Cisco Unified Communications Manager リリース 11.0(1) 上の IM and Presence サービス向け Microsoft Exchange

初版：2015 年 06 月 08 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）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。

© 2016 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章

はじめに

はじめに

Microsoft Exchange と IM and Presence サービスの統合により、ユーザは Microsoft Outlook の予定表/会議のステータスを IM and Presence サービスのアベイラビリティ ステータスに組み込むことができます。

対象読者

この出版物は、IM and Presence サービスとの Microsoft Exchange の統合を設定および管理する経験豊富なユーザを対象としています。

構成

本ガイドは、次の項について説明します。

章	タイトル	説明
1	IM and Presence サービスと Microsoft Exchange の統合の概要，（5 ページ）	IM and Presence サービスとの Microsoft Exchange 統合の概要

章	タイトル	説明
2	IM and Presence サービスと Microsoft Exchange の統合の計画, （9 ページ）	前もって必要な設定タスク、設定およびセキュリティ上の考慮事項、および詳細情報を取得する方法について説明します。
3	Exchange Web サービスを経由した IM and Presence サービスと統合するための Exchange サーバ 2007 以降の設定	Exchange Web サービス経由での IM and Presence サービスと Microsoft Exchange サーバ 2007、2010 および 2013 の統合について説明します。
4	Microsoft Exchange サーバと統合するように IM and Presence サービスを設定する, （31 ページ）	一般的な設定タスクについて説明します。
5	Exchange 予定表統合のトラブルシューティング, （55 ページ）	最も一般的なトラブルシューティング タスクについて説明し、一般的な問題を解決します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	表示
bold フォント	コマンド、キーワード、およびユーザが入力するテキストは、**bold** フォントで記載されます。
italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで記載されます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで記載されます。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 問題の解決に役立つ情報であることを示します。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、次のURLで、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』はRSSフィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSSフィードは無料のサービスです。シスコは現在、RSSバージョン2.0をサポートしています。

第 2 章

IM and Presence サービスと Microsoft Exchange の統合の概要

概要

Microsoft Exchange と IM and Presence サービスの統合では、ユーザの Microsoft Outlook の予定表/会議のステータスを IM and Presence サービスのアベイラビリティ ステータスに組み込むことができます。

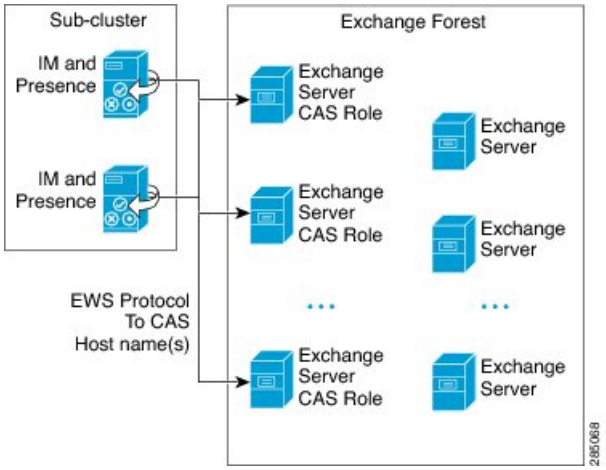
展開

Exchange Web サービス

Exchange Web サービス（EWS）では、HTTP を介して Microsoft Exchange のメールボックスおよびコンテンツとのやりとりを行えます。EWS は、Microsoft Outlook を介して利用できるデータと

ほぼ同じデータにアクセスできます。EWSは、クライアントコンピュータからサーバにいくつかの責任を移動します。

図 *1*：*EWS* を介した *IM and Presence* サービスとの *Microsoft Exchange* 統合



IM and Presence サービスでの Microsoft Outlook の予定表ステータス

Microsoft Exchange と IM and Presence サービスの統合では、ユーザの Microsoft Outlook の予定表/会議のステータスを IM and Presence サービスのアベイラビリティ ステータスに組み込むことができます。次の表は、到達可能性のマッピングと、IM and Presence サービスにおいて会議ステータス（Microsoft Outlook 予定表に表示される）と IM and Presence サービスのユーザのアベイラビリティ ステータスがどのように対応付けられるかを示しています。

表 *1*：予定表ステータスに基づく集約されたアベイラビリティ ステータス

Microsoft Outlook のステータス	IM and Presence サービスのステータス
空き時間/仮の予定	応対可
ビジー	会議中
勤務時間外[1]	退席中
退席中[2]	退席中

[1] Microsoft Outlook 2007 および Microsoft Outlook 2010 のデスクトップ クライアント。

[2] Microsoft Outlook Web Access（OWA）2010。

プレゼンス ゲートウェイのオプション

IM and Presence サービス上で予定表情報を交換するには、Microsoft Exchange サーバをプレゼンス ゲートウェイとして設定する必要があります。Presence Gateway to Exchange により、IM and Presence サービスのノードがユーザ単位でユーザのアベイラビリティ ステータスを反映することができます。

制約事項と制限

次に示すのは、IM and Presence サービスと Microsoft Exchange の統合に関する制限事項です。

- 1 台以上の EWS サーバを追加、更新、または削除できます（上限はありません）。ただし、[プレゼンス ゲートウェイ（Presence Gateway）] ウィンドウの [トラブルシュータ（Troubleshooter）] は、設定した最初の 10 台までの EWS サーバのステータスのみを検証し、レポートするよう作られています。
- IM and Presence サービスの本リリースでは、Exchange の自動検出サービスに対応していません。自動検出サービスでは、ロードバランシング機構がすでにクライアント アクセス サーバ（CAS）またはサーバに配置されていることが前提となっています。

第 3 章

IM and Presence サービスと Microsoft Exchange の統合の計画

必要な設定タスク

Microsoft Exchange の IM and Presence サービスとの統合を設定する前に、次の互換性マトリクスを参照し、統合に必要なコンポーネントのインストールおよび設定が完了していることを確認してください。

表 *2*：互換性マトリクス

コンポーネント	互換性のあるバージョン
Windows Server	• Windows Server 2003（SP2）サービス パック • Windows Server 2008（SP2）サービス パック
Cisco Unified Communications Manager	Cisco Unified Communications Manager のリリースは、IM and Presence サービスのリリースと一致させる必要があります。
IM and Presence サービス	IM and Presence サービスのリリースは、Cisco Unified Communications Manager のリリースと一致させる必要があります。
Microsoft Exchange サーバ 2007	Microsoft Exchange 2007（SP1）サービス パック

コンポーネント	互換性のあるバージョン
Microsoft Exchange サーバ 2010	Microsoft Exchange 2010（SP1）サービス パック
Microsoft Exchange サーバ 2013	Microsoft Exchange 2013（SP1）サービス パック
Active Directory	• Active Directory 2003 と Windows Server 2003（SP2） -- または -- • Active Directory 2008 と Windows Server 2008（SP2） （注） Active Directory 内のユーザ名は、Cisco Unified Communications Manager に定義されたユーザ名と一致している必要があります。
サードパーティの証明書または証明書サーバ	証明書を作成するためには、これらのいずれかが必要。

Exchange サーバ 2007、2010、および 2013 では、Exchange Web サービス（EWS）をサポートしています。

コンフィギュレーションの考慮事項

交換 Web サービスによる Microsoft Exchange サーバとの統合

Microsoft Exchange サーバ 2007 では、Exchange Web サービス（EWS）が導入され、Simple Object Access Protocol（SOAP）に似たインターフェイスを使用して Exchange サーバに予定表を統合できます。

Exchange 統合のために EWS プレゼンス ゲートウェイを [Cisco Unified CM IM and Presence Service Administration] ユーザ インターフェイスで設定する場合は、次の点に注意してください。

- 1 台以上の EWS サーバを追加、更新、または削除できます（上限はありません）。ただし、[プレゼンス ゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [トラブルシュータ（Troubleshooter）] は、設定した最初の 10 台までの EWS サーバのステータスのみを検証し、レポートするように作成されています。
- EWS サーバ ゲートウェイは、最初の EWS サーバ ゲートウェイに対して設定したクレデンシャル（アカウント名とパスワード）を共有します。1 つの EWS サーバ ゲートウェイのクレデンシャルを変更すると、設定されたすべての EWS ゲートウェイのクレデンシャルもそれに準じて変更されます。
- 1 つ以上の EWS サーバを追加、更新、または削除した後に設定の変更を反映するには、Cisco Presence Engine を再起動する必要があります。複数の EWS サーバを連続して追加した場合

は、すべての変更を同時に反映するよう Cisco Presence Engine を一度だけ再起動することができます。

Exchange サーバの管理役割と権限

Exchange Web サービス（EWS）では、すべてのユーザの予定表情報へのアクセスを有効にするために特別なアカウントが必要になります。このアカウントは偽装アカウントと呼ばれます。

Microsoft Exchange サーバ 2007

呼び出し元が Exchange サーバ 2007 で別のユーザの電子メール アカウントにアクセスするには、EWS の統合には偽装権限を持つアカウントが必要となります。呼び出し元は、呼び出し元のアカウントと関連付けられた権限ではなく、偽装したアカウントに関連付けられた権限を使用し、指定したユーザ アカウントを偽装します。

偽装アカウントは、Exchange 2007 を実行するクライアント アクセス サーバ（CAS）上で **ms-Exch-EPI-Impersonation** 権限が付与される必要があります。これで、CAS を使用してユーザの電子メール アカウントを偽装する権限が呼び出し元に与えられます。さらに、呼び出し元は、メールボックス データベースとディレクトリ内の個々のユーザ オブジェクトのいずれかで **ms-Exch-EPI-MayImpersonate** 権限も付与される必要があります。

個々のユーザのアクセス コントロール リスト（ACL）がメールボックス データベース設定に優先するため、呼び出し元にデータベース内のすべてのメールボックスへのアクセスを許可し、必要に応じて同じデータベース内の特定のメールボックスへのアクセスを拒否できます。

Microsoft Exchange サーバ 2010 および 2013

Microsoft Exchange サーバ 2010 および 2013 は、ロールベース アクセス コントロール（RBAC）を使用して偽装アカウントに権限を付与し、ユーザに組織での職務に関連するタスクの実行を許可します。RBAC 権限を適用するには主に 2 つの方法があり、ユーザが管理者またはスーパー ユーザであるかエンドユーザであるかによって使い分けます。

- 管理役割グループ：Exchange のセットアップ プロセス中に 11 のデフォルト管理役割グループが提示されます。各グループには、その役割に固有の権限が関連付けられています。組み込まれている役割グループの例として、「受信者の管理」と「ヘルプデスク」があります。一般に、特定のタスクを実行する必要があるスーパーユーザには適切な管理役割グループが割り当てられ、それに関連付けられた権限を継承します。たとえば、Exchange 組織内の任意のユーザの連絡先情報を修正する必要のある製品サポート担当者は、「ヘルプデスク」管理役割グループのメンバーとして割り当てられます。
- 管理役割割り当てポリシー：管理者またはスーパーユーザではない一般ユーザの場合、管理役割割り当てポリシーは、ユーザが修正できるメールボックスの種類を制御します。**New-ManagementRoleAssignment** コマンドレットを使用してユーザに **ApplicationImpersonation** 役割を割り当てると、アカウントが組織内のユーザを偽装し、そのユーザの代わりにタスクを実行できます。役割の割り当て範囲は、**New-ManagementScope** コマンドレットを使用して個別に管理され、特定の受信者やサーバを対象として絞り込むことができます。

（注） RBAC では、Exchange サーバ 2007 で求められるように ACL を修正および管理する必要はありません。

Exchange サーバの統合におけるプレゼンス ゲートウェイの設定

（EWS 予定表統合が有効になった状態で）多数のユーザをサポートするには、IM and Presence サービスにより複数のクライアント アクセス サーバ（CAS）間で EWS トラフィックの負荷を分散する必要があります。IM and Presence サービスは、EWS 経由で多くの CAS に接続できます。また、次のラウンド ロビン方式を使用することで、遭遇するトラフィック負荷をサポートします。

