますが、これはサポートされている他の Microsoft サーバにも適用されます。

単一のプレゼンス ドメインと複数のプレゼンス ドメインの両方の導入がサポートされます。複数のプレゼンスドメインの導入では、両方のシステムで同じプレゼンスドメインを設定する必要があります。

図 1: 統合の概要



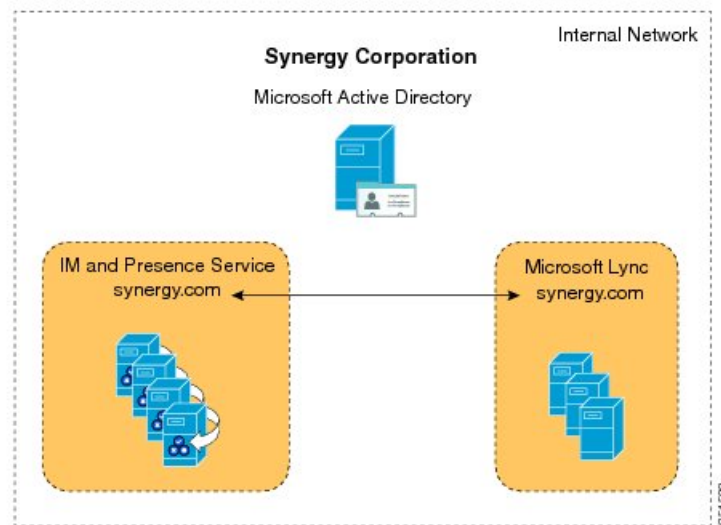
344456

## 単一ドメインの例

この例では、IM and Presence サービス ノードと Microsoft Lync サーバの両方の synergy.com というプレゼンス ドメイン内のユーザは、このドメインが両方のシステムに設定されているため、パーティションイントラドメインフェデレーションを使用してアベイラビリティと IM を交換できま

す。共通の Active Directory によって連絡先を検索し、両方のシステムのすべてのユーザの名前解決を表示できます。

図 2: 単一プレゼンス ドメインのイントラドメイン フェデレーションの例



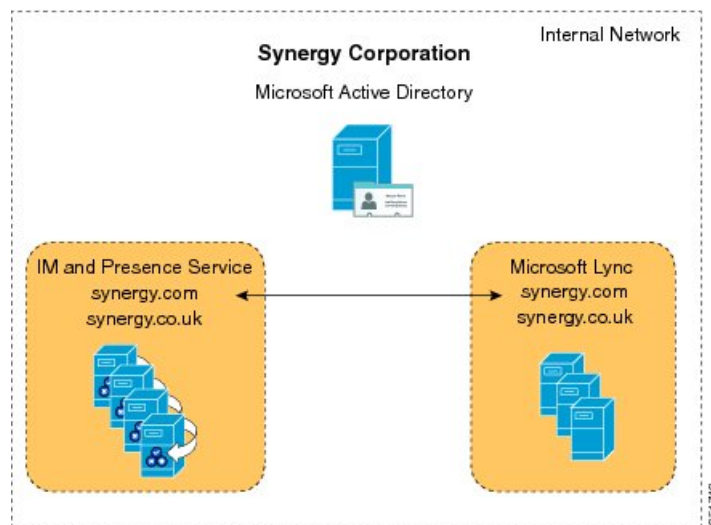
(注) プレゼンス ドメインは同一である必要があります。たとえば、`user1@abc.synergy.com` は `synergy.com` のドメイン内フェデレーションに設定されたフェデレーション ユーザで IM とアベイラビリティを共有できません。 `user1` を `abc.synergy.com` プレゼンス ドメインから `synergy.com` ドメインに移動し、`user1` が、次の例のパーティションイントラドメインフェデレーションに参加できるようにします。

## 複数のドメインの例

この例では、`synergy.com` というプレゼンス ドメイン内のユーザと IM and Presence サービス ノードと Microsoft Lync サーバの両方の `synergy.co.uk` というドメイン内のユーザは、これらのドメインが両方のシステムに設定されているため、イントラドメインフェデレーションを使用して可用

性と IM を交換できます。共通の Active Directory によって連絡先を検索し、両方のシステムのすべてのユーザのプレゼンス名の解決を表示できます。次の図を参照してください。

図 3: 複数ドメインのイントラドメイン フェデレーションの例

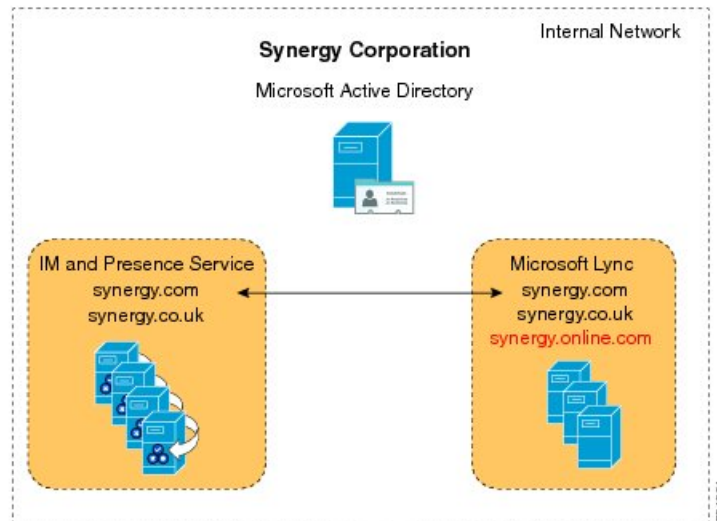


## 複数ドメインの設定ミスの例

この例では、synergy.com と synergy.co.uk というドメインのユーザは、イントラドメイン フェデレーションに適切に設定され、IM およびアベイラビリティを交換できます。ただし、Lync サーバ上の synergy.online.com というドメイン内のユーザは synergy.online.com ドメインが IM and Presence

サービス ノードで設定されていないため、フェデレーテッド IM and Presence サービス システムのユーザとはアベイラビリティと IM を交換することはできません。次の図を参照してください。

図 4: 複数ドメインの設定ミスの例



synergy.online.com のユーザがフェデレーテッド IM and Presence サービス システムのユーザとアベイラビリティと IM を交換できるようにするには、synergy.online.com というドメインを IM and Presence サービス ノードに追加します。



(注) ユーザがそれらのドメインに最初に割り当てられていなくても IM and Presence サービス システムの追加ドメインを設定できます。

## 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

IM and Presence サービスと Microsoft Lync/OCS サーバ間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イネーブルにするには、次の主なコンポーネントを設定します。

- 1 IM and Presence サービス ノード
- 2 Microsoft サーバ
- 3 ユーザの移行





## ヒント

パーティションイントラドメインフェデレーションをイネーブルにするために必要な開始から完了ステップとプロセスの各ステップで実行する手順へのリンクの詳細設定ワークフローを確認します。

IM and Presence サービスと Microsoft のサーバとの間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設定する前に、Microsoft サーバユーザの連絡先リストの情報をバックアップすることを推奨します。

表 1: **IM and Presence** サービス ノードのパーティションイントラドメインフェデレーションのハイ レベル設定タスク

タスク	O = オプション M = 必須
必要なすべてのドメインが IM and Presence サービス ノードに設定されていることを確認し、一致するドメインが Microsoft サーバに設定されていることを確認します。	M
パーティションイントラドメインフェデレーションの有効化	M
Microsoft サーバへのスタティック ルートのセットアップ	M
セットアップのアクセス コントロール リスト	M
Lync サーバへの TLS のセットアップ (Lync サーバを使用する場合は必須)	M
OCS サーバへの TLS のセットアップ	O
専用ルーティング サーバの必須でないサービスの非アクティブ化 (該当する場合)	M

表 2: **Lync** サーバ用パーティションイントラドメインフェデレーションのハイ レベル設定タスク

タスク	O = オプション M = 必須
必要なすべての Lync ドメインが設定されていることを確認し、一致するドメインが IM and Presence サービス ノードで設定されていることを確認します。	M
IM and Presence サービス ノードへのスタティック ルートのセットアップ	M
ホスト認証のセットアップ	M

タスク	O = オプション M = 必須
トポロジのパブリッシュ	M
TLS のセットアップ	M

表 3: OCS サーバ用パーティションイントラドメインフェデレーションのハイレベル設定タスク

タスク	O = オプション M = 必須
必要なすべてのドメインが OCS サーバに設定されていることを確認し、一致するドメインが IM and Presence サービス ノードで設定されていることを確認します。	M
SIP ポートの有効化	M
IM and Presence サービス ノードへのスタティック ルートのセットアップ	M
ホスト認証のセットアップ	M
TLS のセットアップ	O

表 4: パーティションイントラドメインフェデレーションユーザの移行タスク

タスク	O = オプション M = 必須
ツールのダウンロード	M
Lync サブスクライバの通知画面の無効化	M
無制限の連絡先リスト サイズとウォッチャ サイズの設定	M
サブスクライバ要求の自動承認の有効化	M
ローカルの IM and Presence サービス ドメインが移行するユーザの Microsoft サーバのドメインに一致することを確認します。	M
該当する場合は、SIP URI フォーマットが変更された Microsoft サーバの IM and Presence サービス連絡先リストのコンタクト ID 名を変更します。	O
Cisco Unified Communications Manager の Microsoft サーバのユーザのプロビジョニング	M

タスク	<b>O = オプション</b> <b>M = 必須</b>
Microsoft サーバの連絡先リスト情報のバックアップ	M
ユーザの連絡先リストのエクスポート	M
Microsoft サーバのユーザの無効化	M
ユーザ アカウントが無効になっていることを確認します。	M
ユーザを移行するためのデータベースからのユーザデータの削除 (注) Microsoft サーバの配置によっては、複数のデータベースでこの手順を実行する必要があります。	M
IM and Presence サービスにユーザを移行するための連絡先リストのインポート	M
最大連絡先リストとウォッチャ サイズのリセット	M
Lync サブスクライバの通知画面の再有効化	M

#### 関連トピック

[ユーザの Microsoft サーバの連絡先リスト情報のバックアップ](#), (119 ページ)

[Lync を使用した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ワークフロー](#), (47 ページ)

[OCS を使用した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ワークフロー](#), (49 ページ)

[Microsoft サーバから IM and Presence サービスへのユーザの移行のための設定ワークフロー](#), (51 ページ)

[Microsoft Lync ポップアップの無効化](#), (113 ページ)

[リストアの Microsoft Lync のポップアップ動作](#), (113 ページ)

## アベイラビリティ

ここでは、アベイラビリティ機能について説明します。

### アベイラビリティの登録およびポリシー

ここでは、IM and Presence サービスおよび Microsoft Lync または Microsoft Office Communicator のコールフローについて説明します。

## IM and Presence サービス ユーザへのサブスクリプション

Microsoft Lync または Microsoft Office Communicator のユーザが IM and Presence サービス クライアントユーザの可用性を表示するには、SIP SUBSCRIBE 要求は Lync/OCS から IM and Presence サービスにルーティングします。IM and Presence サービスは着信登録を承認し、それを保留中にします。プライバシー ポリシーがこの着信登録要求に適用されます。



- (注) パーティションイントラドメインフェデレーション導入で Microsoft サーバのユーザからの登録に適用されたプライバシー ポリシーは、IM and Presence サービス クライアントユーザからの登録に適用されるプライバシー ポリシーと同じです。

IM and Presence サービスは自動認証が有効になっているかどうか、または IM and Presence サービス クライアントユーザが Microsoft サーバユーザのプレゼンス登録を以前にブロックしたまたは許可したかどうかを確認します。いずれかが true の場合、IM and Presence サービスは、登録要求のポリシー判断を自動で処理します。それ以外の場合は、IM and Presence クライアントユーザは、新規登録に関する警告を受信します。

登録が拒否される場合、Polite Blocking が実装されています。つまり、ユーザのプレゼンス状態が Microsoft サーバユーザにオフラインとして表示されています。登録が認証されると、IM and Presence サービスは可用性のアップデートを Microsoft サーバユーザに送信し、IM and Presence サービス クライアントユーザには Microsoft サーバユーザをその参加者に追加するオプションがあります。

## Microsoft Lync または Microsoft Office Communicator ユーザへのサブスクリプション

IM and Presence サービス クライアントユーザが Microsoft Lync または Microsoft Office Communicator のユーザの可用性を確認する場合は、SIP SUBSCRIBE 要求を IM and Presence サービスから Lync/OCS にルーティングします。Microsoft サーバは着信登録を承認します。ポリシーがこの着信登録要求に適用されます。

Microsoft サーバユーザがこの IM and Presence サーバユーザからのサブスクリプションをすでに承認している場合、登録は自動的に承認され、可用性は Microsoft サーバユーザによって適用されるポリシー レベルに合わせて IM and Presence サービス クライアントユーザに返されます。そうでない場合は、Microsoft サーバユーザは新しい登録に関する警告を受信します。Microsoft サーバユーザは、IM and Presence サービス クライアントユーザを承認またはブロックできます。



- (注) Microsoft サーバは約 1 時間 45 分ごとに SIP SUBSCRIBE の更新を実行します。したがって、IM and Presence サービス ノードが再起動すると、Microsoft Lync または Microsoft Office Communicator ユーザが IM and Presence サービス コンタクトの可用性ステータスなしでいられる最大時間はおよそ 2 時間です。

Microsoft サーバが再起動すると、IM and Presence サービス クライアントが Microsoft Lync または Microsoft Office Communicator コンタクトの可用性ステータスなしでいられる最大時間はおよそ 2 時間です。

## アベイラビリティ マッピング状態

次の表は、Microsoft Lync または Microsoft Office Communicator から次の IM and Presence 対応クライアントへのアベイラビリティ マッピング状態を示します。

- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for iPad
- モバイル向け Cisco Jabber IM (Cisco Jabber IM for iPhone、Android、Blackberry)
- Cisco Unified Personal Communicator リリース 8.x
- サードパーティ製の XMPP クライアント

表 5: Microsoft Lync または Microsoft Office Communicator からのアベイラビリティ マッピング状態

Microsoft Lync または Microsoft Office Communicator 設定	Cisco Jabber <sup>1</sup> 設定	Cisco Unified Personal Communicator 8.x の設定	サードパーティ製の XMPP クライアント 設定
応対可	応対可	応対可	応対可
退席中	退席中	退席中	退席中
すぐに戻ります	退席中	退席中	退席中
ビジー	ビジー	ビジー	ビジー
サイレント	ビジー	ビジー	ビジー
オフライン表示	オフライン	オフライン	オフライン
オフライン	オフライン	オフライン	オフライン

<sup>1</sup> サポートされているすべての Cisco Jabber クライアントに適用されます。

次の表に、サポートされているすべての Cisco Jabber クライアントから Microsoft Lync または Microsoft Office Communicator へのアベイラビリティ マッピング状態を示します。

表 6 : Cisco Unified Personal Communicator Release 8.x から Microsoft Lync または Microsoft Office Communicator へのアベイラビリティ マッピング状態

Cisco Unified Personal Communicator リリース 8.x 設定	Microsoft Lync または Microsoft Office Communicator 設定
応対可	応対可
ビジー	ビジー
電話中	ビジー
会議	ビジー
退席中	退席中
サイレント	ビジー
オフライン	オフライン
オフライン : 電話中	オフライン
オフライン : 会議	オフライン
オフライン : 外出中	オフライン

次の表に、Cisco Jabber から Microsoft Lync または Microsoft Office Communicator への可用性マッピング状態を示します。

表 7 : Cisco Jabber から Microsoft Lync または Microsoft Office Communicator へのアベイラビリティ マッピング状態

Cisco Jabber <sup>2</sup> 設定	Microsoft Lync または Microsoft Office Communicator 設定
応対可	応対可
退席中	退席中
サイレント	ビジー
不在	オフライン
オフライン	オフライン

- 2 サポートされているすべての Cisco Jabber クライアントに適用されます。

次の表はサードパーティ製の XMPP クライアントから Microsoft Lync または Microsoft Office Communicator へのアベイラビリティ マッピング状態を示します。

表 8: サードパーティ製の XMPP クライアントから **Microsoft Lync** または **Microsoft Office Communicator** へのアベイラビリティ マッピング状態

サードパーティ製 XMPP 設定	Microsoft Lync または Microsoft Office Communicator 設定
応対可	応対可
退席中	退席中
退席中 (延長)	退席中
サイレント	ビジー
オフライン	オフライン

## インスタントメッセージ

パーティションイントラドメイン フェデレーションでは、IM and Presence サービス クライアント ユーザと Microsoft Lync または Microsoft Office Communicator ユーザ間のポイントツーポイント IM をサポートしています。次のような IM 機能がサポートされています。

- プレーンテキスト IM フォーマット
- 入力指示
- 基本顔文字

SIP Session Mode IM を使用して、IM and Presence サービス と Microsoft サーバ間でメッセージおよび入力指示を転送します。

IM and Presence サービス クライアント ユーザが IM を Microsoft サーバ ユーザに送信すると、これらの 2 人のユーザ間で既存の IM セッションが確立されていない場合、IM and Presence サービスは SIP INVITE メッセージを Microsoft サーバに送信して、新しいセッションを確立します。このセッションは、これら 2 人のユーザいずれかからの以降の SIP MESSAGE または SIP INFO (入力指示) トラフィックに使用します。



- (注) IM and Presence サービス クライアント ユーザおよびサードパーティ製 XMPP クライアント ユーザは、アベイラビリティがなくても、Microsoft サーバユーザと IM カンバセーションを開始できます。

Microsoft ユーザが IM を IM and Presence サービス クライアント ユーザに送信すると、これらの 2 人のユーザ間で既存の IM セッションが確立されていない場合、Microsoft サーバは SIP INVITE メッセージを IM and Presence サービスに送信します。このセッションは、これら 2 人のユーザいづれかからの以降の SIP MESSAGE または SIP INFO (入力指示) トラフィックに使用します。



- (注) Microsoft サーバグループチャット機能独自の特性により、パーティションイントラドメインフェデレーションでは、IM and Presence サービス クライアント ユーザと Microsoft Lync または Microsoft Office Communicator ユーザ間のグループチャットはサポートされていません。

## 要求のルーティング

この項では、IM and Presence サービス から Lync/OCS、Lync/OCS から IM and Presence サービスへの要求のルーティングについて説明します。

### IM and Presence から Microsoft サーバへの要求のルーティング

IM and Presence サービスから Lync/OCS への基本的な接続を有効にするには、IM and Presence サービス ドメインに対して IM and Presence サービスで SIP スタティック ルートを設定する必要があります。これらのスタティック ルートは Microsoft サーバまたはフロント エンド ロード バランサ (Enterprise Edition Microsoft サーバのみ) の IP アドレスをポイントし、受信者が IM and Presence サービス ユーザでない場合に、IM and Presence サービスが要求を Microsoft サーバにルーティングできるようにします。トランスポート層セキュリティ (TLS) 暗号化をこれらのスタティック ルートで有効にできます。IM and Presence サービスから Microsoft サーバへの基本的な接続をサポートするには、着信アクセスコントロールリスト (ACL) のエントリを設定し、認証がなくても Microsoft サーバが IM and Presence サービス ノードにアクセスできるようにする必要があります。

この基本的な接続に重なるように、パーティションイントラドメインフェデレーションでは、IM and Presence サービスから Microsoft サーバへの要求のルーティングに対して、基本ルーティングおよび高度なルーティングという 2 種類のモードを提供しています。

### パーティションイントラドメインフェデレーションの基本的なルーティング モード

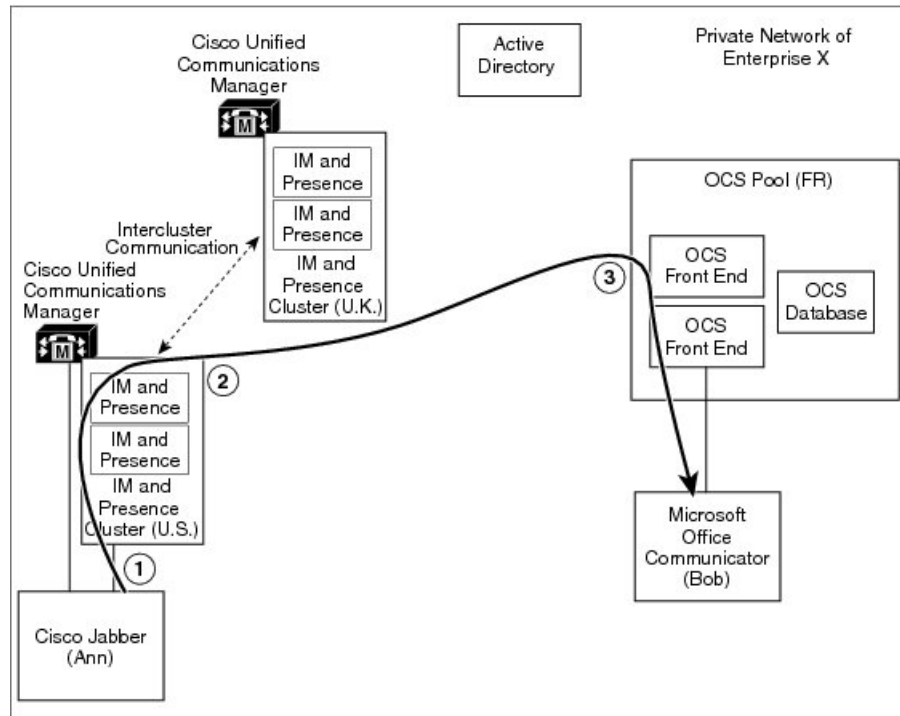
基本的なルーティングは、パーティションイントラドメインフェデレーションのデフォルトルーティングモードです。基本的なルーティングがイネーブルの場合、要求の受信者が IM and Presence



サービスクラスタ内の任意のドメイン内にあるものの、ライセンスされた IM and Presence サービスユーザでない場合に、IM and Presence サービスは要求を Lync/OCS にルーティングします。

次の図は、基本的なルーティングが設定されている場合の IM and Presence サービスから Microsoft サーバへのルーティング要求のシーケンスを示しています。この図は、OCS の配置例を示しますが、他のサポートされている Microsoft サーバにも適用されます。

図 5: Microsoft サーバの要求ルーティングへの IM and Presence サービス



1	Cisco Jabber 8.x ユーザの Ann は、同じプレゼンス ドメインの Microsoft Office Communicator ユーザである Bob に要求を送信します。
2	Bob はローカル ドメイン内にあるものの、ライセンスされた IM and Presence サービスクライアント ユーザではないため、IM and Presence サービスは要求を変換し、それを OCS にルーティングします。
3	OCS サーバは要求を Bob の Microsoft Office Communicator クライアントに転送します。



(注)

- IM and Presence サービスまたは Microsoft サーバのいずれかでプロビジョニングされていない受信者について、Microsoft サーバに転送される要求は、今度は Microsoft サーバにより IM and Presence サービスへ返されます。
- IM and Presence サービスは、この方法で Microsoft サーバからループバックする要求を拒否する組み込みループ検出を備えています。

## パーティションイントラドメイン フェデレーションの高度なルーティング モード

高度なルーティングにより IM and Presence サービス データベースに多数のプロビジョニングされていない、または不明な連絡先がある展開で、IM and Presence サービスおよび Lync/OCS 間のトラフィック量が少なくなります。ただし、高度なルーティングは IM and Presence サービス クラスタそれぞれにストレージオーバーヘッドを追加します。高度なルーティングのロジックを適用できるためには、すべての Microsoft Lync または Microsoft Office Communicator ユーザをクラスタごとに保存する必要があります。

単一クラスタの IM and Presence サービス配置と Cisco Unified Communications Manager が Microsoft サーバで使用される同じ Active Directory からユーザを同期する場合にだけパーティションイントラドメイン フェデレーションに高度なルーティングを設定します。複数 IM and Presence サービス クラスタが配置されている場合、デフォルトの基本ルーティング方式を使用する必要があります。

高度なルーティングに、Active Directory から同期されているユーザのリストには、すべての Microsoft Lync または Microsoft Office Communicator ユーザを含める必要があります。

高度なルーティングがイネーブルの場合、IM and Presence サービスは、次の両方の条件が満たされると Microsoft サーバに要求をルーティングします。

- 要求の受信者は IM and Presence サービス ドメイン内に存在するが、ライセンスされた IM and Presence サービス ユーザではない
- 要求の受信者は有効な Microsoft Lync または Microsoft Office Communicator SIP アドレスが IM and Presence サービス データベースに保存されている

## IM and Presence サービスの要求ルーティングへの Microsoft サーバ

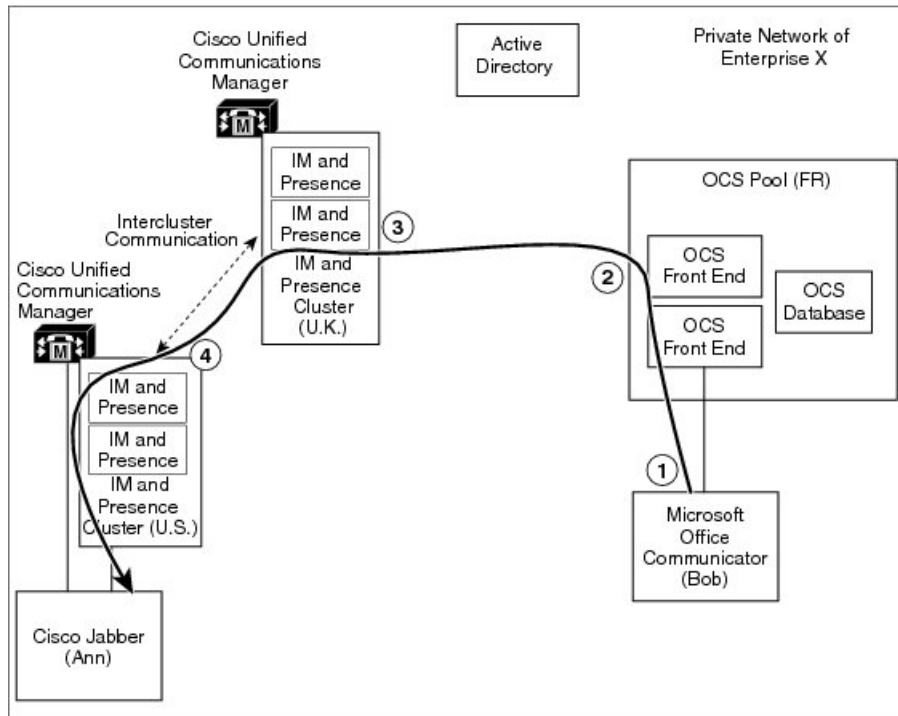
Lync/OCS から IM and Presence サービスへの基本的な接続を有効にするには、IM and Presence サービス クラスタに対して Microsoft サーバで SIP スタティック ルートを設定する必要があります。これらのスタティック ルートは、ルーティング IM and Presence サービス ノードとして指定されている IM and Presence サービス ノードの IP アドレスおよびポートをポイントします。これらによって Microsoft サーバは、受信者が Microsoft サーバでない場合に要求を IM and Presence サービスにルーティングできます。TLS 暗号化をこれらのスタティック ルートで有効にできます。

IM and Presence サービスから SIP 要求を承認するための認証要求が Microsoft サーバに出されないようにするため、Microsoft サーバの IM and Presence サービス ノードごとにホスト認証エントリも設定する必要があります。

すでに説明したように、スタティックルート設定に重なるように、パーティションイントラドメインフェデレーション導入では、Microsoft サーバにはルーティングモードは1つしかありません。Microsoft サーバは、要求の受信者が Microsoft サーバで管理されるいずれかの IM とアベイラビリティドメイン内にあり、Microsoft Lync または Microsoft Office Communicator のユーザではない場合、IM and Presence サービスに要求をルーティングします。

次の図は、Microsoft のサーバからの IM and Presence サービスへのルーティング要求のシーケンスを示しています。この図は、OCS の配置例を示しますが、他の Microsoft サーバ配置にも適用されます。

図 6 : IM and Presence サービスの要求ルーティングへの Microsoft サーバ



1	Microsoft Office Communicator ユーザの Bob は、Cisco Jabber ユーザである Ann に要求を送信します。	3	IM and Presence サービスは要求を承認し、Ann の自宅の IM and Presence サービス ノードに転送します。
2	Ann はローカルプレゼンスドメイン内でも Microsoft Office Communicator のユーザではないため、Microsoft サーバは IM and Presence サービスに要求をルーティングします。	4	IM and Presence サービスは要求を変換し、Ann の Cisco Jabber クライアントに転送します。



- (注) IM and Presence サービスまたは Microsoft サーバのいずれかでプロビジョニングされていない受信者について、Microsoft サーバで IM and Presence サービスに転送される要求は、IM and Presence サービスにより拒否されます。

## クラスタ間展開とマルチノード展開

クラスタ間およびマルチノードクラスタ IM and Presence サービス展開では、アベイラビリティの登録または IM 会話を行う場合、Lync/OCS サーバはすべての SIP メッセージを、ルーティング目的で指定された IM and Presence サービス ノードにルーティングします。IM and Presence サービス ルーティング ノードで受信ユーザがホストされていない場合、メッセージは展開内の適切な IM and Presence サービス ノードにルーティングされます。システムは、ルーティング IM and Presence サービス ノードを介して、この要求に関連付けられたすべての応答をルーティングします。

アベイラビリティの登録または IM 会話を行う場合、どの IM and Presence サービス ノードも SIP メッセージを直接 Microsoft サーバに送信できます。Microsoft サーバがこれらのメッセージに返信すると、返信は、メッセージを開始した IM and Presence サービス ノードに直接送信されます。

## ドメイン間フェデレーション

IM and Presence サービスでは、ドメイン間フェデレーションがサポートされています。この機能は、IM and Presence サービスがパーティションイントラドメインフェデレーションに設定されている場合も使用できます。ただし、IM and Presence サービスで設定されているどのドメイン間フェデレーションも IM and Presence サービス クライアント ユーザ以外には使用できません。

Lync/OCS 展開がすでに Access Edge/Access Proxy サーバを介して SIP ドメイン間フェデレーションに設定されている場合、Microsoft Office Communicator ユーザはこのフェデレーション機能を継続して使用できます。IM and Presence サービス クライアント ユーザがそうした既存のフェデレーション機能を活用できるように、IM and Presence サービス および Microsoft サーバを設定することもできます。



- (注)
- IM and Presence サービスと Microsoft サーバ両方を設定して、同じリモートドメインで直接フェデレーションすることはサポートされていません。
  - IM and Presence サービス ドメイン間フェデレーションの詳細については、マニュアル『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

### 関連トピック

[Microsoft サーバのドメイン間フェデレーション機能の IM and Presence サービスの統合、\(135 ページ\)](#)

[『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』](#)

# ドメイン内フェデレーションのハイ アベイラビリティ

パーティションイントラドメイン フェデレーションは、IM and Presence サービスと Lync/OCS 間の要求のルーティングについて、ハイ アベイラビリティをサポートします。

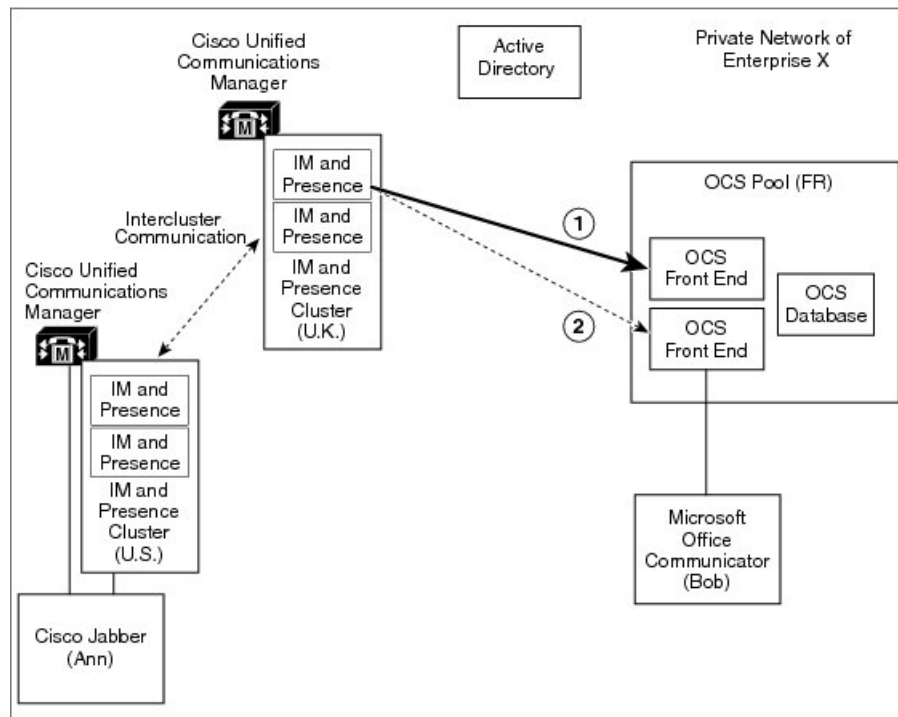
## Microsoft サーバ要求ルーティングへの IM and Presence サービスのハイアベイラビリティ

前述したように、SIP スタティック ルートを IM and Presence サービスで設定して、IM and Presence サービスおよび Lync/OCS 間のイントラドメイン フェデレーションの基本的な接続を有効にする必要があります。

Microsoft サーバとの統合においてハイ アベイラビリティを実現するため、IM and Presence サービスでアドレス パターンごとに複数の SIP スタティック ルートを設定できます。

必要に応じて、これらのスタティック ルートにプライオリティ値を割り当て、プライマリとバックアップのスタティック ルートを定義できます。プライオリティが最も高いルートが最初に試行されます。これらのルートが使用できない場合、次の図に示すように、要求はバックアップルートを使用して再送信されます。この図は、OCS の配置例を示しますが、他のサポートされている Microsoft サーバにも適用されます。

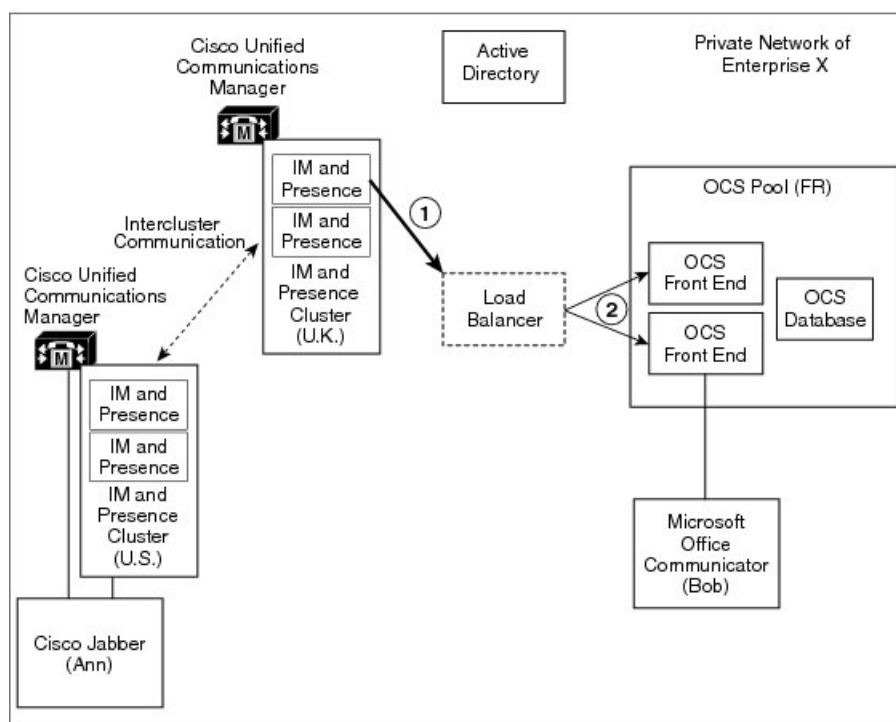
図 7: Microsoft サーバ要求ルーティングへの IM and Presence サービスのハイアベイラビリティ



1 Microsoft サーバにルーティングする場合、IM and Presence サービスは、プライオリティが最も高いスタティックルートを見つけ、要求をそのルートに設定されたネクストホップアドレスに送信しようとします。	2 そのネクストホップが使用できない場合、IM and Presence サービスはプライオリティが次に高いスタティックルートにフォールバックし、要求を関連するネクストホップアドレスに送信しようとします。
---	--

Enterprise Edition Microsoft サーバの場合、フロントエンドロードバランサを展開できます。その場合、SIP スタティックルートに IM and Presence に設定して、Microsoft サーバのフロントエンドロードバランサの IP アドレスをポイントできます。フロントエンドロードバランサは、次の図に示すようにその関連付けられた Microsoft サーバプール内でハイアベイラビリティを実現します。この図は、OCS の配置例を示しますが、他の Microsoft サーバにも適用されます。

図 8: ロードバランサによる IM and Presence から Microsoft サーバへの要求のルーティングのハイアベイラビリティ



1 Microsoft サーバにルーティングする場合、IM and Presence サービスは OCS のフロントエンドロードバランサをポイントするスタティックルートを見つけます。	2 Microsoft サーバのフロントエンドロードバランサは、プール内のアクティブなフロントエンドサーバのいずれかにルーティングします。
---	---

認定されたロードバランサのリストについては次の URL を参照してください。 <http://technet.microsoft.com/en-us/office/ocs/cc843611> ロードバランサを導入し、正しく管理するのはお客様の責任です。



- (注) シスコでは、ロード バランサをポイントするスタティック ルートの設定はサポートしていません。フロントエンドロードバランサをバイパスするためのスタティック ルートを設定することをお勧めします。

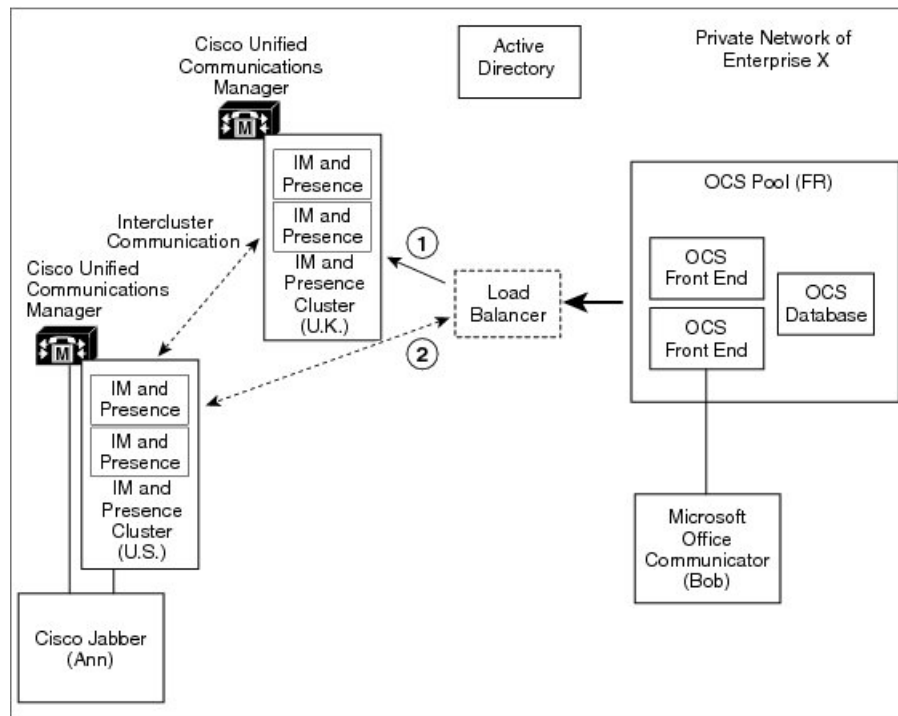
## Microsoft サーバから IM and Presence サービスへの要求のルーティングのハイ アベイラビリティ

