Cisco WebEx Messenger アドミニストレーション ガイド

初版：2015 年 03 月 05 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。

目 次

第 1 章

Cisco WebEx 管理ツール

概要

Cisco WebEx Messenger 管理ツールを使用すると、組織管理者は、Cisco WebEx へのユーザ アクセスをモニタ、管理、制御、および強化することができます。Cisco WebEx の管理者は組織管理者と呼ばれます。組織管理者は、Cisco WebEx ユーザが使用可能な機能を制御し、それらの機能の使用方法を決定します。

重要

Cisco WebEx Connect サービスは、Cisco WebEx Messenger に商標変更されました。Cisco WebEx 管理ツールは、この変更を反映するために近々更新されます。

クライアント アプリケーションは Cisco Jabber としてブランド化されています。

ここでは、Cisco WebEx Messenger 管理ツールを使用して迅速に作業を開始するためのタスクの概要について説明します。

（注）

シングル サインオンまたはディレクトリ統合が有効になっているお客様は、Cisco WebEx の担当者に連絡して、Cisco WebEx Messenger 管理ツールを起動して作業を開始するためのアシスタンスを受ける必要があります。

デスクトップ要件

以下に、次の Cisco WebEx アプリケーションをインストールして実行するために最低限必要な推奨のデスクトップ要件を示します。

Cisco Jabber for Windows

Cisco Jabberアプリケーションをインストールして実行するために最低限必要な推奨のデスクトップ要件については、Cisco Jabber Windows アプリケーションのマニュアル（http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html [英語]）を参照してください。

Cisco Jabber for Mac

Cisco Jabberアプリケーションをインストールして実行するために最低限必要な推奨のデスクトップ要件については、Cisco Jabber Mac アプリケーションのマニュアル（http://www.cisco.com/en/US/products/ps11764/prod_release_notes_list.html [英語]）を参照してください。

Cisco Jabber モバイル クライアント

Cisco Jabberアプリケーションをインストールして実行するために最低限必要な推奨のデスクトップ要件については、次の Cisco Jabber モバイル アプリケーションのマニュアルを参照してください。

- Cisco Jabber for iPhone and iPad：
  http://www.cisco.com/c/en/us/support/customer-collaboration/jabber-iphone-ipad/tsd-products-support-series-home.html [英語]
- Cisco Jabber for Android：
  http://www.cisco.com/c/en/us/support/unified-communications/jabber-android/tsd-products-support-series-home.html [英語]

ネットワークの要件

Cisco WebEx Messenger サービスにアクセスするために必要なネットワーク要件は次のとおりです。アプリケーション コンピュータにインターネット接続があり、次のホストとポートに接続できる必要があります。

注：Cisco WebEx Jabber アプリケーションは、Internet Explorer に設定されている Web プロキシ情報を使用して、アプリケーション設定サービスにアクセスします。お客様のネットワークのプロキシが認証済みプロキシの場合、そのプロキシは認証せずにこのURLにアクセスできるように適切に設定されています。

ドメイン

次のドメインに対して、ポート 80 および 443 を介した接続を開く必要があります。

- webex.com
- webexconnect.com
- それぞれのサブドメイン：*.webex.com および *.webexconnect.com。

  http://adium.im などのサードパーティの XMPP アプリケーションを使用する予定の場合は、ポート 5222 も開く必要があります。サードパーティの XMPP アプリケーションの使用の詳細については、サードパーティ XMPP IM アプリケーション サポート，（7 ページ）を参照してください。

証明書失効リスト（CRL）のドメイン

Cisco Jabber クライアントは、サーバへの TLS 接続を確立する際に、x509 CRL をチェックするか、または Online Certificate Status Protocol（OCSP）を使用します。これらのリストは、x509 証明書に組み込まれている次の URL アドレスから取得されます。これらの URL は証明書の発行局によって制御されます。

シスコは、これらの x509 証明書を定期的に更新し、通常のメンテナンスまたはセキュリティ上の懸念から認証局を変更し、事前の通知なく証明書および認証局を変更する権利を保有します。

以下は、ファイアウォールルールのホワイトリストに含める必要がある証明書プロバイダー ドメインの現在のリストです。

- *.verisign.com
- *.comodo.com
- *.usertrust.com
- *.cisco.com

IP 範囲

WebEx サービスは、次の IP アドレスの範囲で提供されます。

- 64.68.115.0 ～ 64.68.115.255
- 64.68.116.0 ～ 64.68.116.255
- 66.163.32.0 ～ 66.163.63.255
- 209.197.192.0 ～ 209.197.223.255
- 173.243.12.0 ～ 173.243.12.255（サブネット）

WebEx では新しい IP アドレスの取得や、IP アドレスの再割り当てが行われることがあるため、IP アドレスの範囲に基づいてアクセスを制限することは一般的に推奨されません。

Cisco WebEx からの通知を受信するには、mda.webex.com からの電子メールを許可するようにスパム フィルタを設定します。通常、通知には新しい Cisco WebEx アカウントに関する重要な情報、パスワードのリセットおよび同様の情報が含まれていて、電子メールを介してユーザに送信されます。

音声ビデオ ファイアウォールと帯域幅の要件

ここでは、Cisco WebEx Jabber アプリケーションから開始されるビデオ セッションに関する推奨ポートと帯域幅の要件について説明します。

P2P（ピアツーピア）とは、Jabber 間通話を行う機能を指します。

一般的に、音声およびビデオ機能は次のポートを介して提供されます。

項目	ポート タイプ	部品番号
A/V サーバ ポート	TCP	80 および 443
	UDP	5101
STUN サーバ	TCP	80
	UDP	8070/8090
P2P（ピアツーピア）ポート/音声およびビデオ メディア/Jabber 間通話	TCP	ランダム（未サポート）
	UDP	デフォルト 32434 ~ 33598（全範囲）

（注） Jabber 間通話用に別のポート範囲を選択する場合、Cisco WebEx Messenger 管理ツールでポート範囲を変更し、その変更に基づいて企業ネットワークのポートを開く必要があります。

WebEx Messenger 管理ツールにサインインして、[P2P（ピアツーピア）の設定（P2P Settings）]> [ポートの手動設定（Configure Ports Manually）] を選択します。

サーバ接続を確立するために、UDP ポート 5101 が使用されます。接続に失敗すると、接続を確立するためにポート 80/443 が使用されます。

Jabber 間通話では常に UDP ポートが使用され、デフォルトで TCP ポートに設定されることはありません。

Jabber 間通話、HTTP、URL に必要なホスト名の詳細については、以下を参照してください。 https://support.ciscospark.com/customer/en/portal/articles/1911657-firewall-and-network-requirements-for-the-cisco-spark-app

ビデオの帯域幅要件

解像度	Jabber 間通話の帯域幅	備考
90 p	0 ~ 120 kbps	重大なパケット損失が検出されると、追加の帯域幅が使用されることがあります。これで、損失パケットが補われます。
180 p	120 ~ 360 kbps	重大なパケット損失が検出されると、損失パケットを補うために追加の帯域幅が使用されることがあります。
360 p	360 ~ 1200 kbps	実際の解像度には 360 p、432 p、512 p があります。重大なパケット損失が検出されると、追加の帯域幅が使用されることがあります。これで、損失パケットが補われます。
720 p	1200 kbps ~ 2000 kbps	実際の解像度には 576 p と 720 p があります。重大なパケット損失が検出されると、追加の帯域幅が使用されることがあります。これで、損失パケットが補われます。

Jabber 間通話では Cisco Spark プラットフォームが活用されます。結果として、お客様は Jabber 間通話を使用するために、Cisco Media ハイブリッド サービスの UDP ポート範囲の設定を開く必要があります。Spark プラットフォームのネットワークおよびファイアウォールについては、以下を参照してください。 https://support.ciscospark.com/customer/en/portal/articles/1911657-firewall-and-network-requirements-for-the-cisco-spark-app?b_id=8722

Jabber 間通話を有効にしたいお客様は、Spark プラットフォームへのアクセスを制御する Cisco Common Identity システムと自分の組織を同期させる必要があります。詳細またはアシスタンスについては、Customer Success Manager にお問い合わせください。

WebEx と他の IM プロバイダー

Cisco WebEx Messenger は、AIM、IBM Lotus Sametime、Microsoft Lync、および GoogleTalk や Jabber.org などの XMPP ベースの IM ネットワークのような業界をリードするインスタント メッセージング プロバイダーのユーザと関連付けることができます。XMPP に基づいた公衆 IM ネットワークのリストは、XMPP Standards Foundation の Web サイトで確認できます（http://xmpp.org/services）。

XMPP ベースの IM ネットワークまたはまたは XMPP をサポートする IM ソリューションとのフェデレーション

Cisco WebEx と XMPP ベースのインスタント メッセージング ネットワークまたは XMPP をサポートする IM ソリューションとの間のフェデレーションには、DNS でのサービス（SRV）レコード

の公開が必要です。XMPP ベースの IM ネットワークの例には、Google Talk、Jabber.org などがあります。XMPP フェデレーションを有効にする方法の詳細については、「IM フェデレーション設定の指定」を参照してください。

次の例は、acme.com という組織で XMPP フェデレーションをプロビジョニングする方法を示します。

acme.com が外部ドメイン（Cisco WebEx Collaboration Cloud 内にないドメイン）とのフェデレーションを希望する場合、次のサービス（SRV）レコードを DNS で公開します。

```
_xmpp-server._tcp.acme.com. 86400 IN SRV 5 0 5269 s2s.acme.com.webexconnect.com
```

（注） ドメインの SRV レコードは、[設定（Configuration）]タブの [IM フェデレーション（IM Federation）]で確認できます。詳細については、「IM フェデレーション設定の指定」を参照してください。

XMPP フェデレーションを有効にするには、TCP ポート 5269 を開いておく必要があります。

DNS サーバの設定サンプル

次に、使用可能な各オプションに対する IM フェデレーション設定のサンプルを示します。

- SRV (Service):
- Service = _xmpp-server
- Protocol = _tcp
- Name = acme.com (domain name)
- Priority = 5
- Weight = 0
- Port = 5269
- Target = s2s.acme.com.webexconnect.com

フェデレーションの暗号化要求

暗号化が必要な場合、NextPlane サービスを使用することでのみ実現できます。

AOL の IM ネットワークとのフェデレーション

Cisco WebEx Messenger では、AOL の IM ネットワークと関連付けることができます。AOL の IM ネットワークとのフェデレーションをご希望の場合、Cisco WebEx のアカウント担当者にお問い合わせください。

IBM の Lotus Sametime とのフェデレーション

（注） Cisco WebEx Messenger と IBM Lotus Sametime の間のフェデレーションには、NextPlane フェデレーション サービスを使用することが推奨されます。

シスコでは IBM Lotus Sametime XMPP ゲートウェイをサポートしていません。これは、ゲートウェイに存在する多数の既知の問題と、シスコが他社製品をサポートできないことが原因です。

Microsoft Lync とのフェデレーション

（注） Cisco WebEx Messenger と Microsoft Lync の間のフェデレーションには、NextPlane フェデレーション サービスを使用することが推奨されます。

シスコでは Microsoft Lync XMPP ゲートウェイをサポートしていません。これは、ゲートウェイに存在する多数の既知の問題と、シスコが他社製品をサポートできないことが原因です。

サードパーティ XMPP IM アプリケーション サポート

Cisco Jabber for Windows アプリケーションの代わりに、XMPP をサポートするサードパーティ製アプリケーション（たとえば Pidgin for Linux）を基本的な IM 通信に使用できます。ただし、組織のポリシーはサードパーティ製 XMPP アプリケーションに適用できません。さらに、エンドツーエンド暗号化、デスクトップ共有、ビデオ コール、コンピュータ間コール、およびテレビ会議などの機能は、サードパーティ製のアプリケーションではサポートされていません。XMPP をサポートするサードパーティ製アプリケーションのリストは、http://xmpp.org/software/clients.shtml にある XMPP Standards Foundation の Web サイトから入手できます。

Cisco WebEx Messenger サービスでサードパーティ製アプリケーションを使用できるようにするには、Cisco WebEx 管理ツールの設定を有効にする必要があります。詳細については、「IM フェデレーション設定の指定」を参照してください。

また、サードパーティ製 XMPP アプリケーションが Cisco WebEx Collaboration Cloud を使用できるようにするには、DNS のサービス（SRV）レコードを発行する必要があります。たとえば、Cisco WebEx 組織である acme.com は、サードパーティ製 XMPP アプリケーションを使用できるようにするため、DNS の次の SRV レコードを公開します。

_xmpp-client._tcp.acme.com.86400 IN SRV 5 0 5222 c2s.acme.com.webexconnect.com

- ドメインの SRV レコードは、[設定（Configuration）] タブの [IM フェデレーション（IM Federation）] で確認できます。詳細については、IM フェデレーション設定, （58 ページ）を参照してください。
- サードパーティ製 XMPP アプリケーションの使用を有効にするには、TCP ポート 5222 も開いておく必要があります。

- Cisco WebEx 組織のユーザがドメインに接続するためにサードパーティ製 XMPP アプリケーションを使用している場合、ポリシーを適用することはできません。ポリシーは、Cisco Jabber クライアントを使用するユーザにのみ適用することができます。

管理ツールへのログイン

重要 Cisco WebEx Messenger 組織でシングル サインオン統合が有効な場合、Web ブラウザに入力する必要がある URL は次の形式である必要があります。
https://<WAPIserver>/wbxconnect/sso/acme.com/orgadmin.app acme.com はシングル サインオン統合が有効になっている Cisco WebEx Messenger 組織です。

手順

ステップ 1 ログインするには、http://www.webex.com/go/connectadmin に移動します。
[Cisco WebEx Messenger 管理ツール（Cisco WebEx Messenger Administration Tool）]ページが表示されます。

ステップ 2 [ユーザ名（Username）] と [パスワード（Password）] フィールドにログイン情報を入力します。

ステップ 3 サインインするたびにユーザ名を入力することを避けるには、[ユーザ名を保存（Remember Username）]を選択します。

ステップ 4 [サインイン（Sign In）]を選択します。

Cisco WebEx Messenger 管理ツール インターフェイス

Cisco WebEx Messenger 管理ツールには、以下のタブがあります。

タブ	説明
ユーザ（User）	ユーザ情報を追加および設定します。
設定（Configuration）	組織、ドメイン、パスワードの適用、ユーザプロビジョニング、IM の設定に関する一般的な情報、IM フェデレーション、IM のアーカイブ、ユニファイド コミュニケーションなどの追加サービスなど、Cisco WebEx のさまざまな機能の設定を行います。
ポリシー エディタ（Policy Editor）	ユーザのポリシーとルールを設定します。
グループ	グループ ポリシーを割り当てます。

タブ	説明
レポート	ユーザの使用状況レポートを表示します。
バージョン情報（About）	Cisco WebEx Messenger 管理ツールのバージョン情報を表示します。
ヘルプ	Cisco WebEx Messenger の管理者ガイドを表示します。

[管理ツール（Administrative Tools）]タブでは次の操作を実行できます。

- セルフ登録の有効化。
- Cisco WebEx ユーザに送信されるさまざまなシステム生成電子メールのカスタマイズ。
- 新規 Cisco WebEx ユーザの追加、およびユーザへのロールとグループの割り当て。
- パスワード要件の適用。
- カンマ区切り値（CSV）ファイルを介したユーザのインポートとエクスポート。
- ポリシーとポリシー アクションの定義と適用。

（注） ユーザ専用管理者が [組織管理（Organization Administration）] にサインインした場合、[ユーザ（User）]、[レポート（Report）]、[バージョン情報（About）]、[ヘルプ（Help）] タブのみ表示されます。

第 2 章

ユーザ管理

概要

[ユーザ（User）]タブを使用して、組織内のユーザを管理できます。一般的なユーザ管理タスクには、ユーザの検索、特定のユーザの詳細情報の表示、新規ユーザの作成、既存ユーザのアクティブ化と非アクティブ化、ユーザへのポリシー グループの割り当てが含まれます。[ユーザ（User）]タブは、組織管理者が Cisco WebEx Messenger にサインインしたときに表示されるデフォルトのタブです。次の図は、Cisco WebEx Messenger にサインインした後に表示される [ユーザ（Users）]タブのデフォルトの表示を示しています。

[ユーザ（User）]タブのデフォルトの表示には、常に表示される検索ボックス、Cisco WebEx Messenger 組織内のユーザの検索手順が含まれています。ツールバーには、Cisco WebEx Messenger 組織内のユーザに関する特定のタスクを実行するための追加オプションもあります。

[ユーザ（User）]タブには、複数のフィルタを使用した強力な検索機能があり、組織内の特定のユーザをすばやく簡単に見つけることができます。

ユーザと管理者の検索

手順

ステップ 1 ユーザまたは管理者を検索するには、[検索（Search）]ドロップダウンリストで適切な検索基準を選択します。利用可能な検索基準の詳細については、「関連項目」セクションを参照してください。

ステップ 2 選択した検索基準に応じて、対応する検索用語を入力します。たとえば、[すべてのユーザ（All Users）]を選択した場合、検索フィールドにユーザ名の少なくとも 1 文字を入力します。

ステップ 3 [検索（Search）]をクリックすると、検索基準と一致するユーザのリストが表示されます。

ステップ 4 検索結果に表示されるユーザが 1 ページに収まらない場合、**ページ**の下にある矢印アイコン（>> と <<）を使用して検索結果を移動します。

ステップ 5 アクティブ ユーザのリストを表示するには、まずCisco WebEx Messenger 組織のすべてのユーザをエクスポートし、次に Microsoft Excel またはお好きな CSV エディタでアクティブなユーザを確認する必要があります。ユーザをエクスポートする方法については、CSV ファイルを使用したユーザのインポートとエクスポート, （16 ページ）を参照してください。
アクティブ ユーザのみの検索は、現在サポートされていません。

関連トピック

検索条件, （12 ページ）

検索条件

フィルタを使用すると、任意の時点で表示されるユーザ レコードの数を制限することができます。次の表に、ユーザの検索に使用できるさまざまなフィルタを示します。

リスト対象	定義
すべてのユーザ（All Users）	ユーザの名前または姓の最初の文字を少なくとも 1 字入力します。名前がその文字に一致するアクティブなユーザ全員が検索結果に表示されます。
従業員 ID（Employee ID）	ユーザの正確な従業員 ID を入力します。この機能は、組織がディレクトリ統合組織として有効になっている場合のみ表示されます。
非アクティブなユーザ（Inactive Users）	[非アクティブなユーザ（Inactive Users）]を選択し、[検索（Search）]を選択するとすべての非アクティブなユーザが表示されます。検索結果を絞り込むには、ユーザの名前または姓の最初の文字を指定します。

リスト対象	定義
組織管理者（Organization Administrators）	このオプションを選択し、[実行（Go）]を選択すると、組織管理者権限のあるすべてのユーザが表示されます。
ユーザ管理者（User Administrators）	このオプションを選択し、[実行（Go）]を選択するとユーザ管理者権限のあるすべてのユーザが表示されます。
会議中のユーザ（Meeting Users）	このオプションは、Cisco WebEx Messenger 組織が Cisco WebEx Meeting アプリケーションと統合されたときのみ表示されます。 [会議中のユーザ（Meeting Users）]を選択し、[実行（Go）]を選択すると、Cisco WebEx Meeting アプリケーション アカウントを持つすべてのユーザが表示されます。この場合、Cisco WebEx Meeting アプリケーション アカウントを持たないユーザを検索することはできません。
記録ユーザ（Logged Users）	[記録ユーザ（Logged Users）]を選択し、[実行（Go）]を選択すると、アーカイブ用にIMセッションが記録されているすべてのユーザが表示されます。検索結果には、これらのユーザに関連付けられているアーカイブのエンドポイントも表示されます。

新規ユーザ

組織管理者は、**[ユーザ（User）]** タブから一度に 1 人ずつ新規ユーザを追加できます。新たに作成したユーザは、組織管理者が明示的に特定のグループに割り当てている場合を除き、必ずしもどこかのグループに属している必要はありません。新しいユーザのデフォルトのロールは、組織管理者が明示的に**組織管理者**ロールを割り当てていない限り、**メンバー**です。

組織管理者ロールは、最上位グループのメンバーであるユーザにのみ割り当てることができます。Cisco WebEx Messenger 組織の名前が付いた最上位グループは、プロビジョニング時に指定されます。一般的に、最上位グループの名前は、Cisco WebEx Messenger がプロビジョニングされている組織の名前で始まります。

組織管理者はユーザ専用管理者ロールを作成することができます。ユーザ管理者はユーザ管理関連の権限のみ持ちます。ユーザ管理者は新しい組織管理者を作成できません。

組織管理者はユーザ管理者のロールとプロファイルを更新できます。ユーザ管理者はユーザ管理関連の権限のみ持ちます。ユーザ管理者は組織管理者のロールを更新できませんが、名、姓、ビジネス メールなどの他のプロファイル情報は更新できます。

シングル サインオン（SSO）およびディレクトリ統合が有効になっている場合、ユーザの追加および編集のプロセスは異なります。SSO およびディレクトリ統合が有効になっている場合のユーザの追加の詳細については、シングル サインオンおよびディレクトリ統合のユーザ, （20 ページ）を参照してください。

組織管理者は、ユーザが自分のプロファイルを変更できるかどうかを決定できます。この決定には、ユーザが Cisco WebEx Messenger アプリケーション内から自分のプロファイル画像をアップロードできるかどうかの指定も含まれます。この場合、組織管理者は、企業データベースからユーザのプロファイル画像をアップロードできます。

ユーザ管理者ロールの主な目的は、ユーザ管理操作のみを実行できる管理者を設定することです。それらのユーザには、組織レベルで設定やポリシーの変更を行う権限はありません。また、ポリシー グループを作成または更新できる権限もありません。

新しいユーザの作成

手順

ステップ 1 新しいユーザや管理者を作成するには、[ユーザ（User）] > [追加（Add）] を選択します。

ステップ 2 各フィールドに適切な情報を入力します。デフォルトの [ロール（Role）] は [ユーザ（管理者以外）（User (non-administrator)）] です。

（注） [勤務先電子メール（Business Email）] が [ユーザ名（Username）] になります。[ユーザ名（Username）] は編集できません。

ステップ 3 （オプション）ユーザにポリシー グループを割り当てるには、[ポリシー グループの割り当て（Policy Group Assignment）]タブを選択します。ポリシー グループの指定の詳細については、ポリシー グループへのユーザの割り当て, （17 ページ）を参照してください。

ステップ 4 Cisco WebEx Messenger の組織に対して IM のアーカイブが有効になっている場合は、[ユーザの追加（Add User）]ダイアログ ボックスに [IM のアーカイブ（Archive IMs）]チェックボックスが表示されます。アーカイブを目的に、このユーザの IM をログに記録するには、[IM のアーカイブ（Archive IMs）]チェックボックスをオンにします。

[アーカイブ エンドポイント（Archiving endpoint）]の名前が表示されます。アーカイブ エンドポイントを設定するには、IM アーカイブの設定, （62 ページ）を参照してください。

ステップ 5 エンドポイントを変更するには、ドロップダウン リストから別のエンドポイントを選択します。アーカイブ エンドポイントは、Cisco WebEx Messenger 管理ツールの [IMアーカイブ（IM Archiving）] 画面で定義されています。[デフォルト（Default）]を選択すると、[IM のアーカイブ（IM Archiving）] 画面でデフォルトのエンドポイントとして事前に設定したエンドポイントがユーザに割り当てられます。詳細については、IM アーカイブの設定, （62 ページ）を参照してください。

ステップ 6 このユーザをアップグレード サイトに割り当てるには、[アップグレード サイト（Upgrade Site）] ドロップダウン リストからサイトを選択します。

アップグレード サイトの詳細については、アップグレード サイトの作成, （44 ページ）を参照してください。

ステップ 7 Cisco WebEx Messenger の組織が Cisco Unified Communications で有効になっている場合は、[ユーザの追加（Add User）] ダイアログ ボックスに [Unified Communications] タブが表示されます。Cisco Unified Communications で使用可能な設定を表示するには、[Unified Communications]タブを選択します。

ステップ 8 [クラスタ（Cluster）]で、このユーザに追加する適切な Cisco Unified Communications クラスタを選択します。

詳細については、Unified Communications クラスタの作成, （84 ページ）を参照してください。

ステップ 9 Cisco WebEx Messenger の組織が Cisco WebEx Meeting Center の統合で有効になっている場合は、[ユーザの追加（Add User）] ダイアログボックスが表示されます。組織管理者ロールをユーザに割り当てるには、[組織管理者（Organization Administrator）]チェックボックスをオンにします。

（注）
- [会議（Meetings）]ページの[新しいユーザの作成時に会議アカウントを自動的に有効にする（Automatically enable Meeting account when creating a new user）] を有効にしている場合は、[会議アカウント（Meeting Account）]チェックボックスがデフォルトで選択されます。このような場合、[会議アカウント（Meeting Account）] のチェックボックスをクリアすることはできません。詳細については、密結合統合のプロビジョニング, （49 ページ）を参照してください。
- [会議アカウント（Meeting Account）]チェックボックスを選択すると、このユーザに対応する Cisco WebEx Meeting Center アカウントが作成されます。

ステップ 10 [保存（Save）]を選択します。
Cisco WebEx Messenger 管理ツールのウェルカム電子メール テンプレートに基づいて新しいユーザにウェルカム電子メールが送信されます。

ステップ 11 上記のステップを繰り返し、新しいユーザの追加を続行します。

（注） 新しいユーザを追加するときに情報不足またはエラーが発生した場合、エラーは黄色で強調表示され、メッセージが表示されます。

ユーザと管理者の編集

組織管理者は、ユーザが割り当てられているポリシー グループの変更を含めて、既存のユーザのすべてのプロパティを編集できます。

手順

ステップ 1 ユーザまたは管理者を編集するには、[ユーザ（User）]タブで情報を編集するユーザを検索します。
ユーザを検索する方法については、ユーザと管理者の検索, （12 ページ）を参照してください。

ステップ 2 [編集（Edit）]を選択して [ユーザの編集（Edit User）] ダイアログボックスを開きます。
ユーザの既存の情報が表示されます。

ステップ 3 必要な変更を加えます。

ステップ 4 必要に応じて、[ロール（Role）]リストから [ユーザ管理者（User Administrator）] を選択します。

ステップ 5 [保存（Save）]を選択します。

（注） ユーザのパスワードをリセットするには、[ユーザ（Users）]タブでユーザを選択し、[パスワードのリセット（Reset Password）] アイコンを選択します。

CSVファイルを使用したユーザのインポートとエクスポート

カンマ区切り値（CSV）ファイルから、多数のユーザを Cisco WebEx Messenger の組織に簡単にインポートできます。同様に、CSVファイルにユーザをエクスポートすることもできます。インポートは、多数のユーザを組織に簡単に追加して、各ユーザを手動で追加する手間を省く上で、有効な方法です。

インポートが完了すると、インポートを開始した組織管理者にはインポートのステータスを通知する電子メールが届きます。この電子メールには、インポートが成功、失敗、または終了したかが記載されています。

CSV ファイルがインポートされると、[ユーザ（User）]タブにユーザが表示されます。CSV ファイル形式とサンプル ファイルの詳細については、CSV ファイル形式, （143 ページ）を参照してください。

（注） 最適な結果を得るためには、UTF-8 またはUTF-16LE エンコードスプレッドシートを使用します。

ユーザのインポートとエクスポート

手順

ステップ 1 CSV ファイルからユーザをインポートするには、Cisco WebEx Messenger 管理ツールで [ユーザ（User）] タブ > [その他の操作（More Actions）] > [インポート/エクスポート（Import/Export）] を選択します。

ステップ 2 [参照（Browse）]を選択し、インポートするユーザのリストが含まれている CSV ファイルを選択します。

ステップ 3 [インポート（Import）]を選択し、インポート プロセスを開始します。

ステップ 4 ユーザをエクスポートするには、[ユーザのインポート/エクスポート（Import/Export User）]ダイアログ ボックスの [エクスポート（Export）] を選択します。
進捗メッセージにエクスポート プロセスの進捗が表示されます。

ステップ 5 エクスポートされたユーザが含まれているCSVファイルを表示するには、エクスポートメッセージのタイム スタンプを選択します。
確認のプロンプトが表示されます。`Last export: 2009-06-24 09:02:01` のようなメッセージになります。

ステップ 6 [開く（Open）]を選択し、Messengerの組織のユーザが含まれているCSVファイルを表示します。または、[保存（Save）]を選択し CSV ファイルをローカル コンピュータに保存します。

ポリシー グループのユーザ

ポリシー グループにユーザを割り当てると、その特定のグループに適用されているすべてのポリシーがユーザに自動的に適用されます。ユーザごとに 1 つのポリシー グループだけを割り当てることができます。同じユーザに別のポリシー グループの割り当てを試みると、新しいポリシー グループが現在割り当てられているポリシー グループに置き換わります。新しいユーザと既存のユーザの両方に特定のポリシー グループを割り当てることができます。

また、ユーザ情報を含むCSVファイルをインポートすることで、グループに複数のユーザを追加できます。詳細については、CSV ファイルを使用したユーザのインポートとエクスポート，（16 ページ）を参照してください。

（注） デフォルトでは、ユーザはどのポリシー グループに割り当てられておらず、すべての Cisco WebEx Messenger 機能にアクセスできます。ユーザにポリシー グループを割り当てると、ユーザはそのポリシー グループに関連付けられているポリシーに影響を受けます。

ポリシーをグループに適用する方法の詳細については、グループへのポリシーの割り当て，（121 ページ）を参照してください。

ポリシー グループへのユーザの割り当て

手順

ステップ 1 ポリシー グループにユーザを割り当てるには、[ユーザ（User）]タブを選択します。

ステップ 2 新しいユーザにポリシー グループを割り当てる場合は、まず、[追加（Add）]を選択して新しいユーザを作成します。
新規ユーザの追加の詳細については、新規ユーザ，（13 ページ）を参照してください。

ステップ 3 既存のユーザにポリシー グループを割り当てるには、そのユーザを検索します。
ユーザを検索する方法については、ユーザと管理者の検索，（12 ページ）を参照してください。

ステップ 4 検索結果で、該当するユーザの名前をダブルクリックして [ユーザの編集（Edit User）]ダイアログ ボックスを開きます。

ステップ 5 [ポリシー グループの割り当て（Policy Group Assignment）]タブを選択して [ポリシー グループの割り当て（Policy Group Assignment）] ダイアログ ボックスを開きます。

ステップ 6 [検索（Search）]フィールドで、検索してこのユーザに割り当てるポリシー グループ名を 1 文字以上入力します。

ステップ 7 [検索（Search）]を選択します。

ステップ 8 [検索結果（Search Result）]ウィンドウで、該当するポリシー グループを選択し、[割り当て（Assign）] を選択してこのユーザにポリシーを割り当てます。

ステップ 9 [保存（Save）]を選択してポリシー グループの割り当てを保存し、[ユーザ（User）] タブに戻ります。

ユーザの非アクティブ化および再アクティブ化

ユーザを非アクティブ化する理由はさまざまです。たとえば退職やポリシー違反などがあります。ユーザを非アクティブ化しても Cisco WebEx Messenger システムから削除されることはありませんが、ユーザは無効になり、アカウントにログインできなくなります。必要に応じて、非アクティブ化したユーザを後で再アクティブ化できます。

（注） プライマリ管理者を非アクティブにすることはできません。

ユーザの非アクティブ化

手順

ステップ 1 ユーザを非アクティブにするには、[ユーザ（User）]タブで非アクティブにするユーザを検索します。
ユーザを検索する方法については、ユーザと管理者の検索, （12 ページ）を参照してください。

ステップ 2 非アクティブにするユーザを選択します。

ステップ 3 [その他の操作（More Actions）] > [非アクティブ化（Deactivate）] を選択すると確認メッセージが表示されます。

ステップ 4 メッセージ ボックスで [はい（Yes）]を選択してユーザを非アクティブ化します。

ユーザの再アクティブ化

手順

ステップ 1 非アクティブ化したユーザを再アクティブ化する（またはゲスト版ユーザに移行する）には、[非アクティブ ステータス（Inactive Status）]の検索フィルタを使用して、該当するユーザを検索します。検索フィルタの詳細については、ユーザと管理者の検索，（12 ページ）を参照してください。