- 最初にユーザの予定表購読を有効にしたときには、そのユーザには管理者によって設定された対象 CAS ホストのプールから CAS が割り当てられます。
- ユーザへの割り当ては、そのユーザの予定表購読が失敗するまで保持されます。
- ユーザの予定表購読が失敗した場合は、対象 CAS ホストのプールから CAS がユーザに再度割り当てられます。

交換 Web サービスの統合の既知の問題

- Exchange Web サービス（EWS）の統合に影響することが確認されている問題については、このガイドの「Exchange 予定表統合のトラブルシューティング，（55 ページ）」の章を参照してください。
- Microsoft Exchange の統合に影響することが確認されている問題を参照してください。

セキュリティの考慮事項

Windows セキュリティ ポリシーの設定

Microsoft Exchange との IM and Presence サービスの統合では、Windows 統合認証（NTLM）などのさまざまな認証方式がサポートされます。

IM and Presence サービスは、NTLMv1 および NTLMv2 の 2 つの Windows 統合認証をサポートし、デフォルトで NTLMv2 を使用します。

[Lan Manager 認証レベル（Lan Manager authentication level）] を [NTLMv2 応答のみを送信（Send NTLMv2 response only）] を送信します。 Windows ドメイン コントローラの [LM および NTLM を拒否（Refuse LM & NTLM）] は、ドメインで NTLMv2 認証を強制します。

（注） IM and Presence サービスは、NTLMv2 セッションセキュリティをサポートしません。メッセージの機密性と整合性は、セキュアな htttp（https）によって提供されます。

参考情報の入手

Cisco Unified Communications Manager および IM and Presence サービスのマニュアル

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Microsoft Exchange 2007 のマニュアル

http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx

Microsoft Exchange 2010 のマニュアル

http://technet.microsoft.com/en-us/library/bb124558.aspx

Microsoft Exchange 2013 のマニュアル

http://technet.microsoft.com/en-us/library/bb124558%28exchg.150%29.aspx

Microsoft Active Directory 2008 のマニュアル

http://www.microsoft.com/windowsserver2008/en/us/ad-main.aspx

第 4 章

Exchange Web サービスを経由した Microsoft Exchange と IM and Presence サービスの統合

Exchange Web サービスによる Microsoft Exchange 2007 の設定

はじめる前に

Exchange サーバ 2007 サーバの設定手順は、Windows Server 2003 または Windows Server 2008 のどちらを使用するかによって異なります。

Exchange サーバ 2007 上のメールボックスへのアクセスを設定する場合、次の手順を実行します。詳細な手順については、次の URL で Exchange サーバ 2007 のマニュアルを参照してください。
http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx

ヒント　IM and Presence サービスでは、Exchange サーバへの接続時にそのアカウントへログインするのに必要なのはアカウントに対する偽装権限のみです。このアカウントは、通常、メールを受信しないため、領域の割り当てについて考慮する必要はありません。

Windows セキュリティ ポリシーの設定

Microsoft Exchange との IM and Presence サービスの統合では、Windows 統合認証（NTLM）などのさまざまな認証方式がサポートされます。

IM and Presence サービスは、NTLMv1 および NTLMv2 の 2 つの Windows 統合認証をサポートし、デフォルトで NTLMv2 を使用します。

[Lan Manager 認証レベル（Lan Manager authentication level）] を [NTLMv2 応答のみを送信（Send NTLMv2 response only）] を送信します。 Windows ドメイン コントローラの [LM および NTLM を拒否（Refuse LM & NTLM）] は、ドメインで NTLMv2 認証を強制します。

（注）　IM and Presence サービスは、NTLMv2 セッション セキュリティをサポートしません。メッセージの機密性と整合性は、セキュアな htttp（https）によって提供されます。

Windows のセキュリティ設定の確認

手順

ステップ 1　Exchange を実行している Windows ドメイン コントローラおよびサーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。

ステップ 2　[セキュリティ設定（Security Settings）] > [ローカル ポリシー（Local Policies）] > [セキュリティ オプション（Security Options）] に移動します。

ステップ 3　[ネットワーク セキュリティ：NTLM SSP ベース（セキュア RPC など）サーバのための最低限のセッション セキュリティ（Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers）] を選択します。

ステップ 4　[NTLMv2 セッション セキュリティが必要（Require NTLMv2 session security）] チェックボックスがオフになっていることを確認します。

ステップ 5　[NTLMv2 セッション セキュリティが必要（Require NTLMv2 session security）] チェックボックスがオンになっている場合は、次の手順を完了します。

a) [NTLMv2 セッション セキュリティが必要（Require NTLMv2 session security）] チェックボックスをオフにします。

b) [OK] をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Exchange を実行している Windows ドメイン コントローラとサーバをリブートします。

（注） セキュリティ ポリシー設定が変更されたサーバ以外にリブートは必要ありません。

サービスアカウントにローカルでサインインする権限をユーザに付与する

ユーザがサービス アカウントにローカルにログインするように設定するは、次のいずれかの手順を実行します。

はじめる前に

- Exchange の偽装を正常に機能させるには、すべての Microsoft Exchange サーバを Windows Authorization Access Group のメンバにする必要があります。
- サービス アカウントは、Exchange 管理グループのメンバであってはなりません。Exchange は、これらのグループのすべてのアカウントの偽装を明示的に拒否します。

Windows Server 2003 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange View Only Administrator ロールを委任されたサービス アカウントを使用して [Exchange サーバ 2007（Exchange サーバ 2007）] ユーザ インターフェイスにログインします。

ステップ 2 左ペインの [セキュリティ設定（Security Settings）] 下で、[ローカル ポリシー（Local Policies）] > [ユーザ権限の割り当て（User Rights Assignments）] に移動します。

ステップ 3 コンソールの右側のペインで、[ローカル ログオンを許可する（Allow Log On Locally）] をダブルクリックします。

ステップ 4 [ユーザまたはグループを追加する（Add User or Group）] を選択し、作成済みのサービス アカウントに移動して選択します。

ステップ 5 [名前の確認（Check Names）] を選択し、指定されたユーザが正しいことを確認します。

ステップ 6 [OK] をクリックします。

次の作業

サーバ レベルでの偽装権限の設定，（18 ページ）

Windows Server 2008 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange View Only Administrator ロールを委任されたサービス アカウントを使用して Exchange サーバ 2007 にログインします。

ステップ 2 [スタート（Start）] を選択します。

ステップ 3 gpmc.msc と入力します。

ステップ 4 [Enter] を選択します。

ステップ 5 Exchange サーバで [ドメイン コントローラ セキュリティの設定（Domain Controller Security Settings）] ウィンドウを開きます。

ステップ 6 左ペインの [セキュリティ設定（Security Settings）] 下で、[ローカル ポリシー（Local Policies）] > [ユーザ権限の割り当て（User Rights Assignments）] に移動します。

ステップ 7 コンソールの右側のペインで、[ローカル ログオンを許可する（Allow Log On Locally）] をダブルクリックします。

ステップ 8 [これらのポリシーの設定を定義する（Define these policy settings）] チェックボックスがオンになっていることを確認します。

ステップ 9 [ユーザまたはグループの追加（Add User or Group）] を選択し、作成済みのサービス アカウントに移動して選択します。次に、[OK] をクリックします。

ステップ 10 [名前の確認（Check Names）] を選択し、指定されたユーザが正しいことを確認します。次に、[OK] をクリックします。

ステップ 11 [ローカル ログオンを許可する（Allow Log On Locally）] プロパティのダイアログ ボックスで [適用（Apply）] と [OK] をクリックします。

ステップ 12 ユーザ SMTP アドレスが *alias@FQDN* であることを確認します。そうでない場合は、ユーザ プリンシパル名（UPN）を使用して偽装する必要があります。これは *alias@FQDN* と定義されます。

次の作業

サーバ レベルでの偽装権限の設定 , （18 ページ）

サーバ レベルでの偽装権限の設定

次の手順のコマンドは、サーバ レベルで偽装権限を許可することができます。また、データベース、ユーザ、および連絡先レベルでも権限を付与することもできます。

はじめる前に

- 個々の Microsoft Exchange サーバにアクセスするサービス アカウントの権限のみを付与する場合は、

```
Get-OrganizationConfig
```

の文字列を下記に置き換えます。

```
Get-ExchangeServer -Identity ServerName
```

ServerName は Exchange サーバの名前です。

例

```
Add-ADPermission -Identity (Get-ExchangeServer -Identity  exchangeserver1).
DistinguishedName -User (Get-User -Identity user | select-object).identity
-ExtendedRights Send-As
```

- ユーザの SMTP アドレスが alias@FQDN として定義されていることを確認します。そうでない場合は、ユーザ プリンシパル名（UPN）を使用してユーザ アカウントを偽装する必要があります。

手順

ステップ 1 コマンド ライン入力を行うために Exchange 管理シェル（EMS）を開きます。

ステップ 2 この Add-ADPermission コマンドを実行し、サーバに偽装権限を追加します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -AccessRights GenericAll -InheritanceType Descendents
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -AccessRights GenericAll -InheritanceType
Descendents
```

次の作業

サービス アカウントの Active Directory サービス拡張権限の設定, （19 ページ）

サービス アカウントの Active Directory サービス拡張権限の設定

はじめる前に

これらの権限は、クライアント アクセス サーバ（CAS）上で、偽装を実行するサービス アカウントに対して設定する必要があります。

- CAS がロードバランサの背後に配置されている場合は、ロードバランサの背後にあるすべての CAS の Microsoft Exchange 2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。
- お使いのメールボックス サーバが CAS とは異なるマシン上にある場合は、すべてのメールボックス サーバの Exchange 2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。

- この権限は、[Active Directory サイトとサービス（Active Directory Sites and Services）] または [Active Directory ユーザとコンピュータ（Active Directory Users and Computers）] ユーザ インターフェイスを使用して設定することもできます。

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

ステップ 2 EMS で次の Add-ADPermission コマンドを実行して、指定したサービス アカウント（Exchange 2007 など）のサーバに対する偽装権限を追加します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

ステップ 3 EMS で次の Add-ADPermission コマンドを実行して、サービス アカウントに偽装する各メールボックスへの偽装権限を追加します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

次の作業

サービス アカウントおよびユーザ メールボックスへの Send As 権限の付与, （20 ページ）

サービス アカウントおよびユーザ メールボックスへの Send As 権限の付与

サービス アカウントおよびユーザ メールボックスに Send As 権限を付与するには、次の手順に従ってください。

（注） この手順を実行するために、Microsoft Exchange 管理コンソール（EMC）を使用することはできません。

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

ステップ 2 EMS で次の Add-ADPermission コマンドを実行して、サービス アカウントおよび関連するすべてのユーザ メールボックス ストアに Send As 権限を付与します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRights Send-As
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRights Send-As
```

