



Cisco Jabber for Windows 9.7 インストレーション/コンフィギュレーション ガイド

初版：2014 年 03 月 26 日

最終更新：2014 年 06 月 23 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/）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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. 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 and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Google、Google Play、Android、その他の商標は Google Inc. の商標です。

© 2014 Cisco Systems, Inc. All rights reserved.



目次

はじめに 1

資料 1

コミュニティ リソース 2

インストールの計画 3

ハードウェア要件 3

ソフトウェア要件 4

オペレーティング システム 4

オンプレミス サーバ 5

インスタントメッセージおよびプレゼンスのハイ アベイラビリティ 6

クラウドベース サーバ 7

ディレクトリ サーバ 7

Microsoft Internet Explorer 8

Microsoft Office 8

Microsoft Outlook のローカル連絡先 9

Microsoft Outlook から予定表イベントを有効化 9

Microsoft Outlook とのプレゼンス統合の有効化 10

Active Directory ユーザとコンピュータ ツールとのプレゼンスの有効化 10

Microsoft SharePoint 11

Microsoft Office 365 11

カレンダーの統合 12

CTI 従属 12

ポートおよびプロトコル 13

アクセサリ API を使用したコール制御 14

互換性のあるサードパーティ製アクセサリ 14

ベンダーのプラグインのインストール 15

プラグイン バージョン 15

CTI でサポートされるデバイス 15

サポートされるコーデック	15
Cisco Jabber の COP ファイル	16
クライアント側の可用性ステータス	17
インスタント メッセージの暗号化	19
オンプレミス 暗号化	19
クラウドベース 暗号化	21
クライアントの暗号化対応クライアント	22
暗号化アイコン	24
サーバの暗号化対応クライアント用のロック アイコン	24
クライアントの暗号化対応クライアント用の鍵アイコン	24
ローカル チャットの履歴	24
QoS の設定	25
Cisco Media Services Interface	25
DSCP 値の設定	26
Cisco Unified Communications Manager のポート範囲	26
SIP プロファイルでのポート範囲の指定	26
クライアントによるポート範囲の使用方法	27
DSCP 値を設定するオプション	27
Cisco Unified Communications Manager での DSCP 値の設定	27
グループ ポリシーを用いた DSCP 値の設定	28
ネットワーク内の DSCP 値の設定	28
プロトコルハンドラ	29
プロトコルハンドラのレジストリ エントリ	29
HTML ページのプロトコルハンドラ	30
音声およびビデオのパフォーマンス参照	31
オーディオのビット レート	31
ビデオのビット レート	31
プレゼンテーション ビデオのビット レート	32
ネゴシエートされた最大ビット レート	32
帯域幅のパフォーマンス期待値	33
ビデオ レート アダプテーション	34
サーバのセットアップ	35

サーバセットアップ ガイド	35
証明書の検証設定	37
オンプレミス サーバ	37
必要な証明書	37
認証局により署名された証明書の取得	38
証明書署名要求の形式と要件	39
失効サーバ	39
証明書のサーバ識別情報	40
クライアントへの XMPP ドメインの提供	41
クライアント コンピュータのルート証明書のインポート	41
クライアント コンピュータでの証明書の展開	43
クラウドベースのサーバ	44
プロフィール写真の URL の更新	44
展開オプション	47
オンプレミスの導入	47
製品モード	47
デフォルト モードの図	48
Cisco Unified Presence との図	49
Cisco Unified Communications IM and Presence との図	51
電話機モード ダイアグラム	53
クラウドベース展開	54
クラウド ベースの図	55
ハイブリッドクラウド ベースの図	56
クライアントによるサービスへの接続方法	57
推奨される接続方法	58
認証ソース	60
最初の起動シーケンス	60
クライアントによるオーセンティケータの取得方法	61
サービス ディスカバリ	62
クライアントによるサービスの検索方法	64
Client Issues HTTP クエリー	64
Cisco UDS SRV レコード	65

CUP ログイン SRV レコード	67
手動接続設定	68
オンプレミスでの展開における手動接続設定	69
電話モードのオンプレミスの展開における手動接続設定	69
クラウド ベースの展開における手動接続設定	70
サービス ディスカバリの手動接続設定	71
インストーラのスイッチ	71
オンプレミスでの展開のブートストラップの設定	72
電話モードのオンプレミスの展開におけるブートストラップの設定	74
クラウド ベースの展開におけるのブートストラップの設定	75
クラウドベース SSO	76
クラウドベース SSO の有効化	77
Expressway Mobile and Remote Access の展開	77
サポートされるサービス	79
仮想環境での展開	85
Cisco Jabber のインストール	89
インストールの方法	89
コマンドラインの使用	90
インストール コマンドの例	90
MSI の手動による実行	92
カスタム インストーラの作成	92
デフォルト トランスフォーム ファイルの取得	93
カスタム トランスフォーム ファイルの作成	93
インストーラの変換	94
グループ ポリシーを使用した導入	95
言語コードの設定	96
グループ ポリシーでのクライアントの展開	97
コマンドライン引数	98
オーバーライドの引数	98
モード タイプの引数	99
製品モードの設定する場合	100
製品モードの変更	100

Cisco Unified Communications Manager バージョン 9.x 以降の製品モードの変更	100
Cisco Unified Communications Manager バージョン 8.x の製品モードの変更	101
認証引数	102
TFTP サーバアドレス	105
共通のインストール引数	106
SSO 引数	109
クラウドベース SSO 引数	109
インストーラのプロパティ	110
サポートされる言語	110
Cisco Media Services Interface	111
トラフィック マーキング	111
デスクフォン ビデオ機能	112
ネットワークの準備	112
Cisco Media Services Interface のインストール	113
Cisco Jabber for Windows のアンインストール	113
インストーラの使用	113
製品コードの使用	114
Cisco Jabber の設定	115
クライアント設定の概要	115
Cisco Unified Communications Manager でのクライアントの設定	116
サービス プロファイルのパラメータの設定	117
サービス プロファイルのパラメータ	117
UC サービスの追加	120
サービス プロファイルの作成	121
サービス プロファイルの適用	122
デバイスへのユーザの関連付け	122
電話の設定パラメータの設定	123
電話の設定パラメータ	124
クライアント コンフィギュレーション ファイルの作成とホスティング	125
クライアント コンフィギュレーション ファイル	126
グローバル設定ファイル	126

グループ設定ファイル	126
設定ファイルの要件	127
TFTP サーバ アドレスの指定	128
Cisco Unified Presence での TFTP サーバの指定	128
Cisco Unified Communications Manager IM and Presence Service での TFTP サーバの指定	129
電話モードでの TFTP サーバの指定	129
Cisco WebEx 管理ツール による TFTP サーバの指定	130
グローバル設定の作成	130
グループ設定の作成	131
コンフィギュレーション ファイルのホスティング	132
TFTP サーバの再起動	133
設定ファイルの構造	134
グループ要素	134
XML 構造	135
設定パラメータの概要	135
設定例	137
クライアント パラメータ	138
オプション パラメータ	139
電話パラメータ	145
ポリシー パラメータ	148
オンプレミス ポリシー	149
共通のポリシー	149
Cisco WebEx ポリシー	159
プレゼンス パラメータ	159
サービス クレデンシャル パラメータ	160
ボイスメール パラメータ	161
自動更新の設定	162
問題レポートの設定	164
カスタム埋め込みタブ	164
カスタム埋め込みタブの定義	165
ユーザのカスタム タブ	167

カスタム アイコン	167
カスタム タブからのチャットおよびコール	169
UserID トークン	169
JavaScript 通知	169
カスタム タブでのコール イベントの表示	170
カスタム埋め込みタブの例	172
ディレクトリ ソースとの統合	173
ディレクトリの同期化および認証の設定	173
ディレクトリ サーバとの同期	174
同期の有効化	174
ユーザ ID の LDAP 属性の指定	174
同期の実行	175
ディレクトリ サーバでの認証	176
発信元	176
拡張ディレクトリ統合	177
ドメイン名検索	178
ディレクトリ サーバの検出	179
Cisco Unified Communications Manager User Data Service	179
UDS との統合の有効化	180
UDS サービス パラメータの設定	180
UDSサービス パラメータ	181
複数のクラスタでの連絡先の解決	181
ディレクトリ統合のためのクライアント設定	182
ディレクトリ統合を設定する場合	182
サービス プロファイルのディレクトリ統合の設定	183
ディレクトリ プロファイルパラメータ	184
ディレクトリ統合の設定パラメータの概要	188
EDI パラメータ	189
属性マッピングのパラメータ	189
ディレクトリ サーバの属性	190
ディレクトリ接続パラメータ	191
ディレクトリ クエリー パラメータ	197

基本フィルタの例	200
電話番号マスク パラメータ	201
連絡先の写真のパラメータ	202
EDI での連絡先写真の取得	204
連絡先の写真の形式と寸法	205
連絡先写真の形式	205
連絡先写真の寸法	206
連絡先写真の調整	206
UDS パラメータ	207
UDS での連絡先写真の取得	209
連絡先の写真の形式と寸法	209
連絡先写真の形式	210
連絡先写真の寸法	210
連絡先写真の調整	211
ディレクトリ サーバの設定例	212
ドメイン コントローラの接続	212
手動サーバ接続	212
UDS の統合	212
Expressway for Mobile and Remote Access の LDAP 統合	213
Simple Authentication	214
SSL の Simple Authentication	214
OpenLDAP の統合	214
匿名バインド	214
認証済みバインド	215
AD LDS の統合	216
匿名バインド	216
Windows のプリンシパル ユーザ認証	217
AD LDS のプリンシパルのユーザ認証	217
フェデレーション	218
ドメイン間フェデレーション	218
ドメイン内フェデレーション	219
ドメイン内フェデレーションの設定	219

ドメイン内フェデレーションの例	220
Cisco Jabber for Windows のカスタマイズ	223
カスタム顔文字の追加	223
顔文字の定義	225
カスタム埋め込みタブの作成	227
付録	229
Unified Communications Server インフラストラクチャの移行	229
サーバのインフラストラクチャの相違点	229
バージョン 8.x からバージョン 9.x 以降へのサーバのアップグレード	232
ADSI のエラー コード	232



第 1 章

はじめに

Cisco Jabber for Windows は、コラボレーション ソフトウェアの Cisco Jabber スイート内のユニファイドコミュニケーションクライアントです。このドキュメントでは、クライアントのインストールと設定に必要な情報が記載されています。

Cisco Jabber の詳細については、www.cisco.com/go/jabber を参照してください。

- [資料, 1 ページ](#)
- [コミュニティ リソース, 2 ページ](#)

資料

Cisco Jabber for Windows には、このガイドのほかに次のマニュアルが用意されています。

リリース ノート

http://www.cisco.com/en/US/products/ps12511/prod_release_notes_list.html

サーバ セットアップ ガイド

http://www.cisco.com/en/US/products/ps12511/prod_installation_guides_list.html

エンドユーザ ガイド

http://www.cisco.com/en/US/products/ps12511/products_user_guide_list.html

ライセンス情報

http://www.cisco.com/en/US/products/ps12511/products_licensing_information_listing.html

コミュニティ リソース

シスコでは、サポート担当者とやり取りしたり、製品についてディスカッションしている他のコミュニティのメンバーに参加したりすることができるさまざまなコミュニティ リソースを提供しています。

シスコ製品のカンバセーションおよび共有サイト

機能、ライセンス、統合、アーキテクチャ、課題などをディスカッションしている他のコミュニティのメンバーに参加します。役立つ製品リソースとベスト プラクティスを共有してください。

<https://communities.cisco.com/community/technology/collaboration/product>

シスコ サポート コミュニティ

IT のインストール、実装、および管理の質問については、シスコ サポート コミュニティにアクセスします。

<https://supportforums.cisco.com/community/netpro/collaboration-voice-video/jabber>

シスコ サポート およびダウンロード

豊富な製品サポートリソースを見つけ、アプリケーションソフトウェアをダウンロードし、製品およびバージョンに基づいて不具合を発見します。

<http://www.cisco.com/cisco/web/support/index.html>

シスコ エキスパート コーナー

シスコエキスパートとやり取りしたり、共同作業したり、開発したり、共有したりします。シスコ エキスパート コーナーとは、さまざまなエキスパートがコミュニティに寄与するリソース（ビデオ、ブログ、ドキュメント、Web キャストなど）の集まりです。

<https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts>



第 2 章

インストールの計画

インストールを開始する前に、どのクライアントをサポートするかを確認します。ハードウェアおよびソフトウェア要件について説明します。いずれのポートをクライアントが必要としており、それがどのプロトコルを使用しているかを確認してください。

- [ハードウェア要件, 3 ページ](#)
- [ソフトウェア要件, 4 ページ](#)
- [ポートおよびプロトコル, 13 ページ](#)
- [アクセサリ API を使用したコール制御, 14 ページ](#)
- [CTI でサポートされるデバイス, 15 ページ](#)
- [サポートされるコーデック, 15 ページ](#)
- [Cisco Jabber の COP ファイル, 16 ページ](#)
- [クライアント側の可用性ステータス, 17 ページ](#)
- [インスタント メッセージの暗号化, 19 ページ](#)
- [QoS の設定, 25 ページ](#)
- [プロトコル ハンドラ, 29 ページ](#)
- [音声およびビデオのパフォーマンス参照, 31 ページ](#)

ハードウェア要件

搭載されている **RAM**

Microsoft Windows 7 の 2 GB の RAM および Windows 8

物理メモリの空き容量

128 MB

ディスクの空き容量

256 MB

CPU の速度およびタイプ

モバイル AMD Sempron プロセッサ 3600+ (2 GHz)

Intel Core2 CPU T7400 (2.16 GHz)

GPU

Directx 11 (Microsoft Windows 7 の場合)

I/O ポート

USB 2.0 (USB カメラおよび音声デバイス用)

ソフトウェア要件

適切な導入のため、クライアントワークステーションがソフトウェア要件を満たしていることを確認します。

オペレーティング システム

次のオペレーティング システムに Cisco Jabber for Windows をインストールできます。

- Microsoft Windows 8.1 (32 ビット)
- Microsoft Windows 8.1 (64 ビット)
- Microsoft Windows 8 (32 ビット)
- Microsoft Windows 8 (64 ビット)
- Microsoft Windows 7 (32 ビット)
- Microsoft Windows 7 (64 ビット)

**(注)**

Cisco Jabber for Windows には、Microsoft .NET Framework または Java モジュールは必要ではありません。



- (注) Microsoft Windows 7 または 8 の場合、デスクフォンのビデオで使用するために Cisco Media Services Interface (MSI) 4.1 をダウンロードできます。



- 重要 Cisco Jabber for Windows は、デスクトップ モードのみで Microsoft Windows 8 をサポートします。

オンプレミス サーバ

Cisco Jabber では、次のオンプレミス サーバをサポートします。

- Cisco Unified Communications Manager バージョン 8.0(1) 以降
- Cisco Unified Presence バージョン 8.0(3) 以降。
- Cisco Unity Connection バージョン 8.5 以降
- Cisco WebEx Meetings Server バージョン 1.1 以降
- Cisco Expressway Series for Cisco Unified Communications Manager
 - Cisco Expressway-E バージョン 8.1.1
 - Cisco Expressway-C バージョン 8.1.1
- Cisco TelePresence Video Communication Server
 - Cisco VCS Expressway バージョン 8.1.1
 - Cisco VCS Control バージョン 8.1.1

Cisco Jabberでは、Cisco Unified Survivable Remote Site Telephony バージョン 8.5 で次の機能をサポートします。

- 基本コール機能
- コールを保留およびレジュームする機能



- 制約事項 Cisco Jabber には、Cisco Unified Survivable Remote Site Telephony に正常にフォールバックするために、プレゼンス サーバへのアクティブ接続が必要です。

Cisco Unified Survivable Remote Site Telephony の設定については、次の URL の『*Cisco Unified SCCP and SIP SRST System Administrator Guide*』を参照してください。http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html

Cisco Unified Communications Manager Express の詳細については、「Cisco Unified CME」のマニュアルを参照してください。 http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_device_support_tables_list.html

インスタントメッセージおよびプレゼンスのハイ アベイラビリティ

ハイアベイラビリティとは、インスタントメッセージおよびプレゼンスサービスに対してフェールオーバー機能を提供するために複数のノードがサブクラスタに存在する環境を意味します。サブクラスタ内の1つのノードが利用できなくなった場合、インスタントメッセージおよびプレゼンスがそのノードからサブクラスタ内の別のノードにフェールオーバーします。このようにして、ハイアベイラビリティにより、Cisco Jabber のインスタントメッセージおよびプレゼンスサービスの継続性が確実に保証されます。

Cisco Jabber では、次のサーバを使用したハイ アベイラビリティをサポートしています。

- Cisco Unified Presence バージョン 8.5 および 8.6

Cisco Unified Presence でのハイ アベイラビリティの詳細については、「関連情報」セクションにあるリンクから、次の情報を探します。

『Configuration and Administration of Cisco Unified Presence Release 8.6』

「Multi-node Deployment Administration」

「Troubleshooting High Availability」

『Deployment Guide for Cisco Unified Presence Release 8.0 and 8.5』

「Planning a Cisco Unified Presence Multi-Node Deployment」

- Cisco Unified Communications IM and Presence バージョン 9.0 以降

Cisco Unified Communications IM and Presence でのハイ アベイラビリティの詳細については、「関連情報」セクションにあるリンクから、次の情報を探します。

『Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager』

「High Availability Client Login Profiles」

「Troubleshooting High Availability」

クライアントのハイ アベイラビリティ

フェールオーバー中のクライアントの動作

ハイ アベイラビリティがサーバに設定されている場合、プライマリ サーバがセカンダリサーバにフェールオーバー後、クライアントは最大1分間プレゼンスステータスを一時的に失います。サーバに再ログインを試行する前にクライアントが待機する時間を定義するため、再ログインパラメータを設定します。

再ログイン パラメータの設定

Cisco Unified Presence および Cisco Unified Communications IM and Presence では、サーバへの再ログインを Cisco Jabber が試行するまで待機する秒数の最大値および最小値を設定できます。サーバで、次のフィールドに再ログイン パラメータを指定します。

- クライアントの再ログインの下限 (Client Re-Login Lower Limit)
- クライアントの再ログインの上限 (Client Re-Login Upper Limit)

フェールオーバー中の保留状態アクティブ コール

Cisco Unified Communications Manager のプライマリ インスタンスからセカンダリ インスタンスへのフェールオーバーが発生した場合、アクティブ コールを保留状態にすることはできません。

関連トピック

[Cisco Unified Communications Manager 設定ガイド](#)

[Cisco Unified Presence 設定ガイド](#)

クラウドベース サーバ

Cisco Jabber は、次のホストされているサーバとの統合をサポートします。

- Cisco WebEx Messenger サービス
- Cisco WebEx 管理ツール、最低限のサポート対象バージョンは 7.5
- Cisco WebEx Meeting Center、最低限のサポート対象バージョンは次のとおりです。
 - Version T26L Service Pack EP 20
 - Windows T27L Service Pack 9
- Cisco WebEx Meetings (WebEx 11)

ディレクトリ サーバ

次のディレクトリを Cisco Jabber で使用できます。

- Windows Server 2012 R2 の Active Directory Domain Services
- Windows Server 2008 R2 の Active Directory Domain Services
- Windows Server 2003 R2 の Active Directory
- Cisco Unified Communications Manager User Data Service

Cisco Jabber は、次の Cisco Unified Communications Manager バージョンを使用して UDS をサポートします。

Cisco Unified Communications Manager version 9.1(2) 以降（COP ファイル **cmterm-cucm-uds-912-5.cop.sgn** を使用）。

Cisco Unified Communications Manager version 10.0(1)。COP ファイルは必要ありません。

- OpenLDAP
- Active Directory ライトウェイト ディレクトリ サービス (AD LDS) または Active Directory Application Mode; Active Directory アプリケーション モード (ADAM)



制約事項

OpenLDAP、AD LDS、または ADAM とのディレクトリ統合では、Cisco Jabber 設定ファイルで特定のパラメータを定義する必要があります。詳細については、*LDAP* ディレクトリ サーバを参照してください。

Microsoft Internet Explorer

Cisco Jabber for Windows には Microsoft Internet Explorer 7 以降が必要です。Cisco Jabber for Windows は、HTML コンテンツの表示に Internet Explorer レンダリング エンジンを使用します。



注目

Cisco Jabber for Windows にはインスタントメッセージのレンダリングに Internet Explorer アクティブ スクリプトが必要です。アクティブ スクリプトを有効にする手順については、次の Microsoft のマニュアルを参照してください。 <http://windows.microsoft.com/en-US/windows/help/genuine/ie-active-script>

Internet Explorer との既知の問題

- シングル サインオン (SSO) を使用する展開でクラウドベース、問題は Internet Explorer 9 でおこります。Internet Explorer 9 を使用するユーザは、Cisco Jabber for Windows にログインするときにセキュリティ警告が表示されます。この問題を解決するには、[互換性ビュー設定 (Compatibility View Settings)] ウィンドウの Web サイトのリストに `webexconnect.com` を追加します。

Microsoft Office

Cisco Jabber for Windows では、次のソフトウェアの統合をサポートしています。

- Microsoft Office 2007 32 ビット版
- Microsoft Office 2010 32 ビット版

- Microsoft Office 2010 64 ビット版
- Microsoft Office 2013 32 ビット版
- Microsoft Office 2013 64 ビット版
- Microsoft Exchange 2007
- Microsoft Exchange 2010

Microsoft Outlook のローカル連絡先

Cisco Jabber for Windows は、ユーザが Microsoft Outlook に関してユーザ検索をし、ローカル連絡先を追加できるようにします。

クライアントを使用して、Microsoft Outlook でローカル連絡先を検索するために、ユーザは Microsoft Outlook に設定されたプロファイルが必要です。また、ユーザは次のようにする必要があります。

- 1 [ファイル (File)] > [オプション (Options)] を選択します。
- 2 [統合 (Integration)] タブを選択します。
- 3 [なし (None)] または [Microsoft Outlook (Microsoft Outlook)] のいずれかを選択します。

クライアントの連絡先リストにローカルの Microsoft Outlook 連絡先を追加するには、ローカル連絡先は Microsoft Outlook にインスタント メッセージのアドレスを持っている必要があります。

クライアント インターフェイスに連絡先の写真を表示するには、Microsoft Outlook のローカル連絡先がインスタント メッセージのアドレスを持っている必要があります。

クライアントを使用して Microsoft Outlook のローカル連絡先と通信するには、ローカル接続が関連情報を持っている必要があります。連絡先にインスタントメッセージを送信するには、ローカル連絡先がインスタント メッセージのアドレスを持っている必要があります。Microsoft Outlook の連絡先にコールするには、ローカル連絡先が電話番号を持っている必要があります。

Microsoft Outlook から予定表イベントを有効化

Microsoft Outlook の予定表イベントを表示させるために、Cisco Jabber for Windows の設定を適用する必要があります。

手順

-
- ステップ 1** 次の例のように、Microsoft Outlook で電子メール アカウントを開きます。
- a) [ファイル (File)] > [アカウント設定 (Account Settings)] を選択します
 - b) [アカウント設定 (Account Settings)] ウィンドウの [電子メール (Email)] タブを選択します。
- ステップ 2** サーバ名をダブルクリックします。
- ほとんどの場合、サーバ名は Microsoft Exchange です。

- ステップ 3** [キャッシュされた Exchange モードの設定 (Cached Exchange Mode setting)] チェックボックスを選択します。
- ステップ 4** 設定を適用してから、Microsoft Outlook を再起動します。
-

ユーザが予定表イベントを作成すると、Microsoft Outlook[会議 (Meetings)] タブでそれらのイベントが表示されます。

Microsoft Outlook とのプレゼンス統合の有効化

Microsoft Outlook との統合を有効にするには、Microsoft Active Directory の proxyAddresses 属性の値として SIP:user@cupdomain を指定します。ユーザは Microsoft Outlook に在席かどうかを共有できるようになります。

proxyAddresses 属性を変更するには、次の手順を実行します。

Active Directory ユーザとコンピュータなどの Active Directory 管理ツールを使用する

Active Directory ユーザとコンピュータ管理ツールを使用し、Microsoft Windows Server 2008 以降の属性を編集できます。

ADSchemaWizard.exe ユーティリティを使用する

ADSchemaWizard.exe ユーティリティは Cisco Jabber 管理パッケージで使用できます。このユーティリティが生成する LDIF ファイルにより、SIP:user@cupdomain の値を持つ proxyAddresses 属性をすべてのユーザに追加するよう、ディレクトリが変更されます。

ADSchemaWizard.exe ユーティリティは、Microsoft Windows Server 2003 などの Active Directory ユーザとコンピュータ管理ツールの属性編集機能をサポートしないサーバで使用します。ADSIEdit などのツールを使用して、ADSchemaWizard.exe ユーティリティを使用して適用した変更を確認できます。

ADSchemaWizard.exe ユーティリティの使用には、Microsoft .NET Framework バージョン 3.5 以降が必要です。

Microsoft Windows PowerShell でスクリプトを作成する

Microsoft Outlook でのプレゼンスを有効にするスクリプトの作成については、対応する Microsoft のマニュアルを参照してください。

Active Directory ユーザとコンピュータ ツールとのプレゼンスの有効化

次の手順を実行し、Active Directory ユーザとコンピュータ管理ツールを使用して Microsoft Outlook で個別ユーザのプレゼンスを有効にします。

手順

- ステップ 1** Active Directory ユーザとコンピュータ管理ツールを起動します。

Active Directory ユーザとコンピュータ管理ツールを実行するには、管理者権限が必要です。

ステップ 2 メニューバーで [表示 (View)] を選択し、ドロップダウン リストから [拡張機能 (Advanced Features)] オプションを選択します。

ステップ 3 Active Directory ユーザとコンピュータ管理ツールの対象ユーザに移動します。

ステップ 4 ユーザをダブルクリックして [プロパティ (Properties)] ダイアログボックスを開きます。

ステップ 5 [属性エディタ (Attribute Editor)] タブを選択します。

ステップ 6 [属性 (Attributes)] リスト ボックスで、proxyAddresses 属性を見つけて選択します。

ステップ 7 [編集 (Edit)] を選択し、[複数値文字列エディタ (Multi-valued String Editor)] ダイアログボックスを開きます。

ステップ 8 [追加する値 (Value to add)] テキスト ボックスに SIP:user@cupdomain の値を指定します。
例: SIP:msmith@cisco.com

user@cupdomain の値は、ユーザのインスタントメッセージアドレスです。 cupdomain は、Cisco Unified Presence もしくは Cisco Unified Communications IM and Presence のドメインに対応します。

Microsoft SharePoint

Cisco Jabber for Windows では、Microsoft SharePoint の次のバージョンをサポートしています。

- Microsoft SharePoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013



重要

Cisco Jabber for Windows で Microsoft SharePoint サイトのアベイラビリティ ステータスがサポートされるのは、ユーザが Microsoft Internet Explorer を使用してそれらのサイトにアクセスする場合だけです。 Microsoft SharePoint サイトを Microsoft Internet Explorer の信頼できるサイトの一覧に追加します。

Microsoft Office 365

Microsoft Office 365 では、プラン、サブスクリプション、タイプに基づいてさまざまな構成タイプをサポートします。 Cisco Jabber for Windows は、オンプレミス Active Directory サーバを必要とする Microsoft Office 365 の小規模企業プラン P1 でテストされています。

Cisco Jabber for Windows では、次のアプリケーションを持つ Microsoft Office 365 とクライアントサイドの統合をサポートします。

- Microsoft Office 2013 32 ビット版

- Microsoft Office 2013 64 ビット版
- Microsoft Office 2010 32 ビット版
- Microsoft Office 2010 64 ビット版
- Microsoft Office 2007 32 ビット版
- Microsoft SharePoint 2010

カレンダーの統合

予定表の統合のために、次のクライアントアプリケーションを使用できます。

- Microsoft Outlook 2013 32 ビット版
- Microsoft Outlook 2013 64 ビット版
- Microsoft Outlook 2010 32 ビット版
- Microsoft Outlook 2010 64 ビット版
- Microsoft Outlook 2007 32 ビット版
- IBM Lotus Notes 9 32 ビット版
- IBM Lotus Notes 8.5.3 32 ビット版
- IBM Lotus Notes 8.5.2 32 ビット版
- IBM Lotus Notes 8.5.1 32 ビット版
- Google Calendar

関連トピック

[仮想環境での展開, \(85 ページ\)](#)

CTI 従属

Cisco Jabber では、Computer Telephony Integration (CTI) 従属 (サードパーティ アプリケーションからの Cisco Jabber の CTI のコントロール) をサポートしています。

CTI 従属の詳細については、Cisco Unified Communications Manager の適切なバージョンの CTI ドキュメントを参照してください。

Cisco Unified Communications Manager API を通じ、CTI コントロールのアプリケーションを作成する方法について詳しくは、次の Cisco Developer Network サイトを参照してください。

- Cisco TAPI : <http://developer.cisco.com/web/tapi/home>
- Cisco JTAPI : <http://developer.cisco.com/web/jtapi/home>

ポートおよびプロトコル

次の表では、Cisco Jabber を使用する発信ポートおよびプロトコルを示します。

ポート	プロトコル	説明
443	TCP (XMPP および HTTPS)	<p>Cisco WebEx Messenger サービスへの XMPP トラフィック。</p> <p>クラウドベース導入のみで、クライアントはこのポートを介して XMPP トラフィックを送信します。ポート 443 がブロックされた場合、クライアントはポート 5222 にフォールバックします。</p> <p>(注) Cisco Jabber はまた、HTTPS トラフィックのためのこのポートを Cisco Unity Connection および Cisco WebEx Meetings Server に使用できます。</p>
389	UDP/TCP	LDAP ディレクトリ サーバ
636	LDAPS	LDAP ディレクトリ サーバ (セキュア)
3268	TCP	グローバル カタログ サーバ
3269	LDAPS	グローバル カタログ サーバ (セキュア)
5070	UDP	ビデオ デスクトップ共有機能の Binary Floor Control Protocol (BFCP)
5222	TCP (XMPP)	Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service への XMPP トラフィック。
8443	TCP (HTTPS)	Cisco Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Service への XMPP トラフィック。
7080	TCP (HTTPS)	音声メッセージ通知 (新規メッセージ、メッセージ更新、メッセージ削除) 用の Cisco Unity Connection
53	UDP/TCP	ドメイン ネーム システム (DNS) トラフィック
37200	SOCKS5 バイトストリーム	<p>ピア ツー ピア ファイル転送</p> <p>オンプレミスでの展開では、クライアントはまた、画面キャプチャを送信するためにこのポートを使用します。</p>
5060	UDP/TCP	Session Initiation Protocol (SIP) コール シグナリング

ポート	プロトコル	説明
5061	TCP	セキュアな SIP コール シグナリング

追加のサービスおよびプロトコルのポート

この項で示されているポートに加えて、展開されたすべてのサービスおよびプロトコルに必要なポートを確認することを保証する必要があります。バージョンに応じて適切なマニュアルを参照してください。次のマニュアルで様々なサーバのポートとプロトコルの要件を参照してください。

- Cisco Unified Communications Manager、Cisco Unified Communications Manager IM and Presence Service、および Cisco Unified Presence については、『*TCP and UDP Port Usage Guide*』を参照してください。
- Cisco Unity Connection については、『*System Administration Guide*』を参照してください。
- Cisco WebEx Meetings Server については、『*Administration Guide*』を参照してください。
- Cisco WebEx サービスについては、『*Administrator's Guide*』を参照してください。
- Expressway Mobile and Remote Access については、『*Cisco Expressway IP Port Usage for Firewall Traversal*』を参照してください。

アクセサリ API を使用したコール制御

Cisco Jabber には、サードパーティのアクセサリに対するコール制御機能を提供する API が含まれます。この API は、Cisco Jabber で API コール制御機能を使用できるように、ベンダー パートナーのアクセサリを使用可能にするソフトウェア プラグインを作成することができます。

互換性のあるサードパーティ製アクセサリ

ヘッドセット、スピーカ、キーボードおよびオーディオデバイスなどのシスコの特定の互換性のあるデバイスを使用して、デバイスから Cisco Jabber でコール制御処理の実行をします。たとえば、ヘッドセットで、着信コールへの応答、アクティブ コールの終了、音声のミュート、コールの保留をするためにコントロールを使用することができます。

Cisco Jabber と互換性のあるデバイスの一覧に関しては、『*Unified Communications Endpoint and Client Accessories*』サイト (http://www.cisco.com/en/US/prod/voicesw/uc_endpoints_accessories.html) をご覧ください。



- (注) 互換性のあるシスコ製ではない特定のサードパーティ製アクセサリを使用できます。ただし、シスコはこのようなサードパーティ製アクセサリとの最適なユーザエクスペリエンスを保証できません。最高のユーザエクスペリエンスを得るには、Cisco Jabber を持つシスコ製の互換デバイスだけを使用する必要があります。

ベンダーのプラグインのインストール

互換性のあるアクセサリを Cisco Jabber で使用するには、以下の手順に従ってください。

手順

- ステップ1** サードパーティ ベンダーのサイトからの互換プラグインをダウンロードします。
- ステップ2** 別途プラグインを Cisco Jabber にインストールします。

プラグインバージョン

次は、Cisco Jabber との統合に必要な最小限のプラグインバージョンです。

- Jabra PC Suite Version 2.12.3655
- Logitech UC Plugin 1.1.27

CTI でサポートされるデバイス

Cisco Jabber は、Cisco Unified Communications Manager バージョン 8.6(1) と同じ CTI デバイスをサポートします。 *CTI Supported Devices* の *CTI Supported Device Matrix* を参照してください。

関連トピック

[CTI でサポートされるデバイス](#)

サポートされるコーデック

サポートされるオーディオ コーデック

- g.722.1
 - g.722.1 32k
 - g.722.1 24k



(注) g.722.1 は、Cisco Unified Communications Manager 8.6.1 以降でサポートされません。

- g.711
 - g.711 A-law
 - g.711 u-law
- g.729a

サポートされるビデオコーデック

- H.264/AVC

Cisco Jabber の COP ファイル

場合によっては、COP ファイルを Cisco Unified Communications Manager に適用する必要がある場合があります。

次の COP ファイルは、Cisco.com の Cisco Jabber 管理パッケージからダウンロードできます。

COP ファイル	説明	Cisco Unified Communications Manager バージョン
ciscocm.installcsfdevicetype.cop.sgn	Cisco Unified Communications Manager に CSF デバイス タイプを追加します。 詳細については、ソフトウェア要件を参照してください。	7.1.3
cmterm-bfcp-e.8-6-2.cop.sgn	CSF デバイスで BFCP ビデオデスクトップ共有をサポートします。 詳細については、 <i>BFCP</i> 機能用 <i>COP</i> ファイルの適用を参照してください。	8.6.2 のみ
ciscocm.addcsfsupportfield.cop.sgn	グループ設定ファイルの [CSF サポート フィールド (CSF Support Field)] フィールドを追加します。 詳細については、グループ設定の作成を参照してください。	8.6.x 以下

COP ファイル	説明	Cisco Unified Communications Manager バージョン
cmterm-cupc-dialrule-wizard-0.1.cop.sgn	アプリケーションダイヤルルールとディレクトリ ルックアップルールを Cisco Jabber に公開します。 詳細については、ダイヤルルールの発行を参照してください。	サポートされるすべてのバージョン

関連トピック

[「Download software」](#)

クライアント側の可用性ステータス

この項では、[オプション (Options)] ウィンドウの[ステータス (Status)] タブにある[ミーティング中 (マイ カレンダーによる) (In a meeting (according to my calendar))] チェックボックスについて説明します。

クライアントは、カレンダーにイベントがある場合、「ミーティング中」のアベイラビリティステータスの設定に関して 2 つのオプションをサポートします。

Microsoft Exchange から取得した「ミーティング中」のアベイラビリティステータス

Cisco Unified Presence と Microsoft Exchange の統合が要求されます。オンプレミスの展開を適用します。

Cisco Jabber から取得した「ミーティング中」のアベイラビリティステータス

オンプレミス および クラウドベース の展開に適用します。

カレンダーに次のイベントがある場合、アベイラビリティステータスは「ミーティング中」に変更されます。

配備	[ミーティング中 (マイ カレンダーによる) (In a meeting (according to my calendar))] を選択します。	[ミーティング中 (マイ カレンダーによる) (In a meeting (according to my calendar))] を選択しません。
Cisco Unified Presence と Microsoft Exchange の統合を有効にします。	Cisco Unified Presence は、アベイラビリティステータスを設定します。	アベイラビリティステータスは変更されません。

配備	【ミーティング中（マイ カレンダーによる）（In a meeting (according to my calendar)）】を選択します。	【ミーティング中（マイ カレンダーによる）（In a meeting (according to my calendar)）】を選択しません。
Cisco Unified Presence と Microsoft Exchange の統合を有効にしません。	クライアントにより、アベイラビリティステータスが設定されます。	アベイラビリティ ステータスは変更されません。
クラウドベースの導入	クライアントにより、アベイラビリティステータスが設定されます。	アベイラビリティ ステータスは変更されません。



(注)

【ミーティング中（マイ カレンダーによる）（In a meeting (according to my calendar)）】チェックボックスをオンにした場合、Microsoft Outlook、IBM Lotus Notes、Google Calendar などのサポートされているカレンダー クライアントにイベントがある場合で、クライアントは「ミーティング中」というアベイラビリティ ステータスだけを表示します。クライアントは、その他のカレンダー ソースから他のアベイラビリティ ステータスを表示しません。

次のステートメントが オンプレミス の展開に適用されます。

- 「ミーティング中」のアベイラビリティ ステータスを設定するために、Cisco Unified Presence と Microsoft Exchange の統合を無効にする必要があります。

クライアントは、Cisco Unified Presence と Microsoft Exchange の統合が有効か無効かを確認します。クライアントは、統合が無効の場合、「ミーティング中」のアベイラビリティ ステータスの設定だけをします。

- Cisco Unified Presence ユーザ オプション ページには、次のフィールドが含まれます。

マイ プレゼンス ステータスをカレンダー情報に包含する

このフィールドは、クライアントの【ミーティング中（マイ カレンダーによる）（In a meeting (according to my calendar)）】チェックボックスと同等です。両方のフィールドは、Cisco Unified Presence データベースの同じ値を更新します。

ユーザが両方のフィールドを異なる値に設定すると、ユーザが最後に設定したフィールドが優先されます。クライアントが実行されている際に、ユーザが【マイ プレゼンス ステータスをカレンダー情報に包含する（Include Calendar information in my Presence Status）】フィールドの値を変更すると、ユーザはその変更を適用させるためにクライアントを再起動する必要があります。

クライアント側のアベイラビリティ ステータスを比較し、Cisco Unified Presence と Microsoft Exchange を統合します。

クライアント側の「ミーティング中」のアベイラビリティステータスの有効化	Cisco Unified Presence と Microsoft Exchange を統合します。
「ミーティング中」のアベイラビリティステータスは、サポートされません。	「ミーティング中」のアベイラビリティステータスは、サポートされます。
「ミーティング中」のアベイラビリティステータスは、ユーザの予定表に表示されないイベントに関してサポートされます。	「ミーティング中」のアベイラビリティステータスは、ユーザの予定表に表示されないイベントに関してサポートされません。

- ・「ミーティング中はオフライン」のアベイラビリティステータスは、ユーザがクライアントにログインしていないが、ユーザのカレンダーにイベントがあることを意味します。
- ・ユーザの予定表に表示されないイベントとは、アドホック会議などのイベントを指します。たとえば、ユーザ A が未スケジュールの Cisco WebEx 会議を作成します。ユーザ A は、インスタントメッセージでその会議 URL を送信することによって、ユーザ B を招待します。

インスタントメッセージの暗号化

Cisco Jabberは、TLS を使用して、クライアントとサーバ間のネットワークに XMPP トラフィックを確保します。Cisco Jabberは、ポイントツーポイントのインスタントメッセージやグループチャットを暗号化します。

オンプレミス 暗号化

次の表は、オンプレミス展開でのインスタントメッセージ暗号化に関する詳細を要約したものです。

接続	プロトコル	ネゴシエーション証明書	予想される暗号化アルゴリズム
クライアントからサーバへ	XMPP over TLS	X.509 公開キーインフラストラクチャ証明書	AES 256 ビット

サーバおよびクライアントのネゴシエーション

次のサーバは、X.509 公開キーインフラストラクチャ (PKI) を使用している Cisco Jabber で TLS 暗号化をネゴシエートします。

- ・Cisco Unified Presence
- ・Cisco Unified Communications IM and Presence

サーバおよびクライアントが TLS 暗号化をネゴシエートした後、インスタント メッセージ トラフィックを暗号化するため、クライアントとサーバの両方がセッション キーを生成し、交換します。

次の表に、Cisco Unified Presence と Cisco Unified Communications IM and Presence の PKI 証明書キー長を示します。

バージョン	キー長
Cisco Unified Communications IM and Presence バージョン 9.0.1 以降	2048 ビット
Cisco Unified Presence バージョン 8.6.4 以降	2048 ビット
Cisco Unified Presence バージョン 8.6.4 以前	1024 ビット

XMPP の暗号化

Cisco Unified Presence および Cisco Unified Communications IM and Presence の両方は、Cisco Jabber とプレゼンス サーバ間のインスタント メッセージ トラフィックをセキュアにするため、AES アルゴリズムで暗号化される 256 ビット長のセッション キーを使用します。

サーバ ノード間のトラフィックに追加のセキュリティが必要な場合、Cisco Unified Presence または Cisco Unified Communications IM and Presence で XMPP のセキュリティ設定を行うことができます。セキュリティ設定に関する詳細については、次のマニュアルを参照してください:

- Cisco Unified Presence: *Configuring Security on Cisco Unified Presence*
- Cisco Unified Communications IM and Presence: *Security configuration on IM and Presence*

インスタント メッセージのロギング

必要に応じて、規制ガイドラインへの準拠のために、インスタント メッセージをログに記録し、アーカイブできます。インスタント メッセージを記録するには、外部データベースを設定するか、またはサードパーティ製のコンプライアンス サーバと統合します。Cisco Unified Presence および Cisco Unified Communications IM and Presence では、外部データベースまたはサードパーティ製のコンプライアンス サーバに記録したインスタント メッセージは暗号化しないでください。記録をしたインスタント メッセージを保護するため、外部データベースまたはサードパーティ製のコンプライアンス サーバを適切に設定する必要があります。

コンプライアンスの詳細については、次のマニュアルを参照してください。

- Cisco Unified Presence: *Instant Messaging Compliance Guide*
- Cisco Unified Communications IM and Presence: *Instant Messaging Compliance for IM and Presence Service*

AES などの対称キー アルゴリズムまたは RSA などの公開キー アルゴリズムなど、暗号化レベルおよび暗号化アルゴリズムに関する詳細情報は、「*Next Generation Encryption*」を参照してください。

X.509 公開キー インフラストラクチャ証明書に関する詳細情報については、「*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*」マニュアルを参照してください。

関連トピック

[インスタント メッセージングのコンプライアンス ガイド](#)

[IM and Presence サービスのセキュリティ設定](#)

[IM and Presence サービスのインスタント メッセージングのコンプライアンス](#)

[IM and Presence のセキュリティ設定](#)

[『Internet X.509 Public Key Infrastructure Certificate and CRL Profile』](#)

[次世代暗号化](#)

クラウドベース 暗号化

次の表は、クラウドベース展開でのインスタントメッセージ暗号化に関する詳細を要約したものです。

接続	プロトコル	ネゴシエーション証明書	予想される暗号化アルゴリズム
クライアントからサーバへ	TLS 内の XMPP	X.509 公開キー インフラストラクチャ証明書	AES 128 ビット
クライアントからクライアントへ	TLS 内の XMPP	X.509 公開キー インフラストラクチャ証明書	AES 256 ビット

サーバおよびクライアントのネゴシエーション

次のサーバは、Cisco WebEx Messenger サービスで X.509 公開キー インフラストラクチャ (PKI) の証明書を使用して、Cisco Jabber で TLS 暗号化をネゴシエートします。

サーバおよびクライアントが TLS 暗号化をネゴシエートした後、インスタントメッセージトラフィックを暗号化するため、クライアントとサーバの両方がセッションキーを生成し、交換します。

XMPP の暗号化

Cisco WebEx Messenger サービスは、AES アルゴリズムで暗号化される 128 ビットの長さのセッションキーを使用して、Cisco Jabber と Cisco WebEx Messenger のサービス間でインスタントメッセージトラフィックを保護します。

クライアント間のトラフィックを確保するため、オプションで 256 ビットのクライアント間 AES 暗号化のトラフィックを有効にできます。

インスタントメッセージのロギング

Cisco WebEx Messenger サービスは、インスタントメッセージにログインできますが、暗号化された形式のこれらのインスタントメッセージをアーカイブすることはできません。しかし、Cisco

WebEx Messenger サービスは、SAE-16 および ISO-27001 監査などの厳重なデータセンター セキュリティを使用して、記録したインスタント メッセージを保護します。

Cisco WebEx Messenger サービスは、AES 256 ビット クライアント間の暗号化を有効にする場合、インスタント メッセージにログインできません。

AES などの対称キー アルゴリズムまたは RSA などの公開キー アルゴリズムなど、暗号化レベルおよび暗号化アルゴリズムに関する詳細情報は、「*Next Generation Encryption*」を参照してください。

X.509 公開キー インフラストラクチャ証明書に関する詳細情報については、「*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*」 マニュアルを参照してください。

関連トピック

[クライアントの暗号化対応クライアント](#)

[『Internet X.509 Public Key Infrastructure Certificate and CRL Profile』](#)

[次世代暗号化](#)

クライアントの暗号化対応クライアント

デフォルトでは、クライアントと Cisco WebEx Messenger サービス間のインスタント メッセージトラフィックは安全です。クライアント間のインスタント メッセージトラフィックを確保するために、オプションで Cisco WebEx 管理ツールのポリシーを選択します。

次のポリシーは、インスタント メッセージのクライアント間の暗号化を指定します。

IM の AES 符号化をサポートする

送信側クライアントは、AES 256 ビット アルゴリズムでインスタント メッセージを暗号化します。受信側クライアントは、インスタント メッセージの暗号を解除します。

IM の符号化をサポートしない

クライアントは、暗号化をサポートしない他のクライアントとの間でインスタント メッセージを送受信できます。

次の表では、これらのポリシーで設定できるさまざまな組み合わせを示しています。

ポリシーの組み合わせ	クライアントの暗号化対応クライアント	リモートクライアントが AES 暗号化をサポートしている場合	リモートクライアントが AES 暗号化をサポートしていない場合
IM の AES 符号化をサポートする = False IM の符号化をサポートしない = True	No	Cisco Jabber は暗号化されていないインスタントメッセージを送信します。 Cisco Jabber はキー交換をネゴシエートしません。そのため、他のクライアントは Cisco Jabber の暗号化されたインスタントメッセージを送信しません。	Cisco Jabber は暗号化されていないインスタントメッセージを送受信します。
IM の AES 符号化をサポートする = True IM の符号化をサポートしない = True	Yes	Cisco Jabber は暗号化されたインスタントメッセージを送受信します。 Cisco Jabber には、インスタントメッセージが暗号化されていることを示すアイコンが表示されます。	Cisco Jabber は暗号化されたインスタントメッセージを送信します。 Cisco Jabber は暗号化されていないインスタントメッセージを受信します。
IM の AES 符号化をサポートする = True IM の符号化をサポートしない = False	Yes	Cisco Jabber は暗号化されたインスタントメッセージを送受信します。 Cisco Jabber には、インスタントメッセージが暗号化されていることを示すアイコンが表示されます。	Cisco Jabber は、リモートクライアントに対してインスタントメッセージの送受信を行いません。 ユーザがリモートクライアントにインスタントメッセージを送信しようとすると、Cisco Jabber にエラーメッセージが表示されます。