ステップ 2 アクティブにするユーザを選択します。

ステップ 3 [その他の操作（More Actions）]>[アクティブ化（Activate）] を選択すると確認メッセージが表示されます。

ステップ 4 メッセージ ボックスで [はい（Yes）]を選択してユーザを再アクティブ化します。

ユーザ タブ表示のカスタマイズ

ニーズに合わせて [ユーザ（Users）]タブのデフォルト表示をカスタマイズできます。カスタマイズ設定には、列の表示や非表示、ユーザの表示順序の並び替えなどがあります。

手順

ステップ 1 [ユーザ（Users）] タブの表示をカスタマイズするには、[ユーザ（Users）]>[その他のアクション（More Actions）] > [表示をカスタマイズ（Customize View）] を選択します。

ステップ 2 [ユーザ タブで表示する列を選択（Select columns for display in the user tab）]で、該当するフィールドを選択するか、または選択を解除します。
Cisco WebEx Meeting アプリケーションとの統合を有効にしている場合、デフォルト フィールドに加えて [ミーティング アカウント（Meeting Account）]フィールドが表示されます。同様に、IM アーカイブと Cisco Unified Communications Manager を有効にすると、[IM アーカイブのエンドポイント（IM Archiving Endpoint）]と [CUCM クラスタ（CUCM Cluster）] フィールドが表示されます。

ステップ 3 [ユーザ レコードのデフォルトの並び順を選択（Select default sort order of user records）]で、ユーザのリストを並び替えるフィールド（または列）を選択します。

ステップ 4 並び順として、[昇順（Ascending）]または [降順（Descending）] を選択します。

ステップ 5 [保存（Save）]を選択します。

シングル サインオンおよびディレクトリ統合のユーザ

シングル サインオンおよびディレクトリ統合が有効になっているユーザを追加する手順は、これらの機能が有効でないユーザを追加する手順とは異なります。シングル サインオンおよびディレクトリ統合の詳細については、「シングル サインオンおよびディレクトリ統合」を参照してください。

シングル サインオンおよびディレクトリ統合を有効にすると、[ユーザ（Users）]タブの次の機能は使用できません。

- ユーザのインポートとエクスポート
- ユーザ パスワードのリセット
- 既存のユーザ情報の編集
- 新規ユーザの作成

Cisco WebExにディレクトリ統合が実装されている場合：

- ユーザおよびグループは、会社が提供する企業のディレクトリ ファイルから作成されます。
- 組織管理者は、ユーザおよびグループ データを直接編集することはできません。ユーザおよびグループ データの更新が必要な場合、会社が Cisco WebEx にインポートできる最新のディレクトリ ファイルを提供します。
- CSV ファイル インポート機能は使用できません。

Guest Edition ユーザから Business Edition ユーザへの移行

Cisco WebEx Messenger が特定のドメイン名を使用してプロビジョニングされている場合、同じドメイン名でバージョン 5.x 以前の Cisco WebEx Connect アプリケーションを使用しているユーザは Cisco WebEx Messenger にサインインできません。それらのユーザには、Cisco WebEx Messenger のアカウントが非アクティブ化されたことを知らせる電子メールが届きます。

Cisco WebEx Messenger の旧バージョンは、Cisco WebEx 管理ツールの [移行（Migration）]タブに表示されます。[移行（Migration）]タブには、Business Edition の Cisco WebEx Messenger への移行が保留になっている Guest Edition のユーザのリストが表示されます。移行が保留中のユーザが存在しない場合、[移行（Migration）]タブは表示されません。

Cisco WebEx Messenger のバージョン 6.0 以降では、[移行（Migration）]タブは表示されません。移行が保留中の Guest Edition ユーザは、非アクティブ ユーザとして表示されます。

組織管理者は Guest Edition ユーザを Business Edition の Cisco WebEx Messenger に移行する必要があります。

移行後、それらのユーザは組織管理者が設定したポリシーの対象となります。ユーザが Business Edition ユーザとして使用するすべてのリソースには、Cisco WebEx Messenger 組織に割り当てられているリソース（ユーザ ライセンスとストレージ）の総量の一部を形成する Cisco WebEx Messenger ライセンスが含まれます。

Guest Edition ユーザから Business Edition ユーザへの移行

手順

ステップ 1 Cisco WebEx 管理ツールの「非アクティブな」ユーザのリストを確認し、Cisco WebEx Messenger Business Edition に移行する必要があるユーザを特定します。

ステップ 2 選択したユーザに対して、最新バージョンの Cisco WebEx アプリケーションのダウンロード用 URL を含む手順を送信します。この URL は、サービスをプロビジョニングするときに管理者に送信されている電子メールに記載されています。

ステップ 3 ステータスを[アクティブ（active）]に設定し、選択したユーザのパスワードをリセットします。非アクティブなユーザを有効化する方法の詳細については、ユーザの非アクティブ化および再アクティブ化, （18 ページ）を参照してください。
これらのユーザに、パスワードのリセット リンクを含む電子メールが送信されます。このリンクから新しいパスワードを指定することができます。ユーザは次に、この新しいパスワードを使用して Cisco WebEx Messenger Business Edition の最新バージョンにサインインすることができます。ユーザの連絡先は Business Edition に転送されません。

第 3 章

[構成] タブ

概要

[設定（Configuration）] タブでは、Cisco WebEx Messenger サービスを制御します。このタブでの設定は、ライセンス、ポリシー、ユーザ管理、追加サービスとの統合などの領域に影響します。そのため、特定の設定を変更すると、組織全体に影響することがあります。設定に変更を加える前に十分に計画することをお勧めします。

[設定（Configuration）] タブには、特定のカテゴリで設定可能な項目が表示されます。たとえば、[システム設定（System Settings）] カテゴリでドメイン名と URL を設定し、[接続クライアント（Connect Client）] カテゴリで連絡先リストの設定ができます。各カテゴリでは、特定の設定項目の実際の設定を入力する作業領域が開きます。

特定の設定項目をクリックすると、その項目の設定可能な詳細が表示されます。たとえば、[リソース管理（Resource Management）] をクリックすると組織のライセンス情報を確認でき、ユーザに対するストレージの適用を有効にできます。

（注） Apple Push Notification をサポートするためには、Jabber IOS クライアント バージョン 11.x 以降が必要です。クラウドベースの Push Notification Service は、バックグラウンドで実行中の iPhone および iPad クライアントの Cisco Jabber にインスタント メッセージ通知を送信します。詳細については、「Deploying Push Notifications for iPhone and iPad with the IM and Presence Service and WebEx Messenger」および Cisco Unified Communications Manager Express システム管理者ガイド [英語] を参照してください。

組織情報

[組織情報（Organization Information）]ウィンドウでは、Cisco WebEx Messenger 組織に関する関連情報を入力できます。Cisco WebEx Messenger 組織とは、Cisco WebEx Messenger を購入し、プロビジョニングしている組織を示します。

（注） 会社名は入力も変更もできません。会社名は、購入時に入力した名前と同じ名前です。

所在地や職場電話などの連絡先情報は情報目的のために使用されます。

通知電子メール アドレスは、デフォルトでは組織管理者の電子メール アドレスです。この電子メール アドレスは、配布リストを含む他の電子メール ID に変更できます。

組織情報の入力

手順

ステップ 1 Cisco WebEx Messenger 組織の情報を入力するには、[設定（Configuration）]タブを選択すると、デフォルトの表示として [組織情報（Organization Information）] ウィンドウが開きます。

ステップ 2 各設定フィールドに適切な情報を入力します。

ステップ 3 Cisco WebEx Messenger 組織の [プライマリ管理者（Primary Administrator）]の名前と電子メール アドレスがすでに存在していることを確認します。
この情報は、Cisco WebEx Messenger 組織をプロビジョニングするときに設定されます。新しいバージョンの可用性やメンテナンス スケジュールなど、Cisco WebEx サービスに関するすべての重要な情報がこの電子メール アドレスに送信されます。この情報を変更するには、Cisco WebEx の営業担当者にお問い合わせください。

ステップ 4 [通知用電子メール（Notification Email）]フィールドに、重要なイベントが発生したときに管理者にアラートを送信するために使用する電子メール アドレスを指定します。
重要なイベントの代表的例として、組織のストレージ使用量が割り当ての上限を超えた場合などがあります。

ステップ 5 組織情報を保存するには、[保存（Save）]を選択します。

ドメイン情報

[ドメイン（Domain）]ウィンドウでは、Cisco WebEx Messenger 組織に対してプロビジョニングされているドメインを確認できます。また、Messenger組織外の「信頼できる」ドメインのリストであるドメイン ホワイトリストを指定できます。

Cisco WebEx Messenger 組織のプロビジョニング プロセスは、Cisco WebEx Messenger プロビジョニング チームが Cisco WebEx Messenger を購入した企業または組織からプロビジョニング要求を受け取ったときに開始されます。プロビジョニング要求の一環として Cisco WebEx Messenger 組織を作成する場合、通常はその Cisco WebEx Messenger 組織の一部となるドメインの名前またはサブドメインの名前を入力します。

ドメインの例には、acme.com、mydomain.net、myorg.com などがあります。サブ ドメインの例には、test.acme.com、docs.mydomain.net、prod.myorg.com があります。

ドメイン ホワイトリストは、Cisco WebEx Messenger 組織のドメインおよびサブ ドメインの外部にある信頼できるドメインのリストです。信頼できるドメインは、Cisco WebEx Messenger 組織のドメインと信頼関係が構築されているドメインです。たとえば、acme.com が Cisco WebEx 組織の場合、customeracme.com、vendoracme.com などの（外部）ドメインとの信頼関係を構築した後で、それらのドメインをドメイン ホワイトリストに追加できます。

[ドメイン（Domain(s)）]ボックスに表示されるドメイン名のリストは、Cisco WebEx Messenger 組織のプロビジョニング時に Cisco WebEx Messenger プロビジョニング チームによってすでに作成されています。ドメイン名の追加、変更、削除については、Cisco WebEx の担当者にお問い合わせください。

[ドメイン（Domain(s)）]ボックスと [ドメイン ホワイトリスト（Domain Whitelist）] ボックスに入力するドメインは、Cisco Jabber アプリケーションでの連絡先の追加方法に影響します。

ドメイン ホワイトリストに属している連絡先は、ユーザ プロファイルの表示設定を行うときに [自分の組織とネットワーク（My Organization & My Network）]選択した場合のみ表示できます。詳細については、Cisco Jabber アプリケーションの連絡先リスト設定の入力, （35 ページ）およびユーザ プロファイルの表示設定の入力, （38 ページ）を参照してください。

ドメイン情報の入力

手順

ステップ 1 ドメイン情報を入力するには、[設定（Configuration）]タブを選択します。

ステップ 2 [システム設定（System Settings）]で [ドメイン（Domain(s)）] を選択し、[ドメイン（Domain(s)）] ウィンドウを開きます。

ステップ 3 [ドメインのホワイトリスト（DomainWhitelist）]ボックスに、信頼されるドメインの名前を入力します。
ドメインのホワイトリストは、ポリシーと組み合わせて使用されます。詳細については、Cisco WebEx で使用可能なポリシー アクション, （107 ページ）を参照してください。

ステップ 4 ドメイン情報の設定を保存するには、[保存（Save）]を選択します。

リソース管理情報

リソース管理情報には、ユーザ ライセンスの数および Cisco WebEx Messenger 組織に割り当てられた記憶域を指定する詳細情報が含まれます。

ご自分の Cisco WebEx Messenger 組織で購入したユーザ ライセンスの数だけを閲覧できます。また、ご自分の Cisco WebEx Messenger 組織のアクティブなユーザの人数も閲覧できます。アクティ

ブユーザとは、Cisco Jabber アプリケーションを実際に使用しているユーザです。アクティブ ユーザの数は、ユーザをアクティブ化または非アクティブ化すると自動的に更新されます。ユーザのアクティブ化と非アクティブ化の詳細については、ユーザの非アクティブ化および再アクティブ化, （18 ページ）を参照してください。

ユーザ ライセンス数を増やすには、Cisco WebEx の担当者にお問い合わせください。

ストレージ

すでに使用済みのストレージの総容量は、使用済みストレージとして表示されます。合計使用済みストレージには、Messenger 組織でユーザが作成したすべての領域内のファイルおよび永続的なチャットによって消費される領域が含まれます。

すでに使用済みのストレージの総容量は、使用済みストレージとして表示されます。合計使用済みストレージには、Messenger 組織でユーザが作成したすべての領域内のファイルおよび永続的なチャットによって消費される領域が含まれます。

NBR（ネットワーク ベースの録画）を保存するために使用される領域は、使用済みストレージの計算には使用されません。

[購入した IM ログ記録ユーザ ライセンス（IM Logging User Licenses Purchased）] および [使用済み IM ログ記録ユーザ ライセンス（IM Logging User Licenses Used）] の各フィールドは、お客様の組織が IM アーカイブ機能を購入している場合に表示されます。詳細については、IM アーカイブの設定, （62 ページ）を参照してください。

デフォルトでは、ストレージの適用は各ユーザに対して有効になっていません。このような場合、ストレージは「早いもの勝ち」を基本として、合計ストレージ使用率がライセンス ストレージの上限に達するまで、使用されます。

各ユーザに対するストレージの適用を有効にすると、組織管理者は、新しいユーザの作成時にデフォルトのストレージの上限を指定できます。この値を変更しても、[ユーザの追加（Add User）] または [ユーザの編集（Edit User）] ダイアログボックスで指定したストレージの上限は変更されません。

リソース管理情報の入力

手順

ステップ 1 リソース管理情報を指定するには、[設定（Configuration）]タブを選択します。

ステップ 2 [システム設定（System Settings）]で、[リソース管理（Resource Management）] を選択します。

ステップ 3 Messenger 組織の各ユーザに対して一定量の記憶域を割り当てるには、[各ユーザのストレージの適用を有効にする（Enable storage enforcement for each user）]を選択します。

ステップ 4 [ユーザごとのデフォルトのファイル記憶域の配賦（Default file storage allocation per use）]に、デフォルトの記憶域として各ユーザに割り当てる記憶域をメガバイト単位で入力します。

ステップ 5 [保存（Save）]を選択します。

URL 設定

[URL 設定（URL Configuration）]画面では、次の Web サイトの URL を指定することができます。

- [パスワードの取得（Password retrieval）] : ユーザが自分のパスワードを取得することができます。
- [Cisco WebEx Messenger サポート Web サイト（Cisco WebEx Messenger support website）] : お客様のサポート リクエストを記録します。

URL 設定情報の入力

手順

ステップ 1 URL 設定情報を指定するには、[設定（Configuration）]タブを選択します。

ステップ 2 [システム設定（System Settings）]で、[URL 設定（URL Configuration）] を選択します。

ステップ 3 [パスワードを忘れた場合の URL（Forgot Password URL）]フィールドに、パスワード取得ページの URL を入力します。
組織管理者は、カスタムの [パスワードを忘れた場合の URL（Forgot Password URL）]を指定することでデフォルト URL を上書きできます。企業または組織が SAML 統合を有効にした特殊な場合にカスタマイズできます。

ステップ 4 [接続サポート URL（Connect Support URL）]フィールドに、Cisco WebEx Messenger サポート ページの URL を入力します。組織管理者は、社内の最初のレベルのサポート ページを指定することで、デフォルトの Cisco WebEx サポート URL を上書きできます。

ステップ 5 URL 設定情報を保存するには、[保存（Save）]を選択します。

セキュリティ設定

パートナー委任認証画面では、Cisco WebEx によって認定されている委任認証パートナー組織を Cisco WebEx Messenger 組織と統合するためのオプションを指定することができます。このオプションは、スーパー管理者構成から、事前に定義された相関関係が設定されたときのみ使用できます。パートナー組織の統合とは、単純に、パートナー組織が Cisco WebEx Messenger 組織をメンバー、組織管理者、またはその両方として認証できるようにすることを意味します。このような認証を有効にすると、これらの Cisco WebEx 認定パートナー組織が開発したアプリケーションを使用しているユーザは、個別のクレデンシャル セットを使用せずに Cisco WebEx Messenger にアクセスできます。

たとえば、acme.com は、Cisco WebEx Messenger の認定パートナーである Verizon Communications との統合を有効にした Cisco WebEx Messenger 組織です。acme.com のユーザは、Verizon Communications が提供するアプリケーションを認証でき、別のサインイン資格情報を使用せずに Cisco WebEx Messenger にアクセスできます。

組織管理者アクセス権を付与すると、パートナー組織は、Cisco WebEx Messenger 組織とパートナー組織上で管理タスクを実行できます。複数のパートナー組織とのパートナー組織の統合を有効にすることができます。

パートナー組織の統合はいつでも無効にすることができます。

（注） SSO 関連オプションのリンク表示は、スーパー管理者によって設定されます。

セキュリティ設定の入力

手順

ステップ 1 パートナー組織の統合を有効にするには、[設定（Configuration）]タブで、[セキュリティ設定（Security Settings）] > [SSO 関連オプション（SSO Related Options）] を選択します。

ステップ 2 次を選択します。

- 「委任認証」が設定されていない組織の管理者向けダイアログを表示するには、[パートナーの委任認証（Partner Delegated Authentication）]パートナーの委任認証の設定，（78 ページ）を参照してください。.

- シングル サインオンを有効にした管理者向けダイアログを表示するには、[フェデレーテッド Web SSO 構成（Federated Web SSO Configuration）]。フェデレーテッド Web SSO 設定，（73 ページ）を参照してください。.
- シングルサインオンを有効にしたか、「委任認証」の管理者用の管理者向けダイアログを表示するには、[組織の証明書管理（Organization Certificate Management）]。組織の証明書管理の設定，（76 ページ）を参照してください。.
- シングル サインオンを有効にした管理者向けダイアログを表示するには、[WebEx 証明書管理（WebEx Certificate Management）]。WebEx 証明書管理の設定，（76 ページ）を参照してください。.
- 「委任認証」である管理者向けダイアログを表示するには、[パートナーの Web SSO 設定（Partner Web SSO Configuration）]を選択します。パートナーの委任認証の設定，（78 ページ）を参照してください。.

SSO 関連オプションの詳細については、「関連項目」セクションを参照してください。

ステップ 3 各パートナー組織で許可する適切なアクセス レベルとして、[メンバー（Member）]または [組織管理者（Org Admin）]のいずれかを選択します。[組織管理者（Organization Administrator）]を選択した場合、[メンバー（Member）] はデフォルトで選択されます。
NameID の選択は、Cisco WebEx Messenger の組織の識別子と一致している必要があります。たとえば、組織が EmployeeID に基づいて認証されている場合、委任認証パートナーは、ユーザ アカウントを関連付けるために EmployeeID を使用する必要があります。使用可能な選択肢は、ユーザ名、電子メール、EmployeeID です。

ステップ 4 [保存（Save）]を選択すると確認メッセージが表示されます。

ステップ 5 パートナー組織の統合設定を保存するには、[パートナーにアクセス権を付与（Grant Partner Access）] を選択します。

関連トピック

SSO 関連オプション，（30 ページ）

SSO 関連オプション

SSO 関連オプションのリンク表示を判別するには、次の表を使用します。

SSO 組織	委任認証組織	表示
偽（False）	偽（False）	SSO 関連オプション • パートナーの委任認証

SSO 組織	委任認証組織	表示
正（True）	偽（False）	SSO 関連オプション • フェデレーテッド Web SSO 設定 • 組織の認定管理 • WebEx の認定管理 • パートナーの委任認証
正（True）	正（True）	SSO 関連オプション • フェデレーテッド Web SSO 設定 • 組織の認定管理 • WebEx の認定管理 • パートナーの委任認証
偽（False）	正（True）	SSO 関連オプション • 組織の認定管理 • パートナーの Web SSO 設定

ディレクトリの設定

このトピックは、Cisco WebEx Messenger 組織がディレクトリ統合を有効にしている場合のみ当てはまります。詳細については、ディレクトリ統合の設定, （124 ページ）およびディレクトリ統合のインポート プロセスとファイル形式, （124 ページ）を参照してください。

パスワード設定

組織管理者は、Cisco WebEx Messenger 組織内のユーザのパスワードの設定を指定できます。パスワードの設定内容により、新規ユーザが Cisco WebEx Messenger アカウントにサインアップした場合、既存ユーザがパスワードの変更を希望している場合など、さまざまなシナリオにおけるパスワードの適用方法が決まります。

パスワードは、この画面で設定するすべてのルールを満たすまで有効になりません。

パスワード設定の入力

手順

ステップ 1 パスワード設定を指定するには、[システム設定（System Settings）]で、[パスワード設定（Password Settings）] を選択します。

ステップ 2 画面の指示に従って、適切な選択肢を設定します。
デフォルトでは、Cisco WebEx Messenger の各組織は次のパスワード設定でプロビジョニングされます。

- パスワードの最小文字数 = 6
- アルファベットの最小文字数 = 1
- 数字の最小文字数 = 1

これらのパスワード長さの最小要件をリセットするには、Cisco WebEx の担当者にお問い合わせください。

ステップ 3 [受け入れられないパスワードのリスト（List of Unacceptable Passwords）]で、パスワードに使用することを禁止する用語または単語を入力します。通常、これらには組織名、単語のパスワード、URL のような用語が含まれます。各用語はカンマで区切ります。

ステップ 4 [保存（Save）]を選択します。

電子メール テンプレート

Cisco WebEx Messenger 管理ツールには、Cisco WebEx Messenger のユーザが受信する電子メール通知およびアラート用のテンプレートが用意されています。組織管理者は電子メール テンプレートをカスタマイズできます。カスタマイズすると、Cisco WebEx によってそれらのテンプレートに加えられた更新はすべて失われます。ただし、いつでもデフォルトのテンプレートに戻すことができます。

変数を使用して、電子メール テンプレートをより詳細にカスタマイズできます。変数を使用して電子メールテンプレートをカスタマイズする方法の詳細については、電子メールテンプレートの変数, （33 ページ）を参照してください。

Cisco WebEx の電子メール テンプレートのコンテンツは随時強化されます。電子メール テンプレートをカスタマイズしていない組織管理者は、更新されたコンテンツを自動的に取得します。

電子メール テンプレートをカスタマイズすると、カスタマイズしたテンプレートのみ使用されます。組織管理者は、電子メールテンプレートを選択し、[デフォルトにリセット（Reset to Default）] をクリックすることで、Cisco WebEx のデフォルトの電子メール テンプレートを使用する状態に戻せます。

電子メール テンプレートに加えた変更はすべて、Cisco WebEx のデフォルトの電子メール テンプレートにリセットすると失われます。

電子メール テンプレートの変数

このトピックでは、Cisco WebEx Messenger で使用可能なさまざまな電子メール テンプレート、およびそれらのテンプレートの編集またはカスタマイズ方法について説明します。通常、電子メール テンプレートはその組み込み変数を編集することでカスタマイズできます。変数は、電子メール テンプレート（およびそのテンプレートに基づく電子メール）に含まれる内容を定義する構成要素です。たとえば、[ウェルカム メッセージ（Welcome Message）]電子メール テンプレートには%USERNAME%変数が含まれています。この変数は、ユーザに送信される電子メールに含まれている Cisco WebEx Messenger ユーザのユーザ名を表示します。

すべての電子メール テンプレートの [メッセージ（Message）] ボックスには既存のメッセージ テキストが含まれています。それらのテキストは要件に応じてカスタマイズまたは変更できます。

Cisco WebEx Messenger 電子メール テンプレートは、適切なテンプレートに事前に入力されているため、すぐに使用できます。

次の表で、各電子メールテンプレート、各電子メールテンプレートで使用される変数およびそれらの定義について説明します。

電子メール テンプレート	変数とマクロ
[ウェルカム メッセージ（Welcome Message）]：デフォルトの電子メールには、パスワード リセットのリンク、アプリケーション ダウンロードのリンク、ドキュメントのリンク、およびコミュニティ リンクが含まれています。	%USERNAME%：ユーザの名前。 %CLIENTDOWNLOADURL%：ウェルカム メッセージが表示される URL。 %NEWPASSWORDURL%：新しいパスワード変数。
[パスワード電子メールの取得またはリセット（Get or Reset Password Email）]：Cisco WebEx Messenger 管理者がパスワードをリセットすると電子メールが送信されます。	%NEWPASSWORDURL%：パスワードをリセットできる URL。

電子メール テンプレートの選択

手順

ステップ 1 電子メール テンプレートを使用するには、[システム設定（System Settings）]で、[電子メール テンプレート（Email Templates）] を選択します。

ステップ 2 変更する電子メール テンプレートを選択します。

[電子メール テンプレートの編集（Edit Email Template）]ウィンドウが表示されます。

ステップ 3 [電子メールの名前（Email Name）]で始まる各フィールドに適切な情報を入力します。

ステップ 4 [メッセージ（Message）]ボックスに、電子メール テンプレートのテキストを入力します。

ステップ 5 [保存（Save）]を選択します。

ユーザ プロビジョニング情報

ユーザのプロビジョニングには、登録などのユーザ プロビジョニング情報の指定や、ユーザのプロファイルを作成するときに必要なフィールドの指定が含まれています。ここで行う設定は、Cisco WebEx Messenger の組織にユーザをプロビジョニングするタイミングに影響します。たとえば、特定のフィールドをここで必須に指定すると、ユーザがユーザ プロファイルを作成する際に、それらのフィールドへの入力が強制されます。

Cisco WebEx Messenger のお客様は、SAML またはディレクトリ統合が有効になっていない場合は、セルフ登録を有効にすることができます。このような場合、組織管理者は登録URLを指定する必要はありません。登録が有効になっていない場合は、お客様がカスタム Web ページを指定できます。お客様のドメインに一致する電子メール アドレスでユーザが登録しようとすると、カスタム Web ページにリダイレクトされます。お客様はこの Web ページを使用して、新しい Cisco WebEx Messenger アカウントの作成に必要な内部プロセスに関する情報を表示できます。

次に例を示します。
Cisco WebEx Messenger サービスを取得するには、ithelpdesk@mycompany.com 宛に電子メールをお送りいただくか、または +1 800 555 5555 までお電話でご連絡ください。

ユーザ プロビジョニング情報の入力

手順

ステップ 1 ユーザ プロビジョニング情報を入力するには、[設定（Configuration）]タブで、[システム設定（System Settings）] > [ユーザ プロビジョニング（User Provisioning）] を選択します。

ステップ 2 ユーザによる Cisco Jabber アプリケーションでのアカウントのセルフ登録を有効にするには、[Cisco WebEx 登録ページを使用したユーザのセルフ登録の有効化（Enable user self-registration using Cisco WebEx registration page）]を選択します。
セルフ登録ページの URL は www.webex.com/go/wc です。通常、Cisco WebEx Messenger の組織管理者がこの URL を提供します。

（注） [Cisco WebEx 登録ページを使用したユーザのセルフ登録の有効化（Enable user self-registration using Cisco WebEx registration page）] を選択しなかった場合は、[カスタム登録 URL（Custom Registration URL）] フィールドと [カスタム メッセージ（Custom Message）] ボックスが表示されます。この場合は、カスタム ユーザ登録ページの URL を入力する必要があります。

ステップ 3 [カスタム登録 URL（Custom Registration URL）]フィールドに、カスタマイズされたセルフ登録ページの URL を入力します。
カスタム URL を入力しなかった場合は、セルフ登録ページ（デフォルト）の URL である www.webex.com/go/wc が表示されます。

ステップ 4 [カスタム メッセージ（Custom Message）]ボックスにカスタム セルフ登録ページの説明を入力します。

ステップ 5 セルフ登録ページを使用してユーザが登録するたびに、電子メールで組織管理者に通知するには、[ユーザが Cisco WebEx 登録ページを使用してセルフ登録したときに通知を管理者に送信する（Send notification to Administrator when users self register using Cisco WebEx registration page）]を選択します。

ステップ 6 [ユーザ プロファイルの必須フィールドの設定（Set mandatory fields for user profile）]で、ユーザのプロファイルを作成または表示するたびに強制的に表示するフィールドを選択します。これらのフィールドは、次を実行する際に常に表示されます。

- 新規ユーザの作成
- 既存のユーザ プロファイルの編集
- CSV ファイルからのユーザのインポート

ステップ 7 [保存（Save）]を選択します。

Cisco Jabber アプリケーションの連絡先リスト設定の入力

[連絡先リスト（Contact List）]画面では、Cisco WebEx Messenger 組織のユーザの連絡先リストの管理方法に関する設定を指定できます。これらの設定は、連絡先の写真の表示、ユーザの連絡先リスト内のクイック連絡先やオブザーバ グループの表示といった機能を制御します。

手順

ステップ 1 [構成（Configuration）]タブを選択して、[組織情報（Organization Information）] を開きます。

ステップ 2 連絡先リストの設定を指定するには、[クライアントを接続（Connect Client）]で [連絡先リスト（Contact List）] を選択します。

ステップ 3 適切な設定値を指定します。

連絡先リストの詳細については、「関連項目」セクションを参照してください。

ステップ 4 [保存（Save）]を選択します。

関連トピック

連絡先リストの設定, （36 ページ）

連絡先リストの設定

選択	結果
[[連絡先リストに連絡先の画像を表示（Show contact pictures in my contact list）] の設定をユーザに許可（Allow users to set "Show contact pictures in my contact list"）] （注） このオプションは、バージョン 6.x 以前の Cisco WebEx Messengerにのみ適用できます。	組織管理者は、ユーザが連絡先の画像を確認できるかどうかを直接制御できます。 このオプションを選択すると、Cisco Jabber アプリケーションに [連絡先リストに連絡先の画像を表示（Show contact pictures in my contact list）]チェックボックスが表示され、ユーザは連絡先の画像表示の設定を指定できます。 このオプションを選択しないと、Cisco Jabber アプリケーションに [連絡先リストに連絡先の画像を表示（Show contact pictures in my contact list）]チェックボックスは表示されません。
[連絡先リストに連絡先の画像を表示（Show contact pictures in my contact list）] （注） このオプションは、バージョン 6.x 以前の Cisco WebEx Messengerにのみ適用できます。	このオプションを選択すると、Cisco Jabber アプリケーションのユーザの連絡先リストに連絡先の画像が表示されます。連絡先の画像は連絡先の名前の右側に表示されます。 [[連絡先リストに連絡先の画像を表示（Show contact pictures in my contact list）] の設定をユーザに許可（Allow users to set "Show contact pictures in my contact list"）]が選択されている場合、このオプションはグレー表示になります。

選択	結果
[[クイック連絡先を表示（Show quick contacts）] の設定をユーザに許可（Allow users to set "Show quick contacts"）] （注） このオプションは、バージョン 6.x 以前の Cisco WebEx Messenger にのみ適用できます。	組織管理者は、ユーザが Cisco Jabber アプリケーションでクイック連絡先グループを確認できるかどうかを直接制御できます。 このオプションを選択すると、Cisco Jabber アプリケーションに [クイック連絡先を表示（Show quick contacts）]チェックボックスが表示され、ユーザは適宜設定を指定できます。 このオプションを選択しないと、Cisco Jabber アプリケーションに [クイック連絡先を表示（Show quick contacts）]チェックボックスは表示されません。
[クイック連絡先を表示（Show quick contacts）] （注） このオプションは、バージョン 6.x 以前の Cisco WebEx Messenger にのみ適用できます。	このオプションを選択すると、Cisco Jabber アプリケーションのユーザの連絡先リストにクイック連絡先が表示されます。クイック連絡先は、Cisco Jabber アプリケーションで連絡先をグループ化する方法です。 [[クイック連絡先を表示（Show quick contacts）] の設定をユーザに許可（Allow users to set "Show quick contacts"）]が選択されている場合、このオプションはグレー表示になります。
[[連絡先リストにオブザーバ グループを表示（Show observer group on my contact list）] の設定をユーザに許可（Allow users to set "Show observer group on my contact list"）] （注） このオプションは、バージョン 6.x 以前の Cisco WebEx Messenger にのみ適用できます。	組織管理者は、ユーザが Cisco Jabber アプリケーションでオブザーバ グループを確認できるかどうかを直接制御できます。 このオプションを選択すると、Cisco Jabber アプリケーションに [連絡先リストにオブザーバ グループを表示（Show observer group on my contact list）]チェックボックスが表示され、ユーザは適宜設定を指定できます。 このオプションを選択しないと、Cisco Jabber アプリケーションに [連絡先リストにオブザーバ グループを表示（Show observer group on my contact list）]チェックボックスは表示されません。

