ユニファイドメッセージングを設定する

Cisco Unity Connection を Microsoft Exchange 2019、2016、Office 365、Gmail サーバーと統合して、ユニファイドメッセージング機能を導入できます。

Exchange サーバーとの Unity Connection 通信の概要

Unity Connection と Exchange 間の通信を定義するユニファイド メッセージング サービスを追加する際に、Unity Connection が特定の Exchange サーバーと直接通信するか、または Unity Connection が Exchange サーバーを検索するかを選択できます。

ここでの選択により、Unity Connection がアクセスできる Exchange メールボックスが決まります。

- 特定の Exchange 2016 クライアント アクセス サーバーを選択すると、Unity Connection は Exchange 組織内のすべての Exchange 2016 メールボックスにアクセスできますが、Exchange 2019 メールボックスにはアクセスできません。
- 特定の Exchange 2019 クライアント アクセス サーバーを選択すると、Unity Connection は Exchange 組織内のすべての Exchange 2019 と Exchange 2016 のメールボックスにアクセスできます。
- Unity Connection に Exchange サーバーの検索を許可する場合、これらの Exchange サーバーに権限を付与する必要があります。 以下の項を参照して、適切な Exchange サーバーに権限を付与してください。

Exchange 2013、Exchange 2016 または Exchange 2019 の権限を与える （16 ページ）

（注） ユニファイド メッセージング サービスを追加するときに特定の Exchange サーバーを選択する場合、Unity Connection が Exchange 組織内のすべてのメールボックスにアクセスできるように、場合によっては複数のユニファイドメッセージングサービスを追加する必要があります。表 1 は、複数のユニファイド メッセージング サービスを追加する必要がある状況を示しています。

表 *1 : Exchange* のバージョンに基づいてユニファイド メッセージング サービスを追加する

Unity Connection がアクセスできるようにする **Exchange** のバージョン（メールボックス付き）			
Exchange 2016	Exchange 2019	Office 365	次のユニファイドメッセージングサービスを作成します
不可	不可	可	Unity Connection がアクセスできるようにする Office 365 サーバー用。
不可	可	可	• 1 つは Exchange 2019 用です。 • Unity Connection がアクセスできるようにする Office 365 サーバー用。
可	可	可	• 1 つは Exchange 2019 用です。このサービスは Exchange 2016 メールボックスにもアクセスできます。 • Unity Connection がアクセスできるようにする Office 365 サーバー用。

Unity Connection がアクセスできるようにする Exchange のバージョン（メールボックス付き）			
可	可	可	• 1 つは Exchange 2019 用です。このサービスは Exchange 2016 メールボックスにもアクセスできます。 • Unity Connection がアクセスできるようにする Office 365 サーバー用。
可	不可	可	• 1 つは Exchange 2016 用です。 • Unity Connection がアクセスできるようにする Office 365 サーバー用。
可	不可	不可	1 つは Exchange 2016 用です。
可	不可	可	• 1 つは Exchange 2016 用です。 • Unity Connection がアクセスできるようにする Office 365 サーバー用。
不可	不可	可	• Unity Connection がアクセスできるようにする Office 365 サーバー用。

- Unity Connection に Exchange サーバーの検索を許可する場合、Exchange のあるバージョンから別のバージョンにメールボックスを移動すると、Unity Connection は自動的にそれを検出し、Unity Connection のユーザー設定を自動的に更新します。
- 特定の Exchange サーバーを選択すると、メールボックスをある Exchange サーバーから別のサーバーに移動するときに、Unity Connection がそれを検出し、自動的に新しい場所の Exchange メールボックスにアクセスします。 Unity Connection が新しいメールボックスを

検出できない場合、ユニファイド メッセージング サービスまたはユニファイド メッセージング アカウントを手動で更新する必要があります。

- ユニファイド メッセージング サービスによりアクセスされるすべての *Exchange* メールボックスを移動した場合： 別の Exchange サーバーにアクセスするようにユニファイド メッセージング サービスを更新します。
- ユニファイド メッセージング サービスによりアクセスされる一部の *Exchange* メールボックスのみを移動した場合： ユニファイド メッセージング アカウント設定を更新して、新しい場所のメールボックスにアクセスするユニファイドメッセージング サービスを使用します。

表 2 は、Unity Connection が Exchange サーバー間でのメールボックスの移動を自動的に検出するタイミングを示しています。 Unity Connection がメールボックスの移動を検出できない場合に Unity Connection のユーザー設定を更新する方法については、「Exchange メールボックスを移動、復元する」の章を参照してください。

表 *2*: 特定の *Exchange* サーバーの選択：*Exchange* サーバー間でメールボックスを移動する際に、*Unity Connection* が検出された場合

特定の	**Unity Connection は、次の Exchange バージョン間でのメールボックスの移動を自動的に検出できます**				
	2016	**2019**	**2016 および 2016**	**2016 および 2019**	**2019 および 2019**
Exchange 2016 サーバー	可	不可	可	不可	不可
Exchange 2019 サーバー	可	可	可	可	可

Unity Connection が DNS を使用するように設定されていない場合、特定の Exchange サーバーを選択する必要があります。 このセクションで前述したように、組織内のすべての Exchange メールボックスへのアクセスが許可されない場合は、複数のユニファイドメッセージング サービスを作成する必要があります。

特定の Exchange サーバーを選択し、そのサーバーが機能を停止した場合、Unity Connection は Exchange メールボックスにアクセスできません。 Unity Connection による Exchange サーバーの検索を許可する場合、そして Unity Connection が現在通信している Exchange サーバーが機能を停止した場合、Unity Connection は別の Exchange サーバーを検索し、そのサーバーを通じてメールボックスにアクセスを開始します。

ユニファイドメッセージングと Google Workspace

Unity Connection 14 以降では、ユーザーの Gmail アカウントでメールやボイスメッセージにアクセスするための新しい方法をユーザーに提供します。 これにより、管理者はユニファイド

メッセージングを Google Workspace と統合できます。 Google Workspace を使用して、Unity Connection を設定して、Unity Connection と Gmail サーバー間でボイスメッセージを同期することができます。 ユーザーに送信されるすべての Unity Connection ボイスメッセージは、まず Unity Connection に保存された後、ユーザーの Gmail アカウントと同期されます。

ユニファイドメッセージングを設定するための前提条件

ユニファイドメッセージングを設定する前に、次の前提条件が満たされている必要があります。

1. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/requirements/b_14cucsysreqs.html にある「Cisco Unity Connection のシステム要件、リリース 14」の「ユニファイドメッセージング機能の使用の要件」のセクションをレビューしてください。

2. *Unity Connection* が *LDAP* ディレクトリと統合されている場合：Cisco Unity Connection 管理に移動して、以下を確認します。

   - **[システム設定（System Settings）]** を展開し、**[LDAP ディレクトリ設定（LDAP Directory Configuration）]** を選択します。 適切な LDAP ディレクトリ設定を選択します。 [LDAP ディレクトリ設定（LDAP Directory Configuration）]ページで、**[Cisco Unified Communications Manager ユーザーフィールド（Cisco Unified Communications Manager User Fields）]** の **[メール ID（Mail ID）]** フィールドが、**[LDAP 属性（LDAP Attribute）]** と同期されていることを確認します。

     これにより、**[LDAP メール（LDAP mail）]** フィールドの値が、インポートされた LDAP ユーザーの **[企業メールアドレス（Corporate Email Address）]** フィールドに表示されます。

   - **[ユーザー（Users）]** を展開し、**[ユーザー（Users）]** を選択します。 適切なユーザーを選択します。 [ユーザーの基本設定の編集（Edit User Basics）] ページで **[会社のメールアドレス（Corporate Email Address）]** を入力します。

   - ユーザーページで **[編集（Edit）]** を選択し、**[Unified メッセージアカウント（Unified Messaging Account）]** を選択します。 ユーザーの [ユニファイド メッセージング アカウント（Unified Messaging Account）] ページで、**[メールアドレス（Email Address）]** フィールドの値が指定されていることを確認してください。

ユニファイドメッセージングを設定するためのタスクリスト

Exchange 2013、Exchange 2016 または Exchange 2019 でユニファイドメッセージングを設定するためのタスクリスト

ステップ 1 ユニファイドメッセージングを設定する前に、前提条件を満たしていることを確認してください。「ユニファイドメッセージング設定の前提条件」の項を参照してください。

ステップ 2 ユニファイド メッセージ ユーザーが Exchange 2013、Exchange 2016、または Exchange 2019 と通信するための Active Directory アカウントを作成します。Active Directory でのユニファイド メッセージング サービス アカウントの作成と権限の付与については、Active Directory にユニファイドメッセージングを設定するの項を参照してください。

