IM and Presence Service リリース 14 および SU 向け Microsoft Outlook 予定表統合

初版：2021 年 3 月 31 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/

目 次

第 1 章 はじめに 1

はじめに 1

新機能および変更された機能に関する情報 1

対象読者 2

本書の構成 2

表記法 3

マニュアルの入手方法およびテクニカル サポート 3

第 2 章 新機能および変更された機能に関する情報 5

新機能および変更された機能に関する情報 5

第 3 章 概要 7

概要 7

展開 7

Exchange Web サービス 7

IM and Presence Service での Microsoft Outlook の予定表ステータス 8

制約事項と制限 8

第 4 章 予定表統合の計画 11

前提条件 11

設定に関する考慮事項 13

Exchange Web サービスによる Microsoft Exchange Server との統合 13

Exchange Server の管理の役割とアクセス許可 14

Exchange Server の統合向けのプレゼンスゲートウェイの設定 15

Exchange Web サービス統合の既知の問題 15
セキュリティに関する考慮事項 15
Windows セキュリティポリシーの設定 15
詳細情報 16

第 5 章 予定表統合のための Microsoft Exchange の設定 17
Exchange Web サービスによる Microsoft Exchange 2007 の設定 17
Windows セキュリティポリシーの設定 18
Windows セキュリティ設定の確認 18
サービスアカウントにローカルでサインインするアクセス許可をユーザーに付与する 19
Windows Server 2003 での Microsoft Exchange 2007 の設定 19
Windows Server 2008 での Microsoft Exchange 2007 の設定 20
サーバーレベルでの偽装権限の設定 20
サービスアカウントの Active Directory サービス拡張権限の設定 21
サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与 22
サービスアカウントおよびユーザーメールボックスへの偽装権限の付与 23
Microsoft Exchange 2007 アカウントでのアクセス許可の確認 24
Exchange Web サービスによる Microsoft Exchange 2010 および 2013 の設定 25
Windows セキュリティポリシーの設定 26
Windows セキュリティ設定の確認 26
Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定 27
Exchange 2013 または 2016 の特定のユーザーまたはグループに Exchange の偽装権限を設定 29
Microsoft Exchange 2010 アカウントのアクセス許可の確認 30
Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認 32
Exchange 仮想ディレクトリでの認証の有効化 34
Windows Server 2003 を実行する Exchange 2007 での認証の有効化 34
Windows Server 2008 を実行する Exchange 2010、2013 または 2016 の認証の有効化 35

第 6 章 Microsoft Exchange の設定 37
予定表統合のための Microsoft Exchange の構成 37

Microsoft Exchange 2007 設定タスクフロー 38
Windows セキュリティ設定の確認 39
Windows Server 2003 での Microsoft Exchange 2007 の設定 40
Windows Server 2008 での Microsoft Exchange 2007 の設定 40
サーバーレベルでの偽装権限の設定 41
サービスアカウントの Active Directory サービス拡張権限の設定 42
サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与 43
サービスアカウントおよびユーザーメールボックスへの偽装権限の付与 44
Microsoft Exchange 2007 アカウントでのアクセス許可の確認 44
Windows Server 2003 を実行する Exchange 2007 での認証の有効化 45
Microsoft Exchange 2010/2013/2016 の設定タスクフロー 46
Windows セキュリティ設定の確認 47
Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定 48
Exchange 2013 または 2016 の特定のユーザーまたはグループに Exchange の偽装権限を設定 49
Microsoft Exchange 2010 アカウントのアクセス許可の確認 51
Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認 53
Windows Server 2008 を実行する Exchange 2010、2013 または 2016 の認証の有効化 55
SAN およびワイルドカード証明書のサポート 55
Exchange Server の証明書の設定タスクフロー 56
Windows Server 2003 での CA のインストール 57
Windows Server 2008 での CA のインストール 58
証明書署名要求の生成：Windows Server 2003 を実行している場合 59
証明書署名要求の生成：Windows Server 2008 を実行している場合 61
CA サーバー/認証局への証明書署名要求の送信 62
署名付き証明書のダウンロード 63
署名付き証明書のアップロード：Windows 2003 を実行している場合 64
署名付き証明書のアップロード：Windows 2008 を実行している場合 66
ルート証明書のダウンロード 67
IM and Presence Service ノードへのルート証明書のアップロード 67

第 7 章 **Microsoft Office 365 の設定** 75

Microsoft Office 365 予定表統合 75

Microsoft Office 365 予定表統合のタスクフロー 75

予定表統合のための Office 365 アクセス許可の設定 76

Microsoft IM and Presence Service への証明書のアップロード 76

第 8 章 **IM and Presence Service の設定** 79

IM and Presence 予定表統合のタスクフロー 79

プレゼンスゲートウェイの設定 80

認証タイプ OAuth の Office 365 事前構成 81

Office 365 統合のプル間隔の設定 82

Exchange 統合のサービスパラメータの設定 83

Cisco Presence Engine の再起動 85

LDAP 同期ユーザーの予定表の有効化 85

機能グループテンプレートへの予定表統合の追加 86

LDAP ディレクトリ同期への機能グループテンプレートの追加 86

予定表統合の一括有効化 87

ユーザーごとの予定表統合の有効化 88

第 9 章 **予定表統合のための IM and Presence Service の設定** 89

Microsoft Exchange との統合向けのプレゼンスゲートウェイの設定 89

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 90

SAN およびワイルドカード証明書のサポート 92

IM and Presence Service と Microsoft Exchange 間のセキュアな証明書交換の設定 93

認証局サービスのインストール方法 93

Windows Server 2003 での CA のインストール 93

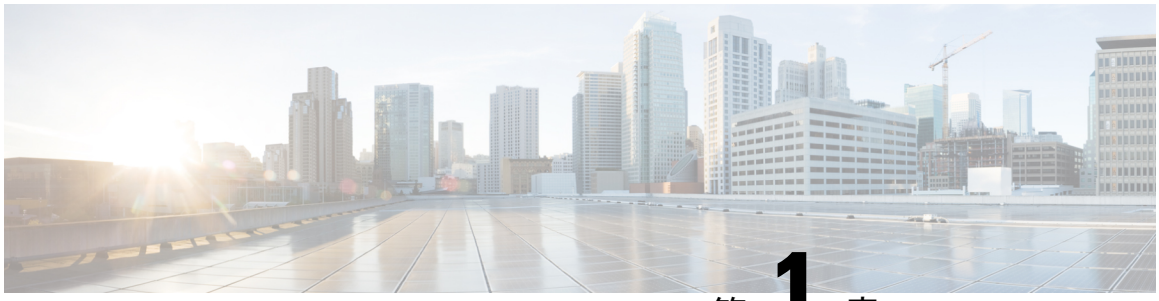
Windows Server 2008 での CA のインストール 94

Microsoft Exchange Server の IIS での証明書署名要求の生成 95

証明書署名要求の生成：Windows Server 2003 を実行している場合 95

証明書署名要求の生成：Windows Server 2008 を実行している場合 97
CA サーバー/認証局への証明書署名要求の送信 98
署名付き証明書のダウンロード 99
署名付き証明書の Exchange IIS へのアップロード 100
署名付き証明書のアップロード：Windows 2003 を実行している場合 100
署名付き証明書のアップロード：Windows 2008 を実行している場合 101
ルート証明書のダウンロード 103
IM and Presence Service ノードへのルート証明書のアップロード 103
予定表統合の有効化 109
個人ユーザーに対する予定表統合の有効化 109
予定表統合の一括有効化 110
[任意] Exchange Web サービスで送信される Exchange カレンダー通知の頻度の設定 110
[任意] Microsoft Exchange 通知ポートの設定 111
[任意] Microsoft Exchange カレンダー通知の接続時間の設定 112
その他の Microsoft Exchange カレンダーパラメータ 113
不在ステータス 114

第 10 章 **Exchange カレンダー統合のトラブルシューティング** 117
Exchange Server の接続ステータスに関するトラブルシューティング 117
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 118
Microsoft Exchange の統合に影響することが確認されている問題 126
予定表の統合に関する規模の上限 126
ユーザーが Microsoft Exchange Server 間を移動すると予定表ステータスが更新されない 126
LDAP ユーザーの削除が IM and Presence Service にレプリケートされるまで 24 時間以上かかる 127
Microsoft Exchange Server URL に「Calendar」の訳語が含まれることの確認 127



第 1 章

はじめに

- はじめに （1 ページ）
- 新機能および変更された機能に関する情報 （1 ページ）
- 対象読者 （2 ページ）
- 本書の構成 （2 ページ）
- 表記法 （3 ページ）
- マニュアルの入手方法およびテクニカル サポート （3 ページ）

はじめに

IM and Presence Service の予定表統合では、Microsoft Outlook の予定表および会議のステータスを IM and Presence の在席ステータスに組み込むことができます。

新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Unified Communications Manager* と *IM and Presence Service* の新機能と変更された動作

機能または変更	説明	参照先	日付
リリース 14 のマニュアルの初回リリース	—	—	2021 年 3 月 31 日
リリース 14SU1 のマニュアルの初回リリース	—	—	2021 年 10 月 27 日
リリース 14SU2 のマニュアルの初回リリース	—	—	2022 年 6 月 16 日

対象読者

この出版物は、IM and Presence Service 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ーを対象としています。

本書の構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
1	はじめに （1 ページ）	この章には、本書の構成、対象読者、このガイドの目的に関する情報が含まれています。
2	概要 （7 ページ）	この章では、IM and Presence Service 向けの Microsoft Outlook 予定表統合機能の概要が説明されています。
3	新機能および変更された機能に関する情報 （1 ページ）	この章では、新機能および変更された機能に関する情報について説明します。
4	予定表統合の計画 （11 ページ）	この章には、予定表の統合を計画するための、前提条件に関する情報が含まれています。
5	Microsoft Exchange の設定 （37 ページ）	この章は、Outlook の予定表統合のためにオンプレミスの Microsoft Exchange Server に接続する場合にのみ参照してください。この章では、統合のために Exchange Server を設定する方法について説明します。
6	Microsoft Office 365 の設定 （75 ページ）	この章は、Outlook の予定表統合のためにクラウドでホストされている Office 365 サーバーに接続する場合にのみ参照してください。この章では、統合のために Office 365 サーバーを構成する方法について説明します。
7	IM and Presence Service の設定 （79 ページ）	この章は、Outlook の予定表統合のために IM and Presence Service を設定するために参照してください。オンプレミスの Exchange Server かクラウドでホストされている Office 365 サーバーのどちらに接続しているかに関係なく、この章を使用してください。
8	Exchange カレンダー統合のトラブルシューティング （117 ページ）	この章では、トラブルシューティング タスクと一般的な問題の修正について説明します。

表記法

このマニュアルでは、以下の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザーが入力するテキストは**太字**で記載されます。
イタリック体フォント	文書のタイトル、新規用語、強調する用語、およびユーザーが値を指定する関数は、イタリック体で示しています。
`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` フォントで示しています。

（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 「問題解決に役立つ情報」です。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。

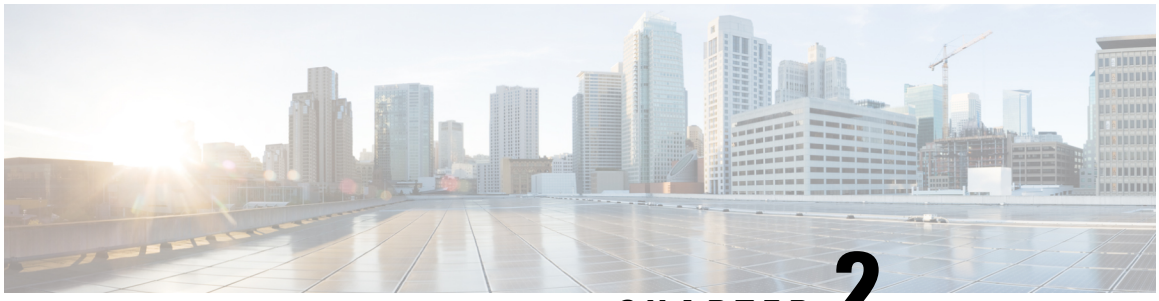
注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

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、毎月更新される『更新情報』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。



CHAPTER 2

新機能および変更された機能に関する情報

• 新機能および変更された機能に関する情報, on page 5

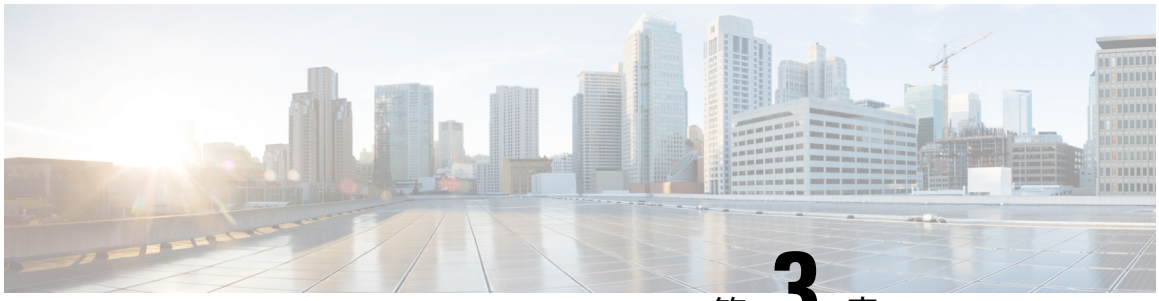
新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

***Table 2: Unified Communications Manager* と *IM and Presence Service* の新機能と変更された動作**

機能または変更	説明	参照先	日付
リリース 14 のマニュアルの初回リリース	—	—	2021 年 3 月 31 日
リリース 14SU1 のマニュアルの初回リリース	—	—	2021 年 10 月 27 日
リリース 14SU2 のマニュアルの初回リリース	—	—	2022 年 6 月 16 日

新機能および変更された機能に関する情報



第 3 章

概要

- 概要 （7 ページ）
- 展開 （7 ページ）
- IM and Presence Service での Microsoft Outlook の予定表ステータス （8 ページ）
- 制約事項と制限 （8 ページ）

概要

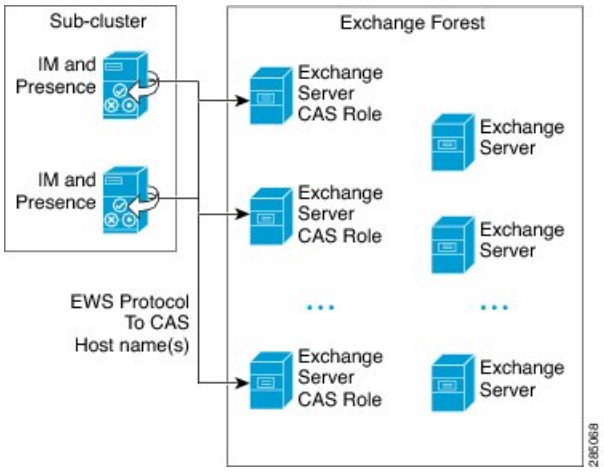
Microsoft Outlook の IM and Presence Service との予定表統合では、Microsoft Outlook の予定表/会議のステータスを IM and Presence Service サーバーの在席ステータスに組み込むことができます。この機能は、IM and Presence Service をオンプレミス Microsoft Exchange Server またはホスト型 Office 365 サーバーに接続することによって実現することができます。