選択	結果
[連絡先リストにオブザーバ グループを表示（Show observer group on my contact list）] （注） このオプションは、バージョン 6.x 以前の Cisco WebEx Messengerにのみ適用できます。	このオプションを選択すると、Cisco Jabber アプリケーションにオブザーバ グループが表示されます。オブザーバ グループは、Cisco Jabberアプリケーション内の連絡先の特別なグループです。デフォルトでは、このオプションが選択されています。 [[連絡先リストにオブザーバ グループを表示（Show observer group on my contact list）] の設定をユーザに許可（Allow users to set "Show observer group on my contact list"）]が選択されている場合、このオプションはグレー表示になります。

ユーザ プロファイルの表示設定の入力

Cisco WebEx Messenger組織のユーザを閲覧できる人を指定できます。さらに、ユーザによるCisco Jabber アプリケーションのユーザ プロファイルの表示設定の変更を許可できます。ユーザ プロファイルは通常、Cisco Jabber アプリケーションでビジネス用の名刺と同様に表示されます。

手順

ステップ 1 ユーザ プロファイルの表示設定を指定するには、[クライアントを接続（Connect Client）] > [プロファイル設定（Profile Setting）] を選択します。

ステップ 2 ユーザがプロファイルの表示設定をCisco Jabberアプリケーションで直接変更することを許可する場合は、[ユーザによるプロファイル表示設定の変更を許可する（Allow users to change their profile view settings）]を選択します。
このオプションを有効にすると、ユーザは Cisco Jabber アプリケーションでユーザ プロファイルを直接開いて編集できます。

（注）
- [ユーザによるプロファイル表示設定の変更を許可する（Allow users to change their profile view settings）] を解除すると、ユーザは Cisco WebEx アプリケーションでユーザ プロファイルに関する情報を変更できなくなります。
- 組織管理者は、[表示プロファイル設定の編集（Edit View Profile Setting）]のポリシー アクションを適用することで、ユーザによるプロファイル表示設定の変更を制限できます。このポリシーアクションをFALSEに設定すると、[ユーザによるプロファイル表示設定の変更を許可する（Allow users to change their profile view settings）]チェックボックスが選択されていたとしても、プロファイル表示設定を変更することはできなくなります。

このポリシーの詳細については、Cisco WebEx で使用可能なポリシー アクション，（107 ページ）を参照してください。

ステップ 3 [デフォルトのユーザ プロファイル表示設定（Default user profile view settings）]で、次のいずれかのオプションを選択します。

- [全員（Anyone）]：すべてのユーザにユーザ プロファイル情報の表示を許可します。信頼関係が確立されている Cisco WebEx Messenger 組織の外部ユーザも含まれます。
- [自社組織と自社ネットワーク（My Organization & My Network）]：勤務先の Cisco WebEx Messenger 組織とネットワーク内のすべてのユーザと、連絡先リストに追加された外部ドメインに属する任意のユーザに、ユーザ プロファイル情報の表示を許可します。
- [自社組織（My Organization）]：Cisco WebEx Messenger 組織内のすべてのユーザに、ユーザ プロファイル情報の表示を許可します。プロファイルを表示できるユーザは、Cisco WebEx Messenger 組織のプロビジョニング方法に従って決定されます。この設定では、ユーザはホワイトリストに追加された外部ドメインに属するユーザプロファイルを表示することはできません。

ステップ 4 [保存（Save）]を選択します。

インスタント メッセージのブロック設定の入力

インスタント メッセージング（IM）のブロック設定には、次の項目の指定が含まれます。

- IM 通信上でのやり取りを禁止するファイル タイプ
- IM 通信上でのアクセスを禁止する URL

（注） 組織向けの構成パラメータを含む XML ファイルを作成できます。次に、[Jabber クライアント構成ファイルのインポート（Import Jabber Client Config File）]を使用して、Cisco WebEx Messenger 管理ツールにその XML 構成ファイルをアップロードできます。ユーザがサインインすると、Messenger 管理ツールが XML ファイルを取得して構成を適用します。詳細については、最新の『Deployment and Installation Guide for Cisco Jabber』を参照してください。

手順

ステップ 1 [構成（Configuration）]タブを選択して、[組織情報（Organization Information）] を開きます。

ステップ 2 インスタントメッセージのブロック設定を入力するには、[クライアントを接続（Connect Client）] で [IM ブロック設定（IM Block Settings）] を選択します。

ステップ 3 [ブロックされたファイル タイプ（Blocked File Types）]ボックスで、IM 通信でブロックするファイルの種類を入力します。各ファイル タイプはセミコロンで区切ります。

ステップ 4 [ブロックされた URL（Blocked URLs）]ボックスで、IM 通信でブロックする URL を入力します。各 URL はセミコロンで区切ります。

ステップ 5 [保存（Save）]を選択します。

XMPP IM クライアント

XMPP IMクライアント ウィンドウを使用すると、Cisco WebEx Messenger 組織内のユーザが、サードパーティ製 IM アプリケーションを使用してログインできるかどうかを指定することができます。

Cisco Jabber アプリケーションの代わりに、XMPP をサポートするサードパーティ製アプリケーション（たとえば Pidgin for Linux）を基本的な IM 通信に使用できます。ただし、組織のポリシーはサードパーティ製 XMPP アプリケーションに適用できません。さらに、エンドツーエンド暗号化、デスクトップ共有、ビデオ コール、コンピュータ間コール、およびテレビ会議などの機能は、サードパーティ製のアプリケーションではサポートされていません。XMPP をサポートするサードパーティ製アプリケーションのリストは、http://xmpp.org/software/clients.shtml にある XMPP Standards Foundation の Web サイトから入手できます。

XMPP IM クライアントの設定

手順

ステップ 1 XMPP IM クライアントを設定するには、[設定（Configuration）] タブ > [クライアントを接続（Connect Client）] > [XMPP IM クライアント（XMPP IM Clients）] を選択します。

ステップ 2 Cisco WebEx Messenger 組織のユーザがサードパーティ製の XMPP ベースの IM クライアントを使用してログインできるようにするには、[未接続 XMPP IM クライアントの使用を許可（Allow use of non-Connect XMPP IM clients）]を選択します。
ドメインの SRV レコードは、[設定（Configuration）]タブの [IM フェデレーション（IM Federation）] 画面で確認できます。詳細については、IM フェデレーション設定の指定, （59 ページ）を参照してください。

ステップ 3 [保存（Save）]を選択します。

アップグレード管理設定

[アップグレード管理（Upgrade Management）]ウィンドウでは、Cisco Jabber アプリケーションへのアップグレードをどのように組織内のユーザに展開するかを指定できます。次のアップグレード モードを使用してアップグレードを展開できます。

- [デフォルト（Default）]：すべてのユーザが Cisco Jabber の最新バージョンに自動的にアップグレードされます。これはデフォルトのアップグレード モードです。
- [カスタム（Custom）]：アップグレードをユーザに展開する方法を手動で設定できます。この場合、基準のバージョンを選択してからアップグレード タスクを作成する必要があります。これにより、アップグレードの展開方法を定義します。

  2 つのアップグレード モードはどの時点でも切り替えることができますが、この切り替えはアップグレードの展開方法に影響します。たとえば（カスタムモードを使用して）ユーザに展開する特定のバージョンを選択し、次にデフォルトモードに切り替えた場合、デフォルトバージョン以降のバージョンを実行している場合を除き、ユーザはその時点でのクライアントのデフォルト バージョンに無条件にアップグレードされます。

  すべてのユーザに同じバージョンのアプリケーションを実行させたい場合、基準のバージョンを設定できます。この場合、古いバージョンを使用しているすべてのユーザがアップグレードする必要がありますが、基準より新しいバージョンのアプリケーションを使用しているユーザがダウングレードする必要はありません。

  基準バージョンの設定は任意です。基準バージョンは、現在および将来のすべてのユーザに対して、最小バージョンとして実行することを要求するアプリケーションバージョンに設定することをお勧めします。

  基準バージョンを設定すると、プロビジョニングされる新しいユーザが、基準として設定したバージョンのクライアントをダウンロードするようになります。

  アップグレード タスクを作成することで、1 人以上のユーザを基準バージョン以降のバージョンのアプリケーションにアップグレードできます。ただし、このアップグレード管理サービスでは、ユーザは旧バージョンのアプリケーションを実行できなくなります。基準以前のバージョンを実行しているユーザは、ログイン時に基準のバージョンにアップグレードするように求められます。基準のバージョンを設定すると、すべての既存ユーザと新規ユーザが、少なくともそのバージョンのアプリケーションを実行するようになります。

  基準バージョンを設定しないように決定した場合、プロビジョニングされる新しいユーザは、アプリケーションの最新のデフォルトバージョンをダウンロードするように指示されます。

アップグレード管理設定

手順

ステップ 1 基準のバージョンを設定するには、[アップグレードモード（Upgrade Mode）]セクションで [変更（Change）] を選択し、使用可能なアップグレード モードを確認します。

ステップ 2 アップグレード モードを選択します。

ステップ 3 必要に応じて、基準を選択します。

ステップ 4 展開するバージョンを選択し、[OK]を選択します。

（注） 基準を選択しないと、次のメッセージが表示されます。「基準のバージョンを設定していません（You have not set baseline versions）」Cisco Jabber クライアントをダウンロードするためのウェルカム メールに記載される URL は、どちらのプラットフォームでも Cisco Jabber の最新バージョン用のものです。

ステップ 5 [ベースライン バージョン（Baseline Versions）]の下にリストアップされている [アップグレード管理（Upgrade Management）] 画面で選択したバージョンを表示するには、[はい（Yes）] を選択します。
ステップ 7 で古いバージョンを選択すると、それよりも新しいすべてのバージョンが [基準バージョン（Baseline Versions）]の上部に表示されます。

ステップ 6 （任意）該当するバージョンの隣にある [ダウンロード（Download）]を選択してアプリケーションをダウンロードします。

ステップ 7 そのバージョンのリリース ノートの隣にある [リリース ノート（Release Notes）]を選択します。
[基準バージョン（Baseline Versions）]の下に表示されているバージョンが、組織で展開されているバージョンです。

アップグレード タスクの作成

手順

ステップ 1 アップグレード タスクを作成するには、[設定（Configuration）] タブ > [クライアントを接続（Connect Client）] > [アップグレード管理（Upgrade Management）] を選択します。

ステップ 2 [アップグレード タスクの作成（Create Upgrade Task）]を選択し、アップグレード管理作業エリアで [Windows 向けアップグレード タスクの作成（Create Upgrade Task for Windows）] を開きます。

ステップ 3 [ターゲット バージョン（Target Version）]ドロップダウンから、展開する該当バージョンを選択します。
ターゲット バージョンとして事前に設定した基準以降のバージョンを選択する必要があります。

ステップ 4 [カスタマイズした URL を指定（Provide Customized URL）]を選択し、Cisco WebEx Messenger のセットアップ プログラムをダウンロードするカスタム リンクを指定します。このフィールドは任意です。

ステップ 5 [任意アップグレード（Optional Upgrade）]ダイアログ ボックスで、任意のアップグレードを展開する日時を選択します。または、[スキップ（Skip）]を選択して任意のアップグレードの適用をスキップします。

ステップ 6 [必須アップグレード（Mandatory Upgrade）]ダイアログ ボックスで、アップグレードを展開する日時を選択します。または、[スキップ（Skip）]を選択して必須アップグレードの適用をスキップします。

ステップ 7 [タイムゾーン（Time zone）]ドロップダウン リストから、アップグレードを展開する基準となるタイム ゾーンを選択します。
任意アップグレードと必須アップグレードに選択した日時は、このタイム ゾーンに基づいて計算されます。

ステップ 8 [ターゲット ユーザ（Target User）]で、以下のいずれかを選択します。

- [すべてのユーザ（Allusers）]：組織内のすべてのユーザにアップグレードを展開します。
- [特定のアップグレード サイト（Specific UpgradeSites）]：アップグレードを選択したアップグレード サイトに展開します。この場合、アップグレードはそれらのサイト内のすべてのユーザに展開されます。アップグレードサイトがリストアップされていない場合、リストを作成する必要があります。詳細については、アップグレード サイトの作成, （44 ページ）を参照してください。

ステップ 9 [保存（Save）]を選択します。
アップグレードは [アップグレード管理（Upgrade Management）]ページに表示されます。

アップグレード タスクの編集またはキャンセル

手順

ステップ 1 編集するには、[編集（Edit）]を選択してアップグレード タスクの詳細を編集します。

ステップ 2 またはアップグレード タスクをキャンセルし、[アップグレード タスクを閉じる（Close Upgrade Task）]を選択します。

ステップ 3 アップグレード タスクを削除するには [はい（Yes）]をクリックします。

アップグレード サイト

アップグレード サイトでは、どのユーザに Cisco Jabber クライアント アップグレードを展開するかを指定することができます。アップグレード サイトは、組織の特定のユーザにアップグレードを展開するアップグレードタスクを作成するときに使用します。アップグレードタスクの作成の詳細については、アップグレード管理設定, （42 ページ）を参照してください。

アップグレード サイトの作成

手順

ステップ 1 [設定（Configuration）] タブ > [クライアントを接続（Connect Client）] > [アップグレード管理（Upgrade Management）] を選択します。

ステップ 2 必要に応じて下にスクロールし、[アップグレード サイト（Upgrade Site）]セクションに移動します。
アップグレード モードとして [デフォルト（Default）]を選択していると、[アップグレード サイト（Upgrade Site）]セクションは表示されません。また、アップグレード サイトが作成されていない場合、このセクションは空欄になります。

ステップ 3 [追加（Add）]をクリックして、[アップグレード サイトの追加（Add Upgrade Site）] ウィンドウを開きます。

ステップ 4 [アップグレード サイト名（Upgrade Site Name）]ボックスにアップグレード サイトの名前を入力し、[保存（Save）] を選択します。
新しいアップグレード サイトが [アップグレード管理（Upgrade Management）]画面に表示されます。任意の数のアップグレード サイトを組織に追加できます。

ステップ 5 アップグレードサイトに属しているユーザを表示するには、[ユーザを表示（View Users）]アイコンを選択します。
ユーザをアップグレード サイトに追加する方法については、新しいユーザの作成, （14 ページ）を参照してください。

P2P（ピアツーピア）の設定

P2P（ピアツーピア）とは、Jabber 間通話を行う機能を指します。

[P2P（ピアツーピア）の設定（P2P Settings）]ウィンドウには、P2P（ピアツーピア）の次の設定オプションがあります。

- UDP ポートの手動設定：お客様の組織の管理者は、Cisco Jabber アプリケーションが Jabber 間通話を試みるときに使用される UDP ポートの範囲を手動で指定できます。お客様の管理者がポート範囲を手動で指定できることで、Cisco Jabber アプリケーションはその範囲内の

ポートのみ ping するため、セキュリティ リスクを最小限に抑えることができます。ポート範囲は、最小および最大のポート番号内で許可されるポート番号として指定します。

- たとえば、範囲が 7050 ～ 7550 の場合、Cisco Jabber アプリケーションはこの範囲内のすべてのポートのみスキャンします。指定されたポート範囲が狭すぎる場合、ユーザは Jabber 間通話を使用できません。

（注） Jabber 間通話では Cisco Spark プラットフォームが活用されます。結果として、お客様は P2P（ピアツーピア）を使用するために、Cisco Media ハイブリッド サービスの UDP ポート範囲の設定を開く必要があります。Spark プラットフォーム ネットワークおよびファイアウォールの設定については、次の URL を参照してください。https://support.ciscospark.com/customer/en/portal/articles/1911657-firewall-and-network-requirements-for-the-cisco-spark-app?b_id=8722 [英語]

- [最大（Max）]ポート番号は常に [最小（Min）]ポート番号よりも大きい番号にする必要があります。たとえば、[最小（Min）] が 1034で [最大（Max）] が 1024 のポート範囲は無効です。
- [最小（Min）]と [最大（Max）]のポート範囲の下限値と上限値はシステムによって定義されます。これらの事前定義された範囲（1024 ～ 65525 および 1034 ～ 65535）に含まれるポート番号のみ入力できます。

P2P（ピアツーピア）の設定

手順

ステップ 1 [設定（Configuration）] タブ > [クライアントを接続（Connect Client）] > [P2P 設定（P2P Settings）] を選択します。

ステップ 2 [ポートを手動で設定（Configure Ports Manually）]を選択し、UDP ポート範囲を手動で指定します。

ステップ 3 [UDP ポート範囲（UDP Port Range）]で以下を入力します。

- [最小（Min）]ボックスに最小ポート番号。1024 ～ 65525 の任意のポート番号を入力できます。
- [最大（Max）]ボックスに最大ポート番号。1034 ～ 65535 の任意のポート番号を入力できます。

ステップ 4 [保存（Save）]を選択します。

ステップ 5 以前の P2P 設定に戻すには、[リセット（Reset）]を選択します。

追加サービスの把握

Cisco WebEx Messenger は、すべての Cisco WebEx Messenger 展開の一部である通常オプションやデフォルト オプションに加えて、特定の追加サービスを提供します。追加サービスには、Cisco WebEx Messenger にシームレスに統合できるような個別の構成が含まれます。

次の追加サービスが使用できます。

- Cisco WebEx Meeting アプリケーションとの統合：Cisco WebEx Messenger と Cisco WebEx アプリケーション間の統合を有効にすると、ユーザの管理とユーザエクスペリエンスを簡素化することができます。Cisco WebEx Meeting アプリケーションとの統合を指定する方法の詳細については、Cisco WebEx Messenger と Cisco WebEx アプリケーションの統合の概要, （46 ページ）を参照してください。
- Unified Communications との統合：Cisco WebEx Messenger 組織のユーザが、Cisco Unified Communications Integration（クリックツーコール）および Cisco Unified Call Manager（CUCM）を Cisco WebEx Messenger から直接使用できるようにします。Unified Communications Integration を指定する方法の詳細については、Cisco Unified Communications と Cisco WebEx の統合, （79 ページ）を参照してください。
- 古い Cisco WebEx Messenger 組織と Cisco WebEx アプリケーションとの統合：古い Cisco WebEx Messenger 組織と Cisco WebEx アプリケーションとの統合を有効にした場合、疎結合統合のみ有効にできます。Cisco WebEx Messenger および Cisco WebEx アプリケーションにログインするには、引き続き別の資格情報を使用する必要があります。詳細については、Cisco Unified Communications と Cisco WebEx の統合, （79 ページ）を参照してください。
- IM フェデレーション：Cisco WebEx 組織のユーザが Google Talk などのパブリック XMPP ネットワークを使用して通信できるように、IM フェデレーション設定を指定できます。IM フェデレーションを指定する方法の詳細については、IM フェデレーション設定の指定, （59 ページ）を参照してください。
- IM ログ記録とアーカイブ：Cisco WebEx Messenger で、組織のユーザが相互に交換する IM を記録し、アーカイブすることができます。詳細については、IM アーカイブ通知, （60 ページ）を参照してください。

Cisco WebEx Messenger と Cisco WebEx アプリケーションの統合の概要

Cisco WebEx Messenger と Cisco WebEx アプリケーション間の統合を有効にすると、ユーザの管理とユーザ エクスペリエンスを簡素化することができます。この統合は、密結合と疎結合の 2 つのレベルで行うことができます。管理者は、それぞれの要件および関連する特定の展開シナリオに基づいて適切なレベルの統合を選択する必要があります。次の表に、この 2 つのレベルの統合の主な特徴と相違点を示します。

密結合統合	疎結合統合
Cisco WebEx Meeting アプリケーションのすべてのユーザは、Cisco WebEx Messenger のアカウントを持っている必要があります。追加設定なしで「ワンクリックで会議」体験を提供します。	追加設定なしで「ワンクリックで会議」体験を提供します。
ユーザ プロビジョニング、ユーザのパスワード管理、およびユーザ管理のシングルポイントを提供します。	Cisco WebEx Messenger および Cisco WebEx Meeting アプリケーションは独立したサービスとして管理されます。Cisco WebEx Messenger のすべてのユーザが Cisco WebEx アプリケーションのアカウントを持っている必要はなく、その逆もまた同様です。
Cisco WebEx Messenger および Cisco WebEx アプリケーションの両方で使用できる単独のサインイン資格情報を有効にします。	ユーザは、Cisco WebEx アプリケーションにログインするためのサインイン資格情報を引き続き使用して、Cisco WebEx の Web サイトにログインできます。

一般に、密結合統合は、シングルサインオン システムを展開していない企業で推奨されます。疎結合統合は、シングルサインオン システムを展開している企業で推奨されます。ただし、シングルサインオン システムを展開していない企業でも疎結合統合を有効にすることはできます。各統合レベルの詳細については、以下を参照してください。

- 密結合統合の概要, （47 ページ）
- 疎結合統合の概要, （54 ページ）

  密結合と疎結合のどちらのレベルでも、統合プロセスにはさまざまな異なるシナリオが含まれます。

  密結合統合と疎結合統合は、Cisco WebEx Messenger 組織が、アプリケーションから WebEx ミーティングを開始するための既存の Cisco WebEx Meeting Center サイトをサポートする場合に適用されます。

密結合統合の概要

密結合統合により、Cisco WebEx Messenger 管理ツールからシングル ポイントでのユーザ管理が可能になります。組織管理者は Cisco WebEx Messenger アカウントを作成し、それらのアカウントに対して Cisco WebEx Meeting アプリケーション サービスを有効にしたり、有効にしなかったりできます。組織管理者は、Cisco WebEx Messenger 管理ツールから Cisco WebEx Meeting アプリケーションの管理ツールにアクセスして、Cisco WebEx Meeting アプリケーション アカウントに固有の管理機能を実行できます。

密結合統合は、エンタープライズ シングル サインオン インフラストラクチャと統合してないお客様に大きな価値をもたらします。エンタープライズ シングル サインオン インフラストラクチャと統合しているお客様は、エンタープライズ ID 管理システムをユーザ管理の主な手段として使用します。疎結合統合は、次のようなお客様に推奨されます。

次の表に、企業の密結合統合を有効にするために使用できる 3 つの一般的なシナリオを示します。

統合のシナリオ	Cisco WebEx Messenger	Cisco WebEx Meeting アプリケーション
1	新規導入	新規導入
2	新規導入	既存の導入。企業にすでに Cisco WebEx Meeting アプリケーションが導入されていて、完全に機能している。
3	既存の導入。企業にすでに Cisco WebEx Messenger が導入されていて、完全に機能している。	新規導入

Cisco WebEx Messenger と Cisco WebEx Meeting アプリケーション間の密結合統合を有効にするための手順は、各シナリオで異なります。各シナリオの詳細については、以下のトピックを参照してください。

- Cisco WebEx および Cisco WebEx Meeting アプリケーション両方の新規展開時の密結合統合の成功確認, （52 ページ）
- 新規展開の Cisco WebEx Messenger と既存展開の Cisco WebEx Meeting アプリケーションとの密結合統合の成功確認, （53 ページ）
- 新規展開の Cisco WebEx Meeting アプリケーションと既存展開の Cisco WebEx Messenger との密結合統合の成功確認, （54 ページ）

密結合統合のシステム要件

密結合統合を有効にする前に、次のシステム要件を満たしていることを確認します。

項目	要件
Cisco WebEx Meeting アプリケーション	バージョン T27L SP 9 以降。1 つの Cisco WebEx Meeting アプリケーション サイトのみ Cisco WebEx Messenger と統合できます。 現在実行している Cisco WebEx Meeting アプリケーションのバージョンを確認するには、使用ブラウザのアドレス バーに、次の形式で Cisco WebEx Meeting アプリケーションの URL を入力します。 https://[sitename].webex.com/version/wbxversionlist.do?siteurl=[sitename] または、Cisco WebEx のセールス担当者に連絡してバージョンを確認してください。 XML API バージョン 5.3.0 以降
Organization	• 密結合統合は、シングル サインオンによる認証をサポートしていません。 • シングル サインオンに対応していない Cisco WebEx Messenger 組織は、シングル サインオンに対応していない Cisco WebEx Meeting アプリケーション サイトとのみ統合できます。

密結合統合のプロビジョニング

次に、3 種類の密結合統合の各シナリオに対するプロビジョニング手順について説明します。密結合統合のさまざまなシナリオの詳細については、密結合統合の概要, （47 ページ）を参照してください。

シナリオ 1：Cisco WebEx Messenger および Cisco WebEx Meeting アプリケーション両方の新規展開時の密結合統合

Cisco WebEx Meeting アプリケーションと Cisco WebEx との間で密結合統合を有効にする前に、次の準備手順が完了していることを確認します。

1. Cisco WebEx プロビジョニング チームが新しい Cisco WebEx Meeting アプリケーション サイトを作成します。
2. Cisco WebEx プロビジョニング チームが、Cisco WebEx Meeting アプリケーション サイト（URL）が密結合統合に指定された新しい Cisco WebEx Messenger 組織を作成します。
3. [構成（Configuration）]タブの下の[会議（Meetings）]画面に Cisco WebEx Meeting アプリケーションのサイト URL が表示された場合、統合は成功です。また、組織管理者が Cisco WebEx Meeting アプリケーション サイトにログインすると、対応する管理者アカウントがサイトで自動的に作成されます。詳細については、Cisco WebEx および Cisco WebEx Meeting アプリケーション両方の新規展開時の密結合統合の成功確認, （52 ページ）を参照してください。

シナリオ 2：新規展開の Cisco WebEx Messenger と既存展開の Cisco WebEx Meeting アプリケーションとの密結合統合

Cisco WebEx Meeting アプリケーションと Cisco WebEx Messenger との間で密結合統合を有効にする前に、次の準備手順が完了していることを確認します。

1. Cisco WebEx Meeting アプリケーションのユーザ アカウントすべての電子メール アドレスを変更します。変更した電子メールアドレスのドメインは、Cisco WebEx Messenger 組織の電子メールのドメインに一致させる必要があります。たとえば、Cisco WebEx Meeting アプリケーションのユーザ アカウントの既存の電子メール アドレスが user@domain.com であり、新しい Cisco WebEx Messenger 組織の電子メールのドメインが acme.com である場合、Cisco WebEx Meeting アプリケーションの user@domain.com を user@acme.com に変更します。
2. 既存の Cisco WebEx Meeting アプリケーション アカウントに合わせて Cisco WebEx Messenger アカウントを作成します。既存の Cisco WebEx Meeting アプリケーション ユーザに合わせて Cisco WebEx Messenger アカウントを作成しないと、Cisco WebEx Meeting アプリケーションユーザは Cisco WebEx Meeting アプリケーション サイトにログインできなくなります。残りの手順では、既存の Cisco WebEx Meeting アプリケーション アカウントに合わせて Cisco WebEx Messenger アカウントを作成する手順について説明します。
3. すべての Cisco WebEx Meeting アプリケーションのユーザ アカウントをエクスポートします。
4. Cisco WebEx Meeting アプリケーションのユーザ アカウントを含む、エクスポートしたファイルを開きます。次の表に示すように列ヘッダーを変更します。次に示すもの以外にも追加の列ヘッダーがある場合、それらを変更または削除する必要はありません。

列ヘッダー名	変更内容
UserName	この列を削除
FirstName	firstName に名称変更
LastName	lastName に名称変更
Email	email に名称変更
Address1	address1 に名称変更
Address2	address2 に名称変更
City	city に名称変更
State/Prov	state に名称変更
Zip/Postal	zipCode に名称変更
Country/Region	country に名称変更
PhoneCntry	phoneBusinessCountryCode に名称変更

列ヘッダー名	変更内容
PhoneLocal	phoneBusinessNumber に名称変更
CellCntry	phoneMobileCountryCode に名称変更
CellLocal	phoneMobileNumber に名称変更
すべてのトラッキング コード	定義したトラッキング コードの量に基づいて「TC#」に名前を変更します。

5 UTF-8 形式または UTL-16 LE 形式でファイルを保存します。

6 この変更したファイルを、Cisco WebEx Messenger 管理ツールから Cisco WebEx Messenger 組織にインポートします。

7 インポート ステータス ファイルの [ステータス（status）] および [ステータス メッセージ（statusMessage）] 列を確認することで、Cisco WebEx Messenger アカウントが Cisco WebEx Meeting アプリケーション ユーザ用に作成されていることを確認します。

密結合統合がアクティブになると、Cisco WebEx Meeting アプリケーション ユーザは以前のサインイン資格情報（ユーザ名/パスワードなど）ではサインインできなくなります。WebEx Meeting アプリケーション ユーザが Cisco WebEx Meeting アプリケーションにサインインする場合、その Cisco WebEx Messenger のサインイン資格情報（ユーザ名/パスワードなど）を使用する必要があります。すべてのユーザがこの変更と変更時期について認識していることを確認します。組織管理者は、すべてのユーザに考えられる変更内容を事前に通知することが推奨されます。

Cisco WebEx プロビジョニング チームに Cisco WebEx Messenger と Cisco WebEx Meeting アプリケーションの間で密結合統合を有効にするように要求します。

8 統合の成功を確認するには、新規展開の Cisco WebEx Messenger と既存展開の Cisco WebEx Meeting アプリケーションとの密結合統合の成功確認, （53 ページ）を参照してください。

シナリオ 3：新規展開の Cisco WebEx Meeting アプリケーションと既存展開の Cisco WebEx Messenger との密結合統合

新規展開の Cisco WebEx Meeting アプリケーションと既存展開の Cisco WebEx Messenger との密結合統合を有効にするためのプロビジョニング手順は、新規展開の Cisco WebEx Meeting アプリケーションと新規展開の Cisco WebEx Messenger との密結合統合を有効にする場合と似ています。詳細については、上記のシナリオ *1* を参照してください。

Cisco WebEx および Cisco WebEx Meeting アプリケーション両方の新規展開時の密結合統合の成功確認

Cisco WebEx および Cisco WebEx Meeting アプリケーション両方の新規展開時の密結合統合の成功を確認する前に、すべてのプロビジョニング手順が完了していることを確認します。詳細については、のシナリオ *1* を参照してください。 密結合統合のプロビジョニング, （49 ページ）

手順

ステップ 1 密結合統合の成功を確認するには、[設定（Configuration）]タブを選択し、[追加サービス（Additional Services）] セクションで、[会議（Meetings）] を選択します。

ステップ 2 Cisco WebEx の「ボール」が Cisco WebEx Meeting アプリケーション サイトの URL の前に表示されていることを確認します。サイト URL は変更できません。

ステップ 3 Cisco WebEx と Cisco WebEx Meeting アプリケーションの統合を有効にするには、[会議の統合を有効化（Enable Meeting Integration）]を選択します。
Cisco WebEx バージョン 7.2.2 以降を使用していて、このチェックボックスを無効にしている場合、すべての会議関連の設定オプションと機能は、Cisco WebEx アプリケーションのユーザに対して表示されなくなります。

ステップ 4 Cisco WebEx Meeting アプリケーション サイトの URL をユーザに対して表示するには、アプリケーションのホスト アカウント セットアップ セクションで [ユーザに表示（Display to User）]チェックボックスを選択します。

ステップ 5 [概要説明（Brief Description）]ボックスで、Cisco WebEx Meeting アプリケーション サイトについてわかりやすい説明を入力します。

ステップ 6 特定の Cisco WebEx Meeting アプリケーション URL に対して、[デフォルトとして選択（Select as Default）]ボタンを選択すると、ユーザがアプリケーションでホストアカウントをセットアップするときに表示するデフォルト サイトとして、その URL が表示されます。Cisco WebEx Meeting アプリケーション URL が 1 つある場合、それがデフォルトとして選択されます。

ステップ 7 [新しいユーザの作成時に会議アカウントを自動的に有効にする（Automatically enable Meeting account when creating a new user）]がデフォルトで選択されていることを確認します。すべてのユーザにデフォルトで Cisco WebEx Meeting アプリケーション サービスを提供する予定がない場合は、このチェックボックスをオフにします。
これにより、Cisco WebEx Messenger 組織で作成した新規ユーザごとに、対応する Cisco WebEx Meeting アプリケーションのアカウントが自動的に作成されます。

（注） [新しいユーザの作成時に会議アカウントを自動的に有効にする（Automatically enable Meeting account when creating a new user）]をクリアすると、作成した新規ユーザごとに、Cisco WebEx Meeting アプリケーション アカウントを手動で有効にする必要があります。

ステップ 8 Cisco WebEx Meeting アプリケーション アカウントが自動的に作成されたかどうかを確認するには、新規作成したユーザのプロファイルを開き、[詳細設定（Advanced Settings）]をクリックします。

Cisco WebEx Meeting アプリケーションの [サイト管理（Site Administration）]ページが開き、ユーザ プロファイルが表示されます。