ステップ 3 Unity Connection がさまざまな Exchange 2013、Exchange 2016、または Exchange 2019 サーバーを検索して通信できるようにするのか、特定のサーバーのホスト名または IP アドレスがわかっている場合に特定の Exchange 2013、Exchange 2016、または Exchange 2019 サーバーと通信するようにするのかを決定します。次のステップを実行します。

a) Exchange 2013、Exchange 2016 または Exchange 2019 の権限を与える

b) （オプション） Exchange 2013、Exchange 2016、または Exchange 2019 認証と SSL 設定を確認する

（注） Unity Connection は、HTTP または HTTPS プロトコルのどちらを使用するかを決定し、関連するユニファイド メッセージング サービスで指定された設定に基づいて証明書を検証するかどうかを決定します。

ステップ 4 BAT Connection が DNS を使用するように設定されていない場合、次の CLI コマンドを使用して DNS を設定します。

- **set network dns**
- **set network dns options**

（注） Active Directory 環境が記録を公開しているのと同じ DNS 環境を使用するように Unity Connection を設定することをお勧めします。

CLI コマンドの詳細については、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html にある該当する『*Cisco Unified Communications Solutions* のコマンド ライン インターフェイス リファレンス ガイド』を参照してください。

ステップ 5 （選択した設定のみ）：次のいずれかまたは両方の条件では、Unity Connection と Exchange の間、および Unity Connection と Active Directory の間の通信を暗号化するために、Unity Connection サーバーに SSL 証明書をアップロードする必要があります。

- ステップ 3 b で HTTPS を使用するように Exchange を設定している場合、Exchange サーバーの証明書を検証するようにユニファイド メッセージング サービスを設定します。

- 異なる Exchange サーバーを検索して通信し、LDAPS を使用してドメインコントローラーと通信し、ドメインコントローラーの証明書を検証するように Unity Connection を設定した場合。

注意 Unity Connection が異なる Exchange サーバーを検索して通信することを許可すると、Unity Connection は、基本認証を使用して、Active Directory サーバーと通信します。 デフォルトでは、ユニファイドメッセージング サービス アカウントのユーザー名とパスワード、および Unity Connection サーバーと Active Directory サーバー間の他のすべての通信はクリアテキストで送信されます。 このデータを暗号化する場合は、ユニファイドメッセージング サービスがセキュア LDAP（LDAPS）プロトコルを使用して Active Directory ドメインコントローラと通信するように設定する必要があります。

詳細については、Exchange および Active Directory 用に CA 公開証明書をアップロードするの項を参照してください。

ステップ 6 Unity Connection で 1 つ以上のユニファイド メッセージング サービスを設定します。 詳細については、権限を付与するの項を参照してください。

ステップ 7 ユニファイド メッセージ ユーザーの設定を更新します。 詳細については、Unity Connection ユーザーで構成する設定の項を参照してください。

ステップ 8 1 つ以上のユニファイド メッセージ アカウントを設定して、Unity Connection ユーザーを通信先のメールサーバーとリンクします。 詳細については、ユーザーのユニファイド メッセージ アカウントの項を参照してください。

ステップ 9 ユニファイドメッセージングの設定をテストします。 詳細については、ユニファイドメッセージングの設定をテストするの項を参照してください。

Office365でユニファイドメッセージングを設定するためのタスクリスト

ステップ 1 ユニファイドメッセージングを設定する前に、前提条件を満たしていることを確認してください。 ユニファイドメッセージングを設定するための前提条件の項を参照してください。

ステップ 2 Unity Connection ユニファイド メッセージング ユーザーが Office 365 と通信するために使用する Active Directory アカウントを作成します。Active Directory でユニファイド メッセージング サービス アカウントを作成し、権限を付与する方法の詳細については、Active Directory にユニファイドメッセージングを設定するの項を参照してください。

ステップ 3 Unity Connection で Office 365 クライアント アクセス サーバーにログインするために使用する認証の種類を決定し、選択します。 これを実行するには、Cisco Unity Connection 管理で**ユニファイドメッセージング（Unified Messaging）>ユニファイド メッセージング サービス（Unified Messaging Services）**に移動し、**[新規追加（Add New）]**を選択します。 [新しいユニファイドメッセージング サービス（New Unified Messaging Service）] ページで、**[ウェブベース認証モード（Web-Based Authentication Mode）]** フィールドからいずれかを選択します。

- **ベーシック（Basic）**：デフォルトの認証モード。
- **NTLM**：NTLM 認証モードに切り替える前に、Office 365 サーバーで同じモードが設定されていることを確認してください。

- **Oauth2**：Oauth 2.0 ベースの認証モード。

（注） Microsoft により基本認証が廃止されました

Cisco Unity Connection は、Office 365 でユニファイドメッセージングを設定するための **OAuth2** 認証モードをサポートしています。OAuth2 ウェブ認証モードを使用するには、ユニファイドメッセージング サービスに対応するアプリケーションを Microsoft Azure ポータルに作成して登録する必要があります。 詳細については、ステップ 4 を参照してください。

既存のユニファイド メッセージング サービスについては、[ユニファイドメッセージングサービスの編集（Edit Unified Messaging Service）] ページで上記の設定を選択します。

ステップ 4 （*OAuth2* ウェブ認証モードにのみ該当）Azure ポータルでアプリケーションを登録するには、以下の手順を参照してください。

（注） Microsoft から入手できる最新の更新により、手順が変更される場合があります。

a) Azure ポータル管理者を使用して portal.azure.com の Azure ポータル グローバル エンド ポイントにサインインし、ユニファイド メッセージング サービス アカウントを作成します。 他の適用可能な Azure ポータルエンドポイントについては、https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-national-cloud のリンクで入手可能な Microsoft ドキュメントの**「アプリ登録エンドポイント」**の項を参照してください。

b) ポータルで、**[Azure Active Directory]** を選択します。 Azure Active Directory の新しいウィンドウが表示されます。

c) Azure Active Directory ウィンドウで、**[アプリの登録（App registrations）]** を選択し、新しいアプリケーションを作成するには **[新規登録（New registration）]** フィールドを選択します。 アプリケーションの登録に成功すると、ユニファイドメッセージングの設定に使用される **[アプリケーション（クライアント）ID（Application (Client) ID）]** および **[ディレクトリ ID（Directory ID）]** の値が取得できます。

d) **[証明書とシークレット（Certificates & secrets）]** を選択して、新しい **[クライアントシークレット（Client Secret）]** を作成します。これは、ユニファイドメッセージングの設定に使用されるクライアントシークレット値を提供します。

（注） 作成時にクライアントシークレットの値をコピーするようにしてください。コピーしない場合、アプリケーションについて新しいクライアントシークレットを作成する必要があります。

e) **APIPermissions**>**権限を追加（Add a persmission）**>**[自分の組織が使用する API（APIs my organization uses）]** を選択します。 検索バーに**「Office 365 Exchange Online」**と入力して、選択します。

f) （*14SU2* 以前のリリースが対象）**[代理権限（Delegated permissions）]** をクリックし、アプリケーションに以下の権限を追加します。

機能	権限（Permissions）
EWS	EWS.AccessAsUser.All
メール	Mail.Read Write、Mail.Send

カレンダーと連絡先にアクセスするには、アプリケーションに以下の権限を追加する必要があります。

機能	権限（Permissions）
カレンダー	Calendars.ReadWrite
連絡先	Contacts.ReadWrite

g) （*14SU3* 以降のリリースが対象）**[アプリケーションの権限（Application permissions）]** をクリックし、アプリケーションに **full_access_as_app** 権限を追加します。権限を制限するには、メールボックスへのアプリケーション権限を制限するためのタスクリスト（11 ページ） に記載されているステップを参照してください。

h) API パーミッションウィンドウで、**[Cisco Systems に管理者の同意を付与する（Grant admin consent for Cisco Systems）]** を選択して、リクエストされた権限について管理者の同意を与えます。

Azure ポータルでのアプリケーションの登録についての詳細は、https://docs.microsoft.com/en-us/graph/auth-register-app-v2 を参照してください。

ステップ 5 （*OAuth2* ウェブ認証モードにのみ適用可能） ステップ 4 で Azure ポータルから取得した以下のフィールドの値を入力します。

- **アプリケーション（クライアント） ID**
- **ディレクトリ ID**
- **クライアントシークレット**
- **AD 認証エンドポイント** デフォルト値は https://login.microsoftonline.com です。

（注） その他の適用可能な AD 認証エンドポイントについては、https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-national-cloud のリンクで入手可能な Microsoft ドキュメントの「**Azure AD 認証エンドポイント**」の項を参照してください。