SIP スタティック ルートを Lync/OCS で設定して、Microsoft サーバおよび IM and Presence サービス間のドメイン内フェデレーションの基本的な接続を有効にする必要があります。

ただし、Microsoft サーバはドメインごとに 1 つの SIP スタティック ルートの設定だけをサポートしているため、スタティック ルートは単一の IM and Presence サービス ノードのみポイントできることを意味します。

従って、IM and Presence サービスを Microsoft サーバと統合する場合にハイ アベイラビリティを実現するには、次の図に示すように、IM and Presence サービス ノードと Microsoft のサーバの間にロードバランサを組み込む必要があります。この図は、OCS の配置例を示しますが、他の Microsoft サーバにも適用されます。

図 9 : Microsoft サーバから IM and Presence サービスへの要求のルーティングのハイ アベイラビリティ



1	ロードバランサは、アクティブ/バックアップモードで動作します。プライマリ IM and Presence サービスノードに対してそのサーバの実行中に要求がルーティングされ、ハートビート信号を使用して IM and Presence サービスノードがアライブかどうか確認します。	2	IM and Presence サービスが失敗すると、ロードバランサにより、以降のすべての要求がバックアップ IM and Presence サービスサーバにルーティングされます。
---	--	---	--

## 連絡先の検索

パーティションイントラドメインフェデレーションでは、IM and Presence サービス対応クライアントと Microsoft Lync または Microsoft Office Communicator の両方で全検索機能を実現しています。

IM and Presence サービス対応クライアントによる Active Directory (AD) 検索は、ユーザがプロビジョニングされた場所に関係なく、ユーザを返します。Microsoft サーバアドレス帳検索は引き続き、すべての Microsoft サーバユーザ、および IM and Presence サービスに移行したあらゆる IM and Presence サービスクライアントユーザを返します。

連絡先カード情報は、すべての連絡先について両方のクライアントで使用できます。



(注) IM and Presence サービスクライアントユーザが Microsoft のサーバでプロビジョニングされていなかった場合は、該当ユーザの [msRTC SIP-PrimaryUserAddress] フィールドに対して Active Directory のアップデートを実行し、ユーザが Microsoft のサーバ検索を使用できるようにする必要があります。

## ユーザの移行

ユーザ移行の管理フローは大まかに次のようになります。

- 1 移行するユーザの Lync/OCS SIP URI 形式を確認します。
- 2 必要に応じて、IM and Presence サービスの連絡先のコンタクト ID の名前を変更します。
- 3 Microsoft サーバユーザを IM and Presence サービスに移行するライセンスを取得して割り当てます。
- 4 移行する Microsoft サーバユーザ用の Microsoft サーバデータをバックアップします。
- 5 移行する Microsoft サーバユーザごとに Microsoft サーバの連絡先リストをエクスポートします。
- 6 移行する Microsoft サーバユーザの Microsoft サーバのユーザアカウントをディセーブルにします。
- 7 移行する Microsoft サーバユーザの Microsoft サーバのユーザデータを削除します。



- 8 Microsoft サーバの連絡先リストを移行したユーザの IM and Presence サービス データベースにインポートします。
- 9 移行したユーザのデスクトップで IM and Presence サービス対応クライアントを展開します。

管理者向けの移行プロセスをさらに支援するため、この機能では数多くのツールが使用できます。パーティションイントラドメインフェデレーション導入の主な利点の1つに、企業内で Microsoft サーバから IM and Presence サービスへシームレスに遷移できる点があります。パーティションイントラドメインフェデレーションには、次のような利点があります。

- IM and Presence サービス クライアント ユーザ、Microsoft Lync または Microsoft Office Communicator のユーザは、同じプレゼンス ドメインを共有します。
- ユーザは、その共有ドメイン内でアベイラビリティおよびインスタントメッセージを交換できます。
- ユーザまたは連絡先がプロビジョニングされている場所に関係なく、ユーザは連絡先を検索し、追加できます。
- IM and Presence サービス IM アドレスはユーザの ID が移行中も維持されるように Lync SIP URI (msRTCSIP-PrimaryUserAddress) と一致するように設定できます。

IM アドレスおよびユーザの移行の設定に関する詳細情報については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

## IM アドレスの例

次の表は、IM and Presence サービスで使用可能な IM アドレス オプションの例を示しています。

<b>IM and Presence Service Default Domain:</b> cisco.com		
<b>User:</b> John Smith		
<b>Userid:</b> js12345		
<b>Mailid:</b> jsmith@cisco-sales.com		
<b>SIPURI:</b> john.smith@webex.com		
IM アドレス形式	ディレクトリ URI マッピング	IM アドレス (IM Address)
<userid>@<domain>	適用対象外	js12345@cisco.com
Directory URI	mailid	jsmith@cisco-sales.com
Directory URI	msRTCSIP-PrimaryUserAddress	john.smith@webex.com

IM アドレスの設定の詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

## ユーザ移行ツール

IM and Presence サービスは、次の Lync/OCS ユーザ移行手順に対するツールを提供しています。

- 移行する Microsoft サーバユーザごとに Microsoft サーバの連絡先リストをエクスポートします。
- 移行する Microsoft サーバユーザの Microsoft サーバのユーザアカウントをディセーブルにします。
- 移行する Microsoft サーバユーザの Microsoft サーバのユーザデータを削除します。
- Microsoft サーバの連絡先リストを移行したユーザの IM and Presence サービスデータベースにインポートします。
- IM and Presence サービスデータベースの移行されたユーザのコンタクト ID の名前を変更します。



(注)

- ユーザ移行ツールのいずれかを実行しようとする時、「アプリケーションが正常な初期化に失敗しました (Application failed to initialize properly)」というエラーが表示される場合があります。このエラーの原因は、.NET 4.0 フレームワークのインストールされていないユーザ移行ツールを実行しようとしていることです。シスコが提供する各ユーザ移行ツールを使用するには、.NET Framework の少なくともバージョン 2.0 が、そのツールを実行している場所からサーバにインストールされている必要があります。

NET 2.0 フレームワークは、Windows Server 2003 R2 以降で標準としてインストールされています。

- エクスポート、ディセーブル化および削除ツールは、[cisco.com](http://cisco.com) で zip ファイルで提供されます。インポートツールは **Cisco Unified CM IM and Presence Administration** のユーザインターフェースを使用してアクセスできます。

**移行する Microsoft サーバユーザごとに Microsoft サーバの連絡先リストをエクスポートします。**

この IM and Presence サービスツールは、Microsoft サーバからの連絡先リストの一括エクスポートを可能にします。エクスポートされた連絡先リストは、IM and Presence サービスの Contact List Import Bulk Administration Tool (BAT) で承認できるカンマ区切り値 (CSV) ファイルに書き込まれます。これらのツールを組み合わせ、連絡先リストを一括管理して、エンドツーエンドで移行できます。

**Microsoft サーバユーザを移行するための Microsoft サーバのユーザアカウントをディセーブルにします。**

IM and Presence サービスには、Microsoft サーバのユーザアカウントを一括して無効にするツールが入っています。このツールは、Active Directory に接続し、必要に応じてユーザの Microsoft サーバに固有な属性を変更することで、Microsoft サーバアカウントを無効にします。

### OCS ユーザを移行するための Microsoft サーバのユーザ データを削除する

Microsoft サーバユーザは、Microsoft サーバから削除し、Microsoft サーバからの IM and Presence サービスへのパーティションイントラドメイン フェデレーションルーティングを可能にする必要があります。ただし、ユーザが Microsoft サーバから削除されると、Microsoft Lync または Microsoft Office Communicator 内のユーザの連絡先リストからも削除されます。この IM and Presence サービスツールは Microsoft サーバユーザのデータを一括して削除すると同時に、ユーザが Microsoft Office Communicator ユーザの連絡先リストから削除されないようにします。

**Microsoft サーバの連絡先リストを移行したユーザの IM and Presence サービス データベースにインポートします。**

IM and Presence サービス BAT 一括サポート連絡先リストのインポート。この一括インポートの入力として CSV ファイルを取得します。Microsoft サーバのエクスポートの連絡先リストのツールとともに使用すると、Microsoft サーバから IM and Presence サービスに連絡先リストを移動できます。

**IM and Presence サービス データベースで移行されたユーザのコンタクト ID の名前を変更します。**



(注) この移行ツールは、IM and Presence サービスの IM アドレス形式が Microsoft サーバと異なる場合にのみ必要です。IM and Presence サービス リリース 10.0 から、IM and Presence サービスを構成することが可能になり、2つのシステム間の IM アドレス形式に不一致がないことを確実にします。

IM and Presence サービス BAT は、SIP URI 形式が IM and Presence サービスと Microsoft のサーバとで異なる場合の移行をサポートしています。IM and Presence サービスの以前のリリースでは、ユーザの最初のバッチを移行する前に、IM and Presence サービス SIP URI 形式に一致させるために、移行するすべての Microsoft サーバユーザの SIP URI を変更する必要があります。このリリースでは、Microsoft サーバから IM and Presence サービスにユーザの各バッチを移行する直前に、移行するユーザの SIP URI を変更できます。Bulk Administration Tool は入力として移行されたユーザのリストがある CSV ファイルを取得し、移行されたユーザを連絡先として持つすべてのユーザの連絡先リストを更新します。



(注) ユーザの移行ツールを実行しても、Microsoft Lync または Microsoft Office Communicator に署名された他の Microsoft サーバユーザ機能への影響はありません。ただし、あらかじめスケジュールされたメンテナンスの時間帯にユーザ移行ツールを実行して Microsoft サーバおよび Active Directory システムの負荷を減らすことをお勧めします。





## 第 2 章

### 統合の計画

---

- サポート対象のパーティションイントラドメインフェデレーションの統合, 27 ページ
- ハードウェア要件, 29 ページ
- ソフトウェア要件, 30 ページ
- 統合の準備, 32 ページ
- IM and Presence サービスの前提条件の設定, 34 ページ
- IM and Presence サービス ノードのルーティングの追加構成, 34 ページ
- IM and Presence サービス機能サービスの開始, 35 ページ
- オフピーク期間中のサービス再起動の計画, 36 ページ

## サポート対象のパーティションイントラドメインフェデレーションの統合

Microsoft Lync を持つパーティションイントラドメインフェデレーション TLS を設定する必要があります。TCP はサポートされません。詳細については、「パーティションイントラドメインフェデレーション用 *Microsoft Lync* の設定」の章を参照してください。

この章では、IM and Presence サービスと Microsoft Lync/OCS との間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イネーブルにするための設定手順について説明します。次の Microsoft サーバプラットフォームがサポートされます。

- Microsoft Lync Server 2010、Standard Edition および Enterprise Edition
- Microsoft Lync Server 2013、Standard Edition および Enterprise Edition
- Microsoft Office Communications Server 2007 リリース 2、Standard Edition および Enterprise Edition

IM and Presence サービスは、パーティションイントラドメインフェデレーションの ASA をサポートしません。



(注) Lync および OCS サーバ両方の混合配置がある場合、Lync ユーザのユーザ移行ツールを実行してから、OCS ユーザのユーザ移行ツールを実行する必要があります。

#### 関連トピック

[ハードウェア要件](#), (29 ページ)

[ソフトウェア要件](#), (30 ページ)

## Presence Web Service の API サポート

オープン インターフェイスである Presence Web Service を使用すると、クライアントアプリケーションはユーザ プレゼンス情報を IM and Presence サービスと共有できます。サードパーティ開発者は、このインターフェイスを使用して、ユーザのプレゼンス状態に関する更新を送信および取得するクライアントアプリケーションを構築できます。Presence Web Service の API サポートについて、次の制限事項に注意してください。

- パーティションイントラドメインフェデレーションでは、Presence Web Service の API を使用してシスコ以外のクライアントからプレゼンス情報を取得することはできません。

Presence Web Service の詳細については、<https://developer.cisco.com/site/collaboration/call-control/unified-presence/documentation/index.gsp>の『*IM and Presence Service Developer Guide*』を参照してください。

## Microsoft Lync の統合に関する制約事項

パーティションイントラドメインフェデレーションを追加することで既存の Microsoft Lync の統合が破損するシナリオは2つあります。

- すでに Cisco VCS または Cisco Expressway でビデオ用にイントラドメインフェデレーションを設定している状態で、IM and Presence サービス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追加する場合：Microsoft Lync は、Cisco VCS または Cisco Expressway と統合され、ローカル Lync プレゼンスドメインのビデオと音声のトラフィックを Cisco VCS または Cisco Expressway にルーティングするスタティックルートが Lync で設定されます。IM and Presence サービス（パーティションイントラドメインフェデレーションの要件）をポイントするようにスタティックルートを変更すると、Cisco VCS または Cisco Expressway のためのトラフィックが代わりに IM and Presence サービスにルーティングされるため、既存のビデオ統合が破損します。IM and Presence サービスにビデオ統合とパーティションイントラドメインフェデレーションの両方を含めることはできません。
- すでに Microsoft Exchange のユニファイドメッセージングとの統合を設定している状態で、IM and Presence サービス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追加す

る場合：Microsoft Lync サーバが、Microsoft Exchange へのユニファイドメッセージング用に設定されます（オンプレミスまたはクラウド（Office365）向け）。ローカル Lync プレゼンスドメイン用に Lync からのスタティック ルートを追加し、IM and Presence サービス（パーティションイントラドメインフェデレーションの要件）をポイントすると、ドメイン用のすべてのユニファイドメッセージング SIP トラフィックが IM and Presence サービスにルーティングされるため、ドメイン用の Lync と Microsoft Exchange の間のユニファイドメッセージングの統合が中止されます。IM and Presence サービスに、Microsoft Exchange のユニファイドメッセージングへの統合とパーティションイントラドメインフェデレーションの両方を含めることはできません。



(注) 同じドメインを共有している場合、Microsoft Lync と IM and Presence サービスで Microsoft Exchange のユニファイドメッセージングと Cisco VCS（または Cisco Expressway）のいずれとの統合も、パーティションイントラドメインフェデレーションでサポートされません。

## ハードウェア要件

IM and Presence サービス と Lync/OCS 間のパーティションイントラドメインフェデレーションでは、次に示すシスコハードウェアが必要です。

- IM and Presence サービス ノード。IM and Presence サービス ハードウェア サポートについては、IM and Presence サービス 互換性マトリクスを参照してください。
- Cisco Unified Communications Manager のノード。Cisco Unified Communications Manager のハードウェア サポートについては、Cisco.com で入手できる Cisco Unified Communications Manager のマニュアルの互換性情報を参照してください。



(注) リリース 10.0(1) 以降では、シスコは Cisco Unified Communications Manager（Unified Communications Manager）や Cisco Unified Computing System サーバ上か、シスコ認定サードパーティサーバ設定の IM and Presence サービス展開のみを仮想化します。リリース 10.0(1) 以降では、シスコは Cisco Unified Communications Manager または Cisco Media Convergence Server サーバの IM and Presence サービス導入をサポートしません。

仮想化環境での Cisco Unified Communications Manager または IM and Presence サービスの詳細については、[http://docwiki.cisco.com/wiki/Unified\\_Communications\\_in\\_a\\_Virtualized\\_Environment](http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment) を参照してください。

### 関連トピック

『[Compatibility Information for IM and Presence Service and Cisco Unified Communications Manager](#)』ソフトウェア要件、(30 ページ)

# ソフトウェア要件

次の項では、IM and Presence サービスと Lync/OCS 間のパーティションイントラドメイン フェデレーションに必要なソフトウェアについて説明しています。

## サーバソフトウェア

パーティションイントラドメイン フェデレーションには、次に示すサーバソフトウェアが必要です。

### シスコソフトウェア

- IM and Presence サービス
- Cisco Unified Communications Manager

### Microsoft ソフトウェア

- 展開に応じて、次のいずれかになります。
  - Microsoft Lync Server 2010、Standard Edition または Enterprise Edition
  - Microsoft Lync Server 2013、Standard Edition または Enterprise Edition
  - Microsoft Office Communications Server 2007 リリース 2、Standard または Enterprise Edition
- 展開に応じて、次のいずれかになります。
  - Lync の管理ツール (Lync のインストール中にオプションのインストール項目が入手可能)
  - OCS 管理ツール (OCS のインストール中にオプションのインストール項目が入手可能)
- Microsoft Active Directory

### その他のソフトウェア

シスコが提供する各ユーザ移行ツールを使用するには、.NET Framework の少なくともバージョン 2.0 が、そのツールを実行している場所からサーバにインストールされている必要があります。ユーザ移行ツールのいずれかを実行しようとする、と、「アプリケーションが正常な初期化に失敗しました (Application failed to initialize properly)」というエラーが表示される場合があります。このエラーの原因は、.NET 2.0 以降のフレームワークのインストールされていないユーザ移行ツールを実行しようとしていることです。

NET 2.0 フレームワークは、Windows Server 2003 R2 以降で標準としてインストールされています。



## クライアントソフトウェア

IM and Presence サービスおよび Lync/OCS 間のパーティションイントラドメイン フェデレーション導入に必要なクライアントソフトウェアは、ご使用の導入によって異なります。パーティションイントラドメインフェデレーション導入では、IM and Presence サービス対応クライアントを任意に組み合わせることができます。

### IM and Presence サービス対応クライアント

次の IM and Presence サービス クライアントは IM and Presence サービスおよび Lync/OCS 間のパーティションイントラドメインフェデレーション導入でサポートされます。

#### シスコ ソフトウェア

- Cisco Unified Personal Communicator リリース 8.5
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- モバイル向け Cisco Jabber IM (Cisco Jabber IM for iPhone、Android、Blackberry)
- Cisco Jabber for iPad
- Cisco Jabber for Cius



(注) すべての Cisco Jabber クライアントのバージョンの互換性については、該当する Cisco Jabber クライアントのマニュアルを参照してください。

ディレクトリ URIIM アドレススキームを展開で使用する場合は、クライアントソフトウェアはディレクトリ URI をサポートする必要があります。

#### サードパーティ製ソフトウェア

サードパーティ製の XMPP クライアント

### Microsoft サーバ対応クライアント

導入に応じて、次に示すクライアントがサポートされます。

- Microsoft Lync 2010
- Microsoft Lync 2013
- Microsoft Office Communicator 2005
- Microsoft Office Communicator 2007 リリース 2
- Communicator Web Access 2005

- Communicator Web Access 2007 リリース 2

## 関連項目

ハードウェア要件, (29 ページ)

# 統合の準備

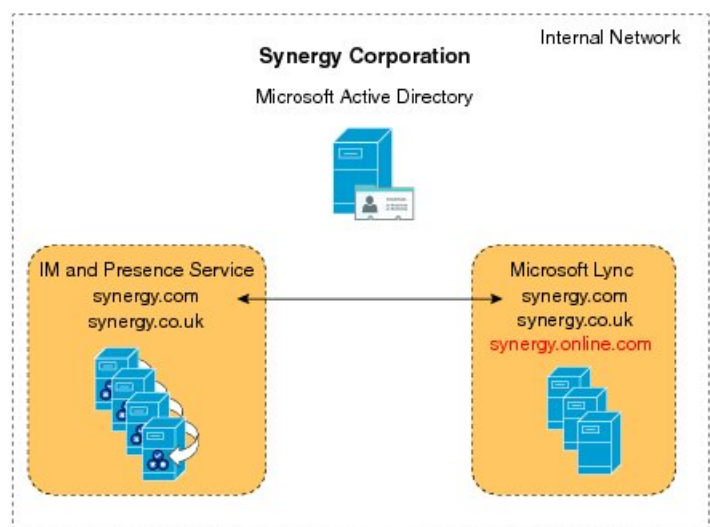
IM and Presence サービスおよび Lync/OCS 間のパーティションイントラドメイン フェデレーションの設定は、慎重に計画することが大切です。この統合の設定を開始する前に、この項に記載の項目をお読みください。

## プレゼンス ドメイン

パーティションイントラドメインフェデレーションは、その特性上、両方のシステム上で設定される共通プレゼンス ドメイン内で IM and Presence サービス および Microsoft サーバ間の統合をサポートします。IM and Presence サービスと Microsoft サーバの両方が、複数ドメインの設定をサポートします。ただし、一致する IM and Presence サービス ドメインに対して設定されていない Microsoft Lync または Microsoft Office Communicator のユーザはパーティションイントラドメインフェデレーションの通信に参加できません。

たとえば、次の図では、synergy.online.com ドメインが IM and Presence サービスで設定されていないため、synergy.online.com ドメインに設定されているユーザは、synergy.com と synergy.co.uk ドメインに設定されている IM and Presence サービス ユーザと IM 可用性や電子メールを共有できません。ユーザがイントラドメインフェデレーションの他のユーザと可用性を共有する前に、IM and Presence サービスに synergy.online.com ドメインを追加する必要があります。

図 10: 複数のドメインを持つパーティションイントラドメインフェデレーション



## ユーザの移行

ユーザが、この統合の一環として Lync/OCS から IM and Presence サービスに移行中の場合、次の点を考慮します。

この統合の一環としてユーザが Lync/OCS から IM and Presence サービスに移行中の場合は、Directory URI IM アドレススキームが設定されるときに、IM and Presence サービスがユーザの Microsoft サーバ ID を維持する点に留意してください。その後、アドレススキームは Lync SIP URI にマッピングされる場合があります。



(注) Directories URI IM アドレススキームを使用するには、すべてのクライアントの IM and Presence サービス クラスタは Directories URI をサポートする必要があります。

ユーザ移行計画の詳細については、ユーザ移行計画に関連するトピックを参照してください。

## DNS の設定

ドメイン ネーム システム (DNS) の “A” レコードは、すべての IM and Presence サービスおよび Lync/OCS サーバについて、企業内で公開する必要があります。

Microsoft サーバは、すべての IM and Presence サービス ノードの完全修飾ドメイン名 (FQDN) および IP アドレスを解決できなければなりません。

同様に、IM and Presence サービス ノードは、すべての Microsoft サーバおよびプール FQDN の FQDN および IP アドレスを解決できなければなりません。

## 認証権限サーバ

このパーティションイントラドメイン フェデレーションの一環として TLS 暗号化が有効になっている場合、外部または内部の認証局 (CA) を使用して、IM and Presence サービスおよび Lync/OCS のセキュリティ証明書に署名できます。同じ CA を使用して Microsoft サーバおよび IM and Presence サービス証明書に署名することを推奨します。そうでない場合、ルート証明書を CA ごとに Microsoft サーバおよび IM and Presence サービス ノードにアップロードする必要があります。

## 高可用性

パーティションイントラドメインフェデレーション導入で、どのようにしてアベイラビリティを設定するか考える必要があります。

IM and Presence サービス パーティションイントラドメイン フェデレーション機能を高度に利用可能にする場合、指定の (ルーティング) IM and Presence サービス ノードの前にロードバランサを展開できます。



(注) ロードバランシングを導入するには (ラウンドロビンなど)、ハードウェアロードバランサをインストールする必要があります。IM and Presence サービスでロードバランサをポイントするスタティックルートを作成します。

#### 関連項目

[ドメイン内フェデレーションのハイアベイラビリティ](#), (19 ページ)

## IM and Presence サービスの前提条件の設定

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を開始する前に、IM and Presence サービスで次のタスクを実行する必要があります。

- 1 IM and Presence サービスをインストールし、設定します。
- 2 IM and Presence サービスシステムが正しく動作しているか、次に示す点を確認します。
  - IM and Presence サービスシステム設定トラブルシュータを実行します。
  - ローカルな連絡先を IM and Presence サービスの Jabber クライアント追加できることを確認します。
  - クライアントが IM and Presence サービスノードからアベイラビリティステータスを受信していることを確認します。

## IM and Presence サービスノードのルーティングの追加構成

マルチサーバ構成では、IM and Presence サービスノードは IM and Presence サービスのルーティングノードとして専用にする必要があります。つまり、このサーバは Lync/OCS からすべての新しい着信 SIP 要求を受け取り、要求の受信者がホームとしている IM and Presence サービスノードにルーティングするフロントエンドサーバになります。

ユーザは一切ルーティング IM and Presence サービスノードに割り当てないことをお勧めします。これによりルーティング IM and Presence サービスノードは、Microsoft からの大量の SIP トラフィックを処理する能力を備えることができます。

ルーティング IM and Presence サービスノードにはユーザは割り当てられないため、多数の機能サービスを非アクティブ化して、ルーティング IM and Presence サービスノード上のリソースを解放できます。ルーティング IM and Presence サービスノードでの機能サービスの非アクティブ化

- Cisco Presence Engine
- Cisco XCP Text Conference Manager

- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP XMPP Federation Connection Manager
- Cisco XCP Message Archiver
- Cisco XCP Directory Service
- Cisco XCP Authentication Service

#### 関連項目

[ルーティング IM and Presence サービス ノードでの機能サービスの非アクティブ化](#), (66 ページ)

## IM and Presence サービス機能サービスの開始

パーティションイントラドメインフェデレーションをサポートするには、次のサービスが IM and Presence サービス ノードごとに実行されている必要があります。

- Cisco SIP Proxy
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP Router

Cisco XCP Router はネットワーク サービスであるため、デフォルトで開始されます。Cisco SIP Proxy および Cisco XCP SIP Federation Connection Manager は、開始しなければならない機能サービスです。

次の手順では、Cisco SIP Proxy および Cisco XCP SIP Federation Connection Manager 機能サービスを開始する方法について説明します。すべての IM and Presence サービス ノードでこの手順を実行する必要があります。



(注) 専用ルーティング IM and Presence サービス ノードについては、Cisco XCP SIP Federation Connection Manager サービスをアクティブにしないでください。専用ルーティング IM and Presence サービス ノードにはユーザは割り当てられていないためです。

#### 手順

- ステップ 1** [Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール (Tools) ] > [サービス アクティベーション (Service Activation) ] を選択します。
- ステップ 2** [サーバ (Server) ] メニューで IM and Presence サービス ノードを選択します。
- ステップ 3** 次のサービスを確認します。
  - a) Cisco SIP Proxy

b) Cisco XCP SIP Federation Connection Manager

**ステップ 4** [保存 (Save) ] をクリックします。

---

## オフピーク期間中のサービス再起動の計画

統合プロセス中に、Lync/OCS サーバフロントエンドサービスを再起動する必要があります。ユーザへの影響を最小限に抑えるため、メンテナンス時間帯などのオフピーク期間中にサービスの再起動を実行するように計画します。詳細は、パーティションイントラドメインフェデレーション設定ワークフローと、サーバのタイプに応じたサービスの再起動に関連するトピックを参照してください。



## 第 3 章

# ユーザの移行計画

- [移行中のユーザ ID の保守, 37 ページ](#)
- [詳細なユーザ移行計画, 41 ページ](#)
- [ユーザ移行ツールの時間に関するガイドライン, 43 ページ](#)

## 移行中のユーザ ID の保守

Lync/OCS から IM and Presence サービスへの移行時には、Microsoft Lync および Microsoft Office Communicator のユーザは同じ ID（URI：ユニフォームリソース ID）を維持する必要があります。移行中に同じ ID を保守する場合、次のような利点があります。

- ユーザの ID が変わらないため、ユーザのアベイラビリティ状態は維持され、既存のフォロワーに継続的にモニタリングされます。
- また、ユーザの連絡先リストを Microsoft サーバから IM and Presence サービスに直接インポートできるため、ユーザの連絡先リストをより単純に移行できます。

IM and Presence サービスの URI は、Cisco Unified Communications Manager のユーザ ID と IM and Presence サービス ドメインを次のように結合して構成されます。

<userid>@<domain>

ユーザが Cisco Unified Communications Manager ユーザ インターフェイスまたは Cisco Unified Communications Manager Bulk Administration Tool (BAT) を通して手作業で追加されている場合、ユーザ作成時に指定したユーザ ID がユーザの Microsoft サーバ URI のユーザ部分と一致していることを確認する必要があります。たとえば、Microsoft ユーザの URI が bobjones@foo.com の場合、bobjones というユーザ ID で CUCM ユーザを作成する必要があります。

Cisco Unified Communications Manager が Active Directory からのユーザと同期するよう設定されている場合、Cisco Unified Communications Manager のユーザ ID へのマッピングに使用する [Active Directory] フィールドが Microsoft サーバの URI のユーザ部分と一致していることを確認する必要があります。次の点に注意してください。

- Cisco Unified Communications Manager は、限定された数の [Active Directory] フィールドの userID とマッピングします。ほとんどの場合、ID は sAMAccountName です。
- Cisco Unified Communications Manager が userID を sAMAccountName にマッピングする場合、移行ユーザの Microsoft サーバの URI も <sAMAccountName>@<domain> というフォーマットに一致する必要があります。
- Bob Jones の sAMAccountName が bjones の場合、Microsoft サーバの URI は bjones@cisco.com でなければなりません。
- Microsoft のサーバの URI がどれも <sAMAccountName>@<domain> フォーマットに一致しない場合、IM and Presence サービスにそのバッチを移行する前に、Microsoft Server ユーザの各バッチの URI を変更できます。

## 移行前のタスク

Lync/OCSSIP URI が IM and Presence サービス URI 形式の <userid>@<domain> に一致しない場合、段階的にユーザを移行する Microsoft Server URI を変更できます。以前のリリースでは、移行プロセスを開始する前にすべての移行ユーザの URI を変更しなければなりませんでした。このリリースでは、バッチを移行する直前にユーザの各バッチの URI を変更できます。

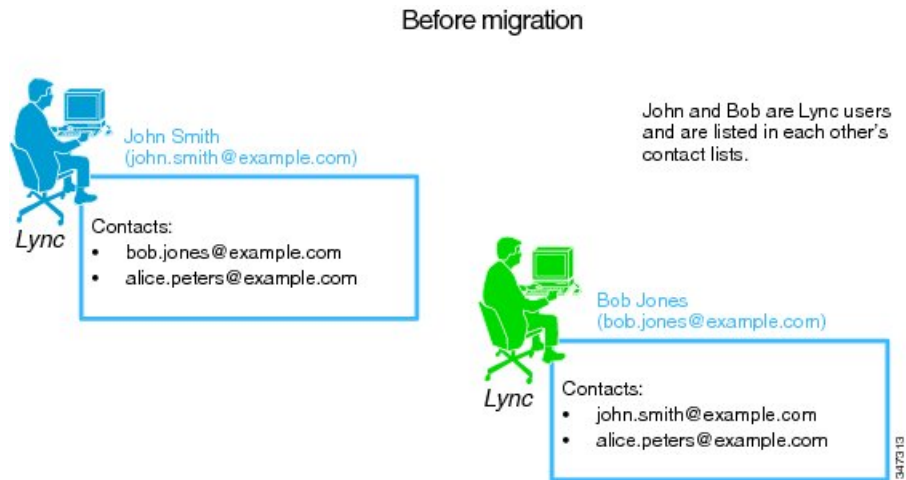
各バッチを移行する直前に Microsoft サーバ SIP URI を変更する場合は、Microsoft Server ユーザの各バッチを移行する前に、IM and Presence サービスの連絡先リストを更新し、移行しようとしている Microsoft サーバユーザの最新の SIP URI（接続 ID）を含めることを保障しなければなりません。次の例を考えてみます。



移行例

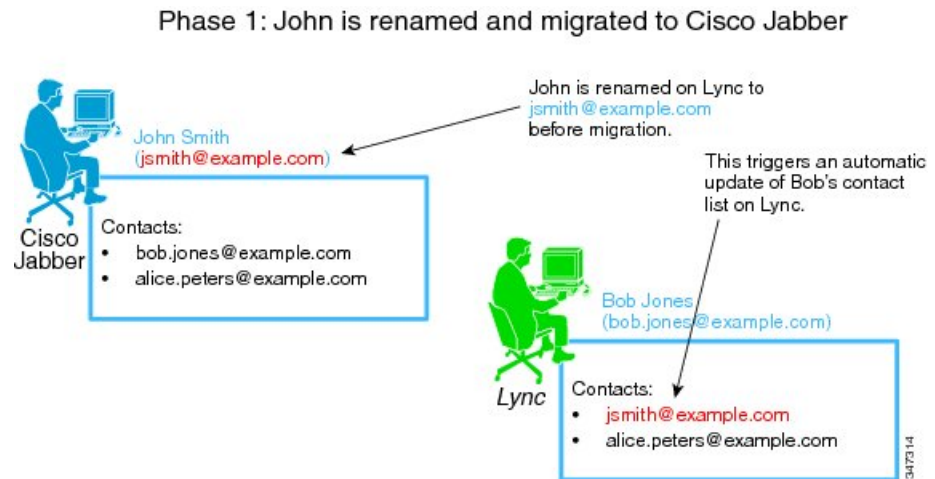
John Smith、Bob Jones は、Lync のユーザで、互いの連絡先リストの両方に表示されます。Lync URI は、john.smith@example.com と bob.jones@example.com です。John は移行のフェーズ 1 中に IM and Presence サービスに移行され、Bob は移行のフェーズ 2 中に移行されます。

図 11：移行前



ユーザの移行フェーズ 1 が始まり、John の Lync URI は jsmith@example.com に変更されます。それから、John が IM and Presence サービスに移動されます。John と Bob 間でアベイラビリティと IM は維持されます。

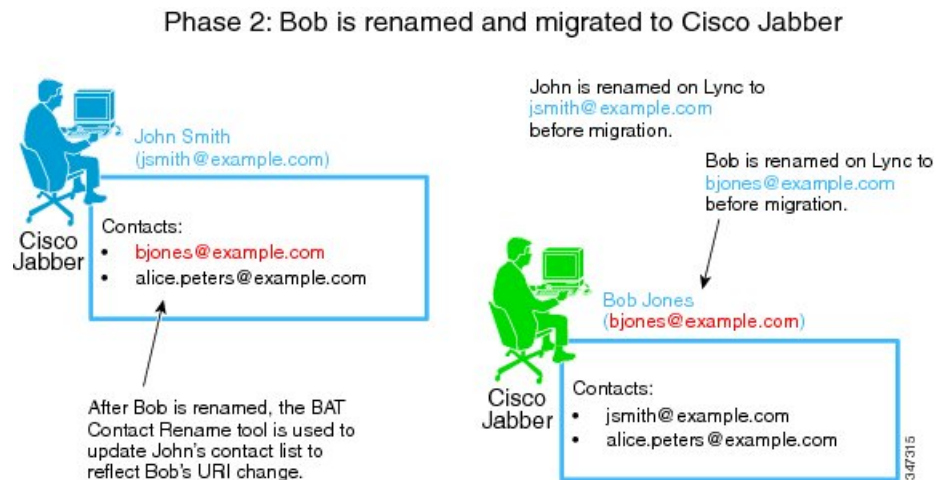
図 12：ユーザの移行フェーズ 1



ユーザの移行フェーズ 2 が始まり、Bob の Lync URI は bjones@example.com に変更されます。IM and Presence サービスの John のコンタクトリストはフェーズ 2 に移行されるユーザすべてとの新

しい接続 ID で更新されます。それから、Bob が IM and Presence サービスに移動されます。John と Bob 間でアベイラビリティと IM は維持されます。

図 13: ユーザの移行フェーズ 2



## Microsoft サーバ SIP URI 変更

どのLync/OCS URI も IM and Presence サービス サービス URI 形式に一致しない場合、移行プロセスを開始する前に Microsoft サーバ URI を変更する必要があります。Microsoft サーバ URI を変更する方法の詳細については、ユーザ移行の Microsoft サーバの SIP URI 形式の確認に関するトピックを参照してください。

### 関連トピック

[移行するユーザ用の Microsoft サーバ SIP URI 形式の確認, \(114 ページ\)](#)

## IM and Presence サービス ユーザの連絡先の名前変更

IM and Presence サービス一括管理ツールを使用すると、IM and Presence サービスのユーザの連絡先リスト内の連絡先 ID の名前を段階的に変更できます。これは、IM and Presence サービス連絡先リストを、Lync/OCSURI が変更される度に更新できることを意味しています。



(注) IM and Presence サービス連絡先リストを更新する必要がある場合、この更新は、(変更された URI を持つ) Microsoft サーバユーザが Cisco Unified Communications Manager 上で IM and Presence サービスに対して有効にされる前に実行する必要があります。

より多くの情報に対するアクセス ID 名の変更については、以下の関連トピックを参照してください。

関連トピック

[IM and Presence サービスの連絡先リスト内のコンタクト ID の変更](#), (116 ページ)

## 詳細なユーザ移行計画

IM and Presence サービスおよび Lync/OCS 間のパーティション イントラドメイン フェデレーション統合は、Microsoft サーバから IM and Presence サービスへの段階的移行中にユーザ間で基本的な通信を実現するよう設計されています。

ただし、パーティション イントラドメイン フェデレーション統合により、パフォーマンス上のオーバーヘッドが発生します。このため、IM and Presence サービスは、サーバあたり最大 130,000 件の SIP ドメイン内フェデレーションの連絡先をサポートします。Microsoft サーバから IM and Presence へのユーザ移行中に IM and Presence サービス ノード上でこのフェデレーションされた連絡先のしきい値を超えないようにするため、詳細な移行計画が必要な場合があります。

次の計算式を使用して、上記のフェデレーションされた連絡先のしきい値を超えずにサポートできる、IM and Presence サービス ユーザの最大数を見積もることができます。

最大対応ユーザ = 130,000 / 連絡先リストの平均サイズ

この計算式に基づいて、次の表は 130,000 件のフェデレーションされた連絡先のしきい値を超えずにサポートできる、IM and Presence サービス ユーザの最大数を示しています。

表 9: IM and Presence サービスの最大対応ユーザ数

連絡先リストの平均サイズ	最大対応ユーザ (ハイアベイラビリティなし)	最大対応ユーザ (ハイアベイラビリティあり) <sup>3)</sup>
200	650	325
150	866	433
100	1300	650
75	1733	866
50	2600	1300
25	5000	2500

<sup>3)</sup> これは、アクティブ/アクティブモードで動作している 2 ノードサブクラスタを想定しています

ご使用の展開内の IM and Presence サービス ノードでプロビジョニングされるユーザ数が該当の上限值を超える場合、詳細なユーザ移行計画が必要です。シスコのサポート担当者に連絡し、詳細な移行計画の定義を始めてください。