ステップ 9 [保存（Save）]を選択します。

新規展開の Cisco WebEx Messenger と既存展開の Cisco WebEx Meeting アプリケーションとの密結合統合の成功確認

はじめる前に

Cisco WebEx および Cisco WebEx Meeting アプリケーション両方の新規展開時の密結合統合の成功を確認する前に、すべてのプロビジョニング手順が完了していることを確認します。詳細については、次を参照してください。 密結合統合のプロビジョニング，（49 ページ）

手順

ステップ 1 密結合統合の成功を確認するには、[設定（Configuration）] タブ > [追加サービス（Additional Services）] > [会議（Meetings）] を選択します。

ステップ 2 Cisco WebEx の「ボール」が Cisco WebEx Meeting アプリケーション サイトの URL の前に表示されていることを確認します。サイト URL は変更できません。

ステップ 3 Cisco WebEx と Cisco WebEx Meeting アプリケーションの統合を有効にするには、[会議の統合を有効化（Enable Meeting Integration）]を選択します。
Cisco WebEx バージョン 7.2.2 以降を使用していて、このチェックボックスを無効にしている場合、すべての会議関連の設定オプションと機能は、Cisco WebEx アプリケーションのユーザに対して表示されません。

ステップ 4 会議のホスト時および参加時に Cisco WebEx Meeting アプリケーション サイトの URL をユーザに対して表示するには、[ユーザに表示（Display to User）]チェックボックスを選択します。

ステップ 5 [概要説明（Brief Description）]ボックスで、Cisco WebEx Meeting アプリケーション サイトについて関連する説明を入力します。

ステップ 6 特定の Cisco WebEx Meeting アプリケーション URL に対して、[デフォルトとして選択（Select as Default）]ボタンを選択すると、ユーザがアプリケーションでホストアカウントをセットアップするときに示されるデフォルト サイトとして、その URL が表示されます。
Cisco WebEx Meeting アプリケーション URL が 1 つある場合、それがデフォルトとして選択されます。

ステップ 7 [新しいユーザの作成時に会議アカウントを自動的に有効にする（Automatically enable Meeting account when creating a new user）]がデフォルトで選択されていることを確認します。すべてのユーザにデフォルトで Cisco WebEx Meeting アプリケーション サービスを提供する予定がない場合は、このチェックボックスをオフにします。
これにより、Cisco WebEx Messenger 組織で作成した新規ユーザごとに、対応する Cisco WebEx Meeting アプリケーションのアカウントが自動的に作成されます。

（注） [新しいユーザの作成時に会議アカウントを自動的に有効にする（Automatically enable Meeting account when creating a new user）]をクリアすると、作成した新規ユーザごとに、Cisco WebEx Meeting アプリケーションアカウントを手動で有効にする必要があります。

ステップ 8 Cisco WebEx Meeting アプリケーション アカウントが自動的に作成されたかどうかを確認するには、新規作成したユーザのプロファイルを開き、[詳細設定（Advanced Settings）]をクリックします。
Cisco WebEx Meeting アプリケーションの [サイト管理（Site Administration）]ページが開き、ユーザ プロファイルが表示されます。

ステップ 9 [保存（Save）]を選択します。

新規展開の Cisco WebEx Meeting アプリケーションと既存展開の Cisco WebEx Messenger との密結合統合の成功確認

新規展開の Cisco WebEx Meeting アプリケーションと既存展開の Cisco WebEx Messenger との密結合統合の成功を確認する前に、すべてのプロビジョニング手順が完了していることを確認します。このプロビジョニング手順は、新規展開の Cisco WebEx Meeting アプリケーションと新規展開の Cisco WebEx Messenger との密結合統合の手順と似ています。プロビジョニング手順については、「密結合統合のプロビジョニング手順」のシナリオ 3 というタイトルのセクションを参照してください。

密結合統合が成功したかどうかを確認する手順は、Cisco WebEx Messenger および Cisco WebEx Meetingアプリケーション両方の新規展開時の密結合統合の成功を確認するトピックで説明した手順と同じです。

密結合統合が完了すると、Cisco WebEx Messenger 組織管理者は通常、次の管理タスクを実行します。

- 既存または新しい Cisco WebEx Messenger ユーザに対して Cisco WebEx Meeting アプリケーション アカウントを作成します。ユーザの作成の詳細については、新しいユーザの作成，（14 ページ）を参照してください。
- CSV ファイルを使用して、Cisco WebEx Messenger に Cisco WebEx Meeting アプリケーションのアカウントを直接インポートします。詳細については、CSV ファイルを使用したユーザのインポートとエクスポート，（16 ページ）を参照してください。

疎結合統合の概要

疎結合統合を行うと、Cisco WebEx Messenger 組織に必要な構成を最小限に抑えることができます。疎結合統合を行うことでユーザは、Cisco WebEx Messenger 内に Cisco WebEx Meeting アプリケーションのアカウントを手動で設定する必要がなくなります。

疎結合統合は、一般的に次のような組織に推奨されます。

- Cisco WebEx Meeting アプリケーションのユーザだが、Cisco WebEx Messenger のユーザではないユーザがいる組織
- 既存の Cisco WebEx Meeting アプリケーション サイトがあり、Cisco WebEx Meeting アプリケーション サイトへのユーザのサインイン方法を変更したくない組織

企業の疎結合統合を有効にするための一般的なシナリオは次の 2 つです。

- シングル サインオン統合をしている企業
- シングル サインオン統合をしていない企業

Cisco WebEx Messenger と Cisco WebEx Meeting アプリケーション間の疎結合統合を有効にするための手順は、各シナリオで異なります。各シナリオの詳細については、以下のトピックを参照してください。

- 疎結合統合のプロビジョニング, （56 ページ）
- シングル サインオン インフラストラクチャがある組織の疎結合統合の成功の確認, （56 ページ）
- シングル サインオン インフラストラクチャのない組織の疎結合統合の成功の確認, （57 ページ）

疎結合統合のシステム要件

疎結合統合を有効にする前に、次のシステム要件が満たされていることを確認します。

項目	要件
Cisco WebEx Meeting アプリケーション	Version T26L Service Pack EP 20 または Windows T27L Service Pack 9 現在実行している Cisco WebEx Meeting アプリケーションのバージョンを確認するには、使用ブラウザのアドレス バーに、次の形式で Cisco WebEx Meeting アプリケーションの URL を入力します。 https://[sitename].webex.com/version/wbxversionlist.do?siteurl=[sitename] または、Cisco WebEx のセールス担当者に連絡してバージョンを確認してください。

項目	要件
組織	• シングル サインオンに対応する Cisco WebEx Messenger 組織は、シングル サインオンに対応する Cisco WebEx Meeting アプリケーション サイトとのみ統合できます。 • シングル サインオンに対応していない Cisco WebEx Messenger 組織は、シングル サインオンに対応していない Cisco WebEx Meeting アプリケーション サイトとのみ統合できます。

疎結合統合のプロビジョニング

ここでは、Cisco WebEx Messenger と Cisco WebEx Meeting アプリケーションの間で密結合統合を有効にするためのプロビジョニング手順を説明します。このプロビジョニング手順は、シングル サインオン インフラストラクチャの有無にかかわらず、どの組織でも同じです。シングル サインオン インフラストラクチャを使用していない組織では、単独の Cisco WebEx Meeting アプリケーション サイトだけを Cisco WebEx Messenger と統合できます。疎結合統合の詳細については、疎結合統合の概要, （54 ページ）を参照してください。

Cisco WebEx Messenger と Cisco WebEx Meeting アプリケーションの間で疎結合統合を有効にする前に、次の準備手順が完了していることを確認します。

- シングル サインオンに対応する Cisco WebEx Meeting アプリケーション サイトとの疎結合統合を設定するように Cisco WebEx プロビジョニング チームに依頼します。
- Cisco WebEx Meeting アプリケーション サイトの URL と、Cisco WebEx Messenger と Cisco WebEx Meeting アプリケーションの間の共通ユーザ アイデンティティを提供します。
- Cisco WebEx Messenger 管理ツールにログインして、疎結合統合が成功したことを確認します。

シングル サインオン インフラストラクチャがある組織の疎結合統合の成功の確認

統合の成功を確認する前にプロビジョニング手順を完了していることを確認します。詳細については、疎結合統合のプロビジョニング, （56 ページ）を参照してください。

手順

ステップ 1 疎結合統合の成功を確認するには、[設定（Configuration）] タブ > [追加のサービス（Additional Services）] > [会議（Meetings）] を選択します。

ステップ 2 複数の Cisco WebEx Meeting アプリケーション サイトとの統合を有効にしている場合は、それらすべてのサイトが表示されていることを確認します。

ステップ 3 Cisco WebEx Messenger 組織のデフォルトとなる Cisco WebEx Meeting アプリケーションに対して、[デフォルトとして設定（Set as default）]を選択します。
ユーザが Cisco Jabber アプリケーションからワンクリックミーティングを開始するたびに、このデフォルト サイトが使用されます。

ステップ 4 [保存（Save）]を選択します。

（注） [共通ユーザ ID（Common User Identity）]により、Cisco WebEx Messenger と Cisco WebEx Meeting アプリケーション間のユーザの 1 対 1 のマッピングが決まります。

シングル サインオン インフラストラクチャのない組織の疎結合統合の成功の確認

統合の成功を確認する前にプロビジョニング手順を完了していることを確認します。詳細については、疎結合統合のプロビジョニング, （56 ページ）を参照してください。

手順

ステップ 1 疎結合統合の成功を確認するには、[設定（Configuration）] タブ > [追加のサービス（Additional Services）] > [会議（Meetings）] を選択します。

ステップ 2 疎結合統合を有効にした Cisco WebEx Meeting アプリケーション サイトの URL が表示されていることを確認します。

（注） [統合の有効化（Activate Integration）]ボタンを使用すると、Cisco WebEx Meeting アプリケーションとの密結合統合が有効になります。密結合統合の概要, （47 ページ）を参照してください。.

古い Cisco WebEx Messenger 組織と Cisco WebEx Meeting アプリケーションの統合

手順

ステップ 1 Cisco WebEx Messenger 組織と Cisco WebEx アプリケーション間の統合を有効にするには、[設定（Configuration）] タブ > [追加サービス（Additional Services）] > [会議（Meetings）] を選択します。

ステップ 2 [サイト URL（Site URL）]フィールドに、Cisco WebEx Messenger 組織と統合させる Cisco WebEx Meeting アプリケーションのサイトの URL を入力します。[サイト URL（Site URL）]フィールドは、最初は空欄です。
サイト URLを設定した後、[会議、サイト オプション（Meetings, Site Options）]ウィンドウが表示されます。

ステップ 3 [概要説明（Brief Description）]ボックスで、統合を有効にする Cisco WebEx アプリケーション サイトの説明を入力します。

ステップ 4 [保存（Save）]を選択し、Cisco WebEx Messenger および Cisco WebEx アプリケーションの統合設定を保存します。

IM フェデレーション設定

Cisco WebEx Messenger は、Google Talk などのパブリック XMPP ベースの IM ネットワークとのフェデレーションを有効にするように設定できます。また、サードパーティの XMPP アプリケーションを使用した Cisco WebEx Messenger ドメインへの接続も可能にします。

（注） DNS には次の 2 種類のレコードを公開できます。

- 最初の SRV レコードを公開すると、ユーザはパブリック XMPP ネットワークのユーザと通信できるようになります。
- 2 番目の SRV レコードを公開すると、ユーザはサードパーティの XMPP アプリケーションを使用して Cisco WebEx Messenger ドメインに接続できるようになります。

IM フェデレーション設定の指定

手順

ステップ 1 IM フェデレーション設定を指定するには、[設定（Configuration）]タブを選択し、[追加サービス（Additional Services）] の下にある [IM フェデレーション（IM Federation）] を選択します。

ステップ 2 [IM フェデレーション（IM Federation）]画面に表示される情報に従って DNS SRV レコードを更新します。

IM ログ記録とアーカイブの概要

Cisco WebEx Messenger では、組織内のユーザが社内または社外のユーザと交換するインスタントメッセージ（IM）をログに記録して、アーカイブすることができます。IM ログ記録とアーカイブを使用すると、組織は IM の交換をモニタして確認することができます。ほとんどの場合、これは企業の情報監査プロセスに準拠するために行われます。

Cisco WebEx Messenger 組織内のユーザに対して IM ログ記録とアーカイブを有効にすることができます。Cisco WebEx Messenger では、アーカイブ対象のログに記録したメッセージを次のアーカイブ ソリューションに送信できます。

- HP Autonomy DRC-CM（旧 Iron Mountain DRC-CM）
- Global Relay Message Archiver
- セキュア SMTP サービス（Secure SMTP Service）：このオプションを使用すると、電子メールの本文にある IM を受信するように SMTP サーバを設定できます。この場合、IM は電子メールと同じアーカイブ システムの一部になり、電子メールに使用しているのと同じアーカイブおよび監査ソリューションを使用できるようになります。

  HP Autonomy DRC-CM および Global Relay Message Archiver は、SaaS ベースのメッセージ アーカイブ サービスです。

IM セッションで記録される情報

以下は、IM セッションで記録される情報です。

- 日付および時刻（Date and Time）
- 参加者（ユーザ名）
- プレーン テキスト
- HTML（顔文字と同等のテキストを含む）

- 招待および参加者の参加と脱退などのシステム メッセージ
- ファイル転送の開始と終了（ファイルの名前、ファイルのサイズを含む）
- ビデオ コールの開始と終了
- PC 間コールの開始と終了
- 音声会議の開始と終了
- Cisco WebEx Meeting の開始と終了
- デスクトップの共有の開始と終了
- 電話の開始と終了

ログ記録される IM ユーザの制限

ログ記録される IM ユーザには次の制限事項が適用されます。

- IM のログ記録が必要なユーザは、Cisco Jabber アプリケーション バージョン 9.x 以降のデスクトップ クライアントを使用する必要があります。ただし、他の参加者はそれよりも古い、または異なるIMアプリケーションを使用しながらログ記録ユーザとしてIMセッションに参加できます。
- ログ記録されるユーザがサードパーティ製 IM アプリケーションを使用することはシステム上できません。
- ログ記録されるユーザがエンドツーエンド（AES）暗号化を有効にすることはできません。ログ記録されるユーザがエンドツーエンドの暗号化を有効にしている場合、ユーザの「記録」ステータスが優先され、そのユーザに対するエンドツーエンドの暗号化は無効になります。
- ログ記録されるユーザは暗号化されているグループ チャット セッションに参加できません。
- ログ記録されるユーザはフェデレーテッド ユーザ（AIM または GoogleTalk ネットワークなどのユーザ）がホストするグループ チャットに参加できません。ただし、フェデレーテッド ユーザは Cisco WebEx Messenger のログ記録されるユーザがホストするグループ チャットには参加できます。

  IMは、セキュリティで保護されたチャネル経由でお客様のサーバに送信されるまで、シスコのデータセンターに一時的に保存されます。送信が完了すると、これらのIMはシスコのデータセンターから完全に削除されます。

IM アーカイブ通知

IM アーカイブ通知を設定することで、ユーザの IM がアーカイブされていることをユーザに通知するかどうかを選択できます。この通知はシステムによって送信されます。デフォルトのメッセージ テキストは以下のとおりです。

このセッションで送信されるインスタント メッセージはすべてこのアカウントを介して行われます。また、その他すべての通信方法（音声コール、ビデオ コールなど）の開始と終了はログに記録され、アーカイブ、モニタリング、レビュー、および受信者以外のユーザへの情報開示の対象になります。

ただし、自分の組織の要件に合わせてデフォルトのメッセージ テキストをオーバーライドすることができます。詳細については、IM ログ記録の設定とアーカイブ通知, （64 ページ）を参照してください。

1 人以上の IM ログイン済みユーザが 1 対 1 のチャットまたはグループ チャットに参加している場合、会話はログに記録されていて、1 人以上のユーザの組織によってアーカイブされているという通知メッセージが、システムから関係しているすべてのユーザに送信されます。

IM ログ記録およびアーカイブ通知の頻度

通知は会話に参加しているすべてのユーザに送信され、会話内のログイン済みユーザごとに 1 つ送信されます。たとえば、5 人のユーザがグループ チャットに参加していて 3 人がログインしている場合、5 人のユーザ全員に 3 つの通知が送信されます。この例外は次のとおりです。

- 重複を避けるため、ユーザには同一テキストの通知メッセージのコピーは 1 つだけ送信されます。ユーザが 1 対 1 のチャットまたはグループ チャットに参加しているかどうかに関係なく、ユーザが同一テキスト メッセージ（デフォルトまたはカスタム）を使用している組織のメンバーの場合、そのユーザには 1 つの通知のみ表示されます。
- 会話に参加しているいずれかのログイン済みユーザの組織がカスタム通知メッセージを使用している場合、すべてのユーザにそのメッセージが表示されます。たとえば、グループチャットに参加している 3 人のユーザのうち、2 人のメッセージがデフォルトで、1 人のメッセージがカスタムの場合、すべてのユーザに 2 つの通知（デフォルトとカスタム）が表示されます。

  システムから特定の会話に対して通知が送信されるのは 1 時間に 1 回だけです。

  通知のタイムアウト期限が切れると、IM の交換やユーザがグループ チャットに参加するなどの新しいアクティビティが発生しない限り、新しい通知は送信されません。

IM アーカイブ エンドポイントの定義

Cisco WebEx Messenger 組織の IM アーカイブの設定には、Cisco WebEx Messenger 管理ツールでのアーカイブ エンドポイントの設定作業が含まれます。IM アーカイブのエンドポイントは、ログに記録された IM データが送信される場所です。複数のエンドポイントを設定できます。

エンドポイントの設定では、次のパラメータを指定する必要があります。

- エンドポイント名
- エンドポイント タイプ
- エンドポイントのパラメータ：パラメータはエンドポイントのタイプによって異なります。

  IM アーカイブ エンドポイントの設定方法については、IM アーカイブの設定, （62 ページ）を参照してください。

IM アーカイブのエンドポイントを設定したら、ログに記録するユーザを Cisco WebEx Messenger 組織に割り当てる必要があります。以下に示すように、ログに記録するユーザを割り当てるためのプロビジョニング方法は複数あります。

- 新規ユーザを作成する。詳細については、新しいユーザの作成, （14 ページ）を参照してください。
- CSV ファイルを使用する。詳細については、CSV ファイル形式, （143 ページ）を参照してください。
- ディレクトリ統合を行う。詳細については、ディレクトリ統合のインポートプロセスとファイル形式, （124 ページ）を参照してください。
- SAML を使用する。詳細については、Cisco WebEx Messenger 管理ツールでのシングル サインオンの設定, （69 ページ）を参照してください。

組織の IM ログ記録およびアーカイブの有効化

IM アーカイブは、Cisco WebEx からプロビジョニングするために必要な別のソリューションです。組織の IM アーカイブをプロビジョニングする方法の詳細については、Cisco WebEx Customer Success Manager にお問い合わせください。

プロビジョニング情報は、[設定（Configuration）] タブの [リソース管理（Resource Management）] の下にある Cisco WebEx 管理ツールに表示されます。IM アーカイブは、Cisco WebEx Messenger 組織でプロビジョニングされているユーザ数を上回るユーザに対しては機能しません。詳細については、リソース管理情報, （26 ページ）を参照してください。

IM アーカイブの設定

[IM アーカイブ（IM Archiving）]画面では、Cisco WebEx Messenger 組織のユーザ間で交換されるインスタント メッセージをアーカイブするエンドポイントを設定することができます。複数のエンドポイントを設定できます。ただし、1 人のユーザを割り当てることができるエンドポイントは、一度に 1 つだけです。

手順

ステップ 1 IM アーカイブを設定するには、[設定（Configuration）] タブ > [IM アーカイブ（IM Archiving）] を選択します。
エンドポイントを設定しない場合、[IM アーカイブ（IM Archiving）]ウィンドウは空欄です。

ステップ 2 [追加（Add）]を選択して、[アーカイブ エンドポイントの追加（Add Archiving Endpoint）] ウィンドウを開きます。

ステップ 3 [エンドポイント名（Endpoint Name）]フィールドに、エンドポイントの名前を入力します。エンドポイント名にスペースを含めることはできません。

ステップ 4 選択したエンドポイントの種類に応じて、入力する必要があるフィールドは異なります。[タイプ（Type）]ドロップダウンリストから、エンドポイントのタイプを選択します。

- グローバル リレー メッセージ アーカイバ
- HP Autonomy DRC-CM（旧称 Iron Mountain DRC-CM）
- セキュア SMTP サービス
- （注） Cisco WebEx Messenger は、アーカイブ エンドポイントへのセキュアな接続を常にネゴシエートします。アーカイブ エンドポイントでは、安全な SMTP サービスのために次の設定が必要です。
  - STARTTLS のサポートが必要です。SSL が使用されている場合でも、エンドポイントは STARTTLS をサポートする必要があります。
  - SSL を使用する場合、ポート 25 ではなくポート 465 を使用します。
  - アーカイブ エンドポイントによって提供される証明書は、公的に信頼されている証明書認証局（CA）によって発行されたものである必要があります。自己署名証明書はサポートされません。

ステップ 5 すべてのフィールドに入力したら、エンドポイント設定をテストするため、[テスト（Test）]を選択します。
テストが成功するまでエンドポイントを保存することはできません。テストに失敗した場合はエラー メッセージが表示されます。

ステップ 6 [結果を表示（View Results）]を選択し、テストが失敗した原因となった設定の問題を確認します。問題を修正したら、再度 [テスト（Test）]を選択できます。テストに成功すると、成功メッセージが表示されます。

ステップ 7 設定テストに成功したら、[保存（Save）] を選択し、エンドポイントの設定を保存して に戻ります。

ステップ 8 別のエンドポイントを追加するには、このセクションで上述した同じ手順を実行します。

ステップ 9 正常に設定されたエンドポイントが [IM アーカイブ（IM Archiving）]ウィンドウのエンドポイント リストに表示されない場合、[更新（Refresh）] を選択します。

ステップ 10 デフォルトのエンドポイントとしてエンドポイントを設定するには、[デフォルトエンドポイント（Default Endpoint）]の列の下で適切なボタンを選択します。
特定のエンドポイントに（名前によって）割り当てられていないユーザは、デフォルトのエンドポイントに割り当てられます。

ステップ 11 ユーザをエンドポイントに関連付けている場合、エンドポイントに関連付けられているユーザのリストを表示するには [ユーザの表示（View Users）]を選択します。

エンドポイントは、最長でも 1 時間以内にログの受信を開始します。システムは、この時間を使用してエンドポイントを登録します。

電子メールでの IM のバッチ処理

アーカイブ サービスは、2 人のユーザまたは 1 人のユーザとグループ チャット ルーム間のメッセージを単一の電子メールにグループ化しようとします。ユーザの通信は一括で行われるため、サービスは 8 時間待機してから、一連のユーザ メッセージを送信します。このため、各電子メールに少数の IM が含まれている電子メールを大量に送信することを回避できます。このバッチ処理の結果、メールのエンドポイントでは 8 時間経過する前にアーカイブ済みの電子メールを受信しなくなります。

（注） アーカイブのエンドポイントに送信する際には、最大 50 件のメッセージが一度にバッチ処理されます。

アーカイブのエンドポイントが到達不能な場合のシステムの動作

アーカイブのエンドポイントが到達不能な場合、Cisco WebEx Messenger は、1 時間、2 時間、4 時間、および 8 時間の間隔でエンドポイントへの送信を再試行します。8 時間を超えた場合、Cisco WebEx Messenger は最大 90 日間、1 日に一度再試行します。各再試行では、組織管理者に対して設定されている電子メール アドレス宛に電子メール通知が送信されます。各再試行およびアーカイブ エンドポイントの応答のログを確認するには、[設定（Configuration）] > [IM のアーカイブ（IM Archiving）] > [結果の表示（View Results）]を選択します。

重要 組織管理者は、電子メール通知を受信したらすぐにアーカイブ エンドポイントの問題を修正する操作を行い、送信待ちメッセージのバックログが発生しないようにする必要があります。

IM ログ記録の設定とアーカイブ通知

[IM アーカイブ（IM Archiving）]画面では、IM ユーザの間で交換されるインスタント メッセージが記録され、アーカイブされたことを伝える自動通知を IM ユーザに対して送信することもできます。

手順

ステップ 1 IM ログ記録とアーカイブ通知を設定するには、[設定（Configuration）] タブ> [IM ログ記録（IM Archiving）] を選択し、次のいずれかを実行します。

- [IM がアーカイブされていることを組織内のユーザに通知する（Notify users in your Organization that their IMs are being archived）]を選択します。これはデフォルトで有効であり、1 人以上のログインしているユーザとの 1 対 1 またはグループでのチャット セッションが開始されたときに、組織のすべてのユーザに通知が送信されます。この設定が無効な場合は、組織のユーザに通知は送信されません。
- [デフォルトの通知メッセージを上書き（Override default notification message）]は、組織のニーズに合わせて、デフォルトのアーカイブ通知メッセージのテキストを編集するために選択します。カスタム通知メッセージは、500 文字（UTF-8）までに制限されます。

  （注） デフォルトの通知テキストを編集した後で、元のデフォルトのテキストに戻したい場合は、[リセット（Reset）]を選択します。

ステップ 2 [保存（Save）]を選択します。

（注） 上記の設定に対する変更が適用されるには数時間かかります。これは、すべてのサーバに変更を伝えるために必要な時間です。

IM トランスクリプトの形式は、インスタント メッセージが記録されるときにアーカイブ エンドポイントに送信されます。

記録されたメッセージ テキスト、タイムスタンプ、エンドポイントで設定される電子メールの件名などの詳細を確認できます。

[タイムスタンプ（Timestamps）]は、CCYY-MM-DDThh:mm:ss 形式の XEP-0082 プロトコルに従って、UTC のタイム ゾーンで表示されます。

第 4 章

シングル サインオン

概要

標準構成では、ユーザのサインイン名とパスワードは、企業または組織で使用されている認証資格情報とは無関係です。そのため、ユーザは別の一連のサインイン資格情報を覚える必要があります。また、組織管理者は別の一連のユーザ アカウントを管理する必要があります。

シングル サインオンを採用している企業は、社内のシングル サインオン システムを使用して、Cisco WebEx 管理の管理を簡素化できます。シングル サインオンにより、ユーザは自社のサインイン資格情報を使用してアプリケーションに安全にサインインできます。ユーザのサインイン資格情報は Cisco WebEx に送信されないため、ユーザの会社のサインイン情報は保護されます。

シングルサインオン設定オプションを設定すると、ユーザの初回サインイン時にユーザアカウントが自動的に作成されます。シングルサインオンを使用すると、会社のサインインアカウントが非アクティブ化されている場合に、ユーザが Cisco WebEx アプリケーションにアクセスするのを防ぐこともできます。

Cisco WebEx アプリケーションは、業界標準のセキュリティ アサーション マークアップ言語（SAML2）および WS-Federation プロトコルに基づくシングル サインオン システムをサポートします。

Cisco WebEx および Cisco WebEx Meeting アプリケーションでの SSO の使用

Cisco WebEx サービスの 1 つの目的は、組織のユーザ アイデンティティを包括的に管理することです。ユーザ アイデンティティの管理には、認証と認可のための安全な機能の提供が含まれます。これらの機能は、組織内のユーザ ロールとグループ関係に基づいた使い勝手を高め、ポリシー制御を容易にします。

SAML2（セキュリティ アサーション マークアップ言語）およびWSフェデレーションなどのフェデレーテッド シングル サインオン標準は、そのような安全な認証機能を提供しています。SAML 対応のアイデンティティ管理システムは、Cisco WebEx サービスに SAML アサーションを送信します。SAML アサーションは、情報カテゴリに関する信頼されたステートメントが記述された XML ドキュメントです。通常、これらの信頼されたステートメントには、ユーザ名、電子メール、およびその他のプロファイル情報などの情報が含まれます。信頼性を確保するために、SAML アサーションはデジタル署名されます。

通常、企業はユーザ アイデンティティの管理のためにフェデレーテッド ID と Access Management System（IAM）を展開しています。これらのIAMシステムは、ユーザアイデンティティ管理アクティビティに SAML および WS フェデレーション標準を使用します。より優れたエンタープライズクラスの IAM システムには、CA SiteMinder、Ping Federate、および Windows Active Directory Federation Services（ADFS）などがあります。これらの IAM システムが社内のイントラネットの一部を形成し、従業員やパートナーのユーザ認証およびシングル サインオン要件に対応します。IAM システムは、ファイアウォールの外側にあるパートナー Web サイトと相互運用するため、SAML または WS フェデレーション プロトコルを使用します。顧客、パートナー、ベンダーは、IAM システムを使用して Cisco WebEx サービスに対してそのユーザを自動的に認証することができます。ユーザは Cisco WebEx サービスを使用するために自分のユーザ名とパスワードを思い出す必要がないため、効率が向上します。

また、退職する従業員を外部管理ツールで明示的に無効にする必要もありません。従業員が顧客の IAM システムから削除されると、Cisco WebEx サービスのいずれに対してもその従業員を認証できなくなります。

（注） Cisco WebEx Messenger でシングル サインオンを有効にするには、担当のカスタマー サクセス マネージャにお問い合わせください。

シングル サインオンの要件

Cisco WebEx 組織にフェデレーテッド シングル サインオンを実装するには、次のシステム要件が必要です。これらのシステム要件は、Cisco WebEx Messenger および Cisco WebEx Meeting アプリケーションと同じです。

項目	要件	注記
アイデンティティとアクセス管理（IAM）システム	SAML バージョン（Cisco WebEx Meeting のみ）2.0 または WS フェデレーション 1.0 標準に準拠した IAM。	お客様は、OpenSAML のようなプログラミング ライブラリを使用して独自の SAML 対応 IAM システムを開発することも、Ping Federate、CA SiteMinder、Microsoft Windows Server ADFS、Oracle Identity Federation/OpenSSO、Novell Identity Manager および IBM Tivoli Federated Identity Manager などの民間企業のサードパーティ製 IAM システムを購入することもできます。
X.509 証明書に公開キーがあり、デジタル署名が秘密キーを使用する	PEM 形式の、VeriSign や Thawte のような信頼できる組織からのもの。	または、自己署名証明書を使用する、社内で開発した独自の X.509 証明書を使用することもできます。

Cisco WebEx Messenger 管理ツールでのシングル サインオンの設定

組織管理者は Cisco WebEx 管理ツールを使用して、シングル サインオンの設定を行い、Cisco WebEx 組織のセキュリティ設定および証明書を変更できます。オプションは、管理者が設定する組織の設定に基づいて表示されます。すべてのオプションが常に表示されるわけではありません。

- [フェデレーテッド Web SSO 構成（Federated Web SSO Configuration）]を選択すると、シングル サインオンを有効にしている組織の管理者向けのダイアログが表示されます。
- [組織証明書の管理（Organization Certificate Management）]を選択すると、シングル サインオンを有効にしている組織の管理者、または「委任認証」管理者用の、管理者向けダイアログが表示されます。これは、X.509 証明書を手動でインポート、検証、または削除するために使用します。組織証明書の管理は、組織管理者のための管理ツールです。
- [WebEx 証明書の管理（WebEx Certificate Management）]を選択すると、シングル サインオンを有効にしている組織の管理者向けのダイアログが表示されます。これは、組織管理者がサービス プロバイダーの証明書を作成するための管理ツールとして使用されます。このツールは、SP からの開始によって使用されます。自己署名証明書は Cisco WebEx によって生成され、IAM システムにアップロードする必要があります。証明書は以下の場合に生成されます。
  - AuthnRequest に署名するため
  - SAML アサーションの暗号化のため
  - シングル ログアウトを有効にするため

自己署名証明書または認証局は事前に生成されており、インポート可能になっています。管理者は組織に適用するものを選択できます。

- [パートナー Web SSO 構成（Partner Web SSO Configuration）]を選択すると、「委任認証」の組織の管理者向けダイアログが表示されます。パートナー委任では、管理者がパートナーアプリケーション向けに単一のユーザ名とパスワード認証によるサインオンページを設定することができます。管理者は、この機能を使用してセキュリティを高め、サインオンとパスワードの複数の要件を減らし、ユーザが複数のサインオン資格情報を追跡する必要性を排除する必要があります。
- SAML 2.0 の構成も設定できます。属性は次の表に表示されています。