(注)

- Cisco Jabber では、グループ チャットによるクライアント間の暗号化をサポートしていません。Cisco Jabber は、ポイントツーポイントチャットのみに関して、クライアント間の暗号化を使用します。

暗号化および Cisco WebEx ポリシーの詳細については、Cisco WebEx のマニュアルの「*About Encryption Levels*」トピックを参照してください。

関連トピック

[「About Encryption Levels」](#)

暗号化アイコン

暗号化レベルを表示するには、クライアントが表示するアイコンを確認します。

サーバの暗号化対応クライアント用のロック アイコン

オンプレミスとクラウドベースの展開では、Cisco Jabberにより次のアイコンが表示され、サーバの暗号化対応クライアントに指示が出されます。



クライアントの暗号化対応クライアント用の鍵アイコン

クラウドベースの展開では、Cisco Jabberはクライアントの暗号化を示す次のアイコンを表示します。



ローカル チャットの履歴

ローカルチャット履歴を有効にすると、Cisco Jabberにより、暗号化形式でインスタントメッセージをアーカイブされません。チャット履歴へのアクセスを制限するために、Cisco Jabber はアーカイブを %USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db ディレクトリに保存します。

ローカルのチャット履歴を有効にする方法の詳細については、『*Server Setup Guide*』の「*Provision Instant Messaging and Presence*」の項を参照してください。

QoS の設定

Cisco Jabber は、ネットワークを通過するように、Real-Time Transport Protocol (RTP) トラフィックの優先および分類のための 2 種類の方法をサポートします。

- Cisco Media Services Interface での展開
- RTP メディア パケットの IP ヘッダーで DSCP 値を設定



ヒント

Cisco Media Services Interface (MSI) で展開することを推奨します。このメソッドにより、効果的にエクスペリエンスの質が向上し、導入および運用のコストが削減されます。MSI により、クライアントはネットワーク アウェアにすることができ、ネットワークの状況に動的に適応し、ネットワークとより緊密に統合できます。

Cisco Media Services Interface

Cisco Media Services Interface では、Cisco Prime Collaboration Manager および Cisco Medianet 対応ルータと連動する Microsoft Windows サービスを提供し、Cisco Jabber がネットワークで遅延やパケット損失を最小限に抑えて音声メディアとビデオ メディアを送信できるようにします。

Cisco Jabber では、音声メディアまたはビデオ メディアを送信する前に、Cisco Media Services Interface をチェックします。

- このサービスがコンピュータ上で機能していれば、Cisco Jabber は Cisco Media Services Interface にフロー情報を提供します。
その後、サービスはネットワークに信号を送信するため、ルータがフローを分類して Cisco Jabber のトラフィックにプライオリティを設定できるようになります。
- サービスが存在しない場合には、Cisco Jabber ではサービスを使用せずに、通常どおりに音声メディアとビデオ メディアを送信します。



(注)

Cisco Jabberでは、音声コールまたはビデオ コールごとに Cisco Media Services Interface をチェックします。

Cisco Media Services Interface は個別にインストールし、ネットワークが Cisco Medianet 対応であることを確認する必要があります。また、Cisco Prime Collaboration Manager と、Cisco Medianet に対応するルータもインストールする必要があります。

関連トピック

[Cisco Media Services Interface のインストール](#), (113 ページ)

DSCP 値の設定

ネットワークを通過するように、Cisco Jabber トラフィックを順位付ける RTP メディア パケットのヘッダーの DiffServ コード ポイント (DSCP) 値を設定します。

Cisco Unified Communications Manager のポート範囲

クライアントは、Cisco Unified Communications Manager の SIP プロファイルで使用するポート範囲を定義します。クライアントは、このポート範囲を使用して、ネットワークに RTP トラフィックを送信します。

SIP プロファイルでのポート範囲の指定

クライアントが RTP トラフィックを使用できるように、ポート範囲を指定するには、次のとおりに実行します。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
- ステップ 2** [デバイス (Device)] > [デバイスの設定 (Device Settings)] > [SIP プロファイル (SIP Profile)] の順に選択します。
- ステップ 3** 適切な SIP プロファイルを検索するか、新しい SIP プロファイルを作成します。
[SIP プロファイルの設定 (SIP Profile Configuration)] ウィンドウが開きます。
- ステップ 4** 次のフィールドにポート範囲を指定してください。
- 開始メディアポート (Start Media Port)
- メディア ストリームの開始ポートを定義します。このフィールドは、範囲の最小ポートを設定します。
- 終了メディア ポート (Stop Media Port)
- メディア ストリームの終了ポートを定義します。このフィールドは、範囲の最大ポートを設定します。
- ステップ 5** [設定の適用 (Apply Config)] を選択し、[OK] をクリックします。
-

関連トピック

[『8.6.x: SIP Profile Configuration』](#)

[『9.0.x: SIP profile setup』](#)

クライアントによるポート範囲の使用方法

Cisco Jabber は、SIP プロファイルで設定するポート範囲を均等に区切ります。クライアントは、次のようにポート範囲を使用します。

- ポート範囲の下半分は、オーディオ ストリーム用
- ポート範囲の上半分は、ビデオ ストリーム用

たとえば、3000 のスタート メディア ポートおよび 4000 のエンド メディア ポートを使用する場合、クライアントはポート経由で次のようにメディアを送信します。

- オーディオ ストリームのポート : 3000 ~ 3501
- ビデオ ストリームのポート : 3502 ~ 4000

オーディオメディアおよびビデオメディアのポート範囲を分割する結果として、クライアントにより識別可能なメディア ストリームが作成されます。IP パケットのヘッダー内の DSCP 値を設定することで、それらのメディア ストリームを分類し、優先させることができます。

DSCP 値を設定するオプション

次の表に、DSCP 値の設定に関するオプションを示します。

DSCP 値を設定する方式	Microsoft Windows 7
Microsoft グループ ポリシーを用いた DSCP 値の設定	Yes
ネットワーク スイッチおよびルータでの DSCP 値の設定	Yes
Cisco Unified Communications Manager での DSCP 値の設定	No

Cisco Unified Communications Manager での DSCP 値の設定

Cisco Unified Communications Manager で、音声およびビデオ メディア用の DSCP 値を設定できます。Cisco Jabber により、デバイス設定から DSCP 値が取得され、RTP メディア パケットの IP ヘッダーに直接適用されます。



制約事項

Microsoft Windows 7 といった新しいオペレーティング システムでは、Microsoft により、アプリケーションが IP ヘッダーで DSCP の値の設定をできないようにするセキュリティ機能が実行されます。したがって、Microsoft グループ ポリシーなど、DSCP 値をマークする代替方式を使用する必要があります。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
- ステップ 2** [システム (System)] > [サービス パラメータ (Service Parameters)] の順に選択します。
[サービス パラメータ設定 (Service Parameter Configuration)] ウィンドウが開きます。
- ステップ 3** 適切なサーバを選択してから、[Cisco CallManager (Cisco CallManager)] サービスを選択します。
- ステップ 4** [クラスタ全体のパラメータ (システム: QOS) (Clusterwide Parameters (System-QOS))] セクションを見つけます。
- ステップ 5** 適切な DSCP 値を設定し、[保存 (Save)] を選択します。
-

グループ ポリシーを用いた DSCP 値の設定

Microsoft Windows 7 といったそれ以降のオペレーティング システムで Cisco Jabber for Windows を展開する場合、Microsoft グループ ポリシーを使用して、DSCP 値を適用します。

グループ ポリシーを作成するには、次の Microsoft サポート記事の手順に従います: <http://technet.microsoft.com/en-us/library/cc771283%28v=ws.10%29.aspx>。

次の属性を用いて音声メディアとビデオメディアに別々のポリシーを作成する必要があります。

属性	音声ポリシー	ビデオ ポリシー	シグナリング ポリシー
アプリケーション名	CiscoJabber.exe	CiscoJabber.exe	CiscoJabber.exe
プロトコル	UDP	UDP	TCP
ポート番号または範囲	Cisco Unified Communications Manager の SIP プロファイルからの対応するポート番号または範囲。	Cisco Unified Communications Manager の SIP プロファイルからの対応するポート番号または範囲。	SIP は 5060 安全な SIP の場合は 5061
DSCP 値	46	34	24

ネットワーク内の DSCP 値の設定

スイッチおよびルータを設定し、RTP メディアの IP ヘッダーで DSCP 値をマーキングします。

ネットワーク内の DSCP 値を設定するには、クライアントアプリケーションからの異なるストリームを識別する必要があります。

メディア ストリーム

クライアントは、オーディオ ストリームとビデオ ストリームに異なるポート範囲を使用するため、それらのポート範囲に基づいて音声およびビデオ メディアを区別できます。SIP プロファイルのデフォルトのポート範囲を使用して、次のようにメディア パケットをマーキングする必要があります。

- 音声メディアは、EF として、16384 ～ 24574 のポートでストリーミング
- ビデオ メディアは、AF41 として、24575 ～ 32766 のポートでストリーミング

シグナリング ストリーム

SIP、CTI QBE、XMPP に必要な各種ポートに基づいて、クライアントおよびサーバ間のシグナリングを識別できます。たとえば、Cisco Jabber と Cisco Unified Communications Manager 間の SIP シグナリングは、ポート 5060 を介して行われます。

AF31 としてシグナリング パケットをマーキングする必要があります。

プロトコル ハンドラ

Cisco Jabber は、次のプロトコル ハンドラをオペレーティング システムに登録し、クリック ツール コールまたはクリック ツール IM 機能を Web ブラウザやその他のアプリケーションから使用できるようにします。

- XMPP:
Cisco Jabber でインスタント メッセージを開始し、チャット ウィンドウを開きます。
- IM:
Cisco Jabber でインスタント メッセージを開始し、チャット ウィンドウを開きます。
- TEL:
Cisco Jabber で音声またはビデオ コールを開始します。
- CISCOTEL:
Cisco Jabber で音声またはビデオ コールを開始します。
- SIP:
Cisco Jabber で音声またはビデオ コールを開始します。
- CISCOTELCONF:
Cisco Jabber との電話会議を開始します。

プロトコル ハンドラのレジストリ エントリ

プロトコル ハンドラとして登録するには、クライアントは Microsoft Windows レジストリの次の場所へ書き込みます。

- HKEY_CLASSES_ROOT\tel\shell\open\command
- HKEY_CLASSES_ROOT\xmpp\shell\open\command
- HKEY_CLASSES_ROOT\im\shell\open\command

2 つ以上のアプリケーションが同一プロトコルのハンドラとして登録される場合は、レジストリに最後に書き込まれたアプリケーションが優先されます。たとえば、Cisco Jabber が XMPP: のプロトコルハンドラとして登録され、その後に別のアプリケーションが XMPP: のプロトコルハンドラとして登録された場合、別のアプリケーションが Cisco Jabber よりも優先されます。

HTML ページのプロトコルハンドラ

HTML ページに、href 属性の一部としてプロトコルハンドラを追加します。HTML ページに表示されるハイパーリンクをクリックすると、クライアントはプロトコルに対して適切な処理を実行します。

HTML ページの TEL: および IM: プロトコルハンドラの例。

```
<html>
<body>
  <a href="TEL:1234">Call 1234</a><br/>
  <a href="IM:msmith@domain">Send an instant message to Mary Smith</a>
</body>
</html>
```

前の例では、ユーザがハイパーリンクをクリックして 1234 に発信すると、クライアントはその電話番号への音声コールを開始します。ユーザが Mary Smith にインスタントメッセージを送信するハイパーリンクをクリックすると、クライアントは Mary とのチャットウィンドウを開きます。

HTML ページの CISCOTEL:、SIP: および CISCOTELCONF: プロトコルハンドラの例。

```
<html>
<body>
  <a href="CISCOTEL:1234">Call 1234</a><br/>
  <a href="SIP:msmith@domain">Call Mary</a><br/>
  <a href="CISCOTELCONF:msmith@domain;amckenzi@domain">Weekly conference call</a>
</body>
</html>
```

前の例では、ユーザが 1234 へコールまたは Mary にコールのハイパーリンクをクリックすると、クライアントはその電話番号への音声コールを開始します。ユーザが ウィークリー会議コールのハイパーリンクをクリックすると、Mary、Adam およびリンクをクリックしたユーザの間で会議コールがセットアップされます。



ヒント

CISCOTELCONF: ハンドラ用の連絡先リストを追加し、会議コールを作成します。連絡先を区切るには、次の例のようにセミコロンを使用します。

```
CISCOTELCONF:user_a@domain.com;user_b@domain.com;user_c@domain.com;user_d@domain.com
```

HTML ページの XMPP: プロトコルハンドラを使用したグループチャットの例。

```
<html>
<body>
  <a href="XMPP:msmith@domain;amckenzi@domain">Create a group chat with Mary Smith and Adam McKenzie</a>
```

```
</body>
</html>
```

前の例では、ユーザが Mary Smith および Adam McKenzie とのグループ チャットを作成するハイパーリンクをクリックすると、クライアントは Mary および Adam とのグループ チャット ウィンドウを開きます。



ヒント

XMPP: および IM: ハンドラに連絡先リストを追加し、グループ チャットを作成します。連絡先を区切るには、次の例のようにセミコロンを使用します。

```
XMPP:user_a@domain.com;user_b@domain.com;user_c@domain.com;user_d@domain.com
```

音声およびビデオのパフォーマンス参照

Cisco Jabber のオーディオおよびビデオのパフォーマンスについて学習します。



注目

次のデータは、ラボ環境でのテストに基づいています。このデータは、帯域幅の使用状況の点で予想できる内容を提供することを目的としています。このトピックの内容は、完全な内容を示したり、帯域幅の使用状況に影響を与える可能性があるすべてのメディア シナリオを反映したりするものではありません。

オーディオのビット レート

次の表に、音声のビット レートを示します。

コーデック	RTP ペイロード (kbit/秒)	実際のビットレート (kbit/秒)	注記
g.722.1	24/32	54/62	高品質な圧縮
g.711	64	80	標準的な非圧縮
g.729a	8	38	低品質な圧縮

ビデオのビット レート

次の表に、g.711 音声でのビデオのビットレートを示します。

解像度	ピクセル	g.711 音声で測定されたビットレート (kbit/秒)
w144p	256 x 144	156

解像度	ピクセル	g.711 音声で測定されたビットレート (kbit/秒)
w288p これが Cisco Jabber のビデオ レンダリングウィンドウのデフォルト サイズです。	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1280 x 720	1300

上記の表に関する注意事項:

- この表は、想定される解像度をすべて網羅しているわけではありません。
- 測定されたビット レートは、実際の使用帯域幅 (RTP ペイロード + IP パケットのオーバーヘッド) です。

プレゼンテーションビデオのビットレート

次の表に、プレゼンテーションビデオのビットレートを示します。

ピクセル	2 fps でのワイヤビットレートの概算値 (kbit/秒)	8 fps でのワイヤビットレートの概算値 (kbit/秒)
720 x 480	41	164
704 x 576	47	188
1024 x 768	80	320
1280 x 720	91	364
1280 x 800	100	400

上記の表に関する注意事項:

- Cisco Jabber は、8 fps でキャプチャし、2 ~ 8 fps で伝送します。
- この表の値には、音声は含まれていません。

ネゴシエートされた最大ビットレート

[領域の設定 (Region Configuration)] ウィンドウで Cisco Unified Communications Manager のペイロードの最大ビットレートを指定します。この最大ペイロードビットレートには、パケット

オーバーヘッドは含まれません。したがって、使用される実際のビット レートは、指定した最大ペイロード ビット レートよりも大きくなります。

次の表では、Cisco Jabber によるペイロードの最大ビット レートの割り当て方法について説明します。

デスクトップ共有セッション	オーディオ	双方向ビデオ（メイン ビデオ）	プレゼンテーションビデオ（デスクトップ共有ビデオ）
No	Cisco Jabber では、音声の最大ビット レートを使用します。	Cisco Jabber では、次のように残りのビット レートを割り当てます。 ビデオ コール の最大ビット レートから音声のビット レートを引きます。	-
Yes	Cisco Jabber では、音声の最大ビット レートを使用します。	Cisco Jabber では、音声のビット レートを引いた後に残りの帯域幅の半分を割り当てます。	Cisco Jabber では、音声のビット レートを引いた後に残りの帯域幅の半分を割り当てます。

帯域幅のパフォーマンス期待値

Cisco Jabber では、音声のビット レートを分けてから、インタラクティブ ビデオとプレゼンテーション ビデオの間で残りの帯域幅を均等に分けます。次の表では、帯域幅ごとに達成できるパフォーマンスを理解するのに役立つ情報について説明します。

アップロード速度	オーディオ	音声 + インタラクティブビデオ（メイン ビデオ）	音声 + プレゼンテーションビデオ（デスクトップ共有ビデオ）	音声 + インタラクティブビデオ + プレゼンテーションビデオ
125 kbps（VPN）	g.711 の帯域幅のしきい値レベルです。帯域幅は g.729a および g.722.1 用に十分です。	帯域幅はビデオ用に不十分です。	帯域幅はビデオ用に不十分です。	帯域幅はビデオ用に不十分です。
384 kbps（VPN）	帯域幅は音声コーデック用に十分です。	w288p（512x288）（30 fps）	1280 x 800（2 fps 以上）	w144p（256 x 144）（30 fps） + 1280 x 720（2 fps 以上）

アップロード速度	オーディオ	音声+インタラクティブビデオ（メインビデオ）	音声+プレゼンテーションビデオ（デスクトップ共有ビデオ）	音声+インタラクティブビデオ+プレゼンテーションビデオ
384 kbps（企業ネットワーク）	帯域幅は音声コーデック用に十分です。	w288p（512x288）（30 fps）	1280 x 800（2 fps 以上）	w144p（256 x 144）（30 fps）+ 1280 x 800（2 fps 以上）
1000 kbps	帯域幅は音声コーデック用に十分です。	w576p（1024x576）（30 fps）	1280 x 800（8 fps）	w288p（512 x 288）（30 fps）+ 1280 x 800（8 fps）
2000 kbps	帯域幅は音声コーデック用に十分です。	w720p30（1280 x 720）（30 fps）	1280 x 800（8 fps）	w288p（1024 x 576）（30 fps）+ 1280 x 800（8 fps）

VPN でペイロードのサイズを大きくすると、帯域幅の消費が増えることに注意してください。

ビデオ レート アダプテーション

Cisco Jabber はビデオ レート アダプテーションを利用し、最適なビデオ品質を調整します。ビデオ レート アダプテーションは、ビデオのビット レートのスループットを動的に増減して、有効な IP パスの帯域幅でリアルタイムの変動を処理します。

Cisco Jabber ユーザは、ビデオ コールが低解像度で開始し、短期間に高解像度になることを想定します。Cisco Jabber では、履歴を保存して、後続のビデオ コールが最適な解像度で開始するようにします。



第 3 章

サーバのセットアップ

クライアントをインストールする前に、サーバをセットアップします。ユーザを環境に追加し、サービスでユーザをプロビジョニングします。

- [サーバセットアップガイド, 35 ページ](#)

サーバ セットアップ ガイド

『*Cisco Jabber Server Setup Guide*』は、Cisco Jabber のサービスの設定を完了するために必要な作業について説明します。

関連トピック

- [サーバセットアップガイド](#)



第 4 章

証明書の検証設定

Cisco Jabber では、証明書の検証を使用して、サーバとのセキュア接続を確立します。

セキュア接続を確立しようとする場合、サーバは Cisco Jabber に証明書を提示します。

Cisco Jabber では、Microsoft Windows 証明書ストアの証明書に対して証明書を検証します。

クライアントが証明書を検証できない場合、ユーザに証明書を受け入れるかどうか確認するよう指示されます。

Expressway Mobile and Remote Access 展開では、オンライン証明書ステータスプロトコル (OCSP) またはオンライン証明書失効リスト (CRL) を使用して証明書の失効状態を取得する場合、Cisco Jabber クライアントは 5 秒未満の応答時間を予期します。接続は、応答時間が予測された 5 秒を超えた場合、失敗します。

- ・ [オンプレミス サーバ, 37 ページ](#)
- ・ [クラウドベースのサーバ, 44 ページ](#)

オンプレミス サーバ

オンプレミス サーバがどの証明書をクライアントに提示するかを確認し、また、署名された証明書の取得作業も確認します。

必要な証明書

オンプレミス サーバは、Cisco Jabber とのセキュアな接続を確立するために、次の証明書を提示します。

サーバ	証明書
Cisco Unified PresenceまたはCisco Unified Communications Manager IM and Presence Service	HTTP (Tomcat) XMPP

サーバ	証明書
Cisco Unified Communications Manager	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)
Cisco WebEx Meetings Server	HTTP (Tomcat)
Cisco VCS Expressway Cisco Expressway-E	Server certificate (HTTP および XMPP に使用)

特記事項

- 証明書の署名プロセスを開始する前に、Cisco Unified PresenceまたはCisco Unified Communications Manager IM and Presence Serviceの最新の Service Update (SU) を適用する必要があります。
- 必要な証明書は、すべてのサーババージョンに適用されます。
- クラスタ、サブスクリバおよびパブリッシャの各ノードは、Tomcat サービスを実行し、HTTP の証明書でクライアントを提示できます。
クラスタ内の各ノードの証明書に署名する必要があります。
- クライアントとCisco Unified Communications Manager間の SIP シグナリングを確立するには、Certification Authority Proxy Function (CAPF) 登録を使用する必要があります。

認証局により署名された証明書の取得

シスコは、次の認証局 (CA) のいずれかにより署名されたサーバ証明書を使用することを推奨します。

パブリック CA

サードパーティ企業が、サーバの識別情報を確認し、信頼できる証明書を発行します。

プライベート CA

自身でローカルの CA を作成および管理し、信頼できる証明書を発行します。

署名プロセスは、各サーバごとに異なり、サーバのバージョン間でも異なります。各サーバのすべてのバージョンに関する詳細な手順については、このマニュアルの範囲外になります。CA により署名された証明書を取得する方法の詳細な指示については、該当するサーバのマニュアルを参照してください。ただし、手順の概要を次に示します。

手順

-
- | | |
|---------------|--|
| ステップ 1 | クライアントに証明書を提示できる各サーバで証明書署名要求（CSR）を作成します。 |
| ステップ 2 | CA に各 CSR を送信します。 |
| ステップ 3 | CA が各サーバに発行する証明書をアップロードします。 |
-

証明書署名要求の形式と要件

パブリック CA は、通常 CSR に特定の形式に確認するよう要求します。たとえば、パブリック CA は、次のような CSR を受け入れる場合があります。

- Base 64 エンコードである。
- 組織、OU、その他フィールドに @&! などの特定の文字を含まない。
- サーバの公開キーで特定のビット長を使用する。

同様に、複数ノードから CSR を送信すると、パブリック CA は、すべての CSR で情報の整合性がとれていることを必要とする場合があります。

CSR の問題を回避するために、CSR を送信するパブリック CA からの形式の要件を確認する必要があります。次に、サーバを構成する際に、入力する情報がパブリック CA が要求する形式に適合していることを保証する必要があります。

FQDN あたり証明書 1 つ：いくつかのパブリック CA は、完全修飾ドメイン名（FQDN）あたり 1 つの証明書にのみ署名します。

たとえば、単一 Cisco Unified Communications Manager IM and Presence Service ノードの HTTP および XMPP の証明書に署名するには、異なる各パブリック CA に各 CSR を送信する必要がある場合があります。

失効サーバ

証明書を検証するには、失効情報を提供できる到達可能なサーバの [CDP] または [AIA] フィールドに HTTP URL が証明書に含まれている必要があります。

次のシナリオのいずれかの場合、無効な証明書のダイアログメッセージが表示されます。

- 証明書に失効情報が含まれない。
- 失効サーバにアクセスできない。

証明書が検証済みであることを確認するには、認証局（CA）が発行した証明書を取得したときに、次の要求のいずれかを満たしている必要があります。

- [CRL Distribution Point (CDP)] フィールドに、失効サーバの認証失効リスト (CRL) への HTTP URL が含まれていることを確認します。
- [Authority Information Access (AIA)] フィールドに、オンライン証明書ステータス プロトコル (OCSP) サーバの HTTP URL が含まれている。

証明書のサーバ識別情報

署名プロセスの一部として、CA は証明書のサーバ識別情報を指定します。クライアントがその証明書を検証する場合、次のことを確認します。

- 信頼できる機関が証明書を発行している。



(注) パブリック CA は、通常、サーバの識別情報として、IP アドレスではなく、ドメインを含む完全修飾ドメイン名 (FQDN) を必要とします。

ID フィールド

クライアントは、識別情報の一致に関して、サーバ証明書の次の識別子フィールドを確認します。

XMPP 証明書

- SubjectAltName\OtherName\xmppAddr
- SubjectAltName\OtherName\srvName
- SubjectAltName\dnsNames
- Subject CN

HTTP 証明書

- SubjectAltName\dnsNames
- Subject CN



ヒント [件名 CN (SubjectCN)] フィールドには、左端の文字 (たとえば、*.cisco.com) としてワイルドカード (*) を含めることができます。

ID の不一致の防止

ユーザが IP アドレスでサーバに接続し、サーバ証明書が FQDN でサーバを識別しようとする、クライアントは、信頼できるポートとサーバを識別できないため、ユーザにとって良い結果をもたらしません。

サーバ証明書が FQDN でサーバを識別する場合、環境全体の FQDN として各サーバ名を指定する必要があります。

クライアントへの XMPP ドメインの提供

クライアントは、FQDN ではなく XMPP ドメインを使用して、XMPP 証明書を識別します。XMPP の証明書は ID フィールドに XMPP ドメインを含める必要があります。

クライアントがプレゼンス サーバに接続しようとする、プレゼンス サーバはクライアントに XMPP ドメインを提供します。その際に、クライアントは XMPP 証明書に対するプレゼンス サーバの識別情報を検証します。

プレゼンス サーバがクライアントに XMPP ドメインを提供することを保証するため、次の手順を実行します。

手順

- ステップ 1** 次のとおり、プレゼンス サーバの管理インターフェイスを開きます。

Cisco Unified Communications Manager IM and Presence Service

[Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] インターフェイスを開きます。

Cisco Unified Presence

[Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] インターフェイスを開きます。

- ステップ 2** [システム (System)] > [セキュリティ (Security)] > [設定 (Settings)] を選択します。

- ステップ 3** [XMPP 証明書の設定 (XMPP Certificate Settings)] セクションを検索します。

- ステップ 4** [XMPP サーバ間証明書のサブジェクト代替名のドメイン ネーム (Domain name for XMPP Server-to-Server Certificate Subject Alternative Name)] フィールドにプレゼンス サーバのドメインを指定します。

- ステップ 5** [XMPP サーバ証明書のサブジェクト代替名のドメイン ネームを使用 (Use Domain Name for XMPP Certificate Subject Alternative Name)] チェックボックスを選択します。

- ステップ 6** [保存 (Save)] を選択します。

クライアントコンピュータのルート証明書のインポート

サーバ証明書はクライアントコンピュータの信頼ストアに存在する関連のルート証明書が必要です。Cisco Jabberは、サーバが信頼ストアのルート証明書に対して提示する証明書を検証します。

パブリック CA によって署名されたサーバ証明書を取得する場合、パブリック CA はすでにクライアントコンピュータの信頼ストアで提示されるルート証明書を持っている必要があります。この場合、クライアントコンピュータのルート証明書をインポートする必要はありません。

次の場合、Microsoft Windows 証明書ストアにルート証明書をインポートする必要があります。

- 証明書がプライベート CA などの信頼ストアではない CA によって署名されます。

[信頼されたルート証明機関 (Trusted Root Certification Authorities)] ストアにプライベート CA 証明書をインポートします。

- 証明書には自己署名します。

[エンタープライズ信頼 (Enterprise Trust)] ストアに自己署名した証明書をインポートします。



重要

ルート証明書が信頼ストアにない場合、Cisco Jabberは環境内の各サーバからの証明書を受け入れるようユーザに指示します。

クライアントがユーザ証明書を受け入れるよう指示すると、ユーザは次のことを実行することができます。

証明書の受け入れ

クライアントは、[エンタープライズ信頼 (Enterprise Trust)] ストアに証明書を保存します。

証明書の拒否

クライアントは、次のことを実行しません。

- 証明書を保存する。
- サーバに接続する。
- エラー通知を表示する。

ユーザがクライアントを再起動した場合、再度証明書を受け入れるように指示します。

次のことを含め、Microsoft Windows 証明書ストアに証明書をインポートする適切な方式を使用できます。証明書のインポートの詳細については、適切なMicrosoftマニュアルを参照してください。

- 個別に証明書をインポートするために、[証明書のインポート ウィザード (Certificate Import Wizard)] を使用します。
- Microsoft Windows Server で CertMgr.exe コマンドライン ツールを持つユーザに証明書を展開します。



(注) このオプションでは、Microsoft 管理コンソールの CertMgr.msc ではなく、Certificate Manager ツールの CertMgr.exe を使用する必要があります。

- Microsoft Windows Server でグループ ポリシー オブジェクト (GPO) でユーザに証明書を展開します。

クライアントコンピュータでの証明書の展開

すべてのサーバ証明書は、クライアントコンピュータの Keychain で関連する証明書が必要です。Cisco Jabber は、サーバが Keychain に対して証明書として提示する証明書を検証します。



重要

ルート証明書が Keychain がない場合、Cisco Jabber は環境内の各サーバからの証明書を受け入れるようユーザに指示します。

クライアントがユーザ証明書を検証するよう指示すると、ユーザは次のことを実行することができます。

サーバ名を常に信頼する。

クライアントは、Keychain に証明書を保存する。

キャンセル (Cancel)

クライアントは、次のことを実行しません。

- 証明書を保存する。
- サーバに接続する。

続行 (Continue)

クライアントは接続されますが、ユーザがクライアントを再起動した場合、再度証明書を受け入れるように指示されます。

Cisco Unified OS の管理インターフェイスから証明書をダウンロードすることで、警告ダイアログが表示されないようになります。ユーザに対して自己署名証明書を展開するには、次の手順を実行します。

手順

-
- ステップ 1** シスコの各サーバに対して、Cisco Unified OS 管理インターフェイスから対応する“tomcat-trust”証明書をダウンロードします。[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。
- ステップ 2** .pem の拡張子で証明書を 1 つのファイルに連結します（たとえば、“companyABCcertificates.pem”）。
- ステップ 3** ファイルを Cisco Jabber ユーザに送信し、ダブルクリックするよう要求します。これにより、Keychain Access アプリケーションが起動し、証明書がインポートされます。
- （注） オペレーティングシステムでは、ユーザがインポートされている各証明書の Mac OS X 管理のパスワードを入力する必要があります。
-

クラウドベースのサーバ

Cisco WebEx Messenger および Cisco WebEx Meeting Center は、Cisco Jabber に対して次の証明書を提示します。

- CAS
- WAPI


重要

Cisco WebEx は、証明書はパブリックな認証局 (CA) によって署名されます。Cisco Jabber は、これらの証明書を検証し、クラウドベースサービスのセキュアな接続を確立します。ただし、クラウドサービスを使用する場合に、証明書を発行したり、署名したりする必要はありません。

プロフィール写真の URL の更新

クラウドベースの展開では、ユーザを追加またはインポートする際に、Cisco WebEx により、プロフィール写真に一意的 URL が割り当てられます。Cisco Jabber により連絡先情報が解決される場合、写真がホスティングされている URL の Cisco WebEx からプロフィール写真が取得されます。

プロフィール写真の URL は、HTTP セキュア (https://server_name/) を使用して、クライアントに証明書を提示します。URL のサーバ名が次の場合：

Cisco WebEx ドメインを含む完全修飾ドメイン名 (FQDN)

クライアントは、Cisco WebEx 証明書に対してプロフィール写真をホスティングしている Web サーバを検証します。

IP アドレス

クライアントは、Cisco WebEx 証明書に対してプロフィール写真をホスティングしている Web サーバを検証しません。

この場合、プロフィール写真の URL の IP アドレスで連絡先をルックアップする場合は常に、証明書を受け入れるようクライアントがユーザに指示します。



重要

- シスコは、サーバ名としての IP アドレスを含むすべてのプロフィール写真の URL を更新することを推奨します。クライアントが証明書を受け入れるようにユーザに指示しないことを保証するために、Cisco WebEx ドメインを含む FQDN と IP アドレスを置き換える必要があります。
- 写真を更新すると、Cisco Jabber で写真が更新されるまで最大 24 時間かかることがあります。

プロフィール写真の URL を更新するには、次の手順を実行します。詳細については、該当する Cisco WebEx マニュアルを参照してください。

手順

- ステップ 1** Cisco WebEx 管理ツールを使用して、CSV ファイルのユーザ連絡先データを CSV ファイル形式でエクスポートします。
- ステップ 2** 必要に応じて、userProfilePhotoURL フィールドの Cisco WebEx ドメインと IP アドレスを置き換えます。
- ステップ 3** CSV ファイルを保存します。
- ステップ 4** Cisco WebEx 管理ツールを使用して、CSV ファイルをインポートします。



第 5 章

展開オプション

Cisco Jabber の展開オプションについて説明します。

- [オンプレミスの導入, 47 ページ](#)
- [クラウドベース展開, 54 ページ](#)
- [クライアントによるサービスへの接続方法, 57 ページ](#)
- [クラウドベース SSO, 76 ページ](#)
- [Expressway Mobile and Remote Access の展開, 77 ページ](#)
- [仮想環境での展開, 85 ページ](#)

オンプレミスの導入

オンプレミス展開では、コンピュータ ネットワーク上のすべてのサービスを設定、管理、保守します。

製品モード

次のモードでクライアントを展開できます。

フル UC と Cisco Jabber for Everyone (IM のみ)

デフォルトの製品モードは、ユーザのプライマリ認証が既存のサーバにある 1 つです。最低でも、ユーザはインスタント メッセージとプレゼンス機能を有しています。

フル UC と Cisco Jabber for Everyone の両方の展開には、デフォルトの製品モードを使用します。

フル UC を展開するために、インスタント メッセージとプレゼンス機能を有効にします。ボイス メールと会議機能に加えて、オーディオおよびビデオ用のデバイスを持つユーザをプロビジョニングします。

Cisco Jabber for Everyone を展開するために、インスタント メッセージとプレゼンス機能を有効にします。オプションとして、クライアントで制御できるデスク フォン デバイスを持つユーザをプロビジョニングできます。

電話機モード

電話機モードで、ユーザのプライマリ認証は Cisco Unified Communications Manager にあります。

電話機モードを展開するには、音声およびビデオ機能のデバイスを持つユーザをプロビジョニングします。また、ボイス メールなどの追加サービスを持つ個人をプロビジョニングできます。

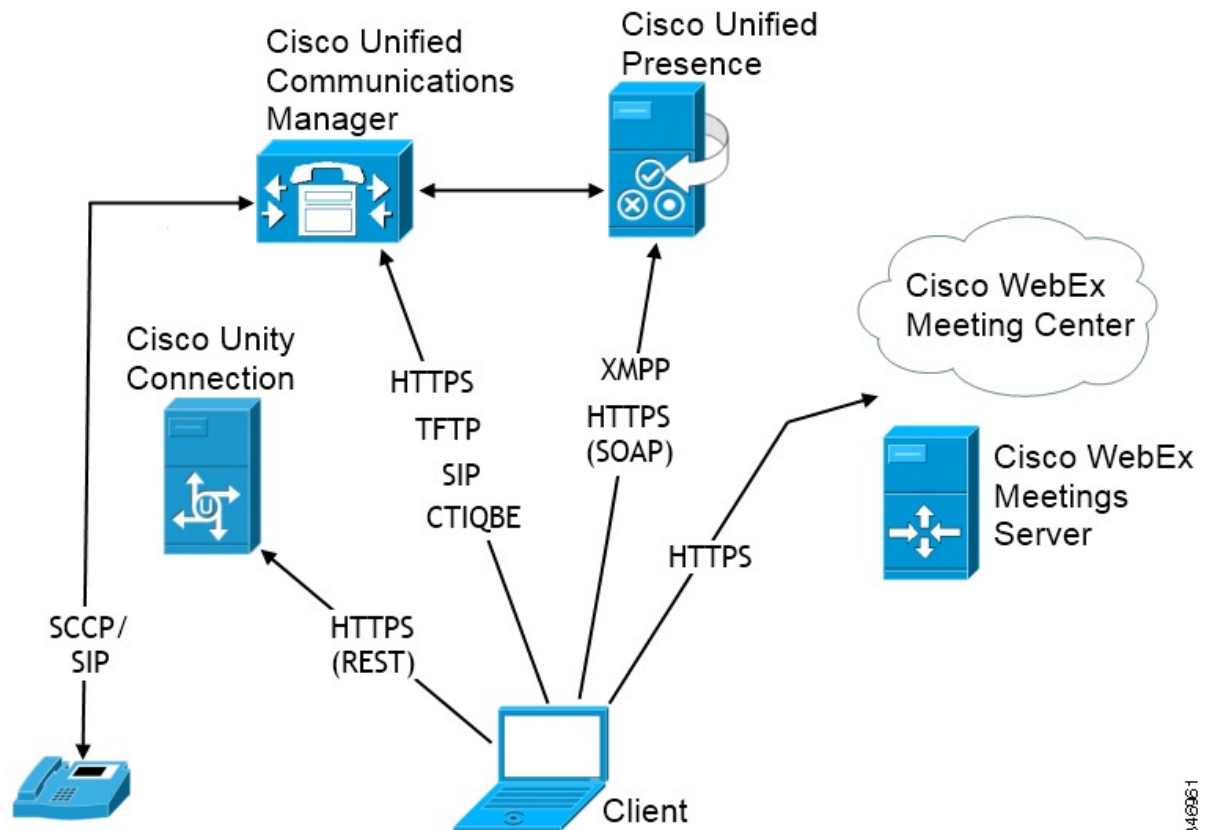
デフォルト モードの図

デフォルトの製品モードでの オンプレミス 導入のためのアーキテクチャ図を確認します。

Cisco Unified Presence との図

次の図は、Cisco Unified Presence を含む オンプレミス 展開のアーキテクチャを示しています。

図 1: オンプレミスのアーキテクチャ



次は、オンプレミス 展開で使用可能なサービスです。

プレゼンス

ユーザは、アベイラビリティを公開し、Cisco Unified Presence を介して、その他のユーザのアベイラビリティを登録します。

チャット/IM

ユーザは、Cisco Unified Presence を介してインスタント メッセージを送受信します。

音声通話

ユーザは、デスク フォン デバイスを介して、またはCisco Unified Communications Manager を介してコンピュータで音声コールを発信します。

ビデオ

ユーザは、画面を共有し、Cisco Unified Communications Manager を介してビデオ コールを発信します。

ボイスメール

ユーザは、Cisco Unity Connection を介してボイス メッセージを送受信します。

会議

次のいずれかと統合します。

Cisco WebEx Meeting Center

ホステッド会議機能を実現します。

Cisco WebEx Meetings Server

オンプレミス会議機能を提供します。

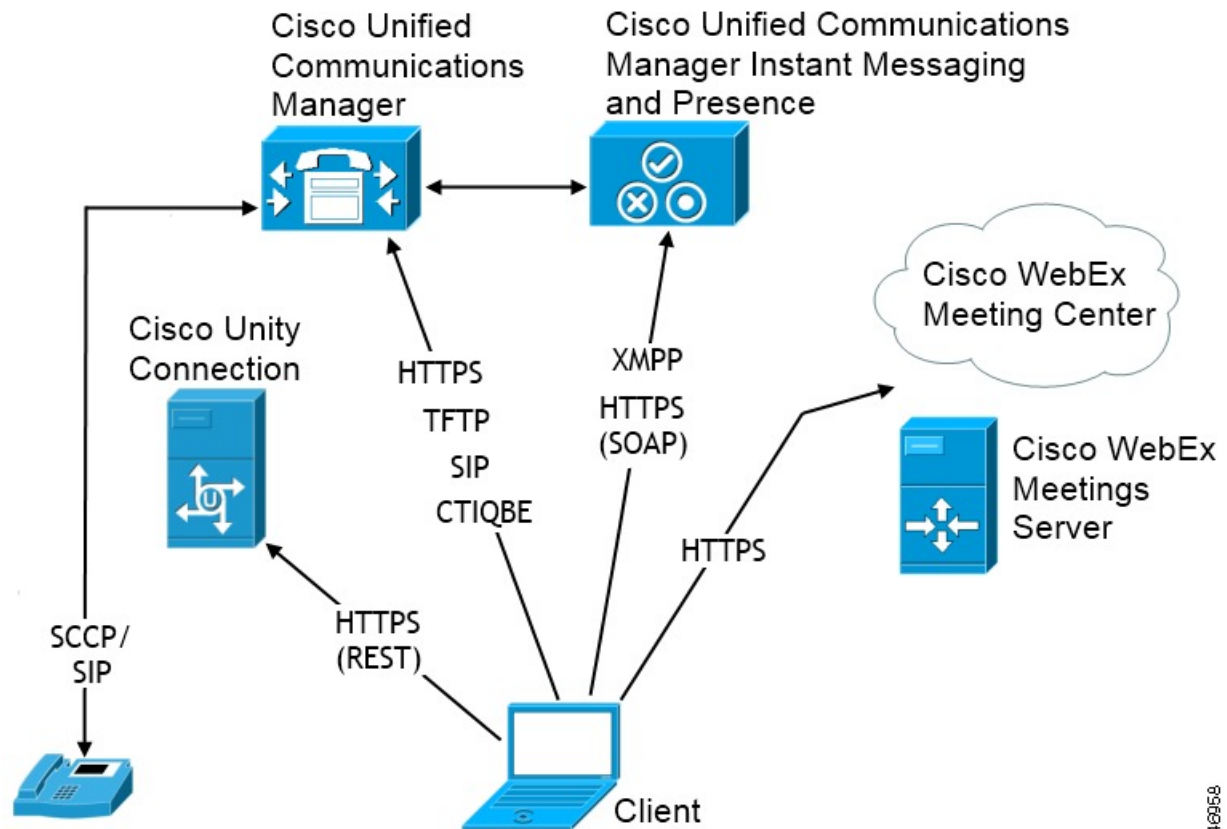
関連トピック

[ディレクトリ ソースとの統合, \(173 ページ\)](#)

Cisco Unified Communications IM and Presence との図

次の図は、Cisco Unified Communications IM and Presence を含む オンプレミス 展開のアーキテクチャを示しています。

図 2: オンプレミスのアーキテクチャ



次は、オンプレミス 展開で使用可能なサービスです。

プレゼンス

ユーザは、アベイラビリティを公開し、Cisco Unified Communications IM and Presence を介して、その他のユーザのアベイラビリティを登録します。

チャット/IM

ユーザは、Cisco Unified Communications IM and Presence を介してインスタントメッセージを送受信します。

音声通話

ユーザは、デスク フォン デバイスを介して、またはCisco Unified Communications Manager を介してコンピュータで音声コールを発信します。

ビデオ

ユーザは、画面を共有し、Cisco Unified Communications Manager を介してビデオ コールを発信します。

ボイスメール

ユーザは、Cisco Unity Connection を介してボイス メッセージを送受信します。

会議

次のいずれかと統合します。

Cisco WebEx Meeting Center

ホステッド会議機能を実現します。

Cisco WebEx Meetings Server

オンプレミス会議機能を提供します。

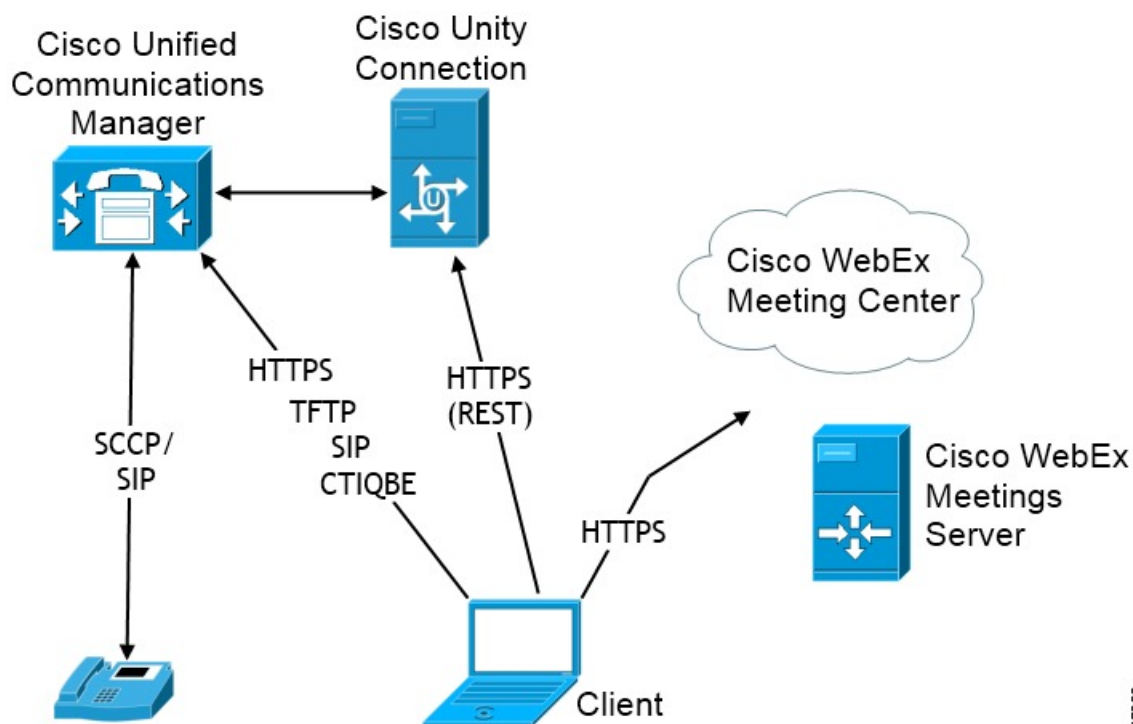
関連トピック

[ディレクトリ ソースとの統合, \(173 ページ\)](#)

電話機モード ダイアグラム

次の図は、電話機モードでの オンプレミス 展開のアーキテクチャを示しています。

図 3: 電話機モードのアーキテクチャ



346903

次は、電話機モード 展開で使用可能なサービスです。

音声通話

ユーザは、デスク フォン デバイスを介して、またはCisco Unified Communications Manager を介してコンピュータで音声コールを発信します。