## 注記

- 1 上記の表にある最大対応ユーザ数の値は、最悪の場合の数字、つまりすべての連絡先がフェデレーションされている場合に基づいています。  
適切な移行計画により、130,000 件のフェデレーションされた連絡先のしきい値を超えずに、最大数のユーザを IM and Presence サービス ノードに段階的に展開できます。
- 2 高可用性が有効な場合、各 IM and Presence サービス ノードは、IM and Presence サービス 2 ノードサブクラスタ内のすべてのユーザに関連した負荷を処理できなければなりません。これは、ノード障害が発生した場合に、クラスタ内の 2 番目のノードが単独ですべてのユーザに対応するためです。そのため、ノードごとの制限は半分にする必要があります。
- 3 ご使用の Microsoft サーバ展開内の連絡先リスト平均サイズがわからない場合、移行計画が必要かどうか判断する際に最悪のケース（200 件の連絡先）を想定します。
- 4 上記の表にある最大対応ユーザ数の値は、5000 ユーザの IM and Presence サービス OVA テンプレートに基づくシスコ対応仮想プラットフォームを想定しています。1000 ユーザの OVA に対する同等の数字を次に詳しく説明します。

## 1000 ユーザ OVA

IM and Presence サービスは 1000 ユーザの OVA でノードあたり最大 18,000 の SIP イントラドメインフェデレーション接続をサポートできます。次の表は、18,000 件のフェデレーションされた連絡先のしきい値を超えずにサポートできる、IM and Presence サービス ユーザの最大数を示しています。

表 10: サポートされている IM の最大数および 1000 ユーザの OVA を持つ既存のサービス ユーザ

連絡先リストの平均サイズ	最大対応ユーザ（ハイアベイラビリティなし）	最大対応ユーザ（ハイアベイラビリティあり） <sup>4</sup>
200	90	45
150	120	60
100	180	90
75	240	120
50	360	180
25	720	360
18	1000	500

<sup>4</sup> これは、アクティブ/アクティブ モードで動作している 2 ノードサブクラスタを想定しています

## 5000 ユーザ OVA

IM and Presence サービスは 5000 ユーザの OVA でノードあたり最大 90,000 の SIP イントラドメインフェデレーション接続をサポートできます。次の表は、90,000 件のフェデレーションされた連絡先のしきい値を超えずにサポートできる、IM and Presence サービス ユーザの最大数を示しています。

表 11: サポートされている IM の最大数および 5000 ユーザの OVA を持つ既存のサービス ユーザ

連絡先リストの平均サイズ	最大対応ユーザ (ハイアベイラビリティなし)	最大対応ユーザ (ハイアベイラビリティあり) <sup>5)</sup>
200	450	225
150	600	300
100	900	450
75	1200	600
50	1800	900
25	3600	1800
18	5000	2500

<sup>5)</sup> これは、アクティブ/アクティブモードで動作している 2 ノードサブクラスタを想定しています

## ユーザ移行ツールの時間に関するガイドライン

シスコは、Lync/OCS から IM and Presence サービスへユーザを一括して移行できる多数のツールを提供しています。移行計画を立てるには、多数のユーザを移行している場合に、各ツールが実行するのに必要な時間を知っておくことが重要です。ここでは、次に示すツールごとの予想実行時間について説明します。



(注) Lync および OCS サーバ両方の混合配置がある場合、Lync ユーザに対してツールを実行し、次に OCS ユーザに対して再びツールを実行する必要があります。

## 連絡先リストエクスポート ツール

連絡先リストエクスポート ツール (ExportContacts.exe) は、平均毎秒 800 件の連絡先 (つまり、毎分 48,000 件の連絡先) の速度で Lync/OCS から連絡先をエクスポートできます。次に示す等式

をガイドとして使用し、Microsoft サーバユーザのセットに対するこのツールの予想実行時間を見積もることができます。

連絡先のエクスポート時間 (分) = Microsoft サーバユーザ数 x 連絡先リスト平均サイズ/48000

次の表は、多数のサンプル ケースの予想実行時間を示しています。

表 12: 連絡先リストエクスポート ツールの予想実行時間サンプル

Microsoft サーバユーザ数	連絡先リストの平均サイズ	連絡先エクスポート時間
2000	100	5 分
5000	75	8 分
15000	60	19 分

## アカウント無効化ツール

アカウント無効化ツール (DisableAccount.exe) は、平均毎秒 13 アカウント (毎分 800 アカウント) の速度で Lync/OCS アカウントを無効にできます。次に示す等式をガイドとして使用し、Microsoft サーバユーザのセットに対するこのツールの予想実行時間を見積もることができます。

アカウントを無効にする時間 (分) = Microsoft サーバユーザ数/800

次の表は、多数のサンプル ケースの予想実行時間を示しています。

表 13: アカウント無効化ツールの予想実行時間サンプル

Microsoft サーバユーザ数	アカウントを無効にする時間
2000	3 分
5000	7 分
15000	20 分

## アカウント削除ツール

アカウント削除ツール (DeleteAccount.exe) は、平均毎秒 13 アカウント (毎分 800 アカウント) の速度で Lync/OCS アカウントを削除できます。次に示す等式をガイドとして使用し、Microsoft サーバユーザのセットに対するこのツールの予想実行時間を見積もることができます。

アカウントを削除する時間 (分) = Microsoft サーバユーザ数/800

次の表は、多数のサンプル ケースの予想実行時間を示しています。

表 14: アカウント削除ツールの予想実行時間サンプル

Microsoft サーバ ユーザ数	アカウントを削除する時間
2000	3 分
5000	7 分
15000	20 分

## 一括管理ツールの連絡先リストのインポート

IM and Presence 一括管理ツール (BAT) は、IM and Presence サービスプラットフォームに応じて、さまざまな速度で連絡先をインポートできます。次の表は、選択した IM and Presence サービスプラットフォームの予想インポート速度を示しています。

表 15: 仮想マシン上の *IM and Presence* サービス *BAT* のインポート速度

OVA テンプレート	インポート速度
2000 ユーザ OVA	6 秒
5000 ユーザ OVA	12 秒
15000 ユーザ OVA	22 秒

次の表は、多数のサンプル ケースの予想実行時間を示しています。

表 16: *BAT Contact List Import* ユーティリティの予想実行時間サンプル

ユーザ数	連絡先リストの平均サイズ	インポート時間 (速度 = 22/秒) ( <sup>6</sup> )
2000	100	2 時間 32 分
5000	75	4 時間 45 分
15000	60	11 時間 22 分

<sup>6</sup> これらの数字は、連絡先のインポート速度 22/秒をサポートする最高仕様のマシンに適用されます

### 注記

- 1 連絡先リストエクスポート ツール、アカウント無効化ツール、およびアカウント削除ツールの計算式は、2Ghz 以上の CPU 処理能力、および 2GB の RAM を備えたハードウェアで実行する Lync/OCS および Active Directory (AD) に基づいています。
- 2 これらのユーザ移行ツールを実行しても、Microsoft Lync または Microsoft Office Communicator にサインインしている他の Microsoft サーバユーザ機能への影響はありません。
- 3 あらかじめスケジュールされたメンテナンスの時間帯にユーザ移行を実行して Microsoft サーバおよび AD システムの負荷を減らすことをお勧めします。

## 一括管理ツールの連絡先の名前変更

一括管理ツールの連絡先の名前変更ユーティリティ期間のレートは、2つの主要な要因によって影響されます。

- クラスタ内の、連絡先リスト内で名前の変更された連絡先 ID を持つユーザの数
- そのようなユーザごとに名前が変更された連絡先 ID の平均数

これらの要因は、各展開ごとに異なります。大規模なアクションとして（名称変更された 1000 タッチ ID）、実行するジョブの時間がかかる場合があります。考えられるジョブの完了率を概算するには、影響を受けるレートがユーザ アップデートされる見るようにジョブ経過表示インジケータを参照してください。





## 第 4 章

# 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ワークフロー

この章では、サポートされている Microsoft サーバでの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ワークフローと、Lync/OCS から IM and Presence サービスにユーザを移行するワークフローについて説明します。

- Microsoft Lync サーバ (Lync) 2010
- Microsoft Lync サーバ (Lync) 2013
- Microsoft Office Communications Server (OCS) 2007 R2
- [Lync を使用した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ワークフロー, 47 ページ](#)
- [OCS を使用した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ワークフロー, 49 ページ](#)
- [Microsoft サーバから IM and Presence サービスへのユーザの移行のための設定ワークフロー, 51 ページ](#)
- [IM and Presence と Microsoft サーバドメイン間フェデレーションフェデレーション機能との統合の設定ワークフロー, 52 ページ](#)

## Lync を使用した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ワークフロー

IM and Presence サービスおよび Microsoft Lync サーバ間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設定するには、次のワークフローを使用します。

## IM and Presence サービスの設定

- 1 必要なプレゼンス ドメインが、クラスタのすべての IM and Presence サービス ノードに設定されていることを確認します。IM and Presence サービスの設定済みドメインを確認し、新規ローカルドメインを追加する手順については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。
- 2 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する：フェデレーション用の [Microsoft Lync のスタティック ルートを設定](#)、(73 ページ) を参照してください。
- 3 スタティック ルートを Lync の配置に設定する： [スタティック ルートの設定](#)、(56 ページ) を参照してください。
- 4 Lync 配置のアクセス コントロール リストを設定する： [着信アクセス コントロール リストの設定](#)、(58 ページ) を参照してください。
- 5 IM and Presence サービスおよび Lync 間の TLS 暗号化の設定
  - a アプリケーション リスナーの設定： [アプリケーション リスナー ポートを設定](#)します。、(60 ページ) を参照してください。
  - b TLS ピア サブジェクトの設定： [TLS ピア サブジェクトの設定](#)、(61 ページ) を参照してください。
  - c ピア認証 TLS コンテキストの設定： [ピア認証 TLS コンテキストの設定](#)、(62 ページ) を参照してください。
  - d 認証局 (CA) のルート証明書のインポート： [認証局のルート証明書のインポート](#)、(63 ページ) を参照してください。
  - e CA 署名付き証明書の要求： [IM and Presence サービスの証明書署名要求の生成](#)、(64 ページ) を参照してください。
  - f CA 署名付き証明書のインポート： [認証局からの署名付き証明書のインポート](#)、(65 ページ) を参照してください。
- 6 (任意) 専用ルーティング IM and Presence サービス ノードを設定している場合、ルーティング IM and Presence サービス ノードの不要な機能サービスを非アクティブ化する： [ルーティング IM and Presence サービス ノードでの機能サービスの非アクティブ化](#)、(66 ページ) を参照してください。



(注) パーティションイントラドメインフェデレーションは、IM and Presence サービスおよび Microsoft Lync または OCS 間の連続したフェデレーションのみをサポートします。フェデレーションサーバ間のファイアウォール (ASA) はサポートされません。

## Lync の設定

- 1 Lync サーバで設定されたイントラドメイン フェデレーションのプレゼンス ドメインに、IM and Presence サービス ノードで設定されたプレゼンス ドメインと一致するドメインがあることを確認します。IM and Presence サービスの設定済みドメインを確認し、新規ローカルドメイ

ンを追加する手順については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

- 2 IM and Presence サービス導入への Lync のスタティック ルートの設定：を参照してください。
- 3 IM and Presence サービス導入用のホスト認証を追加し、ポート 5061 をイネーブルにする：[Enterprise Edition Lync Server](#) での IM and Presence サービスに対するホスト認証の追加、(76 ページ) を参照してください。
- 4 トポロジのパブリッシュ：[トポロジのパブリッシュ](#)、(80 ページ) を参照してください。
- 5 CA ルート証明書が LCS サーバごとにインストールされるようにする：[Lync への認証局のルート証明書のインストール](#)、(81 ページ) を参照してください。
- 6 すべての Lync サーバに必要な署名付き証明書があるようにする：[既存の Lync 署名付き証明書の検証](#)、(83 ページ) を参照してください。
- 7 認証局から要求の署名付き証明書を要求する：[Lync の認証局から署名付き証明書を要求](#)、(84 ページ) を参照してください。
- 8 CA サーバから証明書をダウンロードする：[CA サーバから証明書をダウンロード](#)、(86 ページ) を参照してください。
- 9 署名付き証明書のインポート：[Lync の署名付き証明書をインポート](#)、(86 ページ) を参照してください。
- 10 証明書の割り当て：[Lync への証明書の割り当て](#)、(87 ページ) を参照してください。
- 11 サービスの再起動：[Lync サーバでのサービスの再起動](#)、(88 ページ) を参照してください。



#### ヒント

ユーザへの影響を最小限に抑えるために、オフピーク時にフロント エンド サービスを再起動するように計画します。

サーバを設定した後、ユーザを移行することができます。

## OCS を使用した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ワークフロー

次のワークフローを使用して、IM and Presence サービスと OCS 2007 R2 間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設定します。

### IM and Presence サービスの設定

- 1 必要なプレゼンス ドメインが、クラスタのすべての IM and Presence サービス ノードに設定されていることを確認します。IM and Presence サービスの設定済みプレゼンス ドメインを確認し、新規ローカルプレゼンス ドメインを追加する手順については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

- 2 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する：パーティションイントラドメインフェデレーションオプションの設定、(54 ページ) を参照してください。
- 3 OCS 展開へのスタティック ルートの設定：スタティック ルートの設定、(56 ページ) を参照してください。
- 4 OCS 展開のアクセス コントロール リストの設定：着信アクセス コントロール リストの設定、(58 ページ) を参照してください。
- 5 (任意) IM and Presence サービスおよび OCS 間の TLS 暗号化の設定：
  - a アプリケーション リスナーの設定：アプリケーション リスナー ポートを設定します。、(60 ページ) を参照してください。
  - b TLS ピア サブジェクトの設定：TLS ピア サブジェクトの設定、(61 ページ) を参照してください。
  - c ピア認証 TLS コンテキストの設定：ピア認証 TLS コンテキストの設定、(62 ページ) を参照してください。
  - d 認証局 (CA) のルート証明書のインポート：認証局のルート証明書のインポート、(63 ページ) を参照してください。
  - e CA 署名付き証明書の要求：IM and Presence サービスの証明書署名要求の生成、(64 ページ) を参照してください。
  - f CA 署名付き証明書のインポート：認証局からの署名付き証明書のインポート、(65 ページ) を参照してください。
- 6 (任意) 専用ルーティング IM and Presence サービス ノードを構成している場合は、ルーティングする IM and Presence サービス ノードで不要な機能サービスを無効にします。ルーティング IM and Presence サービス ノードでの機能サービスの非アクティブ化、(66 ページ) を参照してください。

## OCS の設定

- 1 OCS サーバで設定されたイントラドメインフェデレーションのドメインに IM and Presence サービス ノードで設定されるドメインと一致するプレゼンス ドメインがあることを確認します。IM and Presence サービスの設定済みドメインを表示し、新しいローカルドメインを追加する手順については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。
- 2 ポート 5060 の有効化：OCS サーバでのポート 5060/5061 の有効化、(92 ページ) を参照してください。
- 3 IM and Presence サービス導入にスタティック ルートを設定する：IM and Presence サービスをポイントする OCS のスタティック ルートの設定、(96 ページ) を参照してください。
- 4 IM and Presence サービス導入にホスト認証を追加する：OCS での IM and Presence サービスのホスト認証の追加、(97 ページ) を参照してください。
- 5 (任意) IM and Presence サービスおよび OCS 間の TLS 暗号化の設定：
  - a TLS 相互認証が OCS サーバごとに設定されるようにする：TLS 相互認証の OCS での設定、(100 ページ) を参照してください。

- b CA ルート証明書が OCS サーバごとにインストールされるようにする：[認証局ルート証明書の OCS へのインストール](#)、(101 ページ) を参照してください。
  - c すべての OCS サーバに必要な署名付き証明書を持たせる：[既存の OCS 署名付き証明書の検証](#)、(103 ページ) を参照してください。
  - d 必要に応じて、新しい署名付き証明書を要求する：[OCS サーバの認証局から署名付き証明書の要求](#)、(104 ページ) を参照してください。
- 6 サービスの再起動：[OCS フロントエンドサーバでのサービスの再起動](#)、(98 ページ) を参照してください。



## ヒント

ユーザへの影響を最小限に抑えるために、オフピーク時にフロントエンドサービスを再起動するように計画します。

サーバを設定した後、ユーザを移行することができます。

## Microsoft サーバから IM and Presence サービスへのユーザの移行のための設定ワークフロー

Lync/OCS から IM and Presence サービスにユーザを移行するには、次のワークフローを使用します。

- 1 ユーザ移行ツールのダウンロード：[シスコのユーザ移行ツール](#)、(109 ページ) を参照してください。
- 2 無制限の連絡先リストサイズとウォッチャ サイズを IM and Presence サービスで設定する：[無制限の連絡先リストとウォッチャの設定](#)、(111 ページ) を参照してください。
- 3 登録要求の自動承認を有効にする：[サブスクリプション要求の自動許可の有効化](#)、(111 ページ) を参照してください。
- 4 移行するユーザの Microsoft サーバ SIP URI 形式を確認する：[を参照してください。移行するユーザ用の Microsoft サーバ SIP URI 形式の確認](#)、(114 ページ)
- 5 必要に応じて、IM and Presence サービス連絡先リストのコンタクト ID の名前を変更する：[を参照してください。IM and Presence サービスの連絡先リスト内のコンタクト ID の変更](#)、(116 ページ)
- 6 IM and Presence サービスで移行するユーザのプロビジョニングをする：[Cisco Unified Communications Manager の Microsoft サーバのユーザ プロビジョニング](#) を参照してください。
- 7 移行するユーザ用の Microsoft サーバデータのバックアップする：[ユーザの Microsoft サーバの連絡先リスト情報のバックアップ](#) を参照してください。
- 8 移行するユーザ用の Microsoft サーバの連絡先リストをエクスポートする：[ユーザを移行するための連絡先リストのエクスポート](#)、(119 ページ) を参照してください。

- 9 移行するユーザ用の Microsoft サーバアカウントを無効する：[Microsoft サーバのユーザの無効化](#)を参照してください。
- 10 移行するユーザ用の Microsoft サーバアカウントが無効になっていることを確認する：[Active Directory の更新が Microsoft サーバと同期していることの確認](#)を参照してください。
- 11 移行するユーザ用の Microsoft サーバのユーザデータを削除する：[ユーザを移行するためのデータベースからのユーザデータの削除](#), (128 ページ)を参照してください。
- 12 移行するユーザ用の IM and Presence サービスに連絡先リストをインポートする：[IM and Presence にユーザを移行するための連絡先リストのインポート](#), (130 ページ)を参照してください。
- 13 IM and Presence サービスの連絡先リストおよびウォッチャ制限をリセットする：[連絡先リストと最大ウォッチャの最大サイズのリセット](#), (133 ページ)を参照してください。

## IM and Presence と Microsoft サーバドメイン間フェデレーションフェデレーション機能との統合の設定ワークフロー



(注)

このワークフローを開始する前に、Lync/OCS 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設定し、正しく動作するようにします。ご使用の導入内での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については、該当するワークフローを参照してください。

- 1 IM and Presence サービスのフェデレーテッドプレゼンスドメインをそれぞれ設定する：次を参照してください。[Microsoft サーバのドメイン内フェデレーション接続を介したドメイン間フェデレーションのリモートドメインのセットアップ](#), (137 ページ)
- 2 IM and Presence サービスでリモートプレゼンスドメインをホストしている各サービスにスタティックルートを設定する：次を参照してください。[リモートドメインへのスタティックルートの設定](#), (138 ページ)





## 第 5 章

# パーティションイントラドメインフェデレーションの IM and Presence サービスノードの設定

- [パーティションイントラドメインフェデレーションのドメイン設定, 53 ページ](#)
- [パーティションイントラドメインフェデレーション オプションの設定, 54 ページ](#)
- [スタティック ルートの設定, 56 ページ](#)
- [着信アクセス コントロール リストの設定, 58 ページ](#)
- [TLS 暗号化の設定, 59 ページ](#)
- [ルーティング IM and Presence サービス ノードでの機能サービスの非アクティブ化, 66 ページ](#)

## パーティションイントラドメインフェデレーションのドメイン設定

パーティションイントラドメインフェデレーションの IM and Presence サービスをセットアップする前に、IM and Presence サービス クラスタのすべてのノードに必要なプレゼンス ドメインがすべて設定されていることを確認します。Lync/OCS サーバに一致するプレゼンス ドメインがあることを確認します。必要に応じて、**Cisco Unified IM and Presence Administration** ユーザーインターフェイスを使用して、クラスタ内のノードでローカルプレゼンスドメインを追加するか更新します。

ディレクトリ URI が IM アドレス スキームとして設定されている場合に複数のドメインが IM and Presence サービス クラスタでサポートされます。クラスタ内のすべてのノードは IM アドレス スキームとしてディレクトリ URI を使用するディレクトリ URI をサポートする必要があります。

クラスタに対して Directory URI IM アドレス スキームを設定する詳細に関しては、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

ドメイン間フェデレーションの複数のドメインのセットアップについては、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager Guide*』を参照してください。

## IM アドレス ドメインの表示

IM and Presence サービスの展開全体で、システムおよび管理者によって管理されるすべてのプレゼンス ドメインは、[プレゼンス (Presence)]>[ドメイン (Domains)]>[ドメインの検索/一覧表示 (Find and List Domains)] ウィンドウに表示されます。いずれかの情報フィールドのチェックマークは、ドメインがローカルクラスタに、または任意のピアのクラスタに関連付けられているかどうかを示します。管理者が管理するプレゼンス ドメインに関して、次の情報フィールドが表示されます。

- ドメイン
- ローカルクラスタに設定されている
- ピアのクラスタに設定されている

システムが管理するプレゼンス ドメインに関して、次の情報フィールドが表示されます。

- ドメイン
- ローカルクラスタで使用中
- ピアのクラスタで使用中

### 手順

[Cisco Unified CM IM and Presence Administration]>[プレゼンス (Presence)]>[ドメイン (Domains)] を選択します。[ドメインの検索と一覧表示 (Find and List Domains)] ウィンドウが表示されます。

## パーティションイントラドメイン フェデレーション オプションの設定

次の手順では、IM and Presence サービスで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、ルーティング モードを選択する方法について説明します。

マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。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する、またはルーティング モードを選択する場合、これらの設定はクラスタ全体で有効になります。したがって、任意のクラスタ内の IM and Presence サービス パブリッシュ ノードで有効にするだけで設定できます。



**注意**

フェデレーションの電子メールアドレスは、パーティションイントラドメインフェデレーションが設定された導入ではサポートされません。Lync/OCS のドメイン間フェデレーション機能を使用する導入では、フェデレーションの電子メールアドレスはドメイン間フェデレーションでもサポートされません。フェデレーションの電子メールアドレスがこれらの展開シナリオのどの展開でも有効になっていないこと、[ドメイン間フェデレーションのために電子メールアドレスの使用を有効化 (Enable use of Email Address for Inter-domain Federation) ] オプションがクラスタに選択されていないことを確認します。

**手順**

- ステップ 1** [Cisco Unified Communications Manager IM and Presence Administration] ユーザーインターフェースにログインします。[プレゼンス (Presence) ]>[設定 (Settings) ]>[標準設定 (Standard Configuration) ]
- ステップ 2** [LCS/OCS/Lync とのパーティションドメイン間フェデレーションを有効化 (Enable Partitioned Intradomain Federation with LCS/OCS/Lync) ] チェックボックスをオンにします。
- ステップ 3** 警告メッセージに目を通し、[OK] をクリックします。
- ステップ 4** [パーティションイントラドメインフェデレーションルーティングモード (Partitioned Intradomain Federation Routing Mode) ] ドロップダウンリストから次のいずれかを選択します。
- ライセンスのない IM and Presence サービス要求の受信者が IM and Presence サービスドメイン内に存在する場合、[基本ルーティングモード (Basic Routing Mode) ] (デフォルト) ] を選択します。基本ルーティングモードでは、IM and Presence サービスは Microsoft サーバにこれらの受信者の要求をルーティングします。
  - ライセンスされていて、有効な Microsoft Lync または Microsoft Office Communicator SIP アドレスが IM and Presence サービスデータベースに保存されている要求の受信者が IM and Presence サービスドメインにある場合は [高度ルーティングモード (Advanced Routing Mode) ] を選択します。Cisco Unified Communications Manager が Microsoft サーバが使用する Active Directory からユーザを同期している場合のみ、[高度ルーティングモード (Advanced Routing Mode) ] を選択します。
- (注) Active Directory から同期されたユーザのリストには、すべての Microsoft Lync または Microsoft Office Communicator ユーザが記載されている必要があります。
- ステップ 5** [保存 (Save) ] をクリックします。
- ステップ 6** 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するか、ルーティングモードを選択した後、クラスタのすべての IM and Presence サービスノードの Cisco XCP ルータを再起動する必要があります。Cisco XCP ルータを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザーインターフェースにログインし、[ツール (Tools) ]>[コントロールセンター-ネットワークサービス (Control Center - Network Services) ] を選択します。適切な IM and Presence サービスノードをクリックしてスクロールダウンし、[Cisco XCP ルーター (Cisco XCP Router) ] を選択して [再起動 (Restart) ] をクリックします。
- (注) パーティションフェデレーションをイネーブルにするときに SIP プロキシを再起動するように促されます。

## 関連トピック

[IM and Presence から Microsoft サーバへの要求のルーティング](#), (14 ページ)

## スタティック ルートの設定

次の手順では、IM and Presence サービスと Lync/OCS 間のパーティションイントラドメイン フェデレーションのルーティングをイネーブルにするようにスタティック ルートを設定する方法について説明します。各 Microsoft サーバのプレゼンス ドメインの個々のスタティック ルートを追加する必要があります。スタティック ルートには、共通のネクスト ホップ アドレスを設定できません。Microsoft の Server 要求に経路指定に IM and Presence サービスから Microsoft のサーバ要求ルーティングと、基本および高度なルーティング モードに関連するトピックを参照してください。



(注) パーティションイントラドメイン フェデレーションを Microsoft サーバのドメイン間フェデレーション機能と統合している場合、各リモート ドメインの IM and Presence サービスにスタティック ルートを設定します。詳細については、リモート ドメインのスタティック ルートの設定に関するトピックを参照してください。



(注) 各 Microsoft サーバのプレゼンス ドメインに対してこの手順を実行します。

Microsoft サーバのプレゼンス ドメインのスタティック ルートについて、次の点に注意してください。

- Standard Edition Microsoft サーバについて、スタティック ルートは特定の Standard Edition サーバの IP アドレスをポイントする必要があります。
- フェデレーション トラフィックを IM and Presence サービス クラスタから直接いずれかのフロント エンド Microsoft サーバにルーティングする場合は、スタティック ルートはそのフロント エンド ロード バランサの IP アドレスをポイントする必要があります。

認定されたロード バランサのリストについては次の URL を参照してください。 <http://technet.microsoft.com/en-us/office/ocs/cc843611> ロード バランサを導入し、正しく管理するのはお客様の責任です。



(注) シスコでは、ロード バランサをポイントするスタティック ルートの設定はサポートしていません。フロント エンド ロード バランサをバイパスするためのスタティック ルートを設定することをお勧めします。

ハイ アベイラビリティのために、各 Microsoft サーバのプレゼンス ドメインの追加のバックアップスタティック ルートを設定できます。

バックアップ ルートの優先順位は低く、プライマリ スタティック ルートの次のホップ アドレスに到達できない場合にのみ使用されます。



- (注) マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、任意のクラスタ内の IM and Presence サービス データベース パブリッシュ ノードでのみ設定する必要があります。

## 手順

- ステップ 1** [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス (Presence)] > [ルーティング (Routing)] > [スタティック ルート (Static Routes)] を選択します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** ドメインが元に戻るよう [宛先パターン (Destination Pattern)] 値を入力します。たとえば、ドメインが「domaina.com」であれば、[宛先パターン (Destination Pattern)] の値は「.com.domaina.\*」となります。
- ステップ 4** [ネクスト ホップ (Next Hop)] フィールドに Microsoft サーバの IP アドレスを入力します。
- ステップ 5** [ルート タイプ (Route Type)] で [domain] を選択します。  
(注) ルート タイプのデフォルト設定はユーザです。
- ステップ 6** [ネクスト ホップ ポート (Next Hop Port)] および [プロトコル タイプ (Protocol Type)] を次のように設定します。
- TLS 暗号化の場合：
    - [ネクスト ホップ ポート (Next Hop Port)] の番号は **5061**
    - [プロトコル タイプ (Protocol Type)] は、**TLS**
  - TCP の場合：
    - [ネクスト ホップ ポート (Next Hop Port)] の番号は **5060**
    - [プロトコル タイプ (Protocol Type)] は、**TCP**
- ステップ 7** [プライオリティ (Priority)] 値を次のように入力します。
- プライマリ スタティック ルートについては、デフォルトの [プライオリティ (Priority)] 値 **1** を入力します。
  - バックアップスタティック ルートについては、1 より大きい [プライオリティ (Priority)] 値を入力します (値が小さいほど、スタティック ルートのプライオリティは上がります)。

- ステップ 8 他のすべてのパラメータにはデフォルト値を選択します。
- ステップ 9 [保存 (Save)] をクリックします。

### 次の作業

ネクスト ホップの Microsoft Lync サーバ IP アドレスとともに、宛先パターンの FQDN を逆順に使用し、追加のスタティックルートを作成します。たとえば、ドメインが「`lyncserver.domaina.com`」であれば、[宛先パターン (Destination Pattern)] の値は「`com.domaina.lyncserver`」となります。

## 着信アクセスコントロールリストの設定

次の手順では、Lync/OCS サーバが認証されなくても IM and Presence サービスにアクセスできるよう、着信アクセスコントロールリスト (ACL) のエントリを設定する方法について説明します。



- (注) マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、任意のクラスタ内の IM and Presence サービス パブリッシャ ノードでのみ設定する必要があります。

着信 ACL の設定方法は、どの程度厳格に IM and Presence サービス へのアクセスを制御するかにより異なります。

- IM and Presence サービスへのオープンアクセスを許可するには、[すべて (All)] のアドレスパターンのエントリを追加します。
- 特定のネットワーク ドメインから IM and Presence サービスへのアクセスを許可する場合は、アドレスパターンが特定のドメインと一致するエントリを追加します。たとえば、`foo.com` DNS ドメイン内の任意のサーバからアクセスできるようにするには、アドレスパターンに **foo.com** を入力します。
- 特定のサーバから IM and Presence サービスへのアクセスを許可するには、IP アドレスと一致するアドレスパターンとこれらのサーバの FQDN を持つ ACL エントリを追加します。各サーバで IP アドレスと FQDN の 2 つの ACL エントリを作成する必要があります。たとえば、サーバ `ocs1.foo.com` (10.1.10.100) からのアクセスを許可するには、1 つの ACL エントリとして **ocs1.foo.com** と入力し、別の ACL エントリの宛先パターンとして **10.1.10.100** と入力します。

パーティションイントラドメイン フェデレーションについて、IM and Presence サービスへのアクセスを特定の Microsoft サーバ FQDN または IP アドレスのみに制限する場合、次のエンティティの ACL エントリを追加する必要があります。

- 各 Microsoft サーバ Enterprise Edition フロントエンドまたは Standard Edition サーバ
- Microsoft の各サーバ プール FQDN (Enterprise Edition のみ)

サーバの FQDN を使用してアクセスを制限する場合は、フロントエンドサーバまたはプールと同じ IP アドレスに解決する他の DNS レコードの ACL エントリを追加する必要があります。たとえば、admin.lync.com などのいずれかの Lync のフロントエンドサーバと同じ IP アドレスに解決する Lync コントロールパネルにアクセスする DNS レコードを Lync サーバに作成できます。

**注意**

特定のサーバの FQDN または ACL エントリの IP アドレスを入力する場合、説明通りのすべての必要な ACL エントリの作成に失敗すると、Lync 2013 クライアントの安定性の問題が生じる場合があります。

**手順**

- ステップ 1** [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[システム (System)] > [セキュリティ (Security)] > [着信 ACL (Incoming ACL)] を選択します。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- ステップ 3** [説明 (Description)] フィールドに、Lync Server など、エントリの説明を入力します。
- ステップ 4** [アドレス パターン (Address Pattern)] フィールドにアドレス パターンを入力します。次の選択肢があります。
- IM and Presence サービスへのオープン アクセスを許可するには、「Allow from all」と入力します。
  - 特定のネットワーク ドメイン名を入力します (例: Allow from foo.com)。
  - 特定の IP アドレスを入力します (例: Allow from 10.1.10.100)。
  - 特定の FQDN を入力します (例: Allow from admin.lync.com)。
- (注) アドレス パターンとして「Allow from All」を入力しない場合、サーバの IP アドレスとサーバの FQDN の少なくとも 2 つの ACL エントリを作成する必要があります。ドメイン名の入力オプションです。
- [e] > [ルーティング (Routing)] > [設定 (Settings)] > [すべてのプロキシ サービスのリスタート (Restart All Proxy Services)]
- ステップ 5** [保存 (Save)] をクリックします。
- ステップ 6** SIP プロキシ サービスを再起動します。[プレゼンス (Presence)] > [ルーティング (Routing)] > [設定 (Settings)] > [すべてのプロキシ サービスのリスタート (Restart All Proxy Services)]

## TLS 暗号化の設定

IM and Presence サービスと Lync/OCS の間で TLS 暗号化を設定するには、この項の手順を完了する必要があります。TLS 暗号化は、Lync サーバを持つパーティションイントラドメインフェデレーションに必須です。



- (注) マルチクラスタ展開をしている場合、クラスタごとにこの手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、任意のクラスタ内の IM and Presence サービス パブリッシャー ノードでのみ設定する必要があります。

## アプリケーション リスナー ポートを設定します。

サーバ認証とピア認証の両方の [デフォルト Cisco SIP Proxy TLS リスナー (Default Cisco SIP Proxy TLS Listener)] 値を変更する必要があります。IM and Presence サービスは、デフォルトではポート 5062 でピア (相互) TLS 認証を実行します。ポート 5061 でピア TLS 認証が行われるようにするには、このデフォルト設定を変更し、サーバ TLS 認証ポート値を 5062 に設定する必要があります。

### 手順

- ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[システム (System)] > [アプリケーション リスナー (Application Listeners)] を選択します。
- ステップ 2 アプリケーション リスナーがまだ表示されていない場合、[検索 (Find)] を選択して、すべてのアプリケーション リスナーを表示します。
- ステップ 3 [デフォルト Cisco SIP Proxy TLS リスナー - サーバ認証 (Default Cisco SIP Proxy TLS Listener - Server Auth)] を選択します。
- ステップ 4 [ポート (Port)] 値を 5063 に変更します。
- ステップ 5 表示されるポップアップウィンドウで、[保存 (Save)] をクリックし、[OK] をクリックします。
- ステップ 6 [関連リンク (Related Links)] ドロップダウンリストで、[検索/一覧表示に戻る (Back to Find/List)] を選択し、[OK] を選択してアプリケーション リスナー リストに戻ります。
- ステップ 7 [デフォルト Cisco SIP Proxy TLS リスナー - ピア認証 (Default Cisco SIP Proxy TLS Listener - Peer Auth)] を選択します。
- ステップ 8 [ポート (Port)] 値を 5061 に変更します。
- ステップ 9 表示されるダイアログボックスで [Save (保存)] をクリックし、[OK] をクリックします。
- ステップ 10 [関連リンク (Related Links)] ドロップダウンリストで、[検索/一覧表示に戻る (Back to Find/List)] を選択し、[OK] を選択してアプリケーション リスナー リストに戻ります。
- ステップ 11 [デフォルト Cisco SIP Proxy TLS リスナー - サーバ認証 (Default Cisco SIP Proxy TLS Listener - Server Auth)] を選択します。
- ステップ 12 **5063 ~ 5062** のポート値を変更します。
- ステップ 13 [保存 (Save)] をクリックします。
- ステップ 14 クラスタのすべての IM and Presence サービス ノードで SIP Proxy サービスを再起動します。SIP プロキシサービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] を選択します。

## 次の作業

[TLS ピア サブジェクトの設定, \(61 ページ\)](#)

## 関連トピック

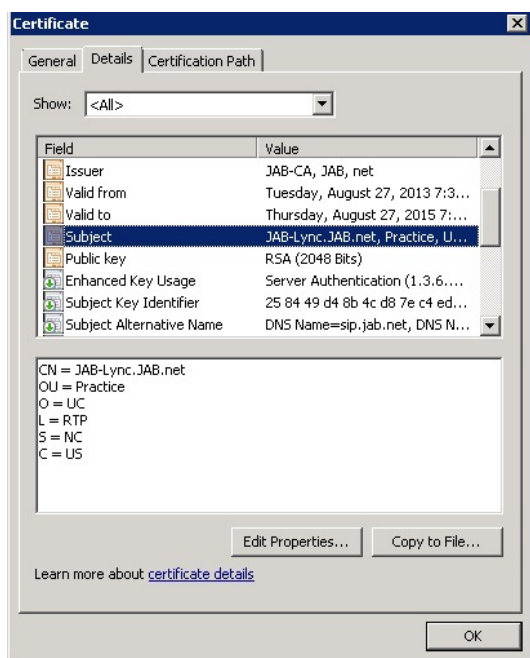
[統合のトラブルシューティング, \(143 ページ\)](#)

## TLS ピア サブジェクトの設定

ピア TLS 認証の場合、IM and Presence サービスでは、ピアにより提示されるセキュリティ証明書から件名共通名 (CN) が [TLS ピア サブジェクト (TLS Peer Subject)] リストに含まれている必要があります。[Cisco Unified IM and Presence Administration] ユーザーインターフェイスを使用して、件名 CN をこのリストに追加します。

[TLS ピア サブジェクト (TLS Peer Subject)] リストには件名 CN だけを含めます。[TLS ピア サブジェクト (TLS Peer Subject)] リストに [サブジェクト名の別名 (Subject Alternate Name)] エントリを含めないでください。次の図は、件名 CN が強調表示されている件名 CN 証明書の例を示します。

図 14 : 件名共通名の証明書



パーティションイントラドメインフェデレーションについては、次に示すエンティティの TLS ピア サブジェクトを追加する必要があります。

- 各 Lync/OCS Enterprise Edition フロント エンド サーバまたは Standard Edition サーバ

- 各 Lync/OCS プールの完全修飾ドメイン名 (FQDN) (Enterprise Edition のみ)