次の作業

サービス アカウントおよびユーザ メールボックスへの偽装権限の付与, （21 ページ）

サービス アカウントおよびユーザ メールボックスへの偽装権限の付与

サービスアカウントおよびユーザメールボックスに偽装権限を付与するには、次の手順に従ってください。

（注） この手順を実行するために、Microsoft Exchange 管理コンソール（EMC）を使用することはできません。

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

ステップ 2 サービスアカウントの偽装権限に関連付けられているすべてのメールボックスストアを許可する EMS で次の **Add-ADPermission** コマンドを実行してください。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity User | select-object) .identity -ExtendedRights Receive-As
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity EX2007 | select-object) .identity -ExtendedRights Receive-As
```

（注） IM and Presence サービスでは、Exchange サーバへの接続時にそのアカウントへログインするのに必要なのはアカウントに対する偽装権限のみです。このアカウントは、通常、メールを受信しないため、領域の割り当てについて考慮する必要はありません。

次の作業

Microsoft Exchange 2007 アカウントの権限の確認, （22 ページ）

Microsoft Exchange 2007 アカウントの権限の確認

Exchange 2007 アカウントに権限を割り当てた後は、その権限がメールボックスのレベルまで伝播し、選択されたユーザがメールボックスにアクセスしたり別のユーザのアカウントを偽装したりすることが可能なことを確認する必要があります。Exchange 2007 では、権限がメールボックスに伝播されるまでに時間を要します。

はじめる前に

Exchange 2007 アカウントに適切な権限を委任してください。Exchange Web サービスによる Microsoft Exchange 2007 の設定, （15 ページ）を参照してください。.

手順

ステップ 1 Exchange サーバ 2007 の Exchange 管理コンソール（EMC）で、コンソール ツリーの [Active Directory サイトとサービス（Active Directory Sites and Services）] を右クリックします。

ステップ 2 [表示（View）] をポイントし、[サービス ノードの表示（Show Services Node）] を選択します。

ステップ 3 サービス ノード（`Services/MS Exchange/First Organization/Admin Group/Exchange Admin Group/Servers` など）を展開します。

ステップ 4 クライアント アクセス サーバ（CAS）が、選択したサービス ノードに表示されていることを確認します。

ステップ 5 各 CAS サーバの [プロパティ（Properties）]“ ”を表示し、[セキュリティ（Security）] タブで以下を確認します。

a) サービス アカウントがリストされている。

b) サービス アカウントに付与されている権限が（オンになっているチェックボックスにより）アカウントに Exchange Web サービスの偽装権限が付与されていることを示している。

（注） アカウントまたは偽装権限が手順 5 のとおりに表示されない場合は、サービス アカウントを再度作成し、必要な偽装権限をアカウントに付与する必要があります。

ステップ 6 サービス アカウント（Ex2007 など）にストレージ グループおよびメールボックス ストアに対する Allow impersonationpermission が付与され、個人情報の交換や別のユーザ アカウントでの送受信が可能であることを確認します。

ステップ 7 変更を有効にするために、Exchange サーバの再起動が必要となる場合があります。これはテストによって確認されています。

次の作業

Exchange 2007 以降のエディションの仮想ディレクトリでの認証の有効化

Exchange Web サービスによる Microsoft Exchange 2010 および 2013 の設定

Microsoft Exchange 2010 および 2013 サーバ上のメールボックスへのアクセスを設定する場合は、次のタスクを実行します。

- Windows のセキュリティ設定の確認
- 特定のユーザまたはグループへの Exchange 偽装権限の設定
- Microsoft Exchange 2010 または 2013 アカウントの権限の確認, （27 ページ）

はじめる前に

Exchange 2010 および 2013 サーバを IM and Presence サービスと統合するために Exchange Web サービス（EWS）を使用する前に、Exchange サーバにスロットル ポリシー パラメータ値を設定していることを確認します。これらの値は、EWS の予定表と IM and Presence サービスとの統合を正常に機能させるために必要な値です。

制約事項

これらは、Exchange サーバ 2010 向けのコマンドと設定です。Exchange サーバ 2013 の設定については、現在スケール試験を行っています。

- 設定は、Exchange サーバのバージョンによって異なります。正しく設定を行うには、EWS を使用して Exchange サーバ 2013 を統合するときに、設定を試行することが必要になる場合があります。
- コマンドは、Exchange サーバのバージョンによって異なる場合があります。詳細については、Exchange サーバ 2013 のコマンド マニュアルを参照してください。

表 *3*：*Exchange* サーバ *2010* で推奨されるスロットル ポリシーの設定

パラメータ	推奨設定値：Exchange サーバ 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null

パラメータ	推奨設定値：Exchange サーバ 2010
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60
[1] シスコの試験時には、予定表を使用するユーザ 50% に対応するにはデフォルトのスロットル ポリシー値で十分でした。 Client Access Server（CAS）への EWS リクエストの負荷が高い場合は、パラメータを 100 に増やすことを推奨します。	

表 *4*：*Exchange* サーバ *2013* で推奨されるスロットル ポリシーの設定

パラメータ[1]	推奨設定値：Exchange サーバ 2013
EwsCutoffBalance	まだ使用できない
EwsMaxBurst	まだ使用できない
EwsMaxConcurrency	まだ使用できない
EwsMaxSubscriptions	まだ使用できない
EwsRechargeRate	まだ使用できない
[1] これらは、Exchange サーバ 2013 で変更できる唯一の EWS パラメータです。	

関連トピック

Exchange サーバ 2010
Exchange サーバ 2013

Windows セキュリティ ポリシーの設定

Microsoft Exchange との IM and Presence サービスの統合では、Windows 統合認証（NTLM）などのさまざまな認証方式がサポートされます。

IM and Presence サービスは、NTLMv1 および NTLMv2 の 2 つの Windows 統合認証をサポートし、デフォルトで NTLMv2 を使用します。

[Lan Manager 認証レベル（Lan Manager authentication level）] を [NTLMv2 応答のみを送信（Send NTLMv2 response only）] を送信します。 Windows ドメイン コントローラの [LM および NTLM を拒否（Refuse LM & NTLM）] は、ドメインで NTLMv2 認証を強制します。

（注） IM and Presence サービスは、NTLMv2 セッション セキュリティをサポートしません。メッセージの機密性と整合性は、セキュアな htttp（https）によって提供されます。

Windows のセキュリティ設定の確認

手順

ステップ 1 Exchange を実行している Windows ドメイン コントローラおよびサーバで、[スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。

ステップ 2 [セキュリティ設定（Security Settings）] > [ローカル ポリシー（Local Policies）] > [セキュリティ オプション（Security Options）] に移動します。

ステップ 3 [ネットワーク セキュリティ：NTLM SSP ベース（セキュア RPC など）サーバのための最低限のセッション セキュリティ（Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers）] を選択します。

ステップ 4 [NTLMv2 セッション セキュリティが必要（Require NTLMv2 session security）] チェックボックスがオフになっていることを確認します。

ステップ 5 [NTLMv2 セッション セキュリティが必要（Require NTLMv2 session security）] チェックボックスがオンになっている場合は、次の手順を完了します。

a) [NTLMv2 セッション セキュリティが必要（Require NTLMv2 session security）] チェックボックスをオフにします。

b) [OK] をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Exchange を実行している Windows ドメイン コントローラとサーバをリブートします。

（注） セキュリティ ポリシー設定が変更されたサーバ以外にリブートは必要ありません。

特定のユーザまたはグループへの Exchange 偽装権限の設定

特定のユーザまたはユーザ グループに Exchange の偽装権限を設定するには、Microsoft Exchange 管理シェル（EMS）を使用して次の手順を実行します。

制約事項 これらは、Exchange サーバ 2010 向けのコマンドと設定です。Exchange サーバ 2013 の設定については、現在スケール試験を行っています。

- 設定は、Exchange サーバのバージョンによって異なる場合があり、EWS を使用して Exchange サーバ 2013 を統合するときに、適切な設定を行うために設定を試行することが必要になることがあります。
- コマンドは、Exchange サーバのバージョンによって異なる場合があります。詳細については、Exchange サーバ 2013 のコマンド マニュアルを参照してください。

手順

ステップ 1 Active Directory でアカウントを作成します。

ステップ 2 コマンド ライン入力を行うために EMS を開きます。

ステップ 3 EMS で New-ManagementRoleAssignment コマンドを実行し、他のユーザ アカウントを偽装する権限を指定する既存のドメイン サービス アカウント（*Ex2010* など）に付与します。

構文

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

例

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2010@contoso.com
```

ステップ 4 この New-ManagementRoleAssignment コマンドを実行し、偽装権限が適用される範囲を定義します。この例では、指定された Exchange サーバのすべてのアカウントを偽装する権限が、*Ex2010* アカウントに付与されます。

構文

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

例

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

ステップ 5 Exchange Web サービスによる Microsoft Exchange 2010 および 2013 の設定, （23 ページ） で定義された推奨値を含む新しいスロットル ポリシーを作成するには、New-ThrottlingPolicy コマンドを実行します。

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EWSMaxConcurrency:100 -EWSPercentTimeInAD:50
-EWSPercentTimeInCAS:90 -EWSPercentTimeInMailboxRPC:60 -EWSMaxSubscriptions:NULL
-EWSFastSearchTimeoutInSeconds:60 -EWSFindCountLimit:1000
```

例

```
New-ThrottlingPolicy -Name:IM_and_Presence_ThrottlingPolicy -EWSMaxConcurrency:100
-EWSPercentTimeInAD:50 -EWSPercentTimeInCAS:90 -EWSPercentTimeInMailboxRPC:60
-EWSMaxSubscriptions:NULL -EWSFastSearchTimeoutInSeconds:60 -EWSFindCountLimit:1000
```

注：サポートされる Exchange SP1 でのみ使用可能です。

ステップ 6 Set-ThrottlingPolicyAssociation コマンドを実行し、新しいスロットリング ポリシーと手順 2 で使用されたサービス アカウントを関連付けます。

構文

```
Set-ThrottlingPolicyAssociation -Identity Username -ThrottlingPolicy Policy_Name
```

例

```
Set-ThrottlingPolicyAssociation -Identity Ex2010 -ThrottlingPolicy
IM_and_Presence_ThrottlingPolicy
```

次の作業

Microsoft Exchange 2010 または 2013 アカウントの権限の確認, （27 ページ）

関連トピック

Exchange サーバ 2010
Exchange サーバ 2013

Microsoft Exchange 2010 または 2013 アカウントの権限の確認

Exchange 2010 または 2013 アカウントに権限を割り当てた後で、その権限がメールボックスのレベルまで伝播し、指定されたユーザがメールボックスにアクセスしたり別のユーザのアカウントを偽装したりできることを確認する必要があります。Exchange 2010 または 2013 では、権限がメールボックスに伝播されるまでに時間を要します。

制約事項 これらは、Exchange サーバ 2010 向けのコマンドです。コマンドは Exchange サーバのバージョンによって異なる場合があるので、Exchange サーバ 2013 を使用する場合は、コマンド マニュアルを参照する必要があります。

手順

ステップ 1 Active Directory サーバで、偽装アカウントが存在することを確認します。

ステップ 2 コマンド ライン入力を行うために Exchange 管理シェル（EMS）を開きます。

ステップ 3 Exchange サーバで、サービス アカウントに必要な次の偽装権限が付与されていることを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ManagementRoleAssignment role: ApplicationImpersonation
```

b) コマンド出力に、指定アカウントに対する ApplicationImpersonation の役割割り当てが示されることを確認します。

例：コマンド出力

Name	Role	RoleAssigneeName	RoleAssigneeType	AssignmentMethod	EffectiveUserName
_suImpersonateRoleAs	ApplicationImpersonation	ex2010	ユーザ（User）	Direct	ex2010

ステップ 4 サービス アカウントに適用される管理の範囲が正しいことを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ManagementScope _suImpersonateScope
```

b) 次のように、コマンド出力に偽装アカウント名が含まれていることを確認します。

例：コマンド出力

Name	ScopeRestrictionType	Exclusive	RecipientRoot	RecipientFilter	ServerFilter
_suImpersonateScope	ServerScope	いいえ（False）	ユーザ（User）	Direct	識別名（DistinguishedName）

ステップ 5 次のコマンドを EMS で実行して、ThrottlingPolicy パラメータが Exchange Web サービスによる Microsoft Exchange 2010 および 2013 の設定, （23 ページ） で定義されている内容と一致することを確認します。