- **リソース URI** デフォルト値は https://outlook.office365.com です。

（注） 以下に対してステップ 4 と 5 を繰り返します。

- 複数のクラスターの場合、上記のフィールドは各クラスター設定で一意である必要があります。
- Unity Connection で複数のユニファイド メッセージング サービスを設定する場合、各サービスに対して一意のクライアント ID を作成する必要があります。

ステップ 6 （*14SU2* 以前のリリースが対象）Office 365 サーバーで次のタスクを行い、自動検出機能を有効にします。これにより、Unity Connection が別の Office 365 サーバーを検索し、通信することができます。

a) リモート Exchange Management Power Shell を使用して Office 365 にアクセスする

b) （14SU2 以前のリリースに適用） Office 365 のアプリケーション偽装ロールを指定する

（注） Unity Connection は、HTTPS プロトコルを使用して、該当するユニファイド メッセージング サービスの設定に基づいて証明書を検証します。

ステップ 7 同期スレッドの設定は、Unity Connection と Office 365 サーバー間の遅延に基づいて行う必要があります。詳細については、以下にある『*Cisco Unity Connection* 設計ガイド、リリース *14*』の「Single Inbox」の章の「レイテンシー」の項を参照してください。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/design/guide/b_14cucdg.html

ステップ 8 次の CLI コマンドを実行して、DNS を設定します。

- **set network dns**
- **set network dns options**

（注） Active Directory 環境が記録を公開しているのと同じ DNS 環境を使用するように Unity Connection を設定することをお勧めします。

CLI コマンドの詳細については、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html にある該当する『*Cisco Unified Communications Solutions* のコマンド ライン インターフェイス リファレンス ガイド』を参照してください。

ステップ 9 （選択した設定のみ）：Unity Connection サーバーに SSL 証明書をアップロードして、Unity Connection と Office 365 間の通信を暗号化します。証明書をアップロードすることで次のことが可能になります。

- Exchange サーバーの証明書を確認します。 これを行うには、Unity Connection 管理の **[Exchange サーバーの証明書を確認する（Validate Certificates for Exchange Servers）]** チェックボックスをオンにします。
- Unity Office 365 サーバーを検索して通信するための接続を設定している場合は通信を保護してください。

詳細については、パブリック証明書を Unity Connection サーバーにアップロードする、および Office 365 および Cisco Unity Connection の証明書をアップロードするを参照してください

ステップ 10 **[ユニファイド メッセージング サービス（Unified Messaging Service）]** を作成し、そのサービスアカウントですべてのユーザーを設定します。

（注） Unity Connection サーバーがボイスメールサービスのテナントによって共有されている場合、複数の **[ユニファイド メッセージング サービス（Unified Messaging Service）]** アカウントが必要です。

ステップ 11 ユニファイド メッセージ ユーザーの設定を更新します。 詳細については、Unity Connection ユーザーで構成する設定の項を参照してください。

ステップ 12 次の CLI コマンドを実行して、ストリーミングスレッドごとに集計されるユーザー数と、メールボックス同期の 1 時間ごとの定期的な完全再同期フラグを設定します。

a) 既存のユーザー数を確認します。

```
run cuc dbquery unitydirdb select fullname,name,value from vw_Configuration where name like
'MbxSynchUserCountPerStreamingSubscription'
```

[value] パラメータが 5000 の場合、設定がすでに有効になっていることを意味します。 値が 5000 ではない場合、次の CLI コマンドを実行してユーザー数を設定します。

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyLong(pFullName='System.Messaging.MbxSynch.MbxSynchUserCountPerStreamingSubscription',pvalue=5000)
```

b) メールボックス同期の 1 時間ごとの定期的な完全再同期フラグの既存の設定を確認します。

```
run cuc dbquery unitydirdb select fullname,name,value from vw_Configuration where name like
'MbxSynchBackgroundSyncEnable'
```

[value] パラメータが 0 の場合、設定がすでに有効になっていることを意味します。値が 0 でない場合、以下の CLI コマンドを実行してフラグを設定します。

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyBool(pFullName='System.Messaging.MbxSynch.MbxSynchBackgroundSyncEnable',pvalue=0)
```

c) 上記の CLI の変更を有効にするには、**Connection Mailbox Sync** サービスを再起動する必要があります。

（注） クラスタの場合、パブリッシャサーバーでのみコマンドを実行し、その後、データベースのレプリケーションが正常に機能していることを確認します。

ステップ 13 ユニファイドメッセージング サービスをテストします。 詳細については、ユニファイドメッセージングの設定をテストするを参照してください。

メールボックスへのアプリケーション権限を制限するためのタスクリスト

ステップ 1 **メールが有効なセキュリティグループ**を作成します。 これは、メッセージを配信したり、Active Directory 内のリソースへのアクセス許可を付与するために使用できます。 https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-mail-enabled-security-groups#use-the-exchange-admin-center-to-manage-a-mail-enabled-security-group にあるステップを参照してください。

ステップ 2 昇格した Powershell で **Exchange Online 管理モジュール**をインストールします。 https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2?view=exchange-ps#install-and-maintain-the-exchange-online-powershell-module にあるステップを参照してください。

ステップ 3 **Exchange Online の PowerShell** に接続します。 https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps にあるステップを参照してください。

ステップ 4 **New-ApplicationAccessPolicy** コマンドレットを実行します。 New-ApplicationPolicy を実行する場合、**OrganizationConfiguration** のロールが必要です。 次のコマンドを使用して、現在のロールを確認できます。

```
Get-ManagementRole -Cmdlet <Cmdlet>
```

以下のステップを実行して、OrganizationConfiguration ロールを管理者ユーザーに割り当てます。

a) https://admin.exchange.microsoft.com/ にある Exchange 管理センターにログインします。
b) **[ロール - 管理者ロール（Roles - Admin Roles）]** を選択します。
c) ユーザーに対して、**[Organization Management]** のロールを選択します。
d) Power Shell を再起動して、新しいロールの割り当てが有効になっていることを確認します

ステップ 5 **New-ApplicationAccessPolicy** のコマンドレットを次のコマンドで実行します。

```
New-ApplicationAccessPolicy -AppId "**" -PolicyScopeGroupId "**" -AccessRight RestrictAccess
-Description "Restrict this app to members."
```

（注） AppId はアクセスを制限するアプリケーションのアプリケーション ID です。 これは、アプリケーションの Azure Active Directory ポータルに記載されているクライアント ID になります。 複数のアプリ ID をコンマで区切って指定することもできます。 PolicyScopeGroupId はグループを識別するための ID です。 **ステップ 1** で言及したメールが有効なセキュリティグループになります。

（注） Microsoft から入手できる最新の更新により、手順が変更される場合があります。

Google Workspace でユニファイドメッセージングを設定するためのタスクリスト

Gmail API はサーバープッシュ通知を提供します。この通知を通じて、ユーザーは Gmail サーバー上のユーザーのメールボックスの変更を確認できます。 ユーザーのメールボックスに変更があるたびに、Gmail API は Unity Connection に通知を送信します。

ステップ 1 ユニファイドメッセージングを設定する前に、前提条件を満たしていることを確認してください。 ユニファイドメッセージングを設定するための前提条件の項を参照してください。

Google Workspace でユニファイドメッセージングを設定する前に、Google Workspace でアカウントを作成するためのドメインが必要です。

ステップ 2 Google Workspace に移動し、「管理コンソール」でドメイン名を使用してアカウントを作成してください。詳細なステップについては、https://workspace.google.com/signup/businessstarter/welcome?hl=en-IN を参照してください。

ステップ 3 「Google Cloud Platform（GCP）コンソール」に移動し、ステップ 2 で作成した管理者アカウントで Google Cloud コンソールにログインして、新しいプロジェクトを作成します。

プロジェクトは、サービスアカウントの作成に使用されるドメインを指定します。

ステップ 4 Google Cloud Platform で新規プロジェクトを作成するには、組織ドメインのドロップダウンメニューから **[新規プロジェクト（NEW PROJECT）]** オプションを選択し、必要な情報を入力してから **[作成（CREATE）]** を選択します。

ステップ 5 プロジェクトを作成したら、組織ドメインのドロップダウンメニューからプロジェクトを選択します。

ステップ 6 プロジェクトのホームページで、メニュー（Menu）> IAM & Admin > サービスアカウント（Service accounts）>サービスアカウントの作成（Create service account）に移動します。

ステップ 7 [サービスアカウントの作成（Create Service Account）] ページで必要な情報を入力し、**[作成して続行（CREATE AND CONTINUE）]** を選択します。

ステップ 8 サービスアカウントにすべての権限を与えるには、**[このサービスアカウントにプロジェクトへのアクセス権を付与する（Grant this sevice account access to project）]** フィールドの下の **[ロール（Role）]** のドロップダウンメニューから **[所有者（Owner）]** のロールを選択します。