## 手順

- 
- ステップ 1** [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。 [システム (System) ] > [セキュリティ (Security) ] > [TLS ピア サブジェクト (TLS Peer Subjects) ] を選択します。
- ステップ 2** [新規追加 (Add New) ] をクリックします。
- ステップ 3** ピア サブジェクト名を入力します。
- Microsoft サーバの Enterprise Edition フロント エンドまたは Standard Edition サーバには、サーバの FQDN を入力します。
  - Microsoft サーバプールの完全修飾ドメイン名 (FQDN) には、IM and Presence サービスに提示する証明書の件名 CN を入力します。
- ステップ 4** [説明 (Description) ] フィールドに、OCS Server など、件名の説明を入力します。
- ステップ 5** [保存 (Save) ] をクリックします。
- ステップ 6** クラスタのすべての IM and Presence サービス ノードで Cisco SIP Proxy サービスを再起動します。Cisco SIP プロキシ サービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[ツール (Tools) ] > [コントロール センター - 機能サービス (Control Center - Feature Services) ] を選択します。[CUCM IM and Presence サーバ (CUCM IM and Presence Server) ] をクリックし、[SIP プロキシ(SIP Proxy) ] を選択して [再起動 (Restart) ] をクリックします。
- 

## 次の作業

[ピア認証 TLS コンテキストの設定, \(62 ページ\)](#)

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

# ピア認証 TLS コンテキストの設定

IM and Presence サービス および Lync/OCS 間の TLS 暗号化をサポートするには、IM and Presence サービス のピア認証 TLS コンテキスト設定を変更する必要があります。



## 手順

- ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。 [システム (System) ]>[セキュリティ (Security) ]>[TLS コンテキスト設定 (TLS Context Configuration) ] を選択します。
- ステップ 2 [検索 (Find) ] をクリックします。
- ステップ 3 デフォルト Cisco UP SIP プロキシ ピア認証 TLS コンテキスト用のリンクをクリックします。
- ステップ 4 [空の TLS フラグメントを無効化 (Disable Empty TLS Fragments) ] のチェックボックスがオンになっていることを確認します。
- ステップ 5 [TLS 暗号化マッピング (TLS Cipher Mapping) ] 領域の [利用可能な TLS 暗号化 (Available TLS Ciphers) ] リストで、すべての暗号を選択し、[右に移動 (Move Right) ] 矢印をクリックし、これらの暗号を [選択した TLS 暗号化 (Selected TLS Ciphers) ] リストに移動します。
- ステップ 6 [TLS ピアサブジェクトマッピング (TLS peer Subject Mapping) ] 領域の [利用可能な TLS ピアサブジェクト (Available TLS Peer Subjects) ] リストで、[TLS ピアサブジェクトの設定, \(61 ページ\)](#) で設定した TLS ピアサブジェクトを選択し、[Move Right (右に移動) ] 矢印をクリックし、[Selected TLS Peer Subjects (選択された TLS ピアサブジェクト) ] リストに移動します。
- ステップ 7 [保存 (Save) ] をクリックします。
- ステップ 8 クラスタのすべての IM and Presence サービスノードで Cisco SIP Proxy サービスを再起動します。 SIP プロキシサービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[ツール (Tools) ]>[コントロールセンター - 機能サービス (Control Center - Feature Services) ] を選択します。 CUCM IM and Presence サービスサーバをクリックし、[Cisco SIP プロキシ (Cisco SIP Proxy) ] 選択して [再起動 (Restart) ] をクリックします。

## 次の作業

[認証局のルート証明書のインポート, \(63 ページ\)](#)

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

# 認証局のルート証明書のインポート

通常、すべての Lync/OCS セキュリティ証明書は認証局 (CA) により署名されています。 IM and Presence サービス証明書も、Microsoft サーバと同じ認証局によって署名する必要があります。 IM and Presence サービスが Microsoft サーバ CA で署名された証明書を使用し、その同じ CA で署名された Microsoft サーバ証明書を承認するには、CA のルート証明書を IM and Presence サービス信頼ストアにアップロードする必要があります。

## はじめる前に

ルート証明書をインポートする前に、認証局から証明書を取得し、それをローカルコンピュータにコピーします。

## 手順

- 
- ステップ 1** [Cisco Unified IM and Presence OS Administration] ユーザ インターフェイスにログインします。 [セキュリティ (Security) ] > [証明書管理 (Certificate Management) ] を選択します。
- ステップ 2** [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate chain) ] をクリックします。
- ステップ 3** [証明書の名前 (Certificate Name) ] ドロップダウンリストで、cup-trust を選択します。
- ステップ 4** [説明 (Description) ] フィールドに、「認証局のルート証明書」など、証明書の説明 (わかりやすい名前) を入力します。
- ステップ 5** [参照 (Browse) ] を選択して、ローカル コンピュータ上のルート証明書を見つけます。
- ステップ 6** [アップロード (Upload) ] をクリックし、証明書を IM and Presence サービス ノードにアップロードします。
- ステップ 7** クラスタのすべての IM and Presence サービス ノードで Cisco SIP Proxy サービスを再起動します。Cisco SIP プロキシ サービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[ツール (Tools) ] > [コントロールセンター - 機能サービス (Control Center - Feature Services) ] を選択します。[CUCM IM and Presence サーバ (CUCM IM and Presence Server) ] をクリックし、[Cisco SIP プロキシ (Cisco SIP Proxy) ] を選択して [再起動 (Restart) ] をクリックします。
- 

## 次の作業

[IM and Presence サービスの証明書署名要求の生成, \(64 ページ\)](#)

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

# IM and Presence サービスの証明書署名要求の生成

IM and Presence サービス証明書が Lync/OCS により使用される同じ認証局 (CA) で署名する必要があります。CA 署名付き証明書を入手するには、次に示す 2 段階のプロセスを実行する必要があります。

- 1 IM and Presence サービス証明書署名付き要求 (CSR) の生成
- 2 CA 署名付き証明書を IM and Presence サービスにアップロードします。

次の手順では、IM and Presence サービスから CSR を生成して、ダウンロードする方法について説明します。IM and Presence サービス CSR のサイズは、2048 ビットです。

## 手順

- ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。 IM and Presence サービスで、[セキュリティ (Security)] > [証明書管理 (Certificate Management)] を選択します。
- ステップ 2 [CSR を作成 (Generate CSR)] をクリックします。
- ステップ 3 [証明書目的 (Certificate Purpose)] ドロップダウン リストで、cup を選択します。
- ステップ 4 [CSR を作成 (Generate CSR)] をクリックします。
- ステップ 5 [ステータス (Status)] “”に「成功：証明書署名要求が作成されました (Success: Certificate Signing Request Generated)」と表示されている場合、[閉じる (Close)] を選択します。
- ステップ 6 [CSR をダウンロード (Download CSR)] をクリックします。
- ステップ 7 [証明書の名前 (Certificate Name)] ドロップダウン リストで、cup を選択します。
- ステップ 8 [CSR をダウンロード (Download CSR)] を選択し、証明書をローカルコンピュータにダウンロードします。
- ステップ 9 証明書がダウンロードされたら、[閉じる (Close)] を選択します。

## 次の作業

CSR をダウンロードしたら、それを使用して選択した CA から署名付き証明書を要求できます。これは、有名なパブリック CA または内部 CA の場合があります。

[認証局からの署名付き証明書のインポート、\(65 ページ\)](#)

## 関連トピック

[統合のトラブルシューティング、\(143 ページ\)](#)

# 認証局からの署名付き証明書のインポート

次の手順では、CA 署名付き証明書を IM and Presence サービスにアップロードする方法について説明します。

## はじめる前に

IM and Presence サービス から CSR を生成し、ダウンロードします。 [IM and Presence サービスの証明書署名要求の生成、\(64 ページ\)](#) を参照してください。

## 手順

- 
- ステップ 1** [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[セキュリティ (Security)] > [証明書管理 (Certificate Management)] を選択します。
- ステップ 2** [証明書をアップロード (Upload Certificate)] をクリックすると [証明書/証明書チェーンをアップロード (Upload Certificate/Certificate chain)] ダイアログボックスが開きます。
- ステップ 3** [証明書の名前 (Certificate Name)] ドロップダウン リストで、cup を選択します。
- ステップ 4** [説明 (Description)] フィールドに、「CA 署名付き証明書」など、証明書の説明 (わかりやすい名前) を入力します。
- ステップ 5** [参照 (Browse)] を選択して、ローカル コンピュータ上の証明書ファイルを見つけます。
- ステップ 6** [アップロード (Upload)] をクリックし、証明書を IM and Presence サービス ノードにアップロードします。
- ステップ 7** 証明書をアップロードしたら、クラスタのすべての IM and Presence ノードで Cisco SIP Proxy サービスを再起動します。Cisco SIP プロキシサービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール (Tools)] > [コントロールセンターの機能サービス (Control Center - Feature Services)] を選択します。[CUCM IM and Presence サーバ (CUCM IM and Presence Server)] をクリックし、[Cisco SIP プロキシ (Cisco SIP Proxy)] を選択して [再起動 (Restart)] をクリックします。
- 

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

# ルーティング IM and Presence サービス ノードでの機能サービスの非アクティブ化

ルーティング IM and Presence サービス サーバが Lync/OCS からの SIP トラフィックを処理できる容量を備えるには、ユーザをルーティング IM and Presence サービス ノードに割り当ててはいけません。つまり、割り当てユーザをサポートしている多数の IM and Presence サービス 機能サービスをルーティング IM and Presence ノードで非アクティブ化できるということです。これらのサービスを非アクティブ化すると、ルーティング IM and Presence サービス ノードは、その SIP ルーティングの役割を果たすために処理能力が追加されます。次の手順では、機能サービスを非アクティブ化する方法について説明します。



### 制約事項

次の項は、フェデレーショントラフィックのルーティングにのみ使用される (Jabber ログインに使用されない) 専用の IM and Presence サービス ノードがある場合にのみ適用されます。このルーティング IM and Presence サービス ノードは、Cisco Jabber ログインのために導入された IM and Presence サービス ノードから分離されます。

---

## 手順

- 
- ステップ 1** [Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。 [ツール (Tools) ] > [サービス アクティベーション (Service Activation) ] を選択します。
- ステップ 2** [Server (サーバ) ] ドロップダウン リストから、 [IM and Presence サービス ノードをルーティング (Routing IM and Presence Service node) ] を選択します。
- ステップ 3** 次の機能サービスのチェックボックスをそれぞれオフにします。
- Cisco Presence Engine
  - Cisco XCP Text Conference Manager
  - Cisco XCP Web Connection Manager
  - Cisco XCP Connection Manager
  - Cisco XCP SIP Federation Connection Manager
  - Cisco XCP XMPP Federation Connection Manager
  - Cisco XCP Message Archiver
  - Cisco XCP Directory Service
  - Cisco XCP Authentication Service
- ステップ 4** [保存 (Save) ] をクリックします。
- 

## 関連トピック

[IM and Presence サービス ノードのルーティングの追加構成、 \(34 ページ\)](#)





## 第 6 章

# パーティションイントラドメインフェデレーション用 Microsoft Lync の設定

パーティションイントラドメインフェデレーション用の Microsoft Lync を設定するには、次の手順を記載されている順序で実行します。設定が完了したら、Lync サーバでサービスを再起動する必要があります。



(注) 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の TLS を設定する必要があります。Lync では TCP はサポートされません。

- [Lync サーバのドメインの確認, 70 ページ](#)
- [Microsoft Lync サーバ コンフィギュレーション タスク リストにフェデレーション リンク, 70 ページ](#)
- [フェデレーション用の Microsoft Lync のスタティック ルートを設定, 73 ページ](#)
- [Enterprise Edition Lync Server での IM and Presence サービスに対するホスト認証の追加, 76 ページ](#)
- [IM and Presence サービスのホスト認証をスタンダード エディションの Lync サーバに追加, 78 ページ](#)
- [トポロジのパブリッシュ, 80 ページ](#)
- [Lync への認証局のルート証明書のインストール, 81 ページ](#)
- [既存の Lync 署名付き証明書の検証, 83 ページ](#)
- [Lync の認証局から署名付き証明書を要求, 84 ページ](#)
- [CA サーバから証明書をダウンロード, 86 ページ](#)
- [Lync の署名付き証明書をインポート, 86 ページ](#)
- [Lync への証明書の割り当て, 87 ページ](#)

- [Lync サーバでのサービスの再起動, 88 ページ](#)

## Lync サーバのドメインの確認

パーティションイントラドメインフェデレーションの IM and Presence サービスをセットアップする前に、Microsoft Lync サーバに一致するプレゼンス ドメインが設定されていることと、IM and Presence サービス クラスタにすべてのノードがあることを確認します。

**Cisco Unified CM IM and Presence Administration** ユーザ インターフェイスで [プレゼンス (Presence) ] > [ドメイン (Domains) ] > [検索 (Find) ] を選択し、IM and Presence サービスに設定されたローカル ドメインと、外部サーバに設定されたシステム管理ドメインを確認します。

## Microsoft Lync サーバ コンフィギュレーション タスク リストにフェデレーション リンク

次の項に、IM and Presence サービス と Microsoft Lync サーバとの間のフェデレーション リンクを設定するエンドツーエンドの手順の概要を示します。

次の表に、IM and Presence サービス ノードと Microsoft Lync サーバとの間のフェデレーション リンクにスタティック ルートを設定する手順の概要を示します。IM and Presence サービスとフェデレーション用 Microsoft Lync 間の TLS のスタティック ルートを設定します。Microsoft Lync サーバにフェデレーションされているリンクに使用するスタティック ルートの設定に関する詳細については、<https://technet.microsoft.com/en-us/library/gg615051.aspx> を参照してください。

IM and Presence サービス ドメインごとにスタティック ルートを作成します。

表 17: **Microsoft Lync** サーバに連合リンクのスタティック ルートを設定するためのタスク リスト

手順	説明
IM and Presence サービスのスタティック ルートの設定	IM and Presence サービス上で、Lync サーバにスタティック ルートを作成します。[プロトコルタイプ (Protocol Type) ] に [TLS]、[次のホップポート (Next Hop Port) ] の番号として [5061] を選択します。



手順	説明
Lync での IM and Presence サービスのスタティック ルートの設定	<p>IM and Presence サービスの Lync のサーバのスタティック ルートを作成します。IM and Presence サービスルーティング ノード（ルータ ノードとして設定されている ノードがない場合はパブリッシャ ノード）だけにスタティック ルートを作成しなければなりません。IM and Presence サービス導入に複数のクラスタがある場合でも、加入者ノードにスタティック ルートとクラスタ間ピア ノードはいずれも作成する必要はありません。</p> <p>ただし、スタティック ルートは、各 IM and Presence サービスプレゼンス ドメインで必要です。</p> <p>(注) TLS で、IM and Presence サービスピアの認証のリスナーポートはデフォルトで 5062 に設定されます。Microsoft サーバのスタティックルートに合わせてピア認証のリスナーポートを 5061 に切り替えてください。ただし、サーバ認証のリスナーポートはデフォルトで 5061 であるため、これを別のポートに変更する必要があります。</p> <p>ポート 5061 を使用するように IM and Presence サービスのピア認証のリスナーポートを設定し、サーバ認証のリスナーポートを変更する</p> <p><b>Cisco Unified CM IM and Presence Administration</b> にログインし、[システム (System)] &gt; [アプリケーションリスナー (Application Listeners)] を選択します。</p> <ul style="list-style-type: none"> <li>必ずピア認証リスナーポートを 5061 にします。</li> <li>サーバ認証のリスナーポートが 5061 に設定されている場合は、5063 など、別の値に変更する必要があります。</li> </ul>
ルートの永続	この手順は、ルーティング ノードにのみ必要です。

スタティックルートを設定した後、ホスト認証を設定し、トポロジをパブリッシュします。以下の表は、ホスト認証をセットアップし、トポロジをパブリッシュするタスクを示します。

表 18: ホスト認証の設定およびトポロジのパブリッシュのためのタスク リスト

手順	説明
信頼できるアプリケーションプールの作成	<p>エンタープライズエディションの場合は、IM and Presence サービスノードを表す信頼済みアプリケーションのコンピュータを保存する単一の信頼できるアプリケーションプールを作成する必要があります。</p> <p>標準エディションの場合は、各 IM and Presence サービスノードの信頼済みアプリケーションプールを作成しなければなりません。</p>

手順	説明
作成されたプールに信頼できるアプリケーションのコンピュータを追加する	<p>ルーティング IM and Presence サービス ノードを除き、各 IM and Presence サービス ノードに作成されたプールに信頼できるアプリケーションのコンピュータを追加する必要があります。</p> <p>Enterprise Edition の構成にだけこの手順を実行します。</p>
作成されたプールへの信頼済みアプリケーション サーバの追加	<p>エンタープライズ エディションの場合は、IM and Presence サービス導入に対して作成されたプールにアプリケーション サーバを追加します。</p> <p>スタンダードエディションの場合は、ノード用に作成された各プールにアプリケーション サーバを追加します。</p>
トポロジをイネーブルにします。	<p>トポロジをイネーブルにする前に、次の項目が完了したことを確認してください。</p> <ul style="list-style-type: none"> <li>• IM and Presence サービス ノードのルーティングに TLS ルートを定義します。</li> <li>• IM and Presence サービス ノードのルーティングに新しいスタティック ルートを持続します。</li> <li>• IM and Presence サービス展開の信頼済みアプリケーション プールを作成します。</li> <li>• 各 IM and Presence サービス ノードに作成されたプールに信頼済みアプリケーションのコンピュータを追加します。</li> <li>• IM and Presence サービスの展開に作成されたプールに信頼済みアプリケーション サーバを追加します。</li> </ul>

Microsoft Lync サーバと IM and Presence サービス ノードに CA 署名付き証明書を追加しなければなりません。

表 19: Microsoft Lync サーバと IM and Presence サービス ノードの証明書を設定するためのタスク リスト

手順	説明
Lync の各サーバの証明書を設定します。	<p>CA ルート証明書および Lync の署名付き証明書を取得するには、次の手順を実行します。</p> <ul style="list-style-type: none"> <li>• CA 証明書チェーンをダウンロードおよびインストールします。</li> <li>• CA サーバの署名付き証明書を要求します。</li> <li>• Lync の証明書をインポートして割り当てます。</li> </ul> <p>Lync サーバ証明書をインポートし、割り当てる詳細については Microsoft Lync のマニュアルを参照してください (<a href="http://technet.microsoft.com/en-us/library/gg558664.aspx">http://technet.microsoft.com/en-us/library/gg558664.aspx</a>)。</p>
IM and Presence サービスでの証明書の設定	<p>IM and Presence サービスに Lync サーバ証明書に署名した CA のルート証明書をアップロードします。また、IM and Presence サービス用の CSR を生成し、CA によって署名されるようにします。CA 署名付き証明書を IM and Presence サービスにアップロードします。</p> <p>その後、Lync サーバの IM and Presence サービスで TLS ピアサブジェクトを追加します。詳細な手順については、証明書のセットアップに関するトピックを参照してください。</p>

## フェデレーション用の Microsoft Lync のスタティック ルートを設定

IM and Presence サービスは Microsoft Lync サーバとのフェデレーションの Transport Layer Security (TLS) をサポートします。IM and Presence サービスルーティング ノードのみにスタティック ルートを作成する必要があります。IM and Presence サービス展開に複数のクラスタがある場合でも、加入者ノードにスタティックルートとクラスタ間ピアノードはいずれも作成する必要はありません。

ただし、スタティック ルートは、各 IM and Presence サービス ドメインで必要です。

次の表に、この手順で使用した設定パラメータ例を示します。

表 20: Microsoft Lync の TLS スタティック ルート用のサンプルパラメータ

説明	サンプルパラメータ
IM and Presence サービス ノード FQDN (IM and Presence サービス ノードをルーティング) FQDN が正しい IP アドレスに解決できることを確認します。	impserverPub.sip.com
IM and Presence サービス ノード IP アドレス (IM and Presence サービス ノードをルーティング)	10.10.1.10
IM and Presence サービス ノードの TLS ポート TLS ポート値が設定されたインターフェイスのユーザ インターフェイスと一致させる必要があります。値を確認するには、 <b>[Cisco Unified CM IM and Presence Administration]</b> ユーザ インターフェイスにログインし、[システム (System)] > [アプリケーションリスナー (Application Listeners)] > [デフォルト Cisco SIP プロキシ TLS リスナー - ピア認証 (Default Cisco SIP Proxy TLS Listener - Peer Auth)] を選択します。 (注) シスコはポート 5061 を推奨します。ただし、ポート 5062 を使用できます。	5061
IM and Presence サービス ノードのドメイン	sip.com
Lync 登録サーバ	lyncserver.synergy.com



(注)

- Transport Layer Security (TLS) を使用する場合は、スタティック ルートの宛先パターンで使用する FQDN は、Lync のフロント エンド サーバから解決可能である必要があります。FQDN がスタティック ルートが指す IM and Presence サービス ノードの IP アドレスに解決されることを確認します。
- Lync FQDN をパーティションイントラドメインフェデレーションに使用される IM and Presence サービス ドメインに一致させることはできません。

## 手順

**ステップ 1** Lync Server サーバ管理シェルがインストールされたコンピュータに、ドメイン管理者などのロールでログインします。

**ヒント** RTCUniversalServerAdmins グループのメンバか、**New-CsStaticRoute** コマンドレットを割り当てたロールベースアクセスコントロール (RBAC) ロールとして、ログインする必要があります。

**ステップ 2** [スタート (Start) ]>[すべてのプログラム (All Programs) ]>[Microsoft Lync Server 2010]>[Lync Server 管理シェル (Lync Server Management Shell) ]の順に選択します。

ヒント Microsoft Lync サーバのバージョンに応じて、Microsoft Lync Server 2010 または 2013 を入力します。

**ステップ 3** TLS ルートを定義するには、次のコマンドを入力します。

```
$tlsRoute = New-CsStaticRoute -TLSSource
-Destinationfqdn_of_imp_routing_node-Portlistening_port_imp_routing_node-usedefaultcertificate
$true -MatchUridestination_domain
```

例 :

```
$tlsRoute = New-CsStaticRoute -TLSSource
-DestinationimpserverPub.sip.com-Port5061-usedefaultcertificate $true -MatchUriisip.com
```

引数の説明

パラメータ	説明
-Destination	IM and Presence サービス ルーティング ノードの FQDN。
-Port	IM and Presence サービスのルーティング ノードのリスニング ポート。
-MatchUri	宛先IM and Presence サービス ドメイン。

- (注)
- ドメインの子ドメインに一致させるには、**-MatchUri** パラメータに、たとえば \*.sip.com などのワイルドカード値を指定できます。この値は sip.com サフィックスを持つどのドメインにも一致します。
  - Microsoft Lync Server 2013 で IPv6 を使用する場合、**-MatchUri** パラメータの \* ワイルドカード オプションはサポートされていません。
  - usedefaultcertificate** を FALSE に設定した場合は、TLSCertIssuer および TLSCertSerialNumber パラメータを指定する必要があります。これらのパラメータには、それぞれ、スタティックルートで使用される証明書を発行する認証局 (CA) の名前と TLS 証明書のシリアル番号を指定します。これらのパラメータの詳細については、Lync Server 管理シェルを参照してください。

**ステップ 4** 新しく作成されたスタティックルートを中央管理ストアで保持されていることを確認します。次のコマンドを入力します。

```
Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}
```

- (注) IM and Presence サービス ノードをルーティングする場合のみこの手順を実行します。

**ステップ 5** 新しいスタティックルートを保持するように設定した場合、コマンドが正常に実行されたことを確認します。次のコマンドを入力します。

```
Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route
```

- ステップ 6** [外部ユーザ アクセス (External User Access) ]エリアで、Lync のコントロール パネルを開きます。
- [新規 (New) ]をクリックし、Lync が (IM and Presence サービスと) IM and Presence サービス ノードの FQDN とのフェデレーションを実行しているドメインのパブリック プロバイダーを作成します。
  - 新しいパブリック プロバイダーで、このプロバイダーとのすべての通信を許可するユーザーレベルの検証を設定します。

## Enterprise Edition Lync Server での IM and Presence サービスに対するホスト認証の追加

Lync が許可を求められることなく SIP 要求を IM and Presence サービス から受け入れられるようにするには、IM and Presence サービス ノードごとに Lync でホスト認証のエントリを設定する必要があります。Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。



(注) 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の TLS を設定する必要があります。TCP はサポートされません。

Lync と IM and Presence サービス間の TLS 暗号化に必要なホスト認証エントリを設定するには、各 IM and Presence サービス ノードの FQDN のホスト認証エントリを追加する必要があります。

### 手順

- ステップ 1** 以下のコマンドを使用して、IM and Presence サービス展開に対して信頼できるアプリケーション サーバを作成します。

**ヒント** プールの登録サービスの FQDN 値を検証するために **Get-CsPool** を入力できます。

```
New-CsTrustedApplicationPool -Identitytrusted_application_pool_name_in FQDN_format-Registrar  
Lync_Registrar_service_FQDN -SiteID_for_the_trusted_application_pool_site-TreatAsAuthenticated  
$true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly $false  
-Computerfqdnfirst_trusted_application_computer
```

例 :

```
New-CsTrustedApplicationPool  
-Identitytrustedpool.sip.com-Registrarlyncserver.synergy.com-Site1-TreatAsAuthenticated  
$true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly $false  
-ComputerfqdnimpserverPub.sip.com
```

引数の説明

パラメータ	説明
-Identity	IM and Presence サービス展開の信頼済みアプリケーションプールの名前を入力します。これは FQDN 形式である必要があります。例： trustedpool.sip.com  ヒント ActiveDirectory にはないマシンに関する警告メッセージを無視し、変更を適用します。
-Registrar	プールのレジストラ サービス ID または FQDN。例： lyncserver.synergy.com  この値は、コマンド Get-CsPool を使用して確認できます。
-Site	信頼できるアプリケーションプールを作成するサイトの数値。  ヒント Get-CsSite 管理シェルコマンドを使用します。
-Computerfqdn	IM and Presence サービス ルーティング ノードの FQDN。例： impserverPub.sip.com  <ul style="list-style-type: none"> <li>• impserverPub = IM and Presence サービス ホスト名。</li> <li>• sip.com = IM and Presence サービス ドメイン。</li> </ul>

**ステップ 2** 各 IM and Presence サービス ノードに次のコマンドを入力し、新しいアプリケーションプールに信頼できるアプリケーションのコンピュータとしてノードの FQDN を追加します。

```
New-CsTrustedApplicationComputer -Identity imp_FQDN-Poolnew_trusted_app_pool_FQDN
```

例：

```
New-CsTrustedApplicationComputer -Identity impserver2.sip.com-Pooltrustedpool.sip.com
```

引数の説明

パラメータ	説明
-Identity	IM and Presence サービス ノードの FQDN。例：impserver2.sip.com  (注) このコマンドを使用して、信頼できるアプリケーションのコンピュータとして IM and Presence サービス ルーティング ノードを追加しないでください。
-Pool	IM and Presence サービス展開で使用される信頼済みアプリケーションプールの FQDN。例：trustedpool.sip.com

**ステップ 3** 新しい信頼済みアプリケーションを作成し、それを新規アプリケーションプールに追加するには、次のコマンドを入力します。

**New-CsTrustedApplication**

```
-ApplicationIDnew_application_name-TrustedApplicationPoolFqdnnew_trusted_app_pool_FQDN-Port
5061
```

例：

**New-CsTrustedApplication**

```
-ApplicationIDimptrustedapp.sip.com-TrustedApplicationPoolFqdntrustedpool.sip.com-Port 5061
```

引数の説明

パラメータ	説明
-ApplicationID	アプリケーションの名前。これは任意の値にすることができます。 例：imptrustedapp.sip.com。
-TrustedApplicationPoolFqdn	IM and Presence サービス展開の信頼済みアプリケーションプールサーバの FQDN。例：trustedpool.sip.com
-Port	IM and Presence サービス ノードの SIP リスニング ポート。TLS の場合、ポートは 5061 です。

## 次の作業

トポロジのパブリッシュを続行します。

## 関連トピック

[統合のトラブルシューティング](#), (143 ページ)

## IM and Presence サービスのホスト認証をスタンダードエディションの Lync サーバに追加

Lync が認証確認を求められずに IM and Presence サービスから SIP 要求を受け入れられるようにするには、展開しているすべての標準エディション Lync サーバの各 IM and Presence サービス ノードのホスト認証エントリを設定しなければなりません。Lync サーバ上で各 IM and Presence サービス ノードの 1 本の信頼済みアプリケーションプールを作成します。



(注) 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の TLS を設定する必要があります。TCP はサポートされません。

Lync と IM and Presence サービス間の TLS 暗号化に必要なホスト認証エントリを設定するには、各 IM and Presence サービス ノードの FQDN のホスト認証エントリを追加する必要があります。



## 手順

**ステップ 1** 次のコマンドを使用して各 IM and Presence サービスの信頼済みアプリケーション サーバプールを作成します。

ヒント プールの登録サービスの FQDN 値を検証するために **Get-CsPool** を入力できます。

**New-CsTrustedApplicationPool**

```
-Identity fqdn_of_the_im_and_presence_service_node Registrar fqdn_of_the_lync_registrar_service Site site_id_for_where_you_want_to_create_trusted_app_pool TreatAsAuthenticated
$true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly $false
```

例 :

**New-CsTrustedApplicationPool**

```
-IdentityimpserverPub.sip.com-Registrarlyncserver.synergy.com-Site1-TreatAsAuthenticated
$true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly $false
```

引数の説明

パラメータ	説明
-Identity	信頼できるアプリケーションプールとして IM and Presence サービス ノードの FQDN 名を入力します。例：impserverPub.sip.com ヒント ActiveDirectory にはないマシンに関する警告メッセージを無視し、変更を適用します。
-Registrar	プールのレジストラ サービス ID または FQDN。例：lyncserver.synergy.com この値は、コマンド Get-CsPool を使用して確認できます。
-Site	信頼できるアプリケーションプールを作成するサイトの数値。 ヒント Get-CsSite 管理シェルコマンドを使用します。

**ステップ 2** 各 IM and Presence サービス ノードの場合は、ノードの信頼済みアプリケーションを作成し、そのノードの信頼できるアプリケーションのサーバプールに割り当てるには、次のコマンドを入力します。

**New-CsTrustedApplication**

```
-ApplicationIDnew_app_name-TrustedApplicationPoolFqdnnew_trusted_app_pool_fqdn-Port 5061
```

例 :

**New-CsTrustedApplication**

```
-ApplicationIDimptrustedapp.sip.com-TrustedApplicationPoolFqdnimpserverPub.sip.com-Port
5061
```

引数の説明

パラメータ	説明
-ApplicationID	ノードの FQDN にもなる信頼済みアプリケーションのコンピュータのアプリケーション ID。例: impserverPub.sip.com
-TrustedApplicationPoolFqdn	IM and Presence サービス導入で使用される信頼済みアプリケーションプールの FQDN。例: impserverPub.sip.com
-Port	IM and Presence サービス ノードの SIP リスニング ポート。TLS の場合、ポートは 5061 です。

### 次の作業

[トポロジのパブリッシュ, \(80 ページ\)](#)

### 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

## トポロジのパブリッシュ

次の手順は、トポロジをコミットする例を示します。

### 手順

- 
- ステップ 1** Lync Server 管理シェルで次のコマンドを実行し、トポロジを有効にします。  
**Enable-CsTopology**
- ステップ 2** 次のコマンドを実行し、トポロジを topology.xml という XML ファイルに書き出し、ファイルを C ドライブに保存します。  
**Get-CsTopology -AsXml | Out-File C:\topology.xml**  
(注) トポロジ情報を出力するファイルの名前と保存場所は自由に設定できます。
- ステップ 3** topology.xml ファイルを開きます。
- ステップ 4** クラスタの FQDN セクションで、信頼できるプールに追加した各 IM and Presence サービス ノードの IP アドレスを "0.0.0.0" から IP アドレス パラメータに変更します。
- ステップ 5** topology.xml ファイルを保存します。
- ステップ 6** Lync Server 管理シェルで次のコマンドを実行します。  
**Publish-CsTopology -FileName "C:\topology.xml"**
-

## 次の作業

[Lync への認証局のルート証明書のインストール](#), (81 ページ)

# Lync への認証局のルート証明書のインストール

TLS の設定は、IM and Presence サービスと Lync との間のパーティションイントラドメインフェデレーションに使用する必要があります。TCP は使用できません。IM and Presence サービスおよび Lync 間の TLS 暗号化をサポートするには、Lync サーバごとに署名付きセキュリティ証明書がなければなりません。この署名付き証明書は、証明書に署名した認証局 (CA) のルート証明書とともに、Lync サーバごとにインストールする必要があります。

Lync と IM and Presence サービス サーバで同じ CA を共有することをお勧めします。そうしないと、IM and Presence サービスの証明書に署名した CA のルート証明書も Lync サーバごとにインストールする必要があります。

通常、Lync CA のルート証明書は Lync サーバごとにあらかじめインストールされています。したがって、Lync と IM and Presence サービスが同じ CA を共有する場合、ルート証明書をインストールする必要はありません。ただし、ルート証明書が必要な場合は、次の詳細を参照してください。

Microsoft 認証局を使用している場合、Microsoft 認証局から Lync へのルート証明書のインストールについて、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照してください。

- CA 証明書チェーンのダウンロード
- CA 証明書チェーンのインストール

別の CA を使用する場合は、次の手順が Lync サーバにルート証明書をインストールするための一般的な手順です。CA からルート証明書をダウンロードする手順は、選択した CA によって異なります。



(注) 『*Integration Guide for Configuring IM and Presence Service for Interdomain Federation*』 マニュアルでは、Access Edge サーバについて説明しています。パーティションイントラドメインフェデレーションについては、Access Edge サーバへの参照を Lync Standard Edition サーバまたは Enterprise Edition フロント エンド サーバと置き換えることができます。

## はじめる前に

CA からルート証明書または証明書チェーンをダウンロードし、Lync サーバのハードディスクに保存します。

## 手順

- ステップ 1 Lync サーバで、[スタート (Start)] > [実行 (Run)] を選択します。
- ステップ 2 mmc と入力し、[OK] をクリックします。
- ステップ 3 [ファイル (File)] メニューで、[スナップインの追加と削除 (Add/Remove Snap-in)] を選択します。
- ステップ 4 [スナップインの追加と削除 (Add/Remove Snap-In)] ダイアログボックスで、[追加 (Add)] を選択します。
- ステップ 5 [利用可能なスタンドアロン スナップイン (Available Standalone Snap-ins)] リストで、[証明書 (Certificates)] を選択し、[追加 (Add)] を選択します。
- ステップ 6 [コンピュータ アカウント (Computer Account)] を選択し、[次へ (Next)] をクリックします。
- ステップ 7 [コンピュータを選択 (Select Computer)] ダイアログボックスで、[ローカル コンピュータ (このコンソールを実行中のコンピュータ) (Local Computer (the computer this console is running on))] チェックボックスをオンにし、[終了 (Finish)] を選択します。
- ステップ 8 [閉じる (Close)] をクリックしてから、[OK] をクリックします。
- ステップ 9 [証明書 (Certificates)] コンソールの左側のペインで、[証明書 (ローカル コンピュータ) (Certificates (Local Computer))] を展開します。
- ステップ 10 [信頼されたルート証明機関 (Trusted Root Certification Authorities)] を展開します。
- ステップ 11 [証明書 (Certificates)] を右クリックし、[すべてのタスク (All Tasks)] を選択します。
- ステップ 12 [インポート (Import)] をクリックします。
- ステップ 13 [インポート (Import)] ウィザードで、[次へ (Next)] をクリックします。
- ステップ 14 [参照 (Browse)] を選択して、ルート証明書または証明書チェーンを保存した場所に移動します。
- ステップ 15 ファイルを選択し、[開く (Open)] をクリックします。
- ステップ 16 [次へ (Next)] をクリックします。
- ステップ 17 [証明書をすべて次のストアに配置する (Place all certificates in the following store)] というデフォルト値のままにして、[証明書ストア (Certificate store)] の下に [信頼されたルート証明機関 (Trusted Root Certification Authorities)] が表示されていることを確認します。
- ステップ 18 [次へ (Next)] をクリックしてから、[終了 (Finish)] をクリックします。
- ステップ 19 他の CA について、必要に応じて手順 11 ~ 18 を繰り返します。

## 次の作業

[既存の Lync 署名付き証明書の検証](#), (83 ページ)

## 関連トピック

[統合のトラブルシューティング](#), (143 ページ)

## 既存の Lync 署名付き証明書の検証

IM and Presence サービス および Lync 間の TLS 暗号化をサポートするには、Lync サーバごとに、クライアント認証をサポートする署名付きセキュリティ証明書がなければなりません。署名付き証明書がすでに Lync サーバにインストールされている場合、次の手順では、既存の署名付き証明書がクライアント認証をサポートしているかどうかを確認する方法について説明します。

次のいずれかの OID 値が証明書に割り当てられていることを確認します。

- サーバおよびクライアント認証の両方に証明書が設定されている場合、OID 値は“1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2”です。
- 証明書がサーバ認証のみに設定されている場合、OID 値は“1.3.6.1.5.5.7.3.1”です。



(注)

- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロント エンド サーバでこの手順を実行する必要があります。

## 手順

- ステップ 1 Lync サーバで、[スタート (Start)] > [実行 (Run)] を選択します。
- ステップ 2 mmc と入力し、[OK] をクリックします。
- ステップ 3 [ファイル (File)] メニューで、[スナップインの追加と削除 (Add/Remove Snap-in)] を選択します。
- ステップ 4 [スナップインの追加と削除 (Add/Remove Snap-In)] ダイアログボックスで、[追加 (Add)] を選択します。
- ステップ 5 [利用可能なスタンドアロン スナップイン (Available Standalone Snap-ins)] リストで、[証明書 (Certificates)] を選択し、[追加 (Add)] を選択します。
- ステップ 6 [コンピュータ アカウント (Computer Account)] を選択し、[次へ (Next)] をクリックします。
- ステップ 7 [コンピュータを選択 (Select Computer)] ダイアログボックスで、[ローカル コンピュータ (このコンソールを実行中のコンピュータ) (Local Computer (the computer this console is running on))] チェックボックスをオンにし、[終了 (Finish)] を選択します。
- ステップ 8 [閉じる (Close)] をクリックしてから、[OK] をクリックします。
- ステップ 9 [証明書 (Certificates)] コンソールの左側のペインで、[証明書 (ローカル コンピュータ) (Certificates (Local Computer))] を展開します。
- ステップ 10 [パーソナル (Personal)] を展開して、[証明書 (Certificates)] を選択します。
- ステップ 11 右側のペインで、現在 Lync で使用されている署名付き証明書を見つけます。
- ステップ 12 [クライアント認証 (Client Authentication)] が [使用目的 (Intended Purposes)] カラムに記載されていることを確認します。

## 次の作業

[Lync の認証局から署名付き証明書を要求](#), (84 ページ)

## 関連トピック

[統合のトラブルシューティング](#), (143 ページ)

# Lync の認証局から署名付き証明書を要求

IM and Presence サービスと Lync との間で TLS 暗号化をサポートするには、Lync の各サーバには、クライアント認証とサーバ認証をサポートする署名付きセキュリティ証明書が必要です。次の手順は、認証局 (CA) からの新しい署名付き証明書を要求し、Lync サーバにインストールする方法について説明します。