```
Get-ThrottlingPolicy -Identity Policy_Name | findstr ^EWS
```

次の作業

Exchange 2007 以降のエディションの仮想ディレクトリでの認証の有効化

関連トピック

Exchange サーバ 2010
Exchange サーバ 2013

Exchange 仮想ディレクトリの認証のイネーブル化

はじめる前に

Exchange Web サービス（EWS）の統合が正しく機能するには、基本認証、Windows 統合認証またはその両方を Exchange サーバ 2007、2010 および 2013 の EWS 仮想ディレクトリ（/EWS）でイネーブルにする必要があります。

Windows Server 2003 を実行する Exchange 2007 の認証の有効化

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット情報サービス（Internet Information Services）] を開き、サーバを選択します。

ステップ 2 [Web サイト（Web Sites）] を選択します。

ステップ 3 [デフォルト Web サイト（Default Web Site）] を選択します。

ステップ 4 [EWS] ディレクトリ フォルダを右クリックし、[プロパティ（Properties）] を選択します。

ステップ 5 [ディレクトリ セキュリティ（Directory Security）] タブを選択します。

ステップ 6 [認証およびアクセス コントロール（Authentication and access control）] で、[編集（Edit）] をクリックします。

ステップ 7 [認証方法（Authentication Methods）] で、次のチェックボックスがオフになっていることを確認します。

- [匿名アクセスを有効化（Enable anonymous access）]

ステップ 8 [認証方法：認証付きアクセス（Authentication Methods Authenticated Access）] で、次のチェックボックスの両方がオンになっていることを確認します。

- 統合された Windows 認証（Integrated Windows Authentication）
- 基本的認証（Basic Authentication）（パスワードがクリア テキストで送信されます）

ステップ 9 [OK] をクリックします。

次の作業

Microsoft Exchange 統合向けのプレゼンス ゲートウェイの設定

Windows Server 2008 を実行する Exchange 2010 / 2013 における認証の有効化

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット情報サービス（Internet Information Services）] を開き、サーバを選択します。

ステップ 2 [Web サイト（Web Sites）] を選択します。

ステップ 3 [デフォルト Web サイト（Default Web Site）] を選択します。

ステップ 4 [EWS] を選択します。

ステップ 5 [IIS] セクションで、[認証（Authentication）] を選択します。

ステップ 6 次の認証方法が有効になっていることを確認します。

- 匿名認証
- Windows 認証や基本認証

ステップ 7 適切に設定するには、[操作（Actions）] カラムで有効または無効のリンクを使用します。

次の作業

Microsoft Exchange 統合向けのプレゼンス ゲートウェイの設定

関連トピック

Outlook Web アプリケーション仮想ディレクトリの管理
Exchange Web サービス仮想ディレクトリでの SSL の有効化または無効化

第 5 章

Microsoft Exchange サーバと統合するように IM and Presence サービスを設定する

Microsoft Exchange 統合向けのプレゼンス ゲートウェイの設定

予定表情報を交換するためには、Exchange サーバ（Microsoft Outlook）をプレゼンス ゲートウェイとして設定する必要があります。Exchange ゲートウェイにより、IM and Presence サービスのノードがユーザ単位でユーザのアベイラビリティ情報を反映することができます。

プレゼンス ゲートウェイを設定すると、次のいずれかの値を使用して Exchange サーバと接続できます。

- FQDN（DNS で解決可能）
- IP アドレス

Exchange 統合のために Exchange Web サービス（EWS）のプレゼンス ゲートウェイを [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスを使用して設定する場合は、次の点に注意してください。

- *1* 台以上の EWS サーバを追加、更新、または削除できます（上限はありません）。ただし、[プレゼンス ゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [トラブルシュータ（Troubleshooter）] は、設定した最初の 10 台までの EWS サーバのステータスのみを検証し、レポートするように作成されています。
- EWS サーバ ゲートウェイは、最初の EWS サーバ ゲートウェイに対して設定した偽装アカウント クレデンシャル（アカウント名とパスワード）を共有します。1 つの EWS サーバ ゲートウェイのクレデンシャルを変更すると、設定されたすべての EWS ゲートウェイのクレデンシャルもそれに準じて変更されます。
- 1 つ以上の EWS サーバを追加、更新、または削除した後に設定の変更を反映するには、Cisco Presence Engine を再起動する必要があります。複数の EWS サーバを連続して追加した場合は、すべての変更を同時に反映するよう Cisco Presence Engine を一度だけ再起動することができます。

（注）
- SAN 証明書については、保護されたホストが [サブジェクトの代替名（Subject Alternative Name）] フィールドのホスト名/IP アドレスのフィールド一覧に含まれている必要があります。
- プレゼンス ゲートウェイの設定時に、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドは [サブジェクトの代替名（Subject Alternative Name）] フィールドに表示されている保護されたホストと完全に一致している必要があります。

Exchange Web サービスを介したプレゼンス ゲートウェイとしての Exchange 2007、2010、または 2013 の設定

はじめる前に

プレゼンス ゲートウェイを設定する前に、IM and Presence サービスに有効な証明書チェーンをアップロードする必要があります。

Microsoft Exchange サーバへの接続を IPv6 経由で行う場合は、導入時に各 IM and Presence サービス ノード上でエンタープライズ パラメータが IPv6 に対し設定され、その Eth0 が IPv6 に対し設定されていることを確認します。IM and Presence サービスでの IPv6 の設定については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。

ステップ 2 [プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 プレゼンス ゲートウェイ タイプの [Exchange -- EWS Server（Exchange -- EWS サーバ）] を選択します。
設定変更を有効にするには、1 つ以上の EWS サーバを追加、更新、または削除した後に Cisco Presence Engine を再起動する必要があります。複数の EWS サーバを連続して追加した場合は、すべての変更を同時に反映するよう Cisco Presence Engine を一度だけ再起動することができます。

ステップ 5 2 種類以上のゲートウェイを設定した場合にプレゼンス ゲートウェイのインスタンスを区別できるよう、[説明（Description）] フィールドに意味のある説明を入力します。

ステップ 6 [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに、プレゼンス ゲートウェイのサーバの場所を入力し、それがサブジェクト共通名（CN）と一致するか、または Exchange サーバ証明書の [サブジェクトの代替名（Subject Alternative Name）] フィールドにあることを確認します。Exchange サーバに接続するには、次のいずれかの値を使用する必要があります。

- [FQDN]
- IP アドレス

プレゼンス ゲートウェイをワイルドカード証明書で使用するよう設定するには、指定したノードの場所の値は、ワイルドカード証明書で保護されたサブドメインの一部である必要があります。たとえば、ワイルドカード証明書がサブドメイン `*.imp.cisco.com` を保護する場合は、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドに *`server_name`*`.imp.cisco.com` というノード値を入力する必要があります。

（注） FQDN を入力する場合、それがサブジェクト共通名（CN）に一致するか、または証明書チェーンの Exchange サーバ リーフ証明書での [サブジェクトの代替名（Subject Alternative Name）] フィールドの保護されたホストのいずれかに一致する必要があります。FQDN は、要求を処理し、証明書を使用するアドレスに解決される必要があります。

IPv6 の場合は、入力する IPv6 アドレスが Exchange サーバ証明書の [SAN] フィールドに入力された値と一致する必要があります。

ステップ 7 IM and Presence サービスが Exchange サーバに接続するときに使用する偽装アカウントの名前を入力します。この形式は、ユーザ プリンシパル名（user@domain など）か、ダウンレベルのログオン名（domain\user など）のどちらかです。

ステップ 8 IM and Presence サービスが Exchange サーバに接続するのに必要な Exchange アカウント パスワードを入力します。確認のためもう一度パスワードを入力します。この値は、Exchange サーバで以前に設定したアカウントのアカウント パスワードと一致している必要があります。

ステップ 9 Exchange サーバとの接続に使用するポートを入力します。Exchange との IM and Presence サービスの統合は、セキュアな HTTP 接続を介して行われます。シスコは、ポート 443（デフォルト ポート）を使用し、それ以外のポートは変更しないことを推奨します。

ステップ 10 [保存（Save）] をクリックします。

ステップ 11 [Exchange サーバ（Exchange Server）] ステータスが次を示すグリーンになっていることを確認します。

- **Exchange の到達可能性（ping 可能）**
- **Exchange SSL の接続/認定の検証**

次の作業

Exchange プレゼンス ゲートウェイを設定後、次の点を確認します。

- IM and Presence サービスと Exchange サーバの接続は成功しましたか。[プレゼンス ゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [Exchange サーバ ステータス（Exchange Server Status）] 領域に接続ステータスが表示されます。修正が必要な場合は、「Exchange サーバの接続ステータスに関するトラブルシューティング」を参照してください。
- Exchange SSL 証明書チェーンのステータスは正しい（確認済み）ですか。[プレゼンス ゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [Exchange サーバ ステータス（Exchange Server Status）] 領域には、証明書のサブジェクト CN の不一致があるかどうかが示されます。修正が必要な場合は、「SSL 接続と証明書のステータスのトラブルシューティング」を参照してください。

SAN およびワイルドカード証明書のサポート

IM and Presence サービスでは、Microsoft Exchange との予定表のセキュアな統合のために、X.509 証明書を使用します。IM and Presence サービスでは、標準の証明書とともに、SAN およびワイルドカード証明書をサポートしています。

SAN証明書を使用すると、複数のホスト名とIPアドレスを単一の証明書で保護できるようになります。これを行うには、ホスト名、IP アドレス、またはその両方の一覧を [X509v3 サブジェクトの代替名（X509v3 Subject Alternative Name）] フィールドで指定します。

ワイルドカード証明書を使用すると、ドメインと無制限のサブドメインを提示できるようになります。これを行うには、ドメイン名にアスタリスク（*）を指定します。名前にはワイルドカード

文字 * を含めることができます。ワイルドカードは単一のドメイン名コンポーネントに対応します。たとえば、*.a.com は foo.a.com と一致しますが、bar.foo.a.com とは一致しません。

（注） SAN 証明書については、保護されたホストが [サブジェクトの代替名（Subject Alternative Name）] フィールドのホスト名/IP アドレスのフィールド一覧に含まれている必要があります。プレゼンス ゲートウェイの設定時に、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドは [サブジェクトの代替名（Subject Alternative Name）] フィールドに表示されている保護されたホストと完全に一致している必要があります。
ワイルドカードは、標準証明書の場合は [共通名（CN）（Common Name (CN)）] フィールドに、SAN 証明書の場合は [サブジェクトの代替名（Subject Alternative Name）] フィールドに使用することができます。

IM and Presence サービスと Microsoft Exchange の間のセキュアな証明書交換の設定

認証局サービスをインストールする方法

認証局（CA）は Exchange サーバ上で実行することもできますが、サードパーティの証明書交換のセキュリティを強化するために、別の Windows サーバを CA として使用することをお勧めします。

- Windows Server 2003 での CA のインストール, （35 ページ）
- Windows Server 2008 での CA のインストール, （36 ページ）

Windows Server 2003 での CA のインストール

はじめる前に

- CA をインストールするには、まず Windows Server 2003 コンピュータにインターネット 情報サービス（IIS）をインストールする必要があります。IIS は、Windows 2003 コンピュータにデフォルトでインストールされません。
- Windows Server ディスク 1 および SP1 ディスクがあることを確認します。

手順

ステップ 1 [スタート（Start）] > [コントロール パネル（□）] > [プログラムの追加と削除（Add or Remove Programs）] の順に選択します。

ステップ 2 [プログラムの追加と削除（Add or Remove Programs）] ウィンドウで、[Windows コンポーネントの追加/削除（Add/Remove Windows Components）] を選択します。

ステップ 3 [Windows コンポーネント（Windows Component）] ウィザードを完了します。