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うことができます。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ーにいくつかの責任を移動します。

図 *1 : EWS* を介した *IM and Presence Service* との *Microsoft Exchange* 統合



IM and Presence Service での Microsoft Outlook の予定表ステータス

Microsoft Exchange または Office 365 を介した Microsoft Outlook の IM and Presence Service との統合では、Microsoft Outlook の予定表/会議のステータスを IM and Presence Service の在席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 Service 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 Service のユーザーの在席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 *3 :* 予定表ステータスに基づく集約された在席ステータス

Microsoft Outlook のステータス	IM and Presence Service のステータス
空き時間/仮の予定	応答可能
取り込み中	会議中
不在[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。

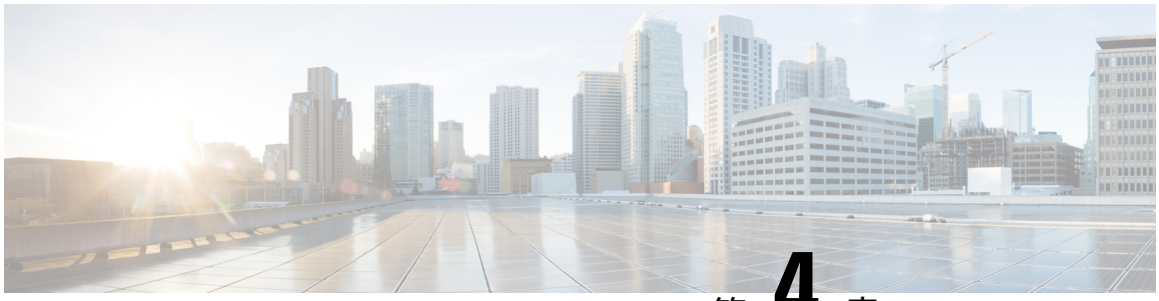
[2] Microsoft Outlook Web Access（OWA）2010。

制約事項と制限

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

- 1 台または複数の EWS サーバーを追加、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の設定（Presence Gateway Configuration）] ウィンドウの [トラブルシューティングツール（Troubleshooter）] は、設定した最初の 10 台の EWS サーバーのステータスのみを検証し、レポートするように設計されています。
- IM and Presence Service 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 サーバー（CAS）またはサーバーに配置されていることが前提となっています。
- Exchange Server または Office 365 サーバーをプレゼンスゲートウェイとして設定すると、ローカルの Outlook から受信したミーティングがある場合、Jabber クライアントは「会議中」ステータスを設定できません。「会議中」ステータスは、プレゼンスゲートウェイ経由でのみ取得できます。プレゼンスゲートウェイが何らかの理由でダウンした場合、クライアントは「会議中」ステータスを設定できません。

（注） 「会議中」ステータスを設定するには、プレゼンスゲートウェイのサービスを復元する必要があります。



第 4 章

予定表統合の計画

- 前提条件 （11 ページ）
- 設定に関する考慮事項 （13 ページ）
- セキュリティに関する考慮事項 （15 ページ）
- 詳細情報 （16 ページ）

前提条件

Microsoft Outlook 予定表の IM and Presence Service へ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ます。

表 *4*: 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 2012 サービスパック（Standard） • Windows Server 2016 サービスパック（Standard） • Windows Server 2019 サービスパック（Standard）
Cisco Unified Communications Manager	標準展開では、Cisco Unified Communications Manager と IM and Presence Service のリリースバージョンが一致する必要があります。 リリース 11.5(1)SU4 では、IM and Presence 集中展開機能により、テレフォニークラスタとは異なるバージョンを使用して IM and Presence クラスタを展開できます。

コンポーネント	互換性のあるバージョン
IM and Presence Service	標準展開では、Cisco Unified Communications Manager と IM and Presence Service のリリースバージョンが一致する必要があります。 リリース 11.5(1)SU4 では、IM and Presence 集中展開機能により、テレフォニークラスタとは異なるバージョンを使用して IM and Presence クラスタを展開できます。
Microsoft Exchange Server 2007	Microsoft Exchange 2007（SP1）サービスパック
Microsoft Exchange Server 2010	Microsoft Exchange 2010（SP1）サービスパック
Microsoft Exchange Server 2013	Microsoft Exchange 2013（SP1）サービスパック
Microsoft Exchange Server 2016	Microsoft Exchange 2016
Microsoft Exchange Server 2019	Microsoft Exchange 2019
Microsoft Office 365	ホスト型 Office 365 サーバーの展開の詳細については、Microsoft のドキュメントを参照してください。
Active Directory	• Windows Server 2012 を使用した Active Directory 2012 • Windows Server 2016 を使用した Active Directory 2016 • Windows Server 2019 を使用した Active Directory 2019 （注） Active Directory 内のユーザ名は、Cisco Unified Communications Manager に定義されたユーザー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ー	証明書を作成するためには、これらのいずれかが必要。 （注） IM and Presence Service との Microsoft Exchange 統合は、RSA 1024 または 2048 ビットキーと SHA1 および SHA256 署名アルゴリズムを使用する証明書をサポートします。

Exchange Server 2007、2010、2013 および 2016 では、Exchange Web サービス（EWS）をサポートしています。

設定に関する考慮事項

この本には、オンプレミスの Microsoft Exchange 展開またはホスト型 Office 365 展開のために、IM and Presence Service と Microsoft Outlook 間の予定表統合を設定する方法を説明する設定タスクが含まれています。次の表を使用して、展開に使用する章を決定します。

表 *5 : Microsoft* 展開の設定タスク

Microsoft 展開	完了する設定の章
Microsoft Exchange（2007、2010、2013、2016）	• Microsoft Exchange 2007 設定タスクフロー（38 ページ）または Microsoft Exchange 2010/2013/2016 の設定タスクフロー（46 ページ） • IM and Presence 予定表統合のタスクフロー（79 ページ）
Microsoft Office 365	• Microsoft Office 365 予定表統合のタスクフロー（75 ページ） • IM and Presence 予定表統合のタスクフロー（79 ページ）

Exchange Web サービスによる Microsoft Exchange Server との統合

Microsoft Exchange Server 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 Server に予定表を統合できます。

Exchange 統合のために EWS のプレゼンスゲートウェイを **Cisco Unified CM IM and Presence Service Administration** ユーザー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 台または複数の EWS サーバーを追加、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の設定（Presence Gateway Configuration）] ウィンドウの [トラブルシューティングツール（Troubleshooter）] は、設定した最初の 10 台の EWS サーバーのステータスのみを検証し、レポートするように設計されています。
- EWS サーバーゲートウェイは、最初の EWS サーバーゲートウェイに対して設定したログイン情報（アカウント名とパスワード）を共有します。1 つの EWS サーバーゲートウェイのログイン情報を変更すると、設定されたすべての EWS ゲートウェイのログイン情報もそれに準じて変更されます。

- 1 つまたは複数の EWS サーバーを追加、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 サーバーを連続して追加した場合は、Cisco Presence Engine を一度だけ再起動してすべての変更を同時に反映できます。

Exchange Server の管理の役割とアクセス許可

Exchange Web サービス（EWS）では、すべてのユーザー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 Server 2007

呼び出し元が Exchange Server 2007 上の別のユーザーの E メールアカウントにアクセスするために、EWS の統合で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、指定したユーザー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 サーバー（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 を使用してユーザーの E メールアカウントを偽装するアクセス許可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ー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。

個々のユーザーのアクセス 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 Server 2010 および 2013

Microsoft Exchange Server 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アクセス許可を付与し、ユーザー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、ユーザーが管理者またはスーパーユーザーであるかエンドユーザー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、その役割に固有のアクセス許可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ー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アクセス許可を継承します。たとえば、Exchange 組織内の任意のユーザー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ーではない一般ユーザーの場合、管理役割割り当てポリシーは、ユーザー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ーに **ApplicationImpersonation** 役割を割り当てると、アカウントが組織内のユーザーを偽装し、そのユーザー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ーを対象として絞り込むことができます。

（注） RBAC では、Exchange Server 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 Server の統合向けのプレゼンスゲートウェイの設定

多数のユーザーをサポートするには（EWS での予定表の統合が有効になった状態で）、IM and Presence Service は複数の CAS サーバー間で 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 Service は、EWS 経由で一部の CAS に接続でき、次のラウンドロビン方式を使用して遭遇するトラフィック負荷をサポートします。

- 最初にユーザーの予定表サブスクリプションを有効にしたときには、そのユーザー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。
- ユーザーへの割り当ては、そのユーザーの予定表サブスクリプションが失敗するまで保持されます。
- ユーザーの予定表サブスクリプションが失敗した場合は、対象 CAS ホストのプールから CAS サーバーが再度割り当てられます。

Exchange Web サービス統合の既知の問題

- 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 カレンダー統合のトラブルシューティング （117 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 （126 ページ）」を参照してください。

セキュリティに関する考慮事項

Windows セキュリティポリシーの設定

IM and Presence Service の Microsoft Exchange との統合では、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 Service は、NTLMv1 と NTLMv2 の両方の Windows 統合認証をサポートし、NTLMv2 がデフォルトとして使用されます。

NTLMv2 応答のみを送信するように **Lan Manager 認証レベル**を設定します。Windows ドメインコントローラで LM と NTLM を拒否すると、ドメインに NTLMv2 認証が適用されます。

（注） IM and Presence Service は NTLMv2 セッションセキュリティをサポートしていません。メッセージの機密性と整合性は、安全な http（https）によって確保されます。

詳細情報

Cisco Unified Communications Manager および IM and Presence Service 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

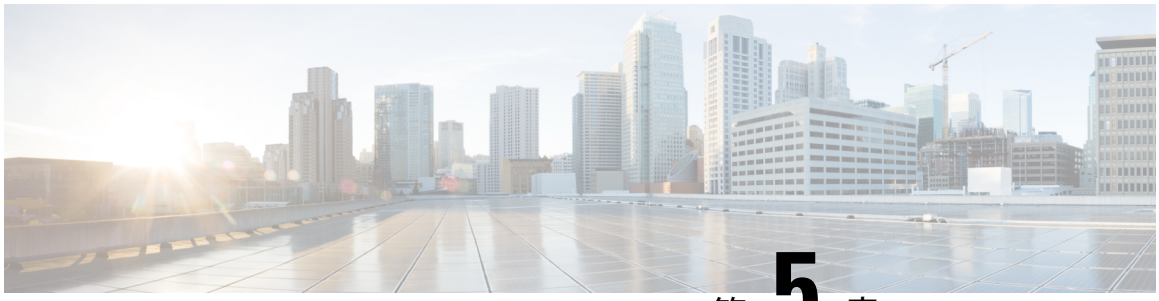
http://technet.microsoft.com/en-us/library/bb124558.aspx

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 5 章

予定表統合のための Microsoft Exchange の設定

- Exchange Web サービスによる Microsoft Exchange 2007 の設定 （17 ページ）
- Exchange Web サービスによる Microsoft Exchange 2010 および 2013 の設定 （25 ページ）
- Exchange 仮想ディレクトリでの認証の有効化 （34 ページ）

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

はじめる前に

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

Exchange Server 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。詳細手順については、次の URL で Exchange Server 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

- Windows セキュリティ設定の確認 （18 ページ）
- サービスアカウントにローカルでサインインするアクセス許可をユーザーに付与する （19 ページ）
- サーバーレベルでの偽装権限の設定 （20 ページ）
- サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与 （22 ページ）
- サービスアカウントおよびユーザーメールボックスへの偽装権限の付与 （23 ページ）
- Microsoft Exchange 2007 アカウントでのアクセス許可の確認 （24 ページ）

ヒント IM and Presence Service では、Exchange Server への接続時にそのアカウントにログインするため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

IM and Presence Service の Microsoft Exchange との統合では、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 Service は、NTLMv1 と NTLMv2 の両方の Windows 統合認証をサポートし、NTLMv2 がデフォルトとして使用されます。

NTLMv2 応答のみを送信するように **Lan Manager 認証レベル**を設定します。Windows ドメインコントローラで LM と NTLM を拒否すると、ドメインに NTLMv2 認証が適用されます。

（注） IM and Presence Service は NTLMv2 セッションセキュリティをサポートしていません。メッセージの機密性と整合性は、安全な http（https）によって確保されます。

Windows 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ーで、**[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）] > [セキュリティのオプション（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ベースクライアント（セキュアなRPCを含む）のサーバー向け最小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ーを再起動します。

（注） 再起動は、セキュリティポリシー設定の変更が実行されたサーバーでのみ必要です。

サービスアカウントにローカルでサインインするアクセス許可をユーザーに付与する

ユーザー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 Server を Windows Authorization Access Group のメンバー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ー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 表示専用管理者の役割を委任されたサービスアカウントを使用して Exchange Server 2007 ユーザー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）] から **[ローカルポリシー（Local Policies）]** > **[ユーザー権利の割り当て（User Rights Assignments）]** の順に選択します。

ステップ 3 コンソールの右ペインで [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 [ユーザー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。

ステップ 5 [名前の確認（Check Names）] を選択し、指定されたユーザー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。

次のタスク

サーバーレベルでの偽装権限の設定 （20 ページ）

Windows Server 2008 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange 表示専用管理者の役割を委任されたサービスアカウントを使用して Exchange Server 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 Server で [ドメインコントローラセキュリティ設定（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）]** から **[ローカルポリシー（Local Policies）]** > **[ユーザー権利の割り当て（User Rights Assignments）]** の順に選択します。

ステップ 7 コンソールの右ペインで [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選択されていることを確認します。

ステップ 9 [ユーザー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、指定されたユーザー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 ユーザー 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、ユーザープリンシパル名（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。

次のタスク

サーバーレベルでの偽装権限の設定 （20 ページ）

サーバーレベルでの偽装権限の設定

次の手順のコマンドを使用すると、サーバーレベルで偽装権限を付与することができます。また、データベース、ユーザー、連絡先レベルでもアクセス許可を付与することもできます。

はじめる前に

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

```
Get-OrganizationConfig
```

を次の文字列に置き換えます。

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

ここで、*ServerName* は Exchange Server 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
```

- ユーザーの 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、ユーザープリンシパル名（UPN）を使用してユーザー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、サーバー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
```

次のタスク

サービスアカウントの Active Directory サービス拡張権限の設定 （21 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

始める前に

これらのアクセス許可は、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（クライアント アクセス サーバー（CAS）上）。

- 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 サーバーが CAS サーバー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ーの Ex2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。
- このアクセス許可は、[Active Directoryサイトとサービス（Active Directory Sites and Services）] または [Active Directory ユーザーとコンピュータ（Active Directory Users and Computers）] ユーザー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）のサーバー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-Impersonation
```

例

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

次のタスク

サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与 （22 ページ）

サービスアカウントおよびユーザー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ーメールボックスに Send As 権限を付与するには、次の手順に従います。

（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ー 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 Receive-As
```

例

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

次のタスク

サービスアカウントおよびユーザーメールボックスへの偽装権限の付与 （23 ページ）

サービスアカウントおよびユーザー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ーメールボックスに偽装権限を付与するには、次の手順に従います。

（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メールボックスストアに偽装権限を付与します。

構文

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

例

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

（注） IM and Presence Service では、Exchange Server への接続時にそのアカウントにログインするため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。