属性	必須（/×）	使用方法
uid	○	
firstname	○	
lastname	○	
email	○	
groupid	×	作成のみサポート、更新は未サポート
updateTimeStamp	×、ただし推奨	長い値、UTC 時間形式、LDIF 時間形式をサポート
displayName	×	
companyName	×	
businessFax	×	
streetLine1	×	
streetLine2	×	
city	×	
state	×	
zipcode	×	
jobTitle	×	
mobilePhone	×	
businessPhone	×	

属性	必須（/×）	使用方法
employeeid	×	
imloggingenabled	×	組織でIMログ記録が有効になっていて、該当する属性が存在しない場合、Falseに設定されます。
imloggingendpointname	×	組織でIMログ記録が有効になっていて、該当する属性が存在しない場合、wbx_default_endpointに設定されます。
ISOCountry	×	2文字のISO国番号
upgrade site	×	ヌル以外の「upgradesite」属性が存在する場合、有効化または無効化されているアカウントの自動作成機能およびアカウントの自動更新機能に対応したアクションが実行されます。 「upgradesite」属性が指定されていないか、または値が空の場合、アクションは不要です。

（注） 組織が認証メカニズムを「クラウドに保存されたユーザ名とパスワード」から「IDPによるSSO」に移行している段階では、[CAS API経由で接続アカウントのユーザ名とパスワードによるログインを許可（Allow Connect account username and password login via CAS API）] チェックボックスが選択されています。これにより、組織は段階的にSSOに移行できます。

フェデレーテッド Web SSO 設定

手順

ステップ 1 [設定（Configuration）] タブ > [システム設定（System Settings）] > [セキュリティ設定（Security Settings）].を選択します。

ステップ 2 [フェデレーテッド Web SSO 設定（Federated Web SSO Configuration）]を選択します。

ステップ 3 [フェデレーション プロトコル（Federation Protocol）]ドロップダウンから、フェデレーション プロトコル [SAML 2.0] を選択します。

ウィンドウに表示されるフィールドに、選択するフェデレーション プロトコルによって異なります。デフォルトで、SAML 2.0 の設定フィールドは [フェデレーテッド Web SSO 設定（Federated Web SSO Configuration）]ウィンドウを開くたびに表示されます。

ステップ 4 [SAML メタデータをインポート（Import SAMLMetadata）] を選択して [フェデレーテッド Web SSO 設定 - SAML メタデータ（Federated Web SSO Configuration - SAML Metadata）] ダイアログボックスを開きます。

ステップ 5 次のいずれかを実行します。

- [フェデレーテッド Web 認証（federated Web authentication）] フィールドに移動し、[SAML メタデータ（SAML Metadata）] ファイルをインポートしてこのフィールドに自動的にデータを入力します。
- [インポート（Import）]、[戻る（Back）]を選択してインポートを完了します。インポートされたメタデータ フィールドは、次のとおりです。
  - AuthnRequestSigned Destination
  - SAML（IDP ID）の発行者
  - 顧客 SSO サービス ログイン URL
- 各フィールドに適切な情報を入力します。
  「関連項目」セクションを参照してください。

ステップ 6 SAML メタデータ ファイルが正常にインポートされたら、[フェデレーテッド Web SSO 設定（Federated Web SSO Configuration）]ウィンドウの関連フィールドにデータが入力されていることを確認します。

関連トピック

フェデレーテッド Web SSO 設定, （73 ページ）

フェデレーテッド Web SSO 設定

フィールド	説明
SSO プロファイル（SSO Profile）	SP 起動：ユーザがサービス プロバイダー（SP）サイトにアクセスし、特別な認証や認可を必要としないリソースに初めてアクセスしたとき。SAML 対応の導入では、その後 SP で保護されたリソースにアクセスを試みると、SP はユーザにサインインを許可するために、認証要求とともにユーザを IDP に送信します。 AuthnRequest 署名付き宛先：選択する場合、WebEx 証明書と宛先を指定する必要があります。この宛先アドレスは、IAM の authnRequest 署名付き設定と一致している必要があります。
	IDP 起動のターゲット ページの URL パラメータ：ユーザが Cisco WebEx サービス（SP）にアクセスすると、SP は認証要求を付けずにユーザを IDP に送信します。
WebEx SAML 発行者（SP ID）（WebEx SAML Issuer（SP ID））	URI は Cisco WebEx Messenger サービスを SP として特定します。この設定は、お客様のアイデンティティ アクセス管理の設定と一致している必要があります。 デフォルト値は http://www.webex.com です。
SAML（IDP ID）の発行者（Issuer For SAML（IDP ID））	URI は IDP を一意に特定します。この設定はお客様の IAM の設定と一致している必要があります。
顧客 SSO サービス ログイン URL（Customer SSO Service Login URL）	企業のシングル サインオン サービスの URL。企業のユーザは通常、この URL からサインインします。
SAML メタデータ WebEx SP 設定ファイルをエクスポートできます。 エクスポートされたメタデータ フィールドには次のものがあります。 • AuthnRequestSigned Destination • SAML（IDP ID）の発行者 • 顧客 SSO サービス ログイン URL（Customer SSO Service Login URL）	

フィールド	説明
NamedID 形式（NamedID Format）	このフィールドは IAM の設定と一致している必要があります。サポートされる形式は以下のとおりです。 • 未指定（デフォルト） • 電子メール アドレス（Email address） • X.509 の件名 • エンティティ識別子 • 永続的な識別子
AuthnContextClassRef	アイデンティティ プロバイダーでの認証動作を記述する SAML ステートメント。このフィールドはIAMの設定と一致している必要があります。
デフォルトの WebEx ターゲット ページ URL（Default WebEx Target page URL）	これはオプションです。認証時には、Web アプリケーションに割り当てられているターゲット ページのみ表示されます。要求には RelyState パラメータは含まれていません。
Web クライアントのシングル ログアウト（Single Logout for Web Client）	サインアウトを要求し、ログアウトURLを設定するにはこのフィールドをオンにします。 注：このオプションは、Web IM アプリケーションにのみ適用されます。
アカウントの自動作成（Auto Account Creation）	ユーザ アカウントの作成を選択します。[UID]、[電子メール（email）]、[姓名（first and last name）] フィールドは、SAML アサーションに存在している必要があります。
アカウントの自動更新（Auto Account Update）	SAML アサーションで「updateTimeStamp」属性を指定します。既存のユーザアカウントを更新する場合は、このフィールドをオンにします。 「updateTimeStamp」の値は、お客様の ID ストア内でユーザのプロファイルが最後に更新された時刻です。たとえば、Active Directory では、「whenChanged」属性にこの値が設定されます。「updateTimeStamp」が属性に含まれていない場合、ユーザ プロファイルは前回の更新から更新されていません。これは、ユーザ プロファイルが [アカウントの自動更新（Auto Account Update）] または [アカウントの自動作成（Auto Account Creation）] を介して更新されたときに初めて更新されます。 オフの場合、更新が行われないことを示しています。

フィールド	説明
Active Directory UPN の UID ドメイン サフィックスを削除（Remove uid Domain Suffix for Active Directory UPN）	このフィールドを選択すると、Active Directory ドメイン部分が UPN から削除されます。 Cisco WebEx Messenger の UID には電子メール ドメインが必要なため、このフィールドをオンにするとエラーになります。その場合は、「ssoid」を使用してユーザを特定します。 デフォルトでは、SAML 2.0 および WS-Federation 1.0 はオフになっています。

WS フェデレーションの設定

SAML メタデータ ファイルが正常にインポートされたら、[フェデレーテッド Web SSO 設定（Federated Web SSO Configuration）]ダイアログ ボックスの関連フィールドにデータが入力されていることを確認します。

手順

ステップ 1 [フェデレーション プロトコル（Federation Protocol）]ドロップダウンから、フェデレーション プロトコル [WS-Federation 1.0]を選択します。[フェデレーテッド Web SSO 設定（Federated Web SSO Configuration）]ダイアログ ボックスに表示されるフィールドは、選択したフェデレーション プロトコルによって異なります。

ステップ 2 以下の追加情報を入力します。

- WebEx サービス URI：この URI は、Cisco WebEx サービスに依存する関係者を特定します。
- フェデレーション サービス URI：この URI は、企業のシングル サインオン サービス（IdP）を特定します。
- 顧客 SSO サービス ログイン URL：企業のシングル サインオン サービスの URL。企業のユーザは通常、この URL からサインインします。シングル サインオン プロファイルに応じて、IdP が開始したログイン URL と、SP が開始したサインイン URL が、IdP 設定に合わせて設定されます。

ステップ 3 [保存（Save）]を選択してフェデレーテッド Web シングル サインオン設定の詳細を保存し、[SSO 関連オプション（SSO Related Options）] 画面に戻ります。

組織の証明書管理の設定

手順

ステップ 1 使用可能な証明書を表示するには、[組織の証明書管理（Organization Certificate Management）]を選択します。
証明書は最大 3 つに制限されており、特定の時期にアクティブにできるのは 1 つだけです。以前にインポートされた X.509 証明書が表示されます。

ステップ 2 証明書の詳細を表示するには、[証明書のエイリアス（Certificate Alias）]列で証明書リンクを選択し、必要に応じて [削除（Remove）] を選択して証明書を削除します。

ステップ 3 [新しい証明書のインポート（Import New Certificate）]を選択します。
[組織の証明書管理（Organization Certificate Management）]ウィンドウが表示されます。

ステップ 4 [組織の証明書管理（Organization Certificate Management）]ウィンドウの [エイリアス（Alias）] フィールドに、会社の Cisco WebEx 組織の名前を入力します。

ステップ 5 [参照（Browse）]を選択して X.509 証明書を選択します。
証明書は CER または CRT ファイル形式である必要があります。1024、2048、または 4096 暗号化ビットおよび RC4-MD5 アルゴリズムによる証明書だけがサポートされています。

ステップ 6 [インポート（Import）]を選択して証明書をインポートします。
証明書が X.509 証明書の指定された形式に従っていない場合は、エラーが表示されます。

ステップ 7 [閉じる（Close）]を選択します。

ステップ 8 [保存（Save）]を選択して新しくインポートした組織の証明書を保存し、[SSO 関連オプション（SSO Related Options）] 画面に戻ります。

WebEx 証明書管理の設定

手順

ステップ 1 以前に生成した Cisco WebEx 証明書を表示するには、[WebEx 証明書管理（WebEx Certificate Management）]を選択します。

ステップ 2 新しい証明書を生成するには、[新しい証明書を生成（Generate New Certificate）]を選択します。
新しい証明書は通常、既存の証明書の期限が切れるときに生成されます。

ステップ 3 [WebEx 証明書管理（WebEx Certificate Management）]ウィンドウで、次の情報を入力します。

- [エイリアス（Alias）]：WebEx 証明書を特定するエイリアス。

- [有効（Val）]：WebEx の証明書の有効日数。WebEx 証明書の有効期間は最小 90 日、最大 3652 日までです。

ステップ 4 生成された証明書の詳細をすべて表示するには、証明書のエイリアスを選択します。

ステップ 5 生成された証明書の画面で、次のいずれかを選択します。

- [削除（Remove）]：証明書を削除します。アクティブな証明書は削除できません。
- [エクスポート（Export）]：証明書をエクスポートし、.cer ファイルとしてコンピュータに保存します。

ステップ 6 [閉じる（Close）]をクリックし、[WebEx 証明書管理（WebEx Certificate Management）] ウィンドウに戻ります。

ステップ 7 [アクティブ（Active）]オプションを選択し、この（新たに生成した）WebEx 証明書をアクティブな証明書としてシングル サインオン関連の認証プロセスに適用します。

ステップ 8 [保存（Save）]を選択して WebEx 証明書の変更を保存し、[SSO 関連オプション（SSO Related Options）] 画面に戻ります。

ステップ 9 アクティブな Cisco WebEx 証明書を IdP にインポートします。

パートナーの委任認証

パートナー委任では、管理者がパートナー アプリケーション向けに単一のユーザ名とパスワード認証によるサインオン ページを設定することができます。管理者は、この機能を使用してセキュリティを高め、サインオンとパスワードの複数の要件を減らし、ユーザが複数のサインオン資格情報を追跡する必要性を排除する必要があります。

パートナーの委任認証の要件

顧客とパートナーの間で信頼関係を確立する必要があります。パートナーは、顧客のユーザに代わってパートナー ルート経由で Cisco WebEx サービスにログオンする機能を果たします。パートナーの委任認証は、信頼関係と同意関係を構築するために使用される次の属性で構成されます。

- 顧客と Cisco WebEx サービス（信頼）
- パートナーと Cisco WebEx サービス（信頼）
- 顧客とパートナー（信頼と同意）

パートナーの委任認証の設定

手順

ステップ 1 証明書をアップロードするには、[WebEx 証明書管理（WebEx Certificate Management）]を使用します。

ステップ 2 SAML 2.0 の設定を構成するには、[パートナーの Web SSO 設定（Partner Web SSO Configuration）]を使用します。

ステップ 3 「委任認証」が設定されていない組織の管理者向けダイアログを表示するには、[パートナーの委任認証（Partner Delegated Authentication）]を選択します。

ステップ 4 パートナーを信頼し、メンバー、またはメンバー プラス組織管理者として行動してもらいます。

ステップ 5 対応する [NameID]フィールドを設定します。

パートナーの Web シングル サインオンの設定

手順

ステップ 1 [パートナーの Web SSO 設定（Partner Web SSO Configuration）]を選択します。

ステップ 2 SAML 設定をインポートしていない場合、[SAML メタデータをインポート（Import SAML Metadata）]を選択して [パートナーの Web シングル サインオン設定 - SAML メタデータ（Partner Web Single sign-on Configuration - SAML Metadata）] ダイアログボックスを開きます。
詳細については、次を参照してください。 フェデレーテッド Web SSO 設定, （71 ページ）

第 5 章

Cisco Unified Communications と Cisco WebEx の統合

概要

Cisco Unified Communications（UC）と Cisco WebEx（クリックツーコール）の統合を行うと、Cisco WebEx で使用可能な次のタイプの Cisco UC Integration ごとに新しいクラスタを作成して設定できます。

- Cisco WebEx クリックツーコール
- Cisco UC と Cisco WebEx の統合
- Cisco UC Manager Express と Cisco WebEx の統合

先に進む前に、以下のトピックを確認することを推奨します。

- Cisco Unified Communications Manager のクリックツーコール設定，（89 ページ）
- Unified Communications，（80 ページ）
- *Cisco Unified Communications Manager Express* のマニュアル（http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html [英語] で入手可能）。

一般的に、企業は複数の Cisco Unified Communications Manager（Unified Communications Manager）クラスタで構成されます。各クラスタは、Cisco WebEx クリックツーコール クラ

スタまたは Cisco UC と Cisco WebEx の統合クラスタになります。ユーザは、特定の事前定義されたグループ基準に基づいて Unified Communications Manager クラスタに割り当てられます。グループ基準の典型的な例では、ユーザは電話番号に基づいて CUCM クラスタに割り当てられます。

Cisco Unified Communications Integration（クリックツーコール）

Cisco Unified Communications Integration の設定は、バージョン 6.x 以前の Cisco WebEx アプリケーションを使用しているユーザにのみ機能します。Cisco Unified Communications Integration では、Cisco WebEx を使用して別のコンピュータや電話に発信することができます。特定のクリックツーコール クラスタの設定を指定したり、組織全体に指定されているデフォルトの設定を使用したりできます。詳細については、Cisco Unified Communications のクリックツーコール設定, （85 ページ）を参照してください。

Cisco UC Integration（Unified Communications Manager）Cisco WebEx

Cisco UC Integration for Cisco WebEx は Cisco WebEx に [電話（Phone）] タブを追加します。この新しいスペースによってユーザのコンピュータはフル機能の電話機に変わり、コールの発信、受信、管理を行うことができます。Cisco UC と Cisco WebEx の統合は、以下の広範な手順から構成されています。

- デバイス タイプを指定した Unified Communications Manager の設定、およびダイヤル ルールの設定。詳細については、*CUCI-Connect* 構成ガイド [英語] を参照してください（http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html [英語] で入手可能）。
- Cisco WebEx 管理ツールで Cisco UC と Cisco WebEx の統合の設定を指定します。詳細については、Cisco Unified Communications のクリックツーコール設定, （85 ページ）を参照してください。
- ビジュアル ボイスメールは、バージョン 7 以降の Cisco WebEx アプリケーションでのみ使用できます。ビジュアル ボイスメールは、音声ボイスメール サービスに代わるものです。詳細については、ビジュアル ボイスメールの設定, （83 ページ）を参照してください。

Cisco UC Call Manager Express（CME）と Cisco WebEx の統合

詳細については、*Cisco Unified Communications Manager Express* のマニュアルを参照してください（http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html [英語] で入手可能）。

Unified Communications

Cisco WebEx との統合には、次のコンポーネントに対する設定オプションの選択が含まれます。

- Cisco Unified Communications Integration（クリックツーコール）
- Cisco UC Integration for Cisco WebEx

- Cisco UC Manager Express Integration for Cisco WebEx

これらのコンポーネントは、Cisco WebEx 組織レベルで、または各コンポーネントのクラスタを作成することで、設定できます。

[Unified Communications]ウィンドウを開くには、[設定（Configuration）] > タブで [Unified Communications] を選択します。

次の 3 つのタブを使用できます。

- **[全般（General）] タブ**：Cisco WebEx のクリックツーコール設定、および Cisco WebEx セットアップ プログラム向けに Cisco UC Integration をダウンロードする URL を指定するために使用されます。詳細については、Cisco WebEx クリックツーコール, （81 ページ）を参照してください。

（注） Cisco WebEx 6.x にのみ適用されます。

- **[ボイスメール（Voicemail）] タブ**：ビジュアル ボイスメールの設定を指定するために使用されます。詳細については、ビジュアル ボイスメールの設定, （83 ページ）を参照してください。
- **[クラスタ（Clusters）] タブ**：Cisco Unified Communications クラスタを作成、変更、削除するために使用されます。

Cisco WebEx クリックツーコール

Cisco WebEx クリックツーコールの設定は、Cisco WebEx アプリケーションのバージョン 6.x を使用しているユーザに対してのみ機能します。構成時の設定は、いずれのクラスタにも属していない Cisco WebEx 組織内のユーザにのみ適用されます。Cisco Unified Communications クラスタの作成方法の詳細については、Unified Communications クラスタの作成, （84 ページ）を参照してください。

詳細については、次のマニュアルを参照してください。

-
- クリックツーコールのタスク フローの設定, （90 ページ）
- Cisco Unified Communications Manager, （89 ページ）
- Cisco Unified Communication Manager Integration と Cisco WebEx Messenger の設定, （86 ページ）
- *CUCI-Connect* 構成ガイド [英語]
（http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html で入手可能）。

Cisco WebEx クリックツーコールの設定

手順

ステップ 1 Cisco WebEx クリックツーコールを設定するには、[設定（Configuration）]タブを選択します。
[システム設定（System Settings）]ウィンドウが開きます。

ステップ 2 [IM]を選択します。
[一般 IM（General IM）]ウィンドウが開きます。

ステップ 3 [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 [Cisco WebEx クリックツーコールの設定（Cisco WebEx Click-to-Call Settings）]で以下を実行します。

- [Cisco WebEx クリックツーコールをデフォルトで有効にする（Enable Cisco WebEx Click-to-Call by default）]を選択して、組織のクリックツーコールの統合をデフォルトで有効にします。このオプションでは、個別のクリックツーコール クラスタを作成したかどうかを問わず、組織のクリックツーコール統合を有効にします。
- [Cisco Unified Communications Manager（CUCM）]ボックスに、Cisco WebEx 組織で設定された Cisco Unified Communications Manager サーバの IP アドレスまたはサーバ名を入力します。

  （注） [Cisco WebEx クリックツーコールをデフォルトで有効にする（Enable Cisco WebEx Click-to-Call by default）]を選択した場合を除き、Cisco Unified Communications Manager の設定を入力することはできません。

- Cisco WebEx 組織のユーザがクリックツーコール設定を手動で指定できるようにするには、[ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択します。このオプションを選択すると、組織管理者が入力したデフォルトのクリックツーコール設定がユーザが入力した設定で上書きされます。

ステップ 5 [Cisco UC Integration for Cisco WebEx の設定（Cisco UC Integration for Cisco WebEx Setting）]に、[Cisco UC Integration for Cisco WebEx セットアップ ダウンロード URL（Cisco UC Integration for Cisco WebEx Setup Download URL）]の URL を入力します。この URL から、Cisco WebEx 組織のユーザが、Cisco Unified Communications Integration（CUCI）機能を Cisco WebEx アプリケーションにインストールするセットアップ プログラムをダウンロードできます。

ステップ 6 [保存（Save）]を選択します。

表示によるボイスメール

ビジュアル ボイスメールは、バージョン 7 以降の Cisco WebEx アプリケーションでのみ使用できます。ビジュアル ボイスメール機能は、音声ボイスメール サービスの代替機能の 1 つです。ビ

ジュアル ボイスメールでは、電話機の画面を使用してボイス メッセージを操作できます。メッセージのリストを表示したり、リスト内のメッセージを再生したりできます。また、メッセージの作成、応答、転送、および削除を行うことができます。

（注） このサービスを使用するには、Cisco UC Integration for Cisco WebEx も設定する必要があります。

Cisco WebEx とビジュアル ボイスメールの統合を有効にすると、Cisco WebEx アプリケーションからビジュアル ボイスメールを直接表示できます。Cisco WebEx とビジュアル ボイスメールの統合を有効にする前に、次のドキュメントを読むことが推奨されます。

- ビジュアル ボイスメールのインストール計画 [英語]：
  http://www.cisco.com/en/US/docs/voice_ip_comm/cupa/visual_voicemail/7.0/english/install/guide/plan.pdf
- ビジュアル ボイスメールのインストールと構成ガイド [英語]：
  http://www.cisco.com/en/US/docs/voice_ip_comm/cupa/visual_voicemail/7.0/english/install/guide/Installation_and_Configuration_Guide_for_Visual_Voicemail_Release_70.pdf
- *CUCI* 接続構成ガイド [英語]：
  http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html

（注） 入力した設定はクラスタのデフォルトのビジュアル ボイスメールの設定であり、特定のサーバに対しては設定されません。また、各クラスタは個別に有効にする必要があります。詳細については、次を参照してください。 Unified Communications クラスタの作成, （84 ページ）

ビジュアル ボイスメールの設定

手順

ステップ 1 ビジュアル ボイスメールを設定するには、[設定（Configuration）] タブ > [Unified Communications] を選択します。
[Unified Communications]ウィンドウが開きます。

ステップ 2 [ボイスメール（Voicemail）]を選択して [CUCI 用のビジュアル ボイスメールのデフォルト設定（Default settings for Visual Voicemail for CUCI）] を選択します。
Unity Connection のお客様は、[ボイスメール サーバ（Voicemail Server）] フィールドまたは [メールストア サーバ（Mailstore Server）] フィールドに Unity Connection サーバの IP アドレスもしくは DNS 名を入力する必要があります。その他のすべての設定はデフォルトのままにしておくことを推奨します。

ステップ 3 ビジュアル ボイスメールを有効にするには、[ビジュアル ボイスメールの有効化（Enable Visual Voicemail）]を選択します。

ステップ 4 ビジュアル ボイスメールの設定を手動で入力する場合は、[ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択します。

ステップ 5 次の情報を入力します。

- [ボイスメールサーバ（Voicemail Server）]：Cisco WebEx アプリケーションがボイスメールを取得する際に通信する必要のあるビジュアル ボイスメール サーバ名。
- [ボイスメールプロトコル（Voicemail Protocol）]：ビジュアル ボイスメール サーバとの通信に使用するプロトコル。[HTTP] または [HTTPS] を選択できます。
- [ボイスメールポート（Voicemail Port）]：ビジュアル ボイスメール サーバに関連付けられたポート。
- [メールストアサーバ（Mailstore Server）]：メールストア サーバ名。
- [メールストアプロトコル（Mailstore Protocol）]：メールストア サーバが使用するプロトコル。[TLS] または [プレーン（Plain）] を選択できます。
- [メールストアポート（Mailstore Port）]：メールストア サーバに関連付けられたポート。
- [IMAPアイドル期限時間（IMAP IDLE Expire Time）]：サーバのボイスメールの確認が自動的に停止する期限までの時間（分単位）。
- [メールストアの受信トレイ フォルダ名（Mailstore Inbox Folder Name）]：メールストア サーバで設定されている受信トレイ フォルダの名前。
- [メールストアのごみ箱フォルダ名（MailstoreTrash Folder Name）]：メールストア サーバで設定されているごみ箱フォルダ（通常は削除済み項目フォルダ）の名前。

ステップ 6 [保存（Save）]を選択します。

Unified Communications クラスタの作成

Cisco Jabber を設定するには、次の Cisco Unified Communications コンポーネントの手順を実行します。

- クリックツーコール用の Cisco Unified Communications の設定
- Cisco Unified Communication Manager と Cisco Jabber の統合
- Cisco Unified Communication Manager Express と Cisco Jabber の統合
- Cisco TelePresence Video Communication Server

設定手順は UC コンポーネントによって異なるため、手順は複数のパートで説明されています。次の資料を参照してください。

- *CUCI-Connect* 構成ガイド [英語]
（http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html [英語] で入手可能）。
- *Cisco Unified Communications Manager Express* のマニュアル
（http://cisco.com/en/US/docs/voice_ip_comm/cucme_webex/configuration/guide/webexconnect_cme.html [英語] で入手可能）。

Cisco Unified Communications のクリックツーコール設定

組織管理者は、CUCI のプロビジョニングに関してカスタマー サポート担当者に連絡する必要があります。

手順

ステップ 1 [設定（Configuration）] タブ > [追加のサービス（Additional Services）] > [Unified Communications] を選択します。

ステップ 2 [クラスタ（Clusters）]を選択します。
以前に作成したクラスタが表示されます。

ステップ 3 [追加（Add）]を選択します。

ステップ 4 [クラスタ名（Cluster Name）]ボックスに新しいクラスタの名前を入力します。

ステップ 5 まだ選択していない場合は、[Cisco WebEx Connect クリックツーコールを有効にする（Enable Cisco WebEx Connect Click-to-Call）]を選択します。

ステップ 6 [ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択して、このクラスタに属するすべてのユーザが各自の Cisco Unified Communication Manager 設定を指定できるようにします。

（注） このオプションを有効にすると、ユーザが入力した設定で Cisco WebEx 組織に対して指定したデフォルトまたはグローバルのクリックツーコール設定が上書きされます。

ステップ 7 [Cisco Unified Communications Manager]ボックスに、Cisco WebEx 組織で設定された Unified Communication Manager の IP アドレスを入力します。Unified Communications Manager に Client ServicesFramework（CSF）と呼ばれるデバイス タイプが含まれることを確認します。

ステップ 8 [保存（Save）]を選択してクリックツーコール クラスタ設定を保存し、[Unified Communications] 画面に戻ります。
Unified Communications Manager を CSF と使用できるように設定する方法の詳細については、『*CUCI* 接続構成ガイド』[英語]
（http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.html）で「Cisco Unified Communications Manager の準備」というタイトルの付いたセクションを参照してください。

新しいクリックツーコール クラスタが [Cisco Unified Communications Clusters]の下に表示されるようになります。

Cisco Unified Communication Manager Integration と Cisco WebEx Messenger の設定

手順

ステップ 1 [設定（Configuration）] タブ > [追加のサービス（Additional Services）] > [Unified Communications] を選択します。

ステップ 2 [クラスタ（Clusters）]タブを選択し、[追加（Add）] を選択します。

ステップ 3 [Cisco WebEx Connect と Cisco UC Manager の統合の有効化（Enable Cisco UC Manager integration with Cisco WebEx Connect）]を選択します。

ステップ 4 [ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択し、ユーザが基本モードのプライマリ サーバの値か、または拡張モードの TFTP/CTI/CCMCIP サーバの値を変更できるようにします。

（注） このオプションを有効にすると、ユーザが入力した設定で Cisco WebEx 組織に対して指定したデフォルトまたはグローバルの Unified Communications Manager の設定が上書きされます。

ステップ 5 [Cisco Unified Communications Manager サーバの設定（Cisco Unified Communications Manager Server Settings）]で、次のように選択します。

- [基本的なサーバ設定（BasicServer Settings）]：Unified Communications Manager サーバの基本的な設定を入力します。
- [詳細なサーバ設定（AdvancedServer Settings）]：Unified Communications Manager サーバの詳細設定を入力します。

（注） サーバ設定のオプションは、基本か詳細かによって変わります。

ステップ 6 [基本的なサーバ設定（Basic Server Settings）]に次の値を入力します。

- [プライマリサーバ（Primary Server）]：プライマリの Unified Communications Manager サーバの IP アドレスを入力します。このサーバは、TFTP、CTI、CCMCIP で設定されます。
- [バックアップサーバ（Backup Server）]：バックアップの Unified Communications Manager サーバの IP アドレスを入力します。このサーバは、TFTP、CTI、CCMCIP で設定され、プライマリの Unified Communications Manager サーバに障害が発生した場合のフェールオーバーサポートを提供します。

ステップ 7 [詳細なサーバ設定（AdvancedServer Settings）] を選択した場合は、TFTP（Trivial File Transfer Protocol）サーバ、CTI（コンピュータ テレフォニー インテグレーション）サーバ、CCMCIP（Cisco Unified Communications Manager IP フォン）サーバの各設定を指定します。

ステップ 8 次のサーバのそれぞれに、IP アドレスを入力します。

（注） TFTP サーバには最大 2 つのバックアップ サーバを、CTI サーバと CCMCIP サーバにはそれぞれ 1 つのバックアップ サーバを指定できます。各バックアップ サーバに適切な IP アドレスを入力します。

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

ステップ 9 [ボイスメールのパイロット番号（Voicemail Pilot Number）]ボックスに、Unified Communications サーバのボイス メッセージ サービスの番号を入力します。
通常は、組織の管理者が Cisco WebEx の組織全体のデフォルトのボイス メッセージ番号を入力します。ただし、[ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]チェックボクスを選択すると、クラスタのユーザがこのデフォルトのボイス メッセージ番号を上書きできるようにすることができます。

ステップ 10 Cisco WebEx 組織にディレクトリ統合が設定されている場合、[LDAP サーバ設定（LDAP Server Settings）]情報を入力します。
LDAP サーバ設定を取得するには、お客様の企業または組織の IT 管理者にお問い合わせください。LDAP サーバ設定は、Cisco WebEx クライアント バージョン 6.x 以前を使用しているユーザのみが使用できます。

ステップ 11 [ボイスメール（Voicemail）]を選択します。

ステップ 12 [ビジュアル ボイスメールの有効化（Enable Visual Voicemail）]を選択します。
ここで入力したビジュアル ボイスメールの設定は、このクラスタに属しているユーザのみに適用されます。

ステップ 13 [クラスタ（Clusters）]タブで、[このクラスタに固有のボイスメール サーバ（Specific voicemail server for this cluster）] を選択してボイスメール サーバを指定します。このサーバは、組織全体に提供されるボイスメール サーバの設定とは異なります。

ステップ 14 [ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択して、ユーザがこのクラスタのビジュアル ボイスメール設定を手動で入力できるようにします。
特定のビジュアル ボイスメール設定の入力については、次を参照してください。 ビジュアル ボイスメールの設定, （83 ページ）

ステップ 15 Unified Communications の設定を保存するには、[保存（Save）]を選択します。
TFTP、CTI、および CCMCIP の各サーバの詳細については、http://www.cisco.com/en/US/products/ps10627/products_installation_and_configuration_guides_list.htm にある『CUCI 接続構成ガイド』を参照してください。

Cisco Unified Communication Manager Express Integration と Cisco WebEx Messenger の設定

手順

ステップ 1 [設定（Configuration）] タブ > [追加のサービス（Additional Services）] > [Unified Communications] を選択します。

ステップ 2 [クラスタ（Clusters）] タブ > [追加（Add）] を選択します。
[新規クラスタ（New Cluster）]ページが開きます。

ステップ 3 [Cisco UC Manager Express と Cisco WebEx Connect の統合の有効化（Enable Cisco UC Manager Express integration with Cisco WebEx Connect）]を選択します。

ステップ 4 [ダウンロード（Download）]リンクを選択して、最新のソフトウェア リリースを取得してダウンロードします。
Cisco Unified CME 統合ダウンロード サーバの設定は自動的には読み込まれません。ダウンロードは、Cisco WebEx Messenger のプラグインだと見なす必要があります。