a) [Windows コンポーネント（Windows Component）] ウィンドウで、[サービスの照明（Certificate Services）] のチェックボックスをオンにし、ドメインのパートナーシップとコンピュータの名前変更の制約に関する警告が表示された場合 [はい（Yes）] をクリックします。

b) [CA タイプ（CA Type）] ウィンドウで、[スタンドアロン ルート CA（Stand-alone Root CA）] を選択し、[次へ（Next）] をクリックします。

c) [CA 識別情報（CA Identifying Information）] ウィンドウで、CA サーバの [共通名（Common Name）] フィールドにサーバの名前を入力します。DNS がない場合は、IP アドレスを入力し、[次へ（Next）] をクリックします。

（注） CA はサードパーティの権限であることを覚えておいてください。CA の共通名と、CSR の生成に使用された共通名を同じにすることはできません。

d) [証明書データベースの設定（Certificate Database Settings）] ウィンドウで、デフォルト設定を受け入れて [次へ（Next）] を選択します。

ステップ 4 インターネット 情報サービスを停止するように求められたら [はい（Yes）] をクリックします。

ステップ 5 Active Server Pages（ASP）を有効にするように求められたら [はい（Yes）] をクリックします。

ステップ 6 インストール手順が完了したら [終了（Finish）] をクリックします。

次の作業

CSR の作成：Windows Server 2003 の実行 , （38 ページ）

Windows Server 2008 での CA のインストール

手順

ステップ 1 [開始（Start）] > [管理ツール（Administrative Tools）] > [サーバ マネージャ（Server Manager）] を選択します。

ステップ 2 コンソール ツリーで、[ロール（Roles）] を選択します。

ステップ 3 [操作（Action）] > [ロールを追加（Add Roles）] を選択します。

ステップ 4 [Add Roles] ウィザードを完了します。

a) [始める前に（Before You Begin）] ウィンドウで、リストされている前提条件がすべて完了していることを確認し、[次へ（Next）] をクリックします。

b) [サーバ ロールを選択（Select Server Roles）] ウィンドウで、[Active Directory 証明書サービス（Active Directory Certificate Services）] チェックボックスをオンにして、[次へ（Next）] をクリックします。
c) [イントロダクション ウィンドウ（Introduction Window）] ウィンドウで、[次へ（Next）] をクリックします。
d) [ロール サービスを選択（Select Role Services）] ウィンドウで、次のチェックボックスをオンにし、[次へ（Next）] をクリックします。
   - Certificate Authority
   - Certificate Authority Web Enrollment
   - Online Responder

e) [セットアップ タイプを指定（Specify Setup Type）] ウィンドウで、[スタンドアロン（Standalone）] をクリックします。
f) [CA タイプを指定（Specify CA Type）] ウィンドウで、[ルート CA（Root CA）] をクリックします。
g) [プライベート キーのセット アップ（Set Up Private Key）] ウィンドウで、[新しいプライベート キーを作成（Create a new private key）] をクリックします。
h) [CA の暗号化を設定（Configure Cryptography for CA）] ウィンドウで、デフォルトの暗号化サービス プロバイダーを選択します。
i) [CA 名を設定（Configure CA Name）] ウィンドウで、CA を識別する共通名を入力します。
j) [有効期間を設定（Set Validity Period）] ウィンドウで、CA 用に生成された証明書の有効期間を設定します。
   （注） CA がここで指定した期日まで有効な証明書を発行します。
k) [証明書データベースを設定（Configure Certificate Database）] ウィンドウで、デフォルトの証明書データベースの場所を選択します。
l) [インストールの選択を確認（Confirm Installation Selections）] ウィンドウで、[インストール（Install）] をクリックします。
m) [インストール結果（Installation Results）] ウインドウで、すべてのコンポーネントに対して「インストールが完了しました（Installation Succeeded）」というメッセージが表示されていることを確認し、[閉じる（Close）] をクリックします。
   （注） Server Manager での役割の 1 つとして [Active Directory 証明書サービス（Active Directory Certificate Services）] が表示されます。

次の作業

CSR の作成：Windows Server 2008 の実行 , （39 ページ）

Microsoft Exchange サーバの IIS での CSR の生成

CSR の作成：Windows Server 2003 の実行

Exchange の IIS サーバで証明書署名要求（CSR）を作成する必要があります。作成した CSR は CA サーバによってその後署名されます。証明書の [サブジェクトの代替名（Subject Alternative Name (SAN)）] フィールドに値が入力されている場合、その値は証明書の共通名（CN）と一致している必要があります。

はじめる前に

自己署名証明書：必要に応じて証明書 CA サービスをインストールします。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット情報サービス（Internet Information Services）] を開きます。

a) [デフォルト Web サイト（Default Web Site）] を右クリックします。
b) [プロパティ（Properties）] を選択します。

ステップ 2 [ディレクトリ セキュリティ（Directory Security）] タブを選択します。

ステップ 3 [サーバ証明書] を選択します。

ステップ 4 [Webサーバの証明書（Web Server Certificate）] ウィンドウが表示されたら、[次へ（Next）] を選択します。

ステップ 5 [サーバ証明書（Server Certificate）] ウィザードを完了します。

a) **[サーバ証明書（Server Certificate）]** ウィンドウで、[新しい証明書を作成する（Create a New Certificate）] を選択し、[次へ（Next）] をクリックします。
b) [証明書の要求の送信方法（Delayed or Immediate Request）] ウィンドウで、[証明書の要求を作成して後で送信する（Prepare the request now, but send it later）] を選択し、[次へ（Next）] をクリックします。
c) [名前とセキュリティの設定（Name and Security Settings）] ウィンドウで、デフォルトの Web サイトの証明書名を受け入れ、ビット長に [1024] を選択し、[次へ（Next）] をクリックします。
d) [組織情報（Organization Information）] ウィンドウで、[組織（Organization）] フィールドに会社名を、[組織部門（Organizational Unit）] フィールドに会社の組織部門を入力し、[次へ（Next）] をクリックします。
e) [サイトの一般名（Your Site's Common Name）] ウィンドウで、Exchange サーバ のホスト名または IP アドレスを入力し、[次へ（Next）] をクリックします。

（注） ここで入力する IIS 証明書の共通名は、IM and Presence サービスでプレゼンス ゲートウェイを設定するときに使用されるため、接続先のホスト（URI または IP アドレス）と一致している必要があります。

f) [地理情報（Geographical Information）] ウィンドウで、地理情報を次のように入力し、[次へ（Next）] をクリックします。

- 国/地域（Country/Region）
- 都道府県（State/province）
- 市区町村（City/locality）

g) [証明書要求ファイル名（Certificate Request File Name）] ウィンドウで、証明書要求に対応する適切なファイル名を入力し、CSR を保存する場所のパスとファイル名を指定して、[次へ（Next）] をクリックします。

（注） CSR は拡張子（.txt）なしで保存してください。この CSR ファイルを後で探す必要があるため、保存場所を覚えておいてください。このファイルを開くには、必ずメモ帳を使用します。

h) [要求ファイルの概要（Request File Summary）] ウィンドウで、[要求ファイルの概要（Request File Summary）] ウィンドウに掲載されている情報が正しいことを確認し、[次へ（Next）] をクリックします。

i) [Web サーバ証明書の完了（Web Server Certificate Completion）] ウィンドウで、[終了（Finish）] を選択します。

次の作業

CA サーバ/認証局への CSR の提出, （40 ページ）

CSR の作成：Windows Server 2008 の実行

Exchange の IIS サーバで証明書署名要求（CSR）を作成する必要があります。作成した CSR は CA サーバによってその後署名されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット情報サービス マネージャ（Internet Information Services (IIS) Manager）] ウィンドウを開きます。

ステップ 2 IIS Manager の左側ペインの [接続（Connections）] 下で、[Exchange サーバ（Exchange Server）] を選択します。

ステップ 3 [サーバ証明書（Server Certificates）] をダブルクリックします。

ステップ 4 IIS Manager の右側ペインの [操作（Actions）] 下で、[証明書要求を作成（Create Certificate Request）] を選択します。

ステップ 5 [証明書要求（Request Certificate）] ウィザードを完了します。

a) [識別名プロパティ（Distinguished Name Properties）] ウィンドウで、次の情報を入力します。

- [共通名（Common Name）] フィールドに、Exchange サーバのホスト名または IP アドレスを入力します。

- [組織（Organization）] フィールドに、会社名を入力します。
- [組織部門（Organization Unit）] フィールドに、会社が属する組織部門を入力します。

b) 地理情報を次のように入力し、[次へ（Next）] をクリックします。

- 市区町村（City/locality）
- 都道府県（State/province）
- 国/地域（Country/Region）

（注） ここで入力する IIS 証明書の共通名は、IM and Presence サービスでプレゼンス ゲートウェイを設定するときに使用されるため、接続先のホスト（URI または IP アドレス）と一致している必要があります。

c) [暗号化サービス プロバイダ プロパティ（Cryptographic Service Provider Properties）] ウィンドウで、デフォルトの暗号化サービス プロバイダを承認し、ビット長に **2048** を選択し、[次へ（Next）] をクリックします。

d) [証明書要求ファイル名（Certificate Request File Name）] ウィンドウで、証明書要求に対応する適切なファイル名を入力し、[次へ（Next）] をクリックします。

（注） CSR は拡張子（.txt）なしで保存してください。この CSR ファイルを後で探す必要があるため、保存場所を覚えておいてください。このファイルを開くには、必ずメモ帳を使用します。

e) [要求ファイルのサマリ（Request File Summary）] ウィンドウで、情報が正しいことを確認し、[次へ（Next）] をクリックします。

f) [証明書要求の完了（Request Certificate Completion）] ウィンドウで、[終了（Finish）] をクリックします。

次の作業

CA サーバ/認証局への CSR の提出, （40 ページ）

CA サーバ/認証局への CSR の提出

IIS で Exchange 用に作成されるデフォルトの SSL 証明書には、Exchange サーバの完全修飾ドメイン名（FQDN）を使用し、IM and Presence サービスが信頼している認証局の署名を付けることを推奨します。この手順により、CA が Exchange IIS からの CSR に署名できます。次の手順を CA サーバで実行し、次の場所にある Exchange サーバの FQDN を設定してください。

- Exchange 証明書
- [Cisco Unified CM IM and Presence Administration] の Exchange プレゼンス ゲートウェイの [プレゼンス ゲートウェイ（Presence Gateway）] フィールド。

はじめる前に

Exchange サーバの IIS で CSR を生成します。

手順

ステップ 1 証明書要求ファイルを CA サーバにコピーします。

ステップ 2 次のいずれかの URL にアクセスします。

- Windows Server 2003 または Windows Server 2008：http://*locall_server*/certserv

または

- Windows 2003：http://127.0.0.1/certserv
- Windows 2008：http://127.0.0.1/certsrv

ステップ 3 [証明書要求（Request a certificate）] を選択します。

ステップ 4 [高度な証明書要求（Advanced certificate request）] をクリックします。

ステップ 5 [Base-64 で暗号化した CMC または PKCS #10 ファイルを使用して証明書要求を提出（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file）] または [Base-64 で暗号化した PKCS #7 ファイルを使用した更新要求を提出（Submit a renewal request by using a base-64-encoded PKCS #7 file）] を選択します。

ステップ 6 メモ帳などのテキスト エディタを使用して、作成した CSR を開きます。

ステップ 7 次の行から、
-----BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST-----

ステップ 8 CSR の内容を [証明書の要求（Certificate Request）] テキストボックスに貼り付けます。

ステップ 9 （任意）[証明書テンプレート（Certificate Template）] ドロップダウン リストのデフォルト値は [管理者（Administrator）]テンプレートです。このテンプレートでは、サーバの認証に適した有効な署名付き証明書が作成されることもあれば、作成されないこともあります。エンタープライズのルート CA がある場合は、[証明書テンプレート（Certificate Template）] ドロップダウン リストから Web サーバ証明書テンプレートを選択します。[Web サーバ（Web Server）]証明書テンプレートは表示されないことがあるため、CA 設定をすでに変更している場合、この手順は不要となることがあります。