ビデオ

ユーザは、画面を共有し、Cisco Unified Communications Manager を介してビデオ コールを発信します。

ボイスメール

ユーザは、Cisco Unity Connection を介してボイス メッセージを送受信します。

会議

次のいずれかと統合します。

Cisco WebEx Meeting Center

ホステッド会議機能を実現します。

Cisco WebEx Meetings Server

オンプレミス会議機能を提供します。

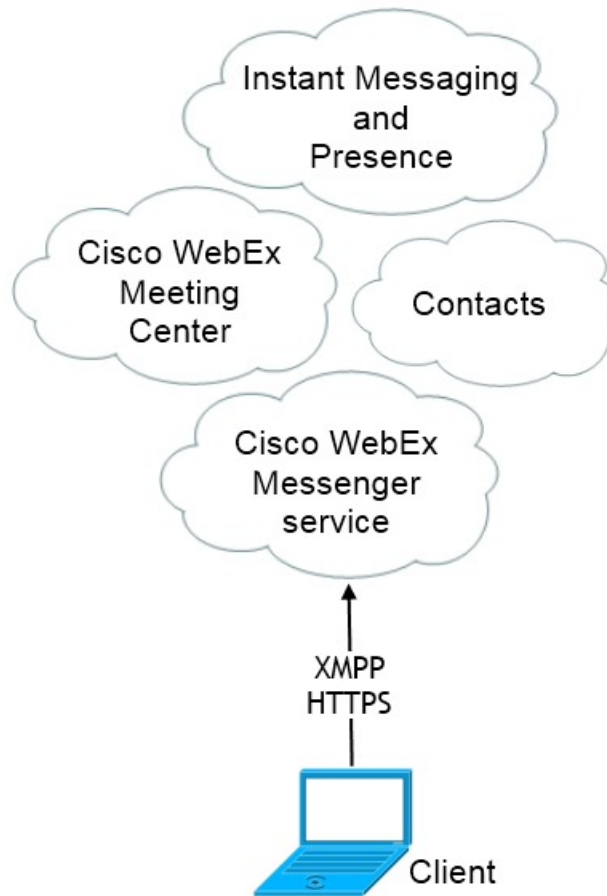
クラウドベース展開

クラウドベースの展開では、ユーザのプライマリ認証はCisco WebEx Messengerサービスに対してです。Cisco WebEx は、すべてのサービスをホスティングします。Cisco WebEx 管理ツールで、クラウドベースの展開を管理および監視します。

クラウドベースの図

次の図は、クラウドベース 展開のアーキテクチャを図示したものです。

図 4: クラウドベースのアーキテクチャ



次は、クラウドベース 展開で使用可能なサービスです。

発信元

Cisco WebEx Messenger サービスは、連絡先の解決を提供します。

プレゼンス

Cisco WebEx Messenger サービスは、ユーザがアベイラビリティを公開し、その他のユーザのアベイラビリティを登録することを可能にします。

チャット/IM

Cisco WebEx Messenger サービスは、ユーザがインスタントメッセージを送受信することを可能にします。

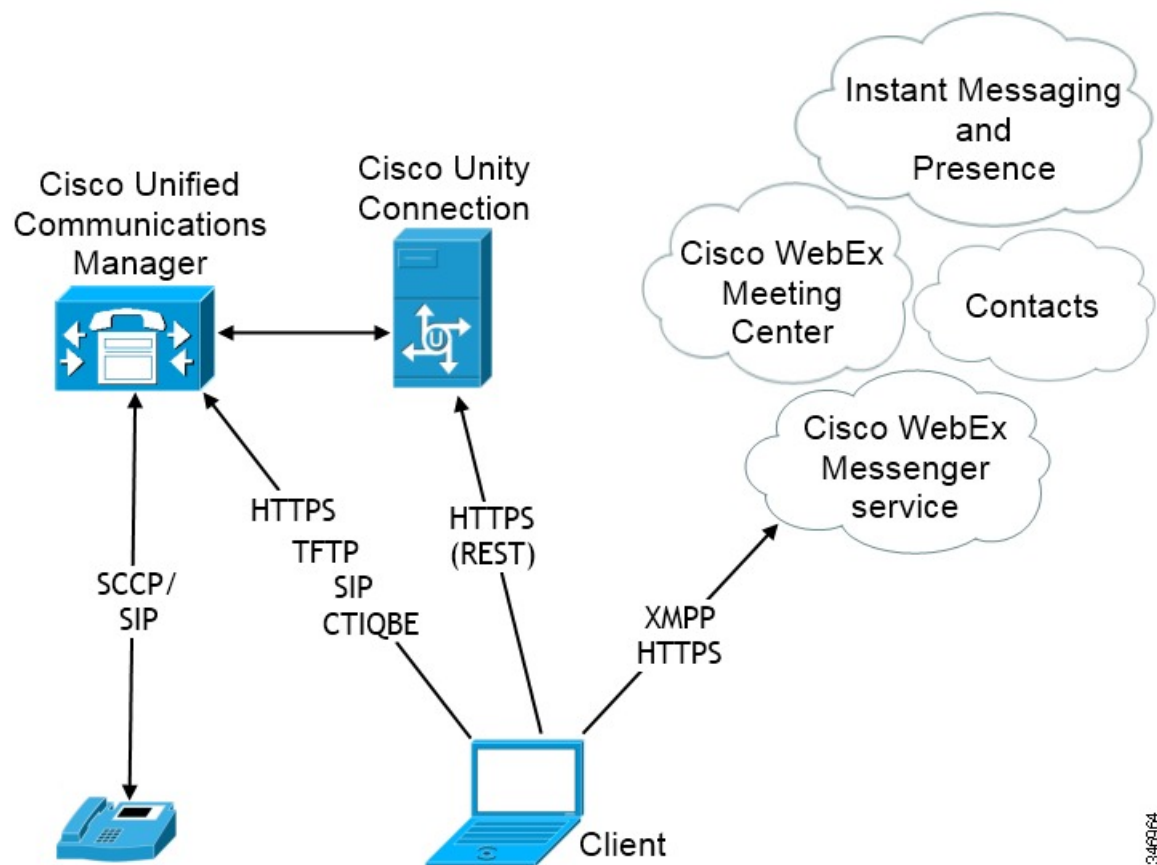
会議

Cisco WebEx Meeting Center ホステッド会議機能を実現します。

ハイブリッドクラウドベースの図

次の図は、ハイブリッドクラウドベース展開のアーキテクチャを図示したものです。

図 5: ハイブリッドクラウドベースのアーキテクチャ



346564

次は、ハイブリッドクラウドベース展開で使用可能なサービスです。

発信元

Cisco WebEx Messenger サービスは、連絡先の解決を提供します。

プレゼンス

Cisco WebEx Messenger サービスは、ユーザがアベイラビリティを公開し、その他のユーザのアベイラビリティを登録することを可能にします。

チャット/IM

Cisco WebEx Messenger サービスは、ユーザがインスタント メッセージを送受信することを可能にします。

会議

Cisco WebEx Meeting Center ホステッド会議機能を実現します。

音声通話

ユーザは、デスク フォン デバイスを介して、またはCisco Unified Communications Manager を介してコンピュータで音声コールを発信します。

ビデオ

ユーザは、画面を共有し、Cisco Unified Communications Manager を介してビデオ コールを発信します。

ボイスメール

ユーザは、Cisco Unity Connection を介してボイス メッセージを送受信します。

クライアントによるサービスへの接続方法

サービスに接続するには、Cisco Jabber により次の情報が要求されます。

- ユーザがクライアントにログインをできるようにする認証ソース。
- サービスのロケーション

次の方法でクライアントに情報を提供することが可能です。

サービス ディスカバリ

クライアントは、自動的にサービスを探し出し、接続します。

手動接続設定

ユーザは、クライアントのユーザ インターフェイスで手動により接続設定を入力します。

ブートストラップ ファイル

インストール時に手動で接続設定を入力します。

推奨される接続方法

サービスの接続に必要な情報をクライアントに提供するために使用する必要がある方法は、導入タイプ、サーバのバージョン、製品モードによって異なります。次の表では、さまざまな導入方法とクライアントに必要な情報を提供する方法について詳しく示しています。

オンプレミス展開

製品モード	サーバのバージョン	検出方法	Non-DNS 方式
フル UC (デフォルトモード)	バージョン 9 以降 : <ul style="list-style-type: none"> Cisco Unified Communications Manager Cisco Unified Communications Manager IM and Presence Service 	<code>_cisco-uds.<domain></code> に対する DNS SRV 要求	次のインストーラスイッチと値を使用する。 <ul style="list-style-type: none"> AUTHENTICATOR=CUP CUP_ADDRESS= <presence_server_address>
フル UC (デフォルトモード)	バージョン 8.x : <ul style="list-style-type: none"> Cisco Unified Communications Manager Cisco Unified Presence 	<code>_cuplogin.<domain></code> に対する DNS SRV 要求	次のインストーラスイッチと値を使用する。 <ul style="list-style-type: none"> AUTHENTICATOR=CUP CUP_ADDRESS= <presence_server_address>
IM 専用 (デフォルトモード)	バージョン 9 以降 : Cisco Unified Communications Manager IM and Presence Service	<code>_cisco-uds.<domain></code> に対する DNS SRV 要求	次のインストーラスイッチと値を使用する。 <ul style="list-style-type: none"> AUTHENTICATOR=CUP CUP_ADDRESS= <presence_server_address>
IM 専用 (デフォルトモード)	バージョン 8.x : Cisco Unified Presence	<code>_cuplogin.<domain></code> に対する DNS SRV 要求	次のインストーラスイッチと値を使用する。 <ul style="list-style-type: none"> AUTHENTICATOR=CUP CUP_ADDRESS= <presence_server_address>

製品モード	サーバのバージョン	検出方法	Non-DNS 方式
電話機モード	バージョン 9 以降 : Cisco Unified Communications Manager	_cisco-uds.<domain> に対する DNS SRV 要求	次のインストーラ スイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUCM • TFTP=<CUCM_address> • CCMCIP=<CUCM_address> • PRODUCT_MODE=phone_mode
電話機モード	バージョン 8.x : Cisco Unified Communications Manager	手動接続設定またはブートストラップ ファイル	次のインストーラ スイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUCM • TFTP=<CUCM_address> • CCMCIP=<CUCM_address> • PRODUCT_MODE=phone_mode



(注) Cisco Jabber バージョン 9.6 以降では、_cuplogin DNS SRV 要求を使用して完全な Unified Communications およびインスタントメッセージサービスのみを検出できますが、_cisco-uds の要求がある場合は要求が優先されます。

新規インストールの最初のログイン時に電子メール画面をバイパスする場合、DNS レコードが存在するドメインの値を指定するために SERVICES_DOMAIN インストーラのスイッチを使用します。



(注) Cisco Jabber for Windows 9.2 からアップグレードしている場合、サービス ドメインがキャッシュ設定から読み取られます。

ハイブリッドクラウドベースの展開

サーバのバージョン	接続方法
Cisco WebEx Messenger	<a href="http://login.webexconnect.com/cas/FederatedSSO?org=<domain>">http://login.webexconnect.com/cas/FederatedSSO?org=<domain> に対する HTTPS 要求

クラウドベース展開

展開タイプ	接続方法
シングル サインオン (SSO)	SSO_ORG_DOMAIN 引数を設定する Cisco WebEx 管理ツール およびブートストラップ ファイル。
SSO に対しては有効ではありません	Cisco WebEx 管理ツール

認証ソース

認証ソースまたはオーセンティケーターにより、ユーザはクライアントにログインすることができます。

認証ソースには、次の 3 つがあります。

Cisco Unified Presence

フル UC または IM のみでのオンプレミスの展開。

Cisco Unified Communications Manager

電話モードでのオンプレミスの展開。

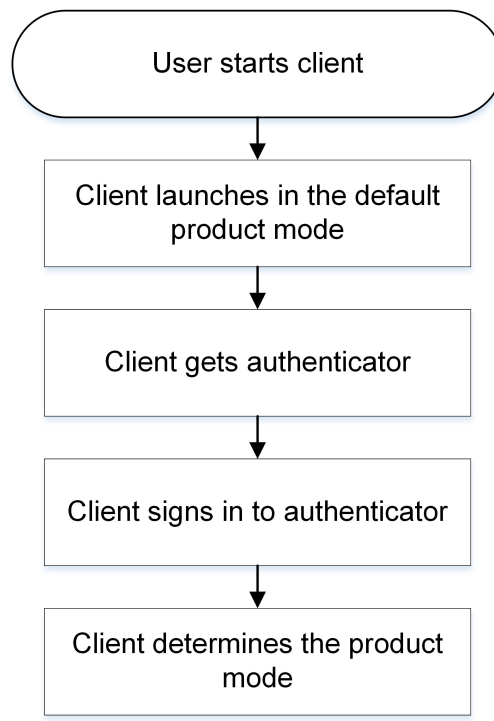
Cisco WebEx Messenger サービス

クラウドベースまたはハイブリッドクラウドベースでの展開。

最初の起動シーケンス

インストール後の最初の起動時、Cisco Jabber はデフォルトの製品モードを開始します。クライアントは、オーセンティケーターを取得し、ユーザをログインさせます。ログイン後、クライアントは製品モードを決定します。

次の図は、最初の起動シーケンスを示しています。



クライアントによるオーセンティケータの取得方法

Cisco Jabber は、次のようにオーセンティケータを検索します。

- 1 クライアントが手動設定のキャッシュを確認します。
ユーザは、クライアント ユーザ インターフェイスを使用して手動でオーセンティケータを入力できます。
- 2 クライアントは、ユーザのドメインが WebEx 組織であるかどうかを検出するためにキャッシュを確認します。
クライアントは、オーセンティケータとして WebEx を選択します。
- 3 クライアントは、ユーザの組織ドメインが WebEx 組織であるかどうかを検出するために、WebEx クラウド サービス HTTP 要求を作成します。
クライアントは、オーセンティケータとして WebEx を選択します。
- 4 クライアントは、サービス ディスカバリのキャッシュを確認します。
クライアントは、サービス (SRV) レコードの以前のクエリーから設定をロードします。
- 5 クライアントは、SRV レコードの問い合わせをします。
クライアントは、サービスを探すために、SRV レコードの DNS ネーム サーバを問い合わせます。
クライアントが、_cisco-uds SRV レコードを見つけると、サービス プロファイルからオーセンティケータを取得できます。

- 6 クライアントは、ブートストラップ ファイルを読み取ります。
- オプションで、インストール中にオーセンティケーターを設定できます。

クライアントがオーセンティケーターを取得できない場合、ユーザは手動でクライアントユーザインターフェイスの認証ソースを選択するようユーザに指示します。

サービス ディスカバリ

サービス ディスカバリにより、クライアントは自動的に企業のネットワークでサービスを検出することができます。サーバローケーションを提供するサービス (SRV) レコードを取得するため、クライアントはドメイン ネーム サーバを問い合わせます。

サービス ディスカバリを使用することの主な利点は次のとおりです。

- 導入までの時間短縮。
- サーバ ローケーションの一元管理が可能。



重要

Cisco Unified Presence 8.x から Cisco Unified Communications IM and Presence 9.0 以降への移行。

Cisco Unified Communications Manager の移行された UC サービスに、Cisco Unified Presence サーバの FQDN を指定する必要があります。[Cisco Unified CM の管理 (Cisco Unified Communications Manager Administration)] インターフェイスを開きます。[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。

IM and Presence タイプを有する UC サービスに関して、Cisco Unified Presence 8.x から Cisco Unified Communications IM and Presence に移行した際、[ホスト名/IP アドレス (Host Name/IP Address)] フィールドにドメイン ネームを入力し、これを Cisco Unified Presence サーバの FQDN に変更する必要があります。

ただし、クライアントは、さまざまなサーバが存在することと、さまざまなサービスを利用できることをクライアントに示す、さまざまな SRV レコードを取得できます。このように、クライアントは、各 SRV レコードを取得するときに、環境に関する特定の情報を取得します。

次の表は、配置可能な SRV レコードを一覧表示し、それぞれのレコードに関する目的とメリットについて説明しています。

SRV レコード	目的	設置の理由
_cisco-uds	<p>Cisco Unified Communications Managerバージョン 9.0 以降の場所が表示されます。</p> <p>クライアントはオーセンティケータを確定するためにサービス プロファイルをCisco Unified Communications Managerから取得できます。</p>	<ul style="list-style-type: none"> インストール引数を指定する必要性を排除します。 UC サービス プロファイルの設定を集中管理できます。 クライアントは、ユーザのホーム クラスタを検出できます。 <p>その結果、クライアントは自動的にユーザのデバイス設定を取得し、デバイスを登録できます。 CCMCIP プロファイルまたは TFTP サーバアドレスのユーザをプロビジョニングする必要はありません。</p> <ul style="list-style-type: none"> 混在製品モードのサポート。 <p>フル UC、IM のみ、もしくは電話機モード機能でユーザを容易に配置できます。</p> <ul style="list-style-type: none"> Expressway Mobile and Remote Access のサポート
_cuplogin	<p>Cisco Unified Presence の場所を提供します。</p> <p>オーセンティケータとして Cisco Unified Presence を設定します。</p>	<ul style="list-style-type: none"> Cisco Unified Communications Manager および Cisco Unified Presence バージョン 8.x で配置をサポートします。 Cisco Unified Communications Manager 9. にまだアップグレードされていないすべてのクラスタの配置をサポートします。
_collab-edge	<p>Cisco VCS Expressway または Cisco Expressway-E の場所を提供します。</p> <p>クライアントは、Cisco Unified Communications Manager からサービスプロファイルを取得してオーセンティケータを特定できます。</p>	<ul style="list-style-type: none"> Expressway Mobile and Remote Access での展開をサポートします。

クライアントによるサービスの検索方法

次の手順は、クライアントが SRV レコードでサービスを検索する方法について説明しています。

- 1 クライアント ホスト コンピュータまたはデバイスは、ネットワーク接続を取得します。
クライアント ホスト コンピュータがネットワーク接続を取得すると、DHCP 設定から DNS ネーム サーバのアドレスを取得します。
- 2 ユーザがクライアントを起動します。
- 3 クライアントは、DHCP 設定から DNS ネーム サーバのアドレスを取得します。
- 4 Cisco WebEx Messenger サービスのため、クライアントは CAS URL に HTTP クエリーを発行します。

このクエリーによって、クライアントはドメインが有効な Cisco WebEx ドメインかどうかを判定できます。

- 5 クライアントは、次の SRV レコードのネーム サーバを優先度順に問い合わせます。

- `_cisco-uds`
- `_cuplogin`
- `_collab-edge`

DNS クエリーの結果をキャッシュに格納し、それ以降の起動時にロードします。

次は、SRV のレコードエントリの例です。

```
_cuplogin._tcp.DOMAIN SRV service location:
priority = 0
weight = 0
port = 8443
svr hostname=192.168.0.26
```

企業の DNS 構造における SRV レコードの配置については、『*Cisco Jabber DNS Configuration Guide*』を参照してください。『*Cisco Jabber DNS Configuration Guide*』は、クライアントによる SRV レコードの取得方法および使用方法に関して詳細な情報を提供し、また、内部および外部サーバに SRV レコードを配置する方法を説明します。

Client Issues HTTP クエリー

利用できるサービスを探すために SRV レコードのネームサーバのクエリーを実行するほか、クライアントは Cisco WebEx Messenger サービスのために CAS URL に HTTP クエリーを送信します。この要求は、ユーザがクラウドベースの展開を決定し、Cisco WebEx Messenger サービスへの認証をすることを可能にします。

クライアントがユーザからドメインを取得すると、次の HTTP クエリーへのドメインに追加されます。

```
http://loginp.webexconnect.com/cas/FederatedSSO?org=
```

たとえば、クライアントがユーザからドメインとして `example.com` を取得した場合、次のクエリーが発行されます。

```
http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com
```

クエリーは、ドメインが有効な Cisco WebEx ドメインであるかどうかを決定するためにクライアントが使用する XML 応答を返します。

クライアントがドメインは有効な Cisco WebEx ドメインであると決定した場合、Cisco WebEx クレデンシャルに入力するようユーザに指示します。その後、クライアントは Cisco WebEx Messenger サービスに認証し、Cisco WebEx Org Admin で設定された設定内容および UC サービスを取得します。

クライアントがドメインは有効なドメインでないと決定した場合、Cisco WebEx クエリーの結果をネーム サーバに使用して、使用可能なサーバを探します。



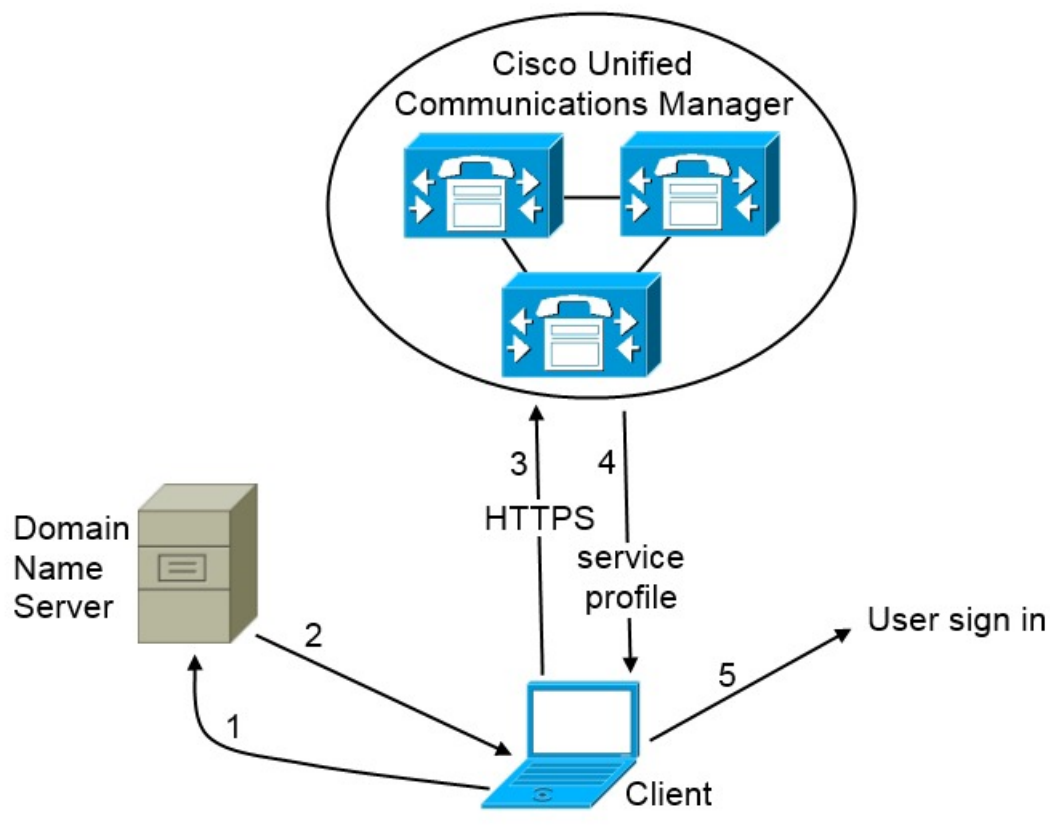
(注) HTTP 要求を CAS URL に送信する場合、クライアントは設定されたシステム プロキシを使用します。この要求へのプロキシのサポートは、次の制約事項があります。

- プロキシ認証はサポートされていません。
- バイパスリストのワイルドカードはサポートされていません。例として、`*.example.com` の代わりに `example.com` を使用します

Cisco UDS SRV レコード

Cisco Unified Communications Manager バージョン 9 以降の展開では、クライアントは自動的に `_cisco-uds` SRV レコードでサービスと設定を自動的に検出できます。

次の図は、クライアントが `_cisco-uds` SRV レコードをどのように使用するかにについて示しています。



380427

- 1 クライアントは、SRV レコードのドメイン ネーム サーバを問い合わせます。
- 2 ネーム サーバは、_cisco-uds SRV レコードを返します。
- 3 クライアントは、ユーザのホーム クラスタを検出します。

自動でのユーザのホームクラスタ検索結果として、クライアントはユーザのデバイス設定を取得し、自動的にテレフォニー サービスを登録できます。



重要

複数の Cisco Unified Communications Manager クラスタを使用した環境では、クラスタ間検索サービス (ILS) を設定する必要があります。ILS は、ユーザのホーム クラスタを検出するために、クライアントを有効にします。

ILS の設定方法については、『*Cisco Unified Communications Manager Features and Services Guide*』の適切なバージョンを参照してください。

- 4 クライアントはユーザのサービス プロファイルを取得します。
ユーザのサービス プロファイルには、UC サービスおよびクライアント設定のアドレスと設定が含まれます。
また、クライアントは、サービス プロファイルからのオーセンティケータを決定します。
- 5 クライアントは、オーセンティケータにユーザをログインさせます。

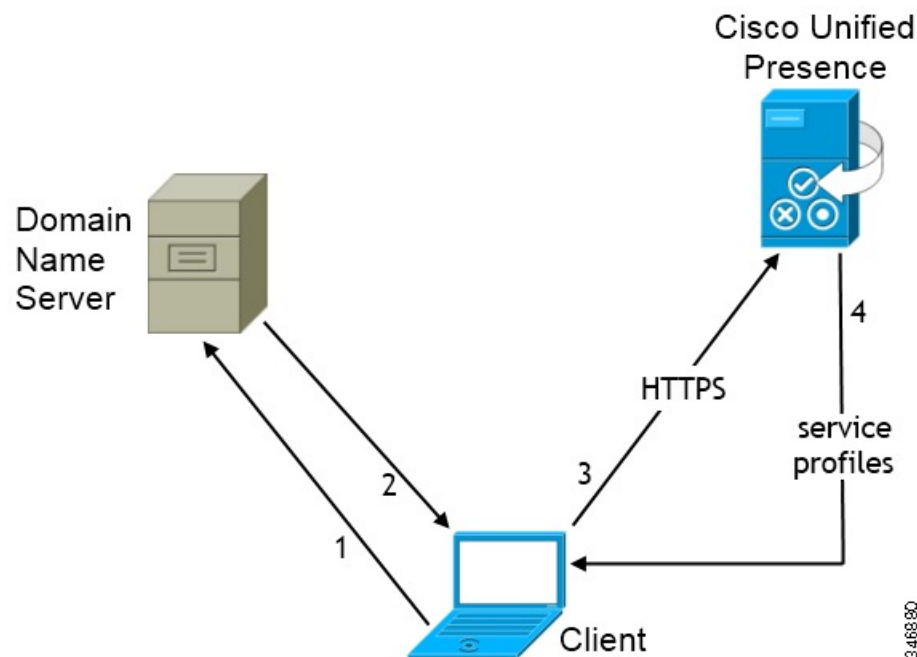
次に、_cisco-uds SRV レコードの例を示します。

```
_cisco-uds._tcp.example.com    SRV service location:
    priority      = 6
    weight        = 30
    port          = 8443
    svr hostname  = cucm3.example.com
_cisco-uds._tcp.example.com    SRV service location:
    priority      = 2
    weight        = 20
    port          = 8443
    svr hostname  = cucm2.example.com
_cisco-uds._tcp.example.com    SRV service location:
    priority      = 1
    weight        = 5
    port          = 8443
    svr hostname  = cucm1.example.com
```

CUP ログイン SRV レコード

Cisco Jabber は、SRV レコード (_cuplogin) を使用して、自動で Cisco Unified Presence もしくは Cisco Unified Communications Manager IM and Presence Service を検出し、接続します。

次の図は、クライアントが _cuplogin SRV レコードをどのように使用するかにについて示しています。



1 クライアントは、SRV レコードのドメイン ネーム サーバを問い合わせます。

2 ネーム サーバは、_cuplogin SRV レコードを返します。

その結果、Cisco Jabber プレゼンス サーバを検出し、Cisco Unified Presence がオーセンティケーターであることを決定することができます。

3 クライアントは、クレデンシャルについてユーザに指示し、プレゼンスサーバを認証します。

4 クライアントは、プレゼンス サーバからサービス プロファイルを取得します。



ヒント

_cuplogin SRV レコードはまた、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウのデフォルトのサーバアドレスを設定します。

次に、_cuplogin SRV レコードの例を示します。

```
_cuplogin._tcp.example.com      SRV service location:
    priority = 8
    weight   = 50
    port     = 8443
    svr hostname = cup3.example.com
_cuplogin._tcp.example.com      SRV service location:
    priority = 5
    weight   = 100
    port     = 8443
    svr hostname = cup1.example.com
_cuplogin._tcp.example.com      SRV service location:
    priority = 7
    weight   = 4
    port     = 8443
    svr hostname = cup2.example.com
```

手動接続設定

手動接続設定は、サービス ディスカバリが展開されていない状況で、サービス ディスカバリのフォールバック メカニズムを提供します。

Cisco Jabber の起動時に、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウでオーセンティケータとサーバアドレスを指定できます。クライアントは、その後の起動でロードするローカル アプリケーションの設定にサーバアドレスをキャッシュします。

Cisco Jabber は、ユーザが初回起動時に **[手動設定とサインイン (Manual setup and sign in)]** ウィンドウで設定をするよう次のように指示します。

Cisco Unified Communications Manager バージョン 9.x 以降を備えるオンプレミス

クライアントがサービス プロファイルからオーセンティケータおよびサーバアドレスを取得できない場合。

Cisco Unified Communications Manager バージョン 8.x を備えるクラウドベースまたはオンプレミス

ブートストラップファイルのオーセンティケータを設定しない場合。クライアントは、ブートストラップファイルで、または SRV レコードを使用して、サーバアドレスを設定しない場合、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウでサーバアドレスを入力するようにユーザに指示します。

SRV レコードやブートストラップの設定などを含む他のソースよりも、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウで入力する設定が優先されます。

オンプレミスでの展開における手動接続設定

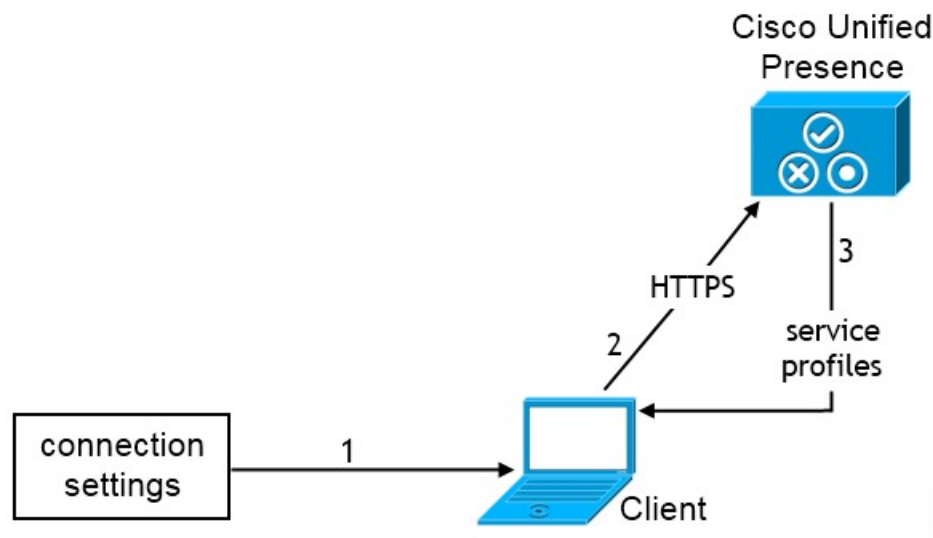
ユーザはオーセンティケータとして Cisco Unified Presence を設定し、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウでサーバアドレスを指定できます。



メモ

自動的に、_cuploginSRV レコードのデフォルトのサーバアドレスを設定することもできます。

次の図は、オンプレミスの展開において、クライアントが手動接続設定をどのように使用できるかを示したものです。



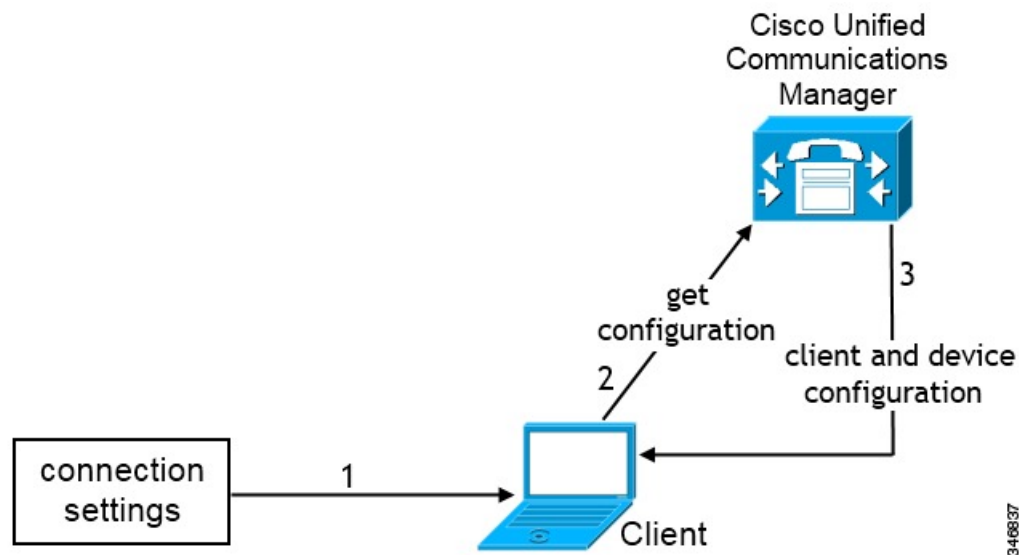
- 1 ユーザは **[手動設定とサインイン (Manual setup and sign in)]** ウィンドウに手動で接続設定を入力します。
- 2 クライアントは、Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service に対して認証します。
- 3 クライアントは、プレゼンス サーバからサービス プロファイルを取得します。

電話モードのオンプレミスの展開における手動接続設定

ユーザはオーセンティケータとして Cisco Unified Communications Manager を設定し、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウで次のサーバアドレスを指定できます。

- TFTP サーバ (TFTP server)
- CTI サーバ (CTI Server)
- CCMCIP サーバ (CCMCIP server)

次の図は、電話モードの展開において、クライアントが手動接続設定をどのように使用できるかを示したものです。

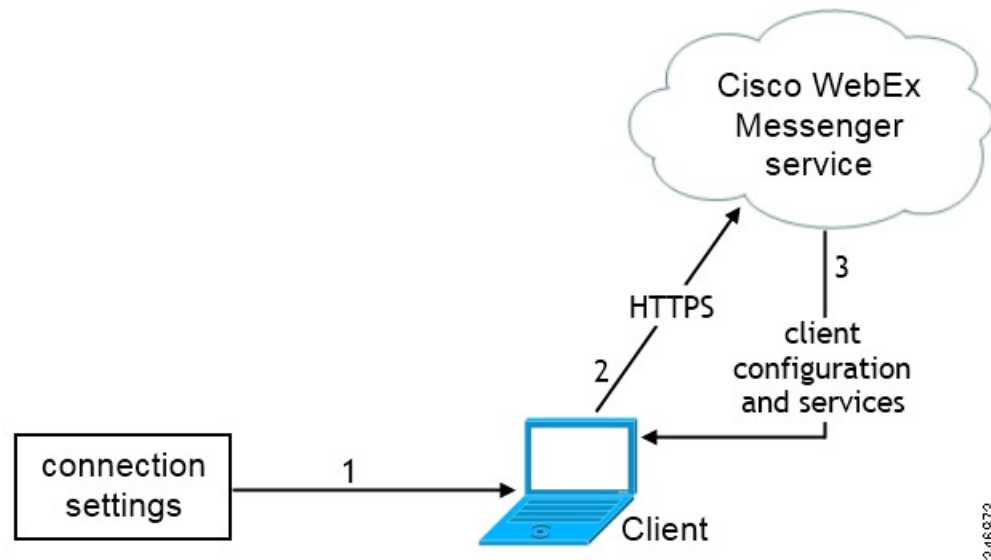


- 1 ユーザは **手動設定とサインイン (Manual setup and sign in)** ウィンドウに手動で接続設定を入力します。
- 2 クライアントが Cisco Unified Communications Manager を認証し、設定を取得します。
- 3 クライアントは、デバイスおよびクライアント設定を取得します。

クラウドベースの展開における手動接続設定

ユーザは、オーセンティケータとして Cisco WebEx Messenger サービスを設定し、**手動設定とサインイン (Manual setup and sign in)** ウィンドウでログイン用の CAS URL を指定できます。

次の図は、クラウドベースの展開において、クライアントが手動接続設定をどのように使用できるかを示したものです。



- 1 ユーザは **[手動設定とサインイン (Manual setup and sign in)]** ウィンドウに手動で接続設定を入力します。
- 2 クライアントにより、Cisco WebEx Messenger サービスが認証されます。
- 3 クライアントは、設定およびサービスを取得します。

サービス ディスカバリの手動接続設定

ユーザは、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウで **[自動 (Automatic)]** オプションを選択できます。

このオプションは、ユーザがサービス ディスカバリを使用して手動でサービス接続の詳細を設定することから変更することができます。たとえば、最初の起動時に、手動でオーセンティケータを設定し、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウ内のサーバアドレスを指定します。

クライアントは、手動設定のキャッシュを常にチェックします。手動設定は、SRV レコードおよびブートストラップ ファイルよりも優先されます。したがって SRV レコードを配置し、サービス ディスカバリを使用する場合は、最初の電源投入から手動設定を上書きする必要があります。

インストーラのスイッチ

ブートストラップ ファイルは、サービス ディスカバリが展開されておらず、手動による接続設定をユーザが好ましく思わない状況で、サービス ディスカバリのフォールバック メカニズムを提供します。

Cisco Jabber をインストールすると、オーセンティケータおよびサーバアドレスを指定できます。インストーラは、ブートストラップファイルにこれらの詳細を保存します。ユーザがクライアントを初めて起動した際に、ブートストラップ ファイルを読み取ります。



(注)

- ブートストラップ ファイルの接続設定は、サービス ディスカバリが配置されている場合、無視されます。
- クライアントは、最初に起動したときのみ、ブートストラップファイルを読み取ります。最初の起動後、クライアントは利用可能なサービスに接続し、設定を取得します。クライアントは、サーバアドレスと設定をキャッシュに格納し、それ以降の起動時にキャッシュから読み込みます。
- Cisco Unified Communications Manager バージョン 9.x 以降を使用して、オンプレミス展開でブートストラップファイルを使用しないよう推奨します。この環境では、クライアントに設定を提供するために、サービス ディスカバリをメカニズムとして使用する必要があります。

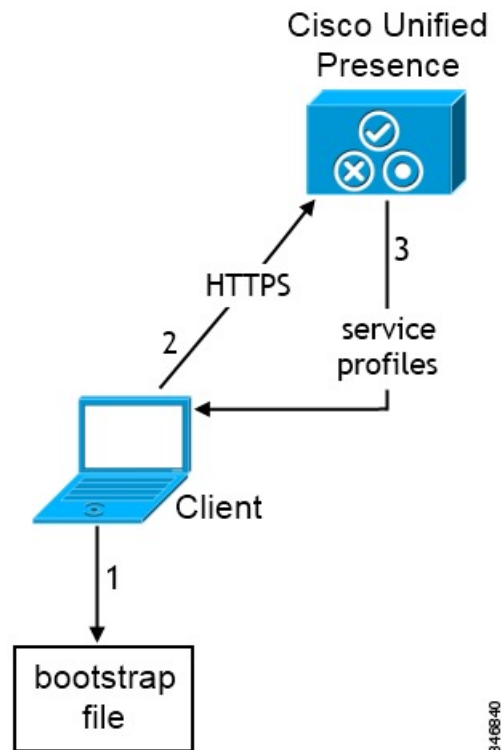
オンプレミスでの展開のブートストラップの設定

次の表は、さまざまな展開タイプの引数値を示します。

製品モード	サーバのバージョン	引数値
フル UC (デフォルトモード)	バージョン 9 以降 : <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service 	次のインストーラ スイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>
フル UC (デフォルトモード)	バージョン 8.x : <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Presence 	次のインストーラ スイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>
IM 専用 (デフォルトモード)	バージョン 9 以降 : <p>Cisco Unified Communications Manager IM and Presence Service</p>	次のインストーラ スイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>

製品モード	サーバのバージョン	引数値
IM 専用 (デフォルトモード)	バージョン 8.x : Cisco Unified Presence	次のインストーラ スイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>

次の図は、クライアントがオンプレミスでの展開の場合、ブートストラップ設定の使用法を示しています。



ユーザがクライアントを初めて起動する際に、次が実行されます。

- 1 クライアントは、ブートストラップ ファイルから設定を取得します。

クライアントは、デフォルト モードで開始され、Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service がオーセンティケータであることを決定します。クライアントは、サービスディスカバリの結果により、その他の指示がなされない限り、プレゼンス サーバのアドレスを取得します。

- 2 クライアントは、Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service に対して認証します。

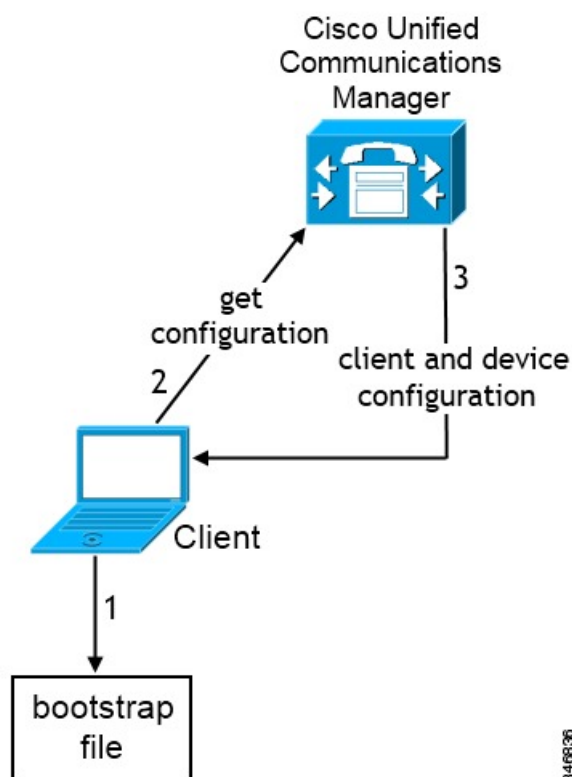
- 3 クライアントは、プレゼンス サーバからサービス プロファイルを取得します。

電話モードのオンプレミスの展開におけるブートストラップの設定

インストール中に、次のように引数の値を設定します。

- AUTHENTICATOR の値として、CUCM を設定します。
- PRODUCT_MODE の値として phone_mode を設定します。
- TFTP の値として、TFTP サーバアドレスを設定します。
- CTI の値として、CTI サーバアドレスを設定します。
- CCMCIP の値として、CCMCIP サーバアドレスを設定します。

次の図は、電話モードの展開において、クライアントがブートストラップ設定をどのように使用できるかを示したものです。



346836

ユーザがクライアントを初めて起動する際に、次が実行されます。

- 1 クライアントは、ブートストラップ ファイルから設定を取得します。

クライアントは、デフォルト モードで開始され、Cisco Unified Communications Manager がオーセンティケーターであることを決定します。クライアントは、サービス ディスカバリの結果により、その他の指示がなされない限り、TFTP および CTI サーバのアドレスを取得します。

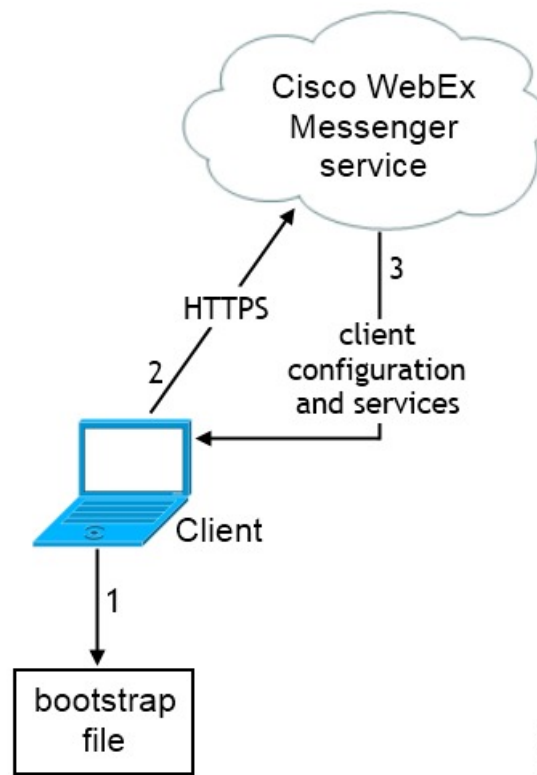
- 2 クライアントが Cisco Unified Communications Manager を認証し、設定を取得します。
- 3 クライアントは、デバイスおよびクライアント設定を取得します。

クラウド ベースの展開におけるのブートストラップの設定

インストール中に、次のように引数の値を設定します。

- AUTHENTICATOR の値として、WebEx を設定します。

次の図は、クラウドベースの展開においてクライアントがブートストラップをどのように使用できるかを示したものです。



346872

ユーザがクライアントを初めて起動する際に、次が実行されます。

- 1 クライアントは、ブートストラップ ファイルから設定を取得します。

クライアントは、デフォルト モードでスタートし、サービス ディスカバリの結果により、その他の指示がなされない限り、Cisco WebEx Messenger サービスがオーセンティケーターであることを確認します。

- 2 クライアントにより、Cisco WebEx Messenger サービスが認証されます。
- 3 クライアントは、設定およびサービスを取得します。

クラウドベース SSO

クラウドベース の展開では、Cisco Jabber for Windows が Cisco WebEx Messenger サービスで SSO をサポートします。

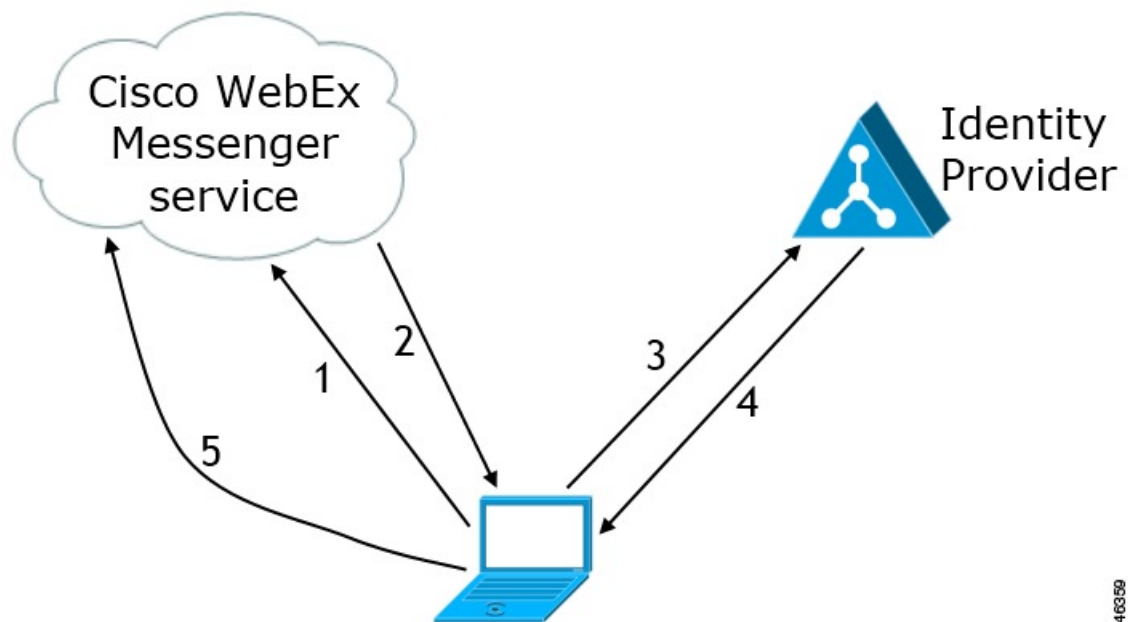
次の手順は、ユーザが Cisco Jabber for Windows を開始した後の、クラウドベース SSO のログイン フローの説明です。