次の手順は、Windows Server 2003 認証局に基づきます。この手順は、他の Windows サーバのバージョンとは多少異なる場合があります。



- (注) CA にはクライアント証明書およびサーバ認証 Extended Key Usage (EKU) をサポートする証明書のテンプレートが必要で、証明書に署名するときにこのテンプレートを使用する必要があります。

Lync サーバに証明書をインストールする前に、次のいずれかの OID 値が証明書に割り当てられていることを確認します。

- サーバおよびクライアント認証の両方に証明書が設定されている場合、OID 値は “1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2” です。
- 証明書がサーバ認証のみに設定されている場合、OID 値は “1.3.6.1.5.5.7.3.1” です。



ヒント 証明書署名要求 (CSR) を生成する場合、特定のテンプレートタイプが指定されない場合、デフォルトテンプレート形式が使用されます。ユーザが証明書の登録プロセス中に指定したテンプレートの種類は、証明書で指定されているテンプレートのタイプに一致する必要があります。それ以外の場合は、証明書の登録プロセスが失敗します。

## 手順

- ステップ 1** Lync Server 管理シェルで CSR ファイルを作成するには、次のコマンドを入力します。  
**Request-CsCertificate -New -Type Default -Outputfilename-ClientEku \$true**
- (注) 内部または外部証明書の特定の要求を作成する場合は、**-Type Internal** の代わりに、**-Type External** または **-Type Default** のパラメータを使用します。
- 証明書に署名するために CA でカスタム証明書テンプレートを使用している場合は、コマンド文字列に **-Template***template\_name* パラメータを追加します。
- ステップ 2** Lync サーバにログインし、Web ブラウザを開きます。
- ステップ 3** 次の URL を開きます。http://ca\_server\_IP\_address/certsrv (SSL 暗号化の場合、HTTP ではなく HTTPS を使用)。
- ステップ 4** [証明書を要求 (Request a certificate)] を選択し、[高度な証明書を要求 (Advanced certificate request)] を選択します。
- ステップ 5** [Base-64 で暗号化した CMC または PKCS #10 ファイルを使用して証明書要求を提出 (Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file)] または [Base-64 で暗号化した PKCS #7 ファイルを使用した更新要求を提出 (Submit a renewal request by using a base-64-encoded PKCS #7 file)] を選択します。
- ステップ 6** テキスト エディタを使用して作成した要求ファイルを開きます。
- ステップ 7** 要求ファイルからすべてのテキストをコピーし、ブラウザの [ベース 64 エンコード証明書要求 (CMC または PKCS #10 または PKCS #7) (Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7))] フィールドに貼り付けます。
- ステップ 8** [送信 (Submit)] をクリックします。

### 次の作業

[CA サーバから証明書をダウンロード, \(86 ページ\)](#)

## CA サーバから証明書をダウンロード

次の手順を実行し、CA サーバからルート証明書をダウンロードします。

### 手順

- 
- ステップ 1 CA サーバにログインします。
  - ステップ 2 [スタート (Start) ]>[管理ツール (Administrative Tools) ]>[認証局 (Certificate Authority) ] を選択し、CA コンソールを起動します。
  - ステップ 3 [保留中の要求 (Pending Requests) ] をクリックします。
  - ステップ 4 右側のペインで送信した証明書の要求を右クリックし、[すべてのタスク (All Tasks) ]>[発行 (Issue) ] を選択します。
  - ステップ 5 Lync サーバにログインし、Web ブラウザを開きます。
  - ステップ 6 次の URL を開きます。http://ca\_server\_IP\_address/certsrv (SSL 暗号化の場合、HTTP ではなく HTTPS を使用)。
  - ステップ 7 [保留中の証明書の要求の状態 (View the Status of a Pending Certificate Request) ] から、証明書の要求をクリックします。
  - ステップ 8 証明書をダウンロードします。
- 

### 次の作業

[Lync の署名付き証明書をインポート, \(86 ページ\)](#)

## Lync の署名付き証明書をインポート

署名付き証明書をインポートするには、次の手順を実行します。



## はじめる前に



(注) 次のいずれかの OID 値が証明書に割り当てられていることを確認します。

- サーバおよびクライアント認証の両方に証明書が設定されている場合、OID 値は“1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2”です。
- 証明書がサーバ認証のみに設定されている場合、OID 値は“1.3.6.1.5.5.7.3.1”です。

## 手順

Lync Server 管理シェルで次のコマンドを入力し、署名付き証明書をインポートします。

```
Import-CsCertificate -Path "signed_certificate_path"-PrivateKeyExportable $false
```

(注) 証明書に秘密キーが含まれる場合、`-PrivateKeyExportable $true` パラメータを使用します。

## 次の作業

[Lync への証明書の割り当て](#), (87 ページ)

## 関連トピック

[統合のトラブルシューティング](#), (143 ページ)

# Lync への証明書の割り当て

次の手順を実行し、証明書を割り当てます。

## 手順

- 
- ステップ 1** [開始 (Start)] > [Lync サーバ展開ウィザード (Lync Server Deployment Wizard)] を選択します。
- ステップ 2** [Lync サーバシステムのインストールまたはアップデート (Install or Update Lync Server System)] を選択します。
- ステップ 3** [もう一度実行 (Run Again)] をクリックし、証明書を要求、インストール、または割り当てます。
- ステップ 4** [証明書ウィザード (Certificate Wizard)] ウィンドウで、デフォルトの証明書を選択します。
- ステップ 5** [割り当て (Assign)] をクリックします。
- ステップ 6** 証明書の割り当てウィンドウで、[次へ (Next)] をクリックします。
- ステップ 7** 証明書ストアウィンドウでインポートされた証明書を選択し、[次へ (Next)] をクリックします。
- ステップ 8** 証明書の割り当ての概要ウィンドウで [次へ (Next)] をクリックします。
- ステップ 9** コマンドの実行ウィンドウで、タスクのステータスに [完了 (Completed)] と表示されるまで待機し、[終了 (Finish)] を選択します。
- ステップ 10** 証明書ウィザードのウィンドウを閉じます。
- 

## 次の作業

[Lync サーバでのサービスの再起動](#), (88 ページ)

# Lync サーバでのサービスの再起動

Lync のすべての手順を実行した後、Lync フロントエンドサービスを再起動して設定を有効にする必要があります。



(注)

- この手順は、あらかじめスケジュールされたメンテナンスの時間帯に実施することをお勧めします。
  - Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
  - Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。
-

## 手順

- 
- ステップ 1** [スタート (Start) ]>[プログラム (Programs) ]>[管理ツール (Administrative Tools) ]>[サービス (Services) ]を選択します。
- ステップ 2** サービス Lync フロントエンドサーバを右クリックして、[リスタート (Restart) ]を選択します。
- 

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)





## 第 7 章

# Microsoft Office Communications Server for Partitioned Intradomain Federation の設定

パーティションイントラドメインフェデレーションの Microsoft Office Communications サーバの設定は、Microsoft Office Communications Server (OCS) 2007 R2 にのみ適用されます。

- [OCS サーバのドメインの確認, 91 ページ](#)
- [OCS サーバでのポート 5060/5061 の有効化, 92 ページ](#)
- [Microsoft OCS サーバ コンフィギュレーション タスク リストへのフェデレーテッドリンク, 93 ページ](#)
- [IM and Presence サービスをポイントする OCS のスタティック ルートの設定, 96 ページ](#)
- [OCS での IM and Presence サービスのホスト認証の追加, 97 ページ](#)
- [OCS フロント エンド サーバでのサービスの再起動, 98 ページ](#)
- [TLS 暗号化の設定, 99 ページ](#)

## OCS サーバのドメインの確認

パーティションイントラドメインフェデレーションの IM and Presence サービスをセットアップする前に、Microsoft LCS サーバに一致するドメインが設定されていることと、IM and Presence サービス クラスタにすべてのノードがあることを確認します。

**Cisco Unified CM IM and Presence Administration** ユーザ インターフェイスを使用して、IM and Presence サービスに設定されたローカル ドメインと、外部サーバに設定されたシステム管理ドメインを確認します。

## OCS サーバでのポート 5060/5061 の有効化

IM and Presence サービス および OCS との間の SIP トラフィックに暗号化されていない TCP 接続を使用する場合は、OCS サーバを SIP TCP ポート 5060 でリッスンするように設定します。フェデレーテッド TLS 接続に、TLS ポート 5061 でリッスンするように OCS サーバを設定します。



- (注)
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
  - Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。

### 手順

- ステップ 1** [スタート (Start) ]> [プログラム (Programs) ]> [管理ツール (Administrative Tools) ]> [Office Communications Server 2007 R2] を選択します。
- ステップ 2** スタンダードエディションまたは Enterprise Edition フロントエンドサーバの FQDN を右クリックし、[プロパティ (Properties) ]> [フロントエンドのプロパティ (Front End Properties) ] を選択します。
- ステップ 3** [全般 (General) ] タブをクリックします。
- ステップ 4** [接続 (Connections) ] にポート 5060 または 5061 が記載されていない場合は、[追加 (Add) ] を選択します。
- ステップ 5** [IP アドレス値 (IP Address Value) ] に [すべて (All) ] を選択します。
- ステップ 6** 輸送およびポート値を入力します。
- TCP の場合、[トランスポート (Transport) ] に TCP、[ポート (Port) ] に 5060 を入力します。
  - TLS の場合、[トランスポート (Transport) ] に TLS、[ポート (Port) ] に 5061 を入力します。
- ステップ 7** [OK] をクリックして、[接続を追加 (Add Connection) ] ウィンドウを閉じます。これで、ポート値が [接続 (Connections) ] リストに記載されているはずですが。
- ステップ 8** [OK] を再度選択して、[フロントエンドサーバプロパティ (Front End Server Properties) ] ウィンドウを閉じます。

### 次の作業

IM and Presence サービスを指すように OCS サーバのスタティック ルートを設定します。

### 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

# Microsoft OCS サーバコンフィギュレーションタスク リストへのフェデレーテッドリンク

次の表では、IM and Presence サービスと Microsoft OCS サーバ間のフェデレーション リンクを設定する手順の概要を示します。

Access Edge サーバまたは Cisco Adaptive Security Appliance なしで IM and Presence サービスから OCS に直接フェデレーションを使用している場合は、OCS サーバの各ドメインで TLS または TCP のスタティック ルートを設定する必要があります。これらのスタティック ルートは IM and Presence サービス ノードをポイントします。Cisco Adaptive Security Appliance または Microsoft Access Edge は必要ではありません。

- Standard Edition では Standard Edition サーバのスタティック ルートを設定する必要があります。
- Enterprise Edition では、すべてのプールにスタティック ルートを設定する必要があります。

表 21 : Microsoft OCS サーバへのフェデレーション リンクのエンドツーエンド設定のタスク リスト

手順	説明
IM and Presence サービスのスタティック ルートの設定	<p>TLS または TCP がサポートされています。</p> <p>TLS では、[プロトコル タイプ (Protocol Type)] に [TLS]、[ネクスト ホップ ポート (Next Hop Port)] の番号として [5061] を選択します。</p> <p>TCP では、[プロトコル タイプ (Protocol Type)] に [TCP]、[ネクスト ホップ ポート (Next Hop Port)] の番号として [5060] を選択します。</p>

手順	説明
OCS での IM and Presence サービスのスタティック ルートの設定	<p>TLS または TCP がサポートされています。</p> <p>TLS の場合、スタティック ルート ポートは 5061 になります。</p> <p>TCP の場合、スタティック ルート ポートは 5060 になります。</p> <p><b>重要</b> OCS のスタティック ルートとともに TLS を使用する場合は、IM and Presence サービス ノードの IP アドレスでなく FQDN を指定する必要があります。</p> <p>ピア認証リスナー ポートを 5061 に設定し、サーバ承認リスナー ポートを変更します。</p> <p><b>Cisco Unified CM IM and Presence Administration</b> にログインし、[システム (System)] &gt; [アプリケーション リスナー (Application Listeners)] を選択します。</p> <ul style="list-style-type: none"> <li>• 必ずピア認証リスナー ポートを 5061 にします。</li> <li>• サーバ認証リスナー ポートが 5061 に設定されている場合は、別の値 (5063) に変更する必要があります。</li> </ul>
IM and Presence サービス用のホスト認証エントリを設定します。	<p>この手順は、TLS および TCP に適用されます。</p> <p>TLS では、IM and Presence サービス ノードそれぞれについて、1 つのエントリに IM and Presence サービス ノードの IP アドレスを使用し、2 つ目のエントリに IM and Presence サービス FQDN を使用して、2 つのホスト認証エントリを追加する必要があります。</p> <p>TCP の場合、IM and Presence サービス IP アドレスを使用する 1 つのホスト認証エントリのみを各 IM and Presence サービス ノードに追加する必要があります。</p>



手順	説明
OCS での証明書の設定	<p>この手順は TLS の場合だけです。</p> <p>CA ルート証明書および OCS の署名付き証明書を取得するには、次の手順を実行します。</p> <ul style="list-style-type: none"> <li>• CA 証明書チェーンをダウンロードおよびインストールします。</li> <li>• CA サーバの証明書を要求します。</li> <li>• CA サーバから証明書をダウンロードします。</li> </ul> <p>OCS の[フロントエンドサーバプロパティ (Front End Server Properties)]で、OCS のポート 5061 で TLS リスナーが設定されていることを確認します (トランスポートは MTLS または TLS の場合もあります)。</p> <p>[OCS フロントエンドサーバのプロパティ (OCS Front End Server Properties)]で、[証明書 (Certificates)]タブを選択し、[証明書の選択 (Select Certificate)]をクリックして、OCS 署名証明書を選択します。</p>
FIPS (SSLv3 よりも、TLSv1) を使用するように OCS を設定し CA ルート証明書をインポートします。	<p>この手順は TLS の場合だけです。</p> <ol style="list-style-type: none"> <li>1 OCS のローカルセキュリティ設定を開きます。</li> <li>2 コンソール ツリーから、[ローカルポリシー (Local Policies)]を選択します。</li> <li>3 [セキュリティ オプション (Security Options)]を選択します。</li> <li>4 [システム暗号化：暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う (System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing)]をダブルクリックします。</li> <li>5 セキュリティ設定を有効にします。</li> <li>6 [OK] をクリックします。</li> </ol> <p>(注) 有効にするには、OCS を再起動する必要があります。</p> <ol style="list-style-type: none"> <li>7 IM and Presence サービス証明書に署名した CA の CA ルート証明書をインポートします。証明書スナップインを使用して OCS の信頼ストアに CA ルート証明書をインポートします。</li> </ol>

手順	説明
IM and Presence サービス証明書の設定	<p>この手順は TLS の場合だけです。</p> <p>IM and Presence サービスに OCS サーバ証明書に署名した CA のルート証明書をアップロードします。また、IM and Presence サービス用の CSR を生成し、CA によって署名されるようにします。CA 署名付き証明書を IM and Presence サービスにアップロードします。</p> <p>その後、OCS サーバの IM and Presence サービスで TLS ピア サブジェクトを追加します。詳細な手順については、証明書のセットアップに関するトピックを参照してください。</p>

## IM and Presence サービスをポイントする OCS のスタティック ルートの設定

ダイレクトフェデレーション用に OCS が IM and Presence サービスに要求をルーティングできるようにするには、各 IM and Presence サービス ドメインについて OCS サーバで TLS または TCP のスタティックルートを設定する必要があります。これらのスタティックルートは IM and Presence サービス ノードをポイントします。



(注)

- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

### 手順

- ステップ 1 [スタート (Start) ]>[プログラム (Programs) ]>[管理ツール (Administrative Tools) ]>[Office Communications Server 2007 R2] を選択します。
- ステップ 2 適宜 Enterprise Edition プール名または Standard Edition サーバ名を右クリックします。
- ステップ 3 [プロパティ (Properties) ]>[フロントエンドプロパティ (Front End Properties) ] を選択します。
- ステップ 4 [ルーティング (Routing) ] タブを選択し、[追加 (Add) ] をクリックします。
- ステップ 5 foo.com など、IM and Presence サービス ノードのドメインを入力します。
- ステップ 6 [電話 URI (Phone URI) ] チェックボックスがオフになっていることを確認します。
- ステップ 7 ネクストホップトランスポート、ポート、IP アドレス/FQDN 値を設定します。
  - TCP の場合は、[ネクストホップトランスポート (Next Hop Transport) ] 値に [TCP] を選択し、[ネクストホップポート (Next Hop Port) ] 値に **5060** を入力します。ネクストホップ IP アドレスとして IM and Presence サービス ノードの IP アドレスを入力します。

- TLS の場合は、[ネクスト ホップ トランスポート (Next Hop Transport) ] 値に [TLS] を選択し、[ネクスト ホップ ポート (Next Hop Port) ] 値に **5061** を入力します。FQDN として IM and Presence サービス ノードの IP アドレスを入力します。

- (注)
- TLS のスタティック ルートに使用するポートは、IM and Presence サービス ノードで設定されたピア認証のリスナー ポートに一致する必要があります。
  - FQDN は OCS サーバで解決可能である必要があります。FQDN が IM and Presence サービス ノードの IP アドレスに解決されることを確認します。

- ステップ 8** [要求 URI のホストを置換 (Replace host in request URI) ] チェックボックスがオフになっていることを確認します。
- ステップ 9** [OK] をクリックして、[静的ルートの追加 (Add Static Route) ] ウィンドウを閉じます。新しいスタティック ルートがルーティング リストに表示されるはずですが。
- ステップ 10** [OK] を再度選択して、[フロント エンド サーバ プロパティ (Front End Server Properties) ] ウィンドウを閉じます。

#### 次の作業

ホスト認証を IM and Presence サービスの OCS に追加します。

## OCS での IM and Presence サービスのホスト認証の追加

認証を求められずに OCS が IM and Presence サービス から SIP 要求を承認できるようにするには、IM and Presence サービス ノードごとに OCS でホスト認証エントリを設定する必要があります。

TCP の場合、IM and Presence サービス IP アドレスを使用する 1 つのホスト認証エントリのみを各 IM and Presence サービス ノードに追加する必要があります。

OCS と IM and Presence サービス間の TLS 暗号化を設定する場合、次のように各 IM and Presence サービス ノードに 2 つのホスト認証エントリを追加する必要があります。

- 最初のエントリには、IM and Presence サービス ノードの FQDN を含める必要があります。
- 2 つ目のエントリには、IM and Presence サービス ノードの IP アドレスを含める必要があります。

TLS 暗号化を設定しない場合は、IM and Presence サービス ノードに 1 つのホスト認証エントリのみを追加します。このホスト認証エントリには、IM and Presence サービス ノードの IP アドレスが含まれている必要があります。

次の手順では、必要なホスト認証エントリを追加する方法について説明します。



- (注)
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
  - Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

## 手順

- ステップ 1** [スタート (Start)] > [プログラム (Programs)] > [管理ツール (Administrative Tools)] > [Office Communications Server 2007 R2] を選択します。
- ステップ 2** 適宜 Enterprise Edition プール名または Standard Edition サーバ名を右クリックします。
- ステップ 3** [プロパティ (Properties)] > [フロントエンドプロパティ (Front End Properties)] を選択します。
- ステップ 4** [ホスト認証 (Host Authorization)] タブを選択し、[追加 (Add)] をクリックします。
- ステップ 5** FQDN を入力している場合、[FQDN] を選択して、IM and Presence サービス ノードの FQDN を入力します。たとえば、imp1.foo.com などです。
- ステップ 6** IP アドレスを入力する場合は、[IP アドレス (IP Address)] を選択し、IM and Presence サービス ノードの IP アドレスを入力します。たとえば、10.x.x.x などです。
- ステップ 7** [発信のみ (Outbound Only)] チェックボックスがオフになっていることを確認します。
- ステップ 8** [サーバとしてのスロットル (Throttle as Server)] チェックボックスをオンにします。
- ステップ 9** [認証付きとして処理 (Treat as Authenticated)] チェックボックスをオンにします。
- ステップ 10** [OK] をクリックして、[承認済みホストの追加 (Add Authorized Host)] ウィンドウを閉じます。
- ステップ 11** IM and Presence ノードごとに手順 4 ~ 10 を繰り返します。
- ステップ 12** すべてのホスト認証エントリを追加したら、[OK] を選択して、[フロントエンドサーバプロパティ (Front End Server Properties)] ウィンドウを閉じます。

## 次の作業

[OCS フロントエンドサーバでのサービスの再起動, \(98 ページ\)](#)

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

# OCS フロントエンドサーバでのサービスの再起動

OCS ですべての設定手順が完了したら、OCS サービスを再起動し、設定を有効にする必要があります。



(注)

- この手順は、あらかじめスケジュールされたメンテナンスの時間帯に実施することをお勧めします。
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。

### 手順

- ステップ 1** [スタート (Start)] > [プログラム (Programs)] > [管理ツール (Administrative Tools)] > [Office Communications Server 2007 R2] を選択します。
- ステップ 2** Standard Edition サーバまたは Enterprise Edition フロントエンドサーバの FQDN を右クリックし、[停止 (Stop)] > [フロントエンドサービス (Front End Services)] > [フロントエンドサービス (Front End Service)] を選択します。
- ステップ 3** サービスが停止したら、Standard Edition サーバまたは Enterprise Edition のフロントエンドサーバの FQDN を右クリックし、[スタート (Start)] > [フロントエンドサービス (Front End Service)] > [フロントエンドサービス (Front End Service)] を選択します。

### 関連トピック

[統合のトラブルシューティング](#), (143 ページ)

## TLS 暗号化の設定

IM and Presence サービスと OCS の間で TLS 暗号化を設定するには、この項の手順を完了する必要があります。

TLS の設定が完了したら、OCS サーバでサービスを再起動する必要があります。 [OCS フロントエンドサーバでのサービスの再起動](#), (98 ページ) を参照してください。

## 連邦情報処理標準コンプライアンスを OCS で有効にする

IM and Presence サービス および OCS 間の TLS 暗号化をサポートするには、OCS サーバで TLSv1 を有効にする必要があります。TLSv1 は連邦情報処理標準 (FIPS) コンプライアンスの一環として Windows サーバに組み込まれています。次の手順では、FIPS コンプライアンスを有効にする方法について説明しています。



- (注)
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
  - Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。

### 手順

- ステップ 1** OCS サーバで、[スタート (Start)] > [プログラム (Programs)] > [管理ツール (Administrative Tools)] > [ローカルセキュリティポリシー (Local Security Policy)] を選択します。
- ステップ 2** コンソールツリーから、[ローカルポリシー (Local Policies)] を選択します。
- ステップ 3** [セキュリティオプション (Security Options)] を選択します。
- ステップ 4** [システム暗号化：暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う (System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing)] をダブルクリックします。
- ステップ 5** セキュリティ設定を有効にします。
- ステップ 6** [OK] をクリックします。
- ステップ 7** [ローカルセキュリティの設定 (Local Security Setting)] ウィンドウを閉じます。

### 次の作業

[TLS 相互認証の OCS での設定, \(100 ページ\)](#)

### 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

## TLS 相互認証の OCS での設定

IM and Presence サービスおよび OCS 間の TLS 暗号化を設定するには、TLS 相互認証について OCS サーバでポート 5061 を設定する必要があります。次の手順では、相互 TLS 認証用にポート 5061 を設定する方法について説明します。



- (注)
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
  - Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。

## 手順

- ステップ 1 [スタート (Start)] > [プログラム (Programs)] > [管理ツール (Administrative Tools)] > [Office Communications Server 2007 R2] を選択します。
- ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンドサーバの FQDN を右クリックし、[プロパティ (Properties)] > [フロントエンドのプロパティ (Front End Properties)] を選択します。
- ステップ 3 [一般 (General)] タブを選択します。
- ステップ 4 ポート 5061 に関連付けられた転送が **MTLS** の場合、手順 8 に進みます。
- ステップ 5 ポート 5061 に関連付けられた転送が **MTLS** ではない場合、[編集 (Edit)] を選択します。
- ステップ 6 [トランスポート (Transport)] ドロップダウンリストから、[MTLS] を選択します。
- ステップ 7 [OK] をクリックし、[接続を編集 (Edit Connection)] ウィンドウを閉じます。これで、ポート 5061 に関連付けられた転送は **MTLS** になるはずですが。
- ステップ 8 [OK] をクリックして、[プロパティ (Properties)] ウィンドウを閉じます。

## 次の作業

[認証局ルート証明書の OCS へのインストール, \(101 ページ\)](#)

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

# 認証局ルート証明書の OCS へのインストール

IM and Presence サービス および OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに署名付きセキュリティ証明書がなければなりません。この署名付き証明書は、証明書に署名した認証局 (CA) のルート証明書とともに、各 OCS サーバにインストールする必要があります。

OCS サーバと IM and Presence サービス ノードで同じ CA を共有することをお勧めします。共有していない場合、IM and Presence サービス証明書に署名した CA のルート証明書も各 OCS サーバにインストールする必要があります。

通常、OCS CA のルート証明書は各 OCS サーバにすでにインストールされています。したがって、OCS と IM and Presence サービスが同じ CA を共有している場合、ルート証明書のインストールは必要ない場合があります。ただし、ルート証明書が必要な場合は、次の詳細を参照してください。

Microsoft 認証局を使用している場合、Microsoft 認証局から OCS へのルート証明書のインストールについて、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照してください。

- CA 証明書チェーンのダウンロード
- CA 証明書チェーンのインストール

代替 CA を使用している場合、次の手順が、ルート証明書を OCS サーバにインストールする一般的な手順になります。CA からルート証明書をダウンロードする手順は、選択した CA によって異なります。

### はじめる前に

CA からルート証明書または証明書チェーンをダウンロードし、OCS サーバのハードディスクに保存します。

### 手順

- 
- ステップ 1 OCS サーバで、[スタート (Start) ]>[実行 (Run) ]を選択します。
  - ステップ 2 `mmc` と入力し、[OK] をクリックします。
  - ステップ 3 [ファイル (File) ]メニューで、[スナップインの追加と削除 (Add/Remove Snap-in) ]を選択します。
  - ステップ 4 [スナップインの追加と削除 (Add/Remove Snap-In) ]ダイアログボックスで、[追加 (Add) ]を選択します。
  - ステップ 5 [利用可能なスタンドアロンスナップイン (Available Standalone Snap-ins) ]リストで、[Certificates (証明書) ]を選択し、[Add (追加) ]を選択します。
  - ステップ 6 [コンピュータ アカウント (Computer Account) ]を選択し、[次へ (Next) ]をクリックします。
  - ステップ 7 [コンピュータを選択 (Select Computer) ]ダイアログボックスで、[ローカルコンピュータ (このコンソールを実行中のコンピュータ) (Local Computer (the computer this console is running on)) ]チェックボックスをオンにし、[終了 (Finish) ]を選択します。
  - ステップ 8 [閉じる (Close) ]をクリックしてから、[OK] をクリックします。
  - ステップ 9 [証明書 (Certificates) ]コンソールの左側のペインで、[証明書 (ローカル コンピュータ) (Certificates (Local Computer)) ]を展開します。
  - ステップ 10 [信頼されたルート証明機関 (Trusted Root Certification Authorities) ]を展開します。
  - ステップ 11 [証明書 (Certificates) ]を右クリックし、[すべてのタスク (All Tasks) ]を選択します。
  - ステップ 12 [インポート (Import) ]をクリックします。
  - ステップ 13 [インポート (Import) ]ウィザードで、[次へ (Next) ]をクリックします。
  - ステップ 14 [参照 (Browse) ]を選択して、ルート証明書または証明書チェーンを保存した場所に移動します。
  - ステップ 15 ファイルを選択し、[開く (Open) ]をクリックします。
  - ステップ 16 [次へ (Next) ]をクリックします。
  - ステップ 17 [証明書をすべて次のストアに配置する (Place all certificates in the following store) ]というデフォルト値のままにして、[証明書ストア (Certificate store) ]の下に[信頼されたルート証明機関 (Trusted Root Certification Authorities) ]が表示されていることを確認します。
  - ステップ 18 [次へ (Next) ]をクリックし、[終了 (Finish) ]をクリックします。
  - ステップ 19 他の CA について、必要に応じて手順 11 ~ 18 を繰り返します。
-





(注) 『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』マニュアルでは、Access Edge サーバについて説明しています。パーティションイントラドメインフェデレーションについては、Access Edge サーバへの参照を OCS Standard Edition サーバまたは Enterprise Edition フロント エンド サーバと置き換えることができます。

#### 次の作業

[既存の OCS 署名付き証明書の検証](#), (103 ページ)

#### 関連トピック

[統合のトラブルシューティング](#), (143 ページ)

[『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』](#)

## 既存の OCS 署名付き証明書の検証

IM and Presence サービスと OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに、クライアント認証をサポートする署名付きセキュリティ証明書がなければなりません。署名付き証明書がすでに OCS サーバにインストールされている場合、次の手順では、その既存の署名付き証明書がクライアント認証をサポートしているかどうか確認する方法について説明します。



- (注)
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
  - Enterprise Edition の場合、すべてのフロント エンド サーバでこの手順を実行する必要があります。

## 手順

- 
- ステップ 1** OCS サーバで、[スタート (Start)] > [実行 (Run)] を選択します。
- ステップ 2** `mmc` と入力し、[OK] をクリックします。
- ステップ 3** [ファイル (File)] メニューで、[スナップインの追加と削除 (Add/Remove Snap-in)] を選択します。
- ステップ 4** [スナップインの追加と削除 (Add/Remove Snap-In)] ダイアログボックスで、[追加 (Add)] を選択します。
- ステップ 5** [利用可能なスタンドアロン スナップイン (Available Standalone Snap-ins)] リストで、[証明書 (Certificates)] を選択し、[追加 (Add)] を選択します。
- ステップ 6** [コンピュータ アカウント (Computer Account)] を選択し、[次へ (Next)] をクリックします。
- ステップ 7** [コンピュータを選択 (Select Computer)] ダイアログボックスで、[ローカル コンピュータ (このコンソールを実行中のコンピュータ) (Local Computer (the computer this console is running on))] チェックボックスをオンにし、[終了 (Finish)] を選択します。
- ステップ 8** [閉じる (Close)] をクリックしてから、[OK] をクリックします。
- ステップ 9** [証明書 (Certificates)] コンソールの左側のペインで、[証明書 (ローカル コンピュータ) (Certificates (Local Computer))] を展開します。
- ステップ 10** [パーソナル (Personal)] を展開して、[証明書 (Certificates)] を選択します。
- ステップ 11** 右側のペインで、現在 OCS により使用されている署名付き証明書を見つけます。
- ステップ 12** [サーバとクライアントの認証の証明書 (Server and Client Authentication)] が [使用目的 (Intended Purposes)] カラムに記載されていることを確認します。
- 

## 次の作業

[OCS サーバの認証局から署名付き証明書の要求, \(104 ページ\)](#)

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

## OCS サーバの認証局から署名付き証明書の要求

この項では、Microsoft Office Communicator Server (OCS) に署名入り証明書をインストールし、TLS ネゴシエーションのためにインストールした証明書を選択する方法について説明します。



- (注) このトピックの手順は、OCS に署名付き証明書が存在しない、または既存の証明書がクライアント認証をサポートしていない場合のみ必要です。

IM and Presence サービスと OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに、クライアント認証をサポートする署名付きセキュリティ証明書がなければなりません。どの OCS サー

バにも署名付きセキュリティ証明書がない場合、次の手順は、認証局から新たに署名した証明書を要求し、その特定の OCS サーバにインストールする方法の概要を説明します。

OCS からの証明書署名要求 (CSR) で使用されている件名共通名 (CN) は、OCS の展開により異なります。

- Standard Edition サーバの場合、Standard Edition サーバの FQDN を件名 CN として使用します。
- Enterprise Edition フロントエンドサーバの場合、フロントエンドサーバが属するプールの FQDN を件名 CN として使用します。

### スタンドアロン Microsoft 認証局

スタンドアロン Microsoft 認証局を使用している場合、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照して、OCS サーバの CA から署名付き証明書を要求します。

- CA サーバからの証明書の要求
- CA サーバからの証明書のダウンロード



(注)

このマニュアルは Access Edge サーバについて説明しています。パーティションイントラドメインフェデレーションについては、Access Edge サーバへの参照を OCS Standard Edition サーバまたは Enterprise Edition フロントエンドサーバと置き換えることができます。

### 企業 Microsoft 認証局

企業 Microsoft 認証局を使用している場合、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照して、CA で必要なテンプレートを生成し、OCS サーバの CA から署名付き証明書を要求します。

- 企業の認証局を使用した Access Edge のカスタム証明書の作成
- サイトサーバの署名付き証明書の要求

### 別の認証局

代替 CA を使用している場合、次の手順が、署名付き証明書を OCS にインストールする一般的な手順になります。署名付き証明書を要求する手順は、選択した CA によって異なります。

### 関連トピック

[『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』](#)

## OCS サーバで署名付き証明書をインストールします。

### はじめる前に

CA から署名付き証明書をダウンロードし、OCS サーバのハードディスクに保存します。

### 手順

- 
- ステップ 1 OCS サーバで、[スタート (Start)] > [実行 (Run)] を選択します。
  - ステップ 2 mmc と入力し、[OK] をクリックします。
  - ステップ 3 [ファイル (File)] メニューで、[スナップインの追加と削除 (Add/Remove Snap-in)] を選択します。
  - ステップ 4 [スナップインの追加と削除 (Add/Remove Snap-In)] ダイアログボックスで、[追加 (Add)] を選択します。
  - ステップ 5 [利用可能なスタンドアロン スナップイン (Available Standalone Snap-ins)] リストで、[証明書 (Certificates)] を選択し、[追加 (Add)] を選択します。
  - ステップ 6 [コンピュータ アカウント (Computer Account)] を選択し、[次へ (Next)] をクリックします。
  - ステップ 7 [コンピュータを選択 (Select Computer)] ダイアログボックスで、[ローカルコンピュータ (このコンソールを実行中のコンピュータ) (Local Computer (the computer this console is running on))] チェックボックスをオンにし、[終了 (Finish)] を選択します。
  - ステップ 8 [閉じる (Close)] をクリックしてから、[OK] をクリックします。
  - ステップ 9 [証明書 (Certificates)] コンソールの左側のペインで、[証明書 (ローカル コンピュータ) (Certificates (Local Computer))] を展開します。
  - ステップ 10 [個人 (Personal)] を展開します。
  - ステップ 11 [証明書 (Certificates)] を右クリックし、[すべてのタスク (All Tasks)] を選択します。
  - ステップ 12 [インポート (Import)] をクリックします。
  - ステップ 13 [インポート (Import)] ウィザードで、[次へ (Next)] をクリックします。
  - ステップ 14 [参照 (Browse)] を選択して、署名付き証明書を保存した場所に移動します。
  - ステップ 15 ファイルを選択し、[開く (Open)] をクリックします。
  - ステップ 16 [次へ (Next)] をクリックします。
  - ステップ 17 [証明書をすべて次のストアに配置する (Place all certificates in the following store)] というデフォルト値のままにして、[証明書ストア (Certificate store)] の下に [個人 (Personal)] が表示されていることを確認します。
  - ステップ 18 [次へ (Next)] をクリックし、[終了 (Finish)] をクリックします。
- 

### 次の作業

[TLS ネゴシエーション用にインストールされた証明書の選択](#), (107 ページ)

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)

## TLS ネゴシエーション用にインストールされた証明書の選択

使用されている CA に関係なく、署名付き証明書が OCS サーバにインストールされたら、次の手順を実行して、TLS が IM and Presence サービスとネゴシエーションする場合に OCS が使用するインストール済み証明書を選択する必要があります。

### 手順

- 
- ステップ 1 [スタート (Start) ]>[プログラム (Programs) ]>[管理ツール (Administrative Tools) ]>[Office Communications Server 2007 R2] を選択します。
  - ステップ 2 スタンダードエディションサーバまたは Enterprise Edition フロント エンドサーバの FQDN を右クリックし、[プロパティ (Properties) ]>[フロントエンドのプロパティ (Front End Properties) ] を選択します。
  - ステップ 3 [セキュリティ (Security) ] タブを選択し、[証明書を選擇 (Select Certificate) ] を選択します。
  - ステップ 4 インストール済み証明書のリストから、新たに署名された証明書を選擇し、[OK] を選擇して [証明書の選擇 (Select Certificate) ] ウィンドウを閉じます。
  - ステップ 5 [OK] をクリックして、[プロパティ (Properties) ] ウィンドウを閉じます。
- 

### 次の作業

[OCS フロント エンドサーバでのサービスの再起動, \(98 ページ\)](#)

## 関連トピック

[統合のトラブルシューティング, \(143 ページ\)](#)





## 第 8 章

# ユーザの移行

- [シスコのユーザ移行ツール](#), 109 ページ
- [移行前の推奨事項](#), 110 ページ
- [移行するユーザ用の Microsoft サーバ SIP URI 形式の確認](#), 114 ページ
- [IM and Presence サービスの連絡先リスト内のコンタクト ID の変更](#), 116 ページ
- [Cisco Unified Communications Manager の Microsoft サーバのユーザ プロビジョニング](#), 118 ページ
- [ユーザの Microsoft サーバの連絡先リスト情報のバックアップ](#), 119 ページ
- [ユーザを移行するための連絡先リストのエクスポート](#), 119 ページ
- [Microsoft サーバのユーザの無効化](#), 125 ページ
- [ユーザを移行するためのデータベースからのユーザ データの削除](#), 128 ページ
- [IM and Presence にユーザを移行するための連絡先リストのインポート](#), 130 ページ
- [ユーザ... への IM and Presence サービスでサポートされているクライアントの導入](#), 132 ページ
- [連絡先リストと最大ウォッチャの最大サイズのリセット](#), 133 ページ

## シスコのユーザ移行ツール

シスコでは、Lync/OCS から IM and Presence サービスへのユーザの移行プロセスを支援するために、次のツールを提供しています。

- [連絡先リスト エクスポート ツール](#) : ユーザの移行用に Microsoft サーバから連絡先リストを一括でエクスポートすることができます。
- [アカウント無効化ツール](#) : 移行するユーザの Microsoft サーバアカウントを無効にできます。

- アカウント削除ツール：移行するユーザを Microsoft サーバから削除することで、それらのユーザへのプレゼンス要求が後から IM and Presence サービスにルーティングされるようになります。

これらのユーザの移行ツールは、[cisco.com](http://software.cisco.com/download/release.html?mdfid=286269517&flowid=50462&softwareid=282074312&release=UTILS&releind=AVAILABLE&relelifecycle=&reletype=latest) の IM and Presence サービス ソフトウェア ダウンロード ページ (<http://software.cisco.com/download/release.html?mdfid=286269517&flowid=50462&softwareid=282074312&release=UTILS&releind=AVAILABLE&relelifecycle=&reletype=latest>) から、zip ファイルとしてまとめてダウンロードできます。

zip ファイルには、3 つのツールと `version.txt` という名前のテキスト ファイルが含まれています。テキスト ファイルには、ツールの現在のバージョン番号が含まれており、ツールと同じフォルダに保存する必要があります。ツールが別のフォルダに保存されている場合は、それぞれの場所にテキスト ファイルのコピーを保存する必要があります。テキスト ファイルが同じフォルダになると、ツールの実行時にエラーが表示され、ツールが実行されません。