ステップ 10 [送信（Submit）] をクリックします。

ステップ 11 [管理ツール（Administrative Tools）] ウィンドウで、[開始（Start）] > [管理ツール（Administrative Tools）] > [証明書（Certification）] > [認証局（Authority）] > [CA 名（CA name）] > [保留中の要求（Pending Request）] を選択して、[認証局（Certification Authority）] ウィンドウを開きます。[認証局（Certificate Authority）] ウィンドウの [保留中の要求（Pending Requests）] の下に、送信したばかりの要求が表示されます。

ステップ 12 要求を右クリックし、次の操作を実行します。

- [すべてのタスク（All Tasks）] を選択します。
- [問題（Issue）] を選択します。

ステップ 13 [発行済み証明書（Issued certificates）] を選択し、証明書が発行されていることを確認します。

次の作業

署名付き証明書のダウンロード, （42 ページ）

署名付き証明書のダウンロード

はじめる前に

自己署名証明書：CA サーバに証明書署名要求（CSR）を送信します。

サードパーティ証明書：認証局に CSR を要求します。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [認証局（Certification Authority）] を開きます。発行した証明書要求が [発行済み要求（Issued Requests）] 領域に表示されます。

ステップ 2 その要求を右クリックし、[開く（Open）] を選択します。

ステップ 3 [詳細（Details）] タブを選択します。

ステップ 4 [ファイルにコピー（Copy to File）] を選択します。

ステップ 5 [証明書のエクスポート（Certificate Export）] ウィザードが表示されたら、[次へ（Next）] をクリックします。

ステップ 6 [証明書のエクスポート（Certificate Export）] ウィザードを完了します。

a) [エクスポート ファイルの形式（Export File Format）] ウィンドウで、[Base-64 encoded X.509] を選択し、[次へ（Next）] をクリックします。

b) [エクスポートするファイル（File to Export）]ウィンドウで、証明書を保存する場所を入力し、証明書名に cert.cer を使用し、`c:\cert.cer` を選択します。

c) [証明書エクスポート ウィザードの完了（Certificate Export Wizard Completion）] ウィンドウで、サマリー情報を確認し、エクスポートが成功したことを確認して、[終了（Finish）] をクリックします。

ステップ 7 IM and Presence サービスの管理に使用するコンピュータに、cert.cer をコピーするか、FTP で送信します。

次の作業

署名付き証明書の Exchange IIS へのアップロード, （43 ページ）

署名付き証明書の Exchange IIS へのアップロード

署名付き証明書のアップロード：Windows 2003 の実行

ここでは、署名付き CSR を IIS にアップロードする手順を説明します。署名付き証明書をアップロードするには、IM and Presence サービスの管理に使用するコンピュータで次の手順を実行します。

はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット情報サービス（Internet Information Services）] を開きます。

ステップ 2 [インターネット情報サービス（Internet Information Services）] ウィンドウで次の手順を実行します。

a) [デフォルト Web サイト（Default Web Site）] を右クリックします。
b) [プロパティ（Properties）] を選択します。

ステップ 3 [デフォルト Web サイトのプロパティ（Default Web Site Properties）] ウィンドウで、次の手順を実行します。

a) [ディレクトリ セキュリティ（Directory Security）] タブを選択します。
b) [サーバ証明書] を選択します。

ステップ 4 [Web サーバ証明書（Web Server Certificate）] ウィザード ウィンドウが表示されたら、[次へ（Next）] をクリックします。

ステップ 5 [Web サーバ証明書（Web Server Certificate）] ウィザードを完了します。

a) [保留中の証明書要求（Pending Certificate Request）] ウィンドウで、[保留中の要求を処理して証明書をインストール（Process the pending request and install the certificate）] を選択し、[次へ（Next）] をクリックします。
b) [保留中の要求を処理（Process a Pending Request）] ウィンドウで、[参照（Browse）] をクリックして、証明書を検索し、適切なパスとファイル名に移動します。
c) [SSL ポート（SSL Port）] ウィンドウで、SSL ポートに 443 を入力し、[次へ（Next）] をクリックします。
d) [Web サーバ証明書の完了（Web Server Certificate Completion）] ウィンドウで、[終了（Finish）] をクリックします。

ヒント

証明書が信頼できる証明書ストアにない場合、署名付き CSR は信頼されません。信頼を確立するには、次の操作を実行します。

- [ディレクトリのセキュリティ（Directory Security）] タブで、[証明書を表示（View Certificate）] をクリックします。
- [詳細（Details）] > [ルート証明書をハイライト（Highlight root certificate）] を選択し、[表示（View）] をクリックします。
- ルート証明書の [詳細（Details）] タブを選択し、証明書をインストールします。

次の作業

ルート証明書のダウンロード, （45 ページ）

署名付き証明書のアップロード：Windows 2008 の実行

ここでは、署名付き CSR を IIS にアップロードする手順を説明します。署名付き証明書をアップロードするには、IM and Presence サービスの管理に使用するコンピュータで次の手順を実行します。

はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット情報サービス マネージャ（Internet Information Services (IIS) Manager）] ウィンドウを開きます。

ステップ 2 IIS Manager の左側ペインの [接続（Connections）] 下で、[Exchange サーバ（Exchange Server）] を選択します。

ステップ 3 [サーバ証明書（Server Certificates）] をダブルクリックします。

ステップ 4 IIS Manager の右側ペインの [操作（Actions）] 下で、[証明書要求を完了（Complete Certificate Request）] を選択します。

ステップ 5 [証明書認証局の応答を指定（Specify Certificate Authority Response）] ウィンドウで、次の操作を実行します。

a) 証明書を検索するには、省略記号（...）を選択します。
b) 正しいパスおよびファイル名に移動します。
c) 証明書のわかりやすい名前を入力します。
d) [OK] をクリックします。完了した証明書が証明書のリストに表示されます。

ステップ 6 [Internet Information Services（インターネット情報サービス）] ウィンドウで、次の手順を実行して証明書をバインドします。

a) [デフォルト Web サイト（Default Web Site）] を選択します。
b) IIS Manager の右側ペインの [操作（Actions）] 下で、[バインディング（Bindings）] を選択します。

ステップ 7 [サイト バインディング（Site Bindings）] ウィンドウで次の手順を実行します。

a) [https] を選択します。
b) [編集（Edit）] を選択します。

ステップ 8 [バインディングの編集（Edit Site Bindings）] ウィンドウで、次の手順を実行します。

a) [SSL 証明書] ドロップダウン リストから、直前に作成した証明書を選択します。証明書に適用される名前が表示されます。
b) [OK] をクリックします。

次の作業

ルート証明書のダウンロード, （45 ページ）

ルート証明書のダウンロード

はじめる前に

署名付き証明書を Exchange IIS にアップロードします。

手順

ステップ 1 CA サーバにログインし、Web ブラウザを開きます。

ステップ 2 使用している Windows プラットフォームの種類に応じ、次のいずれかの URL にアクセスします。

a) Windows Server 2003：http://127.0.0.1/certserv
b) Windows Server 2008：https://127.0.0.1/certsrv

ステップ 3 [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] をクリックします。

ステップ 4 [エンコーディング方法（Encoding Method）] で、[Base 64] を選択します。

ステップ 5 [CA 証明書のダウンロード（Download CA Certificate）] をクリックします。

ステップ 6 証明書（**certnew.cer**）をローカル ディスクに保存します。

ヒント

ルート証明書のサブジェクトの共通名（CN）がわからない場合は、外部の証明書管理ツールを使用して調べることができます。Windows オペレーティング システムで、拡張子が .cer の証明書ファイルを右クリックし、証明書のプロパティを開きます。

次の作業

IM and Presence サービス ノードへのルート証明書のアップロード, （46 ページ）

IM and Presence サービス ノードへのルート証明書のアップロード

はじめる前に

- 自己署名証明書：ルート証明書をダウンロードします。
- サードパーティ証明書：認証局にルート証明書を要求します。CA 署名付きのサードパーティ Exchange サーバ証明書がある場合は、証明書チェーン内のすべての CA 証明書を Cisco Unified Presence の信頼証明書（cup-trust）として IM and Presence サービスにアップロードする必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] の証明書インポート ツールを使用して、証明書をアップロードします。

証明書のアップロード方法	操作
[Cisco Unified CM IM and Presence Administration] の証明書インポート ツール 証明書インポート ツールは、信頼証明書を IM and Presence サービスにインストールするプロセスを簡略化するもので、証明書交換の主要な方法です。このツールでは、Exchange サーバのホストとポートを指定すると、サーバから証明書チェーンがダウンロードされます。承認すると、ツールが欠落している証明書を自動的にインストールします。 （注） この手順では、[Cisco Unified CM IM and Presence Administration] の証明書インポート ツールにアクセスし、設定する方法を 1 つ紹介します。特定のタイプの予定表統合のために Exchange プレゼンス ゲートウェイを設定する場合は、[Cisco Unified Presence Administration] 内の証明書インポート ツールのカスタマイズされたバージョンを表示することもできます（[Cisco Unified CM IM and Presence Administration] にログインし、[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択します）。	1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。 2 [システム（System）] > [セキュリティ（Security）] > [証明書インポート ツール（Certificate Import Tool）] を選択します。 3 証明書をインストールする証明書信頼ストアとして [IM and Presence(IM/P) Trust] を選択します。このストアには、Exchange の統合に必要なプレゼンス エンジン信頼証明書が保存されます。 4 Exchange サーバに接続するために、次のいずれかの値を入力します。 • IP アドレス • ホストネーム • [FQDN] この [ピア サーバ（Peer Server）] フィールドに入力する値は、Exchange サーバの IP アドレス、ホスト名、または FQDN と完全に一致している必要があります。 5 Exchange サーバとの通信に使用するポートを入力します。この値は、Exchange サーバの使用可能なポートと一致している必要があります。 6 [送信（Submit）] をクリックします。ツールが完了すると、テストごとに次の状態が報告されます。 • ピア サーバの到達可能性ステータス：IM and Presence サービスが Exchange サーバに到達（ping）できるかどうかを示します。Exchange サーバの接続ステータスに関するトラブルシューティングを参照してください。 • SSL 接続/証明書の確認ステータス：証明書インポート ツールが指定されたピア サーバから証明書をダウンロードすることに成功したかどうかと、IM and Presence サービスとリモート サーバの間にセキュアな接続が確立されたかどうかを示します。SSL 接続と証明書のステータスのトラブルシューティングを参照してください。

ステップ 2 証明書インポート ツールによって、証明書が欠落していることがわかった場合は（通常、Microsoft サーバでは CA 証明書が欠落します）、[Cisco Unified OS 管理証明書の管理（Cisco Unified OS Admin Certificate Management）] ウィンドウを使用して、手動で CA 証明書をアップロードします。

証明書のアップロード方法	操作
Cisco Unified IM and Presence Operating System Administration Exchange サーバが SSL/TLS ハンドシェイク中に CA 証明書を送信しない場合、それらの証明書は証明書インポート ツールではインポートできません。この場合、証明書管理ツールを使用して手動で欠落している証明書をインポートする必要があります（[Cisco Unified IM and Presence Operating System Administration] にログインします。[セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。	1 IM and Presence サービス ノードの管理に使用するコンピュータに、**certnew.cer** 証明書ファイルをコピーするか、FTP で送信します。 2 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。 3 [セキュリティ（Security）] > [証明書管理（Certificate Management）] を選択します。 4 [証明書リスト（Certificate List）] ウィンドウで、[証明書/証明書チェーンをアップロード（Upload Certificate/Certificate Chain）] を選択します。 5 [証明書/証明書チェーンをアップロード（Upload Certificate/Certificate Chain）] ダイアログボックスが開いたら、次の操作を実行します。 • [証明書名（Certificate Name）] ドロップダウン リストから、[cup-trust] を選択します。 • 拡張子を付けずにルート証明書の名前を入力します。 6 [参照（Browse）] をクリックし、[certnew.cer] を選択します。 7 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 3 証明書のインポート ツール（ステップ 1, （46 ページ））に戻り、すべてのステータス テストが成功したことを確認します。