- 1 Cisco Jabber for Windows は、Cisco WebEx Messenger サービスにログイン要求を送信します。
- 2 Cisco WebEx Messenger サービスは、アイデンティティ プロバイダーが存在するドメインへ Cisco Jabber for Windows のリダイレクトを行います。
- 3 Cisco Jabber for Windows は、リダイレクトに従い、アイデンティティ プロバイダーからログイン トークンを要求します。
- 4 アイデンティティ プロバイダーはログイン トークンを Cisco Jabber for Windows に提供します。
- 5 Cisco Jabber for Windows は、Cisco WebEx Messenger サービスにそのログイン トークンを渡します。

その結果、Cisco Jabber for Windows は Cisco WebEx Messenger サービスを認証します。

次の図は、クラウドベース SSO のログイン フローを示しています。

図 6: クラウドベースの SSO ログイン フロー



3-46359



(注) アイデンティティ プロバイダーは、Security Assertion Markup Language (SAML) である必要があります。Cisco Jabber for Windows は、アイデンティティ プロバイダーとして、次の製品をテストし、サポートします。

- PingFederate
- Microsoft Active Directory Federation Services (ADFS)
- CA SiteMinder
- Oracle Access Manager

クラウドベース SSO の有効化

クラウドベース での展開で SSO の Cisco Jabber for Windows を有効にするには、インストール中に SSO_ORG_DOMAIN 引数を設定する必要があります。



(注) クライアントは、SSO_ORG_DOMAIN 引数でクラウドベースの SSO が正常に有効になる前に、その他の展開方法（サービス ディスカバリ、インストーラのスイッチ、または手動設定）の 1 つを使用して認証ソースとして WebEx を検出する必要があります。

Expressway Mobile and Remote Access の展開

Cisco Unified Communications Manager 用の Expressway Mobile and Remote Access は、ユーザが VPN クライアントを使用せずに、企業のファイアウォールの外から各自のコラボレーション ツールにアクセスできるようにします。シスコのコラボレーション ゲートウェイを使用し、クライアントは Wi-Fi ネットワークまたはモバイルデータ ネットワークなどのリモート ロケーションから社内ネットワークに安全に接続できます。

Expressway Mobile and Remote Access 機能をセットアップするには、次を実行する必要があります。

- 1 Expressway Mobile and Remote Access をサポートするサーバを、Cisco Expressway-E および Cisco Expressway-C.* を使用してセットアップします。
 - a Cisco Expressway サーバをセットアップするには、次のマニュアルを参照してください。
 - 『Cisco Expressway Basic Configuration Deployment Guide』
 - 『Mobile and Remote Access via Cisco Expressway Deployment Guide』

* 現在 Cisco TelePresence Video Communication Server (VCS) 環境を導入している場合、Expressway Mobile and Remote Access をセットアップできます。詳細については、『Cisco

『VCS Basic Configuration (Control with Expressway) Deployment Guide』および『Mobile and Remote Access via Cisco VCS Deployment Guide』を参照してください。

- b** 関係するサーバをすべて Cisco Expressway-C サーバのホワイトリストに追加して、クライアントが社内ネットワークに位置するサービスに確実にアクセスできるようにします。

サーバを Cisco Expressway-C ホワイトリストに追加するには、[HTTP server allow] 設定を使用します。

このリストには、ボイスメール、コンタクトの写真、カスタム HTML タブ、インストーラの更新をホストするサーバを含めることができます。

- 2** `_collab-edge` DNS SRV レコードを含む外部 DNS サーバを設定し、クライアントが Expressway Mobile and Remote Access サーバを検出できるようにします。

DNS サーバを設定する方法の詳細については、『Cisco Jabber DNS Configuration Guide』を参照してください。

- 3** IM and Presence サーバのドメインが音声サーバのドメインと異なるハイブリッドクラウドベースアーキテクチャを展開する場合、音声サービスドメインを設定するようにします。

音声サービスドメインによって、クライアントは `_collab-edge` レコードを含む DNS サーバを検索できます。



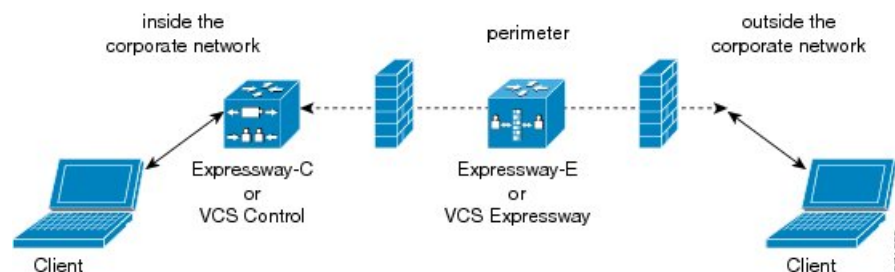
重要

ほとんどの場合、ユーザは最初にクライアントに Expressway Mobile and Remote Access を使用してサインインし、企業のファイアウォールの外からサービスに接続できます。ただし、次の場合にユーザは最初のサインインを社内ネットワーク内で実行する必要があります。

- 音声サービスドメインがサービスドメインとは異なる場合。この場合、ユーザは Jabber config.xml ファイルから正しい音声サービスドメインを取得するために、社内ネットワーク内にいる必要があります。
- クライアントが CAPF 登録プロセス（セキュアモードまたは混合モードのクラスタを使用する場合に必要）を完了する必要がある場合。

次の図は、Expressway Mobile and Remote Access 環境のアーキテクチャを図示したものです。

図 7: アーキテクチャ図



関連トピック

[Cisco Expressway 設定ガイド](#)[Cisco VCS 設定ガイド](#)[Cisco Jabber DNS 設定ガイド](#)

サポートされるサービス

次の表に、クライアントが Expressway Mobile and Remote Access を使用してリモートで Cisco Unified Communications Manager に接続する場合にサポートされるサービスと機能をまとめます。

表 1 : *Expressway Mobile and Remote Access* でサポートされるサービスの概要

サービス		サポート済み	非サポート対象
ディレクトリ			
	UDS ディレクトリ検索	x	
	LDAP ディレクトリ検索		x
	ディレクトリ写真解決	x * HTTP ホワイト リストを Cisco Expressway-C で使用	
	ドメイン内フェデレーション	x * 連絡先検索のサポートはコンタクト ID の形式に依存します。詳細については、以下の注記を参照してください。	
	ドメイン間フェデレーション	x	
インスタント メッセージおよびプレゼンス			
	オンプレミス	x	
	クラウド	x	
	チャット	x	
	グループ チャット	x	
	ハイ アベイラビリティ：オンプレミス展開	x	

サービス		サポート済み	非サポート対象
	ファイル転送：オンプレミス展開		x
	ファイル転送：クラウド展開	x	
	ビデオ デスクトップ共有：BFCP	x	
音声とビデオ			
	音声コールとビデオ コール	x * Cisco Unified Communications Manager 9.1(2) 以降	
	デスク フォン制御モード (CTI)		x
	Extend and Connect		x
	セッションの永続性		x
	アーリー メディア		x
	セルフケアポータル アクセス		x
ボイスメール			
	ビジュアル ボイスメール	x * HTTP ホワイト リストを Cisco Expressway-C で使用	
Cisco WebEx Meetings			
	オンプレミス		x
	クラウド	x	
	Cisco WebEx デスクトップ共有	x	
インストール			
	インストーラ更新	x * HTTP ホワイト リストを Cisco Expressway-C で使用	
カスタマイゼーション			

サービス		サポート済み	非サポート対象
	カスタム HTML タブ	x * HTTP ホワイ ト リ ストを Cisco Expressway-C で使用	
セキュリティ			
	エンドツーエンド暗号化		x
	CAPF 登録		x
トラブルシューティング			
	問題レポートの生成	x	
	問題レポートのアップロード		x

ディレクトリ

クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合、次の制限付きでディレクトリ統合をサポートします。

LDAP 連絡先の解決

クライアントが企業ファイアウォールの外側にいる場合、連絡先の解決に LDAP を使用できません。代わりに、クライアントは接続の解決に UDS を使用する必要があります。

ユーザが企業ファイアウォールの内側にいる場合、クライアントは接続の解決に UDS と LDAP のいずれかを使用できます。社内ファイアウォール内に LDAP を配置する場合は、LDAP ディレクトリを Cisco Unified Communications Manager と同期して、ユーザが企業ファイアウォールの外にいるときにクライアントを UDS に接続させることを推奨します。

ディレクトリ写真解決

クライアントが連絡先写真をダウンロードできるようにするため、連絡先写真をホストするサーバを Cisco Expressway-C のホワイトリストに追加する必要があります。サーバを Cisco Expressway-C ホワイトリストに追加するには、[HTTP server allow] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

ドメイン内フェデレーション

イントラドメイン フェデレーションを展開し、クライアントがファイアウォールの外から Expressway Mobile and Remote Access に接続する場合、連絡先の検索は、コンタクト ID が次のいずれかのフォーマットを使用している場合にのみサポートされます。

- sAMAccountName@domain
- UserPrincipalName (UPN) @domain
- EmailAddress@domain
- employeeNumber@domain
- telephoneNumber@domain

インスタント メッセージおよびプレゼンス

クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合、次の制限付きでインスタント メッセージおよびプレゼンスをサポートします。

ファイル転送

クライアントは、Cisco Unified Communications Manager IM and Presence Service 展開では画面キャプチャを含むファイル転送をサポートしません。 ファイル転送は Cisco WebEx クラウド展開でのみサポートされます。

音声コールとビデオ コール

クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合、次の制限付きで音声コールおよびビデオ コールをサポートします。

Cisco Unified Communications Manager

Expressway Mobile and Remote Access は、Cisco Unified Communications Manager バージョン 9.0 以降でビデオ コールと音声コールをサポートします。 Expressway Mobile and Remote Access は、Cisco Unified Communications Manager バージョン 8.x ではサポートされません。

デスクフォン制御モード (CTI)

クライアントは、エクステンション モビリティを含め、デスク フォン制御モード (CTI) をサポートしません。

Extend and Connect

クライアントは次の用途に使用できません:

- オフィスの Cisco IP Phone でコールを発信および受信する。
- 自宅電話、ホテルの電話、またはオフィスの Cisco IP Phone で、保留と復帰などの通話中制御を実行する。

セッションの永続性

クライアントは、ネットワーク遷移発生時に、音声コールおよびビデオ コールのドロップから復帰できません。たとえば、ユーザがオフィス内で Cisco Jabber コールを開始し、その後建物から離れて Wi-Fi 接続を失った場合、クライアントが Expressway Mobile and Remote Access 使用にスイッチするためコールがドロップされます。

アーリー メディア

アーリー メディアにより、クライアントはデータを接続が確立される前にエンドポイント間で交換できます。たとえば、ユーザが同じ組織に属さない通話者にコールを発信し、相手側がこれを拒否したまたはコールに応答しなかった場合、アーリーメディアによってユーザがビジー トーンを受け取るか、ボイスメールがユーザに送信されます。

Expressway Mobile and Remote Access を使用する場合、相手側通話者がコールを拒否するか応答しても、ユーザにはビジー音が聞こえません。代わりに、ユーザは、コールが終了するまで約 1 分無音を受信します。

セルフケアポータル アクセス

ユーザは、ファイアウォール外では Cisco Unified Communications Manager セルフケア ポータルにアクセスできません。Cisco Unified Communications Manager ユーザ ページには、外部からアクセスできません。

Cisco Expressway-E はファイアウォール内のクライアントとユニファイドコミュニケーション サービス間のすべての通信をプロキシ処理します。ただし、Cisco Expressway-E は Cisco Jabber アプリケーションの一部でないブラウザからアクセスされたサービスはプロキシ処理しません。

ボイスメール

ボイス メール サービスは、クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合にサポートされます。



(注)

クライアントが確実にボイス メール サービスにアクセスできるよう、Cisco Expressway-C サーバのホワイト リストにボイス メール サーバを追加する必要があります。サーバを Cisco Expressway-C ホワイトリストに追加するには、[HTTP server allow] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

Cisco WebEx Meetings

クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合、Cisco WebEx Meeting Center を使用するクラウド ベースの会議のみがサポートされます。

クライアントは、Cisco WebEx Meetings Server にアクセスできず、オンプレミス Cisco WebEx ミーティングも開始できません。

インストール

クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合、インストーラの更新をサポートします。



- (注) クライアントが確実にインストーラの更新をダウンロードできるよう、Cisco Expressway-C サーバのホワイトリストにインストーラの更新をホストするサーバを追加します。サーバを Cisco Expressway-C ホワイトリストに追加するには、[HTTP server allow] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

カスタマイゼーション

クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合、カスタム HTML タブ設定をサポートします。



- (注) クライアントが確実にカスタム HTML タブの設定をダウンロードできるよう、Cisco Expressway-C サーバのホワイトリストにカスタム HTML タブ設定をホストするサーバを追加します。サーバを Cisco Expressway-C ホワイトリストに追加するには、[HTTP server allow] 設定を使用します。詳細については、関連する Cisco Expressway のマニュアルを参照してください。

セキュリティ

クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合、次の制限付きでほとんどのセキュリティ機能をサポートします。

初回 CAPF 登録

Certificate Authority Proxy Function (CAPF) 登録は、Cisco Jabber (または他のクライアント) に証明書を発行する Cisco Unified Communications Manager パブリッシャで実行されるセキュリティ サービスです。正常に CAPF を登録するために、クライアントはファイアウォールの内側から接続するか VPN 接続を使用する必要があります。

エンドツーエンド暗号化

ユーザが Expressway Mobile and Remote Access を経由して内部ネットワークに接続し、コールに参加する場合：

- メディアは、Expressway Mobile and Remote Access を使用して Cisco Unified Communications Manager に登録されたデバイスと Cisco Expressway-C との間のコールパス上で暗号化されます。
- メディアは、ローカルに Cisco Unified Communications Manager へ登録されたデバイスと Cisco Expressway-C との間のコールパス上では暗号化されません。

トラブルシューティング

問題レポートのアップロード

クライアントはHTTPSを介して指定の内部サーバへ問題レポートをアップロードするため、クライアントが Expressway Mobile and Remote Access を使用してサービスに接続する場合には、問題レポートを送信できません。

この問題を回避するには、ユーザはレポートをローカルに保存し、別の方法でレポートを送信できます。

仮想環境での展開

次のソフトウェアを使用して、Cisco Jabber for Windows を仮想環境に展開できます。

- Citrix XenDesktop 7.1
- Citrix XenDesktop 7.0
- Citrix XenDesktop 5.6
- Citrix XenDesktop 5.5
- Citrix XenApp 6.5 Feature Pack 2 Enterprise Edition for Windows Server 2008 Service Pack 2 64 bit, published desktop
- Citrix XenApp 6.5 Feature Pack 1 Enterprise Edition for Windows Server 2008 Service Pack 2 64 bit, published desktop
- Citrix XenApp 6.5 Enterprise Edition for Windows 2008 R2 64 bit, published desktop
- Citrix XenApp 6.0 Enterprise Edition for Windows 2008 R2 64 bit, published desktop
- VMware Horizon View 5.3
- VMware Horizon View 5.2
- VMware View 5.1

サポートされる機能

- 他の Cisco Jabber クライアントとのインスタント メッセージングおよびプレゼンス
- デスクフォン制御
- ボイスメール
- Microsoft Outlook 2007、2010、2013 とのプレゼンスの統合

仮想環境のソフトフォン

Cisco Virtualization Media Engine (VXME) 9.7 を仮想環境でのソフトフォン コールに使用します。

ローミング プロファイル

クライアントは、ユーザのコール履歴および構成ストアキャッシュなどのユーザデータを、ユーザの次のサインインで使用するため、ローカルマシンにストアします。仮想環境では、ユーザがいつも同じ仮想デスクトップにアクセスするわけではありません。一貫したユーザエクスペリエンスを保証するために、これらのファイルは、クライアントが起動されるたびにアクセスする必要があります。

ホストされた仮想デスクトップ間を移動する場合、仮想環境でユーザの個人設定を維持するには、Citrix および VMware からの専用プロファイル管理ソリューションを使用します。

Citrix Profile Management は、XenApp サーバ用のプロファイル ソリューションです。ホストされた仮想デスクトップは、XenDesktop を使用して、プールされたランダムなカタログから作成されます。Citrix Profile Management は、各ユーザのプロファイル全体を、インストールされたシステムとユーザ ストアとの間で同期します。

VMware View Persona Management は、ユーザ プロファイルを保存し、リモート プロファイル リポジトリと動的に同期します。View Persona Management をデスクトッププールに実装するには、View Agent をインストールし、デスクトッププールの作成に使用された親仮想マシンまたはテンプレート仮想マシンのそれぞれに、Persona Management setup オプションを選択します。VMware View Persona Management は Windows ローミング プロファイルを必要としないので、View ユーザ プロファイルの管理では Windows Active Directory をバイパスできます。Persona Management は、既存のローミング プロファイルの機能を強化します。

除外リストに追加することで、同期から除外するファイルとフォルダを指定できます。除外されたフォルダ内のサブフォルダを含めるには、包含リストにサブフォルダを追加します。

ユーザの個人用設定を保持するには、次のディレクトリを除外しないようにします。

```
AppData\Local\Cisco
AppData\Local\JabberWerxCPP
AppData\Roaming\Cisco
AppData\Roaming\JabberWerxCPP
```

クライアント情報の保存

クライアントは、次の場所にユーザ情報を保存します。

C:\Users\username\AppData\Local\Cisco\Unified Communications\Jabber\CSF

フォルダ名	説明
Contacts	コンタクトのキャッシュ ファイル
History	通話履歴とチャット履歴
Photo cache	ディレクトリの画像をローカルにキャッシュ

C:\Users\username\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF

フォルダ名	説明
-------	----

Config	ユーザの Jabber コンフィギュレーションファイルを保持し、コンフィギュレーション ストア キャッシュを格納
Credentials	暗号化されたユーザ名とパスワードを格納

関連トピック

[Citrix プロファイル管理](#)

[VMware View Persona Management 導入ガイド](#)



第 6 章

Cisco Jabber のインストール

インストールのオプションを確認し、Cisco Jabber のインストールのさまざまな方法を学習します。インストールを開始する前に、正常な導入の要件について理解します。

- [インストールの方法, 89 ページ](#)
- [コマンドラインの使用, 90 ページ](#)
- [MSI の手動による実行, 92 ページ](#)
- [カスタム インストーラの作成, 92 ページ](#)
- [グループ ポリシーを使用した導入, 95 ページ](#)
- [コマンドライン引数, 98 ページ](#)
- [インストーラのプロパティ, 110 ページ](#)
- [サポートされる言語, 110 ページ](#)
- [Cisco Media Services Interface, 111 ページ](#)
- [Cisco Jabber for Windows のアンインストール, 113 ページ](#)

インストールの方法

Cisco Jabber for Windows は、MSI インストールパッケージを提供します。このインストールパッケージを使用して次のことを行うことができます。

コマンドラインの使用

インストールプロパティを設定するため、コマンドラインウィンドウで引数を指定します。複数のインスタンスをインストールする場合は、このオプションを選択します。

MSI の手動による実行

クライアントの起動時に、MSI をクライアント ワーク ステーションのファイル システムで手動で実行し、接続プロパティを指定します。

テストまたは評価用に単一インスタンスをインストールする場合は、このオプションを選択します。

カスタム インストーラの作成

デフォルトのインストール パッケージを開き、必要なインストール プロパティを指定し、カスタム インストール パッケージを保存します。

同じインストール プロパティを持つインストール パッケージを配布する場合は、このオプションを選択します。

グループ ポリシーを使用した導入

同じドメインの複数のコンピュータにクライアントをインストールします。

コマンドラインの使用

コマンドライン ウィンドウにインストール引数を指定します。

手順

-
- ステップ 1** コマンドライン ウィンドウを開きます。
 - ステップ 2** 次のコマンドを入力します。
`msiexec.exe /i CiscoJabberSetup.msi`
 - ステップ 3** パラメータ = 値のペアとしてコマンドライン引数を指定します。
`msiexec.exe /i CiscoJabberSetup.msi argument=value`
 - ステップ 4** コマンドを実行して、Cisco Jabber for Windows をインストールします。
-

インストール コマンドの例

Cisco Jabber for Windows をインストールするためのコマンド例を確認します。

Cisco Unified Communications Manager 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

ここで、

CLEAR=1 により、既存のブートストラップ ファイルが削除されます。

/quiet により、サイレント インストールが指定されます。

デフォルト モードの Cisco Unified Communications Manager 8.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP CUP_ADDRESS=1.2.3.4
```

ここで、

CLEAR=1 により、既存のブートストラップ ファイルが削除されます。

AUTHENTICATOR=CUP により、Cisco Unified Presence がオーセンティケーターとして設定されます。

ADDRESS=1.2.3.4 により、1.2.3.4 がプレゼンス サーバの IP アドレスとして指定されます。

/quiet により、サイレントインストールが指定されます。

電話モードの Cisco Unified Communications Manager 8.x

UDS と統合する場合、電話モードでインストールするときは、最初に<PresenceDomain>プレゼンス サーバのドメインアドレス</PresenceDomain> パラメータを設定する必要があります。

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 PRODUCT_MODE=Phone_Mode AUTHENTICATOR=CUCM  
TFTP=1.2.3.4 CTI=5.6.7.8
```

ここで、

CLEAR=1 により、既存のブートストラップ ファイルが削除されます。

PRODUCT_MODE=Phone_Mode により、電話モードにクライアントが設定されます。

AUTHENTICATOR=CUCM により、Cisco Unified Communications Manager がオーセンティケーターとして設定されます。

TFTP=1.2.3.4 により、1.2.3.4 が、クライアント設定をホスティングする TFTP サーバの IP アドレスとして指定されます。

CTI=5.6.7.8 により、5.6.7.8 が CTI サーバの IP アドレスとして設定されます。

/quiet により、サイレントインストールが指定されます。

Cisco WebEx Messenger サービス

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
```

ここで、

CLEAR=1 により、既存のブートストラップ ファイルが削除されます。

AUTHENTICATOR=WEBEX により、オーセンティケーターとしてCisco WebEx Messenger サービスが設定されます。

/quiet により、サイレントインストールが指定されます。

SSO を備える Cisco WebEx Messenger サービス

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX  
SSO_ORG_DOMAIN=example.com
```

ここで、

CLEAR=1 により、既存のブートストラップ ファイルが削除されます。

AUTHENTICATOR=WEBEX により、オーセンティケーターとしてCisco WebEx Messenger サービスが設定されます。

SSO_ORG_DOMAIN=example.comにより、シングルサインオン（SSO）としてexample.comが設定されます。

/quietにより、サイレントインストールが指定されます。

MSI の手動による実行

クライアントの単一インスタンスをインストールし、**[手動設定とサインイン（Manual setup and sign in）]** ウィンドウ内の接続設定を指定するために、インストールプログラムを手動で実行します。

手順

-
- ステップ 1 CiscoJabberSetup.msi を起動します。
インストールプログラムにより、インストールプロセスのウィンドウが開きます。
 - ステップ 2 手順に従ってインストールプロセスを完了します。
 - ステップ 3 Cisco Jabber for Windows を起動します。
 - ステップ 4 **[手動設定およびログイン（Manual setup and sign in）]** を選択します。
[手動設定とサインイン（Manual setup and sign in）] ウィンドウが開きます。
 - ステップ 5 接続設定プロパティの値を指定します。
 - ステップ 6 **[保存（Save）]** を選択します。
-

カスタム インストーラの作成

カスタム インストーラを作成するデフォルトのインストール パッケージを変換できます。



(注) Microsoft Orca を使用して、カスタム インストーラを作成します。Microsoft Orca は、Microsoft Windows SDK for Windows 7 and .NET Framework 4 の一部として使用できます。

Microsoft の Web サイトから Microsoft Windows SDK for Windows 7 and .NET Framework 4 をダウンロードしてインストールします。

関連トピック

[Microsoft Windows SDK for Windows 7 and .NET Framework 4](#)

デフォルト トランスフォーム ファイルの取得

Microsoft Orca でインストール パッケージを修正するために、デフォルト トランスフォーム ファイルが必要です。

手順

-
- | | |
|---------------|---|
| ステップ 1 | Cisco.com から Cisco Jabber 管理パッケージをダウンロードします。 |
| ステップ 2 | CiscoJabberProperties.mst を Cisco Jabber 管理パッケージからファイル システムにコピーします。 |
-

関連トピック

[ソフトウェア ダウンロード](#)

カスタム トランスフォーム ファイルの作成

カスタムインストーラを作成するには、変換ファイルを使用します。トランスフォームファイルは、インストーラに適用するインストールプロパティが含まれます。

デフォルトトランスフォームファイルは、インストーラを変換するとプロパティの値を指定することができます。1つのカスタムインストーラを作成する場合、デフォルト トランスフォーム ファイルを使用する必要があります。

任意でカスタム トランスフォーム ファイルを作成できます。カスタム トランスフォーム ファイルでプロパティの値を指定し、インストーラに適用します。

異なるプロパティの値を持つ複数のカスタムインストーラを必要とする場合、カスタムトランスフォーム ファイルを作成します。たとえば、デフォルト言語をフランス語に設定するトランスフォームファイルと、デフォルト言語をスペイン語に設定するもう1つのトランスフォームファイルを作成できます。インストール パッケージに各トランスフォーム ファイルを個別に適用できます。2つのインストーラを作成したことで、各言語に1つのインストーラが作成されます。

手順

-
- | | |
|---------------|---|
| ステップ 1 | Microsoft Orca を起動します。 |
| ステップ 2 | CiscoJabberSetup.msi を開き、CiscoJabberProperties.mst を適用します。 |
| ステップ 3 | 該当するインストーラ プロパティに値を指定します。 |
| ステップ 4 | トランスフォーム ファイルを生成して保存します。 <ul style="list-style-type: none">a) [トランスフォーム (Transform)] > [トランスフォームの生成 (Generate Transform)] を選択します。b) トランスフォーム ファイルを保存するファイル システムの場所を選択します。 |

- c) トランスフォーム ファイルの名前を指定して [保存 (Save)] を選択します。

作成したトランスフォーム ファイルは、`file_name.mst` として保存されます。このトランスフォーム ファイルを適用して、`CiscoJabberSetup.msi` のプロパティを変更できます。

インストーラの変換

インストーラをカスタマイズするため、トランスフォーム ファイルを適用します。



- (注) トランスフォーム ファイルの適用によって、`CiscoJabberSetup.msi` のデジタル シグニチャが変更されます。`CiscoJabberSetup.msi` の編集やリネームを試行すると、シグニチャが完全に削除されます。

手順

ステップ 1 Microsoft Orca を起動します。

ステップ 2 Microsoft Orca で `CiscoJabberSetup.msi` を開きます。

- a) [ファイル (File)] > [開く (Open)] を選択します。
- b) ファイル システムで `CiscoJabberSetup.msi` の場所を参照します。
- c) `CiscoJabberSetup.msi` を選択し、[開く (Open)] を選択します。

Microsoft Orca のインストール パッケージを開きます。インストーラのテーブルのリストが [テーブル (Tables)] ペインに表示されます。

ステップ 3 1033 (英語) 以外のすべての言語コードを削除します。

制約事項 カスタム インストーラから 1033 (英語) 以外のすべての言語コード削除する必要があります。

Microsoft Orcaでは、デフォルト (1033) 以外のいずれの言語ファイルもカスタム インストーラで保持されません。カスタム インストーラからすべての言語コードを削除しない場合、言語が英語以外のオペレーティングシステムでインストーラを実行できません。

- a) [表示 (View)] > [要約情報 (Summary Information)] を選択します。
[要約情報の編集 (Edit Summary Information)] ウィンドウが表示されます。
- b) [言語 (Language)] フィールドを見つけます。
- c) 1033 以外のすべての言語コードを削除します。
- d) [OK] を選択します。

英語がカスタム インストーラの言語として設定されます。

ステップ 4 トランスフォーム ファイルを適用します。

- a) [トランスフォーム (Transform)] > [トランスフォームの適用 (Apply Transform)] を選択します。
- b) ファイル システムのトランスフォーム ファイルの場所を参照します。
- c) トランスフォーム ファイルを選択し、[オープン (Open)] を選択します。

ステップ 5 [テーブル (Tables)] ペインのテーブルのリストから [プロパティ (Property)] を選択します。CiscoJabberSetup.msi のプロパティのリストがアプリケーション ウィンドウの右側のパネルに表示されます。

ステップ 6 必要とするプロパティの値を指定します。

ヒント CLEAR の値を 1 に設定し、以前のインストールからの既存のブートストラップ ファイルを上書きします。既存のブートストラップ ファイルを上書きしない場合、カスタム インストーラで設定する値は有効ではありません。

ステップ 7 必要のないプロパティを削除します。

設定されていないプロパティをドロップするのは重要です。そうしない場合、設定されたプロパティが有効になりません。必要ない各プロパティを 1 つずつドロップします。

- a) ドロップしたプロパティを右クリックします。
- b) [行を削除 (Drop Row)] を選択します。
- c) Microsoft Orca により続行を指示されたら、[OK] を選択します。

ステップ 8 カスタム インストーラで埋め込みストリームを保存できるようにします。

- a) [ツール (Tools)] > [オプション (Options)] を選択します。
- b) [データベース (Database)] タブを選択します。
- c) [[名前を付けて保存 (Save As)] の選択時に埋め込みストリームをコピーする (Copy embedded streams during 'Save As')] を選択します。
- d) [適用 (Apply)] を選択し、[OK] を選択します。

ステップ 9 カスタム インストーラを保存します。

- a) [ファイル (File)] > [名前を付けて変換を保存 (Save Transformed As)] を選択します。
- b) ファイル システム上の場所を選択してインストーラを保存します。
- c) インストーラの名前を指定してから、[保存 (Save)] を選択します。

関連トピック

[インストーラのプロパティ、\(110 ページ\)](#)

グループ ポリシーを使用した導入

Microsoft Group Policy Management Console (GPMC) を使用して、グループ ポリシー付きで Cisco Jabber for Windows を Microsoft Windows Server にインストールします。



- (注) グループ ポリシーを使用して Cisco Jabber for Windows をインストールするには、Cisco Jabber for Windows を導入する予定のすべてのコンピュータまたはユーザが同じドメインにある必要があります。

言語コードの設定

インストール言語の変更は、シスコが提供する MSI ファイルを使用するグループ ポリシーの配置シナリオでは必要ではありません。このような状況において、インストール言語は Windows ユーザ ロケール（形式）から決定されます。MSI が何らかの形で Orca により変更されている場合のみ、この手順を使用して [言語（Language）] フィールドを 1033 に設定します。

手順

- ステップ 1** Microsoft Orca を起動します。
Microsoft Orca は、Microsoft Web サイトからダウンロードできる Microsoft Windows SDK for Windows 7 and .NET Framework 4 の一部として提供されます。
- ステップ 2** CiscoJabberSetup.msi を開きます。
 - a) [ファイル（File）] > [開く（Open）] を選択します。
 - b) ファイル システムで CiscoJabberSetup.msi の場所を参照します。
 - c) CiscoJabberSetup.msi を選択し、[開く（Open）] を選択します。
- ステップ 3** [表示（View）] > [要約情報（Summary Information）] を選択します。
- ステップ 4** [言語（Language）] フィールドを見つけます。
- ステップ 5** [言語（Languages）] フィールドを 1033 に設定します。
- ステップ 6** [OK] を選択します。
- ステップ 7** カスタム インストーラで埋め込みストリームを保存できるようにします。
 - a) [ツール（Tools）] > [オプション（Options）] を選択します。
 - b) [データベース（Database）] タブを選択します。
 - c) [[名前を付けて保存（Save As）] の選択時に埋め込みストリームをコピーする（Copy embedded streams during 'Save As'）] を選択します。
 - d) [適用（Apply）] を選択し、[OK] を選択します。
- ステップ 8** カスタム インストーラを保存します。
 - a) [ファイル（File）] > [名前を付けて変換を保存（Save Transformed As）] を選択します。
 - b) ファイル システム上の場所を選択してインストーラを保存します。
 - c) インストーラの名前を指定してから、[保存（Save）] を選択します。

関連トピック

[サポートされる言語](#), (110 ページ)

グループ ポリシーでのクライアントの展開

グループ ポリシーで Cisco Jabber for Windows を展開するには、このタスクの手順に従います。

手順

-
- ステップ 1** 導入のためのソフトウェア配布ポイントにインストール パッケージをコピーします。
Cisco Jabber for Windows を導入する予定のすべてのコンピュータまたはユーザは、分散ポイントのインストール パッケージにアクセスする必要があります。
- ステップ 2** [スタート (Start)] > [ファイル名を指定して実行 (Run)] を選択し、次のコマンドを入力します。
GPMC.msc
[グループ ポリシー管理 (Group Policy Management)] コンソールが開きます。
- ステップ 3** 新しいグループ ポリシー オブジェクトを作成します。
a) 左側のペインの適切なドメインを右クリックします。
b) [このドメインに GPO を作成してここにリンクする (Create a GPO in this Domain, and Link it here)] を選択します。
[新しい GPO (New GPO)] ウィンドウが開きます。
c) [名前 (Name)] フィールドにグループ ポリシー オブジェクトの名前を入力します。
d) デフォルト値をそのままにするか、[発信元の開始 GPO (Source Starter GPO)] ドロップダウン リストから適切なオプションを選択し、次に [OK] を選択します。
新しいグループ ポリシーが、ドメインのグループ ポリシーのリストに表示されます。
- ステップ 4** 導入の範囲を設定します。
a) 左側のペインのドメインの下からグループ ポリシー オブジェクトを選択します。
グループ ポリシー オブジェクトが右側のペインに表示されます。
b) [スコープ (Scope)] タブの [セキュリティ フィルタリング (Security Filtering)] セクションで、[追加 (Add)] を選択します。
[ユーザ、コンピュータ、またはグループの選択 (Select User, Computer, or Group)] ウィンドウが開きます。
c) Cisco Jabber for Windows を導入するコンピュータとユーザを指定します。
- ステップ 5** インストール パッケージを指定します。
a) 左側のペインのグループ ポリシー オブジェクトを右クリックして、[編集 (Edit)] を選択します。
[グループ ポリシー管理エディタ (Group Policy Management Editor)] が開きます。

- b) [コンピュータの設定 (Computer Configuration)] を選択して、[ポリシー (Policies)] > [ソフトウェアの設定 (Software Settings)] を選択します。
- c) [ソフトウェアのインストール (Software Installation)] を右クリックして、[新規 (New)] > [パッケージ (Package)] を選択します。
- d) [ファイル名 (File Name)] の横にインストールパッケージの場所を入力します (例: \\server\software_distribution)。
重要 インストールパッケージの場所として Uniform Naming Convention (UNC) パスを入力する必要があります。UNC パスを入力しない場合、グループポリシーは Cisco Jabber for Windows を導入できません。
- e) インストールパッケージを選択して、[開く (Open)] を選択します。
- f) [ソフトウェアの導入 (Deploy Software)] ダイアログボックスで、[割り当て済み (Assigned)] を選択し、[OK] を選択します。

各コンピュータの次回起動時に、グループポリシーによって Cisco Jabber for Windows がそれぞれのコンピュータにインストールされます。

コマンドライン引数

Cisco Jabber for Windows をインストールする際に、指定可能なコマンドライン引数を確認します。

関連トピック

[クラウドベース SSO の有効化, \(77 ページ\)](#)

オーバーライドの引数

次の表では、過去のインストールで得た既存のブートストラップ ファイルを上書きするため、ユーザが指定する必要があるパラメータについて説明します。

引数	値	説明
CLEAR	1	<p>クライアントが過去のインストールで得た既存のブートストラップ ファイルを上書きするかどうかを指定します。</p> <p>クライアントは、ブートストラップ ファイルに、インストール中に設定する値と引数を保存します。クライアントは起動時に、ブートストラップ ファイルから設定をローディングします。</p>

CLEAR を指定すると、インストール中に次のことが起こります。

- 1 クライアントが既存のブートストラップ ファイルを削除する。

2 クライアントが新しいブートストラップ ファイルを作成する。

CLEAR を指定しない場合、クライアントはインストール中に既存のブートストラップ ファイルをチェックします。

- ブートストラップ ファイルがない場合、インストール時に、クライアントはブートストラップ ファイルを作成します。
- ブートストラップ ファイルが見つかる場合、クライアントは、ブートストラップ ファイルを上書きせず、既存の設定を保存します。



(注) Cisco Jabber for Windows を再インストールする場合は、次の点を検討する必要があります。

- クライアントは、既存のブートストラップ ファイルからの設定を保存しません。CLEAR を指定する場合は、必要に応じて他のインストール引数をすべて指定する必要があります。
- クライアントは、既存のブートストラップ ファイルにインストール引数を保存しません。インストール引数の値を変更する場合、または追加のインストール引数を指定する場合、既存の設定を上書きするために CLEAR を指定します。

既存のブートストラップ ファイルを上書きするには、次のようにコマンドラインで CLEAR を指定します。

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

モードタイプの引数

次の表は、製品モードを指定するコマンドラインの引数について説明します。

引数	値	説明
PRODUCT_MODE	Phone_Mode	<p>クライアントの製品モードを指定します。次の値を設定できます。</p> <p>Phone_Mode</p> <p>Cisco Unified Communications Manager は、オーセンティケーターです。</p> <p>基本機能としてオーディオデバイスを持つユーザをプロビジョニングする場合は、この値を選択します。</p>

製品モードの設定する場合

電話モードでの展開において、Cisco Unified Communications Manager がオーセンティケーターです。クライアントがオーセンティケーターを取得すると、製品モードが電話機モードであることが決定されます。ただし、クライアントは最初の起動時にデフォルトの製品モードで常に開始するため、ユーザはログイン後に電話モードにして、クライアントを再起動する必要があります。

Cisco Unified Communications Manager バージョン 9.x 以降

インストール中にPRODUCT_MODE をセットしないでください。クライアントはサービスプロファイルからオーセンティケーターを取得します。ユーザがログインすると、クライアントは、電話モードにして再起動するよう要請します。

Cisco Unified Communications Manager バージョン 8.x

Cisco Unified Communications Manager をオーセンティケーターとして設定するときは、インストール中に電話モードを指定できます。クライアントは、最初の起動時にブートストラップファイルを読み取り、電話機モードで開始するよう決定します。クライアントは、ブートストラップファイルまたは手動設定からオーセンティケーターとして Cisco Unified Communications Manager を取得します。ユーザがログインすると、クライアントの再起動は要求されません。

製品モードの変更

製品モードを変更するには、クライアントのオーセンティケーターを変更する必要があります。クライアントは、オーセンティケーターからの製品モードを決定します。

インストール後の製品モードの変更方法は、ご使用の展開により異なります。



(注) すべての展開において、ユーザは手動で **[手動設定とサインイン (Manual setup and sign in)]** ウィンドウのオーセンティケーターを設定できます。

この場合、製品モードを変更するには、**[手動設定とサインイン (Manual setup and sign in)]** ウィンドウのオーセンティケーターを変更するようにユーザに指示します。クライアントをアンインストールし、その後に再インストールしても、手動設定を上書きすることはできません。

Cisco Unified Communications Manager バージョン 9.x 以降の製品モードの変更

Cisco Unified Communications Manager バージョン 9.x の製品モードを変更するには、サービスプロファイルのオーセンティケーターを変更します。

手順

ステップ 1 適切なユーザのサービス プロファイルでオーセンティケータを変更します。

[デフォルト モード (Default Mode)] > [電話モード (Phone Mode)] を変更します。

IM and Presence を持つユーザのプロビジョニングを行わないでください。

サービス プロファイルが IM and presence サービス設定を含めない場合、オーセンティケータは Cisco Unified Communications Manager です。

[電話モード (Phone Mode)] > [デフォルト モード (Default Mode)] を変更します。

IM and Presence を持つユーザのプロビジョニングを行います。

IM and Presence プロファイルの [製品タイプ (Product Type)] フィールドの値を次に対して設定した場合、

- Unified CM (IM and Presence) オーセンティケータは、Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service です。
- WebEx (IM and Presence) オーセンティケータは、Cisco WebEx Messenger サービスです。

ステップ 2 ユーザにログアウトをしてから再度ログインするように指示します。
ユーザがクライアントにログインすると、サービス プロファイルの変更を取得し、オーセンティケータにユーザをログインさせます。クライアントは製品モードを決定すると、クライアントを再起動するようユーザに指示します。

ユーザがクライアントを再起動した後、製品モードの変更が完了します。

Cisco Unified Communications Manager バージョン 8.x の製品モードの変更

Cisco Unified Communications Manager バージョン 8.x の製品モードを変更するには、Cisco Jabber for Windows を再インストールして、オーセンティケータを変更します。

[デフォルト モード (Default Mode)] > [電話モード (Phone Mode)] を変更します。

最低限でも、次の引数を設定します。

- CLEAR=1 により、既存のブートストラップ ファイルが削除されます。
- AUTHENTICATOR=CUCM により、Cisco Unified Communications Manager がオーセンティケータとして設定されます。
- PRODUCT_MODE=Phone_Mode により、電話モードが製品モードに設定されます。

[電話モード (Phone Mode)] > [デフォルト モード (Default Mode)] を変更します。

最低限でも、次の引数を設定します。

- CLEAR=1 により、既存のブートストラップ ファイルが削除されます。
- AUTHENTICATOR= 次のいずれか。
 - CUP により、Cisco Unified Presence もしくは Cisco Unified Communications Manager IM and Presence Service がオーセンティケーターとして設定されます。
 - WEBEX により、Cisco WebEx Messenger サービスがオーセンティケーターとして設定されます。

認証引数

次の表は、認証ソースの指定をユーザが設定できるコマンドライン引数を説明しています。

引数	値	説明
AUTHENTICATOR	CUP CUCM WebEx	<p>クライアントに認証ソースを指定します。この値は、サービス ディスカバリに失敗した場合に使用されます。値として次のいずれかを設定します。</p> <p>CUP</p> <p>Cisco Unified Presence</p> <p>デフォルトの製品モードでのオンプレミスの展開。デフォルトの製品モードは、フル UC にも IM にもなりえます。</p> <p>CUCM</p> <p>Cisco Unified Communications Manager</p> <p>電話モードでのオンプレミスの展開。</p> <p>WebEx</p> <p>Cisco WebEx Messenger サービス</p> <p>クラウドベースまたはハイブリッドクラウドベースでの展開。</p> <p>Cisco Unified Communications Manager バージョン 9.x以降のオンプレミスの展開では、_cisco-uds SRV レコードを配置する必要があります。クライアントは、自動的にオーセンティケーターを決定することができます。</p>

引数	値	説明
CUP_ADDRESS	IP アドレス ホスト名 FQDN	<p>Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service のアドレスを指定します。値として次のいずれかを設定します。</p> <ul style="list-style-type: none"> • ホスト名 (<i>hostname</i>) • IP アドレス (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)
TFTP	IP アドレス ホスト名 FQDN	<p>TFTP サーバのアドレスを指定します。値として次のいずれかを設定します。</p> <ul style="list-style-type: none"> • ホスト名 (<i>hostname</i>) • IP アドレス (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>) <p>オーセンティケーターとして Cisco Unified Communications Manager を設定する場合は、この引数を指定する必要があります。</p> <p>(注) 展開する場合：</p> <ul style="list-style-type: none"> • 電話モードでは、クライアントコンフィギュレーションをホスティングする TFTP サーバのアドレスを指定する必要があります。 • デフォルトモードでは、デバイス設定をホスティングする Cisco Unified Communications Manager TFTP サービスを指定できます。
CTI	IP アドレス ホスト名 FQDN	<p>CTI サーバのアドレスを設定します。</p> <p>この引数を指定してします。</p> <ul style="list-style-type: none"> • オーセンティケーターとして Cisco Unified Communications Manager を設定します。 • ユーザは、デスクフォンデバイスを持ち、CTI サーバを必要とします。

引数	値	説明
CCMCIP	IP アドレス ホスト名 FQDN	<p>CCMCIP サーバのアドレスを設定します。</p> <p>この引数を指定してします。</p> <ul style="list-style-type: none"> • オーセンティケータとして Cisco Unified Communications Manager を設定します。 • CCMCIP サーバのアドレスが TFTP サーバアドレスと同じではありません。 <p>クライアントは両方のアドレスが同じであれば、TFTPサーバアドレスでCCMCIPサーバを検索できます。</p>
SERVICES_DOMAIN	ドメイン	<p>サービス ディスカバリの DNS SRV レコードが存在するドメインの値を設定します。</p> <p>この情報のインストーラ設定または手動設定をクライアントで使用する場合、この引数はDNS SRV レコードが存在しないドメインに設定します。</p> <p>この引数が指定されない場合、ユーザはサービスドメイン情報を指示されます。</p>
VOICE_SERVICES_DOMAIN	ドメイン	<p>ハイブリッド展開では、CAS検索を介して Webex を検出することが必要なドメインが、DNSレコードが展開されたドメインと異なる場合があります。 この場合、SERVICES_DOMAIN を WebEx の検出に使用されたドメインに設定し（またはユーザに電子メール アドレスを入力させる）、VOICE_SERVICES_DOMAIN を DNS レコードが展開されたドメインに設定します。 この設定が指定された場合、クライアントはサービス ディスカバリとエッジ検出の目的で、VOICE_SERVICES_DOMAIN の値を使用して次の DNS レコードを検索します。</p> <ul style="list-style-type: none"> • _cisco-uds • _cuplogin • _collab-edge <p>この設定は任意です。指定しない場合、DNS は SERVICES_DOMAIN、ユーザによる電子メール アドレス入力、またはキャッシュされたユーザ設定から取得したサービス ドメインで照会されます。</p>

引数	値	説明
EXCLUDED_SERVICES	次のうち 1 つ以上： • CUP • WEBEX • CUCM	<p>Jabber がサービスディスカバリから除外するサービスを示します。たとえば、WebEx の試験導入を実施し、会社のドメインが WebEx に登録されているが、Jabber ユーザが WebEx で認証することは避けたい場合があります。Jabber はオンプレミス CUPS サーバに認証させることになっています。この場合、次のように設定します。</p> <p>EXCLUDED_SERVICES=WEBEX</p> <p>値は、CUP、CUCM、WEBEX です。</p> <p>複数のサービスを除外するには、カンマ区切りの値を使用します。たとえば、CUPS、CUCM を除外するには、EXCLUDED_SERVICES=CUP,CUCM と指定します。すべてのサービスを除外するには、EXCLUDED_SERVICES=CUP,CUCM,WEBEX と指定します。</p> <p>すべてのサービスを除外した場合、Jabber クライアントの設定に手動設定またはブートストラップ設定を使用する必要があります。</p>

TFTP サーバアドレス

Cisco Jabber for Windows は、TFTP サーバから 2 つの異なる設定ファイルを取得します。

- 作成したクライアント設定ファイル。
- ユーザにデバイスをプロビジョニングしたときに Cisco Unified Communications Manager TFTP サービスに配置されたデバイス設定ファイル。