ステップ 9 [DONE] を選択します。

新しいページが開き、プロジェクトの下に作成されたすべてのサービスアカウントが表示されます。

ステップ 10 ステップ 7 で作成したサービスアカウントを選択します。

ステップ 11 サービスアカウントページで、**[詳細（DETAILS）]**タブに移動して、**[ドメイン全体の委任を表示（HOW DOMAIN-WIDE DELEGATION）]** フィールドを選択し、**[Google Workspace ドメイン全体の委任を有効にする（Enable Google Workspace Domain-wide Delegation）]** チェックボックスを選択すると、サービスアカウントに Google Workspace ドメイン上のすべてのユーザーデータへのアクセスを許可することができます。

ステップ 12 [SAVE] を選択します。

ステップ 13 サービスアカウントページで、**[キー（KEYS）]** タブに移動し、**キーの追加（ADD KEY）** > **新しいキー（Create new key）**を選択します。

[キータイプ（Key type）] フィールドで JSON オプションを選択していることを確認します。

アカウントが正常に作成されると、.JSON形式のキーファイルがシステムにダウンロードされます。キーファイルは、Google Workspace とのユニファイドメッセージングの設定に使用されます。

ステップ 14 **メニュー（Menu）** > **API &サービス（API & Services）** > **ライブラリ（Library）**に移動し、Gmail API を検索して有効にします。

同様に、Cloud Pub/Sub API を検索して有効にします。

ステップ 15 ドメイン全体の権限をサービスアカウントに委任するには、メニュー（Menu）> IAM & Admin > サービスアカウント（Service accounts）に移動して、作成したサービスアカウントに対応する**[クライアント ID を表示（View Client ID）]** を選択して、クライアント ID をコピーします。

ステップ 16 [管理者コンソール（Admin Console）] にログインし、メニュー（Menu）>セキュリティ（Security）> API コントロール（API controls）に移動します。

ステップ 17 [API コントロール（API controls）] ページで、[ドメイン全体の委任（Domain-wide Delegation）] を選択し、[新規追加（Add new）] を選択します。

ステップ 18 クライアント ID を入力するための新しいウィンドウが表示されます。

ステップ 19 [新しいクライアント ID の追加（Add a new client ID）] ウィンドウで、ステップ 15 でコピーしたクライアント ID を入力し、OAuth 範囲を指定して、[認証（AUTHORIZE）] を選択します。

必要な範囲：

https://mail.google.com、

https://www.googleapis.com/auth/gmail.labels、

https://www.googleapis.com/auth/gmail.modify、

https://www.googleapis.com/auth/cloud-platform、

https://www.googleapis.com/auth/pubsub

ステップ 20 Admin Console の **[ユーザー（Users）]** アプリケーションを使用して作成します。

ステップ 21 Cisco Unity Connection 管理にログインし、**ユニファイドメッセージング（Unified Messaging）**>**ユニファイド メッセージング サービス（Unified Messaging Services）**に移動し、**[新規追加（Add New）]** を選択します。

ステップ 22 [新しいユニファイド メッセージング サービス（New Unified Messaging Service）] ページで、[新しいユニファイド メッセージング サービス（New Unified Messaging Service）] で [Google Workspace] を選択します。

ステップ 23 Google Workspace でのユニファイドメッセージングの機能を有効にするには、**[有効（Enabled）]** チェックボックスを選択します。

デフォルトでは、このチェックボックスはオンになっています。

ステップ 24 Google Workspace 証明書の検証を有効にするには、**[Google Workspace の証明書の確認（Validate Certificates for Google Workspace）]** チェックボックスをオンにします。

このチェックボックスは、デフォルトでオフになっています。

ステップ 25 新しいユニファイド メッセージング サービスの表示名を入力します。

ステップ 26 必要に応じて、プロキシサーバーの **[プロキシサーバー（アドレス：ポート）（Proxy Server (Address:Port)）** フィールドを入力します。

ステップ 27 **[プロキシサーバーの認証を有効にする（Enable Proxy Server Authentication）]** チェックボックスを選択してプロキシサーバーベースの認証を有効にし、プロキシサーバー用の **[ユーザー名（Username）]** および **[パスワード（Password）]** を指定します。

ステップ 28 **[Google Workspace サービス アカウント キー ファイル（Google Workspace Service Account Key File）]** で、ステップ 13 で作成したキーファイルをアップロードします。

ファイルは .json 形式でアップロードし、そのサイズは 1MB 未満でなければなりません。

ステップ 29 [保存（Save）] を選択します。

ステップ 30 ユニファイド メッセージ ユーザーの設定を更新します。 詳細については、Unity Connection ユーザーで構成する設定の項を参照してください。

ステップ 31 1 つ以上のユニファイドメッセージアカウントを設定して、Unity Connection ユーザーを通信先のメールサーバーとリンクします。 詳細については、ユーザーのユニファイドメッセージアカウントの項を参照してください。

ユニファイドメッセージングを設定するためのタスク

Active Directory にユニファイドメッセージングを設定する

Unity Connection は、ユニファイド メッセージング サービス アカウントと呼ばれる Active Directory アカウントを使用して、Exchange または Office 365 のメールボックスにアクセスします。 アカウントを作成したら、Unity Connection がユーザーの代理として操作を実行するために必要な権限をアカウントに付与します。

Office 365 の場合、Exchange 2019、Exchange 2016、および Exchange 2013 の操作は Exchange ウェブサービス（EWS）を通じて実行されます。 Exchange メールボックスにメッセージをアップロードする

- Exchange でメッセージの変更を追跡する
- Unity Connection で加えた変更でメッセージを更新する
- Exchange のメッセージを Unity Connection で削除されたときに削除する、などの処理を行います。

Unity Connection が通信する Exchange サーバーを含む Active Directory フォレストに 1 つ以上のドメイン ユーザー アカウントを作成する必要があります。

Active Directory でユニファイドメッセージングを設定する際には、以下の点に注意してください。

- アカウントに、Unity Connection のユニファイドメッセージング サービス アカウントであることを示す名前を付けます。
- ドメインユーザーアカウントのメールボックスを作成しないでください。このアカウントのメールボックスを作成すると、ユニファイドメッセージングは適切に機能しなくなります。
- このアカウントを管理者グループに追加しないでください。
- アカウントを無効にしないでください。無効にした場合、Connection はこのアカウントを使用して Exchange または Office 365 のメールボックスにアクセスできません。
- 会社のパスワードセキュリティ要件を満たすパスワードを指定してください。

（注） パスワードは AES 128 ビット暗号化で暗号化され、Unity Connection データベースに保存されます。パスワードの暗号化に使用されるキーにはルートアクセスのみがアクセス可能であり、ルートアクセスは Cisco TAC の支援がある場合にのみ利用可能です。

- クラスタのユニファイドメッセージングを設定している場合、Unity Connection は両方の Unity Connection サーバーに対して同じユニファイドメッセージング サービス アカウントを自動的に使用します。
- サイト間ネットワークまたはサイト内ネットワークのユニファイドメッセージングを構成する場合、複数の Unity Connection サーバーに同じユニファイドメッセージング サービス アカウントを使用できます。ただし、これは必須の機能ではなく、機能やパフォーマンスに影響を与えるものではありません。

権限を付与する

Exchange 2013、Exchange 2016 または Exchange 2019 の権限を与える

ステップ 1 Enterprise Admins グループのメンバーであるアカウント、または設定コンテナ内の Exchange オブジェクトに対する権限を付与できるアカウントのいずれかを使用して、Exchange Management Shell がインストールされているサーバーにログインします。

ステップ 2 Exchange Management Shell で次のコマンドを実行して、アプリケーション偽装管理の役割を Exchange 2013、Exchange 2016 または Exchange 2019 のユニファイドメッセージング サービス アカウントに割り当てます。

New-ManagementRoleAssignment -Name: <RoleName> **-Role:ApplicationImpersonation -User:'** <Account>、ここで

- *RoleName* は割り当てに付ける名前です。たとえば、SSL ConnectionUMServicesAcct です。 *RoleName* に入力する名前は、get-ManagementRoleAssignment を実行するときに表示されます。
- *Account* は、domain\alias 形式のユニファイド メッセージング サービス アカウントの名前です。

複数のユニファイド メッセージング サービス アカウントを作成した場合は、残りのアカウントに対してステップ 2 を繰り返します。 各ユニファイド メッセージング サービス アカウントの *RoleName* に異なる値を指定します。

（注） Exchange 2013、Exchange 2016 または Exchange 2019 のユニファイド メッセージング サービス アカウントを設定する場合、アプリケーションの偽装管理役割をユニファイドメッセージング サービス アカウントに割り当てる必要があります。