ステップ 4 すべての Exchange 信頼証明書をアップロードしたら、Cisco Presence Engine と SIP プロキシ サービスを再起動します。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] の順に選択します。

ヒント

IM and Presence サービスでは、Exchange サーバの信頼証明書をサブジェクトの共通名（CN）あり/なしのどちらでもアップロードできます。

予定表統合の実現

予定表統合は、管理者によって個別またはユーザ グループごとに有効化されます。

（注） プレゼンス ゲートウェイが Cisco Unified Communications Manager に設定されていることを保障します。詳細については、Microsoft Exchange 統合向けのプレゼンス ゲートウェイの設定を参照してください。

個々のユーザの予定表統合を有効にする

手順

ステップ 1 **Cisco Unified CM Administration** のユーザ インターフェイスにログインします。

ステップ 2 [ユーザ管理（User Management）] > [エンド ユーザ（End User）] の順に選択します。

ステップ 3 [サービス設定（Service Settings）] 領域で、既存の会議情報を含めるためのチェックボックスをオンします（Cisco Unified Communications Manager IM and Presence サービス ノードで Exchange プレゼンス ゲートウェイを設定する必要があります）。

予定表の統合を一括して有効にする

手順

ステップ 1 Cisco Unified Communications Manager ノードで、[Cisco Unified CM Administration] ユーザ インターフェイスにログインします。

ステップ 2 予定表の統合は、次のウィンドウから一括して有効にできます。

a) [一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの挿入（Insert Users）]

b) [一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [クエリー（Query）]

c) [一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [カスタム ファイル（Custom File）]

ステップ 3 適切な [ユーザ（Users）] 領域で、ファイル名を選択します。

（注） 正しいファイル形式の [サンプル ファイルを表示（View Sample File）] をクリックします。

ステップ 4 [今すぐ実行（Run Immediately）] または [後から実行（Run Later）] をクリックします。

ステップ 5 [送信（Submit）] をクリックします。

（任意）Exchange Web サービスで送信される Exchange 予定表通知の頻度の設定

（注） この手順は、Microsoft Exchange サーバ 2007、2010、または 2013 を Exchange Web サービス（EWS）経由で統合する場合にのみ必要となります。

EWS Status Frequency パラメータは、Exchange サーバが IM and Presence サービス上のサブスクリプションを更新するまでにかかる間隔（分数）を指定します。このパラメータのデフォルト値は 60 分です。IM and Presence サービス上のプレゼンス エンジンがサブスクリプションを失ったことを60分（デフォルト）よりも短い間隔で検出する必要がある場合は、この間隔をデフォルト値より小さい値に変更してください。この間隔を短くすると、エラーの検出能力は向上しますが、それに伴って Exchange サーバおよび IM and Presence サービス ノードへの負荷も増加します。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。

ステップ 2 [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 3 [サーバ（Server）] ドロップダウン リストから、[IM and Presence サービス（IM and Presence Service）] ノードを選択します。

ステップ 4 [サービス（Service）] ドロップダウン リストから、[Cisco Presence Engine（アクティブ）（Cisco Presence Engine (Active)）] を選択します。

ステップ 5 [予定表設定（すべてのサーバに適用されるパラメータ）（Calendaring Configuration (Parameters that apply to all servers)）] 領域で、[EWS ステータス頻度（EWS Status Frequency）] フィールドのパラメータ値を編集します。このパラメータの最大値は1440分です。このパラメータのデフォルト値は 60 分です。

ステップ 6 [保存（Save）] をクリックします。

次の作業

予定表の統合はユーザ単位で行われるため、[EWS ステータス頻度（EWS Status Frequency）] パラメータの変更はその都度に更新されます。ただし、すべてのユーザについてパラメータの変更を有効にするために、Cisco Presence Engine を再起動することを推奨します。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [サービス アクティベーション（Service Activation）] を選択します。

（任意）Microsoft Exchange 通知ポートの設定

このトピックは、Cisco Presence Engine において Exchange サーバからの通知をネットワーク設定に固有の別のポートで受信する場合にのみ当てはまります。

EWS 統合では、HTTP 通知の受信にデフォルトで TCP ポートが使用されます。

はじめる前に

デフォルト ポート以外のポートを使用する場合は、必ず未使用のポートを割り当ててください。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。

ステップ 2 [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 3 [サーバ（Server）] ドロップダウン リストから、[IM and Presence サービス（IM and Presence Service）] ノードを選択します。

ステップ 4 [サービス（Service）] ドロップダウン リストから、[Cisco Presence Engine（アクティブ）（Cisco Presence Engine (Active)）] を選択します。

ステップ 5 [予定表設定（Calendaring Configuration）] 領域で、[Microsoft Exchange 通知ポート（Microsoft Exchange Notification Port）] フィールドのパラメータ値を編集し、[保存（Save）] をクリックします。

次の作業

一度にすべてのユーザのパラメータ変更を有効にするために、Cisco Presence Engine を再起動することを推奨します。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] の順に選択します。

ヒント

- ポートをデフォルト以外に変更した場合、そのユーザの Exchange サブスクリプションが更新されるまで、Cisco Presence Engine はユーザの既存の予定表情報（会議数、開始時刻、終了時刻など）を使用し続けます。Cisco Presence Engine がユーザの予定表の変更通知を受け取るまでに最大で 1 時間かかることがあります。
- 一度にすべてのユーザの変更を有効にするために、Cisco Presence Engine を再起動することを推奨します。

（任意）MicrosoftExchange予定表通知の接続時間の設定

デフォルトでは、Cisco Presence Engine は会議/取り込み中通知を発生から 50 秒で送信できます。ユーザ数が少ない場合は、この手順に示す方法に従って、この遅延を短くすることを推奨します。ただし、この手順は任意です。ネットワーク設定に特有の理由から接続時間を変更する必要がある場合にのみ実行してください。

はじめる前に

この手順では、フィールド値（秒数）を「割り当てられたユーザの最大数/100」に設定します。たとえば、ユーザの最大数が 1000 である場合、オフセット範囲は 10 秒となります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。

ステップ 2 [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 3 [サーバ（Server）] ドロップダウン リストから、[IM and Presence サービス（IM and Presence Service）] ノードを選択します。

ステップ 4 [サービス（Service）] ドロップダウン リストから、[Cisco Presence Engine（アクティブ）（Cisco Presence Engine (Active)）] を選択します。

ステップ 5 [予定表設定（Calendaring Configuration）] 領域で、[予定表スプレッド（Calendar Spread）] フィールドのパラメータ値を編集します。このパラメータの最大値は59秒です。会議の開始または終了が 1 分を超えて遅れた場合、会議の開始/終了カウンタおよび通知に影響します。このパラメータのデフォルト値は 50 です。

ステップ 6 [保存（Save）] をクリックします。

次の作業

[予定表スプレッド（Calendar Spread）] パラメータの変更は、ユーザ単位で予定表の統合が発生するたびに付加的に更新されます。ただし、すべてのユーザについてパラメータの変更を有効にするために、Cisco Presence Engine を再起動することを推奨します。**Cisco Unified IM and Presence Serviceability** にログインします。[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）] の順に選択します。

ヒント 多数のユーザが会議に出入りすると、大量の通知イベントが発生し、一部の通知に最大で数分の遅れが生じることがあります。

他の Microsoft Exchange 予定表パラメータ

[Cisco Unified CM IM and Presence Administration] の [サービス パラメータ（Service Parameters）] ウィンドウで設定できる Exchange の予定表パラメータには、他にも 3 つあります。

- [Exchange タイムアウト（秒）（Exchange Timeout (seconds)）]：Exchange サーバに対するリクエストがタイムアウトするまでの秒単位の時間。
- [Exchange キュー（Exchange Queue）]：リクエスト キューの長さ。
- [Exchange スレッド（Exchange Threads）]：Exchange リクエストにサービスを提供するために使用されるスレッドの数。

注意 これらのパラメータのデフォルト設定を変更しないことをお勧めします。変更すると、Exchange の統合に悪影響が及ぶ可能性があります。サポートについては、Cisco Technical Assistance Center（TAC）にお問い合わせください。

第 6 章

Exchange 予定表統合のトラブルシューティング

Exchange サーバの接続ステータスに関するトラブルシューティング

Exchange Web サービス（EWS）による予定表の統合を行うために Exchange プレゼンス ゲートウェイを設定後、Exchange サーバ接続のステータスが [Cisco Unified CM IM and Presence Administration] ウィンドウに表示されます（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択）。[プレゼンス ゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [Exchange サーバ ステータス（Exchange Server Status）] 領域には、IM and Presence サービスと Exchange サーバ間の接続に関するステータスがレポートされます。

（注） 1 台以上の EWS サーバを追加、更新、または削除できます（上限はありません）。ただし、[プレゼンス ゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [Exchange サーバ ステータス（Exchange Server Status）] 領域は、設定した最初の 10 台までの EWS サーバのステータスのみを検証し、レポートするように作成されています。

テスト	ステータスの説明と推奨される処置
Exchange の到達可能性（ping 可能）	IM and Presence サービスは Exchange サーバに正常に到達（ping）できました。

テスト	ステータスの説明と推奨される処置
Exchange の到達可能性（到達不可能）	IM and Presence サービス は Exchange サーバに ping を送信できませんでした。フィールド値が誤っているか、またはお客様のネットワークに何らかの問題（ケーブル接続など）があるため、サーバが到達不可になっていると考えられます。 これを解決するには、ネットワークを介して Exchange サーバに到達できるように [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに適切な値（FQDN または IP アドレス）が設定されていることを確認します。UI では、[プレゼンス ゲートウェイ（Presence Gateway）] フィールド値を件名 CN 値にする必要はありません。 Exchange サーバとの接続に問題がある場合は、[Cisco Unified CM IM and Presence Administration] の [システム トラブルシュータ（System Troubleshooter）] も参照のうえ、推奨される解決策を実行してください。[診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）] を選択します。

SSL 接続と証明書のステータスのトラブルシューティング

Exchange Web サービス（EWS）による予定表の統合を行うために Exchange プレゼンス ゲートウェイを設定すると、SSL 接続/証明書の確認ステータスが [Cisco Unified CM IM and Presence Administration] ウィンドウに表示されます（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] を選択）。[プレゼンス ゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [Exchange サーバ ステータス（Exchange Server Status）] 領域には、証明書のサブジェクト CN の不一致または SAN の不一致があるかどうかが示されます。