労力を最小限に抑えるために、Cisco Unified Communications Manager TFTP サービスにあるクライアント設定ファイルをホストする必要があります。すべての設定ファイルに対し TFTP サーバアドレスを 1 つのみ使用します。必要な場合にそのアドレスを指定できます。

ただし、デバイス設定を含む TFTP サーバとは異なる TFTP サーバでクライアント設定をホストできます。この場合、2 つの異なる TFTP サーバアドレスを使用します。一方のアドレスは、デバイス設定をホストする TFTP サーバのアドレスで、もう一方のアドレスは、クライアント設定ファイルをホストする TFTP サーバのアドレスです。

デフォルトの展開

このセクションでは、プレゼンスサーバがある展開で、2 つの異なる TFTP サーバアドレスを処理する方法について説明します。

以下を実行する必要があります。

- 1 プレゼンス サーバにあるクライアント設定をホストする TFTP サーバのアドレスを指定します。
- 2 インストール時に、TFTP 引数を使用して Cisco Unified Communications Manager TFTP サービスのアドレスを指定します。

クライアントは、初回起動時に以下を実行します。

- 1 ブートストラップ ファイルから Cisco Unified Communications Manager TFTP サービスのアドレスを取得します。
- 2 Cisco Unified Communications Manager TFTP サービスからデバイス設定を取得します。
- 3 プレゼンス サーバに接続します。
- 4 プレゼンス サーバのクライアント設定をホストする TFTP サービスのアドレスを取得します。
- 5 TFTP サーバからクライアント設定を取得します。

電話機モードの導入

このセクションでは、電話機モードの導入で、2 つの異なる TFTP サーバアドレスを処理する方法について説明します。

以下を実行する必要があります。

- 1 インストール時に、TFTP 引数を使用して、クライアント設定をホストする TFTP サーバのアドレスを指定します。
- 2 クライアント設定ファイルで、次の `TftpServer1` パラメータを使用して、デバイス設定をホストする TFTP サーバのアドレスを指定します。
- 3 TFTP サーバにあるクライアント設定ファイルをホストします。

クライアントは、初回起動時に以下を実行します。

- 1 ブートストラップ ファイルから TFTP サーバのアドレスを取得します。
- 2 TFTP サーバからクライアント設定を取得します。
- 3 クライアント設定から Cisco Unified Communications Manager TFTP サービスのアドレスを取得します。
- 4 Cisco Unified Communications Manager TFTP サービスからデバイス設定を取得します。

共通のインストール引数

次の表は、すべての展開に共通のコマンドライン引数についての説明です。

引数	値	説明
LANGUAGE	10 進数の LCID	<p>Cisco Jabber for Windows が使用する言語のロケール ID (LCID) を 10 進数で定義します。値は、サポートされる言語に対応する、10 進数の LCID でなくてはなりません。</p> <p>たとえば、次のいずれかを指定できます。</p> <ul style="list-style-type: none"> • 1033 は英語です。 • 1036 はフランス語です。 <p>この引数は省略可能です。値を指定しなかった場合は、Cisco Jabber for Windows はデフォルトとしてシステム ロケールの言語が使用されます。</p> <p>指定可能な言語のリストについては、「サポートされる言語」のトピックを参照してください。</p>
FORGOT_PASSWORD_URL	URL	<p>ユーザが失ったパスワードまたは忘れたパスワードをリセットできる URL を指定します。</p> <p>この引数は任意ですが推奨されています。</p> <p>(注) クラウドベース展開では、Cisco WebEx 管理ツールを使用してパスワード忘れの URL を指定できます。ただし、ユーザがサインインするまで、クライアントはパスワード忘れの URL を取得できません。</p>
TFTP_FILE_NAME	ファイル名	<p>グループ コンフィギュレーション ファイルの一意の名前を指定します。</p> <p>値として、未修飾か完全修飾のファイル名を指定できます。この引数の値として指定するファイル名は、TFTP サーバのその他の設定ファイルよりも優先されます。</p> <p>この引数は省略可能です。</p> <p>メモ Cisco Unified Communications Manager の CSF デバイス設定の [シスコ サポート フィールド (Cisco Support Field)] でグループ コンフィギュレーション ファイルを指定できます。</p>

引数	値	説明
LOGIN_RESOURCE	WBX MUT	<p>複数のクライアント インスタンスへのユーザ ログインを制御します。</p> <p>デフォルトでは、ユーザは、Cisco Jabber の複数インスタンスに同時にログインできます。デフォルトの動作を変更するには、次のいずれかの値を設定します。</p> <p>WBX</p> <p>ユーザは一度に 1 つの Cisco Jabber for Windows インスタンスにログインできます。</p> <p>Cisco Jabber for Windows は、ユーザの JID に wbxconnect サフィックスを付加します。ユーザは、wbxconnect サフィックスを使用する他の Cisco Jabber クライアントにログインできません。</p> <p>MUT</p> <p>ユーザは一度に 1 つの Cisco Jabber for Windows インスタンスにログインできますが、同時に他の Cisco Jabber クライアントにもログインできます。</p> <p>Cisco Jabber for Windows の各インスタンスが、ユーザの JID に固有のサフィックスを付加します。</p>
LOG_DIRECTORY	ローカル ファイル システムの絶対パス	<p>クライアントがログ ファイルを書き込むディレクトリを定義します。</p> <p>パス内での空白文字を回避するため、次の例のように引用符を使用します。</p> <p>"C:\my_directory\Log Directory"</p> <p>指定したパスに Windows の無効な文字を含めることはできません。</p> <p>デフォルト 値: %USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs</p>

引数	値	説明
CLICK2X	無効	<p>Cisco Jabber で click-to-x 機能を無効にします。</p> <p>インストール中にこの引数を指定する場合、</p> <ul style="list-style-type: none"> クライアントは、click-to-x 機能のハンドラとして、オペレーティングシステムで登録しません。 <p>つまり、この引数により、クライアントはインストール中のMicrosoft Windowsレジストリへの書き込みができなくなります。</p> <ul style="list-style-type: none"> クライアントを再インストールし、インストール後にクライアントで click-to-x 機能を有効にするには、この引数を省略します。

SSO 引数

ここでは、シングル サインオン（SSO）機能で Cisco Jabber for Windows を展開するために使用できるコマンドラインの引数について説明します。

クラウドベース SSO 引数

次の表の引数は、クラウドベース 展開にのみ適用されます。

引数	値	説明
SSO_ORG_DOMAIN	ドメイン名	<p>SSO サービスの URL を含む Cisco WebEx 組織のドメイン名を指定します。</p> <p>Cisco Jabber for Windows は、この引数を使用して組織から SSO サービスの URL を取得します。</p> <p>Cisco Jabber for Windows は、SSO サービス URL を取得した後、Cisco WebEx Messenger での認証のためのログイン トークンを要求できます。</p> <p>(注) Cisco WebEx 管理ツールで [カスタマー SSO サービス ログイン URL (Customer SSO Service Login URL)] の値として SSO サービスの URL を指定します。</p>

インストーラのプロパティ

次は、カスタム インストーラで変更可能なプロパティです。

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

これらのプロパティは、インストーラの引数に対応し、同じ値が設定されています。

サポートされる言語

次の表に、Cisco Jabber for Windows でサポートされる言語を示します。ご使用のオペレーティングシステムのコントロールパネルの言語設定を変更して、クライアントが使用する言語を変更できます。言語を選択した後、コンピュータを再起動すると、Cisco Jabber クライアントは自動的にシステム言語の選択と一致するよう言語設定を更新します。

アラビア語	フランス語	ルーマニア語
ブルガリア語	ヘブライ語	ロシア語
カタロニア語	ハンガリー語	セルビア語
クロアチア語	イタリア語	スロバキア語
チェコ語	日本語	スロベニア語
デンマーク語	韓国語	スウェーデン語
ドイツ語	ノルウェー語	タイ語
ギリシャ語	オランダ語	トルコ語

英語 スペイン語 フィンランド語	ポーランド語 ポルトガル語 (ブラジル) ポルトガル語 (ポルトガル)	中国語 (簡体字) 中国語 (繁体字)
------------------------	---	------------------------



(注) Cisco Jabber for Windows では、すべてのサブ言語のロケール ID はサポートしていません。たとえば、フランス語 (カナダ) を指定した場合は、Cisco Jabber for Windows ではフランス語 (フランス) が使用されます。

ロケール ID の詳細については、次のドキュメントを参照してください。

- *Microsoft Windows Locale Code Identifier (LCID) Reference*
- *Locale IDs Assigned by Microsoft*

関連トピック

[Microsoft Windows Locale Code Identifier \(LCID\) Reference](#)
[Locale IDs Assigned by Microsoft](#)

Cisco Media Services Interface

Cisco Jabber for Windows は、Cisco Media Services Interface version 4.1 for Microsoft Windows 7 および 8 をサポートしています。

トラフィック マーキング

Cisco Media Services Interface では、Cisco Prime Collaboration Manager および Cisco Medianet 対応ルータと連動する Microsoft Windows サービスを提供し、Cisco Jabber がネットワークで遅延やパケット損失を最小限に抑えて音声メディアとビデオメディアを送信できるようにします。

Cisco Jabber では、音声メディアまたはビデオメディアを送信する前に、Cisco Media Services Interface をチェックします。

- このサービスがコンピュータ上で機能していれば、Cisco Jabber は Cisco Media Services Interface にフロー情報を提供します。
その後、サービスはネットワークに信号を送信するため、ルータがフローを分類して Cisco Jabber のトラフィックにプライオリティを設定できるようになります。
- サービスが存在しない場合には、Cisco Jabber ではサービスを使用せずに、通常どおりに音声メディアとビデオメディアを送信します。



(注) Cisco Jabberでは、音声コールまたはビデオコールごとに Cisco Media Services Interface をチェックします。

デスクフォン ビデオ機能

デスクフォンのビデオ機能を有効にするために、Cisco Media Services Interface をインストールする必要があります。Cisco Media Services Interface に用意されているドライバにより、Cisco Jabber for Windows では以下のような処理を行うことができます。

- デスクフォン デバイスの検出。
- CAST プロトコルによるデスクフォン デバイスへの接続の確立と維持。

ネットワークの準備

トラフィック マーキングにCisco Media Services Interfaceをインストールするには、ネットワークを準備します。

手順

- ステップ 1** Cisco Prime Collaboration Manager をインストールします。
- ステップ 2** 適切であれば、Cisco Medianet に対応したルータまたはスイッチを設置します。
- ステップ 3** Cisco Media Services Interface によってアプリケーションに適用されるメタデータ属性を扱うようにネットワークを設定します。
ネットワークにあるすべてのデバイスが Cisco Medianet をサポートしている必要はありません。
最初の手順は、Cisco Media Services Interface のメタデータ属性に基づいてトラフィックの優先順位を決めることです。トラフィックがネットワークを通過するときに、他のすべてのデバイスも、そのトラフィックの優先順位を決める必要があります。ただし、そのトラフィックに対する特定の扱いを指定したポリシーがこれらのデバイスに設定されている場合はこの限りではありません。

Cisco Media Services Interface のインストール

手順

-
- ステップ 1** Cisco.com にあるダウンロード サイトから Cisco Media Services Interface のインストール プログラムをダウンロードします。
- ステップ 2** Cisco Jabber をインストールする各コンピュータに Cisco Media Services Interface をインストールします。
- Cisco Media Services Interface のインストールについては、該当の Cisco Medianet マニュアルを参照してください。
-

関連トピック

[「Download software」](#)
[Medianet Knowledge Base Portal](#)

Cisco Jabber for Windows のアンインストール

コマンドラインまたは Microsoft Windows コントロール パネルを使用して、Cisco Jabber for Windows をアンインストールできます。このマニュアルでは、コマンドラインを使用して Cisco Jabber for Windows をアンインストールする方法について説明します。

インストーラの使用

インストーラがファイル システムで利用可能な場合、Cisco Jabber for Windows を削除するために使用します。

手順

-
- ステップ 1** コマンドライン ウィンドウを開きます。
- ステップ 2** 次のコマンドを入力します。
- ```
msiexec.exe /x path_to_CiscoJabberSetup.msi
```
- 次の例を参考にしてください。
- ```
msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet
```
- ここで、/quiet により、サイレント アンインストールが指定されます。
-

コマンドによって、Cisco Jabber for Windows がコンピュータから削除されます。

製品コードの使用

インストーラがファイル システムで利用可能でない場合、Cisco Jabber for Windows を削除するために製品コードを使用します。

手順

-
- ステップ 1** 製品コードを検索します。
- a) Microsoft Windows レジストリ エディタを開きます。
 - b) レジストリ キー HKEY_CLASSES_ROOT\Installer\Products を見つけます。
 - c) [編集 (Edit)] > [検索 (Find)] を選択します。
 - d) [検索 (Find)] ウィンドウの [検索 (Find what)] テキスト ボックスに Cisco Jabber と入力し、[次を検索 (Find Next)] を選択します。
 - e) ProductIcon キーの値を検索します。
製品コードは、ProductIcon キーの値（たとえば、
C:\Windows\Installer\{*product_code*}\ARPPRODUCTICON.exe）です。
- （注） 製品コードは、Cisco Jabber for Windows の各バージョンによって変わります。

- ステップ 2** コマンドライン ウィンドウを開きます。

- ステップ 3** 次のコマンドを入力します。

```
msiexec.exe /x product_code
```

次の例を参考にしてください。

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

ここで、/quiet により、サイレント アンインストールが指定されます。

コマンドによって、Cisco Jabber for Windows がコンピュータから削除されます。



第 7 章

Cisco Jabber の設定

Cisco Jabber の設定方法およびユーザが設定できるコンフィギュレーション パラメータの確認方法について説明します。

- [クライアント設定の概要, 115 ページ](#)
- [Cisco Unified Communications Manager でのクライアントの設定, 116 ページ](#)
- [クライアント コンフィギュレーション ファイルの作成とホスティング, 125 ページ](#)
- [設定ファイルの構造, 134 ページ](#)
- [設定パラメータの概要, 135 ページ](#)
- [設定例, 137 ページ](#)
- [クライアント パラメータ, 138 ページ](#)
- [オプション パラメータ, 139 ページ](#)
- [電話パラメータ, 145 ページ](#)
- [ポリシー パラメータ, 148 ページ](#)
- [プレゼンス パラメータ, 159 ページ](#)
- [サービス クレデンシャル パラメータ, 160 ページ](#)
- [ボイスメール パラメータ, 161 ページ](#)
- [自動更新の設定, 162 ページ](#)
- [問題レポートの設定, 164 ページ](#)
- [カスタム埋め込みタブ, 164 ページ](#)

クライアント設定の概要

Cisco Jabber は、次のソースから設定を取得できます。

サービス プロファイル

Cisco Unified Communications Manager バージョン 9 以降の UC サービス プロファイルでクライアントを設定できます。ユーザがクライアントを初めて起動する際に、DNS SRV レコードを使用して Cisco Unified Communications Manager ホーム クラスタを検出し、UC サービス プロファイルから自動的に設定を取得します。

オンプレミスでの導入の場合のみ適用します。

電話機設定

Cisco Unified Communications Manager バージョン 9 以降の電話設定でクライアントを設定できます。クライアントは、UC サービス プロファイルの設定に加え、電話設定から設定を取得します。

オンプレミスでの導入の場合のみ適用します。

Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service

インスタント メッセージとプレゼンス機能を有効にして、プレゼンス サブスクリプション要求などの特定の設定を構成できます。

Cisco Unified Communications Manager バージョン 9 以降を備えたサービス ディスカバリを使用しない場合、クライアントは UC サービスを Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service から取得します。

オンプレミスでの導入の場合のみ適用します。

クライアント コンフィギュレーション ファイル

設定パラメータを含む XML ファイルを作成できます。そして、TFTP サーバの XML ファイルをホスティングします。ユーザがログインする際に、クライアントは TFTP サーバから XML ファイルを取得し、設定を適用します。

オンプレミスとクラウド ベースの展開に適用します。

Cisco WebEx 管理ツール

Cisco WebEx 管理ツールで、あるクライアントを設定できます。

クラウド ベースの展開にのみ適用します。

Cisco Unified Communications Manager でのクライアントの設定

Cisco Unified Communications Manager バージョン 9 以降の UC サービス プロファイルでクライアントを設定できます。

**重要**

- Cisco Jabber は、クライアントは、DNS クエリーから `_cisco-uds SRV` レコードを取得する場合のみ、Cisco Unified Communications Manager のサービス プロファイルから設定を取得します。

サービス ディスカバリの DNS 環境を設定しない場合、サービス プロファイルにクライアントを設定できません。

ハイブリッド環境では、CAS URL ルックアップが成功した場合、Cisco Jabber は設定内容を Cisco WebEx Messenger サービスから取得し、`_cisco-uds SRV` レコードは無視されます。

- 複数の Cisco Unified Communications Manager クラスタを使用した環境では、クラスタ間検索サービス (ILS) を設定する必要があります。ILS により、クライアントは、ユーザのホーム クラスタの検索とサービスの検出が可能になります。

ILS の設定方法については、『*Cisco Unified Communications Manager Features and Services Guide*』の適切なバージョンを参照してください。

サービス プロファイルのパラメータの設定

クライアントは、サービス プロファイルから UC サービス設定、および他の設定を取得できます。

サービス プロファイルのパラメータ

サービス プロファイルで設定する設定パラメータについて説明します。クライアント コンフィギュレーション ファイル内の対応するパラメータを確認します。

IM and Presence プロファイル

次の表では、インスタント メッセージとプレゼンスのプロファイルで設定できるコンフィギュレーション パラメータを示しています。

IM and Presence サービスの設定	説明
製品タイプ (Product Type)	<p>Cisco Jabber に認証ソースを提供し、次の値を持つ。</p> <p>Unified CM (IM and Presence)</p> <p>Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service は、オーセンティケーターです。</p> <p>WebEx (IM and Presence)</p> <p>Cisco WebEx Messenger サービスは、オーセンティケーターです。</p> <p>(注) このリリースの時点で、クライアントは、SRV レコードのクエリーに加え、HTTP クエリーを発行します。HTTP クエリーは、クライアントが Cisco WebEx Messenger サービスに対して認証するかどうかを指定することができます。</p> <p>HTTP クエリーの結果として、クライアントは、_cisco-uds SRV レコードを取得する前に、クラウドベースの展開で Cisco WebEx Messenger サービスに接続します。サービスが CAS の参照によってすでに検出されている場合、WebEx へ [製品タイプ (Product type)] フィールドの値を設定すると、実用的な効果がない場合があります。</p> <p>未設定 (Not set)</p> <p>サービス プロファイルが IM and presence サービス設定を含めない場合、オーセンティケーターは Cisco Unified Communications Manager です。</p>

IM and Presence サービスの設定	説明
プライマリ サーバ (Primary Server)	<p>プライマリ プレゼンス サーバのアドレスを指定します。</p> <p>オンプレミス展開</p> <p>Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service の完全修飾ドメイン名 (FQDN) を指定する必要があります。</p> <p>クラウドベース展開</p> <p>クライアントは、製品タイプパラメータの値として WebEx を選択する際に、デフォルトとして次の URL を使用します。</p> <p><code>https://loginp.webexconnect.com/cas/auth.do</code></p> <p>このデフォルトの URL は、設定した値を上書きします。</p>

ボイスメール プロファイル (Voicemail Profile)

次の表では、ボイスメールのプロファイルで設定される設定パラメータを示します。

ボイスメール サービスの設定	説明
ボイスメール サーバ (Voicemail server)	<p>ボイスメール サーバに対して接続設定を指定します。</p> <p>サービスプロファイルのボイスメール機能でユーザをプロビジョニングする詳細については、『<i>Server Setup Guide</i>』を参照してください。</p>
ボイスメールサービスのクレデンシャルソース (Credentials source for voicemail service)	<p>ボイスメール サービスでの認証を行うために、クライアントがインスタントメッセージおよびプレゼンス、または会議サービスのクレデンシャルを使用することを指定します。</p> <p>設定したクレデンシャル ソースがボイスメールのクレデンシャルと一致することを確認します。このパラメータに値を設定すると、ユーザは、クライアントユーザインターフェイスでボイスメールサービスのクレデンシャルを指定できません。</p>

会議プロファイル (Conferencing Profile)

次の表では、会議プロファイルで設定される設定パラメータを示します。

会議サービスの設定	説明
会議サーバ (Conferencing server)	会議サーバに対して接続設定を指定します。 サービス プロファイルの会議機能でユーザをプロビジョニングする詳細については、『 <i>Server Setup Guide</i> 』を参照してください。
Web 会議サービスのクレデンシャル ソース (Credentials source for web conference service)	会議サービスでの認証を行うために、クライアントがインスタント メッセージおよびプレゼンス、またはボイスメールサービスのクレデンシャルを使用することを指定します。 設定したクレデンシャル ソースが会議のクレデンシャルと一致することを確認します。

ディレクトリのプロファイル (Directory Profile)

サービス プロファイルのディレクトリ統合に関する詳細については、「*Directory Integration*」章を参照してください。

CTI プロファイル (CTI Profile)

次の表では、CTI プロファイルで設定される設定パラメータを示します。

CTI サービス設定	説明
CTI サーバ (CTI Server)	CTI サーバの接続設定を指定します。 CTI サービスでのユーザのプロビジョニングの詳細については、『 <i>Server Setup Guide</i> 』を参照してください。

UC サービスの追加

UC サービスを使用して、インスタント メッセージやプレゼンス、ボイスメール、会議、ディレクトリといったサービスのアドレス、ポート、プロトコル、その他設定を指定します。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
- ステップ 2** [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。

[UC サービスの検索と一覧表示 (Find and List UC Services)] ウィンドウが開きます。

ステップ 3 [新規追加 (Add New)] を選択します。

[UC サービスの設定 (UC Service Configuration)] ウィンドウが開きます。

ステップ 4 必要な [UC サービス タイプ (UC Service Type)] を選択し、[次へ (Next)] をクリックします

ステップ 5 必要に応じて UC サービスを設定し、[保存 (Save)] を選択します。

次の作業

サービス プロファイルに UC サービスを追加します。

サービス プロファイルの作成

UC サービスを追加して構成したら、サービス プロファイルに追加します。サービス プロファイルの追加設定を適用できます。

手順

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。

ステップ 2 [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [サービス プロファイル (Service Profile)] の順に選択します。

[UC サービスの検索と一覧表示 (Find and List UC Services)] ウィンドウが開きます。

ステップ 3 [新規追加 (Add New)] を選択します。

[サービス プロファイルの設定 (Service Profile Configuration)] ウィンドウが開きます。

ステップ 4 [名前 (Name)] フィールドにサービス プロファイルの名前を入力します。

ステップ 5 サービス プロファイルに、クラスタのデフォルトにする場合は、[システムデフォルトのサービス プロファイルに設定 (Make this the default service profile for the system)] を選択します。

(注) Cisco Unified Communications Manager バージョン 9.x だけで、インスタント メッセージ (IM のみ) 機能だけを持つユーザはデフォルトのサービス プロファイルを使用する必要があります。したがって IM のみのユーザだけにサービス プロファイルを適用する場合は、デフォルトとしてサービス プロファイルを設定する必要があります。

ステップ 6 UC サービスを追加し、追加設定を適用し、[保存 (Save)] を選択します。

次の作業

エンド ユーザ設定にサービス プロファイルを適用します。

サービス プロファイルの適用

UC サービスを追加し、サービス プロファイルを作成すると、ユーザにサービス プロファイルを適用します。ユーザが Cisco Jabber ログインすると、クライアントは、そのユーザのサービス プロファイルを Cisco Unified Communications Manager から取得できます。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
- ステップ 2** [ユーザ管理 (User Management)] > [エンド ユーザ (End User)] を選択します。
[ユーザの検索と一覧表示 (Find and List Users)] ウィンドウが開きます。
- ステップ 3** 既存のユーザを見つけるために検索条件を入力し、リストからユーザを選択します。
[エンド ユーザの設定 (End User Configuration)] ウィンドウが表示されます。
- ステップ 4** [サービス設定 (Service Settings)] セクションを見つけます。
- ステップ 5** [UC サービス プロファイル (UC Service Profile)] ドロップダウン リストからユーザに適用するサービス プロファイルを選択します。
- 重要** **Cisco Unified Communications Manager バージョン 9.x のみ** : ユーザがインスタント メッセージとプレゼンス機能 (IM のみ) のみを持つ場合、[デフォルトを使用 (Use Default)] を選択する必要があります。IM のみのユーザは、Cisco Unified Communications Manager バージョン 9.x で、[UC サービス プロファイル (UC Service Profile)] ドロップダウン リストからの選択内容に関係なく、デフォルトのサービス プロファイルを適用します。
- ステップ 6** 必要に応じてその他の設定を適用し、[保存 (Save)] を選択します。
-

デバイスへのユーザの関連付け

Cisco Unified Communications Manager バージョン 9.x のみにおいて、クライアントがユーザのサービス プロファイルを取得しようとするときは、最初に Cisco Unified Communications Manager からデバイスのコンフィギュレーションファイルを取得します。クライアントは、ユーザに適用したサービス プロファイルを取得するために、デバイス設定を使用できます。

たとえば、CSFAKenzi という名前の CSF デバイスと ADAM McKenzie をプロビジョニングします。クライアントは、Adam がログインした際に、Cisco Unified Communications Manager から CSFAKenzi.cnf.xml を取得します。クライアントは、CSFAKenzi.cnf.xml で次を検索します。

```
<userId serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

したがって、Cisco Unified Communications Manager バージョン 9.x を使用した場合、クライアントがユーザに適用されたサービス プロファイルを取得することが可能であることを保証するには、次を実行する必要があります:

- ユーザをデバイスに関連付けます。

- 適切なユーザにデバイス設定の [オーナーのユーザ ID (Owner User ID)] フィールドを設定します。この値が設定されていない場合、クライアントはデフォルトのサービス プロファイルを取得します。

手順

- ステップ 1** ユーザをデバイスに関連付けます。
- a) [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
 - b) [ユーザ管理 (User Management)] > [エンド ユーザ (End User)] を選択します。
 - c) 適切なユーザを検索し、選択します。
[エンド ユーザの設定 (End User Configuration)] ウィンドウが表示されます。
 - d) [デバイス情報 (Device Information)] セクションで [デバイスの割り当て (Device Association)] を選択します。
 - e) 必要に応じて、デバイスにユーザを関連付けます。
 - f) [エンド ユーザの設定 (End User Configuration)] ウィンドウに戻り、[保存 (Save)] を選択します。
- ステップ 2** デバイス設定の [オーナーのユーザ ID (Owner User ID)] フィールドを設定します。
- a) [デバイス (Device)] > [電話 (Phone)] の順に選択します。
 - b) 適切なデバイスを検索し、選択します。
[電話の設定 (Phone Configuration)] ウィンドウが開きます。
 - c) [デバイス情報 (Device Information)] セクションを探します。
 - d) [オーナー (Owner)] フィールドの値として [ユーザ (User)] を選択します。
 - e) [オーナーのユーザ ID (Owner User ID)] フィールドから対象のユーザ ID を選択します。
 - f) [保存 (Save)] を選択します。

電話の設定パラメータの設定

クライアントは、Cisco Unified Communications Manager の次の場所から電話の設定を取得できます。

Enterprise Phone Configuration

クラスタ全体に適用されます。



- (注) インスタント メッセージングとプレゼンス機能 (IM のみ) を持つ個人に対して、電話の設定パラメータを [エンタープライズ電話の設定 (Enterprise Phone Configuration)] ウィンドウで設定します。

Common Phone Profile Configuration

デバイスのグループを適用し、クラスタ設定より優先します。

Cisco Unified Client Services Framework (CSF) 電話機の設定

個々の CSF のデバイスを適用し、グループ設定より優先します。

電話の設定パラメータ

次の表には、電話機設定の [プロダクト固有の設定 (Product Specific Configuration Layout)] セクションで設定でき、クライアント コンフィギュレーション ファイルから対応するパラメータのマッピングされる設定パラメータを示しています。

デスクトップクライアントの設定	説明
ビデオ コール (Video Calling)	<p>ビデオ機能を有効または無効にします。</p> <p>有効 (Enabled)</p> <p>ユーザはビデオ コールを発信および受信できます。これがデフォルト値です。</p> <p>無効 (Disabled)</p> <p>ユーザはビデオ コールを送受信できません。</p> <p>制約事項 このパラメータは、CSF のデバイス設定でだけ使用可能です。</p>
ファイル転送でブロックするファイルタイプ (File Types to Block in File Transfer)	<p>ユーザに対して、特定のファイルタイプの転送の制限をします。</p> <p>値としてセット ファイル拡張子を設定します (例: .exe)。</p> <p>複数の値を区切るには、セミコロンを使用します。次に例を示します。</p> <p>.exe;.msi;.rar;.zip</p>

デスクトップ クライアントの設定	説明
電話制御での自動起動 (Automatically Start in Phone Control)	<p>クライアント初回起動時のユーザの電話タイプを設定します。初回起動後、ユーザは電話タイプを変更できます。クライアントは、ユーザ設定を保存し、以降の起動でその設定を使用します。</p> <p>有効 (Enabled)</p> <p>コールにデスクフォンデバイスを使用します。</p> <p>無効 (Disabled)</p> <p>コールにソフトフォン (CSF) デバイスを使用します。これがデフォルト値です。</p>
Jabber for Windows ソフトウェア更新サーバ URL (Jabber For Windows Software Update Server URL)	<p>クライアント更新情報を保持する XML ファイルに URL 指定します。クライアントは、Web サーバから XML ファイルを取得するために、この URL を使用します。</p> <p>ハイブリッドクラウドベースの展開では、自動更新を設定するために Cisco WebEx 管理ツールを使用する必要があります。</p>
問題レポートのサーバ URL (Problem Report Server URL)	<p>ユーザが問題レポートを送信できるように、カスタムスクリプトの URL を指定します。</p>

クライアントコンフィギュレーションファイルの作成とホスティング

オンプレミスとハイブリッドクラウドベースの展開で、クライアント コンフィギュレーション ファイルを作成し、Cisco Unified Communications Manager TFTP サービスでホスティングします。

クラウドベースの展開では、Cisco WebEx 管理ツールでクライアントを設定する必要があります。ただし、Cisco WebEx 管理ツールで使用できない設定でクライアントを設定するために、オプションで TFTP サーバを設定することができます。

**重要**

ほとんどの環境では、クライアントがサービスに接続するための設定は必要はありません。次のようなカスタム コンテンツをなどが必要な場合のみ、コンフィギュレーション ファイルを作成する必要があります。

- 埋め込み HTML タブ
- 自動アップデート
- 問題のレポート
- ユーザ ポリシーとオプション

クライアントコンフィギュレーションファイル

コンフィギュレーションファイルを展開する前に、グローバルおよびグループコンフィギュレーションファイルの違いを確認します。正常にコンフィギュレーションファイルを展開するには、サポートされる符号化方式などのコンフィギュレーションファイルの要件を確認する必要があります。

グローバル設定ファイル

グローバル設定ファイルは、すべてのユーザに適用されます。クライアントは、ログインシーケンス中に TFTP サーバのグローバル構成ファイルをダウンロードします。

グローバル設定ファイルのデフォルト名は、jabber-config.xml です。

グループ設定ファイル

グループ設定ファイルは、ユーザのサブセットに適用されます。グループ設定ファイルは、グローバル設定ファイルよりも優先されます。

Cisco Jabber は、ユーザが電話アカウントに初めてサインインした後に、グループ設定ファイルを取得します。クライアントは、ユーザにログインするよう指示します。2 回目のログインシーケンスの間、クライアントは TFTP サーバからグループ設定ファイルをダウンロードします。

Cisco Jabber は、グループ設定ファイルを次の手順で読み込みます。

ユーザがサインインしていない場合

- 1 ユーザがサインインすると、クライアントは設定が変更されたことをユーザに通知します。
- 2 ユーザがサインアウトします。
- 3 ユーザがログインすると、クライアントがグループ設定をロードします。

ログインしたユーザがコールにソフト フォンを使用します。

- 1 クライアントは、設定の変更に關してユーザに通知します。
- 2 ユーザがサインアウトします。
- 3 ユーザがログインすると、クライアントがグループ設定をロードします。

ログインしたユーザがコールにデスク フォンを使用します。

- 1 ユーザがサインアウトします。
- 2 ユーザがサインインすると、クライアントは設定が変更されたことをユーザに通知します。
- 3 ユーザがサインアウトします。
- 4 ユーザがログインすると、クライアントがグループ設定をロードします。

ユーザがサインアウトする前に、ソフト フォンを使用してコールするオプションを選択した場合、クライアントはユーザにサインアウトしてからサインインし直すよう指示し、グループ設定を読み込みます。

グループ設定ファイル名

Cisco Unified Communications Manager の CSF デバイス設定の [シスコ サポート フィールド (Cisco Support Field)] で、グループ設定ファイルの名前を指定します。

Cisco Unified Communications Manager の CSF デバイス設定のグループ設定ファイルの名前を削除すると、クライアントが変更を検出し、ユーザにサインアウトするよう指示し、グローバル設定ファイルを読み込みます。CSF デバイス設定のグループ設定ファイル名を削除するには、`configurationFile=group_configuration_file_name.xml` 文字列全体を削除するか、文字列からグループ設定ファイル名を削除します。

ユーザがデスク フォン以外のデバイスを所有していない場合は、次のコマンドライン引数を使用して、インストール中に異なるグループに対して一意の名前の設定ファイルを指定してください。

`TFTP_FILE_NAME`

設定ファイルの要件

- 設定ファイル名は、大文字と小文字を区別します。エラーを回避し、クライアントが TFTP サーバからファイルを取得できるよう、ファイル名には小文字を使用してください。
- 設定ファイルには、utf-8 エンコーディングを使用する必要があります。
- クライアントは、有効な XML 構造のない設定ファイルは読み込めません。設定ファイルの構造で終了要素をチェックし、要素が正しく入れ子になっていることを確認します。

- XML には、有効な XML 文字エンティティ参照しか含めることができません。たとえば、&ではなく & を使用してください。XML に無効な文字を含めると、クライアントはコンフィギュレーション ファイルを解析できません。



ヒント Microsoft Internet Explorer で設定ファイルを開き、無効な文字やエンティティがないことを確認します。

Internet Explorer に XML 構造の全体が表示される場合は、設定ファイルには無効な文字やエンティティは含まれていません。

Internet Explorer に XML 構造の一部しか表示されない場合は、設定ファイルには無効な文字やエンティティが含まれている可能性があります。

TFTP サーバアドレスの指定

クライアントは、TFTP サーバからコンフィギュレーション ファイルを取得します。クライアント設定の最初のステップは、クライアントがコンフィギュレーション ファイルにアクセスできるようにするため、TFTP サーバのアドレスを指定することです。



注目 Cisco Jabber が、DNS クエリーから `_cisco-uds` SRV レコードを取得すると、自動的にユーザのホーム クラスタの検索ができます。その結果、クライアントは、Cisco Unified Communications Manager TFTP サービスを見つけることができます。

`_cisco-uds` SRV レコードを導入する場合、TFTP サーバアドレスを指定する必要はありません。

Cisco Unified Presence での TFTP サーバの指定

次の手順を実行して、Cisco Unified Presence で TFTP サーバのアドレスを指定します。

手順

- ステップ 1** [Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] インターフェイスを開きます。
- ステップ 2** [アプリケーション (Application)] > [Cisco Jabber][設定 (Settings)] の順に選択します。
 (注) Cisco Unified Presence のバージョンによっては、パスは次のようになります。[アプリケーション (Application)] > [Cisco Unified Personal Communicator] > [設定 (Settings)]。
 [Cisco Jabber の設定 (Cisco Jabber Settings)] Cisco Jabber Settings ウィンドウが開きます。
- ステップ 3** 次のセクションの 1 つで TFTP サーバを指定するフィールドを探します。セクションは、Cisco Unified Presence のバージョンにより異なります。

- Cisco Jabber のセキュリティ設定 (Cisco Jabber Security Settings)
- CUPC グローバル設定 (CUPC Global Settings)

ステップ 4 次のフィールドで、プライマリおよびバックアップの TFTP サーバの IP アドレスを指定します。

- プライマリ TFTP サーバ (Primary TFTP Server)
- バックアップ TFTP サーバ (Backup TFTP Server)
- バックアップ TFTP サーバ (Backup TFTP Server)

ステップ 5 [保存 (Save)] を選択します。

Cisco Unified Communications Manager IM and Presence Service での TFTP サーバの指定

次の手順を実行して、Cisco Unified Communications Manager IM and Presence Service で TFTP サーバのアドレスを指定します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] インターフェイスを開きます。

ステップ 2 [アプリケーション (Application)] > [レガシークライアント (Legacy Clients)] > [設定 (Settings)] の順に選択します。
[レガシークライアントの設定 (Legacy Client Settings)] ウィンドウが開きます。

ステップ 3 [レガシークライアントのセキュリティ設定 (Legacy Client Security Settings)] セクションを探します。

ステップ 4 次のフィールドで、プライマリおよびバックアップの TFTP サーバの IP アドレスを指定します。

- プライマリ TFTP サーバ (Primary TFTP Server)
- バックアップ TFTP サーバ (Backup TFTP Server)
- バックアップ TFTP サーバ (Backup TFTP Server)

ステップ 5 [保存 (Save)] を選択します。

電話モードでの TFTP サーバの指定

電話機モードでクライアントを展開する場合、TFTP サーバのアドレスを次のように指定できます。

- クライアントを起動した際に、ユーザは手動で TFTP サーバアドレスを入力できる。
- TFTP 引数を使用してインストール時に TFTP サーバアドレスを指定する。

Cisco WebEx 管理ツール による TFTP サーバの指定

クライアントが Cisco WebEx Messenger サービスに接続すると、Cisco WebEx 管理ツール で TFTP サーバのアドレスを指定します。

手順

-
- ステップ 1 Cisco WebEx 管理ツール を開きます。
 - ステップ 2 [設定 (Configuration)] タブを選択します。
 - ステップ 3 [追加サービス (Additional Services)] セクションで [Unified Communications] を選択します。
[Unified Communications] ウィンドウが開きます。
 - ステップ 4 [クラスタ (Clusters)] タブを選択します。
 - ステップ 5 適切なクラスタをリストから選択します。
[クラスタの編集 (Edit Cluster)] ウィンドウが開きます。
 - ステップ 6 [Cisco Unified Communications Manager サーバの設定 (Cisco Unified Communications Manager Server Settings)] セクションで [サーバの詳細設定 (Advanced Server Settings)] を選択します。
 - ステップ 7 [TFTP サーバ (TFTP Server)] フィールドでプライマリ TFTP サーバの IP アドレスを指定します。
 - ステップ 8 [バックアップサーバ 1 (Backup Server #1)] フィールドと [バックアップサーバ 2 (Backup Server #2)] フィールドでバックアップ TFTP サーバの IP アドレスを指定します。
 - ステップ 9 [保存 (Save)] を選択します。
[クラスタの編集 (Edit Cluster)] ウィンドウが閉じます。
 - ステップ 10 [Unified Communications] ウィンドウで [保存 (Save)] を選択します。
-

グローバル設定の作成

導入において、すべてのユーザのクライアントを設定します。



メモ

複数の TFTP サーバがある環境の場合、すべての TFTP サーバで設定ファイルを同じにする必要があります。

手順

-
- ステップ 1 任意のテキストエディタを使用して jabber-config.xml という名前のファイルを作成します。

- ファイル名には小文字を使用してください。
- UTF-8 エンコードを使用してください。

ステップ 2 jabber-config.xml で必須の設定パラメータを定義します。

コンフィギュレーションファイルの構造が無効な場合、クライアントでは、設定した値を読み取れません。詳細については、本章の XML サンプルを確認してください。

ステップ 3 TFTP サーバ上でグループ設定ファイルをホストします。

グループ設定の作成

異なるユーザのセットに異なるクライアント設定を適用します。

CSF のデバイスを持つユーザをプロビジョニングする場合、デバイス設定で [シスコ サポート フィールド (Cisco Support Field)] フィールドにグループ コンフィギュレーション ファイル名を指定します。

ユーザに CSF のデバイスがない場合は、引数 TFTP_FILE_NAME を使用してインストール時に各グループの一意の構成ファイル名を設定します。

はじめる前に

[シスコ サポート フィールド (Cisco Support Field)] フィールドは、Cisco Unified Communications Manager バージョン 8.6.x またはそれ以前のバージョンには存在しません。次のように COP ファイルを適用する必要があります。

- 1 Cisco Jabber 管理パッケージをダウンロードします。
- 2 ciscocm.addcsfsupportfield.cop を Cisco Jabber 管理パッケージからファイルシステムにコピーします。
- 3 Cisco Unified Communications Manager に ciscocm.addcsfsupportfield.cop を展開します。

COP ファイルを展開する手順については、Cisco Unified Communications Manager のマニュアルを参照してください。

COP ファイルにより、[電話の設定 (Phone Configuration)] ウィンドウの [デスクトップ クライアントの設定 (Desktop Client Settings)] セクションで [シスコ サポート フィールド (Cisco Support Field)] フィールドが CDF デバイスに追加されます。

手順

ステップ 1 任意のテキスト エディタを使用して XML グループ設定ファイルを作成します。グループ設定ファイルには、適切な名前を指定できます (例 : jabber-groupa-config.xml) 。

- ファイル名には小文字を使用してください。
- UTF-8 エンコードを使用してください。

ステップ 2 グループ設定ファイルで必須の設定パラメータを定義します。

コンフィギュレーションファイルの構造が無効な場合、クライアントでは、設定した値を読み取れません。詳細については、本章の XML サンプルを確認してください。

ステップ 3 グループ コンフィギュレーション ファイル名を指定します。

- [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
- [デバイス (Device)] > [電話 (Phone)] の順に選択します。
- グループ設定ファイルを適用する適切な CSF デバイスを検索して選択します。
[電話の設定 (Phone Configuration)] ウィンドウが開きます。
- [プロダクト固有の設定 (Product Specific Configuration Layout)] > [デスクトップクライアントの設定 (Desktop Client Settings)] に移動します。
- [シスコ サポート フィールド (Cisco Support Field)] フィールドに、
`configurationfile=group_configuration_file_name.xml` を入力します。
たとえば、次のように入力します：`configurationfile=groupa-config.xml`

複数のエントリを区切るには、セミコロンを使用します。複数のグループ コンフィギュレーション ファイルを追加しないでください。クライアントは、[シスコ サポート フィールド (Cisco Support Field)] フィールドの最初のグループ設定だけを使用します。

TFTP サーバ上でデフォルトディレクトリ以外の場所にあるグループ設定ファイルをホストする場合には、パスとファイル名を指定する必要があります (例：

`configurationfile=/customFolder/jabber-groupa-config.xml`)。

- [保存 (Save)] を選択します。

ステップ 4 TFTP サーバ上でグループ設定ファイルをホストします。

コンフィギュレーション ファイルのホスティング

任意の TFTP サーバのコンフィギュレーション ファイルをホストできます。ただし、デバイス コンフィギュレーション ファイルが保存されるのと同じ場所である Cisco Unified Communications Manager TFTP サーバ上のコンフィギュレーション ファイルのホスティングを推奨します。

手順

-
- ステップ 1** Cisco Unified Communications Manager の [Cisco Unified OS の管理 (Cisco Unified OS Administration)] インターフェイスを開きます。
- ステップ 2** [ソフトウェアのアップグレード (Software Upgrades)] > [TFTP ファイル管理 (TFTP File Management)] を選択します。
- ステップ 3** [ファイルのアップロード (Upload File)] を選択します。
- ステップ 4** [ファイルのアップロード (Upload File)] セクションで [参照 (Browse)] を選択します。
- ステップ 5** ファイル システム上の設定ファイルを選択します。
- ステップ 6** [ファイルのアップロード (Upload File)] セクションの [ディレクトリ (Directory)] テキストボックスに値を指定しないでください。
コンフィギュレーションファイルが TFTP サーバ上のデフォルト ディレクトリに存在するようにするため、[ディレクトリ (Directory)] テキストボックスには空の値を残す必要があります。
- ステップ 7** [ファイルのアップロード (Upload File)] を選択します。
-

TFTP サーバの再起動

クライアントがコンフィギュレーション ファイルにアクセスするには、TFTP サーバを再起動する必要があります。

手順

-
- ステップ 1** Cisco Unified Communications Manager の [Cisco Unified サービスアビリティ (Cisco Unified Serviceability)] インターフェイスを開きます。
- ステップ 2** [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。
- ステップ 3** [CM サービス (CM Services)] セクションから [Cisco Tftp] を選択します。
- ステップ 4** [リスタート (Restart)] を選択します。
再起動の確認を求めるウィンドウが表示されます。
- ステップ 5** [OK] を選択します。
「Cisco Tftp サービスの再起動操作が成功しました (Cisco Tftp Service Restart Operation was Successful) 」というステータスが表示されます。
- ステップ 6** [更新 (Refresh)] を選択し、Cisco Tftp サービスが正常に起動していることを確認します。
-

次の作業

設定ファイルが TFTP サーバで使用できることを確認するには、任意のブラウザで設定ファイルを開きます。通常、`http://tftp_server_address:6970/jabber-config.xml` の URL にあるグローバル設定ファイルにアクセスできます。

設定ファイルの構造

次の要素を含む XML 形式のクライアント コンフィギュレーション ファイルを作成します。

XML 宣言

コンフィギュレーション ファイルは、XML 標準に準拠し、次の宣言が含まれている必要があります。

```
<?xml version="1.0" encoding="utf-8"?>
```

ルート要素

ルート要素の `config` には、すべてのグループ要素が含まれます。次のように、ルート要素にバージョン属性を追加する必要があります。

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
</config>
```

グループ要素

グループ要素には、コンフィギュレーションパラメータおよび値が含まれます。グループ要素はルート要素内にネストする必要があります。

グループ要素

次の表で、クライアント設定ファイルで指定できるグループ要素について説明します。

要素	説明
Client	クライアントの設定パラメータが含まれます。
Directory	ディレクトリ統合の設定パラメータが含まれます。
Options	ユーザ オプションの設定パラメータが含まれます。
Phone	電話機サービスの設定パラメータが含まれます。
Policies	ポリシーの設定パラメータが含まれます。
Presence	プレゼンス オプションの設定パラメータが含まれます。
Voicemail	ボイスメール サービスの設定パラメータが含まれます。



(注) ディレクトリ パラメータについては、「*Integrate with Directory Sources*」章を参照してください。

関連トピック

[設定パラメータの概要, \(135 ページ\)](#)

XML 構造

次のスニペットは、クライアント設定ファイルの XML 構造を示します。

```
<Client>
  <parameter>value</parameter>
</Client>
<Directory>
  <parameter>value</parameter>
</Directory>
<Options>
  <parameter>value</parameter>
</Options>
<Phone>
  <parameter>value</parameter>
</Phone>
<Policies>
  <parameter>value</parameter>
</Policies>
<Presence>
  <parameter>value</parameter>
</Presence>
<Voicemail>
  <parameter>value</parameter>
</Voicemail>
```

設定パラメータの概要

次の表は、ユーザがクライアント設定に含めることができるすべてのパラメータを示します。

パラメータ	グループ要素
PrtLogServerUrl	Client
UpdateUrl	Client
jabber-plugin-config	Client
Forgot_Password_URL	Client
Persistent_Chat_Enabled	Client
Set_Status_Away_On_Inactive	Options
Set_Status_Inactive_Timeout	Options
Set_Status_Away_On_Lock_OS	Options