認証と SSL 設定を確認する

ユニファイドメッセージング用の Unity Connection によってアクセスされる Exchange サーバーを選択した後、Exchange サーバーが希望の認証モード（ベーシック、ダイジェスト、または NTLM）およびウェブベースのプロトコル（HTTPS または HTTP）を使用するように設定されていることを確認します。

Unity Connection は、ユニファイドメッセージングの設定のために NTLM 認証モードを選択した場合、NTLMv2 ベースの認証をサポートします。

Exchange サーバーで認証モードとウェブベースプロトコルを設定したら、1 つ以上の Unity Connection ユニファイド メッセージング サービスを作成します。 サーバーで指定したものと同じ認証モードとウェブベースプロトコルを選択します。

Exchange 2013、Exchange 2016、または Exchange 2019 認証と SSL 設定を確認する

ステップ 1 Exchange 2013、Exchange 2016 または Exchange 2019 のクライアント アクセス サーバーへのログインに使用する Unity Connection 認証（**[ベーシック（Basic）]** または **[NTLM]**）のタイプを決定します。 同じタイ

プの認証を使用するには、すべての Exchange 2013、Exchange 2016、または Exchange 2019 クライアント アクセス サーバーを設定する必要があります。

ステップ 2 Unity Connection と Exchange 2013、Exchange 2016、または Exchange 2019 クライアント アクセス サーバー間の通信を SSL 暗号化するかどうかを決定します。 その場合、すべての Exchange 2013、Exchange 2016、または Exchange 2019 クライアント アクセス サーバーで同じ SSL 設定を指定する必要があります。

ステップ 3 Unity Connection でアクセスされるのと同じ Exchange 2013 クライアントサーバーにアクセスできるサーバーにサインインします。 ローカル管理者グループのメンバーであるアカウントを使用します。

ステップ 4 Windows の [スタート（Start）] メニューから、**プログラム（Programs）** > **管理ツール（Administrative Tools）** > **インターネット インフォメーション サービス（IIS）マネージャ（Internet Information Services (IIS) Manager）**を選択します。

ステップ 5 設定を確認する最初の Exchange 2013、Exchange 2016、または Exchange 2019 クライアント アクセス サーバーに対して、左ペインで<servername> >**サイト（Sites）**>**デフォルトのウェブサイト（Default Website）**を展開します。 EWS と自動検出の両方の認証設定を確認する必要があります。

ステップ 6 **[デフォルトのウェブサイト（Default Website）]** で **[Autodiscover]** を選択します。

a) 中央のペインの **[IIS]** セクションで、**[認証（Authentication）]** をダブルクリックします。

ユニファイド メッセージング サービス アカウントが Exchange クライアント アクセス サーバーへのログインに使用する認証の種類が、[ステータス（Status）] 列で **[有効（Enabled）]** になっていることを確認します。

ユニファイド メッセージング サービス アカウントを作成するとき、Unity Connection が同じタイプの認証を使用するように設定します。 Unity Connection は次のタイプの認証のみをサポートします。

- **基本**
- **NTLM**

b) 設定を変更した場合は、右ペインから **[適用（Apply）]** を選択します。

c) 左ペインから再度 **[Autodiscover]** を選択します。

d) 中央のペインで、**[SSL 設定（SSL Settings）]** をダブルクリックします。

e) [SSL 設定（SSL Settings）] ページで、**[SSL を必要とする（Require SSL）]** チェックボックスがオンの場合、

- Unity Connection でユニファイド メッセージング サービスを作成する際、ウェブベースプロトコルに HTTPS を選択する必要があります。
- Exchange サーバーから SSL 証明書をダウンロードし、Unity Connection サーバーにインストールする必要があります。

f) 設定を変更した場合は、右ペインから **[適用（Apply）]** を選択します。

ステップ 7 **[デフォルトのウェブサイト（Default Website）]** で **[EWS]** を選択します。

a) 中央のペインの [IIS] セクションで、**[認証（Authentication）]** をダブルクリックします。

ユニファイド メッセージング サービス アカウントが Exchange メールボックスへのサインインに使用する認証のタイプについて、**[ステータス（Status）]** 列に **[有効（Enabled）]** と表示されていることを確認します。 ユニファイド メッセージング サービス アカウントを作成するとき、Unity Connection が同じタイプの認証を使用するように設定します。

注意 ユニファイドメッセージングサービスアカウントは、自動検出で指定したものと同じタイプの EWS 認証を使用する必要があります。

b) 設定を変更した場合は、右ペインから **[適用（Apply）]** を選択します。
c) 左ペインから再度 **[EWS]** を選択します。
d) 中央のペインで、**[SSL 設定（SSL Settings）]** をダブルクリックします。
e) **[SSL を必要とする（Require SSL）]** チェックボックスがオンの場合、

- Unity Connection でユニファイド メッセージング サービスを作成する際、ウェブベースプロトコルに HTTPS を選択する必要があります。
- Exchange サーバーから SSL 証明書をダウンロードし、Unity Connection サーバーにインストールする必要があります。

注意 ユニファイドメッセージング サービス アカウントは、ステップ e で自動検出用に指定したのと同じ EWS の SSL 設定を使用する必要があります。

f) 設定を変更した場合は、右ペインから **[適用（Apply）]** を選択します。

ステップ 8 Unity Connection がアクセスできるその他の Exchange 2013、Exchange 2016、または Exchange 2019 クライアント アクセス サーバーについては、ステップ 5 からステップ 6 を繰り返します。

ステップ 9 **[IIS マネージャ（IIS Manager）]** を閉じます。

Exchange 2013、Exchange 2016 または Exchange 2019 の Unity 接続のページ表示機能を設定する

ユニファイドユーザーの Exchange メールボックスに、ボイスメールや受信確認を含む 1000 件を超えるメッセージがある場合は、Unity Connection サーバーで EWS ページ ビュー検索機能を有効にします。

メッセージのページビュー機能を有効にするには、[System.Messaging.MbxSynch.MbxSynchUsePaging] パラメーターの値を 1 に設定する必要があります。

ページビュー機能を設定するには、次の操作を行います。

ステップ 1 次の CLI コマンドを入力します。

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModifyBool(pFullName='System.Messaging.MbxSynch.MbxSynchUsePaging',pvalue=1)
```

（注） Unity Connection クラスタが設定されている場合、パブリッシャまたはサブスクライバサーバーでコマンドを実行できます。

ステップ 2 Unity ページビュー検索機能を使用した接続で管理できるボイスメールアイテムの最大数を設定するには、次の CLI コマンドを実行します。

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModify(pFullName='System.Messaging.MbxSynch.MbxSynchVoiceMailCountLimit',pvalue="newvalue")
```

新しい値は、ページングパラメーターが有効になった後に表示できるボイスメールカウント制限の値を指定します。 Unity Connection はデフォルトでメールボックスごとに最初の 25000 件のボイスメールを管理します。これにより、Unity Connection と Exchange サーバー間のメッセージ同期の遅延を回避できます。 このボイスメール数の制限は、最大 75000 まで増やすことができます。

（注） 既定では、[System.Messaging.MbxSynch.MbxSynchUsePaging] パラメーターの値は 1 に設定されています。

リモート Exchange Management Power Shell を使用して Office 365 にアクセスする

ステップ 1 管理者として Windows PowerShell を実行し、次のコマンドを実行します。

Set-ExecutionPolicy Unrestricted

ステップ 2 Windows PowerShell エンドポイントで、次のコマンドを実行し、認証用の Office 365 管理者アカウント資格情報をポップアップウィンドウに入力します。

$LiveCred = Get-Credential

ステップ 3 Office 365 とのリモート Windows PowerShell セッションを確立するには、New-PSSession Windows PowerShell コマンドレットを使用して、http://ps.outlook.com/powershell で汎用のリモート Windows PowerShell エンドポイントに接続します。 次のコマンドを実行してリモート Exchange シェルセッションを作成します。

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell/ -Credential $LiveCred -Authentication Basic -AllowRedirection

（注） Office 365 Exchange Online への接続に使用するユーザーアカウントはリモートシェルに対して有効になっている必要があります。

ステップ 4 次のコマンドを実行して、すべてのリモート Exchange Shell コマンドをローカルのクライアント側セッションにインポートします。

Import-PSSession $Session

エラーメッセージが表示されて失敗する場合は、実行ポリシーを設定して、リモート PowerShell スクリプトの実行を許可する必要があります。Get-ExecutionPolicy を実行します。 返された値が RemoteSigned 以外のものであった場合、値を RemoteSigned running Set-ExecutionPolicy RemoteSigned に変更する必要があります。

http://technet.microsoft.com/en-us/library/jj984289%28v=exchg.150%29.aspx

Import-PSSession を使用するために、現在のセッションの実行ポリシーを [制限（Restricted）] または [すべて署名（All signed）] にすることはできません。これは、Import-PSSession が作成する一時モジュールに、これらのポリシーで禁止されている署名されていないスクリプトファイルが含まれているためです。 ロー

カルコンピューターの実行ポリシーを変更せずに Import-PSSession を使用するには、Set-ExecutionPolicy の Scope パラメーターを使用して、単一のプロセスに対して制限の少ない実行ポリシーを設定します。

http://community.office365.com/en-us/forums/158/t/71614.aspx.