（注） *1* 台以上の EWS サーバを追加、更新、または削除できます（上限はありません）。ただし、[プレゼンス ゲートウェイ（Presence Gateway）] ウィンドウの [トラブルシュータ（Troubleshooter）] は、設定した最初の 10 台までの EWS サーバのステータスのみを検証し、レポートするよう作られています。

テスト	ステータスの説明と推奨される処置
SSL 接続/証明書の確認成功	Exchange サーバとの SSL 接続が IM and Presence サービスによって確認されました。[表示（View）] をクリックして、証明書の詳細を表示します。

テスト	ステータスの説明と推奨される処置
SSL 接続/証明書の確認に失敗：証明書がチェーンに見つからない （注） この手順では、カスタマイズされた証明書のインポート ツールのビューについて説明します。接続のステータスを確認するだけの場合は、ツールには確認済みのステータスが示されますが、その場合は [保存（Save）]することはできません。	

テスト	ステータスの説明と推奨される処置
	Exchange サーバとのセキュアな接続を確立するために IM and Presence サービスで必要な 1 つ以上の証明書が欠落しています。証明書ビューアを使用すると、欠落している証明書の詳細を表示できます。 欠落している証明書を表示するには、証明書ビューアを使用して次の手順を実行します。 **1** [設定（Configure）] を選択して証明書ビューアを開きます。 **2** [証明書チェーンを受け入れ（Accept Certificate Chain）] チェックボックスをオンにします。 **3** [保存（Save）] をクリックします。 **4** 証明書チェーンの詳細が表示されます。ステータスが [見つかりません（Missing）] になっている証明書を書き留めておきます。 **5** 証明書ビューアを閉じます。 証明書チェーンを完成させるには、次の手順を実行します。 **1** 欠落している証明書ファイルを Exchange サーバからダウンロードします。 **2** IM and Presence サービスを管理する目的に使用しているコンピュータに欠落している証明書ファイルをコピーまたはFTP転送します。 **3** [Cisco Unified IM and Presence OS Administration] を使用して、欠落している必要な証明書をアップロードします。 **トラブルシューティングのヒント** • 証明書ビューアに証明書が表示されない場合は、欠落している証明書をExchangeサーバから手動でダウンロードしてインストールし、[Cisco Unified IM and Presence OS Administration] で次のようにアップロードする必要があります。 ◦ [Cisco Unified IM and Presence OS Administration] とユーザ インターフェイスにログインし、証明書をアップロードして証明書チェーンを完了します。 ◦ [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイス下の [プレゼンス ゲートウェイ設定（Presence Gateway Configuration）] ウィンドウに戻り、証明書ビューアを再度開き、証明書チェーン内のすべての証明書のステータスが [確認済み（Verified）] になっていることを確認します。 • Exchange の信頼証明書をアップロード後、Cisco Presence Engine を再起動する必要があります。

テスト	ステータスの説明と推奨される処置
	• [Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。 • [ツール（Tools）] > [サービス アクティベーション（Service Activation）] を選択します。これによって予定表の接続が影響を受ける可能性があることに注意してください。 • [設定（Configure）] または [表示（View）] を選択して証明書チェーン ビューアを開始します。IM and Presence サービス が Exchange サーバからダウンロードした証明書チェーンに問題がある場合は、[設定（Configure）] ボタンが表示されます。たとえば、前述したように証明書が欠落しているなどです。証明書チェーンをインポートし、確認すると、[SSL 接続/証明書の確認（SSL Connection / Certificate Verification）] ステータスが [確認済み（Verified）] に更新され、[設定（Configure）] ボタンの代わりに [表示（View）] ボタンが表示されます。
SSL 接続/証明書の確認失敗 - 件名 CN が一致しない	[プレゼンス ゲートウェイ（Presence Gateways）] フィールドの値は、必ず証明書チェーン内のリーフ証明書の件名 CN 値と一致している必要があります。これは、[プレゼンス ゲートウェイ（Presence Gateways）] フィールドに正しい値を入力することで解決できます。 [プレゼンス ゲートウェイ（Presence Gateways）] フィールドの値が正しいことを次の手順で確認してください。 **1** [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに正しい件名 CN 値を再入力します。IM and Presence サービスでは、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値を使用して、サーバに ping を送信します。入力したホスト（FQDN または IP アドレス）は、IIS 証明書のサブジェクトの CN と完全に一致している必要があります。 **2** [保存（Save）] をクリックします。 **ヒント** [設定（Configure）] または [表示（View）] を選択して証明書チェーン ビューアを開始します。Exchange サーバからダウンロードされた証明書チェーンに問題がある場合は、[設定（Configure）] ボタンが表示されます。たとえば、前述したように証明書が欠落しているなどです。証明書チェーンをインポートし、確認すると、[SSL 接続/証明書の確認（SSL Connection / Certificate Verification）] ステータスが [確認済み（Verified）] に更新され、[設定（Configure）] ボタンの代わりに [表示（View）] ボタンが表示されます。

テスト	ステータスの説明と推奨される処置
SSL 接続/証明書の確認失敗 - SAN が一致しない	[プレゼンス ゲートウェイ（Presence Gateway）] フィールド値は、証明書チェーンのリーフ証明書のサブジェクトの代替名（SAN）値のいずれかと一致する必要があります。これは、[プレゼンス ゲートウェイ（Presence Gateways）] フィールドに正しい値を入力することで解決できます。 [プレゼンス ゲートウェイ（Presence Gateways）] フィールドの値が正しいことを次の手順で確認してください。 **1** [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに正しい SAN 値を再入力します。IM and Presence サービスでは、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値を使用して、サーバに ping を送信します。入力したホスト（FQDN または IP アドレス）は、証明書のサブジェクトの代替名のいずれかのエントリと完全に一致する必要があります。 **2** [保存（Save）] をクリックします。 **ヒント** [設定（Configure）] または [表示（View）] を選択して証明書チェーン ビューアを開始します。Exchange サーバからダウンロードされた証明書チェーンに問題がある場合は、[設定（Configure）] ボタンが表示されます。たとえば、前述したように証明書が欠落しているなどです。証明書チェーンをインポートし、確認すると、[SSL 接続/証明書の確認（SSL Connection / Certificate Verification）] ステータスが [確認済み（Verified）] に更新され、[設定（Configure）] ボタンの代わりに [表示（View）] ボタンが表示されます。

テスト	ステータスの説明と推奨される処置
SSL 接続/証明書の確認に失敗 - 不正な証明書	証明書に不正な情報が含まれているため、その証明書が無効になっています。 通常、この問題は、証明書が必要な件名 CN と一致しているものの公開キーとは一致していない場合に発生します。これは、Exchange サーバが証明書を再生成したが、IM and Presence サービス ノードに古い証明書が保持されたままの場合に見られる現象です。 これを解決するには、次の操作を実行します。 • ログを選択して、このエラーの原因を特定します。 • エラーの原因が不正な署名である場合は、古い証明書を [Cisco Unified IM and Presence OS Administration] の [IM and Presence サービス（IM and Presence Service）] から削除し、新しい証明書を [Cisco Unified IM and Presence OS Administration] にアップロードします。 • このエラーの原因がサポートされていないアルゴリズムの場合は、サポートされているアルゴリズムを含む新しい証明書を Cisco Unified IM and Presence OS の管理にアップロードする必要があります。
SSL 接続/証明書の確認に失敗：ネットワークエラー	応答なしによるタイムアウトなどのネットワーク上の問題が発生したために、IM and Presence サービスが SSL 接続を確認できません。 Exchangeサーバへのネットワークの接続性を検証し、適切なIPアドレスとポート番号でExchangeサーバに接続できることを確認することを推奨します。
SSL 接続/証明書の確認に失敗	不明確な原因または IM and Presence サービスが到達可能性テストを実行できないことにより、検証が失敗しました。 デバッグ ログ ファイルを参照して詳細を確認することを推奨します。

MicrosoftExchangeの統合に影響することが確認されている問題

ここでは、Microsoft Exchange サーバ 2007、2010、および 2013 に共通または固有の既知の問題について説明します。

予定表の統合に関する規模の上限

Cisco Unified Communications Manager IM and Presence サービス と Exchange の予定表の統合は、予定表プレゼンスを購読するユーザの最大 X% と予定表の同時移行（会議への同時出席または同時退席など）を行うユーザの最大 Y% について検証されています。特定の Cisco Unified Presence のリリースに関するパーセンテージ値については、表 1 を参照してください。

表 *5*：特定の *Cisco Unified Presence* リリースの規模の上限

ソフトウェア リリース	予定表プレゼンスを購読するユーザの %	予定表の同時移行を実行するユーザの %
8.5(1)	50	30
8.5(2) 以降	100	50

ユーザが Microsoft Exchange サーバ間で移動すると、予定表ステータスが更新されない

問題

Exchange 管理者が、Exchange 統合内の Exchange サーバ間でユーザを移動すると、そのユーザの予定表ステータスの変更は更新されません。

原因

これは、ユーザがサーバ間を移動したときに Exchange サーバが通知しないために起こる現象です。

ソリューション

IM and Presence サービスの管理者またはユーザは、Exchange 管理者がユーザを Exchange サーバ間で移動した後に、そのユーザの予定表統合を無効にしてから、もう一度有効にする必要があります。

LDAP ユーザの削除が IM and Presence サービスにレプリケートされるまで 24 時間以上かかる

問題

LDAP からユーザを削除すると、そのユーザのステータス変更が Cisco Unified Communications Manager で非アクティブとなり、それ以降、クライアント アプリケーションでのユーザ認証は失

敗します。ただし、Cisco Unified Communications Manager が LDAP からの変更を同期すると、（同期を強制した管理者または特定の時間に発生するようにスケジュールした管理者によって）同期後 24 時間はユーザは削除されないことがテストによって確認されています。

IM and Presence サービスの Cisco Sync Agent は、ユーザが削除されるまでユーザのステータス変更を同期しません。それまで、ユーザは Cisco Unified Communications Manager 上に存在し続け、すべての IM and Presence サービス機能（Exchange 予定表購読を含む）のライセンスは 24 時間そのユーザに与えられたままになります。このような遅延が生じるということは、LDAP から削除される前に Cisco Jabber にログインしていたユーザは、自動的にログアウトされないことを意味します。ユーザの既存の予定表ステータス（利用可能、ビジー）は、ユーザがクライアントからログアウトするまで IM and Presence サービスのそのユーザに保持されます。

原因

これは、Cisco Unified Communications Manager が設定され、LDAP 認証が使用される場合に見られる現象です。ユーザが LDAP から削除されると、そのユーザの予定表購読は少なくとも 24 時間は IM and Presence サービス上に設定されたままの状態で更新されます。

ソリューション

ユーザが LDAP から削除されると、IM and Presence サービスが Exchange の予定表購読をただちに終了し、ユーザをクライアント アプリケーションからログアウトできるよう、そのユーザのライセンスを手動で削除することができます。手動で削除しなければ、24 時間の遅延が生じることがあります。

Microsoft Exchange Server URL にカレンダーの訳語が含まれているかどうかの確認

予定表の統合をローカライズする場合は、Exchange サーバの URL に Calendar の訳語が含まれていることを確認してください。

手順

ステップ 1 IM and Presence Service と Cisco Unified Communications Manager に同じ言語ロケールをインストールします（ロケール インストーラを読み込む）。 IM and Presence Service にロケールをインストー

ルする方法については、「（オプション）予定表と統合する場合の多言語サポートの設定」を参照してください。

ステップ 2 IM and Presence サービス ノードを再起動し、**[Cisco Unified CM IM and Presence Administration]** ユーザ インターフェイスにログインします。

ステップ 3 予定表について別のロケールをサポートしている既存の Exchange プレゼンス ゲートウェイを検索し、削除します（[プレゼンスゲートウェイ（Presence > Gateways）]を選択）。

ステップ 4 新しい Exchange プレゼンス（Outlook）ゲートウェイを追加します。 [新規追加（Add New）]をクリックします。

ステップ 5 データベース（pebackendgateway テーブル）で、インストールした言語ロケールに 'localecalendarname' 属性が含まれていることを確認します。

ステップ 6 IM and Presence サービスの両方にロケールをインストール後、ユーザ ロケールを設定します。必要に応じて、Cisco Unified Communications Manager のユーザ ロケールを切り替えます。