ステップ 5 [ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択して、組織管理者がデフォルトの値を入力して、ユーザが自分のプライマリ サーバの値を変更できるようにします。

ステップ 6 [保存（Save）]を選択します。

Cisco TelePresence Video Communication Server の設定

手順

ステップ 1 [設定（Configuration）] タブ > [追加のサービス（Additional Services）] > [Unified Communications] を選択します。

ステップ 2 [クラスタ（Clusters）]タブを選択し、[追加（Add）] を選択します。

ステップ 3 [Cisco TelePresence Video Communication Server の有効化（Enable Cisco TelePresence Video Communication Server）]を選択します。

ステップ 4 [ユーザによる手動設定の入力を許可（Allow user to enter manual settings）]を選択すると、組織管理者はデフォルト値を指定できますが、ユーザが各自の内部/外部サーバおよび SIP ドメイン値を変更できるようになります。

第 6 章

Cisco Unified Communications Manager のクリックツーコール設定

概要

シスコの呼処理ソフトウェア、電話、エンドポイント デバイスを使用すると、企業または組織は、単一のコンバージドネットワークを介して、音声、データ、およびビデオコミュニケーションを効率的に行うことができます。

シスコはあらゆる規模と種類の組織向けの呼処理ソリューションを提供しています。これらの業界をリードするIP構内交換機（PBX）は、IPフォン、メディア処理デバイス、Voice over IP（VoIP）ゲートウェイ、モバイルデバイス、およびマルチメディアアプリケーション間の音声、ビデオ、モビリティ、およびテレプレゼンス サービスを管理するソリューションです。シスコの呼処理ソリューションには、Cisco Unified Communications Manager が含まれます。

Cisco Unified Communications Manager のクリックツーコール サービスはオプション機能であり、デフォルトでは Cisco WebEx では使用できません。クリックツーコールは無料のサービスとして提供されます。ただし、組織管理者が有効にする必要があります。詳細については、シスコのセールス担当者にお問い合わせください。

Cisco Unified Communications Manager

このエンタープライズ IP テレフォニー呼処理システムは、Cisco Unified Communications の中核です。Cisco Unified Communications Manager は、IP フォン、メディア処理デバイス、VoIP ゲートウェイ、モバイル デバイス、およびマルチメディア アプリケーションに音声、ビデオ、モビリ

ティ、およびプレゼンス サービスを提供します。この強力な呼処理ソリューションは次のような点で役立ちます。

- 生産性の強化：機能豊富なユニファイドコミュニケーションにより、ワーカーは他人に費やす時間を減らし、より生産的な作業に時間を費やすことができます。
- モビリティの有効化：組み込みのユニファイド モビリティ機能を備えたソフトウェアにより、モバイル ワーカーはどこにいても生産性を維持できます。

  Cisco Unified Communications Manager は、以下の点が優れたソリューションにより、幅広い通信機能とアプリケーションをサポートするユニファイド ワークスペースを作成します。
- 拡張性：各 Cisco Unified Communications Manager クラスタでは、最大 30,000 人のユーザをサポートでき、最大 1000 サイトで百万ユーザまでサポートするように拡張できます。
- 再頒布可能：拡張性、冗長性、ロード バランシングを確保。
- 使用可能性：複数レベルのサーバ冗長性および存続性の基盤を提供する、ビジネスの継続性のサポートおよび高可用性によるコラボレーションの向上。

クリックツーコールのタスク フローの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified IP Phone の設定, （91 ページ）	Cisco Unified Communications Manager に IP Phone を設定するために使用します。
ステップ 2	電話機に電話番号を追加する, （91 ページ）	IP Phone に電話番号を追加するために使用します。
ステップ 3	Cisco Unified Communications Manager での Cisco WebDialer のアクティブ化, （92 ページ）	Cisco Unified Communications Manager で Cisco WebDialer をアクティブ化するために使用します。
ステップ 4	Cisco Unified Communications Manager で CTI Manager が実行中であることの確認, （93 ページ）	Cisco Unified Communications Manager で CTI Manager が実行中であることを確認するために使用します。
ステップ 5	Cisco Unified Communications Manager で CCMCIP サービスが実行中であることの確認, （93 ページ）	Cisco Unified Communications Manager で CCMCIP サービスが実行中であることを確認するために使用します。
ステップ 6	正しい電話デバイスがユーザに関連付けられていることの確認, （94 ページ）	正しい電話デバイスがユーザに関連付けられていることを確認するために使用します。

Cisco Unified IP Phone の設定

Cisco Unified IP Phone を使用するには、次の手順を実行して Cisco Unified Communications Manager に電話機を追加する必要があります。また、SIP、H.323 クライアント、CTI ポート、Cisco ATA 186 Telephone Adaptor、または Cisco IP Communicator を実行しているサードパーティ製の電話機も設定できます。

手順

ステップ 1 [デバイス（Device）] > [電話機（Phone）] > [新規追加（Add New）] を選択します。

ステップ 2 [電話機のタイプ（Phone Type）]リストから、適切な電話機のタイプまたはデバイスを選択し、[次へ（Next）] を選択します。
電話機のタイプを選択した後は変更できません。

ステップ 3 [デバイス プロトコルの選択（Select the Device Protocol）] リストが表示された場合、適切なデバイス プロトコルを選択し、[次へ（Next）] を選択します。
[電話の検索/一覧表示（Find and List Phones）]ウィンドウが表示されます。

ステップ 4 適切な設定値を入力します。詳細については、『*Cisco Unified Communications 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。

次の作業

電話機に電話番号を追加する, （91 ページ）

電話機に電話番号を追加する

パターンを電話番号として使用する場合は、電話機の表示およびダイヤル先の電話機に表示される発信者 ID にはどちらも数字以外の文字が含まれます。これを避けるには、[表示（内部発信者 ID）（Display（Internal Caller ID））]、[回線のテキスト ラベル（Line Text Label）] および [外線電話番号マスク（External Phone Number Mask）] の値を指定することが推奨されます。

はじめる前に

Cisco Unified IP Phone の設定, （91 ページ）

手順

ステップ 1 電話機に電話番号を追加するには、ウィンドウの左側に表示される [関連付け情報（Association Information）]セクションで [回線 [1] - 新規 DN の追加（Line [1] - Add a new DN）] などの回線リンクを 1 つ選択します。

ステップ 2 有効な電話番号を入力します。入力した電話番号は、複数のパーティションで表示される可能性があります。

ステップ 3 [保存（Save）]を選択します。

ステップ 4 [電話機のリセット（Reset Phone）]を選択します。

（注） デバイスをできるだけ早く再起動します。このプロセスの間、システムがゲートウェイのコールをドロップする可能性があります。

詳細については、『*Cisco Unified Communications Administration Guide*』を参照してください。

次の作業

Cisco Unified Communications Manager での Cisco WebDialer のアクティブ化, （92 ページ）

Cisco Unified Communications Manager での Cisco WebDialer のアクティブ化

Cisco Unified Communications Integration（クリックツーコール）では、SOAP インターフェイスを使用して、Cisco Unified Communications Manager で WebDialer サーブレットと対話します。クリックツーコールでは HTTP インターフェイスは使用されないため、アプリケーションは Redirector サーブレットとは対話しません。

はじめる前に

電話機に電話番号を追加する, （91 ページ）

手順

ステップ 1 [Cisco Unified Communications Manager 可用性（Cisco Unified Communications Manager Serviceability）] > [ツール（Tools）] > [サービス アクティブ化（Service Activation）] を選択します。

ステップ 2 [サーバ（server）] ドロップダウン リストから Cisco Unified Communications Managerサーバを選択します。

ステップ 3 [CTI Services] で、[Cisco WebDialer Web Service]にチェックマークを付けます。

ステップ 4 [保存（Save）]を選択します。

次の作業

Cisco Unified Communications Manager で CTI Manager が実行中であることの確認, （93 ページ）

Cisco Unified Communications Manager で CTI Manager が実行中であることの確認

Cisco Unified Communications Integration（クリックツーコール）が適切に機能するには、CTI Manager が Cisco Unified Communications Manager で実行されている必要があります。

はじめる前に

Cisco Unified Communications Manager での Cisco WebDialer のアクティブ化, （92 ページ）

手順

ステップ 1 [Cisco Unified Communications Manager 有用性（Cisco Unified Communications Manager Serviceability）]>[ツール（Tools）]>[コントロールセンター（Control Center）]>[機能サービス（Feature Services）]を選択します。

ステップ 2 [server] ドロップダウン リストから Cisco Unified Communications Manager サーバを選択します。

ステップ 3 [Call Manager サービス（Call Manager Services）] で、[Cisco CTIManager]が実行中であることを確認します。

次の作業

Cisco Unified Communications Manager で CCMCIP サービスが実行中であることの確認, （93 ページ）

Cisco Unified Communications Manager で CCMCIP サービスが実行中であることの確認

Cisco Unified Communications Integration（クリックツーコール）では、CCMCIP（Cisco CallManager Cisco IP Phone Services）サービスからユーザの電話機タイプが取得され、クリックツーコール アプリケーションの[電話機設定（Phone Preferences）]画面に電話機タイプが表示されます。CCMCIP サービスは Cisco Unified Communications Manager リリース 6.x 以降でのみ稼働するため、この手順は、Cisco Unified Communications Manager の本リリースを実行している場合に適用されます。

はじめる前に

Cisco Unified Communications Manager で CTI Manager が実行中であることの確認, （93 ページ）

手順

ステップ 1 [Cisco Unified Communications Manager 有用性（Cisco Unified Communications Manager Serviceability）] > [ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）] を選択します。

ステップ 2 [server] ドロップダウン リストから Cisco Unified Communications Manager サーバを選択します。

ステップ 3 [CM サービス（CM Services）] で、[Cisco CallManager Cisco IP Phone]サービス が実行中であることを確認します。

次の作業

正しい電話デバイスがユーザに関連付けられていることの確認, （94 ページ）

正しい電話デバイスがユーザに関連付けられていることの確認

Cisco Unified Communications Manager で正しい電話デバイスがユーザに関連付けられていることを確認する必要があります。正しく関連付けられていないと、その電話機は、クリックツーコールの [電話機設定（Phone Preferences）]画面に表示されません。

はじめる前に

Cisco Unified Communications Manager で CCMCIP サービスが実行中であることの確認, （93 ページ）

手順

ステップ 1 [Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）] > [ユーザ管理（User Management）] > [エンド ユーザ（End User）] を選択します。

ステップ 2 [検索（Find）]を選択します。

ステップ 3 適切なユーザ ID を選択します。

ステップ 4 [デバイスの割り当て（Device Association）]セクションで、[制御するデバイス（Controlled Devices）] ウィンドウに正しいデバイスが表示されていることを確認します。

（注） 電話デバイスにユーザを関連付ける必要がある場合は、[デバイスの割り当て（Device Association）] を選択します。詳細については、Cisco Unified Communications Manager のオンライン ヘルプを参照してください。

アプリケーション ダイヤル ルールの設定

ユーザがダイヤルする電話番号から自動的に数字を削除したり、電話番号に数字を追加したりするアプリケーションのダイヤルルールを設定できます。たとえば、ダイヤルルールを使用して、電話番号の先頭に数字を自動的に追加して、外線に接続することができます。

Cisco Unified Communications Manager のアプリケーション ダイヤル ルールは、[Cisco Unified Communications Manager Administration（Cisco Unified Communications Manager の管理）] > [コール ルーティング（Call Routing）] > [ダイヤル ルール（Dial Rules）] > [アプリケーション ダイヤル ルール（Application Dial Rules）]から設定します。

ここでは、アプリケーション ダイヤル ルールについて簡単に説明します。Cisco Unified Communications Manager でのアプリケーション ダイヤル ルールの設定方法の詳細については、次の資料を参照してください。

- 『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「Application Dial Rules Configuration」の項
- 『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「Dial Plans」の項
- サンプルのアプリケーション ダイヤル プラン, （95 ページ）
- Cisco WebDialer が Cisco Unified Communications Manager のアプリケーション ダイヤル ルールを自動的に使用するための設定, （97 ページ）

サンプルのアプリケーション ダイヤル プラン

名前/説明	番号（先頭の番号）	桁数	削除する総桁数	プレフィックスおよびパターン
国際 12 桁	+	12	1	9011
国際 13 桁	+	13	1	9011
国際 14 桁	+	18	1	9011
国際 15 桁	+	15	1	9011
市内 7 桁 XXX-XXXX		7		9

名前/説明	番号（先頭の番号）	桁数	削除する総桁数	プレフィックスおよびパターン
市内 10 桁 (510) XXX-XXXX	510	10	3	9
国内 10 桁 (XXX) XXX-XXXX		10		91
国内 11 桁 1(XXX) XXX-XXXX		11		9

上記のサンプルのアプリケーション ダイヤル プランでは、9 は外部ダイヤル用のオフネット アクセス コードを表します。国内通話では、市内番号または国内（長距離）番号のいずれかに発信するために、オフネットアクセスコードに適切な桁数を追加します。それぞれの国際ダイヤルルールでは、「+」を、オフネット アクセス コードと適切な国際ダイヤル アクセス コードで置き換えます。

これらのアプリケーション ダイヤルルールは、上記のサンプルのダイヤル プランで設定されます。

- 任意の国際番号。アプリケーション ダイヤルルールでは、番号から「+」が削除され、オフネット アクセス コード 9 と国際ダイヤル アクセス コード 011 が残りの数字の先頭に追加されます。
- 任意の 7 桁の市内番号。アプリケーション ダイヤルルールでは、オフネット アクセス コード 9 が先頭に追加されます。
- 510 で始まる任意の 10 桁の市内番号。アプリケーション ダイヤルルールでは、番号から 510 が削除され、オフネット アクセス コード 9 が残りの数字の先頭に追加されます。
- 任意の 10 桁の国内番号。アプリケーション ダイヤルルールでは、数字 91 が先頭に追加されます。
- 1 で始まる任意の 11 桁の国内番号。アプリケーション ダイヤルルールでは、オフネット アクセス コード 9 が先頭に追加されます。

  [開始番号（Number Begins With）]フィールドが空白の場合は、ダイヤルルールに開始番号の数字を任意に適用できます。たとえば、最初の数字が 1、1408、または 1408526 で始まる場合は、それぞれ着信番号 14085264000 と一致します。

  アプリケーション ダイヤルルール リストは、優先順位の順に設定する必要があります。Cisco Unified Communications Manager では、ダイヤルルール リストで着信番号を検索する最初のダイヤルルールの一致が適用され、リスト中の最適な一致の検索は試行されません。たとえば、次に示すダイヤルルール条件を設定した場合、着信番号 14085264000 の受信時に、Cisco Unified Communications Manager では、ダイヤルルール 1 は無視され、ダイヤルルール 2 が最初の一致であるため、適用されます。ダイヤルルール 3 が最適な一致ですが、最初の一致の

検索後、Cisco Unified Communications Manager ではリスト内の後続のルールはすべて無視されます。

1. 先頭が 9 で、長さが 8 桁の場合は、X を行います。
2. 先頭が 1 で、長さが 11 桁の場合は、Y を行います。
3. 先頭が 1408 で、長さが 11 桁の場合は、Z を行います。

（注） また、Cisco Unified Communications Manager の電話帳の検索ルールも設定できます。電話帳の検索ルールによって、ユーザがダイヤルする番号が電話番号に変換されます。詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「Directory Lookup dial Rules Configuration（電話帳の検索ダイヤルルール）」を参照してください。

Cisco WebDialer が Cisco Unified Communications Manager のアプリケーション ダイヤル ルールを自動的に使用するための設定

手順

ステップ 1 [Cisco Unified Communications Manager Administration（Cisco Unified Communications Manager の管理）] > [System（システム）] > [Service Parameters（サービス パラメータ）] を選択します。

ステップ 2 [サーバ（Server）]メニューから Cisco Unified Communications Manager サーバを選択します。

ステップ 3 [サービス（Service）]メニューから [Cisco WebDialer Web Service（Cisco WebDialer Web サービス）] を選択します。

ステップ 4 [ダイヤル時にアプリケーション ダイヤル ルールを適用（Apply Application Dial Rules on Dial）] パラメータの [True] を選択します。

ステップ 5 Cisco Unified Communications Manager のリリース 6.x または 7.x を実行している場合は、[SOAP ダイヤル時にアプリケーション ダイヤル ルールを適用（Apply Application Dial Rules on SOAP Dial）] パラメータの [True] を選択します。

ステップ 6 Cisco WebDialer サービスを再起動します。

トラブルシューティング（Troubleshooting）

次に、Cisco Unified Communications Manager の使用時に問題が発生した場合のトラブルシューティング情報を示します。

- クリックツーコールのログ ファイルおよびコンフィギュレーション ファイル
- クリックツーコールのログ ファイル

• エラー メッセージ, （98 ページ）

エラー メッセージ

次の表は、Cisco Unified Communications Integration（クリックツーコール）アプリケーションに表示されるエラーメッセージのリスト、およびエラーメッセージごとの推奨処置についての説明です。

エラー メッセージ	問題と推奨処置
接続エラーが発生しました。クリックツーコールが実行中であることを確認してください（A connection error occurred. Verify Click-to-Call is running）	• クリックツーコール アプリケーションが実行中でないときに、クリックツーコール機能を使用して通話が試行されました。 • クリックツーコール アプリケーションを再起動するようエンド ユーザに依頼してください。
ディレクトリ エラーが発生しました。電話管理者に問い合わせてください（A directory error occurred. Contact your phone administrator）	• Cisco Unified Communications Manager のディレクトリ サービスがダウンしている可能性があります。 • 少し待って、接続を再試行してください。再びエラーが発生する場合は、Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
サービス エラーが発生しました。もう一度通話してみてください。（A service error occurred. Retry the call.）問題が解決しない場合は、電話管理者に問い合わせてください（If the problem persists, contact your phone administrator）	• WebDialer アプリケーションで内部エラーが発生しました。 • Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
発信できません。クリックツーコールが実行中であることを確認してください（Cannot make call. Verify Click-to-Call is running）	• クリックツーコール アプリケーションを再起動するようエンド ユーザに依頼してください。

エラー メッセージ	問題と推奨処置
クリックツーコールで Cisco IP Communicator を検出できません。Cisco IP Communicator が実行中であるか確認するか、または別の電話機を選択してください（Click-to-Call cannot find Cisco IP Communicator. Verify it is running or select another phone）	• Cisco IP Communicator ソフト フォンが正常に実行中であるか確認するか、クリックツーコールアプリケーションで使用する電話機を選択するようエンド ユーザに依頼してください。
クリックツーコールの設定が不完全です（Click-to-Call is not fully configured）	• サインイン画面の 1 つ以上の必須フィールドが空白のままになっています。 • サインイン画面で不足している情報を入力し、再試行するようエンド ユーザに依頼してください。
着信先に到達できません（Destination cannot be reached）	• エンド ユーザが間違った番号にダイヤルしたか、正しいダイヤル ルールが適用されていません。 • Cisco Unified Communications Manager のアプリケーション ダイヤル ルールを使用するように Cisco WebDialer サービスが設定されていることを確認してください。
ログインに失敗しました。ユーザ名とパスワードが正しいことを確認してください（Login failed. Verify your user name and password are correct）	• Cisco Unified Communications Manager サーバの正しいユーザ名とパスワードをエンドユーザに提供します。 • サインイン画面でユーザ名とパスワードを入力し、再試行するようエンド ユーザに依頼してください。
使用可能な電話機がありません。電話管理者に問い合わせて確認してください（No phone is available. Verify contact your phone administrator）	• [クリックツーコールの設定（Click-to-Call Preferences）] の [電話（Phones）] 画面で電話機の設定を確認して更新するようユーザに依頼してください。
クリックツーコールで使用する電話機が選択されていません。電話機を選択してください（No phone has been selected for use with Click-to-Call. Select a phone）	• クリックツーコール アプリケーションで使用する電話機をエンド ユーザが選択していません。 • アプリケーションで使用する電話機をクリックツーコール アプリケーションから選択するようエンド ユーザに依頼してください。

エラー メッセージ	問題と推奨処置
プロキシ認証権限が見つかりませんでした。電話管理者に問い合わせてください（Proxy authentication rights could not be found. Contact your phone administrator）	• このエラーは Cisco WebDialer サービスから送信されています。Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
サービスが一時的に使用できません。もう一度通話してみてください。問題が解決しない場合は、電話管理者に問い合わせてください（Service is temporarily unavailable. Retry the call. If the problem persists, contact your phone administrator）	• Cisco Unified Communications Manager サービスがオーバーロードしています。同時セッション数の制限（2つ）に達しました。 • 少し待って、接続を再試行してください。再びエラーが発生する場合は、Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
サービスがオーバーロードしています。もう一度通話してみてください。問題が解決しない場合は、電話管理者に問い合わせてください（The service is overloaded. Retry the call. If the problem persists, contact your phone administrator）	• Cisco Unified Communications Manager サービスがオーバーロードしています。同時セッション数の制限（2つ）に達しました。 • 少し待って、接続を再試行してください。再びエラーが発生する場合は、Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
要求した URL が使用できません。電話管理者に問い合わせてください（The URL you requested is not available. Contact your phone administrator）	• 正しい Cisco Web Dialer またはデバイス クエリー サービスの IP アドレスをエンドユーザに提供してください。 • サインイン画面でこの情報を入力し、再試行するようエンド ユーザに依頼してください。
XML コマンドは要求では使用できません。電話管理者に問い合わせてください（The URL you requested is not available. Contact your phone administrator）	• このエラーは Cisco WebDialer サービスから送信されています。Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
<Number> は有効な電話番号に変換できません（<Number> cannot be converted to a valid phone number）	• エンド ユーザが入力した電話番号が無効です。 • 電話番号を編集し、電話をかけ直すようエンド ユーザに依頼してください。

エラー メッセージ	問題と推奨処置
電話番号の長さは最大で32桁までです（The maximum phone number length is 32 digits）	• エンド ユーザが入力した電話番号が長すぎます。 • 電話番号を編集し、電話をかけ直すようエンド ユーザに依頼してください。
無効な XML コマンドです。電話管理者に問い合わせてください（Invalid XML command. Contact your phone administrator）	• このエラーは Cisco WebDialer サービスから送信されています。Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
Cisco WebDialer サービスが見つかりません。アドレスを確認してください（Cisco WebDialer service cannot be found. Verify the address）	• 正しい WebDialer サーバ アドレスをエンド ユーザに提供してください。 • サインイン画面でこのサーバ アドレスを入力し、再試行するようエンド ユーザに依頼してください。
コールが失敗しました。エクステンション モビリティ デバイスにログインしていることを確認してください。問題が解決しない場合は、電話管理者に問い合わせてください（The call failed. Verify you are logged into your Extension Mobility device. If the problem persists contact your phone administrator）	• すでに進行中のコール要求があるか、Cisco WebDialer サービスが CTI から電話デバイスの回線を取得できませんでした。 • 少し待って、接続を再試行してください。再びエラーが発生する場合は、Cisco Unified Communications Manager のシステム管理者に問い合わせてください。

次の表は、Cisco Jabber アプリケーションの [電話（Phone）] タブ（Cisco Unified Communications Manager Integration）に表示されるエラー メッセージのリスト、およびエラー メッセージごとの推奨処置についての説明です。

エラー メッセージ	問題と推奨処置
問題が解決しない場合は、システム管理者に問い合わせてください。（If you still have problems, contact your system administrator.）	• アカウントまたはデバイス情報を取得する際にエラーが発生しました。 • エンド ユーザがアカウントを持っている場合、[再試行（Retry）] ボタンが表示されます。

エラー メッセージ	問題と推奨処置
クライアントが無効な資格情報を使用して登録を試みました。（Client tried to register with invalid credentials.）	• エンド ユーザが無効なユーザ名またはパスワードを入力しました。 • 有効なユーザ名とパスワードを使用して、再度登録するようエンド ユーザに依頼してください。
バックエンドサーバに接続できません。コールを完了できません。（Unable to connect to backend server; your call cannot be completed.）再度実行してください。（Please try again.）	• バックエンドの Cisco Unified Communications Manager サーバに接続できませんでした。 • Cisco Unified Communications Manager のアドレスが無効である可能性があります。アドレスを確認し、接続を再試行してください。
要求されたな機能は現在利用できません。（The requested feature/capability is not currently available.）	• デスクフォン サービスがサーバによってシャットダウンされています。 • Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
CCMCIP に接続できません。（Could not connect to CCMCIP.）	• ソフトフォン サービスがサーバによってシャットダウンされています。 • Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
このデバイスは選択できません。（Unable to select this device.）別のデバイスを選択して、もう一度試してください。（Please choose a different device and try again.）	• 選択したデバイスは不明か、または取り外されています。 • 別のデバイスを選択して、もう一度接続してみてください。
通話を保留にできませんでした。（Failed to hold a call.）	• 通話の保留が要求されたときにエラーが発生しました。 • [保留（Hold）]ボタンを押し、通話を再度保留にしてみてください。問題が解消されない場合は、クライアント アプリケーションを再起動してください。

エラー メッセージ	問題と推奨処置
コールをマージできませんでした。（Failed to merge calls.）	• コールのマージが要求されたときにエラーが発生しました。 • コールを再度マージしてみてください。問題が解消されない場合は、クライアント アプリケーションを再起動してください。
コールの最大制限値を超えました。（Max Call Limit exceeded.）	• 許可された回線の最大数に達しました。これ以上コールを発信できません。
デバイスが選択されていません。（No device selected.）使用するデバイスを選択し、再度試してください。（Please select the device you want to use and try again.）	• デバイスの選択時にタイムアウトに達しました。 • デバイスを選択して、もう一度接続してみてください。
デフォルトの回線にアクセスできません。（Unable to access the default line.）管理者に連絡してください。（Please contact your administrator.）	• デフォルト回線の選択時にタイムアウトに達しました。 • Cisco Unified Communications Manager のシステム管理者に問い合わせてください。
一時的な制限により、コールを発信できません。（Due to temporary restrictions, you cannot make calls now.）しばらくしてからもう一度試してください。（Please wait a few moments and try again.）	• コールを発信できません。サービスのフェールオーバーまたはフォールバックが原因である可能性があります。 • しばらく待機してから、再度コールを発信してみてください。

第 7 章

ポリシー エディタ（Policy Editor）

概要

Cisco WebEx には、グループのポリシーを定義して適用できるポリシー エディタがあります。ポリシーは、ファイル転送、デスクトップ共有、IM セッションのアーカイブ、Cisco WebEx の自動アップグレードなどの機能を有効化または無効化するために使用できます。ポリシーは、Cisco WebEx 組織内の全ユーザまたは特定のユーザ グループに適用できます。

個人にポリシーを適用することはできません。

ポリシーおよびポリシー アクション

ポリシーは、ユーザのグループまたは Cisco WebEx 組織全体が使用可能な Cisco WebEx 機能を決定するアクションを含む一連のルールです。そのため、ポリシーには、有効、無効、または詳細設定で使用可能な複数のアクションを含めることができます。たとえば、新規従業員に対して Cisco WebEx の特定の機能を制限したいお客様は、新規従業員ポリシーという名前のポリシーを作成して、さまざまなアクションを関連付けることができます。

アクションは、ポリシーによって制限可能な Cisco WebEx の機能です。たとえば、外部ファイル転送アクションは、Cisco WebEx 組織の外部のユーザとのファイル交換機能に対応しています。

ポリシーの定義と適用

組織レベルのポリシーとグループレベルのポリシーの違いを理解することが重要です。

Cisco WebEx 組織に新規ユーザを作成した場合、そのユーザはデフォルトではいずれのグループにも属していません。そのため、すべてのデフォルトのポリシー アクションが Cisco WebEx 組織

ポリシー エディタ（Policy Editor）

全体に適用されます。これは、通常プロビジョニング時に作成される最上位グループには、Cisco WebEx 組織のすべてのユーザが含まれるためです。

組織管理者がグループを作成し、それらのグループに特定のポリシーを適用する場合、グループレベルのポリシーによって組織レベルのポリシーがオーバーライドされます。それらのグループに属しているユーザは、組織レベルのポリシーではなくグループレベルのポリシーによって支配されます。たとえば、組織管理者が特定のグループに対して外部VoIP通信を禁止するポリシーを適用すると、そのグループのユーザはVoIPを使用して通信できなくなります。ただし、組織内の他のすべてのユーザに対しては、外部 VoIP 通信が引き続き有効な場合があります。

ポリシーは、組織レベルで、または特定のグループに対して適用できます。ただし、組織レベルとグループレベル（または親グループとそのサブグループ）の間でポリシーの設定に競合がある場合、最も限定的なアクションが有効になります。たとえば、組織レベルでVoIP機能がオン（[有効（Enabled）]）になっていて、グループレベルでオフ（[無効（Disabled）]）になっている場合、そのグループ内のすべてのユーザの VoIP 機能が無効になります。ただし、組織レベルで VoIP 機能がオフになっている場合、グループレベルで有効にしても、そのグループのユーザのVoIP機能は無効なままです。

ポリシー エディタ（Policy Editor）

ポリシーを設定するには、Cisco WebEx管理ツールを使用します。グループごとに異なるポリシーを設定でき、ポリシーはいつでも変更できます。Cisco WebEx 組織が新しくプロビジョニングされると、デフォルトですべてのユーザに対してすべての機能が有効になります。ただし、ユーザが AES 暗号化を使用しなければならない機能は除きます。

（注） ポリシーを変更または更新した場合、更新されたポリシーを適用するには、Cisco WebEx からログアウトしてから再度ログインする必要があります。

グループにポリシーを適用する方法については、グループへのポリシーの割り当て，（121 ページ）を参照してください。

ポリシーの追加

手順

ステップ 1 [ポリシー エディタ（Policy Editor）]タブを選択します。
[ポリシー（Policy）]画面の左側に [ポリシー リスト（Policy List）]、右側に [アクション リスト（Action List）] が表示されます。

ステップ 2 [ポリシー リスト（Policy List）]で [追加（Add）] を選択します。
既存のポリシーのリストの最上部に新しいポリシーが表示されます。

ステップ 3 ポリシーの一意の名前を入力します。

次の作業

このポリシーにアクションを追加するには、次を参照してください。 ポリシーへのアクションの追加, （107 ページ）

ポリシーへのアクションの追加

手順

ステップ 1 [ポリシー エディタ（Policy Editor）]タブを選択します。
[ポリシー エディタ（Policy Editor）]画面の左側に [ポリシー リスト（Policy List）]、右側に [アクション リスト（Action List）] が表示されます。

ステップ 2 [ポリシー名（Policy Name）]で、アクションを追加するポリシーを選択します。

ステップ 3 アクションを追加するには、画面の右側の [アクション リスト（Action List）]の下にある [追加（Add）] を選択します。
[アクション エディタ（Action Editor）]画面が表示されます。

ステップ 4 [アクション タグ名（Action Tag Name）]リストからポリシー アクションを選択します。
これらのアクションの詳細については、次を参照してください。 ポリシーおよびポリシー アクション, （105 ページ）

ステップ 5 [保存（Save）]を選択します。

ステップ 6 すべてのポリシーにアクションが割り当てられるまで、ステップ 3 ～ 5 を繰り返します。

Cisco WebEx で使用可能なポリシー アクション

ここでは、Cisco WebEx で使用可能なポリシー アクションについて説明します。説明には、ポリシー アクションを制御する機能への影響に関する情報も含まれています。このため、管理するグループに対して最適なポリシーを設定することができます。ポリシー アクションの確認および設定方法の詳細については、ポリシーへのアクションの追加, （107 ページ）を参照してください。

デフォルトでは、新規にプロビジョニングされた Cisco WebEx の組織に対し、ユーザに付与されたすべての機能が備えられています。これは、デフォルトのポリシー アクションでは、すべてのユーザが Cisco WebEx の全機能を使用できることを意味します。

（注） デフォルトでは、エンドツーエンドの暗号化ポリシーのみ有効になっていません。組織管理者はこのポリシーを明示的に有効にする必要があります。その後、管理者は、すべてのユーザまたは特定のユーザ グループに対して特定の機能を無効にする場合のみ、ポリシーを作成する必要があります。

ポリシー アクションは、サードパーティ製の XMPP IM アプリケーションを使用しているユーザには適用できません。

VoIP 会議の参加者が 10 人未満の場合、同じ VoIP 会議に同時に接続できます。

外部ユーザとは、Cisco WebEx 組織に属していないユーザですが、外部ユーザも Cisco WebEx を使用して、Cisco WebEx 組織に属しているユーザと通信することができます。