（*14SU2* 以前のリリースに適用） Office 365 のアプリケーション偽装ロールを指定する

ステップ 1 Office 365 で偽装許可を設定するには、Windows PowerShell スクリプトを実行する必要があります。

ステップ 2 New-ManagementRoleAssignment コマンドレットを実行するには、権限が必要です。 デフォルトでは、管理者はこの権限を持っています。

「New-ManagementRoleAssignment」Exchange Management Shell コマンドレットを使用して、サービスアカウントに組織内のすべてのユーザーを偽装するための権限を付与します。

new-ManagementRoleAssignment -<*Name*>**:RoleName -**<*Role*>**:ApplicationImpersonation -**<*User*>**:Account**

引数の説明

- *Name* パラメータには、ConnectionUMServicesAcct など、新しいロール割り当ての名前を指定します。 RoleName に入力する名前は、get-ManagementRoleAssignment を実行するときに表示されます。
- *Role* パラメータは、ApplicationImpersonation が *User* パラメータに指定されたユーザーに割り当てられていることを示します
- *User* は、alias@domain 形式のユニファイド メッセージング サービス アカウントの名前です。

例

New-ManagementRoleAssignment –Name "ConnectionUMServicesAcct" –Role "ApplicationImpersonation" –User serviceaccount@example.onmicrosoft.com

注意 Active Directory 同期機能を有効にして、ローカル Exchange サーバーから Office 365 に移行する場合、以降のユーザー管理はオンプレミスの Active Directory Services を通じて実行され、Office 365 と自動的に同期されます。 アプリケーション偽装管理の役割が Office 365 サーバーに付与されていることを確認する必要があります。

メールサーバーにアクセスするためのユニファイド メッセージング サービスを作成する

以下の手順を実行して、サポートされているメールサーバーにアクセスするための Unity Connection で 1 つ以上のユニファイド メッセージング サービスを作成します。

（注） サポート対象のメールサーバーが HTTPS を使用するように設定した場合、ユニファイド メッセージング サービスを設定してメールサーバーの証明書を検証する必要があります。 Tomcat-trust と Unity Connection-trust の両方のロケーションに、メールサーバー用の SSL 証明書を発行した認証局から証明書をアップロードする必要があります。 SSL 証明書のアップロードについては、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/security/guide/b_14cucsecx.html にある『*Cisco Unity Connection* セキュリティガイド リリース *14*』の「SSL を使ってクライアント/サーバー接続を保護する」の章を参照してください。

Unity Connection にユニファイド メッセージング サービスを作成する

Unity Connection が個別のメールサーバーと通信するように設定している場合、各メールサーバーに対してユニファイド メッセージング サービスを設定する必要があります。

ステップ 1 Cisco Unity Connection 管理で、**[ユニファイドメッセージング（Unified Messaging）]** を開き、**[ユニファイド メッセージング サービス（Unified Messaging Services）]** を選択します。

ステップ 2 [ユニファイドメッセージングサービスの検索（Search Unified Messaging Services）] ページで、**[新規追加（Add New）]** を選択して新しいユニファイド メッセージング サービスを作成します。 作成済みのユニファイド メッセージング サービスを選択して、その設定を変更することもできます。 [新しいユニファイド メッセージング サービス（New Unified Messaging Services）] ページまたは [ユニファイド メッセージング サービスの編集（Edit Unified Messaging services）] ページが表示されます。

ステップ 3 ユニファイド メッセージング サービスを設定するために必須のフィールドの値を入力し、**[保存（Save）]** を選択します（各フィールドの詳細は、選択したメールサーバーに応じて、 **ヘルプ（Help）>このページ（This Page）**を参照してください）。

Unity Connection が個別のメールサーバーと通信するように設定している場合、各メールサーバーに対してユニファイド メッセージング サービスを設定する必要があります。

Exchange および Active Directory 用に CA 公開証明書をアップロードする

ユニファイド メッセージング サービスを作成するときに、Exchange サーバーまたは Active Directory ドメインコントローラー（DC）の証明書を検証することを選択した場合は、Exchange サーバーと DC の証明書に署名した認証局（CA）からパブリック証明書をアップロードする必要があります。

パブリック証明書により、Unity Connection が Exchange サーバーまたは DC と通信し、ユニファイドメッセージングが適切に機能することを許可します。

1. *Exchange* サーバーの証明書を検証するオプションを選択し、かつ *SSL* 証明書が次のすべてのサーバーにインストールされていない場合：

- Exchange 2019、Exchange 2016 または Exchange 2013 クライアントのアクセスサーバーの証明書を取得してインストールします。

さらに、Active Directory ドメインコントローラーの証明書を検証するオプションを選択し、さらに SSL 証明書が DC にインストールされていない場合、証明書を取得してインストールします。

2. 外部 *CA*（*Verisign* など）を使用して、リストされているサーバーにインストールされた *SSL* 証明書を発行した場合、および *.pem* 形式の *CA* のパブリック証明書がある場合：ファイルを Unity Connection サーバーがアクセスできるネットワーク上の場所に保存します。その後、タスク 6 に進みます。
3. *Microsoft* 証明書サービスまたは *Active Directory* 証明書サービスを使用して *SSL* 証明書を発行した場合、または外部 *CA* を使用し、*.pem* 形式の *CA* の公開証明書を持っていない場合：OpenSSL またはパブリック証明書を .pem 形式に変換できる他のアプリケーションをダウンロードしてインストールします。 Unity Connection は他の形式のパブリック証明書をアップロードできません。
4. *Microsoft* 証明書サービスを使用して *SSL* 証明書を発行した場合：Microsoft 証明書サービスまたは Active Directory 証明書サービスの公開証明書をファイルに保存するの項を実行します。
5. *Microsoft* 証明書サービス、*Active Directory* 証明書サービス、または外部 *CA* を使用し、*.pem* 形式の公開証明書がない場合：ダウンロードしたアプリケーションを使用して、公開証明書を .pem 形式に変換し、Unity Connection サーバーがアクセスできるネットワーク上の場所にファイルを保存します。
6. パブリック証明書を Unity Connection サーバーにアップロードします。 詳細については、パブリック証明書を Unity Connection サーバーにアップロードする、および Office 365 および Cisco Unity Connection の証明書をアップロードするを参照してください

Microsoft 証明書サービスまたは Active Directory 証明書サービスの公開証明書をファイルに保存する

ステップ 1 Microsoft 証明書サービスをインストールし、次のサーバー用に SSL 証明書を発行したサーバーにログインします。

- Exchange 2019、Exchange 2016 または Exchange 2013 クライアントのアクセスサーバーの証明書を取得してインストールします。
- Unity Connection サーバーがアクセスする可能性がある Active Directory ドメインコントローラ。

ステップ 2 Windows の [スタート（Start）] メニューから、**プログラム（Programs）** > **管理ツール（Administrative Tools）** > **証明機関（Certification Authority）**を選択します。

ステップ 3 **[認証局 MMC（Certification Authority MMC）]** の左ペインで、サーバー名を右クリックし、**[プロパティ（Properties）]** を選択します。

ステップ 4 <*servername*> **プロパティ（Properties）**ダイアログボックスの [全般（General）] タブで、**[証明書の表示（View Certificate）]** を選択します。

ステップ 5 **[証明書（Certificate）]** ダイアログボックスで、**[詳細（Details）]** タブをクリックします。

ステップ 6 **[詳細（Details）]** タブで、**[ファイルにコピー（Copy to File）]** を選択します。

ステップ 7 [証明書のエクスポート ウィザードへようこそ（Welcome to the Certificate Export Wizard）] ページで、**[次へ（Next）]** を選択します。

ステップ 8 [エクスポートファイルの形式（Export File Format）] ページで、**[次へ（Next）]** を選択して、**[DER エンコードバイナリ X.509（.CER）（DER Encoded Binary X.509 (.CER)）]** のデフォルト値を受け入れます。

ステップ 9 [エクスポートするファイル（File to Export）] ページで、パブリック証明書のフルパスを指定します。これには、Unity Connection サーバーにアクセスできる場所とファイル名が含まれます。