#### ヒント

ユーザ移行ツールのいずれかを実行しようとする時、「アプリケーションが正常な初期化に失敗しました (Application failed to initialize properly)」というエラーが表示される場合があります。このエラーの原因は、.NET 2.0 フレームワークのインストールされていないユーザ移行ツールを実行しようとしていることです。シスコが提供する各ユーザ移行ツールを使用するには、.NET Framework の少なくともバージョン 2.0 が、そのツールを実行している場所からサーバにインストールされている必要があります。

NET 2.0 フレームワークは、Windows Server 2003 R2 以降で標準としてインストールされています。

## 移行前の推奨事項

シスコでは、Lync/OCS から IM and Presence サービス にユーザを移行する前に次のタスクを実行するのを推奨しています。

- 無制限の連絡先リストとウォッチャの設定
- サブスクリプション要求の自動許可の有効化
- Microsoft Lync で新規ユーザ通知画面の表示を無効化

IM and Presence サービス IM アドレスはユーザの ID が移行中も維持されるように OCS/Lync SIP URI (`msRTCSIP-PrimaryUserAddress`) と一致するように設定できます。それが不可能な場合は、ユーザ名を変更する必要があります。

IM アドレス値をクラスタの IM and Presence サービス ノードに設定する詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。



## 無制限の連絡先リストとウォッチャの設定

Lync/OCS から IM and Presence サービスにユーザを移行する前に、IM and Presence サービスに関する [連絡先リストの最大サイズ (Maximum Contact List Size) ] と [ウォッチャの最大数 (Maximum Watchers) ] の設定を無制限に設定することをシスコでは推奨しています。そうすることで、移行されたユーザの各連絡先リストが IM and Presence サービスに完全にインポートされます。

すべてのユーザが IM and Presence サービスに移行されたら、IM and Presence サービスに関する [連絡先リストの最大サイズ (Maximum Contact List Size) ] と [ウォッチャの最大数 (Maximum Watchers) ] の設定を目的の値にリセットします。システムのデフォルト値は、[連絡先リストの最大サイズ (Maximum Contact List Size) ] が 200 で、[ウォッチャの最大数 (Maximum Watchers) ] が 200 です。

次の手順では、[連絡先リストの最大サイズ (Maximum Contact List Size) ] と [ウォッチャの最大数 (Maximum Watchers) ] の設定に無制限の値を設定する方法について説明します。



- (注) マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。[プレゼンス (Presence) ] の設定を変更すると、変更内容がクラスタ内のすべてのノードに適用されます。そのため、任意のクラスタ内の IM and Presence サービスデータベースのパブリック シャ ノードでのみ設定するようにしてください。

### 手順

- ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス (Presence) ] > [設定 (Settings) ] を選択します。
- ステップ 2 [連絡先リストの最大サイズ (ユーザごと) (Maximum Contact List Size (per user)) ] では、[制限なし (No Limit) ] チェックボックスをオンにします。
- ステップ 3 [ウォッチャの最大数 (ユーザごと) (Maximum Watchers (per user)) ] では、[制限なし (No Limit) ] チェックボックスをオンにします。
- ステップ 4 [保存 (Save) ] をクリックします。
- ステップ 5 クラスタ内のすべての IM and Presence サービス ノード上で Cisco XCP ルータを再起動します。Cisco XCP ルータを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[ツール (Tools) ] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services) ] を選択します。

## サブスクリプション要求の自動許可の有効化

移行中のユーザ エクスペリエンスを改善するために、シスコでは、移行プロセスを開始する前に、サブスクリプション要求の自動許可を許可することをお勧めします。そうしないと、IM and Presence サービスの各ユーザは、IM and Presence サービスに連絡先としてインポートされるごと

にサブスクリプション要求を手動で許可するように強制されます。この設定は、必要に応じて、すべての移行が完了した後に無効にする必要があります。

次の手順は、サブスクリプション要求の自動許可を有効にする方法について説明します。



(注) この設定は、IM and Presence サービス ではデフォルトで有効になっています。



(注) マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。[プレゼンス (Presence) ] の設定を変更すると、変更内容がクラスタ内のすべてのノードに適用されます。そのため、任意のクラスタ内の IM and Presence データベースのパブリッシャノードでのみ設定するようにしてください。

## 手順

- ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[プレゼンス (Presence) ] > [設定 (Settings) ] を選択します。
- ステップ 2 [承認を確認する画面表示なしに他のユーザのアベイラビリティを表示することをユーザに許可 (Allow users to view the availability of other users without being prompted for approval) ] チェックボックスをオンにします。
- ステップ 3 [保存 (Save) ] をクリックします。
- ステップ 4 クラスタ内のすべての IM and Presence サービス ノード上で Cisco XCP ルータを再起動します。Cisco XCP ルータを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール (Tools) ] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services) ] を選択します。

## サブスクリバ通知ポップアップ

Microsoft Lync から IM and Presence サービスにユーザを移行する場合は、Lyncに残っているユーザは移行されたユーザの加入者通知のポップアップを受信することがあります。この通知は、次の場合にのみ発生します。

- 移行されたユーザの連絡先リストに Microsoft Lync のユーザが含まれている  
および
- Microsoft Lync のユーザの連絡先リストには、移行された同じユーザが含まれていない

Microsoft Lync のユーザの連絡先一覧に移行された連絡先も存在する場合、通知ポップアップはありません。Microsoft Lync ユーザによって個々の通知ポップアップが処理されると、再び表示されることはありません。

Lync ユーザに新しい加入者通知ポップアップを受信させないようにする場合は、Lync のポップアップを無効化できます。これらの通知ポップアップを無効化するには2つのオプションがあります。

- ユーザの全移行期間中のポップアップを無効化できます。
- ユーザのバッチの移行時にのみポップアップを無効化できます。

ポップアップをディセーブルにすると、すべてのLyncユーザのすべてのポップアップは、再度有効にするまで無効になります。



(注) Microsoft Lync のポップアップを無効化および有効化するには、Lync フロントエンドサービスを再起動する必要があります。

## Microsoft Lync ポップアップの無効化

Microsoft Lync ユーザのすべてのポップアップを無効にする場合は、ユーザの移行またはバッチのユーザの移行を開始する前に次の手順を完了します。

### 手順

- ステップ 1** Lync のフロントエンドサーバで、[スタート (Start) ]>[すべてのプログラム (All Programs) ]>[Microsoft Lync Server 2010]>[Lync Server 管理シェル (Lync Server Management Shell) ]を選択します。
- ヒント Microsoft Lync サーバのバージョンに応じて、Microsoft Lync Server 2010 または 2013 を入力します。
- ステップ 2** 次の powershell コマンドを入力します。
- ```
Set-CSClientpolicy -EnableNotificationForNewSubscriber $False
```
- ステップ 3** [スタート (Start) ]>[プログラム (Programs) ]>[管理ツール (Administrative Tools) ]>[サービス (Services) ]を選択します。
- ステップ 4** サービス Lync フロントエンドサーバを右クリックして、[リスタート (Restart) ]を選択します。

## リストアの Microsoft Lync のポップアップ動作

Microsoft Lync ユーザの通知ポップアップのための前のクライアント動作を復元するには、ユーザを移行した後、または一括でユーザを移行した後に、次の手順を実行します。

### 手順

- ステップ 1** Lync でクライアントのポップアップ動作を復元するには、次のコマンドを入力します。
- ```
Set-CSClientpolicy -EnableNotificationForNewSubscribers $Null
```

- ステップ 2 [スタート (Start) ]>[プログラム (Programs) ]>[管理ツール (Administrative Tools) ]>[サービス (Services) ]を選択します。
- ステップ 3 サービス Lync フロントエンドサーバを右クリックして、[リスタート (Restart) ]を選択します。

## 移行するユーザ用の Microsoft サーバ SIP URI 形式の確認

次の手順を使用し、IM and Presence サービスに構成された IM アドレス形式が Microsoft サーバの IM アドレス形式と連携することを確認します。

IM and Presence サービスは 2 つの IM アドレス スキームをサポートします。Directory URI IM アドレス スキームを使用する場合は、IM and Presence サービスと Microsoft サーバ間の IM アドレス形式は連携します。ただし、*UserID@Default\_Domain* IM アドレス スキームを使用すると、IM アドレス スキームに不整合が生ずる可能性があります。

*UserID@Default\_Domain* IM アドレス スキーム URI は、Cisco Unified Communications Manager ユーザ ID を IM and Presence サービスのデフォルト ドメインと組み合わせて構成されます。いずれかの Lync/OCS URI が *UserID@Default\_Domain* IM アドレス形式に一致しない場合、移行するユーザの URI を変更する必要があります。Microsoft サーバユーザの各バッチを IM and Presence サービスに移行する前に、Microsoft サーバの URI のバッチを変更できます。



- (注) リリース 10.0(1) 以前のリリースについては、ユーザの最初のバッチを Microsoft サーバから IM and Presence サービスに移行する前にすべての Microsoft サーバ URI を変更する必要があります。

Directory URI IM アドレス スキームを使用する場合、Cisco Unified Communications Manager と IM and Presence サービス クラスタに設定されたドメインと異なるドメインの Microsoft サーバのユーザは、名前を変更する必要はありません。個々のユーザに異なる電子メールドメインを割り当てることができます。Microsoft サーバが異なるドメインにある場合、Microsoft サーバでドメイン間フェデレーションの IM and Presence サービスを設定し、フェデレーション機能に電子メールを設定する必要があります。

SIP URI 形式の詳細については、移行時のユーザの ID の維持に関するトピックを参照してください。

IM and Presence サービス IM アドレス スキームの詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

IM and Presence サービスと Microsoft サーバ間のドメイン間フェデレーションの設定の詳細については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』ガイドを参照してください。

## 手順

- 
- ステップ 1** IM アドレス スキームが Directory URI にセットされ、ディレクトリ URI が Cisco Unified Communications Manager の msRTCSIP-PrimaryUserAddress にマッピングされることを確認します。Directory URI IM アドレス スキームが設定されていて、適切にマッピングされている場合、連携が保証されます。IM and Presence サービスを設定して Directory URI アドレス スキームを使用できない場合は、次の手順に進みます。
- ステップ 2** IM and Presence サービスの現在の IM アドレス スキームの形式が Microsoft サーバで使用される形式と一致することを確認します。IM アドレス形式が連携しない場合、移行前に Microsoft サーバのユーザの名前を変更する必要があります。Microsoft サーバ SIP URI の変更の詳細については、次の手順を参照してください。
- 

## 次の作業

[IM and Presence サービスの連絡先リスト内のコンタクト ID の変更](#)、(116 ページ)

# Lync SIP URI の変更

Lync ユーザの SIP URI 形式を変更するには、次の手順を実行します。

## 手順

- 
- ステップ 1** Lync コントロール パネルから、[ユーザ (Users)] タブを選択します。
- ステップ 2** 変更するユーザを検索し、そのユーザをダブルクリックします。
- ステップ 3** [SIP アドレス (SIP address)] フィールドを変更します。
- ステップ 4** [確定する (Commit)] をクリックします。
- ヒント 複数の SIP URI を変更するには、`Set-CsUser` cmdlet を使用します。詳細については、<http://technet.microsoft.com/en-us/library/gg398510.aspx>を参照してください。
- 

## 次の作業

IM and Presence サービスの連絡先リスト内のコンタクト ID を変更します。

# OCS SIP URI の変更

OCS ユーザの SIP URI 形式を変更するには、Active Directory サーバで次の手順を実行します。

## 手順

- 
- ステップ 1** Active Directory サーバで、[スタート (Start)] > [コントロールパネル (Control Panel)] > [管理ツール (Administrative Tools)] > [Active Directory ユーザとコンピュータ (Active Directory Users and Computers)] 選択します。
- ステップ 2** 変更するユーザを検索し、そのユーザをダブルクリックします。
- ステップ 3** [プロパティ (Properties)] ウィンドウで [Live Communications] タブを選択します。
- ステップ 4** [SIP URI] フィールドを変更します。
- ステップ 5** [OK] をクリックします。
- (注) 複数の SIP URI を変更する場合は、Microsoft が提供する System.DirectoryServices を使用して、影響を受ける各ユーザの msRTCSIP-PrimaryUserAddress プロパティを更新します。詳細については、[http://msdn.microsoft.com/en-us/library/ms180835\(v=vs.80\).aspx](http://msdn.microsoft.com/en-us/library/ms180835(v=vs.80).aspx) を参照してください。
- 

## 次の作業

IM and Presence サービスの連絡先リスト内のコンタクト ID を変更します。

## IM and Presence サービスの連絡先リスト内のコンタクト ID の変更



- (注)
- この手順は、Lync/OCS SIP URI を変更した場合にのみ必要です。URI 形式の詳細については、移行時の維ユーザ ID の維持に関するトピックを参照してください。
  - IM and Presence サービスでは、変更された Microsoft サーバユーザをイネーブルにする前にこの手順を実行する必要があります。
  - このツールは、あらかじめスケジュールされたメンテナンスの時間帯に実行することを推奨します。

一連のユーザのコンタクト ID 名を変更する前に、コンタクト ID のリストとそれに対応する各コンタクト ID の新しい形式を含むファイルをアップロードする必要があります。ファイルは次の形式の CSV ファイルである必要があります。

<Contact ID>, <New Contact ID>

ここでは、[プレゼンス トポロジ ユーザ割り当て (Presence Topology User Assignment)] ウィンドウに表示されるため、Contact ID がユーザの IM アドレスです。

次に、1 つのエントリを持つ CSV ファイルのサンプルを示します。

```
Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com
```



- (注)
- 適切なコンタクト ID がある CSV ファイルをコンパイルする必要があります。
  - ヘッダーのコンタクト ID と新しいコンタクト ID がすべての CSV ファイルにあることを確認する必要があります。

ジョブを実行すると、IM and Presence サービス一括管理ツールは古いコンタクト ID を参照したユーザの連絡先リストを更新します。

CSV ファイルをアップロードして、ユーザのリストのコンタクト ID の名前を変更するには、次の手順を実行します。



- (注) 各IM and Presence サービス クラスタで次の手順を実行する必要があります。

### 手順

- ステップ 1** すべての連絡先リスト内で名前を変更する連絡先 ID のリストを含んだ CSV ファイルをアップロードします。次の手順を実行します。
- a) IM and Presence サービス データベース パブリッシュャ ノードで、[Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[一括管理 (Bulk Administration)] > [ファイルをアップロード/ダウンロード (Upload/Download Files)] を選択します。
  - b) [新規追加 (Add New)] をクリックします。
  - c) [参照 (Browse)] をクリックして、CSV ファイルを検索し選択します。
  - d) ターゲットとして [連絡先 (Contact)] を選択します。
  - e) トランザクションタイプとして [連絡先の名前変更 - カスタム ファイル (Rename Contacts - Custom File)] を選択します。
  - f) [保存 (Save)] をクリックして、ファイルをアップロードします。
- ステップ 2** パブリッシュャ ノードで [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[一括管理 (Bulk Administration)] > [連絡先リスト (Contact List)] > [コンタクト名を変更 (Rename Contacts)] を選択します。
- ステップ 3** [ファイル名 (File Name)] フィールドで、アップロードしたファイルを選択します。
- ステップ 4** 次のいずれかのアクションを選択します。
- 一括管理ジョブをただちに実行するには、[今すぐ実行 (Run Immediately)] をクリックします。

- 一括管理ジョブを実行する時間をスケジュールするには、[後で実行 (Run Later)] をクリックします。BAT でジョブをスケジュールする方法の詳細については、**Cisco Unified CM IM and Presence Administration** のオンラインヘルプを参照してください。

**ステップ 5** [送信 (Submit)] をクリックします。ジョブをただちに実行するように選択した場合は、[送信 (Submit)] をクリックするとジョブが実行されます。

#### 次の作業

[Cisco Unified Communications Manager の Microsoft サーバのユーザ プロビジョニング](#), (118 ページ)

## コンタクト ID のジョブの名前変更結果

[ジョブ スケジューラ (Job Scheduler)] ウィンドウ ([一括管理 (Bulk Administration)] > [ジョブ スケジューラ (Job Scheduler)]) からコンタクト ID の名前の変更ジョブの結果を確認できます。CSV ファイルのエントリ数によって、[一括管理ツール (Bulk Administration Tool)] はファイルの内容を数分で処理します。ただし、連絡先リストすべてを更新するには数時間かかる場合があります。この間に処理している [ジョブのステータス (Job Status)] が表示され、ジョブの現在の進行状態が [ジョブの結果 (Job Results)] セクションに表示されます。



(注) [ジョブ スケジューラ (Job Scheduler)] ページの [ジョブの結果 (Job Results)] 領域は CSV ファイルが処理されている場合にのみ表示されます。[処理されたレコードの数 (Number Of Records Processed)] の値と [失敗したレコードの数 (Number Of Records Failed)] の値は、CSV ファイルで処理されたエントリ数は表しません。これらの値は更新された連絡先リストの数と、更新に失敗した連絡先リストの数を表します。

コンタクト ID の名前が変更されると、Cisco Unified Communications Manager Lync/OCS のユーザをプロビジョニングすることができます。

## Cisco Unified Communications Manager の Microsoft サーバのユーザ プロビジョニング

Microsoft Lync または Microsoft Office Communications Server (OCS) から IM and Presence サービスにユーザを移行する最初の手順としては、Microsoft サーバのユーザを Cisco Unified Communications Manager にプロビジョニングし、IM and Presence サービスと IM and Presence サービスがサポートするクライアントに対してそれらのユーザにライセンスを付与します。





(注) ユーザが Cisco Unified Communications Manager と IM and Presence サービスでプロビジョニングされた後、同じメンテナンス時間帯に完全なユーザの移行プロセスを完了することを推奨します。ユーザを任意の時間帯 IM and Presence サービスと Microsoft サーバの両方にプロビジョニングすると、これらのユーザへのメッセージのルーティングは中断されます。

Cisco Unified Communications Manager での新規ユーザの設定、および IM and Presence サービスと IM and Presence がサポートするクライアントのライセンス要件については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

#### 次の作業

[ユーザの Microsoft サーバの連絡先リスト情報のバックアップ](#)

#### 関連トピック

[『Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager』](#)

## ユーザの Microsoft サーバの連絡先リスト情報のバックアップ

Lync/OCS は、dbimpexp.exe と呼ばれるツールを提供します。後日、必要に応じて Microsoft サーバに関する情報を復元できるように、このツールを使用して Microsoft サーバのユーザ連絡先リストの情報をバックアップすることをお勧めします。

IM and Presence サービスでサポートされているクライアントに Microsoft サーバユーザを移行するには、このツールを使用して個々の Microsoft サーバユーザまたはすべてのユーザの連絡先リストをバックアップできます。

#### 関連項目

dbimpexp.exe ツールの使用方法：[http://www.ocspedia.com/Misc/Explore\\_Dbimpexp.aspx?ArticleID=41](http://www.ocspedia.com/Misc/Explore_Dbimpexp.aspx?ArticleID=41)

#### 次の作業

[ユーザを移行するための連絡先リストのエクスポート](#)、(119 ページ)

## ユーザを移行するための連絡先リストのエクスポート

シスコは、管理者がユーザを移行するために Lync/OCS から連絡先リストを一括でエクスポートできるように、連絡先リストエクスポートツール (ExportContacts.exe) を提供します。ツールは、連絡先リストとエクスポートしてカンマ区切り値 (CSV) ファイルに出力するために、Microsoft サーバのアプリケーションプログラミングインターフェイス (API) を使用します。その後、IM

and Presence サービス 一括管理ツール (BAT) がこのファイルを使用し、これらの同じ連絡先リストを移行時に後から IM and Presence サービスにインポートできます。



(注)

- このツールはサポートされているすべての Microsoft サーバプラットフォームに対して実行できます。
- 任意の Standard Edition サーバまたは Enterprise Edition フロントエンドサーバで実行できます。
- Lync ユーザの連絡先リストをエクスポートするために、連絡先リストエクスポートツールは、Lync RTC データベースへの読み取りアクセスおよび LDAP への読み取りアクセスを要求します。また dbo の実行アカウント権限が RTC データベースに付与されることを確認する必要があります。
- このツールを実行しても、Microsoft Lync または Microsoft Office Communicator にログインしている他の Microsoft サーバユーザの機能には影響しません。ただし、シスコでは、Microsoft サーバおよび Active Directory システムへの負荷を減らすために、予定されたメンテナンス ウィンドウの中でこのツールを実行することをお勧めします。

このツールを実行すると、エクスポートした連絡先のリストを含むファイルが、ツールと同じディレクトリに作成されます。ファイル名は ExportedContacts<Timestamp>.csv になります。ファイルが作成されると、ファイル名にタイムスタンプが追加されるので、連絡先リストエクスポートツールを実行するたびに、一意の出力ファイルが作成されます。

また、連絡先リストエクスポートツールは、連絡先リストのエクスポート用に指定したユーザごとの Microsoft サーバ SIP URI を含む 2 番目のファイルも作成します。ファイル名は、UserList<Timestamp>.txt で、これもツールと同じディレクトリに作成されます。



(注)

UserList<Timestamp>.txt ファイルを連絡先リストエクスポートツールおよびアカウント無効化ツールの入力データとして使用できます。

## ログファイル

さらに連絡先リストエクスポートツールは、ツールを実行するたびに、出力ファイルと同じディレクトリ内に一意のタイムスタンプ付きのログファイルを作成します。ログファイルのファイル名は ExportContactsLog<Timestamp>.txt になります。

連絡先リストエクスポートツールを実行するたびに、ログファイルをチェックすることをお勧めします。その後、ログファイルをスキャンしてあらゆる問題を解決できます。各ログファイルの一番下に、次の情報が要約されています。

- 正常に処理されたユーザ数
- 見つからなかったユーザ数
- エラーが原因で処理されなかったユーザ数

- 連絡先リストの最大サイズ
- 見つかった連絡先の数
- 連絡先リストの平均サイズ

## 実行モード

連絡先リストエクスポート ツールには、NORMAL と STATSONLY という 2 つの実行モードがあります。NORMAL は、ツールを実行する標準的な方法です。このモードでは、エクスポートされた連絡先を含む CSV ファイル、ログ ファイル、およびユーザの Lync/OCS SIP URI ファイルという 3 つのファイルが作成されます。STATSONLY モードでは、連絡先リストエクスポート ツールはログファイルのみを作成します。このモードでツールを実行すると、エクスポートされた連絡先の CSV ファイルと Microsoft サーバの SIP URI ファイルを作成する前に、エラーがあればそれを発見して修正することができます。

## 入力ファイルの形式

連絡先リストエクスポート ツール (ExportContacts.exe) を使用すると、移行するユーザのリストを含む入力ファイルを指定できます。その後、このツールが、入力ファイルで指定されたユーザの連絡先リストを取得します。または、コマンドラインパラメータを指定することで、ローカル Lync/OCS データベース内のすべてのユーザの連絡先リストをエクスポートできます。



- (注) 連絡先リストエクスポート ツールですべてのユーザをエクスポートする場合、それらを IM and Presence サービスに移行するか否かに関係なく、結果として生成される UserList<Timestamp>.txt ファイルにはドメイン内のすべての Microsoft サーバで有効なユーザの連絡先リストが含まれます。後でアカウント無効化ツールおよびアカウント削除ツールへの入力として UserList<Timestamp>.txt ファイルを使用する場合、ドメイン内のすべてのユーザ アカウントがアカウント無効化ツールおよびアカウント削除ツールの影響を受けることに注意してください。

入力ファイルを使用する場合、次の入力ファイル形式がサポートされます。

### 入力ファイル形式 1 : Microsoft サーバ SIP URI

次の点に注意してください。

- 入力ファイルの各行は、連絡先リストの所有者を表します。
- 連絡先リストの所有者は、所有者の Microsoft サーバ SIP URI で表されます。たとえば、sip:bobjones@foo.com などです。
- 次のファイルは、サンプルの入力ファイルです。

```
sip:ann@foo.com
sip:bob@foo.com
sip:joe@foo.com
sip:chuck@foo.com
```

## 入力ファイル形式 2 : Active Directory 内の組織別のユーザ

この入力ファイル形式では、移行するユーザが含まれる Active Directory 内の組織単位 (OU) を指定できます。入力ファイルには、次の形式である必要があります。

```
DN:OU=OrgUnit1,OU=OrgUnit2,DC=DomainComp1,DC=DomainComp2
```

ここで、OrgUnit1 は、OrgUnit2 OU 内の OU で、DomainComp1 と DomainComp2 はドメイン コンポーネントです。ドメインには通常、たとえば cisco.com ドメインに対する cisco および com のように、AD 内の 2 つのドメイン コンポーネントが含まれます。

また、単一の入力ファイルに複数の識別名 (DN) を指定して、別の OU のユーザの連絡先リストをエクスポートできます。複数の DN が指定されている入力ファイルの形式は次のとおりです。

```
DN:OU=firstOU,DC=DomainComp1,DC=DomainComp2  
DN:OU=secondOU,DC=DomainComp1,DC=DomainComp2  
DN:OU=thirdOU,DC=DomainComp1,DC=DomainComp2
```

次の手順は、ユーザの移行用に Microsoft サーバから連絡先リストを一括でエクスポートする方法について説明します。

### 手順

- ステップ 1** Standard Edition サーバまたは Enterprise Edition フロント エンド サーバに、シスコのユーザ移行 ツールを含む zip ファイルをコピーし、解凍します。  
(注) 抽出した後、Microsoft サーバ上の別の場所にシスコのユーザ移行ツールのいずれかを移動した場合は、ツールが現在のバージョンを出力できるように新しい場所に version.txt ファイルもコピーする必要があります。
- ステップ 2** コマンド プロンプトを開き、連絡先リスト エクスポート ツールのある場所にディレクトリを変更します。
- ステップ 3** コマンド プロンプトで、次のようにツールを実行します。

目的	次のコマンドを入力
<p>Microsoft サーバ SIPURI 入力ファイルで指定されるユーザのリストの連絡先リストをエクスポートします。</p> <p>または</p> <p>AD入力ファイル内の組織単位別ユーザで指定したように、組織単位内のユーザのリスト用の連絡先リストをエクスポートする</p>	<p><b>ExportContacts.exe</b></p> <p><b>-s/LDAPServer-f/input_file-l/logLevel-r/run_mode-i/database_instance</b></p> <p>引数の説明</p> <ul style="list-style-type: none"> <li>• <b>LDAPServer</b> : Microsoft サーバユーザが保存される AD サーバの IP または FQDN</li> <li>• <b>input_file</b> : Microsoft サーバの SIP URI のリストを含むテキストファイル、または移行するユーザが含まれている AD の組織単位の識別名のリストを含むテキストファイル</li> <li>• <b>logLevel</b> : ロギング レベル。次のいずれかである必要があります。             <ul style="list-style-type: none"> <li>◦ error</li> <li>◦ info</li> <li>◦ debug (推奨)</li> </ul> </li> <li>• <b>run_mode</b> : 実行モード。次のいずれかである必要があります。             <ul style="list-style-type: none"> <li>◦ NORMAL</li> <li>◦ STATSONLY</li> </ul> </li> <li>• <b>database_instance</b> : Lync データ ストアのインスタンス名。このパラメータは、Lync ユーザの連絡先をエクスポートする場合にのみ必要です。</li> </ul> <p>入力例は次のとおりです。</p> <ul style="list-style-type: none"> <li>◦ Lync 2010 Standard Edition サーバ : localhost \ rtc</li> <li>◦ Lync 2010 Enterprise Edition サーバ : LyncDatastoreFqdn\rtc</li> <li>◦ Lync 2013 Standard Edition サーバ : localhost \ rtclocal</li> <li>◦ Lync 2013 Enterprise Edition サーバ : AnyLyncFrontendServer\rtclocal</li> </ul>

目的	次のコマンドを入力
<p>ドメインのすべての Microsoft サーバで有効なユーザの連絡先リストのエクスポート</p>	<pre><b>ExportContacts.exe -s/LDAPServer-f/ALL</b> <b>-l/logLevel-r/run_mode-i/database_instance</b></pre> <p>引数の説明</p> <ul style="list-style-type: none"> <li>• <b>LDAPServer</b> : Microsoft サーバユーザが保存される AD サーバの IP または FQDN</li> <li>• <b>logLevel</b> : ロギング レベル。次のいずれかである必要があります。 <ul style="list-style-type: none"> <li>◦ error</li> <li>◦ info</li> <li>◦ debug (推奨)</li> </ul> </li> <li>• <b>run_mode</b> : 実行モード。次のいずれかである必要があります。 <ul style="list-style-type: none"> <li>• NORMAL</li> <li>• STATSONLY</li> </ul> </li> <li>• <b>database_instance</b> : Lync データ ストアのインスタンス名。このパラメータは、Lync ユーザの連絡先をエクスポートする場合にのみ必要です。</li> </ul> <p>(注) このコマンドは、指定したドメインのすべての Microsoft サーバで有効なユーザの連絡先リストを、それらを IM and Presence サービスに移行するかどうかに関係なくエクスポートします。アカウント無効化ツールおよびアカウント削除ツールへの入力として UserList&lt;Timestamp&gt;.txt ファイルを使用する場合、ドメイン内のすべてのユーザアカウントがアカウント無効化ツールおよびアカウント削除ツールの影響を受けることに注意してください。</p>

(注) 正しい連絡先リストの移行を確認するには、連絡先リストを IM and Presence サービスにインポートする前に、エクスポートされた連絡先リストの所有者を Microsoft サーバで完全に無効にする必要があります。

次の作業

[Microsoft サーバのユーザの無効化](#)

関連トピック

[連絡先リスト エクスポート ツール, \(156 ページ\)](#)

# Microsoft サーバのユーザの無効化

ここでは、移行するユーザの Lync/OCS アカウントを無効化し、Active Directory の更新内容が Microsoft サーバに同期していることを確認する方法について説明します。

## 移行するユーザの Microsoft サーバアカウントの無効化

シスコでは、移行するユーザの Lync/OCS アカウントを無効にするツールを提供しています。このツール (DisableAccount.exe) は Active Directory (AD) に接続し、アカウントを無効にするユーザの Microsoft サーバ属性を更新します。アカウント無効化ツールの実行は、Microsoft のサーバで移行するユーザを無効にするために必要な 2 段階プロセスの最初の手順です。

- 1 移行するユーザの Microsoft サーバのユーザアカウントを無効にします。
- 2 移行するユーザの Microsoft サーバのユーザのデータを削除します。

移行するユーザのアカウントを無効にした後、削除ユーティリティに進む前に Microsoft サーバの LDAP 変更が同期されるまで待ちます。LDAP 同期は最大 30 分かかります。



(注)

- このツールは、サポートされているすべての Microsoft サーバプラットフォームで実行できます。
- 任意の Standard Edition サーバまたは Enterprise Edition フロントエンドサーバでこのツールを実行できます。
- このツールを実行しても、Microsoft Lync または Microsoft Office Communicator にログインしている他の Microsoft サーバユーザの機能には影響しません。ただし、シスコでは、Microsoft サーバおよび Active Directory システムへの負荷を減らすために、予定されたメンテナンス ウィンドウの中でこのツールを実行することをお勧めします。

アカウント無効化ツールは、次のように 3 つの入力を受け付けます。

- Microsoft サーバが存在する AD サーバの IP または FQDN
- 無効にする、Microsoft のサーバユーザアカウントのリストを含む入力ファイル
- エラー、情報、またはデバッグのいずれかでなければならないロギングレベル (デバッグが推奨設定)

アカウント無効化ツールは、入力ファイルから無効にするユーザのリストを読み込みます。入力ファイルの各行は、連絡先リストの所有者を表します。連絡先リストの所有者は、所有者の Microsoft サーバ SIP URI で表されます。たとえば、sip:bobjones@cisco.com などです。次のファイルは、サンプルの入力ファイルです。

```
sip:ann@cisco.com  
sip:bob@cisco.com
```

```
sip:joe@cisco.com
sip:chuck@cisco.com
```

上記の形式に基づいて独自の入力ファイルを作成できます。ただし、シスコでは、ファイル無効化ツールの入力ファイルとして、UserList<Timestamp>.txt ファイルを使用することをお勧めします。UserList<Timestamp>.txt ファイルには、重複したユーザ、無効なユーザ、または存在しないユーザは含まれません。

アカウント無効化ツールを実行すると、DisableAccountLog<Timestamp>.txt と呼ばれる一意のタイムスタンプが付加されたログファイルがツールと同じディレクトリに生成されます。ログファイルには、発生した障害やエラーに関する詳細が含まれています。

### はじめる前に

このツールを実行するには、AD に対する読み取り/書き込み権限が必要です。

### 手順

**ステップ 1** スタンダードエディションサーバまたは Enterprise Edition フロントエンドサーバに、シスコのユーザ移行ツールを含む zip ファイルをコピーし、解凍します。  
(注) 抽出した後、Microsoft サーバ上の別の場所にシスコのユーザ移行ツールのいずれかを移動した場合は、ツールが現在のバージョンを出力できるように新しい場所に version.txt ファイルもコピーする必要があります。

**ステップ 2** コマンドプロンプトを開き、アカウント無効化ツールのある場所にディレクトリを変更します。

**ステップ 3** コマンドプロンプトで、次のコマンドを入力します。

```
DisableAccount.exe -s/LDAPServer -f/input_file -l/logLevel
```

引数の説明

- **LDAPServer** : ユーザが存在する AD サーバの IP または FQDN
- **input\_file** : 無効にする Microsoft サーバ ユーザ アカウントのリストを含むファイルである UserList<Timestamp>.txt
- **logLevel** : エラー、情報、またはデバッグのいずれかでなければならないロギング レベル (デバッグが推奨設定)

**ステップ 4** アカウント無効化ツールを実行した後は、毎回、DisableAccountLog<Timestamp>.txt ログ ファイルをチェックし、すべてのユーザが正常に無効になったかを確認します。

### 次の作業

[Active Directory の更新が Microsoft サーバと同期していることの確認](#), (126 ページ)

## Active Directory の更新が Microsoft サーバと同期していることの確認

Lync/OCS アカウントを無効にするために Active Directory の更新が行われると、次のステップでは、Microsoft サーバにそれらの更新が同期されたかを確認します。検証は、無効化された Microsoft



サーバアカウントがプロビジョニングされた Standard Edition サーバまたは Enterprise Edition プールで実行されます。Microsoft サーバの LDAP 変更が削除ユーティリティに進む前に、同期するまで待つ必要があります。



(注) Microsoft サーバ配置によっては、これらの変更が Microsoft サーバに同期されるのに 30 分かかる場合があります。

## 手順

**ステップ 1** 配置に応じて、次のいずれかを実行します。

- Lync Server 2010 を使用する場合は、[スタート (Start) ]> [すべてのプログラム (All Programs) ]> [Microsoft Lync Server 2010]> [Lync Server コントロール パネル (Lync Server Control Panel) ] を選択します。

ヒント Microsoft Lync Server 2013 を使用する場合は、[Microsoft Lync Server 2013] を選択します。

- OCS 2007 R2 を使用する場合は、[スタート (Start) ]> [プログラム (Programs) ]> [管理ツール (Administrative Tools) ]> [Office Communications Server 2007 R2] を選択します。

**ステップ 2** 展開に応じて、次を確認してください。

- Lync の場合は、[ユーザ (Users) ] を選択し、無効化にされたユーザがユーザリストに表示されなくなったことを確認します。
- OCS の場合は、[ユーザ (Users) ] を選択し、無効化にされたユーザが有効な OCS ユーザリストに表示されなくなったことを確認します。

## 次の作業

[ユーザを移行するためのデータベースからのユーザデータの削除](#), (128 ページ)

## 関連トピック

[アカウント無効化ツール](#), (158 ページ)

# ユーザを移行するためのデータベースからのユーザデータの削除



(注) ユーザを移行するために Lync/OCS データベースからユーザデータを削除するには、Microsoft サーバのデータベースへの読み取り/書き込み権限を持っている必要があります。

Microsoft サーバは Microsoft サーバ データベースからユーザを削除するための管理方法を提供します。ただし、この方法でデータベースからユーザを削除すると、他のユーザの連絡先リストからそのユーザが削除されます。ユーザが他の Microsoft Lync または Microsoft Office Communicator ユーザの連絡先リストから削除されないようにするため、Microsoft サーバデータベースからユーザを削除する代替方法を提供します。

この代替ツール (DeleteAccount.exe) を使用すると、移行するユーザを削除することで、これらのユーザへの可用性要求が後から IM and Presence サービスにルーティングされるようになります。また、このツールは、削除されたユーザが Microsoft サーバに残っているユーザの連絡先リストから削除されないようにします。アカウント削除ツールの実行は、Microsoft サーバでユーザの移行を無効にするための次の 2 段階のプロセスの 2 番目のステップです。2 段階のプロセスは次のとおりです。

- 1 移行するユーザ用の Microsoft サーバでアカウントを無効にします。
- 2 移行するユーザの Microsoft サーバのユーザのデータを削除します。

移行するユーザのアカウントを無効にした後、削除ユーティリティに進む前に Microsoft サーバの LDAP 変更が同期されるまで待ちます。LDAP 同期は最大 30 分かかります。



- (注)
- このツールは、サポートされているすべての Microsoft サーバプラットフォームで実行できます。
  - 任意の Standard Edition サーバまたは Enterprise Edition プールでこのツールを実行できます。
  - このツールを実行しても、Microsoft Lync または Microsoft Office Communicator にログインしている他の Microsoft サーバユーザの機能には影響しません。ただし、シスコでは、Microsoft サーバおよび Active Directory システムへの負荷を減らすために、予定されたメンテナンス ウィンドウの中でこのツールを実行することをお勧めします。

アカウント削除ツールは、入力ファイルから削除するユーザのリストを読み込みます。入力ファイルの各行は、連絡先リストの所有者を表します。連絡先リストの所有者は、所有者の Microsoft サーバ SIP URI で表されます。たとえば、sip:bobjones@cisco.com などです。次のファイルは、サンプルの入力ファイルです。

```
sip:ann@cisco.com
sip:bob@cisco.com
sip:joe@cisco.com
sip@chuck@cisco.com
```

上記の形式に基づいて、独自の入力ファイルを作成できますが、シスコでは、ファイル削除ツールの入力ファイルとして、`UserList<Timestamp>.txt` ファイルを使用することをお勧めします。`UserList<Timestamp>.txt` ファイルには、重複したユーザ、無効なユーザ、または存在しないユーザは含まれません。

### Standard Edition の配置環境でのアカウント削除ツールの実行

ユーザのリストのデータを削除する際には、各 Standard Edition サーバで一度このツールを実行する必要があります。データベースは、Standard Edition サーバ上で混在します。