次のタスク

Microsoft Exchange 2007 アカウントでのアクセス許可の確認 （24 ページ）

Microsoft Exchange 2007 アカウントでのアクセス許可の確認

Exchange 2007 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザー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 2007 では、アクセス許可がメールボックスに伝播されるまでに多少時間がかかります。

手順

ステップ 1 Exchange Server 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 サーバー（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 サーバーの [プロパティ（Properties）] を表示し、[セキュリティ（Security）] タブで次の点を確認します。「」

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アクセス許可が（チェックされているボックスにより）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ー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 Server 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。

次のタスク

Windows Server 2003 を実行する Exchange 2007 での認証の有効化 （34 ページ）

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 サーバー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。

はじめる前に

Exchange 2010 および 2013 サーバーを IM and Presence Service と統合するために Exchange Web サービス（EWS）を使用する前に、Exchange Server にスロットリング 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 Service との統合を正常に機能させるために必要な値です。

これらは、Exchange Server 2010 および 2013 向けのコマンドと設定です。

表 *6 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリング ポリシー値で十分でした。ただし、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 に引き上げることを推奨します。

表 *7: Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

パラメータ[1]	推奨設定値：**Exchange Server 2013** および **2016**
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**無制限**
EwsRechargeRate	900000

[1] これらは、Exchange Server 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 Server 2010
Exchange Server 2013

Windows セキュリティポリシーの設定

IM and Presence Service の Microsoft Exchange との統合では、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 Service は、NTLMv1 と NTLMv2 の両方の Windows 統合認証をサポートし、NTLMv2 がデフォルトとして使用されます。

NTLMv2 応答のみを送信するように **Lan Manager 認証レベル**を設定します。Windows ドメインコントローラで LM と NTLM を拒否すると、ドメインに NTLMv2 認証が適用されます。

（注） IM and Presence Service は NTLMv2 セッションセキュリティをサポートしていません。メッセージの機密性と整合性は、安全な http（https）によって確保されます。

Windows 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ーで、**[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）] > [セキュリティのオプション（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ベースクライアント（セキュアなRPCを含む）のサーバー向け最小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ーを再起動します。

（注） 再起動は、セキュリティポリシー設定の変更が実行されたサーバーでのみ必要です。

Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定

特定のユーザーまたはユーザーグループに 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。

これらは、Exchange Server 2010 向けのコマンドと設定です。Exchange Server 2013 を使用している場合は、Exchange 2013 または 2016 の特定のユーザーまたはグループに Exchange の偽装権限を設定 （29 ページ） の手順に従います。

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、他のユーザーアカウントを偽装する権限を指定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 Server のすべてのアカウントを偽装する権限が、*Exch2010* アカウントに対して与えられます。

構文

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

例

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

ステップ 5 New-ThrottlingPolicy コマンドを実行し、下の表の推奨値を使用して新しいスロットリングポリシーを作成します。

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
```

表 *8 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：**Exchange Server 2010**
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリング ポリシー値で十分でした。ただし、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 に引き上げることを推奨します。

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 で使用し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
```

次のタスク

Microsoft Exchange 2010 アカウントのアクセス許可の確認 （30 ページ）

関連トピック

Exchange Server 2010
Exchange Server 2013

Exchange2013または2016の特定のユーザーまたはグループにExchangeの偽装権限を設定

特定のユーザーまたはユーザーグループに 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。

これらは、Exchange Server 2013 または 2016 向けのコマンドと設定です。Exchange Server 2010 を使用している場合は、Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定 （27 ページ） の手順に従います。

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、他のユーザーアカウントを偽装するアクセス許可を指定サービスアカウント（*Ex2013* 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:Ex2013@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 Server のすべてのアカウントを偽装するアクセス許可が、*Exch2013* アカウントに対して与えられます。

構文

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

例

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

ステップ 5 New-ThrottlingPolicy コマンドを実行し、下の表の推奨値を使用して新しいスロットリングポリシーを作成します。

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100  -EwsMaxSubscriptions:NULL
-EwsCutoffBalance 3000000 -EwsMaxBurst 300000 -EwsRechargeRate 900000
```

例

```
New-ThrottlingPolicy -Name IMP_ThrottlingPolicy -EwsMaxConcurrency 100
-EwsMaxSubscriptions unlimited -EwsCutoffBalance 3000000 -EwsMaxBurst 300000
-EwsRechargeRate 900000
```

表 *9 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

パラメータ[1]	推奨設定値：**Exchange Server 2013** および **2016**
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**無制限**
EwsRechargeRate	900000

[1] これらは、Exchange Server 2013 で変更できる唯一の EWS パラメータです。

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 で使用し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 ex2013 -ThrottlingPolicy IMP_ThrottlingPolicy
```

次のタスク

Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認 （32 ページ）

Microsoft Exchange 2010 アカウントのアクセス許可の確認

Exchange 2010 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユー

ザー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 では、アクセス許可がメールボックスに伝播されるまでに多少時間がかかります。

これらは、Exchange Server 2010 向けのコマンドです。Exchange Server 2013 を使用している場合は、Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認 （32 ページ）の手順に従います。

手順

ステップ 1 Active Directory サーバーで、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 Server 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) コマンド出力で、次のように、指定アカウントに対する役割「ApplicationImpersonation」の割り当てが示されることを確認します。

コマンド出力の例

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	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。

コマンド出力の例

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

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 EMS 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
```

表 *10 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリングポリシー値で十分でした。ただし、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 に引き上げることを推奨します。

次のタスク

Exchange 仮想ディレクトリでの認証の有効化 （34 ページ）

関連トピック

Exchange Server 2010
Exchange Server 2013

Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認

Exchange 2013 または 2016 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザー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。アクセス許可がメールボックスに伝播されるまでには多少の時間がかかります。

（注） Exchange Server 2010 を使用している場合は、Microsoft Exchange 2010 アカウントのアクセス許可の確認 （30 ページ） の手順に従います。

手順

ステップ 1 Active Directory サーバーで、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 Server 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) コマンド出力で、次のように、指定アカウントに対する役割「ApplicationImpersonation」の割り当てが示されることを確認します。

コマンド出力の例

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	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。

コマンド出力の例

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

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 EMS 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 IMP_ThrottlingPolicy | Format-List | findstr ^Ews
```

表 *11 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

パラメータ[1]	推奨設定値：Exchange Server 2013 および 2016
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**無制限**
EwsRechargeRate	900000

パラメータ[1]	推奨設定値：**Exchange Server 2013** および **2016**
[1] これらは、Exchange Server 2013 で変更できる唯一の EWS パラメータです。	

ステップ 6 ThrottlingPolicy が Exchange アカウントに関連付けられていることを確認します。

```
Get-ThrottlingPolicyAssociation -Identity ex2013
```

Exchange 仮想ディレクトリでの認証の有効化

始める前に

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 Server 2007、2010 および 2013 の EWS 仮想ディレクトリ（/EWS）で有効にする必要があります。

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

手順

ステップ 1 [管理ツール（Administrative Tools）] からインターネットインフォメーションサービス（Internet Information Services）を開き、サーバーを選択します。

ステップ 2 [サイト（Web Sites）] を選択します。

ステップ 3 [既定の 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 [認証とアクセス制御（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）] の下で、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にする（Enable anonymous access）]

ステップ 8 [認証済みアクセス（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。

- **Integrated Windows Authentication**
- **Basic Authentication (password is sent in clear text)**

ステップ 9 [OK] をクリックします。

次のタスク

Exchange Server の証明書の設定タスクフロー （56 ページ）

Windows Server 2008 を実行する Exchange 2010、2013 または 2016 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インフォメーションサービス（Internet Information Services）を開き、サーバーを選択します。

ステップ 2 [サイト（Web Sites）] を選択します。

ステップ 3 [既定の 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（Anonymous Authentication）]
- [Windows 認証（Windows Authentication）] および [Basic 認証（Basic Authentication）]（両方またはどちらか）

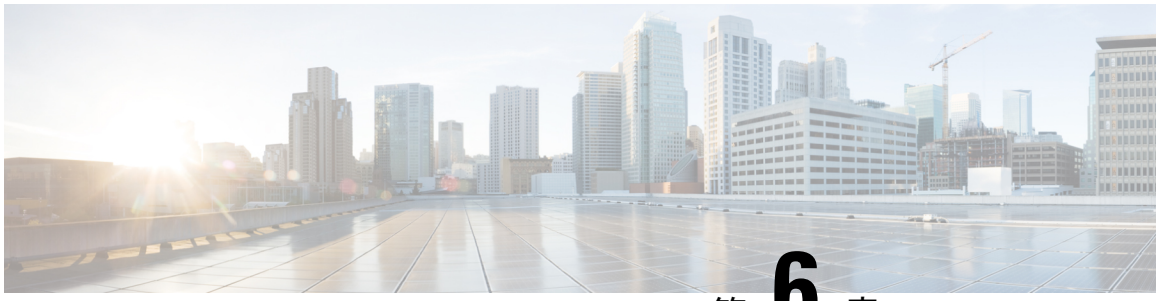
ステップ 7 適切に設定するには、[操作（Actions）] カラムで [有効にする/無効にする（Enable/Disable）] リンクを使用します。

次のタスク

Exchange Server の証明書の設定タスクフロー （56 ページ）

関連トピック

Outlook Web App の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の SSL を有効または無効にする



第 6 章

Microsoft Exchange の設定

- 予定表統合のための Microsoft Exchange の構成 （37 ページ）
- Microsoft Exchange 2007 設定タスクフロー （38 ページ）
- Microsoft Exchange 2010/2013/2016 の設定タスクフロー （46 ページ）
- SAN およびワイルドカード証明書のサポート （55 ページ）
- Exchange Server の証明書の設定タスクフロー （56 ページ）

予定表統合のための Microsoft Exchange の構成

オンプレミスの Microsoft Exchange Server を展開している場合は、この章の手順を実行して、IM and Presence Service と Microsoft Outlook 間の予定表統合のために Microsoft Exchange を設定します。IM and Presence Service は、次の各 Microsoft 展開タイプと統合できます。

表 *12 : IM and Presence Service* との予定表統合のための *Microsoft Exchange* の構成

Microsoft Exchange の展開	Microsoft の構成
Microsoft Exchange 2007	Microsoft Exchange 2007 設定タスクフロー （38 ページ）
Microsoft Exchange 2010、2013 または 2016	Microsoft Exchange 2010/2013/2016 の設定タスクフロー （46 ページ）

（注） テストは、Microsoft Exchange Server のメジャーバージョンを使用して実行されています。これらのメジャーバージョンの他のすべての累積更新プログラムで互換性が維持されるはずです。たとえば、Exchange 2013 について言及する場合、IM and Presence Service は、Exchange 2013 でリリースされたすべての累積更新プログラム (CU) をサポートしていることを示しています。

Microsoft Exchange 2007 設定タスクフロー

これらのタスクを完了して、IM and Presence Service と Outlook の予定表を統合するための Microsoft Exchange 2007 展開を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Windows セキュリティ設定の確認 （18 ページ）	NTLM 要件などの Windows セキュリティ設定を確認します。
ステップ 2	ローカルでサインインする権限をユーザーに付与するように Exchange Server を設定します。 • Windows Server 2003 での Microsoft Exchange 2007 の設定 （19 ページ） • Windows Server 2008 での Microsoft Exchange 2007 の設定 （20 ページ）	（注） Exchange の偽装を正常に機能させるには、すべての Microsoft Exchange Server を Windows Authorization Access Group のメンバー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ー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。
ステップ 3	サーバーレベルでの偽装権限の設定 （20 ページ）	データベース、ユーザー、連絡先レベルでアクセス許可を付与します。
ステップ 4	サービスアカウントの Active Directory サービス拡張権限の設定 （21 ページ）	これらのアクセス許可は、クライアントアクセスサーバー（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。
ステップ 5	サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与 （22 ページ）	サービスアカウントおよびユーザーメールボックスに Send As 権限を付与します。
ステップ 6	サービスアカウントおよびユーザーメールボックスへの偽装権限の付与 （23 ページ）	サービスアカウントおよびユーザーメールボックスへの偽装権限の付与
ステップ 7	Microsoft Exchange 2007 アカウントでのアクセス許可の確認 （24 ページ）	Exchange 2010 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザーのアカウン

	コマンドまたはアクション	目的
		トを偽装したりできることを確認する必要があります。
ステップ 8	Windows Server 2003 を実行する Exchange 2007 での認証の有効化 （34 ページ）	Exchange Server で認証を有効にします。
ステップ 9	Exchange Server の証明書の設定タスクフロー （56 ページ）	このタスクフローを完了して、Microsoft Exchange 展開用の証明書を設定します。

Windows 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ーで、**[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）] > [セキュリティのオプション（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ベースクライアント（セキュアな RPC を含む）のサーバー向け最小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ーを再起動します。

（注） 再起動は、セキュリティポリシー設定の変更が実行されたサーバーでのみ必要です。

Windows Server 2003 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange 表示専用管理者の役割を委任されたサービスアカウントを使用して Exchange Server 2007 ユーザー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）] から **[ローカルポリシー（Local Policies）] > [ユーザー権利の割り当て（User Rights Assignments）]** の順に選択します。

ステップ 3 コンソールの右ペインで [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 [ユーザー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。

ステップ 5 [名前の確認（Check Names）] を選択し、指定されたユーザー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。

次のタスク

サーバーレベルでの偽装権限の設定 （20 ページ）

Windows Server 2008 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange 表示専用管理者の役割を委任されたサービスアカウントを使用して Exchange Server 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 Server で [ドメインコントローラセキュリティ設定（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）]** から **[ローカルポリシー（Local Policies）] > [ユーザー権利の割り当て（User Rights Assignments）] の順に選択します。**

ステップ 7 コンソールの右ペインで [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選択されていることを確認します。

ステップ 9 [ユーザー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、指定されたユーザー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 ユーザー 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、ユーザープリンシパル名（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。

次のタスク

サーバーレベルでの偽装権限の設定 （20 ページ）

サーバーレベルでの偽装権限の設定

次の手順のコマンドを使用すると、サーバーレベルで偽装権限を付与することができます。また、データベース、ユーザー、連絡先レベルでもアクセス許可を付与することもできます。

はじめる前に

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

  Get-OrganizationConfig

  を次の文字列に置き換えます。

  Get-ExchangeServer -Identity *ServerName*

  ここで、*ServerName* は Exchange Server 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
  ```

- ユーザーの 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、ユーザープリンシパル名（UPN）を使用してユーザー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、サーバー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
```

次のタスク

サービスアカウントの Active Directory サービス拡張権限の設定 （21 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

始める前に

これらのアクセス許可は、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（クライアント アクセス サーバー（CAS）上）。

- 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 サーバーが CAS サーバー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ーの Ex2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。
- このアクセス許可は、[Active Directoryサイトとサービス（Active Directory Sites and Services）] または [Active Directory ユーザーとコンピュータ（Active Directory Users and Computers）] ユーザー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）のサーバー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-Impersonation
```

例

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

次のタスク

サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与 （22 ページ）

サービスアカウントおよびユーザー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ーメールボックスに Send As 権限を付与するには、次の手順に従います。

（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ー 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 Receive-As
```