ステップ 10 [次へ（Next）] を選択します。

ステップ 11 [証明書のエクスポートウィザードの完了（Completing the Certificate Export Wizard）] ページで、**[完了（Finish）]** を選択します。

ステップ 12 **[OK]** を 3 回選択して、1 つのメッセージボックスと 2 つのダイアログボックスを閉じます。

ステップ 13 **[認証局 MMC（Certification Authority MMC）]** を閉じます。

ステップ 14 ステップ 1 でリストされているすべてのサーバーに対して、同じ Microsoft 証明書サービスを使って SSL 証明書を発行した場合、この手順はこれで終了です。 この項のタスクリストに戻ります。

ステップ 1 に記載したすべてのサーバーに対して、別の Microsoft 証明書サービスを使用して SSL 証明書を発行した場合、ステップ 1 からステップ 13 を繰り返して、Microsoft 証明書サービスの各インスタンスに対して 1 つのパブリック証明書を取得します。 その後、この項のタスクリストに戻ります。

パブリック証明書を Unity Connection サーバーにアップロードする

ステップ 1 Cisco Unified Operating System の管理ページで、[セキュリティ（Security）] を展開し、**[証明書の管理（Certificate Management）]** を選択します。

ステップ 2 [証明書の管理（Certificate Management）] ページで、**[証明書のアップロード（Upload Certificate）]** を選択します。

ステップ 3 [証明書名（Certificate Name）] リストで、**[tomcat-trust]** を選択します。

ステップ 4 （オプション）**[説明（Description）]** フィールドに説明を入力し、**[参照（Browse）]** を選択します。

ステップ 5 .pem 形式でパブリック証明書を保存した場所を参照し、変換された証明書の 1 つを選択します。

ステップ 6 [ファイルのアップロード（Upload File）] を選択します。

ステップ 7 ステップ 2 からステップ 6 を繰り返します。ただし、[証明書名（Certificate Name）] リストに **[Unity Connection-trust]** を追加します。

ステップ 8 複数の証明機関からのパブリック証明書がある場合は、ステップ 2 からステップ 7 を繰り返します。

Office 365 および Cisco Unity Connection の証明書をアップロードする

ユニファイド メッセージング サービスの作成時に、Office 365 に対して [Exchange サーバーの証明書を確認する（Validate Certificates for Exchange Servers）] を選択した場合、次の手順を実行して、Office 365 ルート証明書を Cisco Unity Connection の tomcat-trust にアップロードする必要があります。

ステップ 1 Office 365 EWS エンドポイント URL https://outlook.office365.com/EWS/Exchange.ASMX を選択し、Office 365 ルート証明書をダウンロードします。

ステップ 2 Cisco Unified Operating System の管理ページで、[セキュリティ（Security）] を展開し、[証明書の管理（Certificate Management）] を選択します。

ステップ 3 [証明書の管理（Certificate Management）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4 [証明書名（Certificate Name）] リストで、[tomcat-trust] を選択します。

ステップ 5 （オプション）**[説明（Description）]** フィールドに説明を入力し、[参照（Browse）] を選択します。

ステップ 6 Office 365 ルート証明書を保存した場所を参照し、証明書を選択します。

ステップ 7 [ファイルのアップロード（Upload File）] を選択します。

注意 Office 365 EWS エンドポイント URL が別のルート証明書を通じて Cisco Unity Connection と通信する場合、同じものを Cisco Unity Connection の tomcat-trust にアップロードする必要があります。

Unity Connection ユーザーで構成する設定

ステップ 1 Cisco Unity Connection の管理で、**[サービスクラス（Class of Service）]** を展開し、**[サービスクラス（Class of Service）]** を選択します。 [サービスクラスの検索（Search Class of Service）] ページで、ユニファイド メッセージングを設定するユーザーに割り当てられたサービスクラスを選択します。（各フィールドの詳細については、**ヘルプ（Help）>このページ（This Page）**を参照してください）。

ステップ 2 [サービスクラスの編集（Edit Class of Service）] ページの **[ライセンス済み機能（Licensed Features）]** セクションで、**[IMAP クライアントやシングルインボックスを使用したボイスメールへのアクセスをユーザーに許可する（Allow Users to Access Voicemail Using an IMAP Client and/ or Single Inbox）]** チェックボックスを選択します。

ステップ 3 メッセージエージングまたはメッセージ割り当てを設定する必要があります。 詳細は、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html にある『*Cisco Unity Connection* システム アドミニストレーション ガイド、リリース *14*』の「メッセージストレージ」の章を参照してください。

（注） ウェブ受信箱からメッセージを完全に削除したい場合は、**[メッセージオプション（Message Options）]** セクションの **[削除済みアイテムフォルダに保存せずにメッセージを削除する（Delete Messages Without Saving to Deleted Items Folder）]** チェックボックスをオンにします。

ステップ 4 （テキスト読み上げ機能のみ）：**[ライセンス済み機能（Licensed Features）]** セクションで、**[詳細機能へのアクセスを許可する（Allow Access to Advanced Features）]** および **[テキスト/スピーチ（TTS）を使用したExchange電子メールへのアクセスを許可する（Allow Access to Exchange Email by Using Text to Speech (TTS)）]** のチェックボックスをオンにします。

ステップ 5 **保存**を選択します。

ユーザーのユニファイド メッセージ アカウント

Unity Connection に関連するユニファイド メッセージ アカウントとユーザーアカウント

ユニファイドメッセージング アカウントは、Unity Connection のユーザーをユニファイド メッセージング サービスに接続します。 ユニファイド メッセージ アカウントは、ユーザーアカウントとは別のオブジェクトです。

- ユーザーアカウントを作成する際、Unity Connection はそのユーザーのユニファイド メッセージ アカウントを自動的に作成しません。
- 1 人のユーザーに対して複数のユニファイド メッセージ アカウントを作成できますが、ユーザーのユニファイドメッセージアカウントで重複する機能を持つことはできません。たとえば、同じユーザーに対して、シングルインボックスを有効にする 2 つのユニファイド メッセージ アカウントを作成することはできません。
- ユーザーに対して複数のユニファイド メッセージング アカウントを作成することは、ユニファイドメッセージング機能へのアクセスを制御する 1 つの方法です。 たとえば、すべてのユーザーに 1 つの受信箱を持たせ、少数のユーザーだけに Exchange メールへのテキスト読み上げのアクセスを持たせたい場合、2 つのユニファイドメッセージング サービスを作成できます。 1 つはシングルインボックスをアクティベートし、もう 1 つは TTS をアクティベートします。 次に、すべてのユーザーに対してユニファイド メッセージ アカウントを作成して、シングルインボックスにアクセスできるようにします。また、TTS を希望するユーザーに対して 2 番目のユニファイド メッセージ アカウントを作成します。
- ユニファイド メッセージ アカウントを追加すると、関連するユーザーアカウントはユニファイド メッセージ アカウントへの参照で更新されます。 ユーザーアカウントにはユニファイド メッセージ アカウントの情報は含まれていません。
- ユーザーアカウントを削除すると、そのユーザーのすべてのユニファイド メッセージ アカウントも削除されます。 ただし、ユニファイド メッセージ アカウントを削除しても、対応するユーザーアカウントは削除されません。 ユーザーアカウントは、ユニファイド メッセージ アカウントへの参照を削除するためにのみ更新されます。

ユーザー用のユニファイド メッセージ アカウントを作成する

一括管理ツールを使用すると、ユニファイド メッセージ アカウントを多数作成できます。 IP ツールを使用したユニファイド メッセージ アカウントの作成、更新、または削除の詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/administration/guide/b_14cucsag.html にある『*Cisco Unity Connection* システム アドミニストレーション ガイド、リリース *14*』の「ツール」の章の「一括管理ツール」の項を参照してください。

後ほどユニファイド メッセージ アカウントのシングル受信箱を無効にする場合の同期動作の詳細については、「Exchange メールボックスの移動と復元」の章を参照してください。

ステップ 1 Cisco Unity Connection Administration で、**[ユーザー（Users）]** を展開し、**[ユーザー（Users）]** を選択します。 [ユーザーの検索（Search Users）] ページで、**[新規追加（Add New）]** を選択して新規ユーザを作成するか、またはユニファイド メッセージ アカウントを作成する適切なユーザーを選択します。

ステップ 2 ユニファイド メッセージ アカウントの設定（各フィールドの情報は、**ヘルプ（Help）>このページ（This Page）**を参照してください）：

a) **[編集（Edit）]** メニューで **[ユニファイド メッセージアカウント（Unified Messaging Accounts）]** を選択します。

b) [ユニファイドメッセージアカウント（Unified Messaging Accounts）] ページで、**[新規追加（Add New）]** を選択します。

c) [新しいユニファイド メッセージング アカウント（New Unified Messaging Accounts）] ページの必須フィールドに値を入力し、**[保存（Save）]** を選択します。