ポリシー アクション	説明	影響	デフォルト値
外部ファイル転送（External File Transfer）	組織のユーザと組織外のユーザ間の IM セッションでのファイル転送を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、少なくとも 1 人の外部ユーザがいるマルチパーティ IM セッションを含む、組織内ユーザと外部ユーザ間のすべてのファイル転送が停止します。	[有効（Enabled）]
内部ファイル転送（Internal File Transfer）	組織内のユーザ間の IM セッションでのファイル転送を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、すべての内部ファイル転送が停止します。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、組織内のすべてのユーザが内部ユーザとファイル交換することができます。	[有効（Enabled）]
外部 IM（External IM）	組織内のユーザと組織外のユーザ間の IM セッションを制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザと組織外のユーザ間のすべての IM セッションが停止します。この場合、音声、ビデオ、VoIP などの依存関係にあるサービスもすべて停止します。	[有効（Enabled）]
外部 VoIP（External VOIP）	組織内のユーザと組織外のユーザ間の IM セッションでの VoIP 通信を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザと組織外のユーザ間の IM セッションでのすべての VoIP 通信が停止します。ただし、テキストベースの IM セッションやファイル転送などの他のサービスは使用できます。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
内部 VoIP（Internal VOIP）	組織内のユーザ間の IM セッションでの VoIP 通信を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザ間の IM セッションでのすべての VoIP 通信が停止します。ただし、テキストベースの IM セッションやファイル転送などの他のサービスは使用できます。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、組織内のすべてのユーザが IM セッションで VoIP 通信を行うことができます。	[有効（Enabled）]
外部ビデオ（External Video）	組織内のユーザと組織外のユーザ間の IM セッションでのビデオサービスを制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザと組織外のユーザ間のIMセッションでのすべてのビデオサービスが停止します。ただし、テキストベースのIMセッションやファイル転送などの他のサービスは使用できます。	[有効（Enabled）]
内部ビデオ（Internal Video）	組織内のユーザ間の IM セッションでのビデオサービスを制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザ間の IM セッションでのすべてのビデオサービスが停止します。ただし、テキストベースの IM セッションやファイル転送などの他のサービスは使用できます。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、組織内のすべてのユーザが IM セッションでビデオ コミュニケーションを行うことができます。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
ローカル アーカイブ（Local Archive）	ユーザがローカルで IM テキストメッセージをアーカイブする機能を制御します。	バージョン7.1のアプリケーション以降、このポリシーを [無効（Disabled）]に設定すると、保存されていたローカル履歴は削除されます。 Cisco WebEx アプリケーションでは、次のオプションは無効になっています。[編集（Edit）] > [設定（Settings）] > [一般 GM（General IM）] > [メッセージ アーカイブ（Message Archive）]。 Cisco WebEx バージョン 5.x から 6.x にアップグレードすると、ユーザのローカル コンピュータに保存されていたチャット履歴のアーカイブは削除され、回復することはできません。組織管理者はCisco WebEx組織のすべてのユーザにこの点を連絡することを推奨します。さらに、ユーザは、Cisco WebExが新しいバージョンにアップグレードされる前に、個人のチャット アーカイブをバックアップする必要があります。 7.1 以降、このポリシーが [無効（Disabled）]に設定されている場合、ローカル履歴は削除されます。	[有効（Enabled）]
ワークスペースへの参加（Join Workspace）			[有効（Enabled）]
外部ワークスペースへの参加（Join External Workspace）			[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
外部デスクトップ共有（External Desktop Share）	組織内のユーザが自身のデスクトップを組織外のユーザと共有する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザは自身の（ローカル）デスクトップを組織外のユーザと共有できなくなります。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、ユーザは自身の（ローカル）デスクトップを組織外のユーザと共有できます。	[有効（Enabled）]
内部デスクトップ共有（Internal Desktop share）	組織内のユーザが自身のデスクトップを組織内の他のユーザと共有する機能を制御します。	このポリシー アクションをオフにすると、組織内のユーザは自身のデスクトップを組織内の他のユーザと共有できなくなります。 このポリシー アクションが明示的に [無効（Disabled）]に設定されていない場合、ユーザは自身のデスクトップを組織内の他のユーザと共有できます。	[有効（Enabled）]
ワークスペース機能（Workspace Feature）			[有効（Enabled）]
ユーザをワークスペースに招待する（Invite Users to Workspace）			[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
ユーザを外部ワークスペースに招待する（Invite Users External Workspace）			[有効（Enabled）]
IM のエンドツーエンドの暗号化のサポート（Support End-to-End Encryption For IM）	ユーザが IM セッションのエンドツーエンドの暗号化のサポートを指定できます。	このアクション ポリシーを [有効（Enabled）]に設定すると、IM セッションのエンドツーエンドの暗号化をサポートできます。 ユーザがログに記録されるように指定されている場合、エンドツーエンドの暗号化ポリシーの設定はオーバーライドされて False になります。エンドツーエンドの暗号化は、ログに記録されたユーザに対してはサポートされません。詳細については、IM ログ記録とアーカイブの概要, （59 ページ）を参照してください。	無効
符号化されていない IM のサポート（Support NO Encoding For IM）	エンドツーエンドの暗号化に対応しているアプリケーションが、エンドツーエンドの暗号化に対応していないアプリケーションやエンドツーエンドの暗号化をサポートしていないサードパーティ製アプリケーションとの IM セッションを開始できるかどうかを制御します。	このポリシーを [無効（Disabled）]に設定すると、エンドツーエンドの暗号化に対応しているアプリケーションが、エンドツーエンドの暗号化に対応していないアプリケーションやエンドツーエンドの暗号化をサポートしていないサードパーティ製アプリケーションとの IM セッションを開始できなくなります。 （注） [IM のエンドツーエンドの暗号化のサポート（Support End-to-End Encryption For IM）]を [有効（Enabled）]に設定すると、ネゴシエートされる暗号化レベルは、相手側がサポートする最高のレベルになります。暗号化レベルの詳細については、暗号化レベル, （116 ページ）を参照してください。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
内部 IM（ホワイトリストに記載されたドメインを含む）（Internal IM（including White Listed domains））	組織内のユーザとホワイトリスト上の特定ドメイン間の IM 通信を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザはホワイトリストに指定されたドメイン内の IM ユーザになれなくなります。ただし、ドメイン内のユーザは互いに IM を続けることができます。このポリシー アクションを [無効（Disabled）] に設定すると、VoIP、ビデオ、ファイル転送などの依存関係にある他のサービスも無効になります。	[有効（Enabled）]
アップロード ウィジェット（Upload Widgets）			[有効（Enabled）]
ユーザによるプロファイルの編集を許可（Allow user to edit profile）	ユーザの自身のプロファイル情報の編集機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、ユーザは自身のプロファイル情報を編集できなくなります。 このポリシー アクションは、[設定（Configuration）]タブの下にある [プロファイルの設定（Profile Settings）] 画面の設定に影響します。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
ユーザによる表示プロファイル設定の編集を許可（Allow user to edit the view profile setting）	ユーザのグループが、ユーザプロファイルの表示設定の変更を制限できる機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、ユーザはユーザプロファイルの表示設定の変更できなくなります。 このポリシー アクションは、[設定（Configuration）]タブの下にある [プロファイルの設定（Profile Settings）] 画面の [ユーザによるプロファイル表示設定の変更を許可（Allow users to change their profile view settings）] チェックボックスに影響します。 このポリシー アクションを [無効（Disabled）]に設定すると、[ユーザによるプロファイル表示設定の変更を許可（Allow users to change their profile view settings）] チェックボックスは、選択している場合でも無意味になります。	[有効（Enabled）]
内部スクリーンキャプチャ（Internal Screen Capture）	組織内のユーザのスクリーンキャプチャ送信機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織内でスクリーンキャプチャを送信できなくなります。	[有効（Enabled）]
外部スクリーンキャプチャ（External Screen Capture）	ユーザが組織外のユーザにスクリーンキャプチャを送信する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織外でスクリーンキャプチャを送信できなくなります。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
内部ブロードキャストメッセージの送信（Send Internal Broadcast Message）	ユーザが組織内のユーザにブロードキャストメッセージを送信する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織内でブロードキャストメッセージを送信できなくなります。	[有効（Enabled）]
外部ブロードキャストメッセージの送信（Send External Broadcast Message）	ユーザが組織外のユーザにブロードキャストメッセージを送信する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織外でブロードキャストメッセージを送信できなくなります。	[有効（Enabled）]
ユーザによるディレクトリグループへのブロードキャストの送信を許可（Allow user to send broadcast to a directory group）	ユーザが組織内のディレクトリ グループにブロードキャストメッセージを送信する機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、組織内のユーザが組織内のディレクトリ グループにブロードキャストメッセージを送信できなくなります。	[有効（Enabled）]

ポリシー アクション	説明	影響	デフォルト値
HD ビデオ（HD Video）	外部ビデオポリシーまたは内部ビデオポリシーが有効になっている場合に、コンピュータ コールに対するコンピュータ上の HD ビデオ機能を制御します。	このポリシー アクションを [無効（Disabled）]に設定すると、コンピュータ コールに対するすべてのコンピュータの HD ビデオが停止します。	[有効（Enabled）]

すべてのユーザに対して以下のポリシー アクションを無効にする組織管理者は、各値を False に設定する必要があります。

- 内部 VoIP（Internal VoIP）
- 外部 VoIP（External VoIP）
- 内部ビデオ（Internal Video）
- 外部ビデオ（External Video）
- 内部ファイル転送（Internal File Transfer）
- 外部ファイル転送（External File Transfer）
- 内部デスクトップ共有（Internal Desktop Share）
- 外部デスクトップ共有（External Desktop Share）

暗号化レベル

通常、Cisco WebEx アプリケーション間で行われるすべての IM 通信は、Cisco WebEx 組織内および組織外の両方で暗号化されます。IM 通信は発信元の Cisco WebEx アプリケーションで暗号化され、宛先のアプリケーションで復号化されます。この暗号化は、テキスト、デスクトップ（およびアプリケーション）共有、ファイル転送、VoIP、およびビデオを含むすべての IM 通信の形態に適用されます。

Cisco WebEx には 3 つのレベルの暗号化が用意されています。

- **256 ビット Advanced Encryption Standard（AES）/エンドツーエンドの暗号化**：追加のセキュリティ層を提供します。データはアプリケーションで AES を使用して暗号化され、その宛先でのみ復号化されます。
- **128 ビット セキュア ソケット レイヤ（SSL）**：アプリケーションとデータセンターの SSL ターミネーション ポイント間の接続が暗号化されます。Cisco WebEx バージョン 6 以降では、Cisco WebEx アプリケーションは常に SSL（セキュア ソケット レイヤ）を使用して Cisco WebEx データセンターに接続します。

- **暗号化なし**：データは暗号化されませんが、接続は SSL で行われることがあります（Cisco WebEx バージョン 5.x の場合）。Cisco WebEx バージョン 6 以降では、常に SSL で接続します。

  暗号化のレベルは、組織管理者が設定しているポリシーによって異なります。組織管理者は、Cisco WebEx 組織全体または特定のグループに対して暗号化ポリシーを適用できます。

  Cisco WebEx アプリケーションは、そのアプリケーションにログインしているユーザに適用可能なポリシーから自動的に暗号化レベルを判断します。したがって、Cisco WebEx 組織のポリシー設定により特定の暗号化レベルが許可されない場合、IMセッションは許可されず、適切なエラー メッセージがその IM セッション内のすべてのアプリケーションに表示されます。

  （注） グループ IM のシナリオでは、最初の招待の送信時にすべてのユーザ間で暗号化レベルがネゴシエートされます。IM セッションが確立されると、後続の出席者は、参加するためにはネゴシエートされた暗号化レベルをサポートしている必要があります。

  次の例は、IM セッションの一般的な暗号化ポリシーを示しています。

  エンドツーエンドの暗号化の導入を選択する組織は、次のポリシー オプションから選択できます。

- エンドツーエンドの暗号化のみ許可。IMのログを記録する必要があるユーザがいる場合、エンドツーエンドの暗号化を排他的に設定しないでください。これは、IM ログ記録がエンドツーエンドの暗号化より優先されるためです。
- エンドツーエンドの暗号化と SSL 暗号化の両方を許可。このオプションは、Cisco WebEx バージョン 5.x を使用している場合に適用されます。
- エンドツーエンドの暗号化、SSL 暗号化を許可、および暗号化なし。

  アクション エディタで、選択したポリシー オプションに基づき各暗号化レベルを [有効（Enabled）]または [無効（Disabled）] に設定する必要があります。

次の表に、これらのポリシー オプションの影響を示します。

アプリケーション A のポリシー	**アプリケーション B の暗号化レベル**		
	エンドツーエンド暗号化	**SSL**	**SSL**
エンドツーエンドの暗号化のみ	エンドツーエンド暗号化	許可しないでください	許可しないでください

アプリケーションAのポリシー	アプリケーション B の暗号化レベル		
エンドツーエンドの暗号化または SSL	エンドツーエンド暗号化	SSL	許可しないでください
エンドツーエンドの暗号化、SSL、または暗号化なし	エンドツーエンド暗号化	SSL	暗号化なし

アクションエディタで、選択したポリシーオプションに基づき各暗号化レベルを [有効（Enabled）] または [無効（Disabled）] に設定する必要があります。

第 8 章

Cisco WebEx Messenger グループ

概要

Cisco WebEx Messenger では、ユーザはグループ（またはポリシー グループ）にまとめられます。組織管理者は以下のことができます。

- 新規グループの作成
- グループ ポリシーの割り当て
- グループの編集
- グループの削除
- グループの編成

グループには、特定のグループに属しているユーザに適用されるアクションを決定するグループ ポリシーが割り当てられます。ユーザは 1 つ以上のグループのメンバーになることができます。グループにポリシーを割り当てる場合、グループおよび適用するポリシーを選択します。複数のポリシーを 1 つのグループに割り当てることができます。グループに子グループが含まれている場合、親グループに割り当てるポリシーも子グループに適用されます。ただし、子グループに割り当てるポリシーは親グループには適用されません。ポリシーの詳細については、ポリシーおよびポリシー アクション，（105 ページ）を参照してください。

グループは関連付けられているユーザがいない空の状態の場合のみ削除できます。一方、グループが空ではない場合は、複数のグループに属しているユーザを削除できます。Cisco WebEx Messenger 組織がプロビジョニングされたときに作成された最上位グループは削除できません。

会社または組織の名前が付いた最上位グループは、Cisco WebEx Messenger 組織がプロビジョニングされるときに作成されます。組織管理者ロールは、最上位グループのメンバーであるユーザにのみ割り当てることができます。

組織管理者は、親グループと子グループを作成して階層方式にグループを編成できます。グループ階層の最上位のグループは常に、Cisco WebEx Messenger 組織がプロビジョニングされるときに作成される最上位グループです。最上位グループの上に別の親グループを作成することはできません。最上位グループの下には、任意の数の親グループと子グループを作成できます。

（注） Cisco WebEx Messenger では、個人ライブラリがユーザと関連付けられたグループとして表示されますが、このグループは変更できません。

[グループ（Group）]ウィンドウを表示するには、Cisco WebEx Messenger 管理ツールの [グループ（Group）] タブを選択します。

（注） 次のオプションは、Cisco WebEx Messenger 組織をディレクトリ統合およびシングル サインオン統合で設定する場合は使用できません。

- 新規グループの作成
- 既存グループの編集
- 既存グループの削除

新規グループの作成

手順

ステップ 1 新しいグループを作成するには、[グループ（Group）] > [追加（Add）] を選択します。
[親グループ（Parent Group）]の名前がこのダイアログ ボックスの上部に常に表示されます。

ステップ 2 選択して [グループの追加（Add Group）]ダイアログボックスを開きます。

ステップ 3 [グループ名（Group Name）]フィールドに、グループの名前を入力します。

ステップ 4 [OK]を選択します。

グループの編集

グループの編集には名前の変更だけが含まれます。

手順

ステップ 1 グループを編集するには、[グループ（Group）]タブを選択します。

ステップ 2 [検索（Search）]フィールドで、編集するグループ名を 1 文字以上入力し、[検索（Search）] を選択します。

ステップ 3 グループを選択し、[名称変更（Rename）]を選択します。

ステップ 4 [グループ名（Group Name）]フィールドにグループの新しい名前を入力し、[OK] を選択します。
名前が変更されたグループが [グループ（Group）]画面に表示されます。

グループの削除

手順

ステップ 1 グループを削除するには、[グループ（Group）]タブを選択します。

ステップ 2 [検索（Search）] フィールドで、削除するグループ名を 1 文字以上入力し、[検索（Search）]を選択します。

ステップ 3 グループを選択し、[削除（Delete）]を選択します。

ステップ 4 メッセージ ボックスで [OK]を選択し、選択したグループを削除します。
削除したグループはもとに戻せません。

グループへのポリシーの割り当て

手順

ステップ 1 グループにポリシーを割り当てるには、[グループ（Group）]タブを選択します。

ステップ 2 [検索（Search）]フィールドで、ポリシーを割り当てるグループ名を 1 文字以上入力し、[検索（Search）] を選択します。

ステップ 3 検索条件に一致するグループのリストで、ポリシーを割り当てるグループを選択します。

ステップ 4 [ポリシー割り当て（Policy Assignment）]フレームで、適用するポリシーを選択します。

ポリシーは一度に 1 つのみ選択できます。ポリシーが割り当てられると、動作が短時間だけ一時停止します。

ステップ 5 ポリシーの割り当てを無効にする場合は、該当するポリシー名の横にあるチェック ボックスをオフにします。

最上位、親、子グループの表示

手順

ステップ 1 最上位、親、子グループを表示するには、[グループ（Groups）]タブを選択します。

ステップ 2 [検索（Search）]フィールドで、親または子グループを表示させるグループ名を 1 文字以上入力し、[検索（Search）] を選択します。

ステップ 3 グループを選択し、[その他の操作（More Actions）]を選択します。

ステップ 4 [その他の操作（More Actions）]リストから、必要に応じて次のいずれかを選択します。

- [グループのユーザを表示（View Group Users）]：選択したグループに属しているユーザのリストを表示します。ユーザのリストが [ユーザ（User）]タブの [ユーザ（User）] 画面に表示されます。
- [最上位グループ（Top Level Group）]：選択したグループの最上位グループを表示します。最上位グループは、必ず Cisco WebEx Messenger 組織をプロビジョニングしたときに作成されるグループです。
- [子グループを表示（View Child Groups）]：選択したグループの子グループを表示します。
- [親グループを表示（View Parent Groups）]：選択したグループの親グループを表示します。

第 9 章

ディレクトリ統合

概要

ディレクトリ統合を行うと、Cisco WebEx 組織に対して次の内容が有効になります。

- ユーザ プロビジョニングとプロビジョニング解除の自動化。
- Cisco WebEx 管理ツールでの社内ディレクトリの情報で更新されたユーザ プロファイル情報の保持。
- ユーザが個々のメンバーを直接追加することなく、連絡先リストにグループを追加できるようにするための、Cisco WebEx 内のユーザへのグループの公開（配布リストなど）。
- ポリシー グループへのユーザの分類。グループにポリシーを適用する方法の詳細については、グループへのポリシーの割り当て，（121 ページ）を参照してください。
- Cisco WebEx 組織がディレクトリ統合を行うことで有効になっている場合、ユーザは自分のプロファイル内のディレクトリ情報を編集できません。ユーザは自分のプロファイルを更新するためには、組織管理者に連絡する必要があります。
- Cisco WebEx 組織がディレクトリ統合を行うことで有効になっている場合、ユーザのアカウントをただちに非アクティブ化する必要がある場合は、ユーザを手動で非アクティブ化できます。

ディレクトリ統合のインポートプロセスとファイル形式

注：組織管理者とユーザ管理者は、ディレクトリ統合プロセスを使用して作成することはできません。

組織のディレクトリ統合を有効にする予定の Cisco WebEx のお客様は、次の手順を実行する必要があります。

- Cisco CSM または担当者に連絡して、ディレクトリ統合を依頼します。
- Cisco WebEx 管理ツールにサインインし、シスコから提供される資格情報とその他の設定を使用して、ディレクトリ統合の設定を行います。
- 以下を実行するためのスクリプトまたはツールを開発して実行します。
- ディレクトリから関連のある情報を抽出します。
- 抽出した情報をCSVファイルに変換します。CSVファイルの詳細については、グループ ファイルの形式, （131 ページ）を参照してください。

（注）

- タブ区切りまたはカンマ区切りの CSV ファイルを使用できます。
- CSV ファイルが ISO-8859-1 形式で符号化されていることを確認します。
- ディレクトリ統合を開始する前に次の 4 つの CSV ファイルをアップロードする必要があります。userInactivation_xxx.csv、userFile_xxx.csv、groupFile_xxx.csv、groupDeletion_xxx.csv。
- CSV ファイルをシスコのセキュア FTP サーバにアップロードします。

ジョブのスケジューリングには CRON 式を使用します。詳細については、CRON 式, （126 ページ）を参照してください。

ディレクトリ統合の設定

手順

ステップ 1 [設定（Configuration）] タブ > [システム設定（System Settings）] > [ディレクトリ設定（Directory Settings）].を選択します。

ステップ 2 [ジョブのスケジューリング（Job Scheduling）]フィールドに、ジョブを実行するスケジュールを入力します。

ステップ 3 [SFTP サーバ（SFTP Server）]で各フィールドの詳細を入力します。
各フィールドの詳細については、「関連項目」の項を参照してください。

SFTPサーバはシスコがホストするサーバであり、顧客にCSVファイルを安全な方法でアップロードおよびダウンロードするアクセス方法を提供します。

ステップ4 [保存（Save）]を選択します。

（注） ジョブ実行時間を最初にスケジュールした担当者が退職した場合、そのジョブ実行時間を再スケジュールする必要があります。Cisco WebEx Messengerアカウントが無効になる、または削除されると、スケジュールされたジョブは自動的に停止します。

[ジョブスケジューリング（Job Scheduling）]フィールドの既存のスケジュールをクリアし、新しいスケジュール時間を入力することによって、ジョブ実行時間を再スケジュールできます。既存のスケジュールをクリアし、新しいスケジュールを入力したら、[保存（Save）]を選択します。

これにより、Messengerサービスがプライマリモードかバックアップモードで動作しているかどうかを問わず、スケジュールの変更を確実に適用します。

ディレクトリ統合の設定

フィールド	説明
[サーバアドレス（Server Address）]	SFTPサーバのIPアドレス。
[ポート（Port）]	STFPサーバのポート番号。通常、SFTPサーバのデフォルトのポート番号は22です。
[ユーザID（User ID）]	SFTPサーバにアクセスできるユーザのID。通常は、お客様のCisco WebEx組織の管理者です。
[パスワード（Password）]	ユーザIDに関連付けられたパスワード。
[入力フォルダパス（Input Folder Path）]	管理者が入力CSVファイルをダウンロードするSFTPサーバのフォルダのパス。デフォルトのフォルダ名は**Input**で、大文字と小文字が区別されます。
[出力フォルダパス（Output Folder Path）]	管理者が入力CSVファイルをダウンロードするSFTPサーバのフォルダのパス。デフォルトのフォルダ名は**Output**で、大文字と小文字が区別されます。
[エラーフォルダパス（Error Folder Path）]	出力ファイルのエラーが保存されるSFTPサーバのフォルダのパス。デフォルトのフォルダ名は**error**で、大文字と小文字が区別されます。

フィールド	説明
[ファイル パスワード（File Password）]	入力 CSV ファイルが暗号化されている場合は、CSV ファイルのパスワードを入力します。Cisco WebEx は標準の gpg 暗号化システムをサポートしています。gpg の詳細については、http://www.gnupg.org/ [英語] を参照してください。このフィールドは空白のままにすることもできます。空白の場合、CSV ファイルはプレーン テキストとして処理されます。

CRON 式

ジョブ スケジュール時間式（ディレクトリ統合のインポート プロセスとファイル形式, （124 ページ）を参照）は、空白で区切られた 6 つまたは 7 つのフィールドで構成される一連の時間を表す文字列であり、通常何らかのルーチンを実行するためのスケジュールとして指定します。フィールドには、使用可能な特殊文字のさまざまな組み合わせとともに、任意の使用可能な値を含めることができます。

CRON ジョブは GMT タイム ゾーンで実行されます。

CRON 式のフィールドは次のとおりです。

フィールド シーケンス	フィールド名	必須	使用可能な値	使用可能な特殊文字
1 番目	[秒（Seconds）]		0 ～ 59	, - * /
2 番目	[分（Minutes）]	○	0 ～ 59	, - * /
3 番目	[時間（Hours）]	○	0 ～ 23	, - * /
4 番目	[日付（Day of Month）]	○	1 ～ 31	, - * ? / L W
5 番目	[月（Month）]	○	1 ～ 12 または JAN～DEC	, - * /
6 番目	[曜日（Day of Week）]	○	0 ～ 7 または SUN ～SAT	, - * ? / L #
7 番目	[年（Year）]	×	空白、1970 ～ 2099	, - * /

特殊文字

- *（「すべての値」）：フィールド内のすべての値を選択するために使用します。たとえば、「分（Minutes）」フィールドの場合は「すべての分」を意味します。
- ?（「特定の値なし」）：文字が許可される 2 つのフィールドのいずれかに含まれる値を指定するために使用します。他のフィールドの値は認められません。たとえば、月の特定の日にジョブを実行するようにスケジュールするが、曜日はいつでもいい場合、[日付（Day of Month）] フィールドに「10」を入力し、[曜日（Day of Week）] フィールドに「?」を入力します。詳しくは以下の例を参照してください。
- -：範囲を指定するために使用します。たとえば、[時間（Hours）] フィールドの「8-10」は 8 時、9 時、および 10 時を意味します。
- ,：追加の値を指定するために使用します。たとえば、[月（Month）] フィールドの「JAN,MAR,MAY」は 1 月、3 月、および 5 月を意味します。
- /：範囲の増分を指定するために使用します。たとえば、1番目のフィールド（[分（Minutes）]）が「5-59/30」の場合、1 時間に 5 分、その後 30 分ごとに増分することを示します。この場合、「-」文字の後に「/」を指定することもできます。これは、「/」の前の「0」と同等です。[日付（Day of Month）] フィールドの「1/5」は、ジョブを月の初日に実行し、その後 5 日ごとに実行するようにスケジュールされていることを示しています。
- L（「最終」）：この文字を使用できる 2 つのフィールドではそれぞれ異なる形で実行されます。たとえば、[日付（Day of Month）] フィールドの「L」は、月の最終日を示します。1 月の場合は 31 日、うるう年以外の 2 月は 28 日など。[曜日（Day of Week）] フィールドに独立型の特殊文字として入力した場合、「7」または「SAT」を示します。[曜日（Day of Week）] フィールドに入力する場合、特定の月の最後の金曜日（「5L」）としてスケジュールを指定できます。「L」オプションを使用する場合は、リストや値の範囲を指定しないでください。
- W（「平日」）：特定の日に最も近い平日（月～金曜日）を指定するために使用します。たとえば、[日付（Day of Month）] フィールドに「20W」と入力した場合、その月の 20 日に最も近い平日を示します。20 日が水曜日の場合、ジョブは 20 日の水曜日に実行されます。しかし、20 日が土曜日の場合、ジョブは 19 日の金曜日に実行されます。同様に、20 日が日曜日の場合、ジョブは 21 日の月曜日に実行されます。ただし、[日付（Day of Month）] の値として「1W」を入力し、1 日が土曜日の場合、月をまたいで実行することはできないので、ジョブは 3 日の月曜日に実行されます。「W」文字は、[日付（Day of Month）] が日付の範囲やリストではなく、単一の日の場合のみ指定できます。

  文字「L」と「W」は、[日付（Day of Month）] フィールドで組み合わせて指定することもできます。「LW」は月の最後の平日を示します。
- #：月の n 番目の日を指定するために使用します。これは [曜日（Day of Week）] フィールドに入力でき、# の後に 1 ～ 5 の数字を指定する必要があります。このため、特定の月の最初の月曜日（「2#1」）、または月の最後の水曜日（「4#5」）などを指定できます。ただし、「#5」と指定し、特定の月の曜日に 5 番目がない場合、その月はジョブが実行されません。
- 注：文字、月の名前、および曜日は大文字と小文字が区別されません。MON は mon と同じです。

例

式	意味
0 0 12 * * ?	毎日午後 12 時（正午）にスケジュールされます。
0 30 11 ? * *	毎日午前 11:30 時にスケジュールされます。
0 30 11 * * ?	毎日午前 11:30 時にスケジュールされます。
0 30 11 * * ? *	毎日午前 11:30 時にスケジュールされます。
0 * 14 * * ?	毎日午後 2 時に始まり 2:59 に終了するまで毎分スケジュールされます。
0 0/5 14 * * ?	毎日午後 2 時に始まり 2:55 に終了するまで 5 分ごとにスケジュールされます。
0 0/5 14,18 * * ?	毎日午後 2 時に始まり 2:55 に終了するまで 5 分ごとにスケジュールされ、かつ午後 6 時に始まり 6:55 に終了するまで 5 分ごとに実行されます。
0 0 12 1/5 * ?	毎月、月の初日に始まり 5 日ごとに午後 12 時（正午）にスケジュールされます。

（注） 現在、[曜日（Day of Week）] と [日付（Day of Month）] の両方に値を指定することはできません。「?」文字は、2 つのフィールドのいずれかに入力する必要があります。

午前 0 時と午前 1:00 時の間にジョブの実行をスケジュールする場合は「夏時間」に注意してください。時間を変更すると、前に調整されるか、後ろに調整されるかによってジョブがスキップされたり、繰り返されたりすることになります。

ユーザ ファイルの形式

ユーザおよびグループのディレクトリ情報は、次の形式のファイルを使用してインポートされます。ユーザおよびグループデータは別々のファイルにインポートされます。ファイルはISO-8859-1形式で保存する必要があります。

ユーザ ファイル名の形式：userFile_yyyy-mm-dd_n.csv

フォーマット	説明
yyyy-mm-dd	ジョブが実行された日付です。日付はグリニッジ標準時のタイムゾーンに基づいています。

フォーマット	説明
n	特定の日付のジョブ インスタンス番号。

例

ジョブが 1 日 4 回実行されるようにスケジュールされていて、ジョブが 2008 年 7 年 28 日に実行された場合、ファイルの名前は次のように指定されます。

```
userFile_2008-07-28_1.csv, userFile_2008-07-28_2.csv,
userFile_2008-07-28_3.csv, userFile_2008-07-28_4.csv
```

ユーザ非アクティブ化ファイル名の形式

userInactivation_yyyy-mm-dd_n.csv

ファイルにヘッダー レコードが含まれてはいけません。

ユーザ非アクティブ化のファイル形式：userSSOID

（注） シングル サインオン（SSO）が有効でない場合、非アクティブ化するユーザの電子メール アドレスを入力するか、userSSOID フィールドを削除する必要があります。

このファイルには、レコードを非アクティブ化または削除する必要がある userSSOID のみが含まれます。

フォーマット	説明
yyyy-mm-dd	ジョブが実行された日付です。日付はグリニッジ標準時のタイム ゾーンに基づいています。
n	特定の日付のジョブ インスタンス番号。

重要 ユーザが組織管理者の場合、システムからユーザが削除されると、そのユーザがスケジュールしたすべてのジョブがブロックされます。この場合、Cisco WebEx Messenger サービス エンジニア チーム（connectteam@cisco.com）にサポートをご依頼ください。

ユーザ ファイルの形式

ファイルにヘッダー レコードが含まれてはいけません。ファイル形式：

```
userSSOId,displayName,firstName,lastName,email,jobTitle,address1,city,state,zip,
country,phoneOffice,phoneCell,homeGroupSSOId,homeGroupName,businessUnit,userProfilePhotoURL,
address2,storageAllocated,CUCMClusterName,IMloggingEnable,EndPointName,autoUpgradeSitName,
center,TC1,TC2,TC3,TC4,TC5,TC6,TC7,TC8,TC9,TC10
```