例

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

次のタスク

サービスアカウントおよびユーザーメールボックスへの偽装権限の付与 （23 ページ）

サービスアカウントおよびユーザー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ーメールボックスに偽装権限を付与するには、次の手順に従います。

（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メールボックスストアに偽装権限を付与します。

構文

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

例

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

（注） IM and Presence Service では、Exchange Server への接続時にそのアカウントにログインするため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。

次のタスク

Microsoft Exchange 2007 アカウントでのアクセス許可の確認 （24 ページ）

Microsoft Exchange 2007 アカウントでのアクセス許可の確認

Exchange 2007 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザー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 2007 では、アクセス許可がメールボックスに伝播されるまでに多少時間がかかります。

手順

ステップ 1 Exchange Server 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 サーバー（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 サーバーの [プロパティ（Properties）] を表示し、[セキュリティ（Security）] タブで次の点を確認します。「」

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アクセス許可が（チェックされているボックスにより）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ー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 Server 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。

次のタスク

Windows Server 2003 を実行する Exchange 2007 での認証の有効化 （34 ページ）

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

手順

ステップ 1 [管理ツール（Administrative Tools）] からインターネット インフォメーション サービス（Internet Information Services）を開き、サーバーを選択します。

ステップ 2 [サイト（Web Sites）] を選択します。

ステップ 3 [既定の 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 [認証とアクセス制御（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）] の下で、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にする（Enable anonymous access）]

ステップ 8 [認証済みアクセス（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。

- **Integrated Windows Authentication**
- **Basic Authentication (password is sent in clear text)**

ステップ 9 [OK] をクリックします。

次のタスク

Exchange Server の証明書の設定タスクフロー （56 ページ）

Microsoft Exchange 2010/2013/2016 の設定タスクフロー

これらのタスクを完了して、IM and Presence Service と Outlook の予定表を統合するための Microsoft Exchange 2010、2013 または 2016 展開を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Windows セキュリティ設定の確認 （47 ページ）	Windows 統合認証（NTLM）の Windows セキュリティ設定を確認します。
ステップ 2	使用するリリースの Exchange アクセス許可を設定します。 • Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定 （27 ページ） • Exchange 2013 または 2016 の特定のユーザーまたはグループに Exchange の偽装権限を設定 （29 ページ）	特定のユーザーまたはユーザーグループに Exchange の偽装権限を設定する
ステップ 3	使用するリリースのアクセス許可を確認します。 • Microsoft Exchange 2010 アカウントのアクセス許可の確認 （30 ページ）	Exchange 2010 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザー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。

	コマンドまたはアクション	目的
	• Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認（32 ページ）	
ステップ 4	Windows Server 2008 を実行する Exchange 2010、2013 または 2016 の認証の有効化（35 ページ）	Exchange Server の EWS 仮想ディレクトリ (/EWS) で、基本認証、Windows 統合認証、またはその両方を有効にする必要があります。
ステップ 5	Exchange Server の証明書の設定タスクフロー （56 ページ）	このタスクフローを完了して、Microsoft Exchange 展開用の証明書を設定します。

Windows 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ーで、**[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）] > [セキュリティのオプション（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ベースクライアント（セキュアな RPC を含む）のサーバー向け最小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ーを再起動します。

（注） 再起動は、セキュリティポリシー設定の変更が実行されたサーバーでのみ必要です。

Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定

特定のユーザーまたはユーザーグループに 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。

これらは、Exchange Server 2010 向けのコマンドと設定です。Exchange Server 2013 を使用している場合は、Exchange 2013 または 2016 の特定のユーザーまたはグループに Exchange の偽装権限を設定 （29 ページ） の手順に従います。

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、他のユーザーアカウントを偽装する権限を指定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 Server のすべてのアカウントを偽装する権限が、*Exch2010* アカウントに対して与えられます。

構文

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

例

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

ステップ 5 New-ThrottlingPolicy コマンドを実行し、下の表の推奨値を使用して新しいスロットリングポリシーを作成します。

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
```

表 *13 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] シスコが行ったテスト時には、予定表を使用するユーザー50%に対応するにはデフォルトのスロットリングポリシー値で十分でした。ただし、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 に引き上げることを推奨します。

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 で使用し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
```

次のタスク

Microsoft Exchange 2010 アカウントのアクセス許可の確認 （30 ページ）

関連トピック

Exchange Server 2010
Exchange Server 2013

Exchange 2013 または 2016 の特定のユーザーまたはグループに Exchange の偽装権限を設定

特定のユーザーまたはユーザーグループに 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。

これらは、Exchange Server 2013 または 2016 向けのコマンドと設定です。Exchange Server 2010 を使用している場合は、Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定 （27 ページ） の手順に従います。

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、他のユーザーアカウントを偽装するアクセス許可を指定サービスアカウント（*Ex2013* 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:Ex2013@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 Server のすべてのアカウントを偽装するアクセス許可が、*Exch2013* アカウントに対して与えられます。

構文

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

例

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

ステップ 5 New-ThrottlingPolicy コマンドを実行し、下の表の推奨値を使用して新しいスロットリングポリシーを作成します。

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100  -EwsMaxSubscriptions:NULL
-EwsCutoffBalance 3000000 -EwsMaxBurst 300000 -EwsRechargeRate 900000
```

例

```
New-ThrottlingPolicy -Name IMP_ThrottlingPolicy -EwsMaxConcurrency 100
-EwsMaxSubscriptions unlimited -EwsCutoffBalance 3000000 -EwsMaxBurst 300000
-EwsRechargeRate 900000
```

表 *14 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

パラメータ[1]	推奨設定値：Exchange Server 2013 および 2016
EwsCutoffBalance	3000000
EwsMaxBurst	300000

パラメータ[1]	推奨設定値：**Exchange Server 2013 および 2016**
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**無制限**
EwsRechargeRate	900000

[1] これらは、Exchange Server 2013 で変更できる唯一の EWS パラメータです。

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 で使用し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 ex2013 -ThrottlingPolicy IMP_ThrottlingPolicy
```

次のタスク

Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認 （32 ページ）

Microsoft Exchange 2010 アカウントのアクセス許可の確認

Exchange 2010 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザー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 では、アクセス許可がメールボックスに伝播されるまでに多少時間がかかります。

これらは、Exchange Server 2010 向けのコマンドです。Exchange Server 2013 を使用している場合は、Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認 （32 ページ）の手順に従います。

手順

ステップ 1 Active Directory サーバーで、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 Server 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) コマンド出力で、次のように、指定アカウントに対する役割「ApplicationImpersonation」の割り当てが示されることを確認します。

コマンド出力の例

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	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。

コマンド出力の例

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

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 EMS 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
```

表 *15 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：**Exchange Server 2010**
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

パラメータ	推奨設定値：Exchange Server 2010
[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリング ポリシー値で十分でした。ただし、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 に引き上げることを推奨します。	

次のタスク

Exchange 仮想ディレクトリでの認証の有効化 （34 ページ）

関連トピック

Exchange Server 2010
Exchange Server 2013

Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認

Exchange 2013 または 2016 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザー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。アクセス許可がメールボックスに伝播されるまでには多少の時間がかかります。

（注） Exchange Server 2010 を使用している場合は、Microsoft Exchange 2010 アカウントのアクセス許可の確認 （30 ページ） の手順に従います。

手順

ステップ 1 Active Directory サーバーで、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 Server 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) コマンド出力で、次のように、指定アカウントに対する役割「ApplicationImpersonation」の割り当てが示されることを確認します。

コマンド出力の例

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	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。

コマンド出力の例

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

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 EMS 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 IMP_ThrottlingPolicy | Format-List | findstr ^Ews
```

表 *16 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

パラメータ[1]	推奨設定値：Exchange Server 2013 および 2016
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**無制限**
EwsRechargeRate	900000

[1] これらは、Exchange Server 2013 で変更できる唯一の EWS パラメータです。

ステップ 6 ThrottlingPolicy が Exchange アカウントに関連付けられていることを確認します。

```
Get-ThrottlingPolicyAssociation -Identity ex2013
```

Windows Server 2008 を実行する Exchange 2010、2013 または 2016 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インフォメーションサービス（Internet Information Services）を開き、サーバーを選択します。

ステップ 2 [サイト（Web Sites）] を選択します。

ステップ 3 [既定の 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（Anonymous Authentication）]
- [Windows 認証（Windows Authentication）] および [Basic 認証（Basic Authentication）]（両方またはどちらか）

ステップ 7 適切に設定するには、[操作（Actions）] カラムで [有効にする/無効にする（Enable/Disable）] リンクを使用します。

次のタスク

Exchange Server の証明書の設定タスクフロー （56 ページ）

関連トピック

Outlook Web App の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の SSL を有効または無効にする

SAN およびワイルドカード証明書のサポート

IM and Presence Service では、Microsoft Exchange との予定表統合をセキュリティ保護するために、X.509 証明書を使用します。IM and Presence Service 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、ホスト名や IP アドレスの一覧を [X509v3サブジェクトの別名（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、ドメイン名にアスタリスクを指定することにより、ドメインと無制限のサブドメインを表すことができます。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 [サブジェクトの別名（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 [サブジェクトの別名（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、[標準証明書の共通名（CN）（Common Name (CN)）]と、SAN 証明書の [サブジェクトの別名（Subject Alternative Name）] に使用することができます。

Exchange Server の証明書の設定タスクフロー

これらのタスクを完了して、Microsoft Exchange 展開用の証明書を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	お使いのバージョンの Windows Server のバージョンに認証局 (CA) をインストールします • Windows Server 2003 での CA のインストール （57 ページ） • Windows Server 2008 での CA のインストール （58 ページ）	認証局（CA）は Exchange Server 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 Server を CA として使用することをお勧めします。
ステップ 2	お使いのバージョンの Windows Server の証明書署名要求を生成します。 • 証明書署名要求の生成：Windows Server 2003 を実行している場合 （59 ページ） • 証明書署名要求の生成：Windows Server 2008 を実行している場合 （61 ページ）	Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバーによって署名されます。
ステップ 3	CA サーバー/認証局への証明書署名要求の送信 （62 ページ）	IIS で Exchange 用に作成されるデフォルトの SSL 証明書には、Exchange Server の完全修飾ドメイン名（FQDN）を使用し、IM and Presence Service 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 からの証明書署名要求に署名できます。

	コマンドまたはアクション	目的
ステップ 4	署名付き証明書のダウンロード （63 ページ）	署名付き証明書をダウンロードします。
ステップ 5	署名付き証明書をお使いのバージョンの Windows Server にアップロードします。 • 署名付き証明書のアップロード：Windows 2003 を実行している場合（64 ページ） • 署名付き証明書のアップロード：Windows 2008 を実行している場合（66 ページ）	ここでは、署名付き証明書署名要求を IIS にアップロードする手順を説明します。
ステップ 6	ルート証明書のダウンロード （67 ページ）	CA サーバーからルート証明書をダウンロードします。
ステップ 7	IM and Presence Service ノードへのルート証明書のアップロード （67 ページ）	ルート証明書を IM and Presence Service にアップロードします。

Windows Server 2003 での CA のインストール

始める前に

- 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インフォメーションサービス（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（Control Panel）]>[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と削除（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 Components）] ウィンドウで、[証明書サービス（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）] を選択します。

b) [CAの種類（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 サーバーの [共通名（Common Name）] フィールドにサーバー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）] を選択します。

（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、証明書署名要求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 インフォメーション サービスを停止するように求められたら [はい（Yes）] を選択します。

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 インストールが完了したら、[完了（Finish）] をクリックします。

次のタスク

証明書署名要求の生成：Windows Server 2003 を実行している場合 （59 ページ）

Windows Server 2008 での CA のインストール

手順

ステップ 1 **[スタート（Start）] > [管理ツール（Administrative Tools）] > [サーバーマネージャ（Server Manager）]** の順に選択します。

ステップ 2 コンソール ツリーで、[役割（Roles）] を選択します。

ステップ 3 **[操作（Action）] > [役割の追加（Add Roles）]** を選択します。

ステップ 4 [役割の追加（Add Roles）] ウィザードを完了します。

a) [開始する前に（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) [サーバーの役割の選択（Select Server Roles）] ウィンドウで、[Active Directory証明書サービス（Active Directory Certificate Services）] の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) [概要（Introduction）] ウィンドウで、[次へ（Next）] をクリックします。

d) [役割サービスの選択（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。

- 証明機関（Certificate Authority）
- 証明機関 Web 登録（Certificate Authority）
- オンライン レスポンダー（Online Responder）

e) [セットアップの種類の指定（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の種類の指定（Specify CA Type）] ウィンドウで、[ルートCA（Root CA）] をクリックします。

g) [秘密キーの設定（Set Up Private Key）] ウィンドウで、[新しい秘密キーを作成する（Create a new private key）] をクリックします。

h) [CAの暗号化を構成（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名を構成（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) [有効期間の設定（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 が発行する証明書は、ここで指定した期日まで有効になります。

k) [証明書データベースを構成（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) [インストールオプションの確認（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) [インストールの結果（Installation Results）] ウインドウで、すべてのコンポーネントに対して「インストールが正常に完了しました（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） サーバーマネージャに役割の 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。

次のタスク

証明書署名要求の生成：Windows Server 2008 を実行している場合 （61 ページ）

証明書署名要求の生成：Windows Server 2003 を実行している場合

Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバーによって署名されます。証明書の [サブジェクトの別名（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。

始める前に

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 [インターネットインフォメーションサービス（Internet Information Services）] を開きます。

a) [既定の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 [サーバー証明書（Server Certificate）] を選択します。

ステップ 4 [サーバー証明書ウィザード（Web Server Certificate Wizard）] 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 **サーバー証明書ウィザード**を完了します。

a) [サーバー証明書（Server Certificate）] ウィンドウで [新しい証明書の作成（Create a new certificate）] を選択し、[次へ（Next）] を選択します。
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）] を選択します。
c) [名前およびセキュリティ設定（Name and Security Settings）] で、デフォルトの Web サイト証明書名を受け入れ、ビット長として [1024] を選択し、[次へ（Next）] を選択します。
d) [組織情報（Organization Information）] ウィンドウの [組織（Organization）] フィールドに会社名、[組織単位（Organizational Unit）] フィールドに部署名をそれぞれ入力し、[次へ（Next）] を選択します。
e) [サイトの一般名（Your Site's Common Name）] ウィンドウで、Exchange Server 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 証明書の一般名は、IM and Presence Service 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）] ウィンドウで次のように地理情報を入力し、[次へ（Next）] を選択します。
   - 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）] ウィンドウに、証明書要求の適切なファイル名を入力し、証明書署名要求を保存するパスとファイル名を指定して [次へ（Next）] を選択します。

（注） 証明書署名要求は拡張子（.txt）なしで保存してください。この証明書署名要求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）] ウィンドウに表示されている情報に誤りがないことを確認し、[次へ（Next）] を選択します。
i) [Webサーバー証明書ウィザードの完了（Web Server Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

次のタスク

CA サーバー/認証局への証明書署名要求の送信 （62 ページ）

証明書署名要求の生成：Windows Server 2008 を実行している場合

Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバーによって署名されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネットインフォメーションサービス（IIS）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 マネージャの左ペインの [接続（Connections）] の下で、[Exchange Server] を選択します。