パラメータ	グループ要素
StartCallWithVideo	Options
Start_Client_On_Start_OS	Options
AllowUserCustomTabs	Options
ShowContactPictures	Options
ShowOfflineContacts	Options
DockedWindowVisible	Options
DockedWindowPosition	Options
DeviceAuthenticationPrimaryServer	Phone
DeviceAuthenticationBackupServer	Phone
TftpServer1	Phone
TftpServer2	Phone
CtiServer1	Phone
CtiServer2	Phone
useCUCMGroupForCti	Phone
CcmcipServer1	Phone
CcmcipServer2	Phone
Meeting_Server_Address	Phone
Meeting_Server_Address_Backup	Phone
Meeting_Server_Address_Backup2	Phone
EnableVideo	Policies
InitialPhoneSelection	Policies
UserDefinedRemoteDestinations	Policies
enableLocalAddressBookSearch	Policies
EnableAccessoriesManager	Policies
BlockAccessoriesManagerPlugins	Policies
ForceFontSmoothing	Policies
Screen_Capture_Enabled	Policies
File_Transfer_Enabled	Policies
Disallowed_File_Transfer_Types	Policies
EnableBFCPVideoDesktopShare	Policies
Meetings_Enabled	Policies

パラメータ	グループ要素
Telephony_Enabled	Policies
Voicemail_Enabled	Policies
EnableTelProtocolHandler	Policies
EnableSaveChatToFile	Policies
EnableSIPURIDialling	Policies
DirectoryURI	Policies
ForceC2XDirectoryResolution	Policies
ServiceDiscoveryExcludedServices	Policies
VoiceServicesDomain	Policies
LoginResource	Presence
PresenceServerAddress	Presence
PresenceServerURL	Presence
VoiceMailService_UseCredentialsFrom	Voicemail
VVM_Mailstore_Server_0	Voicemail

関連トピック

[グループ要素, \(134 ページ\)](#)
[クライアント パラメータ, \(138 ページ\)](#)
[オプション パラメータ, \(139 ページ\)](#)
[電話パラメータ, \(145 ページ\)](#)
[ポリシー パラメータ, \(148 ページ\)](#)
[プレゼンス パラメータ, \(159 ページ\)](#)
[サービス クレデンシャル パラメータ, \(160 ページ\)](#)
[ボイスメール パラメータ, \(161 ページ\)](#)
[ディレクトリ ソースとの統合, \(173 ページ\)](#)

設定例

次は、オンプレミス配置の設定例です。

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <PrtLogServerUrl>http://server_name:port/path/prt_script.php</PrtLogServerUrl>
  </Client>
  <jabber-plugin-config>
    <browser-plugin>
      <page refresh="true" preload="true">
        <tooltip>Cisco</tooltip>
        <icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
      </page>
    </browser-plugin>
  </jabber-plugin-config>
</config>
```

```

    <url>www.cisco.com</url>
  </page>
</browser-plugin>
</jabber-plugin-config>
</Client>
<Options>
  <Set_Status_Inactive_Timeout>20</Set_Status_Inactive_Timeout>
  <StartCallWithVideo>false</StartCallWithVideo>
</Options>
<Policies>
  <Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>
</Policies>
</config>

```

クライアント パラメータ

次の表に、Client要素内で指定できるパラメータを示します。

パラメータ	値	説明
PrtLogServerUrl	URL	問題レポートを送信するためのカスタム スクリプトを指定します。
UpdateUrl	URL	<p>HTTP サーバ上の自動更新 XML 定義ファイルへの URL を指定します。クライアントは、更新 XML ファイルを取得するために、この URL を使用します。</p> <p>ハイブリッドクラウドベースの展開では、自動更新を設定するために Cisco WebEx 管理ツールを使用する必要があります。</p>
jabber-plugin-config	プラグイン定義	HTML コンテンツを表示するカスタム埋め込みタブなどのプラグインの定義が含まれます。
Forgot_Password_URL	URL	<p>パスワードを忘れた場合に、パスワードをリセットまたは取得するための Web ページの URL を指定します。</p> <p>ハイブリッドクラウドベースの展開では、忘れたパスワードをリセットまたは取得するために、Cisco WebEx 管理ツールを使用して、ユーザを Web ページに導きます。</p>

パラメータ	値	説明
Persistent_Chat_Enabled	true false	<p>クライアントで[パーシステントチャット (Persistent Chat)]機能を使用できるようにするかどうかを指定します。</p> <p>true</p> <p>値を true に設定すると、[パーシステントチャット (Persistent Chat)]インターフェイスがクライアントに表示されます。</p> <p>false</p> <p>デフォルト値は false です。デフォルト値は設定ファイルに設定がない場合に使用されます。</p>

関連トピック

[設定パラメータの概要, \(135 ページ\)](#)

オプションパラメータ

次の表に、Options要素内で指定できるパラメータを示します。

パラメータ	値	説明
Set_Status_Away_On_Inactive	true false	<p>ユーザが非アクティブになったときにアベイラビリティステータスを[退席中 (Away)]に変更するかどうかを指定します。</p> <p>true</p> <p>ユーザが非アクティブになると、アベイラビリティステータスが[退席中 (Away)]に変更されます。これがデフォルト値です。</p> <p>false</p> <p>ユーザが非アクティブの場合、アベイラビリティステータスは[退席中 (Away)]に変更されません。</p>
Set_Status_Inactive_Timeout	分単位での時間	<p>ユーザが非アクティブになった場合にアベイラビリティステータスが[退席中 (Away)]に変更される前の時間を分単位で設定します。</p> <p>デフォルト値は 15 です。</p>

パラメータ	値	説明
Set_Status_Away_On_Lock_OS	true false	<p>ユーザがオペレーティング システムをロックしたときに、アベイラビリティ ステータスを [退席中 (Away)] に変更するかどうかを指定します。</p> <p>true</p> <p>ユーザがオペレーティング システムをロックしたときに、アベイラビリティ ステータスは [退席中 (Away)] に変更されます。これがデフォルト値です。</p> <p>false</p> <p>ユーザがオペレーティング システムをロックしても、アベイラビリティ ステータスは [退席中 (Away)] に変更されません。</p>

パラメータ	値	説明
StartCallWithVideo	true false	

パラメータ	値	説明
		<p>ユーザがコールを発信するときのコールの開始方法を指定します。コールは、音声のみ、または音声とビデオにより開始できます。</p> <p>true</p> <p>コールは常に音声およびビデオで始まります。これがデフォルト値です。</p> <p>false</p> <p>コールは常に音声のみで始まります。</p> <p>重要 サーバ設定は、クライアントコンフィギュレーションファイルのパラメータよりも優先されます。ただし、ユーザがクライアントのユーザインターフェイスのデフォルトのオプションを変更する場合、その設定は、サーバとクライアントの両方に優先します。</p> <p>次の手順に従って、サーバの設定を行います。</p> <p>Cisco Unified Presence</p> <ol style="list-style-type: none"> 1 [Cisco Unified Presence の管理 (Cisco Unified Presence Administration)] インターフェイスを開きます。 2 [アプリケーション (Application)] > [Cisco Jabber][設定 (Settings)] の順に選択します。 3 [ビデオは常にミュート状態でコールを起動 (Always begin calls with video muted)] パラメータのオン/オフを切り替え、[保存 (Save)] を選択します。 <p>Cisco Unified Communications Manager バージョン 9.x 以降</p> <ol style="list-style-type: none"> 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。 2 [システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。

パラメータ	値	説明
		3 [ビデオで通話を開始しない (Never Start Call with Video)] パラメータの値を設定し、[保存 (Save)] を選択します。
Start_Client_On_Start_OS	true false	<p>オペレーティング システムが起動したときに、クライアントが自動的に起動するかどうかを指定します。</p> <p>true</p> <p>クライアントは自動的に起動されます。</p> <p>false</p> <p>クライアントは自動的に起動されません。これがデフォルト値です。</p>
AllowUserCustomTabs	true false	<p>ユーザが独自のカスタム埋め込みタブを作成できるようにするかどうかを指定します。</p> <p>true</p> <p>ユーザはカスタム埋め込みタブを作成できます。</p> <p>false</p> <p>ユーザはカスタム埋め込みタブを作成できません。これがデフォルト値です。</p> <p>(注) このパラメータはユーザが作成するカスタム埋め込みタブだけに影響します。</p> <ul style="list-style-type: none"> • ユーザにカスタム埋め込みタブの作成を許可しても、ユーザはクライアントの設定で定義されたタブを変更または削除できません。 • ユーザにカスタム埋め込みタブの作成を許可しなくても、ユーザは定義されたタブを使用できます。

パラメータ	値	説明
ShowContactPictures	true false	<p>連絡先リストに連絡先画像を表示するかどうかを指定します。</p> <p>true</p> <p>連絡先リストに連絡先画像が表示されます。これがデフォルト値です。</p> <p>false</p> <p>連絡先リストに連絡先画像は表示されません。</p>
ShowOfflineContacts	true false	<p>連絡先リストにオフラインの連絡先を表示するかどうかを指定します。</p> <p>true</p> <p>連絡先リストにオフラインの連絡先が表示されます。これがデフォルト値です。</p> <p>false</p> <p>連絡先リストにオフラインの連絡先は表示されません。</p>
DockedWindowVisible	TRUE FALSE	<p>クライアント起動時にドック ウィンドウを表示するかどうかを指定します。</p> <p>true</p> <p>クライアント起動時にドック ウィンドウが表示されます。これがデフォルト値です。</p> <p>false</p> <p>クライアント起動時にドック ウィンドウは表示されません。</p>

パラメータ	値	説明
DockedWindowPosition	TopCenter TopLeft TopRight	<p>ユーザの画面でのドック ウィンドウの位置を設定します。</p> <p>TopCenter</p> <p>ドック ウィンドウの位置は画面の上部中央です。これがデフォルト値です。</p> <p>TopLeft</p> <p>ドック ウィンドウの位置は画面の左上です。</p> <p>TopRight</p> <p>ドック ウィンドウの位置は画面の右上です。</p>

関連トピック

[設定パラメータの概要, \(135 ページ\)](#)

電話パラメータ

次の表に、Phone要素内で指定できるパラメータを示します。

パラメータ	値	説明
DeviceAuthenticationPrimaryServer	ホスト名 IP アドレス FQDN	<p>ユーザが電話モードの展開で認証する Cisco Unified Communications Manager のプライマリ インスタンスのアドレスを指定します。値として次のいずれかを設定します。</p> <ul style="list-style-type: none"> • ホスト名 (<i>hostname</i>) • IP アドレス (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)
DeviceAuthenticationBackupServer	ホスト名 IP アドレス FQDN	<p>ユーザが電話モードの展開で認証する Cisco Unified Communications Manager のバックアップ インスタンスのアドレスを指定します。値として次のいずれかを設定します。</p> <ul style="list-style-type: none"> • ホスト名 (<i>hostname</i>) • IP アドレス (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)

パラメータ	値	説明
TftpServer1	ホスト名 IP アドレス FQDN	<p>デバイスコンフィギュレーションファイルを保存するプライマリ Cisco Unified Communications Manager TFTP サービスのアドレスを指定します。値として次のいずれかを設定します。</p> <ul style="list-style-type: none"> • ホスト名 (<i>hostname</i>) • IP アドレス (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>) <p>次の場合に限り、クライアント設定でこのパラメータを設定する必要があります。</p> <ul style="list-style-type: none"> • 電話モードのクライアントを配置します。 • デバイス設定用の TFTP サーバアドレスとクライアント設定用の TFTP サーバアドレスは異なります。 <p>インストール時に、クライアントコンフィギュレーションファイルが引数 TFTP を保存する TFTP サーバのアドレスを設定する必要があります。</p>
TftpServer2	ホスト名 IP アドレス FQDN	<p>セカンダリ Cisco Unified Communications Manager TFTP サービスのアドレスを指定します。</p> <p>このパラメータはオプションです。</p>
CtiServer1	ホスト名 IP アドレス FQDN	<p>プライマリ CTI サーバのアドレスを指定します。</p> <p>ユーザがデスクフォンデバイスを持っている場合、クライアントコンフィギュレーションで CTI サーバアドレスを指定する必要があります。</p>
CtiServer2	ホスト名 IP アドレス FQDN	<p>セカンダリ CTI サーバのアドレスを指定します。</p> <p>このパラメータはオプションです。</p>

パラメータ	値	説明
useCUCMGroupForCti	true false	<p>Cisco Unified CM グループが CTI サーバのロード バランシングを処理するかどうか指定します。 次のいずれかの値を設定します。</p> <p>true</p> <p>Cisco Unified CM グループが CTI サーバのロード バランシングを処理します。</p> <p>電話モードでの展開のみ、この値を設定する必要があります。 フル UC モードでは、プレゼンス サーバが自動的に CTI ロード バランシングを扱います。</p> <p>false</p> <p>Cisco Unified CM グループが、CTI ロード バランシングを処理しません。 これがデフォルト値です。</p>
CcmcipServer1	ホスト名 IP アドレス FQDN	<p>プライマリ CCMCIP サーバのアドレスを指定します。</p> <p>このパラメータは必須です。</p> <ul style="list-style-type: none"> • CCMCIP サーバのアドレスが TFTP サーバアドレスと同じでない場合のみ。 <p>CCMCIP サーバアドレスが TFTP サーバアドレスと同じ場合、クライアントは CCMCIP サーバに接続するために TFTP サーバアドレスを使用できます。</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager バージョン 8 での導入。 <p>Cisco Unified Communications Manager バージョン 9 以降の展開では、クライアントは、_cisco-uds SRV レコードをプロビジョニングする場合に、CCMCIP サーバを検出できます。</p>
CcmcipServer2	ホスト名 IP アドレス FQDN	<p>セカンダリ CCMCIP サーバのアドレスを指定します。</p> <p>このパラメータはオプションです。</p>

パラメータ	値	説明
Meeting_Server_Address	Cisco WebEx 会議サイトの URL	<p>ユーザにプライマリ Cisco WebEx 会議サイトの URL を指定します。</p> <p>クライアントは、[オプション (Options)] ウィンドウのユーザのホストアカウントで、この会議サイトを入力します。会議サイトにクレデンシャルが必要な場合、ユーザは自分のクレデンシャルを入力してホスト アカウントをセットアップし、自分の Cisco WebEx 会議にアクセスできます。</p> <p>重要 無効な会議サイトを指定すると、ユーザは、クライアント ユーザ インターフェイス内のいずれの会議サイトの追加または編集もできなくなります。</p> <p>このパラメータはオプションです。</p>
Meeting_Server_Address_Backup	Cisco WebEx 会議サイトの URL	<p>ユーザにセカンダリ Cisco WebEx 会議サイトの URL を指定します。</p> <p>このパラメータはオプションです。</p>
Meeting_Server_Address_Backup2	Cisco WebEx 会議サイトの URL	<p>ユーザにターシャリ Cisco WebEx 会議サイトの URL を指定します。</p> <p>このパラメータはオプションです。</p>

関連トピック

[設定パラメータの概要, \(135 ページ\)](#)

[TFTP サーバ アドレス, \(105 ページ\)](#)

ポリシー パラメータ

ポリシー パラメータにより、特定のクライアント機能を制御できます。

関連トピック

[設定パラメータの概要, \(135 ページ\)](#)

オンプレミス ポリシー

次の表は、オンプレミスの展開において、Policies要素内で指定できるパラメータについて示しています。

パラメータ	値	説明
Screen_Capture_Enabled	true false	<p>ユーザが画面キャプチャを取得できるかどうかを指定します。</p> <p>true</p> <p>ユーザは画面キャプチャを取得できます。これがデフォルト値です。</p> <p>false</p> <p>ユーザは画面キャプチャを取得できません。</p>
File_Transfer_Enabled	true false	<p>ユーザが他のユーザとファイルを交換できるかどうかを指定します。</p> <p>true</p> <p>ユーザは他のユーザとファイルを交換できます。これがデフォルト値です。</p> <p>false</p> <p>ユーザは他のユーザとファイルを交換できません。</p>
Disallowed_File_Transfer_Types	ファイル拡張子	<p>ユーザに対して、特定のファイルタイプの転送の制限をします。</p> <p>値としてセット ファイル拡張子を設定します（例：.exe）。</p> <p>複数のファイル拡張子を区切る際は、セミコロンを使用します（例：.exe;.msi;.rar;.zip）。</p>

共通のポリシー

オンプレミス展開とハイブリッドクラウドベース展開の両方において、Policies 要素内で指定できるパラメータを次の表で説明します。

パラメータ	値	説明
EnableVideo	true false	<p>ビデオ機能を有効または無効にします。</p> <p>true</p> <p>ユーザはビデオ コールを発信および受信できます。これがデフォルト値です。</p> <p>false</p> <p>ユーザはビデオ コールを発信または受信できません。</p>
InitialPhoneSelection	deskphone softphone	<p>クライアント初回起動時のユーザの電話タイプを設定します。初回起動後、ユーザは電話タイプを変更できます。クライアントは、ユーザ設定を保存し、以降の起動でその設定を使用します。</p> <p>deskphone</p> <p>通話にデスクフォンデバイスを使用します。</p> <p>softphone</p> <p>通話にソフトフォン（CSF）デバイスを使用します。これがデフォルト値です。</p> <p>クライアントは次の順序でデバイスを選択します。</p> <ol style="list-style-type: none"> 1 ソフトフォン デバイス 2 デスクフォン デバイス <p>ユーザにソフトフォンデバイスをプロビジョニングしない場合、クライアントはデスクフォンデバイスを自動的に選択します。</p>

パラメータ	値	説明
UserDefinedRemoteDestinations	true false	<p>ユーザは、クライアントインターフェイスを使用してリモート接続先を追加、編集、および削除できます。拡張機能と接続機能をプロビジョニングしてデフォルトの動作を変更するには、このパラメータを使用します。</p> <p>デフォルトでは、ユーザのデバイス リストに CTI リモートデバイスだけが含まれる場合、クライアントはユーザがリモート接続先を追加、編集、または削除できないようにします。これは、割り当てられた専用のリモートデバイスをユーザが変更できないようにするためです。ただし、ユーザのデバイス リストにソフトフォンデバイスまたはデスクフォンデバイスが含まれる場合、クライアントはユーザがリモート接続先を追加、編集、および削除できるようにします。</p> <p>true</p> <p>ユーザはリモート接続先を追加、編集、および削除できます。</p> <p>false</p> <p>ユーザはリモート接続先を追加、編集、および削除できません。これがデフォルト値です。</p>
enableLocalAddressBookSearch	true false	<p>ユーザは、ローカル Microsoft Outlook 連絡先を検索し、自分の連絡先リストに追加できます。</p> <p>true</p> <p>ユーザは、ローカル連絡先を検索し、自分の連絡先リストに追加できます。これがデフォルト値です。</p> <p>false</p> <p>ユーザは、ローカル連絡先を検索すること、または自分の連絡先リストに連絡先を追加することができません。</p>

パラメータ	値	説明
EnableAccessoriesManager	true false	<p>クライアントのアクセサリ API を有効にします。この API は、ヘッドセットなどのデバイスのコール管理機能を有効にするプラグインをアクセサリのベンダーが作成できるようにします。</p> <p>true</p> <p>アクセサリ API を有効にします。これがデフォルト値です。</p> <p>false</p> <p>アクセサリ API を無効にします。</p>
BlockAccessoriesManagerPlugins	プラグイン ライブラリ	<p>Jabra や Logitech といったサードパーティベンダーから特定のアクセサリ マネージャプラグインを無効にします。プラグイン DLL ファイルの名前を値として設定します。複数の値を区切るにはカンマを使用します。たとえば、Microsoft Windows では次のようになります。</p> <pre><BlockAccessoriesManagerPlugins> JabraJabberPlugin.dll,lucpcisco.dll </BlockAccessoriesManagerPlugins></pre> <p>デフォルト値はありません。</p>
ForceFontSmoothing	true false	<p>クライアントがスムーズテキストにアンチエイリアシングを適用するかどうかを指定します。</p> <p>true</p> <p>クライアントは、テキストにアンチエイリアスを適用します。これがデフォルト値です。</p> <p>false</p> <p>オペレーティング システムがテキストにアンチエイリアシングを適用します。</p>

パラメータ	値	説明
EnableBFCPVideoDesktopShare	true false	<p>BFCP ビデオ デスクトップ共有機能を有効にします。</p> <p>true</p> <p>クライアントで BFCP ビデオ デスクトップ共有を有効にします。これがデフォルト値です。</p> <p>false</p> <p>BFCP ビデオデスクトップ共有を無効にします。</p> <p>(注) BFCP ビデオ デスクトップ共有をサーバで次のように有効にします。</p> <ul style="list-style-type: none"> • Cisco Unified Communications Manager バージョン 8.x 以前では、[BFCP を使用するプレゼンテーション共有を許可 (Allow Presentation Sharing using BFCP)] チェックボックスを選択する必要があります。 • Cisco Unified Communications Manager バージョン 9.x 以降では、BFCP ビデオ デスクトップ共有はデフォルトで有効です。
Meetings_Enabled	true false	<p>クライアントの会議機能とユーザインターフェイスを有効にします。</p> <p>true</p> <p>会議機能とユーザ インターフェイスを有効にします。これがデフォルト値です。</p> <p>false</p> <p>会議機能とユーザ インターフェイスを無効にします。</p>

パラメータ	値	説明
Telephony_Enabled	true false	<p>クライアントの音声/ビデオ機能とユーザ インターフェイスを有効にします。</p> <p>true</p> <p>音声/ビデオ機能とユーザ インターフェイスを有効にします。これがデフォルト値です。</p> <p>false</p> <p>音声/ビデオ機能とユーザ インターフェイスを無効にします。</p>
Voicemail_Enabled	true false	<p>クライアントのボイスメール機能とユーザ インターフェイスを有効にします。</p> <p>true</p> <p>ボイスメール機能とユーザ インターフェイスを有効にします。これがデフォルト値です。</p> <p>false</p> <p>ボイスメール機能とユーザ インターフェイスを無効にします。</p>
EnableTelProtocolHandler	true false	<p>クライアントを tel: URI のプロトコルハンドラとして登録するかどうかを指定します。</p> <p>true</p> <p>クライアントは tel: URI のプロトコルハンドラとして登録されます。これがデフォルト値です。</p> <p>false</p> <p>クライアントは tel: URI のプロトコルハンドラとして登録されません。</p>

パラメータ	値	説明
EnableSaveChatToFile	true false	<p>ユーザは、HTML ファイルとしてシステムにチャットを保存できます。</p> <p>true</p> <p>ユーザは、ファイルにチャットを保存できます。これがデフォルト値です。</p> <p>false</p> <p>ユーザは、ファイルにチャットを保存できません。</p>
EnableSIPURIDialling	true false	<p>Cisco Jabber で URI ダイヤルを有効にし、ユーザが URI を使用してコールを発信できるようにします。</p> <p>true</p> <p>ユーザは、URI でコールを発信できます。</p> <p>false</p> <p>ユーザは、URI でコールを発信できません。これがデフォルト値です。</p>

パラメータ	値	説明
DirectoryURI	ディレクトリ属性	<p>ユーザの SIP URI を保持するディレクトリ属性を指定します。</p> <p>オンプレミス展開</p> <p>値として次のいずれかを設定します。</p> <ul style="list-style-type: none"> • mail • msRTCSIP-PrimaryUserAddress <p>クラウドベース展開</p> <p>値として次のいずれかを設定します。</p> <ul style="list-style-type: none"> • mail • imaddress • workphone • homephone • mobilephone <p>メール属性がデフォルトで使用されます。</p> <p>重要 指定する値が Cisco Unified Communications Manager または Cisco WebEx 管理ツールのユーザのディレクトリ URI 設定に一致する必要があります。</p>

パラメータ	値	説明
ForceC2XDirectoryResolution	true false	<p>ユーザが click-to-x アクションを実行したときに、連絡先情報を解決するためにクライアントがディレクトリのクエリーを実行するかどうかを指定します。</p> <p>true</p> <p>ユーザが click-to-x アクションを実行したときに、クライアントはディレクトリのクエリーを実行します。これがデフォルト値です。</p> <p>false</p> <p>click-to-x アクションのために、クライアントはディレクトリのクエリーを実行しません。</p> <p>(注) このパラメータは、ユーザが Expressway Mobile and Remote Access を介して社内ネットワークに接続する場合には適用されません。この場合、UDS が連絡先を解決し、クライアントはディレクトリのクエリーを実行できません。</p>

パラメータ	値	説明
ServiceDiscoveryExcludedServices	WEBEX CUCM CUP	<p>サービスディスカバリから特定のサービスを除外するかどうかを指定します。</p> <p>WEBEX</p> <p>この値を設定すると、クライアントは次のように動作します。</p> <ul style="list-style-type: none"> • CAS 検索を実行しません。 • <code>_cisco-uds</code>、<code>_cuplogin</code>、<code>_collab-edge</code> を検索します。 <p>CUCM</p> <p>この値を設定すると、クライアントは次のように動作します。</p> <ul style="list-style-type: none"> • <code>_cisco_uds</code> を検索しません。 • <code>_cuplogin</code>、<code>_collab-edge</code> を検索します。 <p>CUP</p> <p>この値を設定すると、クライアントは次のように動作します。</p> <ul style="list-style-type: none"> • <code>_cuplogin</code> を検索しません。 • <code>_cisco-uds_collab-edge</code> を検索します。 <p>カンマで区切った複数の値を指定して、複数のサービスを除外できます。次に例を示します。</p> <pre><ServiceDiscoveryExcludedServices> WEBEX,CUCM </ServiceDiscoveryExcludedServices></pre>

パラメータ	値	説明
VoiceServicesDomain	FQDN	<p><code>_collab-edge</code> と <code>_cisco-uds</code> の DNS SRV レコードを設定する DNS ドメインを表す完全修飾ドメイン名を指定します。</p> <p>例 :</p> <p>次の DNS SRV レコードがあるとします。</p> <ul style="list-style-type: none"> <code>_collab-edge._tls.voice.example.com</code> <code>_cisco-uds._tcp.voice.example.com</code> <p><code>VoiceServicesDomain</code> の値は <code>voice.example.com</code> になります。</p>

Cisco WebEx ポリシー

インスタントメッセージとプレゼンス機能に Cisco WebEx Messenger サービスを使用する場合、Cisco WebEx 管理ツールによってクライアントのポリシーを設定できます。使用可能なポリシーと説明のリストについては、*Using policy actions available in Cisco WebEx* を参照してください。

関連トピック

[Using policy actions available in Cisco WebEx](#)

[Using policy actions available in Cisco WebEx](#)

プレゼンス パラメータ

次の表に、Presence要素内で指定できるパラメータを示します。

パラメータ	値	説明
LoginResource	multiResource wbxconnect	<p>複数のクライアント インスタンスへのユーザ ログインを制御します。</p> <p>multiResource</p> <p>ユーザは、クライアントの複数インスタンスに同時にログインできます。これがデフォルト値です。</p> <p>wbxconnect</p> <p>ユーザは一度に 1 つのクライアントのインスタンスにログインできます。</p> <p>クライアントはユーザの JID に wbxconnect サフィックスを付加します。ユーザは、wbxconnect サフィックスを使用する他の Cisco Jabber クライアントにログインできません。</p>
PresenceServerAddress	ホスト名 IP アドレス FQDN	<p>オンプレミス展開にプレゼンス サーバのアドレスを指定します。値として次のいずれかを設定します。</p> <ul style="list-style-type: none"> • ホスト名 (<i>hostname</i>) • IP アドレス (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)
PresenceServerURL	CAS の URL	<p>Cisco WebEx Messenger サービスに中央認証サービス (CAS) の URL を指定します。次に、値として設定できる URL の例を示します。</p> <p><code>https://loginp.webexconnect.com/cas/sso/ex_org/orgadmin.app</code></p>

関連トピック

[設定パラメータの概要](#), (135 ページ)

サービス クレデンシャル パラメータ

ユーザが特定サービスで認証を受ける必要をなくすために、サービス クレデンシャル パラメータを指定できます。

ボイスメール サービスのクレデンシャル

Voicemail 要素内で、ボイスメール サービスのクレデンシャルを設定するために、次のパラメータを指定できます。

パラメータ	値	説明
VoiceMailService_UseCredentialsFrom	phone	<p>ボイスメール サービスにアクセスするために、クライアントが電話サービスのクレデンシャルを使用することを指定します。</p> <p>ユーザの電話サービスのクレデンシャルが、ボイスメール サービスのクレデンシャルに一致することを確認します。この設定を行うと、ユーザはクライアントインターフェイスでボイスメールサービスのクレデンシャルを指定できません。</p> <p>デフォルトで、このパラメータは設定されていません。</p> <p>次の展開でのみ、このパラメータを設定する必要があります。</p> <ul style="list-style-type: none"> ハイブリッドクラウドベースの展開。 電話モードの導入。 <p>オンプレミスの展開では、プレゼンスサーバのボイスメール サービスのクレデンシャルのソースを設定する必要があります。</p>

以下は、ボイスメールサービスのクレデンシャル パラメータの例です。

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Voicemail>
    <VoicemailService_UseCredentialsFrom>phone</VoicemailService_UseCredentialsFrom>
  </Voicemail>
</config>
```

関連トピック

[設定パラメータの概要, \(135 ページ\)](#)

[ボイスメール パラメータ, \(161 ページ\)](#)

ボイスメール パラメータ

次の表で、Voicemail 要素内で指定できるボイスメール サービス設定パラメータについて説明します。

キー	値	説明
VVM_Mailstore_Server_0	ホスト名 IP アドレス FQDN	ボイスメールサーバのアドレスを指定します。 値として次のいずれかを設定します。 <ul style="list-style-type: none"> • ホスト名 (<i>hostname</i>) • IP アドレス (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)

関連トピック

[設定パラメータの概要, \(135 ページ\)](#)

[サービス クレデンシャル パラメータ, \(160 ページ\)](#)

自動更新の設定

自動更新を有効にするには、最新バージョン（HTTP サーバのインストールパッケージの URL を含む）の情報が含まれている XML ファイルを作成します。ユーザがサインインしたとき、コンピュータをスリープモードから再開したとき、または[ヘルプ (Help)]メニューから手動更新要求を実行したとき、クライアントは XML ファイルを取得します。



(注) インスタント メッセージングとプレゼンス機能のサービスに Cisco WebEx Messenger を使用する場合、Cisco WebEx 管理ツールを使用して、自動更新の設定をします。

はじめる前に

- HTTP サーバ をインストールおよび設定し、XML ファイルとインストール パッケージをホストします。
 - ワークステーションにソフトウェアアップデートをインストールできる権限がユーザにあることを確認します。
- 一部のケースでは、ユーザがワークステーションの管理権限を所有していない場合、Microsoft Windows はアップデートのインストールを停止します。

手順

- ステップ 1** ご使用の HTTP サーバでアップデート インストール プログラムをホストします。
- ステップ 2** 任意のテキスト エディタを使用して更新の XML ファイルを作成します。

自動更新用の XML ファイルは次のような構造となっています。

```
<JabberUpdate>
  <App name="client ID">
    <LatestBuildNum>value</LatestBuildNum>
    <LatestVersion>value</LatestVersion>
    <Message><![CDATA[your HTML]]></Message>
    <DownloadURL>value</DownloadURL>
  </App>
</JabberUpdate>
```

ステップ 3 XML で次のように値を指定します。

name

次の ID を、アプリケーションの要素の名前属性の値として指定します。

JabberWin

更新は Cisco Jabber for Windows に適用されます。

LatestBuildNum

アップデートのビルド番号。

LatestVersion

アップデートのバージョン番号。

Message

次の形式の HTML :

```
<![CDATA[your_html]]>
```

DownloadURL

HTTP サーバ上のインストール パッケージの URL。

例 :

以下は自動更新の XML の例です。

```
<JabberUpdate>
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.x</LatestVersion>
  <Message><![CDATA[This new version of Cisco Jabber lets you do the
following:<b><i>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
more information click <a target=" blank"
href="http://cisco.com/go/jabber">here</a>.</i>]]></Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>
</JabberUpdate>
```

ステップ 4 更新の XML ファイルを保存して閉じます。

ステップ 5 HTTP サーバ上で更新の XML ファイルをホストします。

ステップ 6 設定ファイルの UpdateUrl パラメータの値として更新の XML ファイルを指定します。

問題レポートの設定

問題レポートをセットアップすると、ユーザはクライアントの使用中に発生した問題の概要を送信できます。次のように、問題レポートを送信する方法は2つあります。

- ユーザは、クライアント インターフェイスを通じて問題レポートを直接送信します。
- 問題レポートをローカルに保存し、後でアップロードする。

クライアントは問題レポートを提出するために HTTP POST 方式を使用します。POST 要求を受け入れるカスタム スクリプトを作成し、設定パラメータとして HTTP サーバ上のスクリプトの URL を指定します。ユーザは問題レポートをローカルに保存できるため、ユーザが問題レポートをアップロードできるようにするフォームを含む HTML ページを作成する必要もあります。

はじめる前に

環境の準備を行うには、次の手順を実行します。

- 1 HTTP サーバ をインストールおよび設定します。
- 2 HTTP POST 要求を受け入れるカスタム スクリプトを作成します。
- 3 ローカルで保存された問題のレポートをアップロードできるように HTML ページを作成します。HTML ページには、.ZIP アーカイブとして保存された問題レポートを受け入れ、カスタム スクリプトを使用して問題レポートを送信するアクションが含まれているフォームがあります。

次に、問題レポートを受け入れるフォームの例を示します。

```
<form name="uploadPrt" action="http://server_name.com/scripts/UploadPrt.php" method="post"
  enctype="multipart/form-data">
  <input type="file" name="zipFileName" id="zipFileName" /><br />
  <input type="submit" name="submitBtn" id="submitBtn" value="Upload File" />
</form>
```

手順

-
- | | |
|--------|--|
| ステップ 1 | HTTP サーバ上でカスタム スクリプトをホストします。 |
| ステップ 2 | 設定ファイルの PrtLogServerUrl パラメータの値としてスクリプトの URL を指定します。 |
-

カスタム埋め込みタブ

カスタム埋め込みタブは、クライアント インターフェイスの HTML コンテンツを表示します。Cisco Jabber のカスタム埋め込みタブ定義を作成する方法について説明します。

関連トピック

[カスタム埋め込みタブの作成](#), (227 ページ)

カスタム埋め込みタブの定義

次の XML スニペットは、カスタム埋め込みタブ定義の構造を示します。

```
<jabber-plugin-config>
  <browser-plugin>
    <page refresh="" preload="">
      <tooltip></tooltip>
      <icon></icon>
      <url></url>
    </page>
  </browser-plugin>
</jabber-plugin-config>
```

次の表は、カスタム埋め込みタブ定義のパラメータの説明です。

パラメータ	値	説明
browser-plugin	カスタムタブのすべての定義	カスタム埋め込みタブのすべての定義が含まれます。
page	カスタム タブの 1 つの定義	1 つのカスタム埋め込みタブ定義が含まれます。
refresh	true false	<p>コンテンツを更新するタイミングを制御します。</p> <p>true</p> <p>ユーザがタブを選択するたびにコンテンツの更新をします。</p> <p>false</p> <p>コンテンツは、ユーザがクライアントを再起動またはログインすると更新されます。これがデフォルト値です。</p> <p>このパラメータはオプションで、page 要素の属性です。</p>

パラメータ	値	説明
preload	true false	<p>コンテンツをロードするタイミングを制御します。</p> <p>true</p> <p>クライアントが起動したときにコンテンツをロードします。</p> <p>false</p> <p>ユーザがタブを選択するときにコンテンツをロードします。これがデフォルト値です。</p> <p>このパラメータはオプションで、page 要素の属性です。</p>
tooltip	Unicode 文字の文字列	<p>カスタム埋め込みタブのマウス オーバーテキストを定義します。</p> <p>このパラメータはオプションです。</p>
icon	URL	<p>タブのアイコンを指定します。次のようにローカルまたはホスティングされたアイコンを指定できます。</p> <p>ローカル アイコン</p> <p>次のように URL を入力します :</p> <p><code>file://file_path/icon_name</code></p> <p>ホステッド アイコン</p> <p>次のように URL を入力します :</p> <p><code>http://path/icon_name</code></p> <p>JPG、.PNG、.GIF 形式を含め、Microsoft Internet Explorer がレンダリングできるアイコンを使用できます。</p> <p>このパラメータはオプションです。アイコンが指定されていない場合、クライアントは HTML ページからファビコンをロードします。ファビコンが使用できない場合、クライアントはデフォルトのアイコンをロードします。</p>

パラメータ	値	説明
url	URL	<p>埋め込みタブのコンテンツが存在する URL を指定します。</p> <p>クライアントは、埋め込みタブのコンテンツを表示するために、Internet Explorer レンダリングエンジンを使用します。したがって、Internet Explorer がサポートするコンテンツを指定できます。</p> <p>(注) Cisco Jabber for Windows では、Internet Explorer バージョン 9 またはそれ以前のバージョンをサポートしています。Internet Explorer バージョン 9 以降がワークステーションにある場合、バージョン 9 モードを使用します。</p> <p>このパラメータは必須です。</p>

ユーザのカスタム タブ

ユーザは、クライアントユーザインターフェイスを使用して、独自のカスタム埋め込みタブを作成できます。

ユーザは、カスタム埋め込みタブを作成することが可能である必要があります。次の手順で、設定ファイルの AllowUserCustomTabs パラメータの値を true に設定します。

```
<Options>
  <AllowUserCustomTabs>true</AllowUserCustomTabs>
</Options>
```



(注) ユーザのカスタム埋め込みタブはデフォルトで無効です。

カスタム アイコン

カスタム埋め込みタブのアイコンには、1 つのイメージ ファイル内の各状態に対して 10 個のフレームがあります。



(注) 最適な結果を得るには、カスタムアイコンは、次のガイドラインに準拠する必要があります。

- 寸法 : 20 x 20 ピクセル
- 各フレーム間に 1 ピクセルのパディング 1 ピクセルのパディングにより、実際に使用できるアイコンの領域は 19 x 19 ピクセルになります。
- トランスペアレント背景
- PNG ファイル形式

アイコンの各フレームは、次の状態を示します。

- 1 標準
- 2 押されている
- 3 ホバー
- 4 無効
- 5 フォーカス済み
- 6 選択済みおよび標準
- 7 選択済みおよび押されている
- 8 選択済みおよびホバー
- 9 選択済みおよびディセーブル
- 10 選択済みおよびフォーカス済み

アイコンの例を次に示します。



上記アイコンの各フレーム用 16 進数のカラーコードを次に示します。 アピアランスの整合性をとるために、アイコンにこれらのカラーコードを使用します。

- 1 #4f6b7c
- 2 #2aa6c7
- 3 #99b5c7
- 4 #FFFFFF
- 5 #19bae3
- 6 #19bae3
- 7 #2aa6c7
- 8 #99b5c7
- 9 #FFFFFF
- 10 #19bae3

カスタム タブからのチャットおよびコール

カスタム埋め込みタブからチャットおよびコールを開始するために、プロトコルハンドラを使用できます。

XMPP: または IM: プロトコルを使用して、チャットを開始します。

TEL: プロトコルハンドラを使用して、音声およびビデオ コールを開始します。

関連トピック

[プロトコルハンドラ](#), (29 ページ)

UserID トークン

`${UserID}` トークンを url パラメータの値の一部として指定できます。ユーザがサインインすると、クライアントにより、`${UserID}` トークンがログインしたユーザのユーザ名に置き換えられます。



ヒント

また、クエリー文字列に `${UserID}` トークンを指定することもできます (例: `www.cisco.com/mywebapp.op?url=${UserID}`)。

次は、`${UserID}` トークンの使用方法の例です。

- 1 カスタム埋め込みタブで次の内容を指定します。

```
<url>www.cisco.com/${UserID}/profile</url>
```

- 2 Mary Smith がログインします。 のユーザ名は `msmith` です。

- 3 クライアントは、Mary のユーザ名に次のように `${UserID}` トークンに置き換えます。

```
<url>www.cisco.com/msmith/profile</url>
```

JavaScript 通知

カスタム埋め込みタブに JavaScript 通知を実装できます。このトピックでは、JavaScript 通知用にクライアントが提供するメソッドについて説明します。また、通知のテストに使用できる JavaScript フォームの例についても説明します。非同期サーバコールに対する JavaScript 通知の実装方法と他のカスタム実装に関する説明は、このマニュアルでは取り扱いません。詳細については、該当する JavaScript のマニュアルを参照してください。

通知メソッド

Cisco Jabber には、JavaScript 通知の次のメソッドを提供するインターフェイスが含まれています。

SetNotificationBadge

JavaScript でクライアントからこのメソッドを呼び出します。このメソッドは、次のいずれかの文字列値を取得します。

- 空
空の値により、既存の通知バッジが削除されます。
- 0 ～ 999 の数字
- 2 桁の英数字の組み合わせなど（例：A1）

onPageSelected

クライアントは、ユーザがカスタム埋め込みタブを選択するとこのメソッドを呼び出します。

onPageDeselected

クライアントは、ユーザが別のタブを選択するときこのメソッドを呼び出します。

JavaScript の例

次に、1 ～ 999 の数字を入力できるフォームを表示するために JavaScript を使用する HTML の例を示します。

```
<html>
<head>
  <script type="text/javascript">
    function onPageSelected()
    {
      window.external.SetNotificationBadge("");
    }
    function onPageDeselected()
    {
      window.external.SetNotificationBadge("");
    }
    function addBadge()
    {
      var cell = document.getElementById("badgeid");
      window.external.SetNotificationBadge(cell.value);
    }
  </script>
</head>
<body>
  <form onsubmit="addBadge()" >
    Badge: <input type="text" name="value" id="badgeid"/><br />
    <input type="submit" value="Submit">
  </form>
</body>
</html>
```

この例の JavaScript フォームをテストするには、前述の例を HTML ページにコピーしてから、そのページをカスタム埋め込みタブとして指定します。

カスタム タブでのコール イベントの表示

カスタム タブでのコール イベントの表示するために、次の JavaScript 関数を使用できます。

OnTelephonyConversationStateChanged

テレフォニー サービスの API により、クライアントはカスタム埋め込みタブでコール イベントを表示することができます。カスタム タブは、OnTelephonyConversationStateChanged の JavaScript 関数を実行できます。クライアントは、テレフォニー会話の状態が変化するたびに、この機能をコールします。この機能により、クライアントがコール イベントを取得するために解析する JSON の文字列を受け入れます。

次のスニペットは、コール イベントを保持する JSON を示します。

```
{
  "conversationId": string,
  "acceptanceState": "Pending" | "Accepted" | "Rejected",
  "state": "Started" | "Ending" | "Ended",
  "callType": "Missed" | "Placed" | "Received" | "Passive" | "Unknown",
  "remoteParticipants": [{participant1}, {participant2}, ..., {participantN}],
  "localParticipant": {
  }
}
```

JSON の各参加オブジェクトは、次のプロパティを有します。

```
{
  "voiceMediaDisplayName": "<displayName>",
  "voiceMediaNumber": "<phoneNumber>",
  "translatedNumber": "<phoneNumber>",
  "voiceMediaPhoneType": "Business" | "Home" | "Mobile" | "Other" | "Unknown",
  "voiceMediaState": "Active" | "Inactive" | "Pending" | "Passive" | "Unknown",
}
```

次は、カスタム埋め込みタブでこの機能を実行する例です。この例では、state および acceptanceState プロパティの値を取得し、カスタム タブで示しています。

```
function OnTelephonyConversationStateChanged(json) {
  console.log("OnTelephonyConversationStateChanged");

  try {
    var conversation = JSON.parse(json);

    console.log("conversation id=" + conversation.conversationId);
    console.log("conversation state=" + conversation.state);
    console.log("conversation acceptanceState=" + conversation.acceptanceState);
    console.log("conversation callType=" + conversation.callType);
  }
  catch(e) {
    console.log("cannot parse conversation:" + e.message);
  }
}
```

次は、すべての可能なフィールドでこの機能を実行する例です。

```
function OnTelephonyConversationStateChanged(json) {
  console.log("OnTelephonyConversationStateChanged");

  try {
    var conversation = JSON.parse(json);

    console.log("conversation state=" + conversation.state);
    console.log("conversation acceptanceState=" + conversation.acceptanceState);
    console.log("conversation callType=" + conversation.callType);

    for (var i=0; i<conversation.remoteParticipants.length; i++) {
      console.log("conversation remoteParticipants[" + i + "]=");
      console.log("voiceMediaDisplayName=" +
conversation.remoteParticipants[i].voiceMediaDisplayName);
      console.log("voiceMediaNumber=" +
conversation.remoteParticipants[i].voiceMediaNumber);
    }
  }
}
```

```

        console.log("translatedNumber=" +
conversation.remoteParticipants[i].translatedNumber);
        console.log("voiceMediaPhoneType=" +
conversation.remoteParticipants[i].voiceMediaPhoneType);
        console.log("voiceMediaState=" +
conversation.remoteParticipants[i].voiceMediaState);
    }

    console.log("conversation localParticipant=");
    console.log("    voiceMediaDisplayName=" +
conversation.localParticipant.voiceMediaDisplayName);
    console.log("    voiceMediaNumber=" + conversation.localParticipant.voiceMediaNumber);

    console.log("    translatedNumber=" + conversation.localParticipant.translatedNumber);

    console.log("    voiceMediaPhoneType=" +
conversation.localParticipant.voiceMediaPhoneType);
    console.log("    voiceMediaState=" + conversation.localParticipant.voiceMediaState);
    }
    catch(e) {
        console.log("cannot parse conversation:" + e.message);
    }
}

```

カスタム埋め込みタブの例

次は、1 つの埋め込みタブを持つコンフィギュレーション ファイルの例です。

```

<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="true" preload="true">
          <tooltip>Cisco</tooltip>
          <icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
          <url>www.cisco.com</url>
        </page>
      </browser-plugin>
    </jabber-plugin-config>
  </Client>
</config>

```




第 8 章

ディレクトリ ソースとの統合

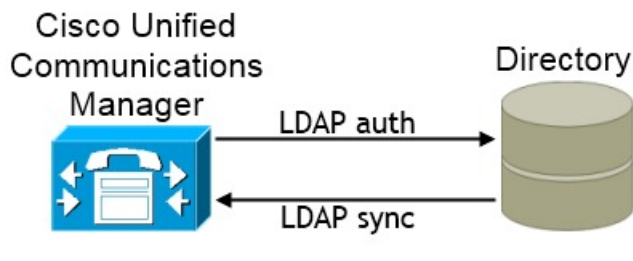
Cisco Jabber は、オンプレミスでの展開のディレクトリ ソースと統合し、連絡先をクエリーし、解決します。なぜディレクトリ ソースと Cisco Unified Communications Manager 間の同期と認証を有効にする必要があるのかを説明します。どのように特定の発信元とディレクトリ統合が連携するかを理解します。ディレクトリ統合のクライアントを設定する必要があることを確認します。特定の統合シナリオの設定例を検索します。

- [ディレクトリの同期化および認証の設定, 173 ページ](#)
- [発信元, 176 ページ](#)
- [ディレクトリ統合のためのクライアント設定, 182 ページ](#)
- [フェデレーション, 218 ページ](#)