ステップ 3 ユーザーの設定を確認するには、**[テスト（Test）]** を選択します。 [タスクの実行結果（Task Execution Results）] ウィンドウにテスト結果が表示されます。

テストに一部でも失敗した場合は、メールサーバー、Active Directory、Unity Connection、および Unity Connection ユーザーの設定を確認します。

ユニファイドメッセージングの設定をテストする

ユニファイドメッセージング設定の概要を表示する

Unity Connection サーバー上のすべてのユニファイド メッセージング アカウントの設定の概要を表示できます。これには次が含まれます。

- Unity Connection 設定の整合性の問題がユニファイドメッセージングが正常に機能していないかどうかを示す、各ユニファイド メッセージング アカウントの接続構成設定の現在のステータス。 ユニファイド メッセージング アカウントの状況アイコンを選択すると、[ユニファイド メッセージング アカウント（Unified Messaging Account）] ページが表示され、ページの状況領域に、問題と考えられる問題の両方が一覧表示されます。

- [ユニファイド メッセージング アカウント（Unified Messaging Account）] ページの **[接続のテスト（Test Connectivity）]** ボタンを使用して、ユニファイド メッセージング アカウントが他のサーバーと接続できるかどうかをテストすることもできます。
- アカウントに関連付けられたユーザーのエイリアスです。 ユニファイド メッセージング アカウントのエイリアスを選択すると、[ユニファイド メッセージング アカウントの編集（Edit Unified Messaging Account）] ページが表示され、ページの状況領域に、問題と考えられる問題の両方が一覧表示されます。
- ユニファイド メッセージング アカウントに関連付けられたユーザーの表示名です。
- ユニファイド メッセージング アカウントに関連付けられているユニファイド メッセージング サービスの名前。 サービス名を選択すると、[ユニファイド メッセージング サービス（Unified Messaging Services）] ページが表示され、サービスの設定が示されます。
- 各ユニファイド メッセージング アカウントの現在のユニファイドメッセージング設定。

Unity Connection のユニファイド メッセージ アカウントの設定の概要を表示する

ステップ 1 Cisco Unity Connection の管理で、**[ユニファイドメッセージング（Unified Messaging）]** を展開し、**[ユニファイド メッセージング アカウントの状況（Unified Messaging Accounts Status）]** を選択します。

ステップ 2 列の値を昇順にソートするには、列の見出しを選択します。 降順でソートするには、再度見出しを選択します。

ステップ 3 次の設定を表示します。

- アカウントに [ユニファイド メッセージング アカウント（Unified Messaging Accounts）] ページを表示するには、アイコンまたは値を選択し、**[エイリアス（Alias）]** 列を適切な行に更新します。
- アカウントに [ユニファイド メッセージング サービス（Unified Messaging Services）] ページを表示するには、**[UM サービス（UM Services ）]** 列を適切な行に更新します。

システム設定およびユニファイドメッセージングと Exchange および Unity Connection をテストする

Unity Connection システムテストを実行できます。これにはユニファイドメッセージング設定のテストが含まれます。このテストでは、設定の問題に関する概要データを提供します。例えば、設定に問題がある特定のユニファイド メッセージング サービスに割り当てられたアカウントの数などです。

以下の作業を行って、システム設定およびユニファイドメッセージング設定を確認します。

ステップ 1 Cisco Unity Connection の管理で、**[ツール（Tools）]** を開き、**[タスク管理（Task Management）]** を選択します。

ステップ 2 [タスク定義（Task Definitions）] ページで、**[システム設定の確認（Check System Configuration）]** を選択し、**[今すぐ実行（Run Now）]** を選択します。

ステップ 3 **[更新]（Refresh）** を選択して、最新の結果へのリンクを表示します。

ステップ 4 結果を確認し、問題があれば解決し、**[システム設定の確認（Check System Configuration）]** のタスクを問題が見つからなくなるまで再実行します。

Unity Connection に向けたカレンダーへのアクセスをテストする

Unity カレンダーへの接続を設定した場合、次の手順でカレンダーへのアクセスをテストできます。

ステップ 1 **Outlook** にサインインします。

ステップ 2 **[移動（Go）]** メニューで、**[カレンダー（Calendar）]** を選択します。

ステップ 3 **[ファイル（File）]** メニューで、**新規（New）> ミーティングリクエスト（Meeting Request）** を選択します。

ステップ 4 必須フィールドに値を入力して新しいタイムのミーティングをスケジュールし、Unity Connection のアカウントを持つユーザーを招待します。 **[送信]** を選択します。

ステップ 5 ステップ 4 で Outlook ミーティングに招待したユーザーの Unity Connection メールボックスにログインします。

ステップ 6 ユーザーアカウントが音声認識アクセスに設定されている場合は、**「Play Meetings」** と言います。

ユーザーアカウントが音声アクセスに構成されていない場合、**6** を押して、プロンプトに従ってミーティングを一覧表示します。 Unity Connection がミーティングに関する情報を読み取ります。

SMTP ドメイン名設定の問題を解決する

シングルインボックスのユーザーがボイスメールを受信すると、Unity Connection からメールサーバーに同期されます。 送信者/受信者のメールアドレスには、Unity Connection ドメイン名が付いています。たとえば、userid@CUC-hostname です。 このため、Microsoft Outlook や IBM Lotus Notes のようなメールクライアントは、アドレス帳の [最近の連絡先（recent contacts）] として Unity Connection アドレスを追加します。 ユーザーがメールに返信したり、メールの作成中に受信者を追加したりすると、Unity Connection アドレスを入力/選択することができます。この場合、NDR になる可能性があります。 ボイスメールが Unity Connection からメールサーバーに同期されるときに、送信者/受信者の電子メールアドレスが会社の電子メールアドレス、たとえば userid@corp-hostname として表示されるようにするには、さらにステップを実行する必要があります。

SMTP ドメイン名の設定の問題を解決するには、次の手順に従います。

ステップ 1 Cisco Unity Connection の管理で、**システム設定（System Settings）> SMTP 設定（SMTP Configuration）** を選択し、**[スマートホスト（Smart Host）]** を選択します。

ステップ 2 [スマートホスト（Smart Host）] ページで、必須フィールドの値を入力し、**[保存（Save）]** を選択します（各フィールドの詳細については、**ヘルプ（Help）>このページ（This Page）**を参照してください）。

（注） Microsoft Exchange サーバーはスマートホストとして使用できます。

ステップ 3 ユーザーの会社メールアドレスを設定します。

a) Cisco Unity Connection Administration で、**[ユーザー（Users）]** を展開し、**[ユーザー（Users）]** を選択します。 [ユーザーの検索（Search User）] ページで、適切なユーザーを選択します。

b) [ユーザーの基本設定の編集（Edit User Basics）] ページで、**[会社メールアドレス（Corporate Email Address）]** フィールドを選択し、**[保存（Save）]** を選択します。

ステップ 4 Cisco Unity Connection の管理で、**[システム設定（System Settings）]** を展開し、**[全般設定（General Configuration）]** を選択します。

ステップ 5 [全般設定（General Configuration）] ページの **[受信者が見つからない場合（When a recipient cannot be found）]** リストで、**[スマートホストにメッセージをリレー（Relay message to smart host）]** を選択します。そうすることで、受信者が見つからない場合にスマートホストにメッセージが送信されるようになります。**[保存（Save）]** を選択します。

ステップ 6 ユーザーのメッセージアクションを設定します。

a) Cisco Unity Connection Administration で、**[ユーザー（Users）]** を展開し、**[ユーザー（Users）]** を選択します。 [ユーザーの基本設定の検索（Search Users Basics）] ページで、適切なユーザーを選択します。

b) [ユーザーの基本設定の編集（Edit User Basics）] ページの**[編集（Edit）]** メニューで、**[メッセージアクション（message Actions）]** を選択します。。 [メッセージアクションの編集（Edit Message Actions）] ページで、**[ボイスメール（Voicemail）]** ドロップダウンリストから **[メッセージを承認する（Accept the Message）]** オプションを選択します。

（注） [メール、FAX、領収書（Email, Fax, and receipt）] ドロップダウンリストから **[メッセージをリレー（Relay the Message）]** オプションを確実に選択します。

ステップ 7 メールサーバーに受信者ポリシーをセットアップします。これにより、Unity Connection エイリアスが **[社内メールアドレス ID（Corporate Email Address ID）]** に決定します。

- Exchange 2019、Exchange 2016 または Exchange 2013 については、次のリンクを参照してください。

  http://technet.microsoft.com/en-us/library/bb232171.aspx

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