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

ステップ 4 IIS マネージャの右ペインにある [操作（Actions）] ウィンドウで [証明書の要求の作成（Create Certificate Request）] を選択します。

ステップ 5 **証明書の要求**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 Server 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。
- [組織単位（Organizational Unit）] フィールドに部署名を入力します。

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 証明書の一般名は、IM and Presence Service 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のプロパティ（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の適切なファイル名を入力し、[次へ（Next）] を選択します。

（注） 証明書署名要求は拡張子（.txt）なしで保存してください。この証明書署名要求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) [要求ファイルの概要（Request File Summary）] ウィンドウに表示されている情報に誤りがないことを確認し、[次へ（Next）] を選択します。
f) [証明書の要求を完了する（Request Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

次のタスク

CA サーバー/認証局への証明書署名要求の送信 （62 ページ）

CA サーバー/認証局への証明書署名要求の送信

IIS で Exchange 用に作成されるデフォルトの SSL 証明書には、Exchange Server の完全修飾ドメイン名（FQDN）を使用し、IM and Presence Service 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 からの証明書署名要求に署名できます。次の手順を CA サーバーで実行し、次の場所にある Exchange Server の FQDN を設定します。

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

始める前に

Exchange Server の IIS で証明書署名要求を生成します。

手順

ステップ 1 証明書要求ファイルを CA サーバーにコピーします。

ステップ 2 次のいずれかの URL にアクセスします。

- Windows 2003 または Windows 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 [証明書の要求（Request a certificate）] を選択します。

ステップ 4 [証明書の要求の詳細設定（advanced certificate request）] を選択します。

ステップ 5 [Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信するか、または Base 64 エンコード PKCS #7 ファイルを使用して更新の要求を送信する（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file or submit a renewal request by using a base-64-encoded PKCS #7 file）] をクリックします。

ステップ 6 メモ帳などのテキスト エディタを使用して、作成した証明書署名要求を開きます。

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 証明書署名要求の内容を [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、サーバー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サーバー（Web Server）] 証明書テンプレートを選択します。[Web サーバー（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 [スタート（Start）] > [管理ツール（Administrative Tools）] > [証明機関（Authority Certification）] > [CA 名] > [保留中の要求（Pending Request）] を選択し、[証明機関（Certification Authority）] ウィンドウを開きます。 > > > > > [証明機関（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。
- [発行（Issue）] を選択します。

ステップ 13 [発行した証明書（Issued certificates）] をクリックし、証明書が発行されたことを確認します。

次のタスク

署名付き証明書のダウンロード （63 ページ）

署名付き証明書のダウンロード

始める前に

自己署名証明書：CA サーバーに証明書署名要求（CSR）を送信します。

サードパーティ証明書：認証局に証明書署名要求を要求します。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [証明機関（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**ウィザードを完了します。

a) [エクスポートファイル形式（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 を使用して `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、概要を確認し、エクスポートが成功したことを確認して [完了（Finish）] を選択します。

ステップ 7 IM and Presence Service 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。

次のタスク

使用するサーバータイプ用の署名付き証明書をアップロードします。

- 署名付き証明書のアップロード：Windows 2003 を実行している場合 （64 ページ）
- 署名付き証明書のアップロード：Windows 2008 を実行している場合 （66 ページ）

署名付き証明書のアップロード：Windows 2003 を実行している場合

ここでは、署名付き証明書署名要求を 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 Service 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。

始める前に

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 インフォメーション サービス（Internet Information Services**）を開きます。

ステップ 2 [インターネットインフォメーションサービス（Internet Information Services）] ウィンドウで次の手順を実行します。

a) [既定の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 [既定の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) [サーバー証明書（Server Certificate）] を選択します。

ステップ 4 [サーバー証明書ウィザード（Web Server Certificate Wizard）] 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 **サーバー証明書ウィザード**を完了します。

a) [保留中の証明書の要求（Pending Certificate Request）] ウィンドウで、[保留中の要求を処理し、証明書をインストールする（Process the pending request and install the certificate）] を選択し、[次へ（Next）] をクリックします。
b) [保留中の証明書を処理（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サーバー証明書ウィザードの完了（Web Server Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

Tip

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

- [ディレクトリセキュリティ（Directory Security）] タブで、[証明書の表示（View Certificate）] をクリックします。
- [詳細（Details）]>[ルート証明書の強調表示（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。

次のタスク

ルート証明書のダウンロード （67 ページ）

署名付き証明書のアップロード：Windows 2008 を実行している場合

ここでは、署名付き証明書署名要求を 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 Service 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。

始める前に

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 インフォメーション サービス（IIS）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 マネージャの左ペインの [接続（Connections）] の下で、[Exchange Server] を選択します。

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

ステップ 4 IIS マネージャの右ペインにある [操作（Actions）] ウィンドウで [証明書の要求の作成（Create Certificate Request）] を選択します。

ステップ 5 [証明機関の応答を指定します（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。要求が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 [インターネット インフォメーション サービス（Internet Information Services）] ウィンドウで次の手順を実行し、証明書をバインドします。

a) [既定の Web サイト（Default Web Site）] を選択します。
b) IIS マネージャの右ペインにある [操作（Actions）] ウィンドウで [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 [サイト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 証明書のドロップダウンリストから、作成した証明書を選択します。証明書に適用した名前が表示されます。
b) [OK] をクリックします。

次のタスク

ルート証明書のダウンロード （67 ページ）

ルート証明書のダウンロード

始める前に

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 サーバーのユーザーインターフェイスにログインし、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 [エンコード方式（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。

Tip

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。

次のタスク

IM and Presence Service ノードへのルート証明書のアップロード （67 ページ）

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

始める前に

- 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 Server 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 Service 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（Certificate Import Tool）] を使用して、次の操作を行います。

証明書のアップロード方法	アクション
Cisco Unified CM IM and Presence Administration の [証明書インポートツール（Certificate Import Tool）] [証明書インポートツール（Certificate Import Tool）] は、信頼証明書を IM and Presence Service 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 Server のホストとポートを指定すると、サーバー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、欠落している証明書が自動的にインストールされます。 （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（Certificate Import Tool）] 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）。	

証明書のアップロード方法	アクション
	1. **Cisco Unified CM IM and Presence Administration** のユーザー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）] > [証明書のインポートツール（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 Presence Engine 信頼証明書が保存されます。 4. Exchange Server 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 • Hostname • FQDN この [ピアサーバー（Peer Server）] フィールドに入力する値は、Exchange Server 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 Server との通信に使用するポートを入力します。この値は、Exchange Server 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。 • ピアサーバーの到達可能性ステータス：IM and Presence Service が Exchange Server に到達（ping）できるかどうかを示します。「Exchange Server の接続ステータスに関するトラブルシューティング（117 ページ）」を参照してください。 • SSL 接続/証明書の確認ステータス：証明書のインポートツールが指定されたピアサーバーから証明書をダウ

証明書のアップロード方法	アクション
	ンロードすることに成功したかどうかと、IM and Presence Service とリモートサーバー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 （118 ページ）」を参照してください。

ステップ 2 証明書の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 サーバーでは CA 証明書が欠落します）、**Cisco Unified OS の管理**画面の [証明書の管理（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てください

証明書のアップロード方法	アクション
Cisco Unified IM およびプレゼンス オペレーティング システムの管理 Exchange Server が SSL/TLS ハンドシェイク中に証明書を提供しない場合、それらの証明書は証明書の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、**[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します）。	1. IM and Presence Service 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** ユーザーインターフェイスにログインします。 3. **[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。 4. [証明書の一覧（Certificate List）] ウィンドウで、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。 5. [証明書/証明書チェーンのアップロード（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-xmpp-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 （68 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。

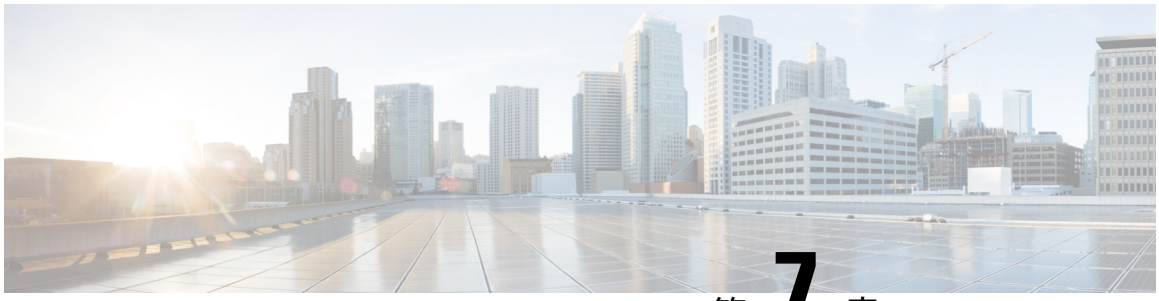
ステップ 4 すべての Exchange 信頼証明書をアップロードしたら、Cisco Presence Engine と SIP プロキシ サービスを再起動します。**Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。**[ツール（Tools）]** > **[コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

ヒント

IM and Presence Service では、Exchange Server 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。

次のタスク

IM and Presence 予定表統合のタスクフロー （79 ページ）



第 7 章

Microsoft Office 365 の設定

- Microsoft Office 365 予定表統合 （75 ページ）
- Microsoft Office 365 予定表統合のタスクフロー （75 ページ）

Microsoft Office 365 予定表統合

IM and Presence Service を Microsoft Outlook 予定表統合用のホスト型 Office 365 サーバーと統合するように設定できます。この設定により、IM and Presence Service が Office 365 でホストされた Microsoft Outlook からユーザーの予定表情報をプルして、それを IM and Presence ユーザーのプレゼンス ステータスの一部として表示します。Outlook がユーザーが会議中であることを示している場合は、そのステータスがそのユーザーのプレゼンス ステータスに表示されます。

この統合は、15,000 の IM and Presence ユーザーシステムでテストして正常動作が確認されています。このテストでは、5,000 人のユーザーが午前零時に会議を開催しました。

Microsoft Office 365 予定表統合のタスクフロー

これらのタスクを完了して、IM and Presence Service と Microsoft Outlook 間の予定表統合のために Microsoft Office 365 展開を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	予定表統合のための Office 365 アクセス許可の設定 （76 ページ）	IM and Presence ユーザーが Microsoft Outlook から予定表情報を取得できるように、Office 365 サーバーに偽装権限を設定します。
ステップ 2	Microsoft IM and Presence Service への証明書のアップロード （76 ページ）	IM and Presence Service との統合に必要な Microsoft 証明書をダウンロードします。

予定表統合のための Office 365 アクセス許可の設定

Office 365 サーバーでこの手順を使用して、IM and Presence の予定表統合のアクセス許可を設定します。IM and Presence Service と統合するには、Discovery Management に **ApplicationImpersonation** 管理者ロールを割り当てる必要があります。

始める前に

この手順は、Office365 の展開が既にセットアップされていることを前提としています。Office 365 の構成については、Microsoft のドキュメントを参照してください。

手順

ステップ 1 Office 365 にログインします。

ステップ 2 **管理者**アイコンをクリックします。

ステップ 3 左側のナビゲーションバーで[管理センター（Admin Center）]タブ（左下）を選択し、[Exchange] をクリックします。

ステップ 4 [アクセス許可（Permissions）] で、[管理者の役割（Admin role）] を選択します。

ステップ 5 [Discovery Management] を選択します。

ステップ 6 鉛筆アイコンをクリックして役割の割り当てを編集します。

ステップ 7 次の手順を実行して、役割 **ApplicationImpersonation** を追加します。

a) [役割（Roles）] で [+] をクリックします。
b) [ApplicationImpersonation] を選択して [追加（Add）] をクリックします。
c) [OK] をクリックします。

ステップ 8 ApplicationImpersonation のメンバーとしてユーザーを割り当てます。

a) [メンバー（Members）] で [+] をクリックします。
b) 追加するユーザーを選択し、[追加（Add）] をクリックします。
c) [OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

Microsoft IM and Presence Service への証明書のアップロード （76 ページ）

Microsoft IM and Presence Service への証明書のアップロード

IM and Presence Service と Office 365 展開が通信するには、IM and Presence Service に Microsoft 証明書をインストールする必要があります。

手順

ステップ 1 Office 365 ルート証明書と中間証明書をダウンロードします。

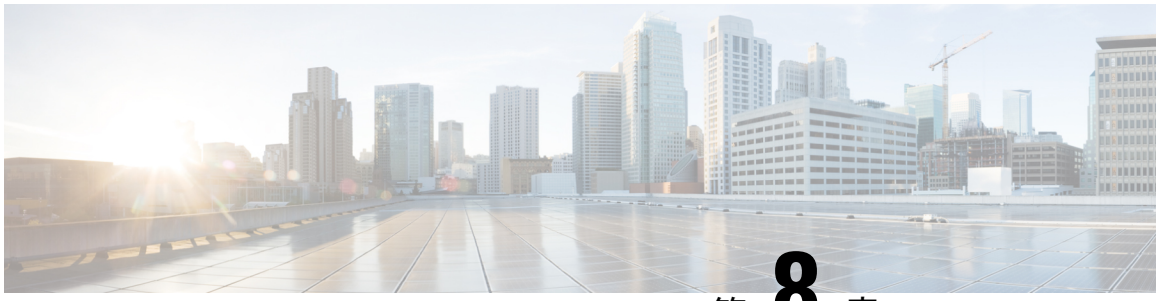
- https://support.office.com/en-us/article/office-365-certificate-chains-0c03e6b3-e73f-4316-9e2b-bf4091ae96bb には、Office 365 がサポートするすべてのルート証明書と中間証明書が一覧表示されています。

ステップ 2 すべての証明書を IM and Presence Service の **cup-trust** および **tomcat-trust** ストアにアップロードします。

（注） IM and Presence Service の証明書の詳細については、『*IM and Presence Service* の設定および管理ガイド』の「IM and Presence Service のセキュリティ設定」の章を参照してください。

次のタスク

IM and Presence 予定表統合のタスクフロー （79 ページ）



第 8 章

IM and Presence Service の設定

- IM and Presence 予定表統合のタスクフロー （79 ページ）

IM and Presence 予定表統合のタスクフロー

IM and Presence Service で次のタスクを完了し、次の Microsoft 展開のいずれかに対して Microsoft Outlook との予定表統合をセットアップします。

- オンプレミス Microsoft Exchange Server
- ホスト型 Microsoft Office 365 サーバー

手順

	コマンドまたはアクション	目的
ステップ 1	プレゼンスゲートウェイの設定 （80 ページ）	IM and Presence サーバーで、Exchange Server または Office 365 サーバーをプレゼンスゲートウェイとして設定します。
ステップ 2	Office 365 統合のプル間隔の設定 （82 ページ）	（Office 365 のみ）IM and Presence Service が Office 365 から予定表情報をプルする間隔のスケジュールを設定します。デフォルト値は 60 分です。
ステップ 3	Exchange 統合のサービスパラメータの設定 （83 ページ）	（Exchange のみ）Microsoft Exchange Server との予定表同期におけるやり取りの要点を表すオプションのサービスパラメータを設定します。
ステップ 4	Cisco Presence Engine の再起動 （85 ページ）	サービスパラメータを編集した場合は、Cisco Presence Engine サービスを再起動します。