### Enterprise Edition の配置環境でのアカウント削除ツールの実行

ユーザのリストのデータを削除する際には、各 Enterprise Edition プールで一度このツールを実行する必要があります。Microsoft サーバのフロントエンドが接続する Lync/OCS データベース インスタンス名はツールの実行時に指定する必要があります。



#### 注意

Lync Enterprise Edition には、このツールを最初にバックエンドのデータベースサーバで、次に各フロントエンドサーバで実行する必要があります。Lync フロントエンドが接続する Lync のデータベース インスタンスの名前は、両方のオプションで指定する必要があります。フロントエンドサーバのデータベースの名前は `rtclocal` です。バックエンドサーバのデータベースのデフォルト名は `rtc` ですが、システムのインストール時に変更できます。

OCS Enterprise Edition のために、ツールはバックエンドデータベースサーバだけで実行する必要があります。

#### 手順

- ステップ 1** このツールを実行する前に、Microsoft サーバ データベースへの読み取り/書き込み権限があることを確認します。
- ステップ 2** Standard Edition サーバまたは Enterprise Edition プールサーバ（フロントエンドまたはバックエンド）の 1 つに、シスコのユーザ移行ツールを含む zip ファイルをコピーし、解凍します。  
 （注） 抽出した後、Microsoft サーバ上の別の場所にシスコのユーザ移行ツールのいずれかを移動した場合は、ツールが現在のバージョンを出力できるように新しい場所に `version.txt` ファイルもコピーする必要があります。
- ステップ 3** コマンドプロンプトを開き、アカウント削除ツールのある場所にディレクトリを変更します。
- ステップ 4** コマンドプロンプトで、次のようにコマンドを入力します。  
`DeleteAccount.exe -s/database_instance-f/input_file-l/logLevel`

#### 引数の説明

- `database_instance` : Lync/OCS プールまたは LCS プールの SQL サーバ インスタンスのデータベースのインスタンス名

- *input\_file* : 削除する Microsoft サーバユーザ アカウントのリストを含むファイルである `UserList<Timestamp>.txt`
- *logLevel* : エラー、情報、またはデバッグのいずれかでなければならないロギング レベル (デバッグが推奨設定)

(注) コマンドを実行すると、アカウント削除ツールによって `DeleteAccountLog<Timestamp>.txt` と呼ばれる一意のタイムスタンプが付加されたログ ファイルがツールと同じディレクトリに生成されます。ログファイルには、発生した障害やエラーに関する詳細が含まれています。

**ステップ 5** Standard Edition サーバまたは Enterprise Edition プールごとに、手順 1 ~ 3 を繰り返します。トラブルシューティングのヒントについては、[を参照してください。アカウント削除ツール](#), (159 ページ)

**ステップ 6** Lync データベースからユーザデータを削除すると、各フロントエンドサーバで手順 2~4 を繰り返して行う必要があります。フロントエンドサーバデータベースにアクセスするには、手順 4 のコマンドはフロントエンドサーバでローカルで実行する必要があります。さらに、データベース インスタンスのパラメータに `front-end_server_hostname\rtclocal` を値として使用する必要があります。

#### 次の作業

[IM and Presence にユーザを移行するための連絡先リストのインポート](#), (130 ページ)

## IM and Presence にユーザを移行するための連絡先リストのインポート

IM and Presence サービスの一括割り当てツール (BAT) を使用して、Lync/OCS ユーザ連絡先リストを IM and Presence サービスにインポートできます。

IM and Presence サービスに Microsoft サーバユーザの連絡先リストをインポートするには、次の手順を実行してください :

- 1 BAT を使用して CSV ファイルをアップロードします。
- 2 新しい一括管理ジョブを作成します。
- 3 一括管理ジョブの結果を確認します。



- (注) デフォルトの連絡先リストのインポート速度は、サーバハードウェアのタイプに基づいています。[Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインし、[システム (System)] > [サービス パラメータ (Service Parameters)] > [Cisco Bulk Provisioning Service] を選択することにより、連絡先リストのインポートレートを変更できます。ただし、デフォルトのインポート速度を上げると、IM and Presence サービスの CPU とメモリの使用率が増加します。

### はじめる前に

Microsoft サーバユーザの連絡先リストをインポートする手順は、ユーザ移行プロセスの最後のステップの1つです。Microsoft サーバユーザの連絡先リストをインポートする前に、以下の手順を完了する必要があります。

- 1 Cisco Unified Communications Manager 上で Microsoft サーバユーザをプロビジョニングします。
- 2 Microsoft サーバユーザがライセンスを取得し、IM and Presence サービスに割り当てられていることを確認します。
- 3 すべての連絡先リストが完全にインポートされるように、IM and Presence サービスの [連絡先リストの最大サイズ (Maximum Contact List Size)] と [ウォッチャの最大数 (Maximum Watchers)] の設定が無制限に設定されていることを確認します。 [無制限の連絡先リストとウォッチャの設定, \(111 ページ\)](#) を参照してください。
- 4 連絡先リスト エクスポート ツールを実行し、ExportedContacts<Timestamp>.csv ファイルを生成します。 [ユーザを移行するための連絡先リストのエクスポート, \(119 ページ\)](#) を参照してください。
- 5 Microsoft サーバユーザが Microsoft サーバで完全にディセーブルになっていることを確認します。 [Microsoft サーバのユーザの無効化, \(125 ページ\)](#) を参照してください。

## BAT を使用した CSV ファイルのアップロード

ExportedContacts<Timestamp>.csv ファイルを BAT を使用して IM and Presence サービスにアップロードする必要があります。CSV ファイルのアップロード方法の詳細は、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

### 関連項目

[『Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager』](#)

### 次の作業

[新しい一括管理ジョブの作成, \(132 ページ\)](#)

## 新しい一括管理ジョブの作成

CSV ファイルをアップロードしたら、**Cisco Unified CM IM and Presence Administration** ユーザ インターフェイスで新しい一括管理ジョブを作成し、ユーザ連絡先リストを更新する必要があります。新しい一括管理ジョブの作成方法に関する手順については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

### 関連項目

[Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager](#)

### 次の作業

[一括管理ジョブの結果](#), (132 ページ)

## 一括管理ジョブの結果

一括管理ジョブが完了すると、IM and Presence サービス BAT ツールは、連絡先リストのインポート ジョブの結果をログ ファイルに書き込みます。新しい一括管理ジョブの作成方法に関する手順については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

### 次の作業

[ユーザ... への IM and Presence サービスでサポートされているクライアントの導入](#), (132 ページ)

### 関連トピック

[Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager ユーザ移行のトラブルシューティング](#), (156 ページ)

## ユーザ... への IM and Presence サービスでサポートされているクライアントの導入

Lync/OCS ユーザを Cisco Unified Communications Manager にプロビジョニングし、IM and Presence サービス と IM and Presence サービスでサポートされているクライアントのライセンスを付与したら、ユーザデスクトップ上にクライアントソフトウェアをインストールできます。IM and Presence サービスにサポートされるクライアントの展開に関する詳細は、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

### 関連トピック

[『Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager』](#)

## 連絡先リストと最大ウォッチャの最大サイズのリセット

Lync/OCS から IM and Presence サービスにユーザを移行する前に、IM and Presence サービスに関する [連絡先リストの最大サイズ (Maximum Contact List Size)] と [ウォッチャの最大数 (Maximum Watchers)] の設定を無制限に設定することをシスコでは推奨しています。そうすることで、移行されたユーザの各連絡先リストが IM and Presence サービスに完全にインポートされます。

すべてのユーザが IM and Presence サービスに移行されたら、IM and Presence サービスに関する [連絡先リストの最大サイズ (Maximum Contact List Size)] と [ウォッチャの最大数 (Maximum Watchers)] の設定を目的の値にリセットします。システムのデフォルト値は、[連絡先リストの最大サイズ (Maximum Contact List Size)] が 200 で、[ウォッチャの最大数 (Maximum Watchers)] が 200 です。



(注) Microsoft サーバから IM and Presence サービスユーザの段階的な移行を実行する場合は、[連絡先リストの最大サイズ (Maximum Contact List Size)] と [ウォッチャの最大数 (Maximum Watchers)] をリセットしないでください。

次の手順では、[連絡先リストの最大サイズ (Maximum Contact List Size)] と [ウォッチャの最大数 (Maximum Watchers)] の設定に値を指定する方法について説明します。



(注) マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。[プレゼンス (Presence)] の設定を変更すると、変更内容がクラスタ内のすべてのノードに適用されます。そのため、任意のクラスタ内の IM and Presence サービスパブリッシャノードでのみ設定するようにしてください。

### 手順

- ステップ 1 [Cisco Unified IM and Presence Administration] ユーザインターフェイスにログインします。[プレゼンス (Presence)] > [設定 (Settings)] を選択します。
- ステップ 2 [連絡先リストの最大サイズ (ユーザごと) (Maximum Contact List Size (per user))] では、[制限なし (No Limit)] オプションをオフにし、希望する制限値を入力します。
- ステップ 3 [ウォッチャの最大数 (ユーザごと) (Maximum Watchers (per user))] では、[制限なし (No Limit)] オプションをオフにし、希望する制限値を入力します。
- ステップ 4 [保存 (Save)] をクリックします。
- ステップ 5 クラスタ内のすべての IM and Presence サービス ノード上で Cisco XCP ルータを再起動します。Cisco XCP ルータを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザインターフェイスにログインし、[ツール (Tools)] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] を選択します。







## 第 9 章

# ドメイン間フェデレーションとイントラドメインフェデレーション導入の統合

- [Microsoft サーバのドメイン間フェデレーション機能の IM and Presence サービスの統合, 135 ページ](#)
- [Microsoft サーバのドメイン間フェデレーション機能の IM and Presence サービスの統合, 136 ページ](#)
- [Microsoft サーバのドメイン内フェデレーション接続を介したドメイン間フェデレーションのリモートドメインのセットアップ, 137 ページ](#)
- [リモートドメインへのスタティックルートの設定, 138 ページ](#)
- [Microsoft サーバのドメイン間フェデレーション機能と IM and Presence サービス統合の削除, 140 ページ](#)

## Microsoftサーバのドメイン間フェデレーション機能のIM and Presence サービスの統合

Microsoft サーバのドメイン間フェデレーション機能の IM and Presence サービスを統合できます。Microsoft サーバは、リモート企業またはパブリック IM プロバイダーとのドメイン間フェデレーションフェデレーションをサポートしています。パーティションイントラドメインフェデレーションが Microsoft サーバおよび IM and Presence サービス間に設定されている場合、Microsoft Lync または Microsoft Office Communicator のユーザはこのドメイン間フェデレーション機能を使用できます。

さらに IM and Presence サービス対応クライアントに移行するユーザがまだ Microsoft サーバで設定されたドメイン間フェデレーション機能を使用できるように、IM and Presence サービスを設定できます。

IM and Presence サービスでのドメイン間フェデレーションフェデレーションの設定については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

## 連携動作と制限事項

- 統合されたドメイン間フェデレーションフェデレーションおよびパーティションイントラドメインフェデレーション導入がある場合は、フェデレーションに電子メールを使用しないでください。フェデレーションの電子メールアドレスは、パーティションイントラドメインフェデレーションが設定された導入ではサポートされません。Lync/OCS のドメイン間フェデレーション機能を使用する導入では、フェデレーションの電子メールアドレスはドメイン間フェデレーションでもサポートされません。フェデレーションの電子メールアドレスがこれらの導入シナリオの導入でイネーブルになっていないことを確認します。
- Microsoft サーバ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が有効な場合、SIP ベースおよびXMPP ベースの両方のドメイン間フェデレーションを IM and Presence サービスのリモートドメインに設定することもできます。ただし、このフェデレーション機能は IM and Presence サービス対応クライアントのユーザのみ使用できます。

## Microsoftサーバのドメイン間フェデレーション機能のIM and Presence サービスの統合

Microsoft サーバのドメイン間フェデレーション機能の IM and Presence サービスを統合できます。

Microsoft サーバは、リモート企業またはパブリック IM プロバイダーとのドメイン間フェデレーションフェデレーションをサポートしています。パーティションイントラドメインフェデレーションが Microsoft サーバおよび IM and Presence サービス間に設定されている場合、Microsoft Lync または Microsoft Office Communicator のユーザはこのドメイン間フェデレーション機能を使用できます。

さらに IM and Presence サービス対応クライアントに移行するユーザがまだ Microsoft サーバで設定されたドメイン間フェデレーション機能を使用できるように、IM and Presence サービスを設定できます。

IM and Presence サービスでのドメイン間フェデレーションフェデレーションの設定については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

# Microsoftサーバのドメイン内フェデレーション接続を介したドメイン間フェデレーションのリモートドメインのセットアップ

IM and Presence サービス ユーザは、既存の Lync/OCS ドメイン間フェデレーション接続または IM and Presence サービスで直接設定する外部ドメインへの接続を使用して、外部ドメインと通信できます。

既存の Microsoft サーバのドメイン内フェデレーション接続を介してドメイン間フェデレーションを設定する場合は、リモートドメインへのすべての要求は IM and Presence サービスと Microsoft のサーバ間の SIP インターフェイス経由でルーティングされます。既存のドメイン内フェデレーション接続を介してドメイン間フェデレーションを設定する前に Microsoft サーバ SIP フェデレーションドメインとして IM and Presence サービスのリモートドメインを設定する必要があります。各リモートドメインに対してこの作業を実行します。

SIP フェデレーションドメインの設定方法に関する手順については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』の SIP フェデレーションドメインの設定への追加に関連する手順を参照してください。

Microsoft サーバで設定されている既存のドメイン内接続を使用してドメイン間フェデレーションに SIP フェデレーションドメインを設定する際は、次のオプションの選択します。

- [ドメイン名 (Domain Name)] には、リモートドメインを入力します。
- [統合タイプ (Integration Type)] には、[ドメイン間から OCS/Lync (Inter-domain to OCS)] を選択します。
- [Direct Federation (ダイレクトフェデレーション)] のチェックボックスがオンになっていることを確認します。



(注) マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、任意のクラスタ内の IM and Presence サービス データベース パブリッシャ ノードでのみ設定する必要があります。

## 次の作業

[リモートドメインへのスタティックルートの設定](#), (138 ページ)

## 関連トピック

[『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』統合のトラブルシューティング](#), (143 ページ)

## リモートドメインへのスタティックルートの設定

Lync/OCS ドメイン間フェデレーション機能と IM and Presence サービスを統合する場合は、各リモートドメインの IM and Presence サービスでスタティックルートを設定する必要があります。



注意

フェデレーションの電子メールアドレスは、パーティションイントラドメインフェデレーションが設定された導入ではサポートされません。フェデレーションの電子メールアドレスは、Microsoft サーバのドメイン間フェデレーション機能を導入で使用する場合は、ドメイン間フェデレーションでもサポートされません。フェデレーションの電子メールアドレスがこれらの導入シナリオの導入でイネーブルになっていないことを確認します。

Standard Edition Microsoft サーバの場合、スタティックルートは特定の Standard Edition サーバの IP アドレスを指す必要があります。

Enterprise Edition Microsoft サーバの場合、スタティックルートは特定の Enterprise Edition フロントエンドサーバの IP アドレスをポイントする必要があります。

Microsoft サーバフロントエンドロードバランサを使用する場合、次の点に注意してください。

- ロードバランサのリストについては、次の URL を参照してください。 <http://technet.microsoft.com/en-us/office/ocs/cc843611> ロードバランサを導入し、正しく管理するのはお客様の責任です。シスコでは、そのようなロードバランサを指すようなスタティックルートの構成をサポートしていません。
- フロントエンドロードバランサをバイパスするためのスタティックルートを設定することをお勧めします。

ハイアベイラビリティのためには、追加のバックアップスタティックルートをリモートドメインごとに設定できます。バックアップルートの優先順位は低く、プライマリスタティックルートの次のホップアドレスに到達できない場合にのみ使用されます。



(注)

マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、任意のクラスタ内の IM and Presence サービスパブリッシャノードでのみ設定する必要があります。

## 手順

- 
- ステップ 1** [Cisco Unified Communications Manager IM and Presence Administration] ユーザーインターフェイスにリンクしています。 [プレゼンス (Presence) ] > [ルーティング (Routing) ] > [スタティックルート (Static Routes) ] を選択します。
- ステップ 2** [新規追加 (Add New) ] をクリックします。
- ステップ 3** ドメイン、つまり FQDN が元に戻るよう [宛先パターン (Destination Pattern) ] 値を入力します。たとえば、ドメインが remote.com である場合、宛先パターンの値 com.remote にならなければなりません。
- ステップ 4** [ルートタイプ (Route Type) ] で [domain] を選択します。
- ステップ 5** [ネクストホップ (Next Hop) ] フィールドに次のホップの IP アドレスを入力します。
- ステップ 6** [ネクストホップポート (Next Hop Port) ] および [プロトコルタイプ (Protocol Type) ] を次のように設定します。
- TLS 暗号化の場合：
    - [ネクストホップポート (Next Hop Port) ] の番号は **5061**
    - [プロトコルタイプ (Protocol Type) ] は、**TLS**
  - TCP の場合：
    - [ネクストホップポート (Next Hop Port) ] の番号は **5060**
    - [プロトコルタイプ (Protocol Type) ] は、**TCP**
- ステップ 7** [プライオリティ (Priority) ] 値を次のように入力します。
- プライマリスタティックルートについては、デフォルトの [プライオリティ (Priority) ] 値 **1** を入力します。
  - バックアップスタティックルートについては、1 より大きい [プライオリティ (Priority) ] 値を入力します (値が低いほど、スタティックルートの優先度が高くなります)。
- ステップ 8** 他のすべてのパラメータにはデフォルト値を選択します。
- ステップ 9** [保存 (Save) ] をクリックします。
- 

## 関連トピック

[統合のトラブルシューティング](#), (143 ページ)

## Microsoftサーバのドメイン間フェデレーション機能とIM and Presence サービス統合の削除

ある段階で、Lync/OCS 上で以前設定したリモート ドメインの 1 つを使用して、ドメイン間フェデレーションの IM and Presence サービスを設定したい場合があります。これに関して最も可能性の高いシナリオとしては、すべての Microsoft Lync または Microsoft Office Communicator ユーザが IM and Presence サービスに移行された場合などが考えられます。この時点で、Microsoft サーバの展開をシャットダウンし、すべてのドメイン間フェデレーション機能は、代わりに IM and Presence サービスから直接有効にできます。

Microsoft サーバのドメイン間フェデレーション機能と IM and Presence サービスの統合を削除するには、[リモート ドメイン用のスタティック ルートの削除](#)、[\(140 ページ\)](#) と [SIP フェデレーション ドメインの削除](#)、[\(140 ページ\)](#) を完了する必要があります。

### リモート ドメイン用のスタティック ルートの削除

#### 手順

- 
- ステップ 1 [Cisco Unified IM and Presence Administration] ユーザー インターフェイスにログインします。[プレゼンス (Presence) ]>[ルーティング (Routing) ]>[スタティック ルート (Static Routes) ]を選択します。
  - ステップ 2 表示されるリストから適切なスタティックルートを選択します。リストが表示されない場合、[検索 (Find) ]を選択します。
  - ステップ 3 [選択項目の削除 (Delete Selected) ]をクリックします。
  - ステップ 4 [OK] をクリックして削除を実行します。
- 

#### 次の作業

[SIP フェデレーション ドメインの削除](#)、[\(140 ページ\)](#)

### SIP フェデレーション ドメインの削除



- 
- (注) マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、任意のクラスタ内の IM and Presence サービス データベース パブリッシャ ノードでのみ設定する必要があります。
-

## 手順

- 
- ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。 [プレゼンス (Presence) ]>[ドメイン間フェデレーション (Inter Domain Federation) ]>[IP フェデレーション (SIP FederationS) ] を選択します。
  - ステップ 2 表示されたリストからドメインを選択します。 リストが表示されない場合、[検索 (Find) ] を選択します。
  - ステップ 3 [選択項目の削除 (Delete Selected) ] をクリックします。
  - ステップ 4 [OK] をクリックして削除を実行します。
- 

## 次の作業

リモートドメインへのスタティックルートを削除し、SIP フェデレーションドメインを削除したら、リモートドメインを使用してドメイン間フェデレーション用の IM and Presence サービスの設定に進むことができます。詳細については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。







# 第 10 章

## 統合のトラブルシューティング

- [IM and Presence サービスのトレース](#), 143 ページ
- [Microsoft サーバ SIP トレース](#), 146 ページ
- [統合の一般的な問題](#), 148 ページ
- [ユーザ移行のトラブルシューティング](#), 156 ページ

### IM and Presence サービスのトレース

IM and Presence サービス ノード上では、SIP Proxy が SIP 要求のルーティングを担当し、XCP SIP Federation Connection Manager は、Microsoft SIP とネイティブ XMPP 間の SIP プロトコル変換を担当します。したがって、これらのサービスは IM and Presence サービスと Lync/OCS 間の SIP パーティションイントラドメインフェデレーション統合の中心となります。

XCP ルータは、IM and Presence サービスの中核サービスです。要求の受信者が Microsoft サーバか IM and Presence サービス ユーザであるかどうかで決まります。

ログファイルの場所は次のとおりです。

- XCP SIP Federation Connection Manager のログ : `/var/log/active/epas/trace/xcp/log/sip-cm-3_000*.log`
- SIP Proxy のログ : `/var/log/active/epas/trace/esp/sdi/esp000*.log`
- XCP Router のログ : `var/log/active/epas/trace/xcp/log/rtr-jsm-1_000*.log`

#### SIP Proxy のログの例

```
2:26:18.719 |PID(25333) sip_protocol.c(5964) Received 536 bytes TCP packet
  from 10.53.56.17:34282SUBSCRIBE sip:ysam@implync.net SIP/2.0^M
From:
<sip:fbear@implync.net>;tag=a4cdaec0-1138350a-13d8-45026-4d755b8a-2162aa7a-4d755b8a^M

To: <sip:ysam@implync.net>^M
Call-ID: a30386f0-1138350a-13d8-45026-4d755b8a-2c25871c-4d755b8a^M
```

```

CSeq: 1 SUBSCRIBE^M
Via: SIP/2.0/TCP
10.53.56.17:5080;branch=z9hG4bK-4d755b8a-926d95b4-3c330144^M
Expires: 7446^M
Accept: application/pidf+xml, application/cpim-pidf+xml^M
User-Agent: Cisco-Systems-Partitioned 8.0^M
Max-Forwards: 70^M
Event: presence^M
Contact: <sip:10.53.56.17:5080;transport=TCP>^M
Content-Length: 0^M
...
22:26:18.719 |ID(25333) sip_sm.c(4977) SIPGW Partitioned Fed UA Header
found in this request
22:26:18.719 |ID(25333) sip_sm.c(5010) This is a partitioned federation
request, skip User Location DB lookup
22:26:18.719 |ID(25333) sip_sm.c(5200) This is an outbound Partitioned
federation request.
22:26:18.719 |Mon Mar 07 22:26:18 2011] PID(25333) mod_sip_routing.c(1435)
Routing: dipping for cuplcs.net
22:26:18.719 |Mon Mar 07 22:26:18 2011] PID(25333) mod_sip_routing.c(1473)
Routing: Found domain route for cuplcs.net:10.53.56.18:5061;TLS pwf 1:1:5
22:26:18.719 |ID(25333) sip_dns.c(811) "A" Query for 10.53.56.18
successful, Got 1 IP addresses
22:26:18.719 |ID(25333) sip_dns.c(139) A Record : 10.53.56.18

```

### SIP Federation Connection Manager のログの例

次の例は、発信要求ログから抽出したものです。

```

21:48:44.277 |SIPGWDir.cpp:463: [FROM XMPP] <presence
from='fbear@implync.net' to='ysam@implync.net' type='probe'>...
...
21:48:44.743 |SIPGWController.cpp:622: Skipping DNS lookup: <presence
from='fbear@implync.net' to='ysam@implync.net' type='probe'>
21:48:44.743 |SIPGWController.cpp:704: Entering _handleOutContinue:
<presence from='fbear@implync.net' to='ysam@implync.net' type='probe'>
21:48:44.743 |SIPGWController.cpp:989: _findSession (JID):
local (fbear@implync.net) remote (ysam@implync.net)
21:48:44.743 |SIPGWController.cpp:999: _findSession: Session not found
21:48:44.743 |SIPHostInfo.cpp:82: hostinfo(0x09a10ce8) refInc: 3
cuplcs.net:cuplcs.net
21:48:44.743 |SIPGWSession.cpp:58: Creating SIPGWSession sess=0x09a5a090
local=fbear@implync.net remote=ysam@implync.net
21:48:44.743 |SIPGWController.cpp:1017: _findSession: Made new session:
sess=0x09a5a090 local (fbear@implync.net) remote (ysam@implync.net)
21:48:44.743 |SIPGWSession.cpp:990: sess=0x09a5a090 Entering handleOut:
<presence from='fbear@implync.net' to='ysam@implync.net' type='probe'>
21:48:44.743 |SIPGWSession.cpp:1090: _createOutgoingSubs
local=fbear@implync.net, remote=ysam@implync.net
48:44.744 |SIPSubs.cpp:1037: from=<sip:fbear@implync.net>
to=<sip:ysam@implync.net> local_contact=sip:10.53.56.17:5080;transport=TCP
remote_contact=sip:ysam@implync.net

```

### XCP Router のログの例

```

12:29:24.762 |debug sdns_plugin-1.gwydlvm453 sdns_plugin handling:<presence
type='subscribed' to='ysam@implync.net'

```

```
from='bbird@implync.net'><status>Already Subscribed</status></presence>
12:29:24.762 |debug ConnectionPool.cpp:166 connection pool checkout:
ccm2/dbuser (success)
12:29:24.762 |debug IdsODBC.cpp:648 Performing SQL operation select userid,
jsmid from enduser, enterprisenode where my_lower(xep106userid) =
my_lower(?) and primarynodeid=id
12:29:24.763 |debug ODBCConnection.cpp:315 (elapsed 0.002407) select
userid, jsmid from enduser, enterprisenode where my_lower(xep106userid)
= my_lower(?) and primarynodeid=id
12:29:24.763 |debug CUPDatabaseAlgorithm.cpp:311 This is probably a
Partitioned OCS user ... redirecting to cm-3-sip-fed-s2s.gwydlvm453
component
12:29:24.763 |debug IdsODBC.cpp:229 (elapsed 0.000137) rollback
12:29:24.763 |debug ConnectionPool.cpp:207 connection pool checkin:
ccm2/dbuser (success)
12:29:24.763 |debug sdns_plugin-1.gwydlvm453 sdns_plugin redirecting to:
cm-3-sip-fed-s2s.gwydlvm453
```

[Cisco Unified IM and Presence Service Serviceability] ユーザ インターフェイス上では、SIP Proxy、XCP SIP Federation Connection Manager、および XCP Router のデバッグ トレースを有効にできます。

## IM and Presence サービスのトレースの設定

次の手順では、[Cisco Unified IM and Presence Serviceability] GUI 上で、SIP Proxy、XCP SIP Federation Connection Manager、および XCP Router のデバッグ トレースを設定する方法について説明します。トレース用に設定するサービスごとに、この手順を繰り返します。



### 注意

デバッグ レベル トレースは、システム パフォーマンスに影響を与えることがあります。必要などきのみデバッグ トレース レベルを有効にし、システム調査が完了した後、ログの設定をデフォルトにリセットします。

### 手順

- ステップ 1 [Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[トレース (Trace)] > [設定 (Configuration)] を選択します。
- ステップ 2 IM and Presence サービス ノードを選択し、[移動 (Go)] を選択します。
- ステップ 3 [サービス グループ (Service Group)] ドロップダウン リストから [IM and Presence サービス (IM and Presence Services)] を選択し、[移動 (Go)] を選択します。
- ステップ 4 [サービス (Service)] ドロップダウン リストから、次のオプションの 1 つを選択し、[移動 (Go)] をクリックしてください。
  - a) Cisco SIP Proxy
  - b) Cisco XCP SIP Federation Connection Manager

c) Cisco XCP Router

**ステップ 5** [トレース (Trace On)] のチェックボックスをオンにします。

**ステップ 6** [フィルター設定をトレース (Trace Filter Settings)] 領域で、ドロップダウンリストから [デバッグ トレース レベル (Debug Trace Level)] を選択します。トレースに対してデバッグ レベル トレースを有効にしたい場合は、[デバッグ (Debug)] を選択します。

**ステップ 7** SIP Proxy 向けにトレースを有効にする場合、[トレース フィルタ設定 (Trace Filter Settings)] にさまざまなトレース オプションがあります。次のトレースのチェックボックスをオンにします。

a) SIP TCP のトレースのイネーブル化 (Enable SIP TCP Trace)

b) SIP TLS のトレースのイネーブル化 (Enable SIP TLS Trace)

c) Server のトレースのイネーブル化 (Enable Server Trace)

d) SIP メッセージとステート マシンのトレースのイネーブル化 (Enable SIP Message and State Machine Trace)

e) Method/Event ルーティングのトレースのイネーブル化 (Enable Method/Event Routing Trace)

f) Routing のトレースのイネーブル化 (Enable Routing Trace)

**ステップ 8** [保存 (Save)] をクリックします。

これらのサービスごとにデバッグ トレースを開始するための詳細については、Cisco Unified IM and Presence Serviceability オンライン ヘルプを参照してください。

---

#### 関連トピック

[Microsoft サーバ SIP トレース, \(146 ページ\)](#)

## Microsoft サーバ SIP トレース

Lync/OCS SIP Proxy コンポーネントは、すべての SIP 要求のルーティングを行います。ルーティングの問題をデバッグするには、Microsoft サーバに固有のメソッドを使用して Microsoft サーバのデバッグ トレース (Standard Edition または Enterprise Edition) をイネーブルにできます。

### Lync での SIP トレースの有効化

次の手順は、Lync 上で SIP トレースを有効にする方法について説明します。

## 手順

- 
- ステップ 1 [スタート (Start)] > [すべてのプログラム (All Programs)] > [Microsoft Lync Server 2010] > [Lync Server ログ ツール (Lync Server Logging Tool)] を選択します。
  - ステップ 2 [コンポーネント (Component)] 領域で、[SIPStack] チェックボックスをオンにします。
  - ステップ 3 [ロギング レベル (Logging Level)] を [すべて (All)] に設定し、[ログの開始 (Start Logging)] を選択します。
  - ステップ 4 トレース停止の準備が整ったら、[ログの停止 (Stop Logging)] を選択します。
  - ステップ 5 [ログファイルの分析 (Analyze Log Files)] を選択し、ログを表示します。
  - ステップ 6 ログのより構造化された分析を行うには、Snooper ツールをダウンロードし、それを使ってログファイルを表示します。
- 

## 関連トピック

[IM and Presence サービスのトレース、\(143 ページ\)](#)  
[Snooper ツール](#)

# OCS 上での SIP トレースの有効化

次の手順は、OCS 上で SIP トレースを有効にする方法について説明します。

## 手順

- 
- ステップ 1 [スタート (Start)] > [プログラム (Programs)] > [管理ツール (Administrative Tools)] > [Office Communications Server 2007 R2] を選択します。
  - ステップ 2 エディションに応じて、次のいずれかを実行します。
    - a) スタンダードエディションを使用する場合は、OCS サーバ名を右クリックして、[ログ ツール (Logging Tool)] > [新しいデバッグセッション (New Debug Session)] を選択します。
    - b) Enterprise Edition を使用する場合は、OCS プール名を右クリックし、[ログ ツール (Logging Tool)] > [新しいデバッグセッション (New Debug Session)] を選択します。
  - ステップ 3 [コンポーネント (Components)] 領域で [SIP スタック (SIPStack)] チェックボックスをオンにし、[レベル (Level)] 領域で [すべて (All)] をクリックします。
  - ステップ 4 ロギングを開始する準備が整ったら、[ログの開始 (Start Logging)] を選択します。
  - ステップ 5 ロギングを停止する準備が整ったら、[ログの停止 (Stop Logging)] を選択します。
  - ステップ 6 OCS SIP Proxy ログ分析を表示するには、[ログ ファイルの解析 (Analyze Log Files)] を選択します。
-

## 関連トピック

[IM and Presence サービスのトレース](#), (143 ページ)

[Snooper ツール](#)

## 統合の一般的な問題

ここでは、統合の一般的な問題について説明します。

### Lync の 2013 クライアントが、IM and Presence サービス ユーザを連絡先リストに追加した後、繰り返しログアウトおよびログインする

## トラブルシューティングの手順

- 1 必要なすべてのアクセス コントロール リスト (ACL) エントリが IM and Presence サービスに追加され、任意の ACL エントリを追加した後に Cisco Sip Proxy サービスが再起動されたことを確認します。
- 2 問題が続く場合は、すべての ACL エントリを追加し、Cisco SIP Proxy を再起動します。

ACL エントリ追加の詳細については、着信アクセス コントロール リストの設定に関するトピックを参照してください。

### Microsoft サーバのユーザを IM and Presence サービス連絡先リストに追加すると、ポップアップを受信しない

## トラブルシューティングの手順

- 1 連絡先について有効な利用可能状態が表示されている場合は、Microsoft Lync または Microsoft Office Communicator のユーザが以前に IM and Presence サービスのクライアント ユーザからの登録を受け入れているかどうかを確認します。

Microsoft サーバ サブスクリプションの承認は永久なので、IM and Presence サービスのクライアント ユーザが Microsoft Lync または Microsoft Office Communicator のユーザを削除して、再度追加すると、2 番目のポップアップが表示されないことを意味します。

- 2 連絡先に「確認の待機中 (Waiting for“”Confirmation)」状態が表示される場合は、必要に応じて残りのトラブルシューティング手順を実行します。
  - 連絡先の MOC SIP URI が有効なことを確認します。
  - Cisco SIP Proxy および Cisco SIP Federation Connection Manager サービスが各 IM and Presence サービス ノードで実行中であることを確認します。

Microsoft サーバのユーザを IM and Presence サービスの連絡先リストに追加すると、ポップアップを受信するが、承認後のアベイラビリティがない

- パーティションイントラドメインフェデレーションが IM and Presence サービス クラスタごとに有効であることを確認します。
- パーティション化されたフェデレーションのルーティング モードが選択した導入に適用されるか確認します。
- 拡張ルーティングは、シングル クラスタの IM and Presence サービス 導入でのみサポートされています。
- IM and Presence サービス スタティック ルートが Microsoft サーバへの要求をルーティングするように正しく設定されているか確認します。 これを行うには、IM and Presence サービス ユーザのホーム ノードにある SIP Proxy ログを確認し、SIP Proxy が Microsoft サーバに対する SIP NOTIFY 要求の SIP 408 要求タイムアウト エラーを返すかどうか確認します。  
また、IM and Presence サービスのスタティック ルートが OCS/Lync ユーザのドメインにあることを確認します。
- TLS 暗号化が設定されている場合、Wireshark または同等の監視ツールを使用して、TLS ハンドシェイクが成功したことを確認します。
- それでも TLS ハンドシェイクが失敗する場合、さらなる TLS トラブルシューティング手順について [IM and Presence サービスおよび Microsoft サーバ間の TLS ハンドシェイク エラー](#)、(155 ページ) をご覧ください。
- Microsoft Server ホスト認証エントリが SIP NOTIFY を送信する IM and Presence サービス ノードにあることを確認します。
- 少なくとも IM and Presence サービス ノードごとに IP アドレス エントリが存在する必要があります。
- TLS 暗号化を設定すると、IM and Presence サービス ノード向けに 2 つ目の FQDN エントリも必要になります。

## Microsoft サーバのユーザを IM and Presence サービスの連絡先リストに追加すると、ポップアップを受信するが、承認後のアベイラビリティがない

### トラブルシューティングのヒント

IM and Presence サービスのアクセス コントロール リスト (ACL) がすべての Lync/OCS サーバ/プールからの要求を許可することを確認します。ACL の問題がある場合は、IM and Presence サービス ノードのルーティングの SIP Proxy ログの中に、「ACL - 信頼されていないアップストリーム - 認証が必要 (ACL - upstream not trusted - need to authenticate)」というエントリが表示されます。

## Microsoft Lync または Microsoft Office Communicator ユーザが連絡先リストにユーザを追加した場合に IM and Presence サービス ユーザにポップアップが表示されない

### トラブルシューティングの手順

- 1 有効な利用可能状態が表示されている場合は、ローカルのプレゼンス ドメイン内のユーザからのサブスクリプション要求を自動的に承認するように IM and Presence サービスが設定されているか確認します。この機能が有効な場合、IM and Presence サービスは IM and Presence サービス ユーザにポップアップを表示することなく、自動的に要求を承認します。
- 2 そうでない場合、「“ステータスが不明 (Status Unknown) ”」または「“プレゼンスが不明 (Presence Unknown) ”」と表示される場合は、必要に応じて残りのトラブルシューティング手順を実行します。
- 3 Cisco SIP Proxy および Cisco SIP Federation Connection Manager サービスが各 IM and Presence サービス ノードで実行中であることを確認します。
- 4 パーティションイントラドメイン フェデレーションが IM and Presence サービス クラスタごとに有効であることを確認します。
- 5 パーティション化されたフェデレーションのルーティングモードが選択した導入に適用されるか確認します。  
拡張ルーティングは、シングル クラスタの IM and Presence サービス導入でのみサポートされています。
- 6 TLS 暗号化が設定されている場合、Wireshark または同等の監視ツールを使用して、TLS ハンドシェイクが成功したことを確認します。
- 7 それでも TLS ハンドシェイクが失敗する場合、さらなる TLS トラブルシューティング手順について [IM and Presence サービスおよび Microsoft サーバ間の TLS ハンドシェイク エラー](#)、(155 ページ) をご覧ください。
- 8 ルーティング IM and Presence サービス ノードをポイントするスタティックルートが Lync/OCS Standard Edition サーバまたは Enterprise Edition プールごとに設定されていることを確認します。スタティックルートも、IM and Presence サービスで構成された各 IM のユーザのドメインに設定する必要があります。
- 9 各 IM and Presence サービス ノードが Microsoft サーバの配置からドメイン ネーム サービス (DNS) によって解決可能であることを確認します。
- 10 Microsoft サーバホスト認証のエントリが SIP NOTIFY メッセージを送信している IM and Presence サービス ノードに存在していることを確認します。
  - a 少なくとも IM and Presence サービス ノードごとに IP アドレス エントリが存在する必要があります。



- b TLS 暗号化を設定すると、IM and Presence サービス ノード向けに 2 つ目の FQDN エントリも必要になります。
- 11 IM and Presence サービスのアクセス コントロール リスト (ACL) がすべての Microsoft サーバ/プールからの要求を許可することを確認します。ACL の問題がある場合は、IM and Presence サービス ノードのルーティングの SIP Proxy ログの中に、「ACL - 信頼されていないアップストリーム - 認証が必要 (ACL - upstream not trusted - need to authenticate)」というエントリが表示されます。
  - 12 これがマルチクラスタ IM and Presence サービスの配置である場合は、クラスタ間ピアリングが正しく設定されていることを確認します。
    - a [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。宛先ルーティング IM and Presence サービス ノードを含むクラスタのパブリッシャ ノードで [プレゼンス (Presence)] > [クラスタ間 (Inter-Clustering)] を選択します。
    - b クラスタ間ピアのリストに IM and Presence サービス ユーザがプロビジョニングされているクラスタ向けのピアが含まれていること、およびそのピアに関連付けられたユーザの数が 0 より大きいことを確認します。
    - c クラスタ間ピアのステータスを検証するために、クラスタ間ピアを選択します。
    - d 強調表示されたエラーが存在しないことを確認してください。