ディレクトリの同期化および認証の設定

オンプレミス展開を設定するときは、次の両方を実行するように Cisco Unified Communications Manager を設定する必要があります。

- ディレクトリ サーバと同期する。
- ディレクトリ サーバで認証する。



ディレクトリ サーバと同期することで、連絡先データはディレクトリから Cisco Unified Communications Manager に複製されます。

ディレクトリ サーバで認証を有効にすることで、クライアントからのディレクトリ サーバに Cisco Unified Communications Manager プロキシ認証を可能になります。このように、ユーザは、Cisco Unified Communications Manager や既存のサーバではなく、ディレクトリ サーバで認証を行います。

関連トピック

[「Configuring Cisco Unified Communications Manager Directory Integration」
サーバセットアップ ガイド](#)

ディレクトリ サーバとの同期

ディレクトリ サーバとの同期により、ディレクトリ サーバ内の連絡先データが Cisco Unified Communications Manager に複製されます。

同期の有効化

ディレクトリ サーバと同期するための最初の手順は、Cisco Unified Communications Manager で同期を有効にすることです。

手順

-
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
 - ステップ 2** [システム (System)] > [LDAP] > [LDAP システム (LDAP System)] を選択します。
[LDAP システムの設定 (LDAP System Configuration)] ウィンドウが開きます。
 - ステップ 3** [LDAP システム情報 (LDAP System Information)] セクションに移動します。
 - ステップ 4** [LDAP サーバからの同期を有効にする (Enable Synchronizing from LDAP Server)] を選択します。
 - ステップ 5** [LDAP サーバタイプ (LDAP Server Type)] ドロップダウン リストから、データの同期元となるディレクトリ サーバのタイプを選択します。
-

次の作業

ユーザ ID の LDAP 属性を指定します。

ユーザ ID の LDAP 属性の指定

ディレクトリのソースから Cisco Unified Communications Manager に同期する場合、ディレクトリの属性からユーザ ID を入力できます。ユーザ ID を保持するデフォルトの属性は sAMAccountName です。

手順

-
- ステップ 1** [LDAP システムの設定 (LDAP System Configuration)] ウィンドウで [ユーザ ID 用 LDAP 属性 (LDAP Attribute for User ID)] ドロップダウン リストを探します。
- ステップ 2** 適切なユーザ ID の属性を指定し、[保存 (Save)] を選択します。
- 重要** ユーザ ID の属性が sAMAccountName 以外で、Cisco Unified Communications Manager IM and Presence Service のデフォルトの IM アドレス スキームを使用している場合、次のようにクライアント設定の UserAccountName パラメータの値として、属性を指定する必要があります。
- ```
<UserAccountName>attribute-name</UserAccountName>
```
- 設定で属性を指定せず、属性が sAMAccountName 以外の場合、クライアントはディレクトリ内の連絡先を解決できません。この結果、ユーザはプレゼンスを取得せず、インスタントメッセージを送信または受信できません。
- 

## 同期の実行

ディレクトリサーバを追加し、必要なパラメータを指定した後、Cisco Unified Communications Manager をディレクトリサーバと同期できます。

### はじめる前に

環境にプレゼンスサーバを含めた場合、ディレクトリサーバと同期させる前に、次の機能サービスがアクティブであり、起動できることを保証する必要があります。

- Cisco Unified Presence: Cisco UP Sync Agent
- Cisco Unified Communications Manager IM and Presence Service: Cisco Sync Agent

このサービスにより、データはプレゼンスサーバと Cisco Unified Communications Manager 間で同期が維持されます。ディレクトリサーバと同期を実行すると、Cisco Unified Communications Manager はプレゼンスサーバとデータを同期します。ただし、Cisco Sync Agent サービスがアクティブであり、起動できる必要があります。

## 手順

- 
- ステップ 1** [システム (System)] > [LDAP] > [LDAP ディレクトリ (LDAP Directory)] を選択します。
- ステップ 2** [新規追加 (Add New)] を選択します。  
[LDAP ディレクトリ (LDAP Directory)] ウィンドウが開きます。
- ステップ 3** [LDAP ディレクトリ (LDAP Directory)] ウィンドウで必要な詳細情報を指定します。  
指定できる値およびフォーマットの詳細については、『Cisco Unified Communications Manager Administration Guide』を参照してください。

**ステップ 4** [保存 (Save) ] を選択します。

**ステップ 5** [完全同期を今すぐ実施 (Perform Full Sync Now) ] を選択します。

(注) 同期プロセスの完了までに要する時間は、ディレクトリ内のユーザの数によって異なります。ユーザ数が数千にもなる大規模なディレクトリの同期を実施する場合、そのプロセスにはある程度の時間がかかると予想されます。

---

ディレクトリ サーバのユーザ データは、Cisco Unified Communications Manager データベースに同期されます。Cisco Unified Communications Manager は、その後、プレゼンス サーバデータベースにユーザ データを同期します。

## ディレクトリ サーバでの認証

ディレクトリ サーバで認証するために、Cisco Unified Communications Manager を設定する必要があります。ユーザがクライアントにログインすると、プレゼンス サーバはその認証を Cisco Unified Communications Manager にルーティングします。Cisco Unified Communications Manager は、その後、その認証をディレクトリ サーバに委任します。

### 手順

---

**ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration) ] インターフェイスを開きます。

**ステップ 2** [システム (System) ] > [LDAP] > [LDAP 認証 (LDAP Authentication) ] を選択します。

**ステップ 3** [エンドユーザ用 LDAP 認証の使用 (Use LDAP Authentication for End Users) ] を選択します。

**ステップ 4** 必要に応じて、LDAP クレデンシャルとユーザ検索ベースを指定します。

[LDAP 認証 (LDAP Authentication) ] ウィンドウのフィールドの詳細については、『Cisco Unified Communications Manager Administration Guide』を参照してください。

**ステップ 5** [保存 (Save) ] を選択します。

---

## 発信元

オンプレミスの展開では、クライアントはユーザ情報のディレクトリ ルックアップを解決するために、発信元を要求します。発信元として、次を使用できます。

### 拡張ディレクトリ統合

拡張ディレクトリ統合 (EDI) は、LDAP ベースの発信元です。

### Cisco Unified Communications Manager User Data Service

Cisco Unified Communications Manager User Data Service (UDS) は、Cisco Unified Communications Manager の発信元です。

UDS は連絡先の解決に次の状況で使用されます。

- クライアント コンフィギュレーション ファイルに `DirectoryServerType` パラメータを設定し “UDS” を使用させる場合。

この設定では、企業のファイアウォールの内側または外側の場合に、クライアントは連絡先の解決に UDS を使用します。

- Expressway Mobile and Remote Access を導入した場合。

この設定では、企業のファイアウォールの内側または外側の場合に、クライアントは連絡先の解決に自動で UDS を使用します。



(注) Cisco Jabber は、次の Cisco Unified Communications Manager バージョンを使用して UDS をサポートします。

- Cisco Unified Communications Manager Version 9.1(2) 以降 (COP ファイル `cmterm-cucm-uds-912-5.cop.sgn` を使用)。
- Cisco Unified Communications Manager Version 10.0(1)。COP ファイルは必要ありません。

ご使用の Cisco Unified Communications Manager ノードがサポートする Cisco Jabber クライアントの最大数の約 50 % を展開できます。

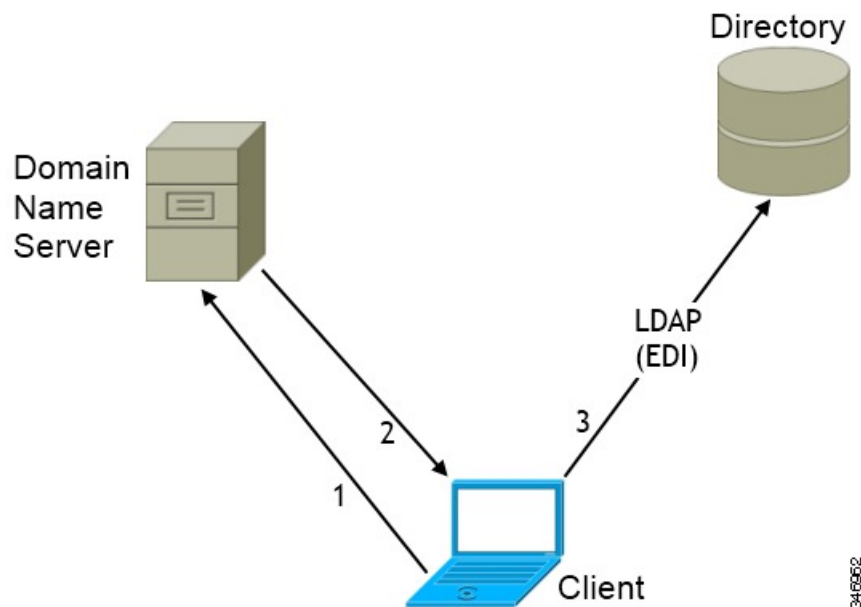
たとえば、Cisco Unified Communications Manager ノードが LDAP ベースのコンタクトソースを使用して 10,000 の Cisco Jabber クライアントをサポート可能な場合、同じノードは UDS をコンタクトソースとして使用して 5,000 の Cisco Jabber クライアントをサポートできます。

## 拡張ディレクトリ統合

EDI は、ディレクトリ サービスから連絡先データを取得するためにネイティブ Microsoft Windows API を使用します。

EDI でのオンプレミス展開のデフォルト設定は次のようになります。

- Cisco Jabber は、発信元として Active Directory と統合します。
- Cisco Jabber は、自動的に グローバル カタログ を検出し、接続します。



上記の図では、クライアントは次のことをデフォルトで行います。

- 1 ワークステーションから DNS ドメインを取得し、グローバルカタログの SRV レコードを検索します。
- 2 SRV レコードから グローバルカタログのアドレスを取得します。
- 3 ユーザのクレデンシャルでログインした グローバルカタログで接続します。

## ドメイン名検索

Cisco Jabber for Windows は、クライアントワークステーションの USERDNSDOMAIN 環境変数から完全修飾 DNS ドメインを取得します。

クライアントが DNS ドメインを取得したら、ドメインネームサーバを見つけ、SRV レコードを取得できます。

場合によっては、USERDNSDOMAIN 環境変数の値は、フォレスト全体のドメインに対応する DNS ドメインに解決されません。たとえば、組織がサブドメインまたはリソースのドメインを使用する場合です。このような場合、USERDNSDOMAIN 環境変数は、親ドメインではなく子ドメインに解決されます。その結果、クライアントは組織のすべてのユーザに関する情報にアクセスできません。

USERDNSDOMAIN 環境変数が子ドメインに解決される場合、次のいずれかのオプションを使用して、Cisco Jabber for Windows が親ドメインのサービスに接続できるようにします。

- グローバルカタログまたはLDAPディレクトリサーバが組織のすべてのユーザにアクセスできることを確実にします。

- Cisco Jabber for Windows によるグローバル カタログ またはLDAP ディレクトリ サーバ の要求時に、組織のすべてのユーザにアクセスできるサーバにクライアントを転送するように、DNS サーバを設定します。
- 親ドメインの FQDN を使用するように Cisco Jabber for Windows を設定します。

次のようにクライアント設定に PrimaryServerName パラメータの値として親ドメインの FQDN を指定します。

```
<PrimaryServerName>parent-domain-fqdn</PrimaryServerName>
```

## 関連トピック

[ディレクトリ接続パラメータ](#)

[Configuring DNS for the Forest Root Domain](#)

[Assigning the Forest Root Domain Name](#)

[Deploying a GlobalNames Zone](#)

[Support for DNS Namespace planning in Microsoft server products](#)

## ディレクトリ サーバの検出

Cisco Jabber は、下記の場合に、自動的にディレクトリ サーバを検出して接続します。

- Cisco Jabber にインストールするワーク ステーションが Microsoft Windows ドメイン上にある。
- クライアントが DNS SRV レコードからディレクトリ サーバのアドレスを取得する

| ディレクトリ サーバ                           | SRV レコード                     |
|--------------------------------------|------------------------------|
| グローバル カタログ                           | _gc._msdcs._tcp.domain.com   |
| ドメイン コントローラ<br>LDAP-based ディレクトリ サーバ | _ldap._msdcs._tcp.domain.com |

## Cisco Unified Communications Manager User Data Service

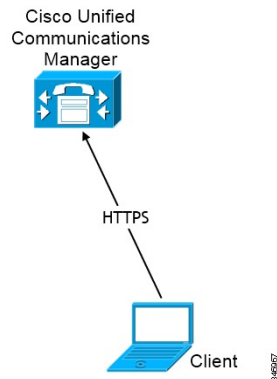
UDS は、連絡先を解決するために用意された Cisco Unified Communications Manager 上の REST インターフェイスです。

UDS は連絡先の解決に次の状況で使用されます。

- クライアント コンフィギュレーション ファイルでの UDS 値を使用するようにパラメータ DirectoryServerType を設定した場合。  
この設定では、企業のファイアウォールの内側または外側の場合に、クライアントは連絡先の解決に UDS を使用します。
- Expressway Mobile and Remote Access を導入した場合。

この設定では、企業のファイアウォールの内側または外側の場合に、クライアントは連絡先の解決に自動で UDS を使用します。

ディレクトリ サーバから Cisco Unified Communications Manager に連絡先データを同期します。その後、Cisco Jabber は UDS から連絡先データを自動的に取得します。



## UDS との統合の有効化

UDS との統合を有効にするには、次の手順を実行します。

### 手順

- 
- ステップ 1** Cisco Unified Communications Manager でディレクトリ ソースを作成します。
  - ステップ 2** 連絡先データを Cisco Unified Communications Manager に同期させます。  
同期の実行後、連絡先データが Cisco Unified Communications Manager に格納されます。
  - ステップ 3** 手動接続の場合、クライアントがサーバを検出できるように、Cisco Unified Communications Manager User Data Service サーバの IP アドレスを指定します。  
次に、Cisco Unified Communications Manager User Data Service サーバの設定例を示します。  

```
<UdsServer>11.22.33.444</UdsServer>
```
  - ステップ 4** クライアントを設定して、UDS との連絡先写真を取得します。  
次に、連絡先写真の取得の設定例を示します。  

```
<UdsPhotoUriWithToken>http://server_name.domain/%%uid%.jpg</UdsPhotoUriWithToken>
```
- 

## UDS サービス パラメータの設定

Cisco Unified Communications Manager の UDS にサービス パラメータを設定することができます。



## 手順

- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
- ステップ 2** [システム (System)] > [エンタープライズ パラメータ (Enterprise Parameters)] を選択します。  
[エンタープライズ パラメータ (Enterprise Parameters Configuration)] ウィンドウが表示されます。
- ステップ 3** [ユーザ データ サービス パラメータ (User Data Service Parameters)] セクションを入力します。

## UDS サービス パラメータ

UDS を設定するために、次のサービス パラメータの値を設定します。

| パラメータ                                   | 説明                                                                                                                          |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| ユーザ検索をすべて有効にする (Enable All User Search) | ディレクトリ内の全ユーザの検索を許可します (姓、名、またはディレクトリ番号を指定しない検索)<br>デフォルト値は <b>true</b> です。                                                  |
| ユーザ検索の上限 (User Search Limit)            | クエリーで返すユーザの数を制限します。<br>デフォルト値は <b>64</b> です。                                                                                |
| 削除桁数 (Number of digits to strip)        | ユーザが電話番号を検索するときに照合する桁数を指定します。<br><b>ヒント</b> PSTN 番号を解決するには、PSTN 番号の桁数に等しい値を設定する必要があります。たとえば、PSTN 番号が 10 桁の場合は、値を 10 に設定します。 |

## 複数のクラスタでの連絡先の解決

複数の Cisco Unified Communications Manager クラスタでの連絡先の解決では、社内ディレクトリのすべてのユーザを各クラスタに同期させます。その後、適切なクラスタにこれらのユーザのサブセットをプロビジョニングします。

たとえば、組織のユーザが 40,000 人としします。20,000 人のユーザが北米にいます。20,000 人のユーザがヨーロッパにいます。組織の各場所に次の Cisco Unified Communications Manager クラスタがあります。

- cucm-cluster-na (北米)
- cucm-cluster-eu (ヨーロッパ)

この例では、40,000 人のすべてのユーザを両方のクラスタに同期させます。その後、北米の 20,000 人のユーザを cucu-cluster-na にヨーロッパの 20,000 人のユーザを cucm-cluster-eu にプロビジョニングします。

ヨーロッパのユーザが北米のユーザにコールすると、Cisco Jabber が cucm-cluster-na からヨーロッパのユーザの連絡先詳細を取得します。

北米のユーザがヨーロッパのユーザにコールすると、Cisco Jabber が cucm-cluster-eu から北米のユーザの連絡先詳細を取得します。

## ディレクトリ統合のためのクライアント設定

ディレクトリ統合は、Cisco Unified Communications Manager 9 以降、またはコンフィギュレーションファイルを使用して、サービスプロファイルにより設定できます。このセクションでは、ディレクトリ統合用のクライアントを設定する方法を説明します。



(注) サービス プロファイルおよびコンフィギュレーション ファイルがある場合、サービス プロファイルの設定が優先されます。



(注) Cisco Unified Presence 8 のプロファイルはディレクトリ統合に使用することはできません。

## ディレクトリ統合を設定する場合



### ワンポイント アドバイス

Active Directory ドメインに登録されているワーク ステーションに Cisco Jabber for Windows をインストールします。この環境では、ディレクトリへ接続するために Cisco Jabber for Windows を構成する必要はありません。クライアントが自動的にディレクトリを検出し、そのドメインの グローバル カタログ サーバに接続します。

発信元として次のいずれかを使用する場合にのみ、ディレクトリに接続するよう Cisco Jabber for Windows を構成する必要があります。

- ドメイン コントローラ
- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory ライトウェイト ディレクトリ サービス
- Active Directory Application Mode; Active Directory アプリケーション モード

オプションで、ディレクトリ統合を設定し、次のタスクを含む展開ニーズに適合させることができます。

- デフォルトの属性マッピングの変更
- ディレクトリ照会設定の調整
- クライアントによる連絡先画像の取得方法の指定
- ドメイン内フェデレーションの実行

## サービス プロファイルのディレクトリ統合の設定

Cisco Unified Communications Manager バージョン 9 以降では、サービス プロファイルでユーザをプロビジョニングし、内部ドメインネームサーバの `_cisco-uds` SRV レコードを配置できます。

クライアントは、ディレクトリ統合の設定を入手するために、自動的に Cisco Unified Communications Manager を検出し、サービス プロファイルを取得できます。

サポート サービス プロファイルにサービス ディスカバリをセットアップするには、次のことが必要になります。

- 内部ドメインサーバに `_cisco-uds` SRV レコードを展開する。
- クライアントがドメイン ネーム サーバアドレスを解決できることを確認する。
- クライアントが Cisco Unified Communications Manager のホスト名を解決できることを確認する。
- クライアントが Cisco Unified Communications Manager の完全修飾ドメイン名 (FQDN) を解決できることを確認する。

Cisco Jabber は、Cisco Unified Communications Manager ユーザデータ サービス (UDS) をサポートしました。LDAP を使用した Active Directory への接続による展開に加え、Jabber を Cisco Unified Communications Manager ユーザデータ サービス コンタクト検索サービスで展開することも可能になりました。UDS サーバ使用時は、サーバのサイズ設定を考慮する必要があります。Cisco Unified Communication ノードは、サーバがサポートする最大デバイス登録数の 50 % の UDS コンタクト サービス接続をサポートできます。

サービス プロファイルのディレクトリ統合を設定するには、以下の手順に従ってください。

### 手順

- 
- ステップ 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] インターフェイスを開きます。
- ステップ 2** ディレクトリ サービスを追加します。
- a) [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [UC サービス (UC Service)] を選択します。  
[UC サービスの検索と一覧表示 (Find and List UC Services)] ウィンドウが開きます。
- b) [新規追加 (Add New)] を選択します。  
[UC サービスの設定 (UC Service Configuration)] ウィンドウが開きます。

- c) [UC サービス タイプ (UC Service Type)] から [ディレクトリ (Directory)] を選択し、[次へ (Next)] を選択します。
- d) ディレクトリ サービスのすべての適切な値を設定したら、[保存 (Save)] を選択します。

**ステップ 3** サービス プロファイルにディレクトリ サービスを適用します。

- a) [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [サービス プロファイル (Service Profile)] の順に選択します。  
[サービス プロファイルの検索と一覧表示 (Find and List Service Profiles)] ウィンドウが開きます。
- b) [新規追加 (Add New)] を選択します。  
[サービス プロファイルの設定 (Service Profile Configuration)] ウィンドウが開きます。
- c) プロファイル ディレクトリにディレクトリ サービスを追加します。
- d) [保存 (Save)] を選択します。

## ディレクトリ プロファイル パラメータ

次の表では、ディレクトリのプロファイルで設定される設定パラメータを示します。

| ディレクトリ サービスの設定                                    | 説明                                                                                                                                |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| プライマリ サーバ (Primary Server)                        | プライマリ ディレクトリ サーバのアドレスを指定します。<br><br>このパラメータは、クライアントが自動的にディレクトリ サーバを検出できない手動接続に必要です。                                               |
| セカンダリ サーバ (Secondary server)                      | バックアップディレクトリサーバのアドレスを指定します。                                                                                                       |
| ターシャリ サーバ (Tertiary Server)                       | ターシャリ ディレクトリ サーバのアドレスを指定します。                                                                                                      |
| コンタクト解決に UDS を使用 (Use UDS for Contact Resolution) | 発信元としてクライアントがUDSを使用するかどうかを設定します。<br><br>(注) デフォルトで、UDS はユーザが Expressway Mobile and Remote Access を介して社内ネットワークに接続す時に、連絡先の解決を提供します。 |

| ディレクトリ サービスの設定                                       | 説明                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ログインしたユーザのクレデンシャルを使用 (Use Logged On User Credential) | <p>クライアントの Microsoft Windows ユーザ名とパスワードを使用して指定します。</p> <p><b>はい (True)</b></p> <p>Windows 認証情報を使用します。これがデフォルト値です。</p> <p><b>いいえ (False)</b></p> <p>Windows 認証情報を使用しないでください。<br/>ConnectionUsername および ConnectionPassword パラメータのクレデンシャルを指定します。</p>                                                                                                                                                                 |
| ユーザ名 (Username)                                      | <p>クライアントがディレクトリ サーバで認証するために使用される共有ユーザ名を手動で指定することができます。</p> <p>このパラメータは、Microsoft Windows クレデンシャルを使用して、ディレクトリ サーバで認証できない展開でのみ、使用する必要があります。</p> <p>デフォルトでは、クライアントは、ディレクトリ サーバに接続する際に統合 Windows 認証を使用します。このパラメータは、ユーザの Microsoft Windows クレデンシャルをディレクトリ サーバで認証することが不可能であるシナリオで、ユーザ名の指定を手動で実行できます。</p> <p>このパラメータを使用する必要がある場合は、よく知られているクレデンシャルかパブリック クレデンシャルを使用する必要があります。クレデンシャルは、読み取り専用権限を持つアカウントにリンクされる必要があります。</p> |

| ディレクトリ サービスの設定                                                                | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パスワード (Password)                                                              | <p>クライアントがディレクトリ サーバで認証するために使用される共有パスワードを手動で指定することができます。</p> <p>このパラメータは、<b>Microsoft Windows</b> クレデンシアルを使用して、ディレクトリ サーバで認証できない展開でのみ、使用する必要があります。</p> <p>デフォルトでは、クライアントは、ディレクトリ サーバに接続する際に統合 <b>Windows</b> 認証を使用します。このパラメータは、ユーザの <b>Microsoft Windows</b> クレデンシアルをディレクトリ サーバで認証することが不可能であるシナリオで、パスワードの指定を手動で実行できます。</p> <p>このパラメータを使用する必要がある場合は、よく知られているクレデンシアルかパブリック クレデンシアルを使用する必要があります。クレデンシアルは、読み取り専用権限を持つアカウントにリンクされる必要があります。</p>                                                                                                             |
| 検索ベース 1 (Search Base 1)<br>検索ベース 2 (Search Base 2)<br>検索ベース 3 (Search Base 3) | <p>検索が開始されるディレクトリ サーバの場所を指定します。つまり、検索ベースはクライアントが検索を実行するルートです。</p> <p>デフォルトでは、ディレクトリ ツリーのルートから検索します。デフォルトの動作を上書きする場合は、最大 3 つの検索ベースの値を <b>OU</b> に指定することができます。</p> <p><b>Active Directory</b> により、検索ベースが要求されることは基本的にありません。特定のパフォーマンス要件のみ <b>Active Directory</b> の検索ベースを指定する必要があります。</p> <p>ディレクトリにロケーションを指定するためのバインディングを作成するために、<b>Active Directory</b> 以外のディレクトリ サーバの検索ベースを指定する必要があります。</p> <p><b>ヒント</b>    <b>OU</b> を指定すると、検索対象を特定のユーザグループに制限することができます。</p> <p>たとえば、ユーザのサブセットにインスタントメッセージングの機能だけがあります。それらのユーザを <b>OU</b> に含め、それを検索ベースとして指定します。</p> |

| ディレクトリ サービスの設定                                           | 説明                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| すべての検索ベースで再帰検索<br>(Recursive Search on All Search Bases) | <p>検索ベースから始まるディレクトリの再帰検索を実行するには、このオプションを選択します。再帰検索を使用して、Cisco Jabber クライアントの連絡先検索クエリーが指定された検索コンテキスト（検索ベース）からのLDAP ディレクトリ ツリーすべてを検索できるようにします。これは、LDAP 検索と共通のオプションです。</p> <p>必須フィールドです。</p> <p>デフォルト値は True です。</p>                                                                                                                                           |
| 検索タイムアウト (Search Timeout)                                | <p>ディレクトリのクエリーのタイムアウト時間を秒数で指定します。</p> <p>デフォルト値は 5 です。</p>                                                                                                                                                                                                                                                                                                  |
| 基本フィルタ (Base Filter)                                     | <p>Active Directory クエリーの基本フィルタを指定します。</p> <p>ディレクトリのサブキー名のみを指定し、ディレクトリへのクエリーの実行時にユーザ オブジェクト以外のオブジェクトを取得します。</p> <p>デフォルト値は (&amp; (objectCategory=person) です。</p>                                                                                                                                                                                          |
| 予測検索フィルタ (Predictive Search Filter)                      | <p>フィルタを予測検索クエリーに適用するように定義します。</p> <p>検索クエリーのフィルタリングをするために、複数の場合は、カンマ区切りの値を定義します。</p> <p>デフォルト値は ANR です。</p> <p>Cisco Jabber for Windows では、予測検索が実行される際、Ambiguous Name Resolution (ANR) を使用したクエリーが発行されます。このクエリーにより、検索文字列が明確化され、ディレクトリ サーバ上で ANR に対して設定された属性に合致する結果が返されます。</p> <p><b>重要</b> クライアントがその属性を探すようにするためには、ディレクトリ サーバを設定して、ANR の属性を設定する必要があります。</p> |

### 属性のマッピング (Attribute Mappings)

サービスプロファイルのデフォルトの属性マッピングを変更することはできません。デフォルトの属性マッピングを変更するには、クライアント構成ファイルの必須のマッピングを定義する必要があります。

## ディレクトリ統合の設定パラメータの概要

このトピックでは、ディレクトリ統合を設定するために指定できるすべてのパラメータをリストします。

### EDI パラメータの概要

次の表に、LDAP ディレクトリ サーバによる属性マッピングに使用できるパラメータをリストします。

| 属性マッピングのパラメータ                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• CommonName</li> <li>• DisplayName</li> <li>• Firstname</li> <li>• Lastname</li> <li>• EmailAddress</li> <li>• SipUri</li> <li>• PhotoSource</li> <li>• BusinessPhone</li> <li>• MobilePhone</li> <li>• HomePhone</li> <li>• OtherPhone</li> </ul> | <ul style="list-style-type: none"> <li>• Title</li> <li>• CompanyName</li> <li>• UserAccountName</li> <li>• DomainName</li> <li>• Location</li> <li>• Nickname</li> <li>• PostalCode</li> <li>• City</li> <li>• State</li> <li>• StreetAddress</li> </ul> |

次の表に、LDAP ディレクトリ サーバへの接続に使用できるパラメータを示します。

| ディレクトリ サーバの接続パラメータ                                                                                                                                                           |                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• ConnectionType</li> <li>• PrimaryServerName</li> <li>• SecondaryServerName</li> <li>• ServerPort1</li> <li>• ServerPort2</li> </ul> | <ul style="list-style-type: none"> <li>• UseWindowsCredentials</li> <li>• ConnectionUsername</li> <li>• ConnectionPassword</li> <li>• UseSSL</li> <li>• UseSecureConnection</li> </ul> |

次の表に、LDAP ディレクトリ サーバによる連絡先の解決とディレクトリのクエリーに使用できるパラメータを示します。



## 連絡先の解決とディレクトリのクエリー パラメータ

- |                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• BaseFilter</li> <li>• PredictiveSearchFilter</li> <li>• DisableSecondaryNumberLookups</li> <li>• PhoneNumberMasks</li> <li>• SearchTimeout</li> <li>• UseWildcards</li> <li>• MinimumCharacterQuery</li> <li>• SearchBase1、 SearchBase2、 SearchBase3、 SearchBase4、 および SearchBase5</li> </ul> | <ul style="list-style-type: none"> <li>• PhotoUriSubstitutionEnabled</li> <li>• PhotoUriSubstitutionToken</li> <li>• PhotoUriWithToken</li> <li>• UseSIPURIToResolveContacts</li> <li>• UriPrefix</li> <li>• IMAddresses</li> <li>• IMAddress</li> </ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## UDS パラメータの概要

次の表に、UDS への接続、および連絡先の解決とディレクトリのクエリーに使用できるパラメータを示します。

## UDS パラメータ

- |                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• DirectoryServerType</li> <li>• PresenceDomain</li> <li>• UdsServer</li> <li>• UdsPhotoUriWithToken</li> </ul> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|

## EDI パラメータ

ここでは、LDAP ベースのディレクトリ統合に設定できるパラメータの詳細を示します。

## 属性マッピングのパラメータ

次の表に、LDAP ディレクトリ属性をマッピングするためのパラメータを説明します。

| パラメータ      | ディレクトリ属性 | デフォルトで<br>グローバル カ<br>タログに存在 | デフォルトで<br>インデックス<br>を付加 | Ambiguous Name<br>Resolution<br>(ANR) がデ<br>フォルトで設定 |
|------------|----------|-----------------------------|-------------------------|-----------------------------------------------------|
| CommonName | cn       | Yes                         | Yes                     | No                                                  |

| パラメータ           | ディレクトリ属性                    | デフォルトで<br>グローバル カ<br>タログに存在 | デフォルトで<br>インデックス<br>を付加 | <b>Ambiguous Name<br/>Resolution<br/>(ANR)</b> がデ<br>フォルトで設定 |
|-----------------|-----------------------------|-----------------------------|-------------------------|--------------------------------------------------------------|
| DisplayName     | displayName                 | Yes                         | Yes                     | Yes                                                          |
| Firstname       | givenName                   | Yes                         | Yes                     | Yes                                                          |
| Lastname        | sn                          | Yes                         | Yes                     | Yes                                                          |
| EmailAddress    | mail                        | Yes                         | Yes                     | Yes                                                          |
| SipUri          | msRTCSIP-PrimaryUserAddress | Yes                         | Yes                     | Yes                                                          |
| PhotoSource     | thumbnailPhoto              | No                          | No                      | No                                                           |
| BusinessPhone   | telephoneNumber             | Yes                         | No                      | No                                                           |
| MobilePhone     | mobile                      | Yes                         | No                      | No                                                           |
| HomePhone       | homePhone                   | Yes                         | No                      | No                                                           |
| OtherPhone      | otherTelephone              | Yes                         | No                      | No                                                           |
| Title           | title                       | Yes                         | No                      | No                                                           |
| CompanyName     | company                     | Yes                         | Yes                     | No                                                           |
| UserAccountName | sAMAccountName              | Yes                         | Yes                     | Yes                                                          |
| DomainName      | userPrincipalName           | Yes                         | Yes                     | No                                                           |
| Location        | co                          | Yes                         | No                      | No                                                           |
| Nickname        | displayName                 | Yes                         | Yes                     | Yes                                                          |
| PostalCode      | postalCode                  | Yes                         | No                      | No                                                           |
| City            | l                           | Yes                         | Yes                     | No                                                           |
| State           | st                          | Yes                         | Yes                     | No                                                           |
| StreetAddress   | StreetAddress               | Yes                         | No                      | No                                                           |

## ディレクトリ サーバの属性

クライアントがコンタクトを解決できるように、LDAP ディレクトリ サーバの属性のインデックスを作成する必要があります。

デフォルトの属性マッピングを使用する場合は、次の属性がインデックス化されていることを確認します。

- sAMAccountName
- displayName

- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber

さらに、セカンダリ番号クエリーについては、次の属性もインデックス化する必要があります。

- otherTelephone
- mobile
- homePhone



(注) セカンダリ番号クエリーは Cisco Jabber ではデフォルトで有効になっています。セカンダリ番号クエリーは、DisableSecondaryNumberLookups パラメータで無効にすることができます。

#### • msRTPSIP-PrimaryUserAddress

ドメイン内フェデレーションのみ、msRTPSIP-PrimaryUserAddress をインデックス化する必要があります。

クライアントがグローバルカタログサーバにデフォルトで接続するため、すべての属性がグローバルカタログサーバに存在することを保証する必要があります。Microsoft Active Directory Schema スナップインなどの適切なツールを使用すると、属性をグローバルカタログサーバに複製できます。

グローバルカタログサーバに属性を複製すると、ドメイン内の Active Directory サーバ間にトラフィックが発生します。したがって、ネットワークトラフィックが過剰負荷を処理できる場合、グローバルカタログサーバに属性を複製する必要があります。

グローバルカタログサーバに属性を複製しない場合は、ドメインコントローラに接続するように Cisco Jabber を設定できます。ただし、クライアントは、ドメインコントローラに接続する場合のみ、単一のドメインに問い合わせます。

## ディレクトリ接続パラメータ

次の表に、LDAP ディレクトリ接続を設定するためのパラメータを示します。

| パラメータ          | 値      | 説明                                                                                                                                                                                                                                                                                       |
|----------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ConnectionType | 0<br>1 | <p>クライアントが グローバル カタログ または ドメイン コントローラ へ接続するかを指定します。</p> <p><b>0</b></p> <p>グローバルカタログに接続します。<br/>これがデフォルト値です。</p> <p><b>1</b></p> <p>ドメイン コントローラ に接続します。</p> <p>(注) デフォルト ポートは次のとおりです。</p> <ul style="list-style-type: none"><li>• グローバル カタログ : 3268</li><li>• ドメインコントローラ : 389</li></ul> |

| パラメータ               | 値                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PrimaryServerName   | IP アドレス (IP Address)<br>FQDN | <p>必須パラメータです。プライマリ ディレクトリ サーバのアドレスを指定します。</p> <p>このパラメータは、クライアントが自動的にディレクトリ サーバを検出できない手動接続に必要です。</p> <p>(注) クライアントは、起動するたびにプライマリ サーバに接続しようと試行します。次の場合に、クライアントはセカンダリ サーバに接続しようとします。</p> <ul style="list-style-type: none"><li>• プライマリ サーバが使用できない。</li><li>• クライアントが接続すると、プライマリ サーバに障害が発生する。</li></ul> <p>セカンダリ サーバに正常に接続できれば、クライアントは次回再起動されるまでセカンダリ サーバへの接続を保持します。</p> <p>クライアントが接続する際に、セカンダリ サーバに障害が発生した場合、クライアントは、プライマリ サーバに接続しようとします。</p> |
| SecondaryServerName | IP アドレス (IP Address)<br>FQDN | <p>バックアップ ディレクトリ サーバのアドレスを指定します。</p> <p>このパラメータは、クライアントが自動的にディレクトリ サーバを検出できない手動接続に必要です。</p>                                                                                                                                                                                                                                                                                                                                                 |
| ServerPort1         | ポート番号                        | プライマリ ディレクトリ サーバのポートを指定します。                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ServerPort2         | ポート番号                        | バックアップ ディレクトリ サーバのポートを指定します。                                                                                                                                                                                                                                                                                                                                                                                                                |

| パラメータ                 | 値      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UseWindowsCredentials | 0<br>1 | <p>クライアントの Microsoft Windows ユーザ名とパスワードを使用して指定します。</p> <p><b>0</b></p> <p>Windows 認証情報を使用しないでください。</p> <p>ConnectionUsername および ConnectionPassword パラメータのクレデンシャルを指定します。</p> <p><b>1</b></p> <p>Windows 認証情報を使用します。これがデフォルト値です。</p>                                                                                                                                                                                                                           |
| ConnectionUsername    | ユーザ名   | <p>クライアントがディレクトリサーバで認証するために使用される共有ユーザ名を手動で指定することができます。このパラメータは、Microsoft Windows クレデンシャルを使用して、ディレクトリサーバで認証できない展開でのみ、使用する必要があります。</p> <p><b>重要</b> クライアントは、プレーンテキストとしてこのユーザ名を転送し、保存します。</p> <p>デフォルトでは、クライアントは、ディレクトリサーバに接続する際に統合 Windows 認証を使用します。このパラメータは、ユーザの Microsoft Windows クレデンシャルをディレクトリサーバで認証することが不可能であるシナリオで、ユーザ名の指定を手動で実行できます。</p> <p>このパラメータを使用する必要がある場合は、よく知られているクレデンシャルかパブリッククレデンシャルを使用する必要があります。統合に使用するアカウントには、ディレクトリに対する読み取り専用アクセス権が必要です。</p> |

| パラメータ              | 値     | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ConnectionPassword | パスワード | <p>クライアントがディレクトリサーバで認証するために使用される共有パスワードを手動で指定することができます。このパラメータは、Microsoft Windows クレデンシアルを使用して、ディレクトリサーバで認証できない展開でのみ、使用する必要があります。</p> <p><b>重要</b> クライアントは、プレーン テキストとしてこれらのパスワードを転送し、保存します。</p> <p>デフォルトでは、クライアントは、ディレクトリサーバに接続する際に統合Windows認証を使用します。このパラメータは、ユーザの Microsoft Windows クレデンシアルをディレクトリサーバで認証することが不可能であるシナリオで、パスワードの指定を手動で実行できます。</p> <p>このパラメータを使用する必要がある場合は、よく知られているクレデンシアルかパブリッククレデンシアルを使用する必要があります。統合に使用するアカウントには、ディレクトリに対する読み取り専用アクセス権が必要です。</p> |

| パラメータ  | 値      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UseSSL | 0<br>1 | <p>ディレクトリへの安全な接続に SSL を使用します。</p> <p><b>0</b></p> <p>SSL を使用しません。これがデフォルト値です。</p> <p><b>1</b></p> <p>SSL を使用します。</p> <p>SSL 接続の証明書を提示する必要があります。</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 証明書ストア内。</li> <li>• クライアントが接続するディレクトリサーバ。</li> </ul> <p>SSL 接続を確立するには、サーバがクライアントに証明書を提示します。クライアントは、クライアント コンピュータ ストアの証明書に対してサーバから証明書を認可します。</p> <p>SSL 接続のデフォルトのプロトコルとポートは、次のとおりです。</p> <p><b>グローバル カタログ</b></p> <p>プロトコル : TCP<br/>ポート番号 : 3269</p> <p><b>ドメイン コントローラ</b></p> <p>プロトコル : TCP<br/>ポート番号 : 636</p> |



| パラメータ               | 値      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UseSecureConnection | 0<br>1 | <p>ディレクトリ サーバに認証のメカニズムを指定します。</p> <p><b>0</b></p> <p>単純な認証を使用します。</p> <p>簡易バインドを使用してディレクトリ サーバに接続するために、この値を設定します。</p> <p>(注) 単純認証により、クライアントはプレーンテキストでクレデンシャルを送信します。 UseSSL パラメータのクレデンシャルを暗号化するには、SSL を有効にします。</p> <p><b>1</b></p> <p>Generic Security Service API (GSS-API) を使用します。これがデフォルト値です。</p> <p>GSS-API はシステム認証メカニズムを利用します。Microsoft Windows 環境では、GSS-API は Kerberos ベースの Windows 認証を使用してディレクトリ サーバに接続することができます。</p> |

## ディレクトリ クエリー パラメータ

次の表に、クライアントによる LDAP ディレクトリへのクエリー方法を設定するためのパラメータを示します。

| パラメータ                  | 値       | 説明                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BaseFilter             | 基本フィルタ  | <p>Active Directory クエリーの基本フィルタを指定します。</p> <p>ディレクトリのサブキー名のみを指定し、ディレクトリへのクエリーの実行時にユーザオブジェクト以外のオブジェクトを取得します。</p> <p>デフォルト値は<br/>(<code>&amp;objectCategory=person</code>)) です。</p> <p>設定ファイルには、有効な XML 文字実体参照のみを含めることができます。カスタム基本フィルタを指定する場合には、<code>&amp;</code> の代わりに <code>&amp;#x26;</code> を使用します。</p>                                                               |
| PredictiveSearchFilter | サーチフィルタ | <p>フィルタを予測検索クエリーに適用するように定義します。</p> <p>検索クエリーのフィルタリングをするために、複数の場合は、カンマ区切りの値を定義します。</p> <p>デフォルト値は <code>anr=</code> です。</p> <p>Cisco Jabber for Windows では、予測検索が実行される際、Ambiguous Name Resolution (ANR) を使用したクエリーが発行されます。このクエリーにより、検索文字列が明確化され、ディレクトリ サーバ上で ANR に対して設定された属性に合致する結果が返されます。</p> <p><b>重要</b> クライアントがその属性を探すようにするためには、ディレクトリサーバを設定して、ANR の属性を設定する必要があります。</p> |

| パラメータ                         | 値      | 説明                                                                                                                                                                              |
|-------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DisableSecondaryNumberLookups | 0<br>1 | <p>携帯電話番号、自宅の電話番号、他の電話番号などの仕事用の番号を使用できない場合に、ユーザが代替連絡先番号を検索できるかどうかを指定します。</p> <p><b>0</b></p> <p>ユーザは代替連絡先番号を検索できます。これがデフォルト値です。</p> <p><b>1</b></p> <p>ユーザは代替連絡先番号を検索できません。</p> |
| SearchTimeout                 | 秒数     | <p>クエリーのタイムアウト時間を秒数で指定します。</p> <p>デフォルト値は 5 です。</p>                                                                                                                             |
| UseWildcards                  | 0<br>1 | <p>ワイルドカード検索を有効にします。</p> <p><b>0</b></p> <p>ワイルドカードを使用しません。これがデフォルト値です。</p> <p><b>1</b></p> <p>ワイルドカードを使用します。</p> <p>ワイルドカードを使用してディレクトリを検索するには、時間がかかる場合があります。</p>               |
| MinimumCharacterQuery         | 数値     | <p>ディレクトリを照会するために連絡先名の最小文字数を設定します。</p> <p>たとえば、このパラメータの値として 2 を設定した場合、ユーザが検索フィールドに少なくとも 2 文字を入力するとクライアントは検索を行います。</p> <p>デフォルト値は 3 です。</p>                                      |

| パラメータ                                                                   | 値                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SearchBase1<br>SearchBase2<br>SearchBase3<br>SearchBase4<br>SearchBase5 | ディレクトリツリーで検索可能な組織単位 (OU) | <p>検索が開始されるディレクトリサーバの場所を指定します。つまり、検索ベースはクライアントが検索を実行するルートです。</p> <p>デフォルトでは、ディレクトリツリーのルートから検索します。デフォルトの動作を上書きする場合は、最大5つの検索ベースの値を OU に指定することができます。</p> <p>Active Directory により、検索ベースが要求されることは基本的にありません。特定のパフォーマンス要件のみ Active Directory の検索ベースを指定する必要があります。</p> <p>ディレクトリにロケーションを指定するためのバインディングを作成するために、Active Directory 以外のディレクトリサーバの検索ベースを指定する必要があります。</p> <p><b>ヒント</b> OU を指定すると、検索対象を特定のユーザグループに制限することができます。</p> <p>たとえば、ユーザのサブセットにインスタントメッセージングの機能だけがあります。それらのユーザを OU に含め、それを検索ベースとして指定します。</p> |

## 関連トピック

[『Ambiguous Name Resolution for LDAP in Windows 2000』](#)

[『LDAP Referrals』](#)

[『Common Default Attributes Set for Active Directory and Global Catalog』](#)

## 基本フィルタの例

次は、特定のロケーションまたはオブジェクトを表示する場合に使用できる基本フィルタの例を示しています。

特定のグループのみ検索：

```
(& (objectClass=user) (memberOf=cn=group-name,ou=Groups,dc=example,dc=com))
```

グループ内のネストされたグループの検索：

```
(& (objectClass=user) (memberOf:search-oid:=cn=group-name,ou=Groups,dc=example,dc=com))
```

有効なアカウントと管理者以外のアカウントを検索：

```
(& (objectCategory=person) (objectClass=user) (! (userAccountControl:search-oid:=2))
(! (sAMAccountName=* _dbo)) (! (sAMAccountName=*-admin)))
```

## 電話番号マスク パラメータ

次の表に、電話番号解決のマスクを設定するパラメータを示します。

| パラメータ            | 値      | 説明                                                                                                                                                                                                                                 |
|------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PhoneNumberMasks | マスク文字列 | <p>ユーザが電話番号を検索するときに使用するマスクを指定します。</p> <p>たとえば、ユーザが +14085550100 からのコールを受信するとします。ディレクトリでは、この番号は + (1) 408 555 0100 です。</p> <p>次のマスクにより、番号が解決されます：<br/>+14081+(#) ### ### #####</p> <p>マスク文字列の長さは、レジストリ サブキー名のサイズ制限を超えることはできません。</p> |

電話マスクは、クライアントでディレクトリを検索する前に電話番号に適用されます。電話マスクを正しく設定すると、クエリーが完全に一致するため、ディレクトリ検索が成功し、ディレクトリ サーバのパフォーマンスへの影響が回避されます。

次の表に、電話マスクに含めることができる要素を示します。

| 要素       | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 電話番号パターン | <p>番号パターンを設定してディレクトリから電話番号を取得します。</p> <p>電話マスクを追加するには、マスクを適用する番号パターンを指定します。</p> <p>たとえば、+1408 で始まる検索に対してマスクを指定するには、+1408 +(#) #### ##### のマスクを使用します。</p> <p>桁数が同じでもパターンが異なる電話番号をマスクで処理できるようにするには、桁数が同じ複数のマスクを使用します。</p> <p>たとえば、会社サイトにサイト A とサイト B があるとします。各サイトでは、次のように電話番号の形式が異なる個別のディレクトリを管理します。</p> <p>+ (1) 408 555 0100<br/>+1-510-5550101</p> <p>+1408 +(#) ### ### ##### +1510 + #-####-##### のマスクにより、両方の番号を正しく使用できます。</p> |

| 要素            | 説明                                                                                                                                                                                                                                                        |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| パイプ記号<br>( )  | 番号パターンとマスクを区切ります。<br>たとえば、+1408 +(#) ### ### +34 +(##) ### ### です。                                                                                                                                                                                        |
| ワイルド<br>カード文字 | 一致すると思われる文字のサブセットの代わりに 1 つ以上の文字を使用します。<br>電話マスクで任意のワイルドカード文字を使用できます。<br>たとえば、アスタリスク (*) は、1 つ以上の文字を表し、+3498 +##*##*#####<br>のようにマスクに適用できます。 ワイルドカードとともにこのマスクを使用すると、電話番号検索で次のいずれかの形式と一致します。<br><br>+34(98)555 0199<br>+34 98 555-0199<br>+34-(98)-555.0199 |
| 逆マスク          | 番号パターンを右から左に適用します。<br>たとえば、+34985590199 に +3498 R+34 (98) 559 ##### のマスクを適用すると、+34 (98) 559 0199 が取得されます。<br><br>順マスクと逆マスクの両方を使用できます。                                                                                                                     |