	コマンドまたはアクション	目的
ステップ 5	次のいずれかの手順を使用して、ユーザーの予定表を有効にします。 • LDAP 同期ユーザーの予定表の有効化 （85 ページ） • 予定表統合の一括有効化 （87 ページ） • ユーザーごとの予定表統合の有効化 （88 ページ）	ニーズに合った手順を選択してください。 • LDAP 同期をまだ完了していない場合は、LDAP 同期を介して予定表を有効にします。 • それ以外の場合は、一括管理ツールを使用して、多数のユーザーの予定表を設定します。 • または、ユーザーごとに機能を有効にします。

プレゼンスゲートウェイの設定

この手順を使用して、Microsoft Outlook との予定表統合をセットアップするためにプレゼンスゲートウェイを設定します。Microsoft Exchange Server または Office 365 サーバーのいずれかをプレゼンスゲートウェイとして割り当てることができます。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] で、以下を選択**[プレゼンス（Presence）]** > **[ゲートウェイ（Gateways）]** を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [プレゼンスゲートウェイタイプ（Presence Gateway Type）] フィールドで、次のオプションのいずれかを選択します。

a) オンプレミスの Exchange Server と統合する場合は、[Exchange - - EWS サーバー（Exchange - - EWS Server）] を選択します。

b) ホスト型 Office 365 サーバーと統合する場合は、[Office 365 サーバー（Office 365 Server）] を選択します。

[Office 365 サーバー（Office 365 Server）] を選択した場合は、[基本（Basic）] または [OAuth] を選択して、ドロップダウンリストから [認証タイプ（Authentication Type）] を選択する必要があります。

（注） [アプリケーション（クライアント）ID（Application (client) ID）]、[ディレクトリ（テナント）ID（Directory (tenant) ID）]、[クライアントシークレット（Client Secret）] のフィールドは、[認証タイプ（Authentication Type）]として [OAuth] を選択した場合にのみ適用されます。

[アプリケーション（クライアント）ID（Application (client) ID）]、[ディレクトリ（テナント）ID（Directory (tenant) ID）]、[クライアントシークレット（Client Secret）] のフィール

ドを設定し、アプリケーションのアクセス許可の設定と管理者の同意の付与を行う方法については、セクション 認証タイプ OAuth の Office 365 事前構成 （81 ページ） を参照してください。

ステップ 4 [説明（Description）] フィールドに、プレゼンスゲートウェイ インスタンスを区別するのに役立つ説明を入力します。

ステップ 5 [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 サーバーの完全修飾ドメイン名または IP アドレスを入力します。この値は、サーバー証明書の [サブジェクトの共通名（CN）（Subject Common Name (CN)）] または [サブジェクトの別名（Subject Alternate Name）] フィールドに表示されるサーバーアドレスと一致する必要があります。

ステップ 6 [アカウント名（Account Name）] フィールドに、サーバーにアクセスするためのアカウントの名前を入力します。

ステップ 7 [アカウントパスワード（Account Password）] フィールドと [パスワードの確認（Confirm Password）] フィールドの両方に、アカウントがサーバーへのアクセスに使用するパスワードを入力します。

ステップ 8 [プレゼンスゲートウェイタイプ（Presence Gateway Type）] が [Office 365 サーバー（Office 365 Server）] で、IM and Presence Service が Office 365 サーバーにアクセスできない場合は、[HTTP/HTTPSプロキシURL（HTTP/HTTPS Proxy URL）] フィールドで、HTTP/HTTPS プロキシサーバーの詳細を割り当てます。

ステップ 9 [HTTP/HTTPSプロキシユーザー名（HTTP/HTTPS Proxy Username）] フィールドに、プロキシサーバーのユーザー名を入力します。

ステップ 10 [HTTP/HTTPSプロキシパスワード（HTTP/HTTPS Proxy Password）] フィールドに、HTTP/HTTPS プロキシサーバーに指定されたユーザー名のパスワードを入力します。

ステップ 11 [プレゼンスゲートウェイの設定（Gateway Configuration）] ウィンドウでその他のフィールドを設定します。フィールドと設定の詳細については、オンラインヘルプを参照してください。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

Microsoft 統合タイプの任意のパラメータを設定できます。

- Office 365 統合のプル間隔の設定 （82 ページ）
- Exchange 統合のサービスパラメータの設定 （83 ページ）

認証タイプ OAuth の Office 365 事前構成

この手順を使用して、プレゼンスゲートウェイの認証タイプを OAuth として設定します。

アプリケーション（クライアント）ID、ディレクトリ（テナント）ID、クライアントシークレットを取得し、アプリケーションのアクセス許可を設定し、Microsoft Azure ポータルから管理者の同意を付与する手順に記載されている手順に従う必要があります。

手順

ステップ 1 https://portal.azure.com から Microsoft Azure Portal にログインします。

ステップ 2 https://docs.microsoft.com/en-gb/azure/active-directory/develop/quickstart-register-app#register-a-new-application-using-the-azure-portal の手順に従って、新しいアプリケーションを登録し、**アプリケーション（クライアント）ID** と**ディレクトリ（テナント）ID** を取得します。

ステップ 3 **クライアントシークレット**を作成するには、**[管理（Manage）]** で、**[証明書とシークレット（Certificates & Secrets）]** > **[新しいクライアントシークレット（New Client Secret）]** をクリックします。

（注） [プレゼンスゲートウェイタイプ（Presence Gateway Type）] を [Office 365サーバー（Office 365 Server）] として選択し、[認証タイプ（Authentication Type）] を [OAuth] として選択する場合は、同じ値を使用して、プレゼンスゲートウェイの設定中に IM and Presence のアプリケーション（クライアント）ID、ディレクトリ（テナント）ID、クライアント シークレットのフィールドを設定します。

ステップ 4 **[管理（Manage）]** > **[API のアクセス許可（API Permissions）]** > **[アクセス許可の追加（Add a permission）]** の順にクリックし、**[組織が使用する API（APIs my organization uses）]** で **[Office 365 Exchange Online]** を選択します。

ステップ 5 アプリケーションの権限を追加するには、**[アプリケーションの権限（Application permissions）]** > **[権限（Permission）]** の順に選択し、**[full_access_as_app]** チェックボックスをオンにし、**[権限を追加（Add permissions）]** をクリックします。

ステップ 6 管理者の同意を与えるには、**[管理（Manage）]** > **[API のアクセス許可（API Permissions）]** をクリックします。

ステップ 7 **[同意の付与（Grant admin consent）]** で、「登録済み Azure Active Directory」の **[管理者の同意を付与（Grant admin consent）]** をクリックし、**[はい（Yes）]** を選択します。

ステップ 8 **[full_access_as_app]** 権限の **[ステータス（Status）]** 列に緑色のチェックマークがあるかどうかを確認します。

Office 365 統合のプル間隔の設定

この手順を使用して、IM and Presence Service が Office 365 から予定表情報をプルする間隔を設定します。

手順

ステップ 1 Cisco Unified CM IM and Presence Administration から、**[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 2 [サーバー（Server）] ドロップダウンリストから、[IM and Presence Serviceパブリッシャ（IM and Presence Service Publisher）] ノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウンリストから、[Cisco Presence Engine] を選択します。

ステップ 4 **Office 365 Calendar Information Pull Interval** サービスパラメータの間隔を分単位で設定します。デフォルトは 60 分です。

ステップ 5 [保存（Save）] をクリックします。

（注） IM and Presence Service は、**Office 365 Calendar Information Pull Interval** サービスパラメータでスケジュール指定された間隔で Office 365 から情報をプルします（デフォルト値は 60 分）。ただし、Office 365 から IM and Presence Service に情報をプッシュするメカニズムはありません。その結果、スケジュールされたプルの間に Office 365 でスケジュールされていないプレゼンスの更新（臨時会議など）が発生した場合、次のスケジュールされたプルの後まで、結果は IM and Presence Service に登録されません。

次のタスク

IM and Presence Service ユーザーの予定表を有効にします。多数のユーザーに対してこの機能を一度に有効にするには、外部 LDAP ディレクトリから同期されるユーザーに対して LDAP 同期を使用するか、非 LDAP ユーザーに対して一括管理ツールを使用します。それ以外の場合は、ユーザーに対して個別に機能を有効にすることができます。

- LDAP 同期ユーザーの予定表の有効化 （85 ページ）
- 予定表統合の一括有効化 （87 ページ）
- ユーザーごとの予定表統合の有効化 （88 ページ）

Exchange 統合のサービスパラメータの設定

この任意の手順を使用して、Outlook の予定表を Microsoft Exchange Server と統合するためのオプションのサービスパラメータを構成します。多くのパラメータはデフォルト値で十分です。

手順

ステップ 1 Cisco Unified CM IM and Presence Administration から、**[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 2 [サーバー（Server）] ドロップダウンリストから、[IM and Presence Serviceパブリッシャ（IM and Presence Service Publisher）] ノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウンリストから、[Cisco Presence Engine] を選択します。

ステップ 4 [予定表の設定（Calendaring Configuration）] で、次のパラメータの値を設定します。

表 *17 : Exchange* 統合のサービスパラメータ

サービス パラメータ	説明
Microsoft Exchange 通知ポート（Microsoft Exchange Notification Port）	Presence Engine が Exchange Server からの着信通知をリッスンするポート番号。WebDav には UDP が使用され、EWS（Exchange Web サービス）には TCP が使用されます。可能な値は 1024 ～ 65535 で、デフォルト値は 50020 です。
秒単位の予定表スプレッド（Calendar Spread (seconds)）	このパラメータは、継続時間の範囲を秒単位で指定します。各ユーザーには、ハッシュによってオフセット期間が割り当てられます。期間は、会議の移行が送信される最上位からの秒数を決定します。ユーザー数が少ない場合は、期間を短縮できます（およそのユーザー数/100 = 秒）。WebDav および EWS（Exchange Web サービス）に使用されます。値の範囲は 0 ～ 59 で、デフォルト値は 50 秒です。
Exchange タイムアウト（秒）（Exchange Timeout (seconds)）	このパラメータは、Exchange Server 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を指定します。この変更には、Cisco Presence Engine の再起動が必要です。可能な値の範囲は 1 ～ 20 で、デフォルト値は 3 秒です。
Exchange キュー（Exchange Queue）	このパラメータは、Exchange 要求キューの最大長を指定します。要求が行われ、キューの長さを超えた場合、要求は失敗し、回復手順が開始されます。この変更には、Cisco Presence Engine の再起動が必要です。可能な値は 1 ～ 5000 で、デフォルト値は 2200 です。
スレッドの交換（Exchange Threads）	このパラメータは、Exchange 要求を処理するために使用されるスレッドの数を指定します。ユーザー数が多い場合（5000 人など）、または一部の Exchange トランザクションに 3 秒以上かかる場合は、この値を増やすことができます。予定表の統合が無効になっている場合は、このパラメータを 1 に設定します。この変更には、Cisco Presence Engine の再起動が必要です。可能な値は 1 ～ 100 で、デフォルト値は 60 です。
EWS ステータスの頻度（分）（EWS Status Frequency (minutes)）	このパラメータは、EWS（Exchange Web サービス）が使用されているときに、通知メッセージが Exchange Server から送信される頻度を指定します。時間は分単位です。可能な値は 10 ～ 1440 で、デフォルト値は 60 です。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

Cisco Presence Engine の再起動 （85 ページ）

Cisco Presence Engine の再起動

Calendaring Configuration サービスパラメーターのいずれかの値を変更した場合は、Cisco Presence Engine サービスを再起動します。

手順

ステップ 1 Cisco Unified IM and Presence Serviceability から、[ツール（Tools）] > [コントロールセンター-機能サービス（Control Center - Feature Services）] > を選択します。

ステップ 2 [サーバー（Server）] ドロップダウン リスト ボックスから、IM and Presence サーバーを選択して、[移動（Go）] をクリックします。

ステップ 3 [IM and Presence Service] で、[Cisco Presence Engine] を選択して、[再起動（Restart）] をクリックします。

次のタスク

IM and Presence Service ユーザーの予定表を有効にします。一度に多数のユーザーに対してこの機能を有効にするには、ユーザーが外部 LDAP ディレクトリから同期されている場合は LDAP 同期を使用し、非 LDAP ユーザーの場合は一括管理ツールを使用します。それ以外の場合は、ユーザーに対して個別に機能を有効にすることができます。

- LDAP 同期ユーザーの予定表の有効化 （85 ページ）
- 予定表統合の一括有効化 （87 ページ）
- ユーザーごとの予定表統合の有効化 （88 ページ）

LDAP 同期ユーザーの予定表の有効化

これらのタスクを完了して、最初の LDAP ディレクトリ同期を介して予定表を有効にします。初期 LDAP 同期を使用して、LDAP ディレクトリから同期されたユーザーの予定表を有効にすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	機能グループテンプレートへの予定表統合の追加 （86 ページ）	機能グループテンプレートに予定表を割り当てます。
ステップ 2	LDAP ディレクトリ同期への機能グループテンプレートの追加 （86 ページ）	予定表が有効な機能グループテンプレートを LDAP ディレクトリ同期に割り当て、同期を完了します。

機能グループテンプレートへの予定表統合の追加

この手順を使用して、Microsoft Outlook 予定表統合を機能グループテンプレートに割り当てます。テンプレートを使用して、LDAP ディレクトリから同期されたすべてのユーザーの Outlook 予定表統合を構成できます。

（注） まだ同期されていない LDAP ディレクトリの機能グループテンプレート設定のみを追加または編集できます。ディレクトリがすでに同期されている場合は、代わりに 予定表統合の一括有効化 （87 ページ） を使用します。

手順

ステップ 1 Cisco Unified CM の管理から、**[ユーザ管理（User Management）] > [ユーザ電話/追加（User Phone/Add）] > [機能グループテンプレート（Feature Group Template）]** の順に選択します。

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。
- [検索（Find）] をクリックし、既存のテンプレートを選択します。

ステップ 3 [Unified CM IM and Presenceでのユーザーの有効化（Enable User for Unified CM IM and Presence）] チェックボックスをオンにします。

ステップ 4 [プレゼンスに会議情報を含める（Include meeting information in Presence）] チェックボックスをオンにします。

ステップ 5 [機能グループテンプレート（Feature Group Template）] の設定ウィンドウの残りのフィールドに入力します。フィールドとその設定の詳細については、オンラインヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

次のタスク

LDAP ディレクトリ同期への機能グループテンプレートの追加 （86 ページ）

LDAP ディレクトリ同期への機能グループテンプレートの追加

この手順を使用して、作成した予定表対応の機能グループテンプレートを LDAP ディレクトリ同期に割り当てます。これにより、この LDAP ディレクトリから同期されたすべてのユーザーに対して Outlook 予定表の統合を有効にすることができます。

（注） 機能グループテンプレートは、まだ同期されていない LDAP ディレクトリにのみ追加できます。ディレクトリがすでに同期されている場合は、代わりに 予定表統合の一括有効化 （87 ページ） を使用します。

始める前に

機能グループテンプレートへの予定表統合の追加 （86 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[System（システム）] > [LDAP] > [LDAP Directory（LDAP ディレクトリ）]** を選択します。

ステップ 2 [検索（Find）] をクリックし、既存の LDAP ディレクトリを選択します。

ステップ 3 [機能グループテンプレート（Feature Group Template）] ドロップダウン リスト ボックスから、前のタスクで作成した機能グループテンプレートを選択します。