フォーマット	説明
userSSOId	必須：Cisco WebEx 組織の社内で使用される userSSOID。これは更新するレコードを判別するために使用されるメインフィールドです。同じ userSSOID を持つユーザが Cisco WebEx データベース内にすでに存在する場合、このようなユーザの詳細情報が更新されます。存在しない場合、新しいユーザがすべての詳細情報によって Cisco WebEx 組織でプロビジョニングされます。
displayName	Cisco WebEx クライアントのユーザの表示名。
firstName	必須：ユーザの名前。
lastName	必須：ユーザの姓。
email	必須：ユーザの電子メールアドレス。 アドレスが更新または変更されるたびに、ユーザ名、ログインおよび IM 連絡先リストが古いユーザ名から新しいユーザ名に自動的に移行されます。そのユーザのすべての連絡先が、新しいユーザ名の新しいプレゼンス サブスクリプション要求を自動的に受信します。
jobTitle	オプション：ユーザの役職名。
address1	オプション：ユーザの電子メールアドレス。
city	オプション：ユーザが住んでいる都市。
state	オプション：ユーザが住んでいる都道府県。
zip	オプション：ユーザが住んでいる都市の郵便番号。
country	オプション：ユーザが住んでいる国。
phoneOffice	オプション：ユーザの勤務先の電話番号。
phoneCell	オプション：ユーザの携帯電話番号。
homeGroupSSOId	オプション：グループを特定するために組織の内部で使用される。グループが Cisco WebEx ですでに作成されているかどうかを決定します。作成されている場合はグループ情報が更新されます。作成されていない場合は新しいグループが作成されます。値が存在する場合、ユーザはそのグループに関連付けられます。
homeGroupName	オプション：グループの名前。名前が指定されていない場合、homeGroupSSOID 自体が使用されます。

フォーマット	説明
businessUnit	オプション：存在する場合、この情報はユーザのプロファイル エリアに配置されます。
userProfilePhotoURL	オプション：ユーザのプロファイル写真が提供される URL。この URL は、Cisco WebEx アプリケーションが写真を表示するためにそのまま使用されます。
address2	オプション：ユーザの別の電子メールアドレス（あれば）。
storageAllocated	オプション：Cisco WebEx でユーザに割り当てられたストレージ容量（MB 単位）。
CUCMClusterName	オプション：ユーザが割り当てられた CUCM クラスタの名前（あれば）。
IMLoggingEnable	オプション：このフィールドの値は true または false となります。 （注） この値は、次に説明する **EndPointName** フィールドとともに使用することができます。
EndPointName	オプション：ユーザに対して設定されている IM アーカイブ エンドポイントの名前（あれば）。 （注） ユーザに対してエンドポイントが設定されておらず、**IMLoggingEnable** が True に設定されている場合、ユーザのエンドポイントは Cisco WebEx 組織のデフォルトのエンドポイントに設定できます。
autoUpgradeSiteName	オプション
center	オプション：ユーザの Cisco WebEx Meeting アカウント（アカウントが作成されている場合）。
TC	オプション：Cisco WebEx と Cisco WebEx Meeting が統合されている場合の、ユーザの Cisco WebEx Meeting アカウントの追跡コード。 （注） 追跡コードは TC1 ～ TC10 の範囲です。

グループ ファイルの形式

ユーザおよびグループのディレクトリ情報は、次の形式のファイルを使用してインポートされます。ユーザおよびグループ データは別々のファイルにインポートされます。ファイルは ISO-8859-1 形式で保存する必要があります。

グループ ファイル名の形式

グループ ファイル名の形式：groupFile_yyyy-mm-dd_n.csv

フォーマット	説明
yyyy-mm-dd	ジョブが実行された日付です。日付はグリニッジ標準時のタイム ゾーンに基づいています。
n	特定の日付のジョブ インスタンス番号。

グループ ファイル形式

ファイルにヘッダー レコードが含まれてはいけません。

グループ ファイルには、次の異なる 3 タイプのレコードが含まれます。グループ情報、子グループ情報、およびメンバー情報。各レコード タイプは、recIndicator（レコード インジケータ）を指定することによって差別化されます。

- グループ情報はレコード インジケータ（**g**）を記録
- 子グループ レコードはレコード インジケータ（**gg**）を記録
- グループ メンバーはレコード インジケータ（**gu**）を記録

グループ レコード

次の表にグループ情報レコードのリストを示します。

recIndicator、ssoGroupId、groupName、groupType

フォーマット	説明
SSOGroupID	このフィールドは、グループが Cisco WebEx Messenger に作成されているかどうかを判断するために使用されます。すでに作成されている場合、グループ情報が更新されます。作成されていない場合は、新しいグループが作成されます。
groupType	これはオプションです。指定する場合は、数値を指定する必要があります。groupType には次の値を指定できます。 • 0：標準（Normal）。通常、ほとんどのグループがこのタイプに属します。 • 4：プレゼンス（Presence）。これらのグループは、Cisco Jabber アプリケーションでの検索に使用できます。 groupType が指定されていない場合、デフォルト値は 0 です。

子グループ レコード

子グループ レコードのフィールドは次のとおりです。

recIndicator、ssoGroupId、RECURRING_subGroupSSOID

たとえば、subgroupSSOIDは、親レコードインジケータおよび属している親グループIDの後にカンマ区切りの形式で指定します。

グループ メンバー レコード

グループ メンバー レコードのフィールドは次のとおりです。

recIndicator、ssoGroupId、RECURRING_memberSSOID

メンバー SSOID は、レコード インジケータおよび属しているグループ ID の後に指定します。

グループ ファイルには、さまざまなタイプのレコードを任意の順序で含めることができます。次の例では、3 タイプのレコードすべてが任意の順序で含まれています。

g、groupSSOID1、Group SSO Name1

g、groupSSOID2、Group SSO Name2

g、groupSSOID3、Group SSO Name3

gu、groupSSOID2、userSSOId6、userSSOId7

g、groupSSOID4、Group SSO Name4

g、groupSSOID5、Group SSO Name5

gg、groupSSOID3、groupSSOID10

gu、groupSSOID1、userSSOId1、userSSOId2、userSSOId3、userSSOId4

gg、groupSSOID1、groupSSOID2、groupSSOID3、groupSSOID4、groupSSOID5

gg、groupSSOID2、groupSSOID3、groupSSOID4

グループ削除ファイル名の形式

グループ削除ファイル名の形式：groupDeletion_yyyy-mm-dd_n.csv

ファイルにヘッダー レコードが含まれてはいけません。

グループ削除ファイルの形式：SSOGroupID。

（注） シングル サインオン（SSO）が有効になっていない場合は、SSOGroupID フィールドに削除するグループの名前を入力する必要があります。

このファイルには、レコードを削除する必要がある SSOGroupID のみ含まれています。

フォーマット	説明
yyyy-mm-dd	ジョブが実行された日付です。日付はグリニッジ標準時のタイム ゾーンに基づいています。

フォーマット	説明
n	特定の日付のジョブ インスタンス番号。

ディレクトリ統合が有効になっている Cisco WebEx 組織へのログイン

ディレクトリ統合を有効にすると、Cisco WebEx 組織でプロビジョニングされたユーザ宛てにウェルカム メールが送信されます。ただし、Cisco WebEx 組織がシングル サインオン統合で有効になっている場合は、ウェルカム メールは送信されません。

ディレクトリ統合が有効になった Cisco WebEx 組織のユーザは、Cisco Jabber アプリケーションにログインして、サインイン パスワードを変更できます。さらに、Cisco WebEx 組織の管理者は、Cisco WebEx 組織全体のパスワードをリセットすることができます。

第 10 章

レポート

概要

Cisco Jabber アプリケーションのアクティビティと使用状況を追跡および測定するためのレポートを生成できます。レポートは13ヵ月前までの分のみ実行できます。レポートの生成は、生成するレポート タイプの選択とレポートの生成から構成される 2 ステップのプロセスです。各レポートには、タイム ゾーンとしてグリニッジ標準時（GMT）を使用しているタイム スタンプが表示されます。

多くのレポートは 15、30、60 分間隔で実行できます。

Cisco WebEx Messenger の組織管理者は、以下のレポートを生成できます。

- Messenger ユーザ レポート，（136 ページ）
- Messenger ウィジェット レポート，（138 ページ）
- Messenger アクティビティ，（138 ページ）
- Messenger ユーザ アクティビティ，（139 ページ）
- 監査証跡レポート，（141 ページ）

  一度に 1 つのレポートのみ実行できます。進捗状況インジケータにレポートの生成ステータスが表示されます。完了ステータスは、レポートが正常に生成されたことを示します。レポートは直接表示することも、CSV ファイルとしてコンピュータに保存することもできます。レポートは生成日から 7 日間保存されます。

レポートの生成

手順

ステップ 1 レポートを編集するには、[レポート（Report）]タブを選択します。

ステップ 2 [レポート タイプ（Report Type）]ドロップダウン リストから、生成するレポートのタイプを選択します。

ステップ 3 （任意）レポートの [期間（Interval）]を選択します。
[期間（Interval）] オプションは次のレポートに対してだけ使用できます。

- [Messenger アクティビティ（Messenger Activity）] : [期間（Interval）]、[月（Month）]、または [年（Year）] を選択します。
- [Messenger ユーザ アクティビティ（Messenger UserActivity）] : [月（Month）]、または [年（Year）] を選択します。

ステップ 4 [レポートの生成（Generate Report）]を選択します。
[Status（ステータス）]列には、レポート生成の進捗を示す[実行中（Running）]ステータスが表示されます。レポートが正常に生成されたら、[ステータス（Status）]列に[完了（Completed）]が表示されます。さらに、レポートをダウンロードする手順を含む電子メールが送信されます。

ステップ 5 レポートを開くか、または保存するには、レポート リンクの名前を選択します。

（注） [実行中（Running）]のステータスが表示されている間にレポートの生成をキャンセルするには、[進行をキャンセル（Cancel the Progress）]を選択します。[停止（Stopped）]ステータスは、レポート生成がキャンセルされたことを示します。

Messenger ユーザ レポート

Messenger ユーザ レポートには、以下のカラムが含まれます（レポートには次の表の表示順に左から右に表示されます）。

カラム	説明
ユーザ名（User Name）	ユーザのサインイン名。
ユーザ ステータス（User Status）	ユーザのステータスが「アクティブ化」または「非アクティブ化」として表示されます。非アクティブ化ユーザは Cisco Jabber アプリケーションにサインインできません。
使用済み合計ストレージ（MB）（Total Storage Used(MB)）	使用されているストレージの合計メガバイト数。

カラム	説明
割り当て済み合計ストレージ（MB）（Total Allocated Storage（MB））	ユーザに割り当てられているストレージ制限の合計メガバイト数。
所有合計スペース数（Total Number of Spaces Owned）	ユーザが所有するスペースの合計数。
メンバーとしてのスペースの合計数（Total Number Of Spaces as Member）	ユーザがメンバーのロールを持つスペースの合計数。
ログイン済みユーザ（Logged User）	ユーザの IM が IM ログ記録およびアーカイブ経由でサインインされているかどうかが表示されます。（True/False）。
アーカイブのエンドポイント（Archiving Endpoint）	ユーザの IM がアーカイブされているエンドポイント。 ログイン済みユーザ（Logged User）が True に設定されている場合、この値はデフォルトに設定されています。 ユーザの IM が、デフォルトのアーカイブ エンドポイントとして指定されているエンドポイントにアーカイブされている場合、この値は [デフォルト（Default）] と表示されます。詳細については、IM アーカイブの設定，（62 ページ）を参照してください。
名簿内のユーザの数（ディレクトリ グループを除く）（Number of Users in roster（excluding Directory Groups））	ユーザの連絡先リストにある連絡先の数が表示されます。ディレクトリ グループ内の連絡先は含まれません。詳細については、ディレクトリ統合，（123 ページ）を参照してください。
名簿内の個人グループの数（Number of Personal Groups in roster）	ユーザの連絡先リストにある連絡先の数が表示されます。この数には、ディレクトリ グループに属している連絡先は含まれません。詳細については、ディレクトリ統合，（123 ページ）を参照してください。
名簿内のディレクトリ グループの数（Number of Directory Groups in roster）	ディレクトリ グループはメンバーシップが事前に決まっているグループです。ユーザは自分の連絡先リストにグループを追加できますが、グループ内のメンバーを変更することはできません。この機能は、お客様がディレクトリ統合機能を使用している場合のみ使用できます。

Messenger ウィジェット レポート

Messenger ウィジェット レポートには、Cisco WebEx Messenger 組織で作成されたウィジェットに関する詳細が表示されます。このレポートは、組織が Cisco WebEx Messenger のスペース機能を使用している場合のみ役立ちます。Messenger ウィジェット レポートには、以下のカラムが含まれます（レポートには次の表の表示順に左から右に表示されます）。

カラム	説明
ウィジェット名（Widget Name）	ウィジェットの名前。
会社名（Company Name）	ウィジェットが作成されている会社の名前。
作成者名（Creator Name）	ウィジェットを作成した人（ユーザ）の名前。
バージョン番号（Version Number）	ウィジェットのバージョン番号。
使用スペース数（Used in Spaces）	このウィジェットが使用されているスペースの数。

Messenger アクティビティ

Messenger アクティビティ レポートには、特定の月に Cisco WebEx Messenger 組織で行われたさまざまなアクティビティの詳細が表示されます。このレポートには、レポートを生成した月における以下のデータが表示されます。

カラム	説明
日付（Date）	日付データが YYYY/MM/DD の形式で表示されます。これはデータ収集の開始日です。
時刻（Time）	時刻データが表示されます。これはデータ収集が開始された時刻です。データの収集および集約は、指定した集約間隔（15、30、および 60 分）で実行されています。
同時ユーザの数（Number of Concurrent Users）	Cisco Jabber アプリケーションに同時にサインインしたユーザの数が表示されます。 （注） メトリックは次のように計算されます。同時ユーザの数＝サインインしたユーザの数（時間間隔の最初）＋サインインしたユーザの数（時間間隔の最中）- サインアウトしたユーザの数（時間間隔の最中）。負の数も可能です。

カラム	説明
ログイン/ログアウトの集約数（Aggregate Number of Logins/Logouts）	サインインとサインアウトの数が表示されます。 （注） これは、同時ユーザの数（現在の間隔）–同時ユーザの数（前の間隔）で求められます。
IM の数（Number of IM's）	発信インスタント メッセージの数が表示されます。
ホストした会議の数（Number of Meetings Hosted）	Cisco Jabber アプリケーションからホストした会議の数が表示されます。
参加した会議の数（Number of Meetings Joined）	Cisco Jabber アプリケーションから参加した会議の数が表示されます。
デスクトップ共有セッションの数（Number of Desktop Share Sessions）	Cisco Jabber アプリケーションから開始されたデスクトップ共有セッションの数が表示されます。
テレフォニー コールの数（Number Telephony of Calls）	Cisco Jabber アプリケーションから開始された会議コールの数が表示されます。
クリックツーコールの数（Number of Click-to-Call Calls）	Cisco Unified Communication Integration を使用して Cisco Jabber アプリケーションから開始されたコールの数が表示されます。
ビデオ コールの数（Number of Video Calls）	発信ビデオ コールの数が表示されます。
PC 間コールの数（Number of PC-to-PC Calls）	発信 VoIP コールの数が表示されます。

Messenger ユーザ アクティビティ

Messenger ユーザ アクティビティ レポートには、特定の月に Cisco WebEx Messenger 組織のユーザが実行したアクティビティの詳細が表示されます。このレポートには、レポートを生成した月における以下のデータが表示されます。

カラム	説明
ユーザ名（User Name）	ユーザの名前（サインイン名）が表示されます。
ログイン回数（Number of Logins）	Cisco Jabber アプリケーションにユーザがサインインした回数が表示されます。
新たに所有したスペースの数（Number of New Spaces Owned）	その月に新たに作成されたスペースの数が表示されます。この数には、ユーザが初めてサインインするときに自動的に作成される 2 つのスペース（MyWebex と Developer Sandbox）が含まれます。
新たに参加したスペースの数（Number of New Spaces Joined）	その月にユーザがメンバー ロールで参加した新しいスペースの数が表示されます。この数には、ユーザが作成したスペースの数は含まれません。
ホストした会議の数（Number of Meetings Hosted）	Cisco Jabber アプリケーションからホストした会議の数が表示されます。
参加した会議の数（Number of Meetings Joined）	Cisco Jabber アプリケーションから参加した会議の数が表示されます。
IM 数（Number of IMs）	発信 IM の数が表示されます。
テレフォニー コールの数（Number of Telephony Calls）	Cisco Jabber アプリケーションからユーザによって開始された会議コールの数が表示されます。
クリックツーコールの数（Number of Click-to-Call Calls）	Cisco Unified Communication Integration を使用して Cisco Jabber アプリケーションからユーザによって開始されたクリックツーコールの数が表示されます。
デスクトップ共有セッションの数（Number of Desktop Share Sessions）	Cisco Jabber アプリケーションからユーザによって開始されたデスクトップ共有セッションの数が表示されます。

カラム	説明
追加の使用ストレージ（MB）（Additional Storage Used（MB））	使用されている追加ストレージの量（MB 単位）が表示されます。 このメトリックは、次のように計算されます。 追加の使用ストレージ = 使用ストレージ – 解放されたストレージ。これは負の数になることがあります。
最終ログイン（Last Login）	ユーザが最後にサインインした時刻と使用しているタイプまたはバージョンが表示されます。
ビデオ コールの数（Number of Video Calls）	ユーザが行ったビデオ コール（発信コール）の数が表示されます。
PC 間コールの数（Number of PC-to-PC Calls）	Cisco Jabber アプリケーションから開始された VoIP コールの数が表示されます。

監査証跡レポート

監査証跡レポートには、Cisco WebEx Messenger の組織管理者によって実行されたすべての操作のリストが表示されます。組織管理者が Cisco WebEx Messenger 管理ツール内で実行するすべての操作はツールによってログに記録され、監査証跡レポートに表示されます。操作には、Cisco WebEx Messenger 管理ツールへのサインイン、インターフェイス上のさまざまなタブのクリック、構成時の設定の変更、監査証跡レポート自体の生成などが含まれます。

監査証跡レポートは CSV ファイルとして利用でき、次の詳細情報が含まれています。

カラム	説明
管理者（Administrator）	操作がログに記録され、このレポートでキャプチャされている組織管理者のサインイン ID。
Timestamp	組織管理者によって実行された各操作のタイムスタンプ。
カテゴリ（Category）	操作が属しているカテゴリ。一般的なカテゴリには、サインイン、構成、ポリシー管理、およびレポート管理があります。
サブ カテゴリ（Sub Category）	操作が属しているサブ カテゴリ。一般的なサブ カテゴリには、会議、XMPP IM クライアント、ポリシー アクションの追加と削除、自動アップグレード、およびユニファイド コミュニケーションがあります。

カラム	説明
詳細（Details）	操作の詳細。たとえば、組織管理者がユニファイド コミュニケーションの設定を変更すると、対応する詳細には、「すべてのクラスタの組織レベルの設定を変更（Changed the Org-Level settings for all clusters）」という表現が含まれます。

第 11 章

CSV ファイル形式

概要

組織にユーザをインポートする場合はCSVファイルを使用します。インポートを成功させるためには、すべてのCSVファイルが特定の形式に従っている必要があります。インポートする前に、CSV ファイルの作成に関する次のガイドラインを確認することを推奨します。

重要 CSVファイルからのユーザのインポートが初めてではない場合は、最初にユーザをエクスポートする必要があります。エクスポートすることで、CSVファイル内の最新情報（更新されている可能性がある電話番号などの詳細）を保持することができます。次に、新しい情報やユーザで最新の CSV ファイルを編集し、UTF-8 または UTF-16LE エンコード スプレッドシートとして保存し、Cisco WebEx Messenger 組織にインポートし直すことができます。

- CSV ファイルは UTF-8 と UTF-16LE の両方の形式をサポートしています。
- CSVファイルのすべての列には、有効な名前の付いたヘッダーが必要です。有効な列名の詳細については、CSV フィールド，（144 ページ）を参照してください。
- フィールドに情報を入力しない場合は、「-」文字を入力します。そのフィールドは空のフィールドとしてデータベースにインポートされます。これはオプションフィールドに対してのみ行えます。「-」を必須フィールドに入力すると、インポート時にエラーが表示されます。N/A 値は使用しないでください。
- 通常、列の名前はユーザのプロファイル内のフィールドの名前に対応している必要があります。たとえば、[ユーザプロファイル（User Profile）] ダイアログボックスの [名（First Name）]

フィールドは、CSV ファイルの [名（firstName）] という名前の列と対応している必要があります。

- CSV ファイルには任意の列名または無効な列名を設定できます。ただし、それらの列はインポート プロセス中にスキップまたは順序変更されます。
- インポートのステータスは、ステータスを示す特定の列とともに、入力ファイルの情報がすべて複製される CSV ファイルに記録されます。
- Cisco WebEx 内に同じ電子メール アドレスを持つユーザがすでに存在する場合、データベース内の既存のレコードは CSV ファイルの値で上書きされます。
- 以前の設定は更新によって置き換えられます。たとえば、ユーザに対して新しいロールが指定されている場合、以前のロールは置き換えられます。
- インポート プロセスはバックグラウンドで実行されます。そのため、Cisco WebEx のその他の管理タスク（設定など）を実行し続けることができます。
- インポートが完了すると、インポートを開始したユーザに確認の電子メールが送信されます。その通知にはインポート結果のサマリーが含まれています。
- 組織管理者は進行中のインポート プロセスをキャンセルすることができます。

（注） 情報は CSV ファイルに指定されているとおりにインポートされます。すべての情報が正しいことを確認する必要があります。たとえば、国番号のない電話番号が提供されると、IM や会議で自動コールアウトが行われません。その場合は、CSV ファイルを変更して正しい国番号を指定し、CSV ファイルを再度インポートする必要があります。

CSV フィールド

注：CSV のインポート プロセスを使用して組織管理者とユーザ管理者を作成することはできません。

Cisco WebEx にユーザをインポートする前に、次のフィールド（順不同）を CSV ファイルに含める必要があります。一部のフィールドは必須項目で、情報を入力する必要があります。また、オプションのフィールドもあります。

注：フィールドに情報を入力しない場合は、文字「-」を入力します。この文字は空のフィールドとしてデータベースにインポートされます。これはオプション フィールドに対してのみ行えます。「-」を必須フィールドに入力すると、インポート時にエラーが報告されます。N/A 値は使用しないでください。

フィールド名	説明
employeeID	必須（*SSO* の有効時のみ）ユーザの ID を入力します。

フィールド名	説明
displayName	オプション ユーザの表示名を入力します。
firstName	必須 ユーザの名を入力します。
lastName	必須 ユーザの姓を入力します。
email	必須 ユーザの電子メール アドレスを入力します。
userName	必須 ユーザのユーザ名を user@email.com の形式で入力します。
jobTitle	オプション ユーザの役職名または担当名を入力します。
address1	オプションユーザの住所の最初の行を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
address2	オプション ユーザの住所の 2 行目を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
city	オプションユーザの居住地の市町村を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
state	オプションユーザの居住地の都道府県を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
zipCode	オプションユーザの郵便番号を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
ISOcountry	オプション 居住する国の 2 文字の国コード（IN、US、CN など）を入力します。詳細については、http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm を参照してください。組織管理者は、このフィールドをユーザに必須となるように設定できます。
phoneBusinessISOCountry	オプションユーザの勤務先電話番号の国コード（IN、US、CN など）を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
phoneBusinessNumber	オプションユーザの勤務先電話番号を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
phoneMobileISOCountry	オプションユーザの携帯電話番号の国コード（IN、US、CN など）を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。

フィールド名	説明
phoneMobileNumber	オプション ユーザの携帯電話番号を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
fax	オプション ユーザのファクス番号を入力します。
policyGroupName	オプション ユーザが属しているデフォルトのポリシー グループを入力します。
userProfilePhotoURL	オプション ユーザのプロフィール写真にアクセスできる URL を入力します。
activeConnect	オプションユーザのステータスが Cisco WebEx で[アクティブ（active）]になっているかどうかを示します。[アクティブ（active）]ステータスであることを示すには[はい（Yes）]を、[非アクティブ（inactive）]ステータスであることを示すには [いいえ（No）] を入力します。
center	オプション Cisco Jabber アプリケーション ユーザのセンター アカウントを割り当てる（Yes）か、削除（No）する際に使用します。センターは 1 つのみ指定できます。
storageAllocated	オプションユーザに割り当てられたストレージをメガバイト単位で入力します。 数値を使用する必要があります。
CUCMClusterName	オプション ユーザが属している Cisco Unified Communications Manager クラスタの名前を入力します。
businessUnit	オプションユーザの部門または部署を入力します。組織管理者は、このフィールドをユーザに必須となるように設定できます。
IMLoggingEnable	オプション IM ロギングがこのユーザに対して有効にされているかどうかを示します。[有効（enabled）]であることを示すには [True] を、[無効（disabled）] であることを示すには [False] を入力します。
endpointName	オプション IM の記録用に設定されたエンドポイントの名前を入力します。
autoUpgradeSiteName	オプション アップグレード サイト名を入力します。

（注） タブ区切りまたはカンマ区切りの CSV ファイルを使用できます。CSV ファイルが、UTF-8 形式または UTF16-LE 形式で符号化されていることを確認します。

エンコード形式としての UTF-8 の選択

手順

ステップ 1 Microsoft Excel で [ファイル（File）]> [名前を付けて保存（Save As）] を選択します。

ステップ 2 [名前を付けて保存（Save As）]ダイアログボックスで、[ツールと Web オプション（Tools and Web Options）] を選択します。

ステップ 3 [Web オプション（Web Options）]ダイアログボックスで、[エンコーディング（Encoding）] タブを選択します。

ステップ 4 [このドキュメントの保存形式（Save this document as）]リストで、[UTF-8] を選択します。

ステップ 5 [OK]をクリックして [名前を付けて保存（Save As）] ダイアログボックスに戻ります。

ステップ 6 [ファイルの種類（Save as type）]リストから、[CSV（カンマ区切り）（*.csv）（CSV (Comma delimited) (*.csv)）] を選択します。

ステップ 7 [ファイル名（File Name）]フィールドに、CSV ファイルの名前を入力し、[保存（Save）] を選択します。

インポートに関する潜在的な問題を解決するための回避策

ユーザを CSV ファイル経由でインポートするときにエラーが発生する場合があります。これは、組織管理者が [国（Country）] フィールドを必須項目として設定した場合に発生します。この問題を回避するには、次のソリューションのいずれかに従ってください。

ソリューション 1：

手順

ステップ 1 [設定（Configuration）] タブ > [システム設定（System Settings）]> [ユーザ プロビジョニング（User Provisioning）].を選択します。

[ユーザ プロビジョニング（User Provisioning）]ウィンドウが開きます。

ステップ 2 [ユーザ プロファイルの必須フィールドの設定（Set Mandatory Fields for User Profile）]で、[国（Country）] フィールドをクリアします。

ステップ 3 CSV インポート プロセスを再度実行します。

ソリューション 2：

手順

ステップ 1 CSV ファイルを開き、[ISOCountry]というタイトルのフィールドを確認します。

ステップ 2 必要に応じて、各ユーザの ISO 国番号を入力します。

ステップ 3 CSV ファイルを保存します。

ステップ 4 CSV インポート プロセスを再度実行します。

ソリューション 3：

手順

ステップ 1 CSV ファイルを開き、[ISOCountry]というタイトルのフィールドを確認します。

ステップ 2 会社で使用しない場合、[ISOCountry]フィールドを削除します。

ステップ 3 CSV ファイルを保存します。

ステップ 4 CSV インポート プロセスを再度実行します。

第 12 章

ライブラリ管理

概要

ライブラリ（アプリケーション）管理アプリケーションを使用すると、ユーザは組織のアプリケーション（ウィジェットやテンプレート）を管理できます（ライブラリへのアプリケーションのアップロード、ライブラリ間でのアプリケーションの移動、アプリケーションの削除など）。

（注） Cisco WebEx Messenger のワークスペース機能はサポートが終了しており、もう提供されていません。

ユーザは権限を持つ任意のライブラリにアプリケーションをアップロードできます。さらに、ユーザはあるライブラリから別のライブラリにアプリケーションをコピーし、ライブラリからアプリケーションを削除することができます。アプリケーションをコピーするには、ライブラリに対する書き込み権限を持っている必要があります。ライブラリに対する書き込み権限を持っていないユーザは、組織管理者に通知を送信してアプリケーションをコピーできます。

Cisco WebEx Messenger 製品およびライブラリ管理ウィジェットの使用に関する詳細については、Cisco WebEx Messenger のヘルプを参照し、「ライブラリ管理」を検索してください。

アプリケーション管理

Cisco Jabber アプリケーションの通常ユーザと組織管理者は、ライブラリ管理ウィジェットを使用してアプリケーションを追加できます。通常ユーザは、それぞれの個人ライブラリでのみアプリケーションの追加や管理ができます。組織管理者は、パブリック ライブラリのアプリケーションも管理できます。

ユーザがライブラリに対する権限を持っていない場合は、組織管理者にリクエストを送信するかどうかを尋ねるエラー メッセージが表示されます。ユーザは [はい（Yes）]または [いいえ（No）] を選択できます。ユーザが [はい（Yes）]を選択すると、通知メールが組織管理者に送信されます。

組織管理者が Cisco WebEx Messenger にサインインして、ライブラリ管理ウィジェットを開くと、[承認待ち（Pending Approval）]の下にアプリケーションのリストが表示されます。組織管理者はウィジェットの上にマウスオーバーして詳細を確認し、そのリクエストを [承認（Approve）]または [拒否（Deny）]できます。アプリケーション追加リクエストの承認方法の詳細については、パブリック ライブラリへのアプリケーション追加依頼の承認, （151 ページ）を参照してください。

リクエストが承認されると、パブリック ライブラリに表示されます。リクエストが拒否されると、[承認保留中（Pending Approval）] リストから要求が削除され、ユーザに通知が送信されます。

（注） ライブラリへのアプリケーション（ウィジェット）の追加方法の詳細については、Cisco Jabber アプリケーションのヘルプを参照してください。

アプリケーションのライブラリへのコピー

これは、Cisco Jabber アプリケーションの一般的なユーザと組織管理者向けの情報です。

手順

ステップ 1 1つのライブラリから別のライブラリにアプリケーションをコピーするには、個人ライブラリまたはパブリック ライブラリでアプリケーションに移動します。

ステップ 2 アプリケーションのリストからアプリケーションを1つ選択し、[ウィジェットのコピー先（Copy widget to …）]を選択します。

ステップ 3 ドロップダウン リストから [パブリック（Public）]または [個人（Personal）] を選択して、[OK] を選択します。

パブリックライブラリへのアプリケーション追加依頼の承認

これは組織の管理者権限を持つユーザのみが行えます。組織管理者は、ユーザがパブリック ライブラリにウィジェット/テンプレートのコピーを要求するたびに、電子メールで通知されます。電子メールの件名は、[パブリック ライブラリへのアプリケーションのコピー依頼（Request to copy application to the Public Library）]などです。

手順

ステップ 1 MyWebEx にログインし、ライブラリ マネージャのウィジェットに移動します。
[承認保留中（Pending Approval）]リスト内のアプリケーションのリストが表示されます。

ステップ 2 ウィジェット（[追加アプリを取得（Get More Apps）] ポップアップと同様のポップアップ）にマウスオーバーして詳細を確認し、要求を [承認（Accept）]または [拒否（Deny）] します。
リクエストが承認されると、パブリック ライブラリに表示されます。リクエストが拒否されると、[承認保留中（Pending Approval）]リストから要求が削除され、ユーザに通知が送信されます。

ライブラリからのアプリケーションの削除

これは、Cisco Jabber アプリケーションの一般的なユーザと組織管理者向けの情報です。

手順

ステップ 1 個人ライブラリのアプリケーションに移動します（組織管理者ユーザの場合は個人およびパブリック）。

ステップ 2 アプリケーションのリストからアプリケーションを 1 つ選択し、[ウィジェットを削除（Remove The Widget…）]を選択します。

ステップ 3 ウィジェットの削除を確認するには、[OK]を選択します。
アプリケーションがユーザの個人ライブラリから削除され、ごみ箱に追加されます。

アプリケーションのライブラリへの復元

これは、Cisco Jabber アプリケーションのユーザと組織管理者向けの情報です。

手順

ステップ 1 [ごみ箱（Recycle Bin）]のリストに移動します。

ステップ 2 アプリケーションのリストからアプリケーションを1つ選択し、[復元（Restore）]を選択します。アプリケーションが最初に削除されたライブラリに復元され、[ごみ箱（Recycle Bin）]から削除されます。