## 連絡先の写真のパラメータ

次の表に、クライアントが LDAP ディレクトリから連絡先の写真を取得する方法を設定するパラメータについて説明します。

| パラメータ                       | 値             | 説明                                                                                                                              |
|-----------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------|
| PhotoUriSubstitutionEnabled | true<br>false | 写真 URI の代替が有効であるかどうかを指定します。<br><br><b>true</b><br>写真 URI の代替が有効。<br><br><b>false</b><br>写真 URI の代替が無効であるかどうかを指定します。これがデフォルト値です。 |

| パラメータ                     | 値        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PhotoUriSubstitutionToken | ディレクトリ属性 | <p>写真URIに挿入するディレクトリ属性を指定します（sAMAccountName など）。</p> <p>PhotoURISubstitutionToken パラメータとの使用がサポートされているのは次の属性だけです。</p> <ul style="list-style-type: none"><li>• Common Name</li><li>• 表示名（Display Name）</li><li>• First Name</li><li>• Last Name</li><li>• Nickname</li><li>• 電子メールアドレス（Email Address）</li><li>• フォト ソース（Photo Source）</li><li>• 会社電話（Business Phone）</li><li>• 携帯電話（Mobile Phone）</li><li>• 自宅電話（Home Phone）</li><li>• 連絡先電話番号</li><li>• 他の電話（Other Phone）</li><li>• 役職（Title）</li><li>• Company Name</li><li>• ユーザ アカウント名（User Account Name）</li><li>• ドメイン名（Domain Name）</li><li>• Location</li><li>• 郵便番号（Post Code）</li><li>• State</li><li>• 市区町村郡（City）</li><li>• Street</li></ul> |

| パラメータ             | 値   | 説明                                                                                                                                                                                                                                                                                              |
|-------------------|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PhotoUriWithToken | URI | <p>変数値としてディレクトリ属性を使用する、写真 URI を指定します<br/>(<code>http://staffphoto.example.com/sAMAccountName.jpg</code> など)。</p> <p>パラメータはLDAPディレクトリ統合に適用されます。</p> <p>写真 URI の代替を設定するには、<b>PhotoUriSubstitutionToken</b> の値としてディレクトリ属性を設定します。</p> <p><b>制約事項</b> クライアントがクレデンシャルなしで Web サーバから画像を取得する必要があります。</p> |

## 関連トピック

[連絡先の写真の形式と寸法, \(205 ページ\)](#)

## EDI での連絡先写真の取得

Cisco Jabber では、次の方法で連絡先写真を取得して表示します。



(注) Active Directory で写真を変更すると、Cisco Jabber で写真が更新されるまで最大 24 時間かかることがあります。

### URI 置換

Cisco Jabber によって、ディレクトリ属性と URL テンプレートを使用して連絡先写真の URL が動的に作成されます。

この方法を使用するには、設定ファイルで次の値を設定します。

- 1 **PhotoUriSubstitutionEnabled** パラメータの値として `true` を指定します。
- 2 動的トークンとして使用するディレクトリ属性を、次の例のように **PhotoUriSubstitutionToken** パラメータの値として指定します。  
`<PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>`
- 3 次の例のように、**PhotoUriWithToken** パラメータの値として URL および動的トークンを指定します。  
`<PhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</PhotoUriWithToken>`

前述の手順の例の値では、`sAMAccountName` 属性がディレクトリの `msmith` に解決されます。その後、Cisco Jabber では、この値を取得してトークンを置換し、`http://staffphoto.example.com/msmith.jpg` の URL を作成します。



## バイナリ オブジェクト

Cisco Jabber によって、データベースから写真のバイナリ データが取得されます。

Active Directory からのバイナリ オブジェクトを使用している場合、PhotoUriWithToken はセットしないでください。

この方法を使用して連絡先写真を取得するには、次の例のように、設定で PhotoSource パラメータの値としてバイナリ データが含まれている属性を指定します。

```
<PhotoSource>jpegPhoto</PhotoSource>
```

## PhotoURL 属性

Cisco Jabber によって、ディレクトリ属性から URL が取得されます。

この方法を使用して連絡先写真を取得するには、次の例のように、設定で PhotoSource パラメータの値として写真の URL が含まれている属性を指定します。

```
<PhotoSource>photoUri</PhotoSource>
```

## 連絡先の写真の形式と寸法

Cisco Jabber で最適な結果を得るには、連絡先の写真は特定の形式と大きさが必要です。サポートされるフォーマットと最適な寸法を確認してください。連絡先の写真にクライアントが行う調整について説明します。

### 関連トピック

[連絡先の写真のパラメータ、\(202 ページ\)](#)

### 連絡先写真の形式

Cisco Jabber では、ディレクトリ内の連絡先写真について次の形式をサポートしています。

- JPG
- PNG
- BMP
- GIF



#### 重要

Cisco Jabber では、GIF 形式の連絡先写真のレンダリングを向上させるための変更は適用されません。その結果、GIF 形式の連絡先写真が不正にレンダリングされたり最適な品質にならない場合があります。最適な品質を得るには、連絡先の写真として PNG 形式を使用する必要があります。

## 連絡先写真の寸法



## ヒント

連絡先写真の最適な寸法は、アスペクト比 1:1 の 128 x 128 ピクセルです。

128 ピクセル x 128 ピクセルは、Microsoft Outlook のローカル連絡先の写真の最大寸法です。

次の表に、Cisco Jabber での連絡先写真のさまざまな寸法を示します。

| 参照先                                                                                                                        | 寸法             |
|----------------------------------------------------------------------------------------------------------------------------|----------------|
| 音声コール ウィンドウ                                                                                                                | 128 x 128 ピクセル |
| 次のような招待やリマインダ <ul style="list-style-type: none"> <li>着信コール ウィンドウ</li> <li>会議リマインダ ウィンドウ</li> </ul>                         | 64 x 64 ピクセル   |
| 次のような連絡先のリスト <ul style="list-style-type: none"> <li>連絡先リスト</li> <li>参加者リスト</li> <li>コール履歴</li> <li>ボイスメール メッセージ</li> </ul> | 32 x 32 ピクセル   |

## 連絡先写真の調整

Cisco Jabber で、次のように連絡先写真を調整します。

## サイズ変更

ディレクトリ内の連絡先写真が 128 x 128 ピクセル以外のサイズである場合、クライアントによって写真のサイズが自動的に変更されます。たとえば、ディレクトリ内の連絡先写真が 64 x 64 ピクセルであるとしします。Cisco Jabber でディレクトリから連絡先写真を取得すると、その写真のサイズが 128 x 128 ピクセルに変更されます。



## ヒント

連絡先写真のサイズ変更により、最適な解像度が得られない場合があります。このため、クライアントによって連絡先写真のサイズが自動的に変更されないように、128 x 128 ピクセルの連絡先写真を使用してください。

## トリミング

Cisco Jabber では、四角形以外の写真を四角形のアスペクト比（つまり、幅が高さと同じアスペクト比 1:1）に自動的にトリミングします。

### 縦方向

ディレクトリ内の連絡先写真が縦方向である場合、クライアントで上端から 30%、下端から 70% をトリミングします。

たとえば、ディレクトリ内の連絡先写真が幅 100 ピクセル、高さ 200 ピクセルである場合、アスペクト比が 1:1 となるように Cisco Jabber で高さから 100 ピクセルをトリミングする必要があります。この場合、クライアントで写真の上端から 30 ピクセルを、写真の下端から 70 ピクセルをトリミングします。

### 横方向

ディレクトリ内の連絡先写真が横方向である場合、クライアントで両方の側から 50% をトリミングします。

たとえば、ディレクトリ内の連絡先写真が幅 200 ピクセル、高さ 100 ピクセルである場合、アスペクト比が 1:1 となるように Cisco Jabber で幅から 100 ピクセルをトリミングする必要があります。この場合、クライアントで写真の右側から 50 ピクセルを、写真の左側から 50 ピクセルをトリミングします。

## 丸め

Cisco Jabber では、ディレクトリから連絡先写真を取得した後、それらの写真の角を丸めます。

# UDS パラメータ

次の表に、UDS への接続、および連絡先の解決とディレクトリのクエリーに使用できるパラメータに関する詳細を示します。

| パラメータ                | 値                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PresenceDomain       | プレゼンス サーバのドメイン               | <p>必須パラメータです。プレゼンス サーバのドメインを指定します。</p> <p>クライアントは、IM アドレスを作成するために、このドメインをユーザ ID に付加します。たとえば、Adam McKenzie という名前のユーザのユーザ ID が amckenzie であるとして、プレゼンス サーバ ドメインとして example.com を指定します。</p> <p>ユーザがログインすると、クライアントは Adam McKenzie に amckenzie@example.com という IM アドレスを構築します。</p>                                                                                                                                                                                                                                             |
| UdsServer            | IP アドレス (IP Address)<br>FQDN | <p>Cisco Unified Communications Manager User Data Service (UDS) サーバのアドレスを指定します。</p> <p>このパラメータは、クライアントが自動的に UDS サーバを検出できない手動接続に必要です。</p>                                                                                                                                                                                                                                                                                                                                                                                |
| UdsPhotoUriWithToken | URI                          | <p>変数値としてディレクトリ属性を使用する、写真 URI を指定します<br/>(http://www.photo/url/path/%%uid%.jpg など)。</p> <p>このパラメータは、UDSディレクトリ統合に適用されます。次のいずれかのケースで連絡先の写真をダウンロードするには、このパラメータを指定する必要があります。</p> <ul style="list-style-type: none"> <li>• DirectoryServerType パラメータを設定して UDS を使用する場合。この設定では、企業のファイアウォールの内側または外側の場合に、クライアントは連絡先の解決に UDS を使用します。</li> <li>• Expressway Mobile and Remote Access を導入した場合。この設定では、企業のファイアウォールの内側または外側の場合に、クライアントは連絡先の解決に自動で UDS を使用します。</li> </ul> <p><b>制約事項</b> クライアントはクレデンシャルなしで、Web サーバから画像を取得する必要があります。</p> |

## UDS での連絡先写真の取得

UDS によって、ディレクトリ属性と URL テンプレートをを使用して連絡先写真の URL が動的に作成されます。

UDS を使用して連絡先写真を解決するには、UdsPhotoUriWithToken パラメータの値として連絡先写真の URL の形式を指定します。また、`%%uid%%` トークンを挿入して、次に例を示すとおり URL の連絡先のユーザ名を置換します。

```
<UdsPhotoUriWithToken>http://server_name/%%uid%%.jpg</UdsPhotoUriWithToken>
```

UDS によって、`%%uid%%` トークンが UDS の `userName` 属性に置換されます。たとえば、Mary Smith という名前のユーザがディレクトリに存在するとします。Mary Smith の `userName` 属性は `msmith` です。Mary Smith の連絡先写真を解決するために、Cisco Jabber では `userName` 属性を取得して `%%uid%%` トークンを置換し、`http://staffphoto.example.com/msmith.jpg` の URL を作成します。



(注) Active Directory で写真を変更すると、Cisco Jabber で写真が更新されるまで最大 24 時間かかることがあります。



### 重要

- Expressway Mobile and Remote Access を導入している場合、ユーザが企業ネットワークの外部からサービスに接続するときに、クライアントは自動的に UDS を連絡先の解決に使用します。UDS 連絡先の解決を Expressway Mobile and Remote Access にセットアップする場合、連絡先写真をホストする Web サーバをご使用の Cisco Expressway-C サーバコンフィギュレーションにある HTTP サーバの許可リストに追加する必要があります。HTTP サーバ許可リストにより、クライアントは社内ネットワーク内の Web サービスへのアクセスが可能になります。
- すべての連絡先写真は、UdsPhotoUriWithToken の値として指定した URL の形式に従っている必要があります。

## 連絡先の写真の形式と寸法

Cisco Jabber で最適な結果を得るには、連絡先の写真は特定の形式と大きさが必要です。サポートされるフォーマットと最適な寸法を確認してください。連絡先の写真にクライアントが行う調整について説明します。

### 関連トピック

[連絡先の写真のパラメータ](#), (202 ページ)

## 連絡先写真の形式

Cisco Jabber では、ディレクトリ内の連絡先写真について次の形式をサポートしています。

- JPG
- PNG
- BMP
- GIF



### 重要

Cisco Jabber では、GIF 形式の連絡先写真のレンダリングを向上させるための変更は適用されません。その結果、GIF 形式の連絡先写真が不正にレンダリングされたり最適な品質にならない場合があります。最適な品質を得るには、連絡先の写真として PNG 形式を使用する必要があります。

## 連絡先写真の寸法



### ヒント

連絡先写真の最適な寸法は、アスペクト比 1:1 の 128 x 128 ピクセルです。

128 ピクセル x 128 ピクセルは、Microsoft Outlook のローカル連絡先の写真の最大寸法です。

次の表に、Cisco Jabber での連絡先写真のさまざまな寸法を示します。

| 参照先                                                                                                                                | 寸法             |
|------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 音声コール ウィンドウ                                                                                                                        | 128 x 128 ピクセル |
| 次のような招待やリマインダ <ul style="list-style-type: none"> <li>• 着信コール ウィンドウ</li> <li>• 会議リマインダ ウィンドウ</li> </ul>                             | 64 x 64 ピクセル   |
| 次のような連絡先のリスト <ul style="list-style-type: none"> <li>• 連絡先リスト</li> <li>• 参加者リスト</li> <li>• コール履歴</li> <li>• ボイスメール メッセージ</li> </ul> | 32 x 32 ピクセル   |

## 連絡先写真の調整

Cisco Jabber で、次のように連絡先写真を調整します。

### サイズ変更

ディレクトリ内の連絡先写真が 128 x 128 ピクセル以外のサイズである場合、クライアントによって写真のサイズが自動的に変更されます。たとえば、ディレクトリ内の連絡先写真が 64 x 64 ピクセルであるとしします。Cisco Jabber でディレクトリから連絡先写真を取得すると、その写真のサイズが 128 x 128 ピクセルに変更されます。



#### ヒント

連絡先写真のサイズ変更により、最適な解像度が得られない場合があります。このため、クライアントによって連絡先写真のサイズが自動的に変更されないように、128 x 128 ピクセルの連絡先写真を使用してください。

### トリミング

Cisco Jabber では、四角形以外の写真を四角形のアスペクト比（つまり、幅が高さと同じアスペクト比 1:1）に自動的にトリミングします。

#### 縦方向

ディレクトリ内の連絡先写真が縦方向である場合、クライアントで上端から 30%、下端から 70% をトリミングします。

たとえば、ディレクトリ内の連絡先写真が幅 100 ピクセル、高さ 200 ピクセルである場合、アスペクト比が 1:1 となるように Cisco Jabber で高さから 100 ピクセルをトリミングする必要があります。この場合、クライアントで写真の上端から 30 ピクセルを、写真の下端から 70 ピクセルをトリミングします。

#### 横方向

ディレクトリ内の連絡先写真が横方向である場合、クライアントで両方の側から 50% をトリミングします。

たとえば、ディレクトリ内の連絡先写真が幅 200 ピクセル、高さ 100 ピクセルである場合、アスペクト比が 1:1 となるように Cisco Jabber で幅から 100 ピクセルをトリミングする必要があります。この場合、クライアントで写真の右側から 50 ピクセルを、写真の左側から 50 ピクセルをトリミングします。

### 丸め

Cisco Jabber では、ディレクトリから連絡先写真を取得した後、それらの写真の角を丸めます。

## ディレクトリ サーバの設定例

ここでは、サポートされている統合シナリオについて説明し、設定例を示します。

### ドメインコントローラの接続

ドメイン コントローラ に接続するには、次のパラメータを設定します。

| パラメータ          | 値 |
|----------------|---|
| ConnectionType | 1 |

設定例を次に示します。

```
<Directory>
 <ConnectionType>1</ConnectionType>
</Directory>
```

### 手動サーバ接続

手動でディレクトリ サーバに接続するには、次のパラメータを設定します。

パラメータ	値
PrimaryServerName	FQDN IP アドレス
ServerPort1	ポート番号
SecondaryServerName	FQDN IP アドレス
ServerPort2	ポート番号

設定例を次に示します。

```
<Directory>
 <PrimaryServerName>primary-server-name.domain.com</PrimaryServerName>
 <ServerPort1>1234</ServerPort1>
 <SecondaryServerName>secondary-server-name.domain.com</SecondaryServerName>
 <ServerPort2>5678</ServerPort2>
</Directory>
```

### UDS の統合

UDS と統合するには、次のパラメータを設定します。

パラメータ	値
DirectoryServerType	UDS



パラメータ	値
UdsServer	UDS サーバの IP アドレス
UdsPhotoUriWithToken	連絡先写真 URL
PresenceDomain (注) このパラメータを使用するのは、 電話機モードだけです。	既存ドメインのサーバアドレス



- (注) すべての連絡先（企業ファイアウォール内外）の解決に UDS を使用する場合にはのみ、DirectoryServerType パラメータを UDS に設定する必要があります。

設定例を次に示します。

```
<Directory>
 <DirectoryServerType>UDS</DirectoryServerType>
 <UdsServer>11.22.33.444</UdsServer>
 <UdsPhotoUriWithToken>http://server-name/%%uid%.jpg</UdsPhotoUriWithToken>
</Directory>
```

## Expressway for Mobile and Remote Access の LDAP 統合

LDAP ディレクトリを使用して Expressway Mobile and Remote Access を展開する場合、クライアントは次のものを使用します。

- 企業ファイアウォール内では LDAP
- 企業ファイアウォール外では UDS



- (注) LDAP はデフォルト設定であるため、クライアント コンフィギュレーション ファイルに DirectoryServerType パラメータを含める必要はありません。

クライアントが企業ファイアウォールの内側でも外側でも連絡先写真を解決できるよう、次のパラメータを設定します。

パラメータ	値
PhotoUriWithToken	企業ファイアウォール内での連絡先写真 URL
UdsPhotoUriWithToken	企業ファイアウォール外での連絡先写真 URL

設定例を次に示します。

```
<Directory>
 <PhotoUriWithToken>http://staffphoto.example.com/SAMAccountName.jpg
 </PhotoUriWithToken>
 <UdsPhotoUriWithToken>http://server-name/%%uid%.jpg</UdsPhotoUriWithToken>
</Directory>
```

## Simple Authentication

単純認証により、次の設定例の場合、簡易バインドを使用してディレクトリ サーバに接続することができます。

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>0</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

この設定は、クライアントが次であることを示しています。

- Microsoft Windows クレデンシャルを使用しない。
- SSL を使用しない。
- 単純認証を使用している。
- カスタム クレデンシャルを使用している。

簡易バインドの結果として、クライアントはプレーンテキストでバインド要求ペイロードのクレデンシャルを送信します。

## SSL の Simple Authentication

UseSSL パラメータでディレクトリ サーバ接続の SSL を有効にします。単純認証を使用する際に、次の設定例の場合、クレデンシャルを暗号化するために SSL を使用できます。

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>1</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

この設定は、クライアントが次であることを示しています。

- Microsoft Windows クレデンシャルを使用しない。
- SSL を使用している。
- 単純認証を使用している。
- カスタム クレデンシャルを使用している。

その結果、クライアントは、クライアント構成のクレデンシャルを暗号化するために、SSL を使用します。

## OpenLDAP の統合

匿名バインドまたは認証されたバインドを使用して、OpenLDAP と統合できます。

### 匿名バインド

匿名のバインドを使用して、OpenLDAP と統合するには、次のパラメータを設定します。

パラメータ	値
ConnectionType	1
PrimaryServerName	IP アドレス ホスト名
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	ディレクトリ サービスまたは組織単位 (OU) のルート
UserAccountName	uid または cn などの固有識別子
BaseFilter	ディレクトリ サービスが使用するオブジェクトクラス (inetOrgPerson など)。
PredictiveSearchFilter	uid または他の検索フィルタ

設定例を次に示します。

```
<Directory>
 <ConnectionType>1</ConnectionType>
 <PrimaryServerName>11.22.33.456</PrimaryServerName>
 <UseWindowsCredentials>0</UseWindowsCredentials>
 <UseSecureConnection>1</UseSecureConnection>
 <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
 <UserAccountName>uid</UserAccountName>
 <BaseFilter>(& (objectClass=inetOrgPerson))</BaseFilter>
 <PredictiveSearchFilter>uid</PredictiveSearchFilter>
</Directory>
```

## 認証済みバインド

認証済みバインドを使用して、OpenLDAP と統合するには、次のパラメータを設定します。

パラメータ	値
ConnectionType	1
PrimaryServerName	IP アドレス ホスト名
UseWindowsCredentials	0
UseSecureConnection	0
SearchBase1	ディレクトリ サービスまたは組織単位 (OU) のルート
UserAccountName	uid または cn などの固有識別子
BaseFilter	ディレクトリ サービスが使用するオブジェクトクラス (inetOrgPerson など)。

パラメータ	値
PredictiveSearchFilter	uid または他の検索フィルタ
ConnectionUsername	ユーザ名
ConnectionPassword	パスワード

設定例を次に示します。

```
<Directory>
 <ConnectionType>1</ConnectionType>
 <PrimaryServerName>11.22.33.456</PrimaryServerName>
 <UseWindowsCredentials>0</UseWindowsCredentials>
 <UseSecureConnection>0</UseSecureConnection>
 <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
 <UserAccountName>uid</UserAccountName>
 <BaseFilter>(& (objectClass=inetOrgPerson))</BaseFilter>
 <PredictiveSearchFilter>uid</PredictiveSearchFilter>
 <ConnectionUsername>cn=lds-read-only-user,dc=cisco,dc=com</ConnectionUsername>
 <ConnectionPassword>password</ConnectionPassword>
</Directory>
```

## AD LDS の統合

特定の設定を使用して、AD LDS または ADAM と統合できます。

### 匿名バインド

匿名のバインドを使用して、AD LDS または ADAM と統合するには、次のパラメータを設定します。

パラメータ	値
PrimaryServerName	IP アドレス ホスト名
ServerPort1	ポート番号
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	ディレクトリ サービスまたは組織単位 (OU) の ルート

設定例を次に示します。

```
<Directory>
 <PrimaryServerName>11.22.33.456</PrimaryServerName>
 <ServerPort1>50000</ServerPort1>
 <UseWindowsCredentials>0</UseWindowsCredentials>
 <UseSecureConnection>1</UseSecureConnection>
 <SearchBase1>dc=adam,dc=test</SearchBase1>
</Directory>
```

## Windows のプリンシパル ユーザ認証

Microsoft Windows プリンシパル ユーザと認証を使用して、AD LDS または ADAM と統合するには、次のパラメータを設定します。

パラメータ	値
PrimaryServerName	IP アドレス ホスト名
ServerPort1	ポート番号
UseWindowsCredentials	0
UseSecureConnection	1
ConnectionUsername	ユーザ名
ConnectionPassword	パスワード
UserAccountName	uid または cn などの固有識別子
SearchBase1	ディレクトリ サービスまたは組織単位 (OU) のルート

設定例を次に示します。

```
<Directory>
 <PrimaryServerName>11.22.33.456</PrimaryServerName>
 <ServerPort1>50000</ServerPort1>
 <UseWindowsCredentials>0</UseWindowsCredentials>
 <UseSecureConnection>1</UseSecureConnection>
 <ConnectionUsername>cn=adminstrator,dc=cisco,dc=com</ConnectionUsername>
 <ConnectionPassword>password</ConnectionPassword>
 <UserAccountName>cn</UserAccountName>
 <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```

## AD LDS のプリンシパルのユーザ認証

AD LDS プリンシパル ユーザと認証を使用して、AD LDS または ADAM と統合するには、次のパラメータを設定します。

パラメータ	値
PrimaryServerName	IP アドレス ホスト名
ServerPort1	ポート番号
UseWindowsCredentials	0
UseSecureConnection	0
ConnectionUsername	ユーザ名

パラメータ	値
ConnectionPassword	パスワード
UserAccountName	uid または cn などの固有識別子
SearchBase1	ディレクトリ サービスまたは組織単位 (OU) のルート

設定例を次に示します。

```
<Directory>
 <PrimaryServerName>11.22.33.456</PrimaryServerName>
 <ServerPort1>50000</ServerPort1>
 <UseWindowsCredentials>0</UseWindowsCredentials>
 <UseSecureConnection>0</UseSecureConnection>
 <ConnectionUsername>cn=administrator,dc=cisco,dc=com</ConnectionUsername>
 <ConnectionPassword>password</ConnectionPassword>
 <UserAccountName>cn</UserAccountName>
 <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```

## フェデレーション

フェデレーションによりは、Cisco Jabber ユーザは異なるシステムでプロビジョニングされるユーザと Cisco Jabber 以外のクライアントアプリケーションを使用するユーザと通信することができます。

## ドメイン間フェデレーション

ドメイン間フェデレーションでは、エンタープライズドメイン内の Cisco Jabber ユーザは、他のドメイン内のユーザとアベイラビリティを共有し、それらのユーザにインスタントメッセージを送信できます。

- Cisco Jabber ユーザは、他のドメインの連絡先を手動で入力する必要があります。
- Cisco Jabber では、次とのフェデレーションがサポートされています。
  - Microsoft Office Communications Server
  - Microsoft Lync
  - IBM Sametime
  - XMPP 標準ベース環境 (Google Talk など)
  - AOL Instant Messenger

Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence Service 上に Cisco Jabber のドメイン間フェデレーションを設定します。詳細については、該当するサーバのマニュアルを参照してください。

## 関連トピック

[Integration Guide for Configuring Cisco Unified Presence Release 8.6 for Interdomain Federation](#)  
[『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

ドメイン内フェデレーションでは、同じドメイン内のユーザはアベイラビリティを共有し、Cisco Unified Presence と Microsoft Office Communications Server、Microsoft Live Communications Server、または他のプレゼンス サーバ間でインスタント メッセージを送信できます。

ドメイン内フェデレーションを使用すると、ユーザを別のプレゼンス サーバから Cisco Unified Presence または Cisco Unified Communications IM and Presence に移行できます。このため、プレゼンス サーバ上で Cisco Jabber のドメイン内フェデレーションを設定します。詳細については、次のマニュアルを参照してください。

- Cisco Unified Presence : 『*Integration Guide for Configuring Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6 and Microsoft LCS/OCS*』
- Cisco Unified Communications IM and Presence : 『*Partitioned Intradomain 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設定

プレゼンス サーバでのドメイン内フェデレーションの設定に加えて、Cisco Jabber コンフィギュレーション ファイルでいくつかの設定が必要になる場合があります。

連絡先の検索時に連絡先を解決したり、ディレクトリから連絡先情報を取得したりするには、Cisco Jabber で各ユーザの連絡先 ID が必要です。Cisco Unified Presence では、Microsoft Office Communications Server、Microsoft Live Communications Server などの他のプレゼンス サーバの形式と常に一致するとは限らない連絡先情報を解決するために特定の形式を使用します。

## 手順

- 
- ステップ 1** UseSIPURIToResolveContacts パラメータの値を true に設定します。
- ステップ 2** Cisco Jabber で使用する連絡先 ID が含まれている属性を指定し、連絡先情報を SipUri パラメータの値として取得します。デフォルト値は msRTCSIP-PrimaryUserAddress です。

(注) イントラドメイン フェデレーションを展開し、クライアントがファイアウォールの外から Expressway Mobile and Remote Access に接続する場合、連絡先の検索は、コンタクト ID が次のいずれかのフォーマットを使用している場合にのみサポートされます。

- sAMAccountName@domain
- UserPrincipalName (UPN) @domain
- EmailAddress@domain
- employeeNumber@domain
- telephoneNumber@domain

**ステップ 3** 各連絡先 ID のプレフィックスとなるテキストを UriPrefix パラメータの値として設定します。プレフィックスとは、連絡先 ID のユーザ名の前にあるテキストです。

たとえば、msRTCSIP-PrimaryUserAddress を SipUri の値として指定します。ディレクトリにおける各ユーザの msRTCSIP-PrimaryUserAddress の値は、sip:username@domain の形式になります。

次の XML スニペットに、設定の例を示します。

```
<Directory>
 <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
 <SipUri>non-default-attribute</SipUri>
 <UriPrefix>sip:</UriPrefix>
</Directory>
```

## ドメイン内フェデレーションの例

このトピックでは、SipUri、UseSIPURIToResolveContacts、およびUriPrefix の各パラメータを使用したドメイン内フェデレーションの連絡先を解決する例について説明します。

この例では、次のように設定されています。

- SipUri パラメータの値は msRTCSIP-PrimaryUserAddress です。
- UseSIPURIToResolveContacts パラメータの値は true です。
- UriPrefix パラメータの値は sip: です。
- ディレクトリには、Mary Smith という名前のユーザの msRTCSIP-PrimaryUserAddress 属性の値として sip:msmith@domain.com が含まれています。



### Cisco Jabber によるディレクトリに接続した連絡先情報の解決

- 1 プレゼンス サーバが msmith@domain.com を Cisco Jabber に渡します。
- 2 Cisco Jabber により、sip: が msmith@domain.com に付加されてから、ディレクトリへのクエリーが実行されます。
- 3 sip:msmith@domain.com が msRTCSIP-PrimaryUserAddress 属性の値と一致します。
- 4 Cisco Jabber により、Mary Smith の連絡先情報が取得されます。

### Cisco Jabber による Mary Smith の検索

Cisco Jabber により、sip:msmith@domain.com から sip: のプレフィックスが削除され、msmith@domain.com の連絡先 ID が取得されます。





## 第 9 章

# Cisco Jabber for Windows のカスタマイズ

インストール後にカスタマイズできる機能を確認します。組織の要件を満たすようにこれらの機能をカスタマイズする方法について学習します。

- [カスタム顔文字の追加, 223 ページ](#)
- [カスタム埋め込みタブの作成, 227 ページ](#)

## カスタム顔文字の追加

カスタム顔文字を Cisco Jabber for Windows に追加するには、XML ファイルで顔文字の定義を作成し、ファイル システムに保存します。



(注) 最適な結果を得るには、カスタム顔文字は、次のガイドラインに準拠する必要があります。

- 寸法 : 17 x 17 ピクセル
- トランスペアレント背景
- PNG ファイル形式
- RGB カラー

### 手順

- ステップ 1** 任意のテキストエディタを使用して `emoticonDefs.xml` という名前のファイルを作成します。
- ステップ 2** 必要に応じて、`emoticonDefs.xml` で顔文字の定義を指定します。  
`emoticonDefs.xml` の構造および有効なパラメータの詳細については、「顔文字の定義」を参照してください。

**ステップ 3** emoticonDefs.xml を保存して閉じます。

**ステップ 4** ファイル システムの適切なディレクトリに emoticonDefs.xml を保存します。  
Cisco Jabber for Windows によって、ファイルシステムの次のディレクトリから顔文字の定義がロードされます。

**Program Files\Cisco Systems\Cisco Jabber\Emoticons**

このフォルダには、Cisco Jabber for Windows のデフォルトの顔文字とデフォルトの emoticonDefs.xml が格納されています。

**Program Files\Cisco Systems\Cisco Jabber\CustomEmoticons**

デフォルトでは、このフォルダは存在しません。管理者は、このフォルダを作成してカスタム顔文字の定義を格納し、組織展開に含めることができます。

CustomEmoticons フォルダで定義した顔文字は、デフォルトの Emoticons フォルダの顔文字の定義よりも優先されます。

**%USERPROFILE%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\CustomEmoticons**

このフォルダには、Cisco Jabber for Windows の個々のインスタンスのカスタム顔文字の定義が格納されます。

このディレクトリで定義した顔文字は、インストール ディレクトリの CustomEmoticons フォルダの顔文字の定義よりも優先されます。

**ステップ 5** Cisco Jabber for Windows を再起動します。

---

Cisco Jabber for Windows によって、emoticonDefs.xml のカスタム顔文字の定義がロードされます。



**メモ**

ユーザは、カスタム顔文字の定義が emoticonDefs.xml でローカルに定義されている場合にのみ、それらの定義を利用することができます。顔文字の定義が異なるユーザにカスタム顔文字を送信すると、それらのユーザはアイコンではなく、デフォルト キーを受信します。次に例を示します。

- 1 ユーザ A は emoticonDefs.xml でカスタム顔文字を定義します。  
カスタム顔文字の定義は、ユーザ A のローカル ファイル システムにのみ存在します。
  - 2 ユーザ A はそのカスタム顔文字をユーザ B に送信します。
  - 3 ユーザ B はカスタム顔文字のデフォルト キーのみを受信します。ユーザ B はアイコンを受信しません。
-

## 顔文字の定義

Cisco Jabber for Windows では、emoticonDefs.xml から顔文字の定義をロードします。

次の XML の抜粋は、顔文字の定義ファイルの基本構造を示します。

```
<emoticons>
 <emoticon defaultKey="" image="" text="" order="" hidden="">
 <alt></alt>
 </emoticon>
</emoticons>
```

次の表に、カスタム顔文字を定義するための要素および属性を示します。

要素または属性	説明
emoticons	この要素には、すべての顔文字の定義が含まれます。
emoticon	この要素には、1 つの顔文字の定義が含まれます。
defaultKey	この属性により、顔文字を描画するデフォルト キーの組み合わせが定義されます。 値として任意のキーの組み合わせを指定します。 この属性は必須です。 defaultKey は emoticon 要素の属性です。
image	この属性では、顔文字イメージのファイルを指定します。 値として顔文字のファイル名を指定します。顔文字イメージは、emoticonDefs.xml と同じディレクトリに存在する必要があります。 この属性は必須です。 Cisco Jabber for Windows では、Internet Explorer で描画可能なアイコン（.jpeg、.png、.gif など）をサポートしています。 image は emoticon 要素の属性です。
text	この属性では、[顔文字の挿入（Insert emoticon）] ダイアログボックスに表示される説明文を定義します。 任意の Unicode 文字の文字列を指定します。 この属性はオプションです。 text は emoticon 要素の属性です。

要素または属性	説明
order	<p>この属性では、[顔文字の挿入 (Insert emoticon) ] ダイアログボックスに顔文字が表示される順序を定義します。</p> <p>値として 1 から始まる序数を指定します。</p> <p>order は emoticon 要素の属性です。</p> <p>この属性は必須です。ただし、hidden の値が true である場合、このパラメータは有効になりません。</p>
hidden	<p>この属性では、[顔文字の挿入 (Insert emoticon) ] ダイアログボックスに顔文字が表示されるかどうかを指定します。</p> <p>値として次のいずれかを指定します。</p> <p><b>true</b></p> <p>[顔文字の挿入 (Insert emoticon) ] ダイアログボックスに顔文字が表示されないことを指定します。ユーザは、顔文字を描画するキーの組み合わせを入力する必要があります。</p> <p><b>false</b></p> <p>[顔文字の挿入 (Insert emoticon) ] ダイアログボックスに顔文字が表示されることを指定します。ユーザは、[顔文字の挿入 (Insert emoticon) ] ダイアログボックスから顔文字を選択するか、顔文字を描画するキーの組み合わせを入力することができます。これがデフォルト値です。</p> <p>この属性はオプションです。</p> <p>hidden は emoticon 要素の属性です。</p>
alt	<p>この要素を使用すると、キーの組み合わせを顔文字にマッピングできます。</p> <p>値として任意のキーの組み合わせを指定します。</p> <p>たとえば、defaultKey の値が :) である場合、alt の値として :-) を指定し、両方のキーの組み合わせで同じ顔文字を描画できるようにします。</p> <p>この要素はオプションです。</p>

**メモ**

デフォルトの顔文字の定義ファイルには、ユーザが他のユーザからコールを要求できる次のキーの組み合わせが含まれています。

- :callme
- :telephone

これらのキーの組み合わせによって、callme の顔文字、または communicon が送信されます。この顔文字を受信したユーザは、アイコンをクリックして音声コールを開始できます。任意のカスタム顔文字の定義ファイルにこれらのキーの組み合わせを含めて、callme の顔文字を有効にします。

**顔文字の定義の例**

```
<emoticons>
 <emoticon defaultKey=":)" image="Emoticons_Smiling.png" text="Smile" order="1">
 <alt>:-)</alt>
 <alt>^_^</alt>
 </emoticon>
 <emoticon defaultKey=":(" image="Emoticons_Frowning.png" text="Frown" order="2">
 <alt>:-(</alt>
 </emoticon>
</emoticons>
```

## カスタム埋め込みタブの作成

クライアントインターフェイスのHTMLコンテンツを表示するカスタム埋め込みタブを作成します。

クライアントコンフィギュレーションファイルの一部として、カスタム埋め込みタブを定義します。詳細については、「カスタム埋め込みタブ」を参照してください。

**関連トピック**

[カスタム埋め込みタブ, \(164 ページ\)](#)







## 第 10 章

### 付録

Cisco Jabber for Windows の展開やトラブルシューティングを支援するその他の情報を確認します。

- [Unified Communications Server インフラストラクチャの移行, 229 ページ](#)
- [ADSI のエラー コード, 232 ページ](#)

## Unified Communications Server インフラストラクチャの移行

統合された通信インフラストラクチャを移行するには、Cisco Unified Presence バージョン 8.x から Cisco Unified Communications Manager IM and Presence Service バージョン 9.x 以降にプレゼンス サーバをアップグレードします。また、Cisco Unified Communications Manager バージョン 8.x からバージョン 9.x 以降にアップグレードします。

移行作業を開始する前に、サーバのバージョンにおけるアーキテクチャの相違点と、この変更がクライアントにどのように影響を与えるかを理解しておく必要があります。

### サーバのインフラストラクチャの相違点

正常な移行の鍵は、サーバのインフラストラクチャの相違点、および、これらの相違点がクライアントにどのように影響するかを理解することです。

#### バージョン 8.x サーバのインフラストラクチャ

バージョン 8.x サーバのインフラストラクチャでは、Cisco Unified Presence は、認証と設定におけるプライマリ ソースです。

サービスでユーザをプロビジョニングし、TFTP、CCMCIP サービスなどを含むサーバのロケーションを Cisco Unified Presence で取得します。これらの詳細は、サーバデータベースに存在しています。クライアントが \_cuplogin SRV レコードから Cisco Unified Presence のロケーションを

取得する場合、クライアントはユーザを認証し、Cisco Unified Presence のインターフェイスを通じて、データベースから詳細を取得します。このように、クライアントは、ユーザがログインした後で、プレゼンス サーバから設定とサービスを取得します。

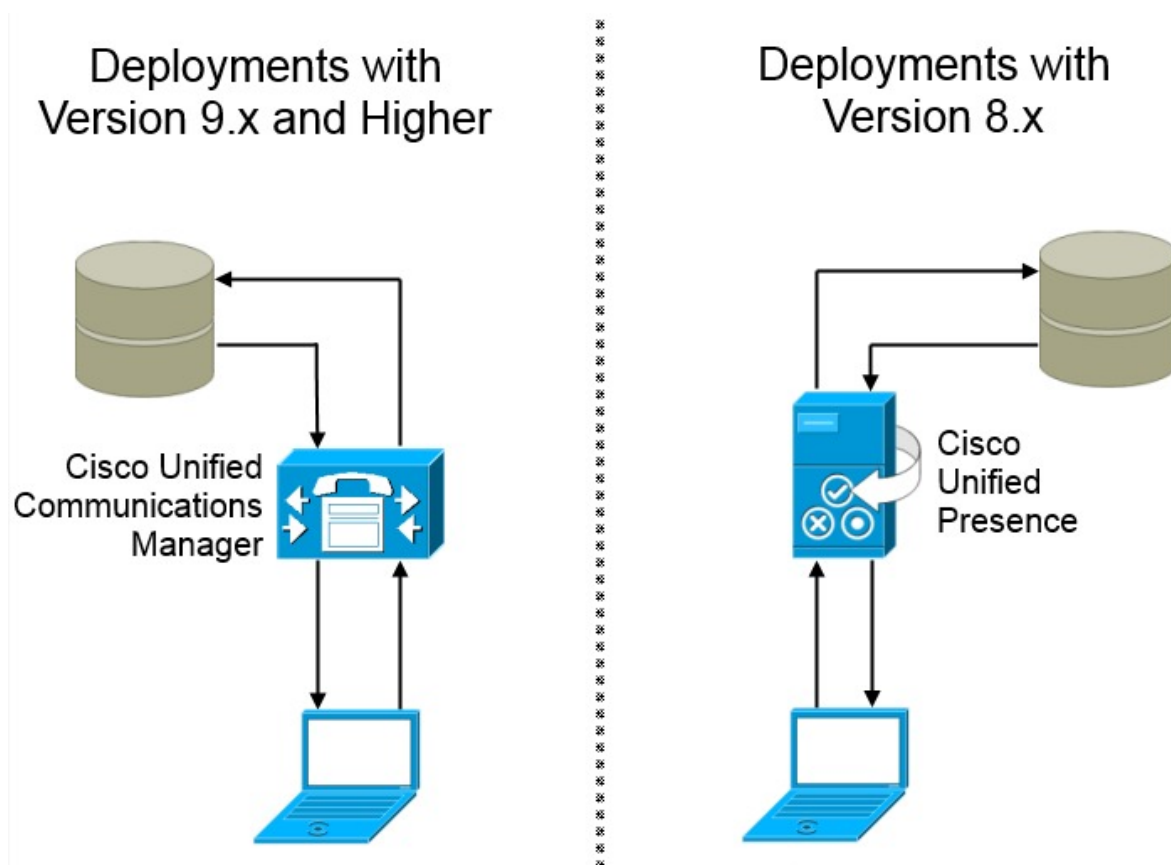
### バージョン 9.x サーバのインフラストラクチャ

バージョン 9.x サーバのインフラストラクチャでは、Cisco Unified Communications Manager がユーザの主な構成のソースです。

は、ユーザ、グループ、またはクラスタに適用されるサービス プロファイルの Cisco Unified Communications Manager で設定を定義します。この設定では、ユーザや他のクライアントの特定の設定をプロビジョニングするサービスのロケーションを保持します。これらの詳細は、サーバ データベースに存在しています。クライアントが `_cisco-uds` SRV レコードを取得すると、ユーザのホーム クラスタを検出できます。クライアントは、TFTP と CCMCIP サービスを検出し、ユーザに設定されたデバイスを手入し、設定されたデバイスを登録できます。クライアントはまた、追加サービスの設定およびクライアント設定を含むサービス プロファイルを取得します。

クライアントがサービス プロファイルを取得した後で、ユーザがログインするオーセンティケータを確定することができます。

次の図は、バージョン 8.x インフラストラクチャとバージョン 9.x インフラストラクチャの違いを示しています。



380622

### サーバインフラストラクチャの相違点の概要

次の図は、バージョン 8.x インフラストラクチャとバージョン 9.x インフラストラクチャの主な相違点を強調しています。

バージョン 8.x サーバのインフラストラクチャ	バージョン 9.x のインフラストラクチャ
_cuplogin SRV レコードを配置します。	_cisco-uds SRV レコードを配置します。
クライアントは、Cisco Unified Presence から設定を取得します。	クライアントは、Cisco Unified Communications Manager から設定を取得します。
Cisco Unified Presence は、認証の主なプライマリ ソースです。	<p>Cisco Unified Communications Manager は、認証の主なプライマリ ソースです。</p> <p>クライアントがサービスプロファイルを取得したら、次のいずれのオーセンティケータのユーザがログインする必要があるかを決定します。</p> <p><b>Cisco Unified Communications Manager IM and Presence Service</b></p> <p>フル UC と IM 導入のみ。</p> <p><b>Cisco Unified Communications Manager</b></p> <p>電話モードの導入。</p> <p><b>Cisco WebEx サービス</b></p> <p>クラウドベースの導入。</p>
クライアント コンフィギュレーション ファイルのディレクトリ統合と追加クライアント設定を設定する必要があります。	サービスプロファイルでディレクトリ統合といくつかのクライアント設定を設定することができます。
TFTP および CCMCIP サービスのテレフォニー機能を持つユーザをプロビジョニングします。	<p>クライアントは、ユーザのホーム クラスタを確認したら、TFTP と UDS サービスを検出します。</p> <p><b>メモ</b> UDS は、Cisco Unified Communications Manager バージョン 9.x インフラストラクチャの CCMCIP に置き換えられます。CCMCIP プロファイルを持つユーザをプロビジョニングする必要はありません。</p>
クライアントは、デバイスの設定を取得し、ログイン後にデバイスの登録をします。	クライアントは、デバイスの設定を取得し、ログイン前にデバイスの登録をします。

## バージョン 8.x からバージョン 9.x 以降へのサーバのアップグレード

バージョン 8.x からバージョン 9.x 以降にサーバをアップグレードするために、段階的なアプローチを取る必要があります。まずサーバのインフラストラクチャをアップグレードし、現在のコンフィギュレーションをそのままにします。インフラストラクチャ全体のすべてのサーバをアップグレードした後、サービスプロファイルを Cisco Unified Presence から Cisco Unified Communications Manager に移行する必要があります。すべてのユーザに Cisco Unified Communications Manager バージョン 9.x のサービスプロファイルが存在する場合、\_cisco-uds SRV レコードを配置できます。

統合された通信サーバのインフラストラクチャを移行する手順は次のとおりです。

### 手順

- 
- ステップ 1**   サーバのインフラストラクチャをアップグレードします。  
クラスタの各ノードをアップグレードするために必要な手順を実行する必要があります。一度につきクラスタは 1 つです。  
すべてのクラスタ間でサーバをアップグレードするまでユーザの設定は現行のままにします。クライアントは、\_cuplogin SRV レコードを使用して、Cisco Unified Presence のサービスに関してユーザが定義する設定を含め、現在のコンフィギュレーションを Cisco Unified Communications Manager IM and Presence Service から取得できます。
- ステップ 2**   Cisco Unified Communications Manager のサービスプロファイルでユーザをプロビジョニングします。
- ステップ 3**   \_cisco-uds SRV レコードを配置します。  
導入において、すべてのユーザが正常にログインし、すべてのプロビジョニングサービスの取得を確認したら、\_cuplogin SRV レコードを取り除く必要があります。
- 

## ADSI のエラーコード

Cisco Jabber for Windows では、Microsoft Active Directory Service Interfaces (ADSI) を使用し、ディレクトリ統合を行います。ディレクトリ統合の問題をトラブルシューティングするには、ADSI エラーコードを参照してください。

ADSI エラーコードの詳細については、次の Microsoft ドキュメントを参照してください。

- *ADSI Error Codes* ([http://msdn.microsoft.com/en-us/library/windows/desktop/aa772195\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa772195(v=vs.85).aspx))
- *Generic ADSI Error Codes* ([http://msdn.microsoft.com/en-us/library/windows/desktop/aa705940\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa705940(v=vs.85).aspx))
- *ADSI 2.5 のエラーコード* (<http://support.microsoft.com/kb/242076>)