ステップ 4 [LDAPディレクトリ（LDAP Directory）] ウィンドウで残りのフィールドを設定します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [完全同期を今すぐ実施（Perform Full Sync Now）] をクリックします。

予定表統合の一括有効化

一括管理を使用して、1 回の操作で多数のユーザーの予定表統合を有効にします。

手順

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

ステップ 2 予定表統合を一括有効化は、次のウィンドウから実行できます。

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

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

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

（注） 更新のさまざまなオプションの詳細については、『*Cisco Unified Communications Manager* 一括管理ガイド』を参照してください。

ステップ 3 予定表統合を有効にするすべてのエンドユーザーについて、次のエンドユーザー設定オプションがオンになっていることを確認してください。

- [Unified CM IM and Presenceのユーザーを有効にする（Enable User for Unified CM IM and Presence）]
- [プレゼンスに会議情報を含める（Include meeting information in Presence）]

ステップ 4 csv ファイルから更新する場合は、適切な [ユーザー（User）] 領域で [ファイル名（File Name）] を選択します。

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

ステップ 5 [今すぐ実行（Run Immediately）] または [後で実行（Run Later）] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

ユーザーごとの予定表統合の有効化

この手順を使用して、IM and Presence Service ユーザーの予定表統合を有効にします。

手順

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

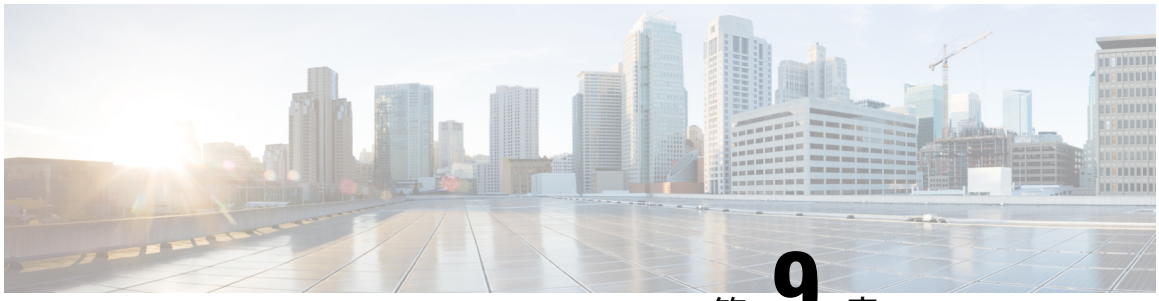
ステップ 2 **[ユーザ管理（User Management）]** > **[エンドユーザー（End User）]** の順に選択します。

ステップ 3 [検索（Find）] をクリックしてエンドユーザーを選択します。

ステップ 4 [Unified CM IM and Presenceでのユーザーの有効化（Enable User for Unified CM IM and Presence）] チェックボックスをオンにします。

ステップ 5 [プレゼンスに会議情報を含める（Include meeting information in Presence）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。



第 9 章

予定表統合のための IM and Presence Service の設定

- Microsoft Exchange との統合向けのプレゼンスゲートウェイの設定 （89 ページ）
- SAN およびワイルドカード証明書のサポート （92 ページ）
- IM and Presence Service と Microsoft Exchange 間のセキュアな証明書交換の設定 （93 ページ）
- 予定表統合の有効化 （109 ページ）
- [任意] Exchange Web サービスで送信される Exchange カレンダー通知の頻度の設定 （110 ページ）
- [任意] Microsoft Exchange 通知ポートの設定 （111 ページ）
- [任意] Microsoft Exchange カレンダー通知の接続時間の設定 （112 ページ）
- その他の Microsoft Exchange カレンダーパラメータ （113 ページ）
- 不在ステータス （114 ページ）

Microsoft Exchange との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には、Exchange Server（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 Service のノードがユーザー単位でユーザーの在席情報を反映できるようになります。

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 Server 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** ユーザー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* 台または複数の EWS サーバーを追加、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の設定（Presence Gateway Configuration）] ウィンドウの [トラブルシューティングツール（Troubleshooter）] は、設定した最初の 10 台の EWS サーバーのステータスのみを検証し、レポートするように設計されています。
- EWS サーバーゲートウェイは、最初の EWS サーバーゲートウェイに対して設定した偽装アカウントログイン情報（アカウント名とパスワード）を共有します。1 つの EWS サーバーゲートウェイのログイン情報を変更すると、設定されたすべての EWS ゲートウェイのログイン情報もそれに準じて変更されます。
- 1 つまたは複数の EWS サーバーを追加、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 サーバーを連続して追加した場合は、Cisco Presence Engine を一度だけ再起動してすべての変更を同時に反映できます。

（注）

- SAN 証明書については、保護されたホストが [サブジェクトの別名（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 [サブジェクトの別名（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

始める前に

プレゼンスゲートウェイを設定する前に、IM and Presence Service 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 Server への接続を IPv6 経由で行う場合は、導入時に各 IM and Presence Service 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 Service での IPv6 の設定の詳細については、『*Cisco Unified Communications Manager* での *IM and Presence Service* 設定および管理』を参照してください。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** のユーザー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のタイプ（Presence Gateway Type）] に [Exchange - EWS サーバー（Exchange -- EWS Server）] を選択します。

設定の変更を反映するには、1 つまたは複数の EWS サーバーを追加、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 サーバーを連続して追加した場合は、Cisco Presence Engine を一度だけ再起動してすべての変更を同時に反映できます。

ステップ 5 1 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ーの場所を入力し、それがサブジェクト共通名（CN）と一致するか、または Exchange Server 証明書の [サブジェクトの別名（Subject Alternative Name）] フィールドにあることを確認します。Microsoft Exchange Server 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、指定するサーバーの場所の値は、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 Server リーフ証明書での [サブジェクトの別名（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 Server 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 Service が Exchange Server 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。この名前は、ユーザープリンシパル名（user@domain など）か、ダウンレベルのログオン名（domain\user など）のどちらかの形式です。

ステップ 8 IM and Presence Service が Exchange Server 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 Server で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 Server との接続に使用するポートを入力します。Exchange との IM and Presence Service の統合は、セキュアな HTTP 接続を介して行われます。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 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**

次のタスク

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 Service と Exchange Server の接続が成功したかどうかを確認します。[プレゼンスゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [Exchange Serverのステータス（Exchange Server Status）] には、 と Exchange Server との接続のステータスが表示されます。修正が必要な場合は、「Exchange Server の接続ステータスに関するトラブルシューティング （117 ページ）」を参照してください。
- Exchange SSL 証明書チェーンのステータスが正しい（[確認が成功しました（Verified）]）かどうかを確認します。[プレゼンスゲートウェイ設定（Presence Gateway Configuration）] ウィンドウの [Exchange Server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 （118 ページ）」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 Service では、Microsoft Exchange との予定表統合をセキュリティ保護するために、X.509 証明書を使用します。IM and Presence Service 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、ホスト名や IP アドレスの一覧を [X509v3サブジェクトの別名（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、ドメイン名にアスタリスクを指定することにより、ドメインと無制限のサブドメインを表すことができます。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 [サブジェクトの別名（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 [サブジェクトの別名（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、[標準証明書の共通名（CN）（Common Name (CN)）]と、SAN 証明書の [サブジェクトの別名（Subject Alternative Name）] に使用することができます。

IM and Presence Service と Microsoft Exchange 間のセキュアな証明書交換の設定

認証局サービスのインストール方法

認証局（CA）は Exchange Server 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 Server 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 （57 ページ）
- Windows Server 2008 での CA のインストール （58 ページ）

Windows Server 2003 での CA のインストール

始める前に

- 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インフォメーションサービス（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（Control Panel）]>[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と削除（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 Components）] ウィンドウで、[証明書サービス（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）] を選択します。

b) [CAの種類（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 サーバーの [共通名（Common Name）] フィールドにサーバー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）] を選択します。

（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、証明書署名要求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 インターネットインフォメーション サービスを停止するように求められたら [はい（Yes）] を選択します。

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 インストールが完了したら、[完了（Finish）] をクリックします。

次のタスク

証明書署名要求の生成：Windows Server 2003 を実行している場合 （59 ページ）

Windows Server 2008 での CA のインストール

手順

ステップ 1 **[スタート（Start）] > [管理ツール（Administrative Tools）] > [サーバーマネージャ（Server Manager）]** の順に選択します。

ステップ 2 コンソールツリーで、[役割（Roles）] を選択します。

ステップ 3 **[操作（Action）] > [役割の追加（Add Roles）]** を選択します。

ステップ 4 [役割の追加（Add Roles）] ウィザードを完了します。

a) [開始する前に（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) [サーバーの役割の選択（Select Server Roles）] ウィンドウで、[Active Directory証明書サービス（Active Directory Certificate Services）] の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) [概要（Introduction）] ウィンドウで、[次へ（Next）] をクリックします。

d) [役割サービスの選択（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。

- 証明機関（Certificate Authority）
- 証明機関 Web 登録（Certificate Authority）
- オンライン レスポンダー（Online Responder）

e) [セットアップの種類の指定（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の種類の指定（Specify CA Type）] ウィンドウで、[ルートCA（Root CA）] をクリックします。

g) [秘密キーの設定（Set Up Private Key）] ウィンドウで、[新しい秘密キーを作成する（Create a new private key）] をクリックします。

h) [CAの暗号化を構成（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名を構成（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) [有効期間の設定（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 が発行する証明書は、ここで指定した期日まで有効になります。

k) [証明書データベースを構成（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) [インストールオプションの確認（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) [インストールの結果（Installation Results）] ウインドウで、すべてのコンポーネントに対して「インストールが正常に完了しました（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） サーバーマネージャに役割の 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。

次のタスク

証明書署名要求の生成：Windows Server 2008 を実行している場合 （61 ページ）

Microsoft Exchange Server の IIS での証明書署名要求の生成

証明書署名要求の生成：Windows Server 2003 を実行している場合

Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバーによって署名されます。証明書の [サブジェクトの別名（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。

始める前に

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 [インターネットインフォメーションサービス（Internet Information Services）] を開きます。

a) [既定の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 [サーバー証明書（Server Certificate）] を選択します。

ステップ 4 [サーバー証明書ウィザード（Web Server Certificate Wizard）] 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 **サーバー証明書ウィザード**を完了します。

a) [サーバー証明書（Server Certificate）] ウィンドウで [新しい証明書の作成（Create a new certificate）] を選択し、[次へ（Next）] を選択します。

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）] を選択します。

c) [名前およびセキュリティ設定（Name and Security Settings）] で、デフォルトの Web サイト証明書名を受け入れ、ビット長として [1024] を選択し、[次へ（Next）] を選択します。

d) [組織情報（Organization Information）] ウィンドウの [組織（Organization）] フィールドに会社名、[組織単位（Organizational Unit）] フィールドに部署名をそれぞれ入力し、[次へ（Next）] を選択します。

e) [サイトの一般名（Your Site's Common Name）] ウィンドウで、Exchange Server 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 証明書の一般名は、IM and Presence Service 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）] ウィンドウで次のように地理情報を入力し、[次へ（Next）] を選択します。

- 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）] ウィンドウに、証明書要求の適切なファイル名を入力し、証明書署名要求を保存するパスとファイル名を指定して [次へ（Next）] を選択します。

（注） 証明書署名要求は拡張子（.txt）なしで保存してください。この証明書署名要求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）] ウィンドウに表示されている情報に誤りがないことを確認し、[次へ（Next）] を選択します。

i) [Webサーバー証明書ウィザードの完了（Web Server Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

次のタスク

CA サーバー/認証局への証明書署名要求の送信 （62 ページ）

証明書署名要求の生成：Windows Server 2008 を実行している場合

Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバーによって署名されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネットインフォメーションサービス（IIS）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 マネージャの左ペインの [接続（Connections）] の下で、[Exchange Server] を選択します。

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

ステップ 4 IIS マネージャの右ペインにある [操作（Actions）] ウィンドウで [証明書の要求の作成（Create Certificate Request）] を選択します。

ステップ 5 **証明書の要求**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 Server 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。
- [組織単位（Organizational Unit）] フィールドに部署名を入力します。

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 証明書の一般名は、IM and Presence Service 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のプロパティ（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の適切なファイル名を入力し、[次へ（Next）] を選択します。

（注） 証明書署名要求は拡張子（.txt）なしで保存してください。この証明書署名要求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) [要求ファイルの概要（Request File Summary）] ウィンドウに表示されている情報に誤りがないことを確認し、[次へ（Next）] を選択します。

f) [証明書の要求を完了する（Request Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

次のタスク

CA サーバー/認証局への証明書署名要求の送信 （62 ページ）

CA サーバー/認証局への証明書署名要求の送信

IIS で Exchange 用に作成されるデフォルトの SSL 証明書には、Exchange Server の完全修飾ドメイン名（FQDN）を使用し、IM and Presence Service 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 からの証明書署名要求に署名できます。次の手順を CA サーバーで実行し、次の場所にある Exchange Server の FQDN を設定します。

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

始める前に

Exchange Server の IIS で証明書署名要求を生成します。

手順

ステップ 1 証明書要求ファイルを CA サーバーにコピーします。

ステップ 2 次のいずれかの URL にアクセスします。

- Windows 2003 または Windows 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 [証明書の要求（Request a certificate）] を選択します。

ステップ 4 [証明書の要求の詳細設定（advanced certificate request）] を選択します。

ステップ 5 [Base 64 エンコード CMC または PKCS #10 ファイルを使用して証明書の要求を送信するか、または Base 64 エンコード PKCS #7 ファイルを使用して更新の要求を送信する（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file or submit a renewal request by using a base-64-encoded PKCS #7 file）] をクリックします。

ステップ 6 メモ帳などのテキスト エディタを使用して、作成した証明書署名要求を開きます。

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 証明書署名要求の内容を [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、サーバー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サーバー（Web Server）] 証明書テンプレートを選択します。[Web サーバー（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 [スタート（Start）] > [管理ツール（Administrative Tools）] > [証明機関（Authority Certification）] > [CA 名] > [保留中の要求（Pending Request）] を選択し、[証明機関（Certification Authority）] ウィンドウを開きます。> > > > > [証明機関（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。
- [発行（Issue）] を選択します。

ステップ 13 [発行した証明書（Issued certificates）] をクリックし、証明書が発行されたことを確認します。

次のタスク

署名付き証明書のダウンロード （63 ページ）

署名付き証明書のダウンロード

始める前に

自己署名証明書：CA サーバーに証明書署名要求（CSR）を送信します。

サードパーティ証明書：認証局に証明書署名要求を要求します。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [証明機関（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**ウィザードを完了します。

a) [エクスポートファイル形式（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 を使用して `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、概要を確認し、エクスポートが成功したことを確認して [完了（Finish）] を選択します。

ステップ 7 IM and Presence Service 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。

次のタスク

使用するサーバータイプ用の署名付き証明書をアップロードします。

- 署名付き証明書のアップロード：Windows 2003 を実行している場合 （64 ページ）
- 署名付き証明書のアップロード：Windows 2008 を実行している場合 （66 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 を実行している場合

ここでは、署名付き証明書署名要求を 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 Service 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。

始める前に

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 インフォメーション サービス（Internet Information Services）**を開きます。