## IM and Presence サービスのユーザが送信した IM を Microsoft サーバのユーザが受信しない

### トラブルシューティングの手順

- 1 Cisco SIP Proxy および Cisco SIP Federation Connection Manager サービスが各 IM and Presence サービス ノードで実行中であることを確認します。
- 2 パーティションイントラドメイン フェデレーションが IM and Presence サービス クラスタごとに有効であることを確認します。
- 3 パーティション化されたフェデレーションのルーティングモードが選択した導入に適用されるか確認します。

拡張ルーティングは、シングル クラスタの IM and Presence サービス導入でのみサポートされています。
- 4 IM and Presence サービス スタティック ルートが Lync/OCS に要求をルーティングするように正しく設定されているか確認します。これを行うには、IM and Presence サービス ユーザのホーム ノードにある SIP Proxy ログを確認し、SIP Proxy が Microsoft サーバに対する SIP INVITE 要求の SIP 408 要求タイムアウト エラーを返すかどうか確認します。

また、IM and Presence サービスのスタティック ルートが OCS/Lync ユーザのドメインにあることを確認します。

- 5 TLS 暗号化が設定されている場合、Wireshark または同等の監視ツールを使用して、TLS ハンドシェイクが成功したことを確認します。
- 6 それでも TLS ハンドシェイクが失敗する場合、さらなる TLS トラブルシューティング手順について [IM and Presence サービスおよび Microsoft サーバ間の TLS ハンドシェイク エラー](#)、(155 ページ) をご覧ください。
- 7 Microsoft サーバホストの認証エントリが SIP INVITE 要求を送信する IM and Presence サービス ノードにあることを確認します。
  - a 少なくとも IM and Presence サービス ノードごとに IP アドレス エントリが存在する必要があります。
  - b TLS 暗号化を設定すると、IM and Presence サービス ノード向けに 2 つ目の FQDN エントリも必要になります。

## Microsoft サーバユーザによって送信された IM を IM and Presence ユーザが受信しない

### トラブルシューティングの手順

- 1 Cisco SIP Proxy および Cisco SIP Federation Connection Manager サービスが各 IM and Presence サーバノードで実行中であることを確認します。
- 2 パーティションイントラドメインフェデレーションが IM and Presence サービス クラスタごとに有効であることを確認します。
- 3 パーティション化されたフェデレーションのルーティングモードが選択した導入に適用されるか確認します。

拡張ルーティングは、シングルクラスタの IM and Presence サービス導入でのみサポートされています。
- 4 Microsoft Lync の場合、TLS 暗号化が設定されていることを確認します。
- 5 TLS 暗号化が設定されている場合、Wireshark または同等の監視ツールを使用して、TLS ハンドシェイクが成功したことを確認します。
- 6 それでも TLS ハンドシェイクが失敗する場合、さらなる TLS トラブルシューティング手順について [IM and Presence サービスおよび Microsoft サーバ間の TLS ハンドシェイク エラー](#)、(155 ページ) をご覧ください。
- 7 ルーティング IM and Presence サービス ノードをポイントするスタティックルートが Lync/OCS Standard Edition サーバまたは Enterprise Edition プールごとに設定されていることを確認します。

また、IM and Presence サービス スタティックルートが Microsoft サーバユーザのドメインにあることを確認します。

- 8 各 IM and Presence サービス ノードが Microsoft サーバの配置から DNS によって解決可能であることを確認します。
- 9 Microsoft サーバホストの許可エントリが SIP INVITE を送信している IM and Presence サービス ノードに存在していることを確認します。
  - a 少なくとも IM and Presence サービス ノードごとに IP アドレス エントリが存在する必要があります。
  - b TLS 暗号化を設定すると、IM and Presence サービス ノード向けに 2 つ目の FQDN エントリも必要になります。
- 10 IM and Presence サービスのアクセス コントロール リスト (ACL) がすべての Microsoft サーバ/プールからの要求を許可することを確認します。ACL の問題がある場合は、IM and Presence サービス ノードのルーティングの SIP Proxy ログの中に、「ACL - 信頼されていないアップストリーム - 認証が必要 (ACL - upstream not trusted - need to authenticate)」というエントリが表示されます。
- 11 これがマルチクラスタ IM and Presence サービスの配置である場合は、クラスタ間ピアリングが正しく設定されていることを確認します。
  - a [Cisco Unified Communications Manager IM and Presence Administration] ユーザ インターフェイスにログインします。宛先ルーティング IM and Presence サービス ノードを含むクラスタのパブリッシャ ノードで [プレゼンス (Presence)] > [クラスタ間 (Inter-Clustering)] を選択します。
  - b クラスタ間ピアのリストに IM and Presence サービス ユーザがプロビジョニングされているクラスタ向けのピアが含まれていること、およびそのピアに関連付けられたユーザの数が 0 より大きいことを確認します。
  - c クラスタ間ピアのステータスを検証するために、クラスタ間ピアを選択します。
  - d 強調表示されたエラーが存在しないことを確認してください。

## Microsoft サーバの更新と IM の表示に最大 40 秒かかる

### トラブルシューティングの手順

このような遅延の最も一般的な理由は、配置内の DNS の設定が不足していることです。IM and Presence サービスは、着信 SIP 要求の送り側となる Lync/OCS の IP アドレスのリバース DNS 検索を実行します。IP アドレスがホスト名に解決されない場合、逆検索は約 20 秒後にタイムアウトします。これが発生すると、SIP Proxy ログに「incoming ACL check took over 2 seconds – check DNS」というログが生成されます。

この問題を解決するには、DNS ポインタ (PTR) レコードが Microsoft サーバの IP アドレスごとに存在することを確認してください。

高度なルーティングがイネーブルの場合にアベイラビリティが IM and Presence サービスと Microsoft サーバの間で交換されない

## 高度なルーティングがイネーブルの場合にアベイラビリティが IM and Presence サービスと Microsoft サーバの間で交換されない

### トラブルシューティングの手順

- 1 Cisco Unified Communications Manager がすべての Lync/OCS ユーザ向けに Active Directory からユーザデータを同期していることを確認します。  
高度なルーティングは、Active Directory から Cisco Unified Communications Manager に同期されている Microsoft サーバ SIP URI に依存します。
- 2 これがシングルクラスタの IM and Presence サービス配置の場合のみ、高度なルーティングが有効であることを確認します。

## IM and Presence サービス ユーザが Microsoft サーバアドレス帳に表示されない

### トラブルシューティングの手順

- 1 IM and Presence サービス ユーザが Microsoft サーバから移行されて以来、Lync/OCS アドレス帳サービスによる完全同期が実施されていることを確認します。この同期は、デフォルトで毎夜実施されます。
- 2 Microsoft Lync または Microsoft Office Communicator のユーザに新しいアドレス帳のダウンロードをトリガするために、サインアウトしてサインインするように要求します。デフォルトでは、Microsoft サーバから新しいアドレス帳をダウンロードするのに1時間以上かかる場合があります。
- 3 IM and Presence サービス ユーザが前に Microsoft Lync または Microsoft Office Communicator のユーザだった場合、IM and Presence サービス ユーザがまだ Active Directory (msRTCSIP-PrimaryUserAddress) に入力した古い Microsoft サーバ SIP URI を持っていることを確認します。
- 4 IM and Presence サービス ユーザが前は Microsoft Lync または Microsoft Office Communicator ユーザでなかった場合、または古い Microsoft サーバ SIP URI が Active Directory から消去されている場合は、Active Directory の [msRTCSIP-PrimaryUserAddress] フィールドに手動で入力し、IM and Presence サービス ユーザが Microsoft サーバアドレス帳に表示されることを確認します。[msRTCSIP-PrimaryUserAddress] フィールドに sip:user's\_uri と入力する必要があります。

## IMandPresenceサービスがドメイン間フェデレーション要求をMicrosoftサーバの配置経路でルーティングできない

### トラブルシューティングの手順

- 1 Lync/OCS の導入がドメイン間フェデレーション用に正しく設定されていることを確認します。これを行うには、Microsoft サーバユーザがフェデレーションできることを確認します。
- 2 Cisco SIP Proxy および Cisco SIP Federation Connection Manager が各 IM and Presence サービスノードで実行中であることを確認します。
- 3 IM and Presence サービスが外部ドメイン用にドメイン間フェデレーション用に設定されており、そのダイレクト フェデレーションが有効になっていることを確認します。
- 4 外部ドメイン用にスタティック ルートが IM and Presence サービスに設定され、スタティック ルートが Microsoft サーバをポイントしていることを確認します。
- 5 外部ドメインが IM and Presence サービスのアクセス コントロール リスト (ACL) に含まれていることを確認します。

## IM and Presence サービスおよび Microsoft サーバ間の TLS ハンドシェイク エラー

### トラブルシューティングの手順

- 1 Lync/OCS がポート 5061 でお互いの TLS 接続をリッスンするように設定されていることを確認します。
- 2 プレゼンスのピア認証ポートが 5061 に設定されているように IM and Presence サービスのアプリケーション リスナーが設定されていることを確認します。
- 3 IM and Presence サービス証明書が Microsoft のサーバと同じ認証局によって署名されていることを確認します。
- 4 Microsoft サーバまたは IM and Presence サービス証明書が期限切れになっていないことを確認します。
- 5 Microsoft のサーバ証明書がサーバ認証とクライアント認証の両方に設定されていることを確認します。
  - そのような証明書には、“1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2” という OID 値が含まれています。
  - 証明書がサーバ認証用にのみ設定されている場合、“1.3.6.1.5.5.7.3.1” という OID 値が含まれています。

Microsoft Lync ユーザまたは Microsoft Office Communicator ユーザが Cisco Unified Personal Communicator の連絡先リストに追加されると、不正な SIP URI がそのユーザに指定される

- 6 IM and Presence サービス TLS ピア サブジェクト リストに、TLS ハンドシェイク時に Microsoft サーバによって提供される証明に使用される件名共通名 (CN) が含まれることを確認します。
- 7 IM and Presence サービス TLS ピア 認証 TLS コンテキストが正しく設定されており、すべての TLS ピア サブジェクトが選択されていることを確認します。

## Microsoft Lync ユーザまたは Microsoft Office Communicator ユーザが Cisco Unified Personal Communicator の連絡先リストに追加されると、不正な SIP URI がそのユーザに指定される

### トラブルシューティングの手順

Cisco Unified Personal Communicator レジストリ の設定が正しいこと、特に LDAP\_AttributeName\_uri and LDAP\_UriSchemeName サブキーが正しいことを確認します。詳細は、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の Active Directory の設定に関連する章を参照してください。

## Cisco Unified Personal Communicator 上の Microsoft Lync または Microsoft Office Communicator の連絡先に表示名が表示されない

### トラブルシューティングの手順

Cisco Unified Personal Communicator レジストリ の設定が正しいこと、特に LDAP\_AttributeName\_uri and LDAP\_UriSchemeName サブキーが正しいことを確認します。詳細は、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の Active Directory の設定に関連するトピックを参照してください。

## ユーザ移行のトラブルシューティング

ここでは、ユーザ移行のトレースとユーザ移行の一般的な問題について説明します。

### ユーザ移行のトレース

ここでは、ユーザ移行のトレースに使用されるツールについて説明します。

### 連絡先リスト エクスポート ツール

連絡先リスト エクスポート ツールを使用すると、管理者はユーザの移行用に Lync/OCS から連絡先リストを一括でエクスポートすることができます。ツールを実行するたびに、ExportContactsLog<Timestamp>.txt と呼ばれるログファイルが生成されます。ログファイルには、

発生した障害やエラーに関する詳細が含まれています。ログファイルは、ツール自体と同じ場所に保存されます。

エラーが発生する一般的な原因の一部は次のとおりです。

- 不正な入力ファイル名が指定された
- 入力ファイルの中にスペルミスがある
- 指定されたユーザがツールの実行対象の Microsoft サーバ/プールに関連付けられていない

連絡先リストエクスポート ツールのログ ファイルの例は次のとおりです。

```
>>----- 18/05/2011 16:59:38 ----->>Version:
2.1
[DEBUG] Enter>> ExportContacts.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> ExportContacts.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> ExportContacts.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> ExportContacts.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> ExportContacts.LdapConnection.CreateDirectoryEntry
[DEBUG] Current line item is: sip:ExampleUser@dtstfedcup2.com
[DEBUG] Exit>>
ExportContacts.ExportContactsUtilities.getAllSipUriFromStandardFile
[DEBUG] Enter>>
ExportContacts.ExportContactsUtilities.getAndPrintContactsForUsers
[DEBUG] Total number of users found is: 1
[DEBUG] Processing user number: 1
[INFO] Preparing to get contacts for User
[sip:ExampleUser@dtstfedcup2.com]
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getContactsAndGroupsForUser
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getUserInstanceID
[DEBUG] Searching for userInstanceId [SELECT * FROM MSFT_SIPESUserSetting
WHERE PrimaryURI = 'sip:ExampleUser@dtstfedcup2.com']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found user with PrimaryURI : sip:ExampleUser@dtstfedcup2.com,
InstanceId : {7D777FD5-A8F6-8243-B4D6-7F331008C58C}
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getUserInstanceID
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getContacts
[DEBUG] Searching for contacts [SELECT * FROM MSFT_SIPESUserContactData
WHERE UserInstanceId = '{7D777FD5-A8F6-8243-B4D6-7F331008C58C}']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found contact: SIPURI : [SIP:lyncContact@dtstfedcup2.com] with
GroupId: [1]
[DEBUG] Found contact: SIPURI : [SIP:ExampleUser@dtstfedcup2.com] with
GroupId: [1]
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getContacts
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.getGroups
[DEBUG] Searching for groups [SELECT * FROM MSFT_SIPESUserContactGroupData
WHERE UserInstanceId = '{7D777FD5-A8F6-8243-B4D6-7F331008C58C}']
[DEBUG] Enter>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.GetScope
[DEBUG] Search results returned
[DEBUG] Found group: groupName : [General] with GroupId: [1]
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getGroups
```

```
[INFO] User Processed Successfully
[DEBUG] Exit>> ExportContacts.OcsWmiConnection.getContactsAndGroupsForUser
[DEBUG] Enter>> ExportContacts.ExportContactsUtilities.PrintContactsForUser
[DEBUG] Exit>> ExportContacts.ExportContactsUtilities.PrintContactsForUser
[DEBUG] Exit>>
ExportContacts.ExportContactsUtilities.getAndPrintContactsForUsers
[INFO] Summary:
[INFO] 1 users successfully processed
[INFO] 0 users not found
[INFO] 0 users could not be processed due to errors
<<----- 18/05/2011 16:59:41 ----->>
```

## 関連トピック

[IM and Presence サービス BAT による連絡先リストのインポート](#), (161 ページ)

## アカウント無効化ツール

アカウント無効化ツールは、Active Directory (AD) に接続し、ユーザの Lync/OCS 属性を更新して Microsoft サーバアカウントを無効にします。ツールを実行するたびに、DisableAccountLog<Timestamp>.txt と呼ばれるログファイルが生成されます。ログファイルには、発生した障害やエラーに関する詳細が含まれています。ログファイルは、ツール自体と同じ場所に保存されます。

このツールでエラーが発生する一般的な原因の一部は次のとおりです。

- 不正な入力ファイル名が指定された
- 入力ファイルの中にスペルミスがある
- ユーザは、Microsoft サーバデータベースに存在しない
- ツールを実行している管理者が AD に対する読み取り/書き込み権限を持っていない
- このツールによって AD に変更内容が適用され、Microsoft サーバデータベースまで伝播するのに必要な時間を管理者が十分に設けていない。変更が Microsoft サーバデータベースに反映されていることを検証せずに、管理者が次の移行ステップに進んだ場合、移行が失敗することがある

アカウント無効化ツールのログファイルの例は次のとおりです。

```
>>----- 18/05/2011 17:02:07 ----->>Version:
2.0
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.AccountDisable.DisableUsersInFile
[DEBUG] Enter>> DisableAccount.AccountDisable.GetSipUriFromLine
[DEBUG] Exit>> DisableAccount.AccountDisable.GetSipUriFromLine
[INFO] Preparing to Disable Communications Server Account for User
[sip:ExampleUser@dtstfedcup2.com]
[DEBUG] Enter>> DisableAccount.LdapConnection.DisableAccount
[INFO] Searching for user [sip:ExampleUser@dtstfedcup2.com]
```



```
[INFO] Search results returned
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateLdapDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.CreateDirectoryEntry
[DEBUG] Enter>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.checkLdapPrefix
[DEBUG] Exit>> DisableAccount.LdapConnection.CreateDirectoryEntry
[INFO] Found user with PrimaryURI : sip:ExampleUser@dtstfedcup2.com,
DisplayName : Example User, Enabled : True
[DEBUG] Committed changes to the AD
[INFO] User Account Disabled
[DEBUG] Exit>> DisableAccount.LdapConnection.DisableAccount
[DEBUG] Enter>> DisableAccount.AccountDisable.GetSipUriFromLine
[DEBUG] Exit>> DisableAccount.AccountDisable.DisableUsersInFile
[INFO] Summary:
[INFO] 1 users successfully processed
[INFO] 0 users not found
[INFO] 0 users could not be processed due to errors
<<----- 18/05/2011 17:02:08 ----->>
```

アカウント無効化ツールの使用方法の詳細については、移行するユーザの Microsoft のサーバアカウントの無効化に関連するトピックを参照してください。

## アカウント削除ツール

アカウント削除ツールを使用すると、移行するユーザを削除することで、それらのユーザへのプレゼンス要求が後から **IM and Presence** サービスにルーティングされるようにします。その一方で、削除されたユーザは、Lync/OCSに残っているユーザの連絡先リストからは削除されません。アカウント削除ツールを実行すると、DeleteAccountLog<Timestamp>.txt と呼ばれるログファイルがツールと同じディレクトリに生成されます。ログファイルには、発生した障害やエラーに関する詳細が含まれています。

このツールでエラーが発生する一般的な原因の一部は次のとおりです。

- 不正な入力ファイル名が指定された
- 不正なデータベース インスタンス名が指定された
- 入力ファイルの中にスペルミスがある
- ユーザは、Microsoft サーバデータベースに存在しない

アカウント削除ツールのログ ファイルの例は次のとおりです。

```
>>----- 02/12/2013 15:13:50 ----->>
Version: 10.x.x-xx
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.GetCommSvrDbCon
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.GetConnection
[DEBUG] Attempting to Open connection with String :
Server=lyncServer\rtclocal;Database=rtc;Trusted_Connection=yes;
[DEBUG] Connection Opened Ok
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.GetConnection
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Resource']
[DEBUG] Found id [1077578877]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
```

```

[INFO] Found the Resource Table, appears to be a valid Communications
Server Database
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Endpoint']
[DEBUG] No result
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'Container']
[DEBUG] Found id [1202103323]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'HomedResource']
[DEBUG] No result
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'CertificateStore']
[DEBUG] Found id [1826105546]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[INFO] Found the CertificateStore table, dealing with a version of Lync.
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists
[DEBUG] SQL is [SELECT id FROM sysobjects WHERE name = 'ForestDirectory']
[DEBUG] Found id [853578079]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists
[INFO] Found the ForestDirectory table, Creating Lync2013 Connection
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.GetCommSvrDbCon
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.CheckConnection
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.CheckConnection
[DEBUG] Enter>> DeleteAccount.DeleteUserData.DisableUsersInFile
[DEBUG] Enter>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[INFO] Preparing to Delete Communications Server Data for User
[lyncUser@lyncDomain.net]
[DEBUG] Enter>> DeleteAccount.DeleteUserData.DeleteOcsUserData
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetResourceIdForUser
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.SqlEscape
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.SqlEscape
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetResourceIdForUser
[INFO] Found user [lyncUser06@cork.com] with ResourceId [1010], proceeding
to delete data
[DEBUG] Enter>> DeleteAccount.Lync2013DbConnection.DeleteResourceDirectory
[DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Exit>> DeleteAccount.CommSvrDbConnection.GetConnection
[DEBUG] Ran dbo.RtcpDeleteHomedResourceTransaction for resource [1010]
[DEBUG] Deleted CachedContainerMember for resource [1010]
[DEBUG] Deleted ContainerMemberUser for resource [1010]
[DEBUG] Deleted PromptedSubscriber for resource [1010]
[DEBUG] Deleted Delegate for resource [1010]
[DEBUG] Ran RtcpDeleteConferenceParticipantByEnterpriseId for resource
[1010]
[DEBUG] Deleted UserPolicy for resource [1010]
[DEBUG] Deleted ResourcePhone for resource [1010]
[DEBUG] Deleted RtcItem for resource [1010]
[DEBUG] Deleted PUIDDirectory for resource [1010]
[DEBUG] Deleted ResourceDirectory for resource [1010]

```

```
[DEBUG] Committing transaction for resource [1010]
[INFO] Completed Updates for resource [1010]
[DEBUG] Exit>> DeleteAccount.Lync2013DbConnection.DeleteResourceDirectory
[DEBUG] Exit>> DeleteAccount.DeleteUserData.DeleteOcsUserData
[DEBUG] Enter>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.GetUserAtHostFromLine
[DEBUG] Exit>> DeleteAccount.DeleteUserData.DisableUsersInFile

Summary:
Users successfully processed:      1
Users not found:                   0
Users not processed due to errors: 0
<<----- 02/12/2013 15:13:50 ----->>
```

アカウント削除ツールの使用方法の詳細については、移行するユーザのデータベースからユーザデータを削除することに関するトピックを参照してください。

## IM and Presence サービス BAT による連絡先リストのインポート

IM and Presence サービス一括管理ツール (BAT) は、連絡先リストのインポート ジョブの結果をログ ファイルに書き込みます。ログ ファイルには、次の情報が含まれています。

- 正常にインポートされた連絡先の数。
- 連絡先をインポートしようとした際に発生した内部サーバエラーの数。
- インポートされなかった (無視された) 連絡先の数。ログ ファイルには、無視されたそれぞれの連絡先の理由がログ ファイルの末尾に記載されます。
- BAT ジョブを早期に終了させたエラーが原因で処理されなかった CSV ファイル内の連絡先の数。このエラーは滅多に起こりません。

このログ ファイルにアクセスするには、次の手順を実行します。

- 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[一括管理 (Bulk Administration) ]>[ジョブ スケジューラ (Job Scheduler) ]を選択します。
- 2 [検索 (Find) ]を選択し、連絡先リストのインポート ジョブのジョブ ID を選択します。
- 3 [ログ ファイル名 (Log File Name) ]リンクをクリックし、ログを開きます。

任意の BAT ジョブの詳細が必要な場合は、一括プロビジョニング サービスのデバッグ ログを参照してください。これらのログには、/var/log/active/cm/trace/bps/log4j/bps000\*.txt からアクセスできます。

一括プロビジョニング サービスのデバッグ ロギングは、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスから有効にできます。

## IM and Presence サービスでの一括プロビジョニング サービス ロギングの設定

次の手順では、IM and Presence サービス で一括プロビジョニング サービスでロギングを設定する方法について説明します。

**注意**

デバッグレベルトレースは、システムパフォーマンスに影響を与えることがあります。必要などきのみデバッグトレースレベルを有効にし、システム調査が完了した後、ログの設定をデフォルトにリセットします。

**手順**

- 
- ステップ 1** [Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[トレース (Trace)] > [設定 (Configuration)] を選択します。
- ステップ 2** IM and Presence サービス ノードを選択し、[移動 (Go)] を選択します。
- ステップ 3** [サービス グループ (Service Group)] ドロップダウンリストから [データベースと管理サービス (Database and Admin Services)] を選択し、[移動 (Go)] を選択します。
- ステップ 4** [サービス (Service)] ドロップダウンリストから [一括プロビジョニングサービス (Bulk Provisioning Service)] を選択し、[移動 (Go)] を選択します。
- ステップ 5** [トレース (Trace On)] を選択します。
- ステップ 6** [フィルター設定をトレース (Trace Filter Settings)] の中で、[デバッグ トレース レベル (Debug Trace Level)] を選択します。トレースに対してデバッグ レベルを有効にしたい場合は、[デバッグ (Debug)] を選択します。
- ステップ 7** [保存 (Save)] をクリックします。
- 

**関連トピック**

[連絡先リストエクスポート ツール, \(156 ページ\)](#)

**IM and Presence サービス一括管理ツールの連絡先の名前変更**

IM and Presence サービス一括管理ツール (BAT) により、ある形式から別の形式にユーザの連絡先リストのコンタクト ID (JID) の名前を変更できます。たとえば、`firstname.lastname@domain.com` から `userid@domain.com` にユーザのコンタクト ID の名前を変更できます。また、BAT は新しいコンタクト ID で各ユーザの連絡先リストを更新します。

一括管理ツールはコンタクトの名前変更ジョブ結果をログ ファイルに書き込みます。ログ ファイルには、次の情報が含まれています。

- 正常に取得された連絡先の数。
- 連絡先を取得しようとした際に発生した内部サーバエラーの数。
- 無視された連絡先の名前変更レコードの数。ログ ファイルには、それぞれの無視されたレコードの理由がログ ファイルの末尾に記載されます。
- 一括ジョブが早く終了するエラーが発生したために処理されなかった CSV ファイル内の連絡先の名前変更レコードの数。このエラーは滅多に起こりません。

- これらの連絡先の変更内容が通知されたユーザの数。
- これらの連絡先の変更内容が通知されなかったユーザの数。

このログ ファイルにアクセスするには、次の手順を実行します。

- 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。  
[一括管理 (Bulk Administration)] > [ジョブ スケジューラ (Job Scheduler)] を選択します。
- 2 [検索 (Find)] をクリックし、連絡先の名前変更ジョブのジョブ ID を選択します。
- 3 [ログ ファイル名 (Log File Name)] リンクをクリックし、ログを開きます。

エラー発生の一般的な理由は次のとおりです。

- Cisco XCP ルータのサービスがクラスタ内のノードで停止する。
- アップロードされた CSV ファイルの形式が誤っている。 ファイル形式が正しいことと、そのファイルにヘッダーがあることを確認する必要があります。 ファイル形式の詳細については、[コンタクト ID の名前変更に関するトピック](#)を参照してください。
- コンタクト ID に無効な文字が含まれているか、最大許容長を超えている。

任意の一括管理ジョブの詳細が必要な場合は、一括プロビジョニングサービスのデバッグログを参照してください。 これらのログに

は、`/var/log/active/cm/trace/bps/log4j/bps000*.txt` からアクセスできます。

一括プロビジョニング サービスのデバッグ ログは、[Cisco Unified Serviceability] ユーザ インターフェイスから有効にできます。 詳細については、[デバッグ ログおよび一括プロビジョニング サービス ログに関するトピック](#)を参照してください。

#### 関連トピック

[IM and Presence サービスの連絡先リスト内のコンタクト ID の変更](#), (116 ページ)

[IM and Presence サービスでの一括プロビジョニング サービス ログの設定](#), (161 ページ)

## ユーザ移行の一般的な問題

ここでは、共通のユーザ移行の問題について説明します。

### アプリケーションが正しく初期化できない：ユーザ移行ツールのいずれかを実行しているときにエラーが発生する

#### トラブルシューティングの手順

ユーザ移行ツールのいずれかを実行しようとする、「アプリケーションが正常な初期化に失敗しました (Application failed to initialize properly)」というエラーが表示される場合があります。 このエラーの原因は、.NET 2.0 フレームワークのインストールされていないユーザ移行ツールを実行しようとしていることです。 シスコが提供する各ユーザ移行ツールを使用するには、.NET

Framework の少なくともバージョン 2.0 が、そのツールを実行している場所からサーバにインストールされている必要があります。

NET 2.0 フレームワークは、Windows Server 2003 R2 以降で標準としてインストールされています。

## 連絡先リスト エクスポート ツールが Lync ユーザ用の出力ファイルを生成しない

### トラブルシューティングの手順

Lyncサーバから連絡先リストをエクスポートするには、データベースインスタンスのパラメータを含む必要があります。データベースインスタンスパラメータを省略するか、誤ったデータベースパラメータを入力した場合、エラーが連絡先リストエクスポートのログに書き込まれます。ログを確認し、データベースパラメータを省略したか、間違ったパラメータを入力したかを特定します。

次の手順に従って各サーバ/プールのデータベース インスタンスを見つけます。

- 1 プールのフロント エンドサーバの powershell ウィンドウを開きます。
- 2 次の cmdlet を実行します。

```
Get-CsManagementConnection
```

データベース インスタンスの名前はコマンド出力のデータ ソース パラメータの値です。

## 連絡先リスト エクスポート ツールのログに getAndPrintContactsForUsers エラーが表示される

### トラブルシューティングの手順

Lync ユーザのエクスポート ツールを実行したときに「getAndPrintContactsForUsers でエラーが発生しました (Error occurred in“ ”getAndPrintContactsForUsers) 」というエラーがログに表示された場合は、連絡先リスト エクスポート ツールは、Lync データベースに接続できません。ツールを実行しているユーザ アカウントに Lync データベースの適切な読み取り権限があることを確認します。dbo 実行アカウント権限が RTC データベースに許可されていることを確認します。問題が解決しない場合は、データベース インスタンスの名前に入力ミスがないことを確認します。

## 連絡先リスト エクスポート ツール - ログの概要にいくつかのユーザが見つからないと表示される

### トラブルシューティングの手順

- 1 IM and Presence サービスのエクスポート済みファイルを入力として使用する場合は、正しいドメインが -d/ パラメータに使用され、ファイル内に入力ミスがないことを確認してください。

- 2 SIP URI ファイルを入力ファイルとして使用している場合は、ユーザが有効（Active Directory [AD] および Lync/OCS に存在する）で、入力ファイルに“sip:”プレフィックス付きで正しく入力されていることを確認します。
- 3 IM and Presence サービスのエクスポート済みファイルあるいは SIP URI ファイルを入力として使用していない場合、または OU 入力ファイルを使用している場合、ユーザアカウントは AD の中で無効になっている可能性が高いです。ユーザアカウントを再度有効にし、このツールを再度実行してください。

## 連絡先リストエクスポートツール - 通常モードで実行すると、ツールは経過表示バーを表示せず、エクスポートされた連絡先の出力ファイルを生成しない

### トラブルシューティングの手順

- 1 連絡先リストエクスポートのログに次のエラーがないか確認します。「“次の IP/FQDN/ホスト名を使用して LDAP に接続することができません : [some\_ip\_or\_hostname] (Unable to connect to LDAP using IP/FQDN/Hostname: [some\_ip\_or\_hostname]) ”」
  - a エラーが存在する場合は、Active Directory (AD) サーバ用に指定されたアドレスが正しいか確認します。
  - b 指定したアドレスが有効な場合は、AD サーバと Lync/OCS サーバ間のネットワークが接続されていることを確認するために AD サーバに ping を実行します。
  - c 接続が確立されている場合、AD サーバにアクセスするのに必要な権限をユーザが持っていることを確認します。
- 2 連絡先リストエクスポートのログに次のエラーがないか確認します。「“ファイルを開くことに失敗しました... (Failed to open file...) ”」
  - a エラーが存在する場合は、-f/ パラメータに使用されるファイル名のスペルが間違っているか無効です。
  - b 入力ファイルのファイル名にスペースや特殊文字が含まれていないことも確認してください。
- 3 OCS のエクスポートの連絡先リストツールを実行する場合は、データベースインスタンスパラメータを入力していないことを確認します。データベースインスタンスのパラメータは、Lync からのみ連絡先をエクスポートするために必要です。

## アカウント無効化ツール - ログには、IP/FQDN/ホスト名を使用して LDAP に接続できないことが記載されている

### トラブルシューティングの手順

- 1 Active Directory (AD) サーバ用に指定されたアドレスが正しいか確認します。
- 2 指定したアドレスが有効な場合は、AD サーバと Lync/OCS サーバ間のネットワークが接続されていることを確認するために AD サーバに ping を実行します。

- 3 接続が確立されている場合、AD サーバにアクセスするのに必要な権限をユーザが持っていることを確認します。

## アカウント削除ツール - Microsoft サーバ データベースまたはサーバインスタンスが見つからない

### トラブルシューティングの手順

- 1 アカウントが正しく削除されていることを確認するには、各データベースインスタンスに対してアカウント削除ツールを実行する必要があります。
- 2 OCS の場合、次の手順に従って各サーバ/プールのデータベース インスタンスを見つけます。
  - a OCS 管理コンソールで、[Enterprise プール (Enterprise Pools)] からプール名を選択するか (Enterprise Edition) 、 [Standard Edition サーバ (Standard Edition Servers)] からサーバ名を選択します (Standard Edition) 。
  - b 右側のペインで [データベース (Database)] タブを選択します。
  - c データベースのインスタンス名は、[全般設定 (General Settings)] の最初の項目です。
- 3 Lync の場合、次の手順に従って各サーバ/プールのデータベース インスタンスを見つけます。
  - a プールのフロント エンドサーバの powershell ウィンドウを開きます。
  - b 次の cmdlet を実行します。

```
Get-CsManagementConnection
```

データベース インスタンスの名前は返された出力のデータ ソース パラメータの値です。

## アカウント削除ツール - SQL Server への接続中にログにエラーが表示される

### トラブルシューティングの手順

- 1 アカウント削除ツールのログをチェックし、このエラーのログを確認します。エラーが「“このユーザは SQL Server の信頼関係接続と関連付けられていません。(The user is not associated with a trusted SQL Server connection)”」である場合、ツールを実行しているユーザが、Lync/OCS データベースに書き込むために必要な権限を持っていません。
- 2 必要な権限を持つユーザ アカウントを使用してツールを再実行してください。



## BAT 連絡先リストの更新：アップロードされた連絡先リストファイルがドロップダウンリストに表示されない

### トラブルシューティングの手順

- 1 [Cisco Unified Communications Manager IM and Presence Administration] ユーザ インターフェースにログインします。[一括管理 (Bulk Administration)] > [ファイルのアップロード/ダウンロード (Upload/Download Files)] を選択し、[検索 (Find)] をクリックします。
- 2 ファイルが存在し、その機能タイプが[ユーザの連絡先のインポート-カスタムファイル (Import Users' Contacts - Custom File)]であることを確認します。
- 3 不正な機能タイプのファイルが存在する場合、そのファイルを削除します。ファイルを削除したか、ファイルが存在しない場合は、もう一度ファイルをアップロードし、そのターゲットが[連絡先リスト (Contact Lists)]であり、そのトランザクションタイプが[ユーザの連絡先のインポート-カスタムファイル (Import Users' Contacts - Custom File)]であることを確認します。

## BAT 連絡先リストの更新：BAT ジョブの後にログファイルが結果ページ上に存在しない

### トラブルシューティングの手順

BAT の連絡先インポート ジョブのログがジョブの結果ページから欠落している場合、BAT ジョブはサブスクリバノードから実行されました。ログは、パブリッシャ ノードからのみアクセス可能です。ログを表示するには、パブリッシャ ノード上の [Cisco Unified Communications Manager IM and Presence Administration] にサインインします。

## BAT 連絡先リストの更新：ユーザの連絡先が BAT ジョブ中にインポートされない

### トラブルシューティングの手順

- 1 具体的なエラーがないかジョブ結果のログファイルをチェックします。
- 2 IM and Presence に対して、ユーザにライセンスが付与されていることを確認します。
- 3 ユーザがこのクラスタ内のノードに割り当てられていることを確認します。
- 4 連絡先のドメインが有効であることを確認します。

## BAT 連絡先リストの更新：ユーザの連絡先が BAT ジョブ中に部分的にインポートされる

### トラブルシューティングの手順

- 1 具体的なエラーがないかジョブ結果のログファイルをチェックします。

- 2 欠落している連絡先が、CSV ファイル内で有効な形式で入力されていることを確認します。
- 3 連絡先のユーザ数が、システムの [連絡先リストの最大サイズ (Maximum Contact List Size)] を超えていないか確認します。
- 4 ウォッチャのユーザ数が、システムの [ウォッチャの最大数 (Maximum Watchers)] を超えていないか確認します。

## BAT 連絡先リストの更新 - 連絡先が BAT ジョブ中にインポートされない

### トラブルシューティングの手順

- 1 具体的なエラーがないかジョブ結果のログ ファイルをチェックします。
- 2 インポート ファイルが、有効な形式で入力されていることを確認します。
- 3 IM and Presence サービスに対して、すべてのユーザにライセンスが付与されていることを確認します。
- 4 すべてのユーザがローカル クラスタ上で割り当てられていることを確認します。
- 5 Cisco Presence Engine サービスがクラスタ内のすべてのノードで実行中であることを確認します。

## ユーザステータスの移行は、移行プロセス中に Microsoft サーバユーザに対して「ステータスが不明 (Status Unknown)」または「プレゼンスが不明 (Presence Unknown)」と表示される

### トラブルシューティングの手順

- 1 このドキュメントで説明したように、連絡先が IM and Presence サービス に完全に移行されていることを確認します。  
  
移行プロセス中、移行連絡先を Microsoft Lync または Microsoft Office Communicator ユーザが利用できない期間があります。シスコでは、そのような問題がなるべく発生しないようにするために、予定されたメンテナンスウィンドウの中でユーザ移行を実行することをお勧めします。
- 2 Microsoft Lync または Microsoft Office Communicator ユーザにログアウトしてから再度ログインするよう要求します。  
  
移行された連絡先が IM and Presence サービス にインポートされても、Microsoft サーバユーザには、クライアントからサインアウトしてサインインするまでそれらの連絡先のプレゼンスは表示されません。
- 3 問題が解決しない場合は、このドキュメントで説明したように移行手順が正しく実行されたことを確認します。
  - アカウント削除ツールを実行する前に、アカウント無効化ツールによって適用された更新が Lync/OCS に同期されたことを確認します。

- すべての Standard Edition Microsoft サーバまたは Enterprise Edition プールの削除のアカウント ツールを実行したことを確認します。
  - これらの手順が正しく実行されなかった場合は、次の手順を繰り返してこの問題を解決します。
    - アカウント無効化ツールを実行します。
    - アカウント無効ツールによって実行された AD 更新が Microsoft サーバに同期したことを確認します。
    - アカウント削除ツールを実行します。
- 4 それでも移行した連絡先が [プレゼンスが不明 (Presence Unknown)] “ ” と表示される場合は、IM and Presence サービスと Microsoft サーバとの間の統合に問題がある可能性があります。統合の問題のトラブルシューティングに関するヘルプについては、[統合の一般的な問題](#)、(148 ページ) を参照してください。