ステップ 2 [インターネットインフォメーションサービス（Internet Information Services）] ウィンドウで次の手順を実行します。

a) [既定の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 [既定の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) [サーバー証明書（Server Certificate）] を選択します。

ステップ 4 [サーバー証明書ウィザード（Web Server Certificate Wizard）] 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 **サーバー証明書ウィザード**を完了します。

a) [保留中の証明書の要求（Pending Certificate Request）] ウィンドウで、[保留中の要求を処理し、証明書をインストールする（Process the pending request and install the certificate）] を選択し、[次へ（Next）] をクリックします。
b) [保留中の証明書を処理（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サーバー証明書ウィザードの完了（Web Server Certificate Completion）] ウィンドウで、[完了（Finish）] をクリックします。

Tip

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

- [ディレクトリセキュリティ（Directory Security）] タブで、[証明書の表示（View Certificate）] をクリックします。
- [詳細（Details）] > [ルート証明書の強調表示（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。

次のタスク

ルート証明書のダウンロード （67 ページ）

署名付き証明書のアップロード：Windows 2008 を実行している場合

ここでは、署名付き証明書署名要求を 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 Service 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。

始める前に

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 インフォメーション サービス（IIS）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 マネージャの左ペインの [接続（Connections）] の下で、[Exchange Server] を選択します。

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

ステップ 4 IIS マネージャの右ペインにある [操作（Actions）] ウィンドウで [証明書の要求の作成（Create Certificate Request）] を選択します。

ステップ 5 [証明機関の応答を指定します（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。要求が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 [インターネット インフォメーション サービス（Internet Information Services）] ウィンドウで次の手順を実行し、証明書をバインドします。

a) [既定の Web サイト（Default Web Site）] を選択します。
b) IIS マネージャの右ペインにある [操作（Actions）] ウィンドウで [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 [サイト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 証明書のドロップダウンリストから、作成した証明書を選択します。証明書に適用した名前が表示されます。
b) [OK] をクリックします。

次のタスク

ルート証明書のダウンロード （67 ページ）

ルート証明書のダウンロード

始める前に

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 サーバーのユーザーインターフェイスにログインし、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 [エンコード方式（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。

Tip

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。

次のタスク

IM and Presence Service ノードへのルート証明書のアップロード （67 ページ）

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

始める前に

- 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 Server 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 Service 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（Certificate Import Tool）] を使用して、次の操作を行います。

証明書のアップロード方法	アクション
Cisco Unified CM IM and Presence Administration の [証明書インポートツール（Certificate Import Tool）] [証明書インポートツール（Certificate Import Tool）] は、信頼証明書を IM and Presence Service 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 Server のホストとポートを指定すると、サーバー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、欠落している証明書が自動的にインストールされます。 （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（Certificate Import Tool）] 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）。	

証明書のアップロード方法	アクション
	1. **Cisco Unified CM IM and Presence Administration** のユーザー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）] > [証明書のインポートツール（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 Presence Engine 信頼証明書が保存されます。 4. Exchange Server 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 • Hostname • FQDN この [ピアサーバー（Peer Server）] フィールドに入力する値は、Exchange Server 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 Server との通信に使用するポートを入力します。この値は、Exchange Server 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。 • ピアサーバーの到達可能性ステータス：IM and Presence Service が Exchange Server に到達（ping）できるかどうかを示します。「Exchange Server の接続ステータスに関するトラブルシューティング（117 ページ）」を参照してください。 • SSL 接続/証明書の確認ステータス：証明書のインポートツールが指定されたピアサーバーから証明書をダウ

証明書のアップロード方法	アクション
	ンロードすることに成功したかどうかと、IM and Presence Service とリモートサーバー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 （118 ページ）」を参照してください。

ステップ 2 証明書の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 サーバーでは CA 証明書が欠落します）、**Cisco Unified OS の管理**画面の [証明書の管理（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てください

証明書のアップロード方法	アクション
Cisco Unified IM およびプレゼンス オペレーティング システムの管理 Exchange Server が SSL/TLS ハンドシェイク中に証明書を提供しない場合、それらの証明書は証明書の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、**[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します）。	1. IM and Presence Service 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** ユーザーインターフェイスにログインします。 3. **[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。 4. [証明書の一覧（Certificate List）] ウィンドウで、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。 5. [証明書/証明書チェーンのアップロード（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-xmpp-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 （104 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** のユーザー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 Service では、Exchange Server 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。

次のタスク

IM and Presence 予定表統合のタスクフロー （79 ページ）

予定表統合の有効化

予定表統合は、管理者によって個別またはユーザー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 で設定されていることを確認します。詳細については、「Microsoft Exchange との統合向けのプレゼンスゲートウェイの設定 （89 ページ）」を参照してください。

個人ユーザーに対する予定表統合の有効化

この手順を使用して、個々のエンドユーザーの Microsoft Outlook 予定表統合を設定します。

手順

ステップ 1 **Cisco Unified CM Administration** のユーザー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）]** > **[エンドユーザー（End User）]** の順に選択します。

ステップ 3 [検索（Find）] をクリックしてエンドユーザーを選択します。

ステップ 4 [Unified CM IM and Presenceでのユーザーの有効化（Enable User for Unified CM IM and Presence）] チェックボックスをオンにします。

ステップ 5 [プレゼンスに会議情報を含める（Include meeting information in Presence）] チェックボックスをオンにします。

ステップ 6 [保存（Save）] をクリックします。

予定表統合の一括有効化

手順

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

ステップ 2 予定表統合を一括有効化は、次のウィンドウから実行できます。

a) **[一括管理（Bulk Administration）] > [ユーザー（Users）] > [ユーザーの挿入（Insert Users）]**
b) **[一括管理（Bulk Administration）] > [ユーザー（Users）] > [ユーザーの更新（Update Users）] > [クエリー（Query）]**
c) **[一括管理（Bulk Administration）] > [ユーザー（Users）] > [ユーザーの更新（Update Users）] > [カスタムファイル（Custom File）]**

（注） 更新のさまざまなオプションの詳細については、『*Cisco Unified Communications Manager* 一括管理ガイド』を参照してください。

ステップ 3 予定表統合を有効にするすべてのエンドユーザーについて、次のエンドユーザー設定オプションがオンになっていることを確認してください。

- [Unified CM IM and Presenceのユーザーを有効にする（Enable User for Unified CM IM and Presence）]
- [プレゼンスに会議情報を含める（Include meeting information in Presence）]

ステップ 4 csv ファイルから更新する場合は、適切な [ユーザー（User）] 領域で [ファイル名（File Name）] を選択します。

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

ステップ 5 [今すぐ実行（Run Immediately）] または [後で実行（Run Later）] をクリックします。

ステップ 6 [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 カレンダー通知の頻度の設定

（注） この手順は、Microsoft Exchange Server 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 ステータスの頻度（EWS Status Frequency）] パラメータは、Exchange Server が IM and Presence Service 上のサブスクリプションを更新する間隔（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 Service 上の Presence Engine 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 Server および IM and Presence サーバーへの負荷も増加します。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** のユーザー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 [サーバー（Server）] ドロップダウンリストから、[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 [予定表の設定（すべてのサーバー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。

次のタスク

予定表の統合はユーザー単位で行われるため、[EWSステータスの頻度（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、すべてのユーザー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** のユーザーインターフェイスにログインします。**[Tools（ツール）] > [Service Activation（サービス アクティベーション）]** 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 Server 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。

始める前に

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** のユーザー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 [サーバー（Server）] ドロップダウンリストから、[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 [予定表の設定（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、[Save（保存）] をクリックします。

次のタスク

一度にすべてのユーザー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** のユーザー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、そのユーザーの Exchange サブスクリプションが更新されるまで、Cisco Presence Engine はユーザー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。Presence Engine がユーザー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ー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] Microsoft Exchange カレンダー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。ユーザー数が少ない場合は、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。

始める前に

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ーの最大数/100」に設定します。たとえば、ユーザーの最大数が 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** のユーザー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 [サーバー（Server）] ドロップダウンリストから、[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 [予定表の設定（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。

次のタスク

[予定表スプレッド（Calendar Spread）] パラメータの変更は、ユーザー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、すべてのユーザー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 多数のユーザー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。

その他の Microsoft Exchange カレンダーパラメータ

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 Microsoft Exchange カレンダーパラメータには、他にも 3 つあります。

- [Exchange タイムアウト（秒）（Exchange Timeout (seconds)）]：Exchange Server 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。

不在ステータス

IM and Presence Service は、ユーザーの在席ステータスとして [不在（Out of Office）] をサポートします。そのため、特定の期間に Microsoft Outlook で不在通知を設定すると、Jabber のプレゼンス ステータスが [退席中（Away）] または [オフライン（Offline）] ではなく [不在（Out of Office）] と表示されます。

さらに、ユーザーステータス情報を収集する際のユーザー体験が向上し、不在であることを不在期間の開始日と終了日とともに他の人に知らせることができます。これにより、ユーザーのプレゼンス状態を明確かつ正確にプロビジョニングすることにより、インスタントメッセージング システムが強化され、ユーザー体験が向上します。

さらに、カスタムプレゼンス設定を使用して不在プレゼンス ステータスを上書きし、必要に応じてアクティブと不在のステータス間を切り替えることができます。これにより、緊急のコミュニケーションや重要な会議に効果的に対処できます。したがって、MS Exchange Server と Office 365 サーバーの両方をサポートするため、オンプレミスとクラウドベースの予定表サービスの間に生じるギャップがなくなります。

たとえば、休暇を取るカスタマーサポートのリードエグゼクティブであるジョン・スミスは、Office 365 で 20XX 年 12 月 10 日 0800 時から 20XX 年 12 月 20 日 2300 時の間に不在通知を設定しました。この機能を実装すると、12 月 10 日の Jabber での彼のプレゼンス ステータスは、「*2019* 年 *3* 月 *10* 日 *10:00 AM GMT* ～ *2019* 年 *3* 月 *12* 日 *6:00 PM GMT* 不在」のメッセージとともにアクティブ/退席中/オフライン（場合による）として表示されます。在席ステータスアイコンがオレンジ色に変わります（ジョンがオフラインの場合を除く）。12 月 14 日、ジョンは上司から電話を受け、緊急の技術的問題に対処するために、Jabber を介してビジネスクリティカルな会議に参加するように求められました。IM and Presence Service のこの新しい機能拡張により、ジョンは不在ステータスを一時的に無効にして、在席ステータスを手動でアクティブにして、顧客との会議に参加できます。会議が終了したら、予定された休暇が終了するまで、プレゼンス ステータスを不在に戻すことができます。

Jabber および Webex Teams の不在通知

MS Exchange や Office 365 などの予定表サービスで不在を設定すると、IM and Presence Service は、定義されたポーリング間隔中に不在通知をプルし、プレゼンス ステータスを不在として表示します。この期間中、ステータスアイコンはオレンジ色で表示されます。不在の期間はローカルタイムゾーンで表示されます。たとえば、メッセージには、*2019* 年 *3* 月 *10* 日 *10:00 AM GMT* から *2019* 年 *3* 月 *12* 日 *6:00 PM GMT* まで不在と表示されます。また、メッセージのローカライズも処理します。

ただし、不在時にオフラインになっている場合は、ステータスが [オフライン（Offline）] と表示され、不在メッセージが表示されます。

IM and Presence 管理コンソールで不在通知を有効にする

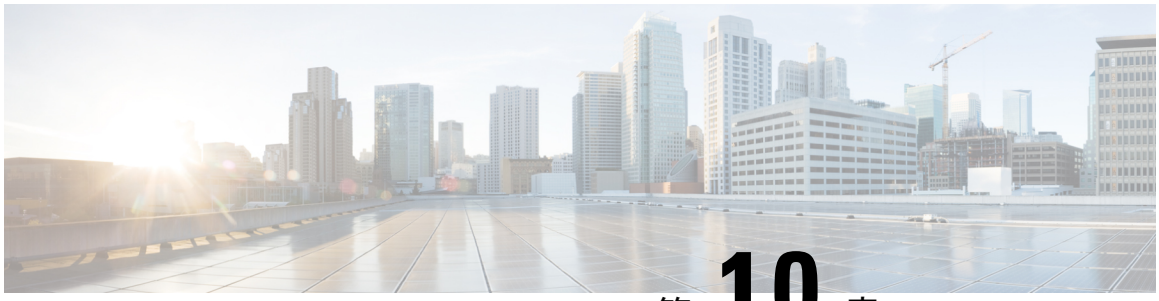
Cisco Presence Service の Calendar Out of Office Information パラメータは、IM クライアント アプリケーションでの不在時の在席ステータスの表示を有効または無効にするのに役立ちます。IM and Presence ノードで不在通知を有効にするには、次の手順を実行します。

（注） マルチモード IM and Presence 展開では、1 つのノードで不在通知オプションを有効にすると、クラスタの他のノードに適用できます。

1. Cisco Unified CM IM and Presence Administration で、[システム（System）] > [サービスパラメータ（Service Parameters）] を選択します。 >
2. [サービスパラメータの設定（Service Parameter Configuration）] ページで、IM and Presence ノードが展開されている**サーバー**を選択します。
3. [サービス（Service）] フィールドで、[Cisco Presence Engine] を選択します。
4. [予定表の設定（すべてのサーバーに適用されるパラメータ）（Calendaring Configuration (Parameters that apply to all servers)）] セクションで、[予定表の不在情報（Calendar Out of Office Information）] フィールドを [不在時の応答可否を表示する（Display Out of Office Availability）] に設定します。これはデフォルトで行われます。
5. [保存（Save）] をクリックします。

不在時の空き情報の表示を無効にするには、[予定表の不在情報（Calendar Out of Office Information）] フィールドで [不在時の応答可否を表示しない（Do not display out of office availability）] を選択し、[保存（Save）] をクリックします。これにより、クラスタ内のすべての IM and Presence ノードでサービスが無効になります。

（注） この変更を行った後、PE サービスを再起動する必要があります。



第 10 章

Exchangeカレンダー統合のトラブルシューティング

- Exchange Server の接続ステータスに関するトラブルシューティング （117 ページ）
- 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 （118 ページ）
- Microsoft Exchange の統合に影響することが確認されている問題 （126 ページ）

Exchange Server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 Server の接続（Exchange Server connection）] 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）]** を選択します）。[プレゼンスゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [Exchange Serverのステータス（Exchange Server Status）] には、 IM and Presence Service と Exchange Server の間の接続のステータスが表示されます。

（注） 1 台または複数の EWS サーバーを追加、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の設定（Presence Gateway Configuration）] ウィンドウの [Exchange Serverのステータス（Exchange Server Status）] 領域は、設定した最初の 10 台までの EWS サーバーのステータスのみを検証し、レポートするように設計されています。

.

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 Service は Exchange Server 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 Service は Exchange Server 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、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、サーバー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 Server 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 Server 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ティングツール（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）]>[システムのトラブルシューティングツール（System Troubleshooter）] の順に選択します。 >

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 Connection/Certificate Verification] 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 Server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* 台または複数の EWS サーバーを追加、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 [トラブルシューティングツール（Troubleshooter）] は、設定した最初の 10 台の EWS サーバーのステータスのみを検証し、レポートするように設計されています。

テスト	ステータスの説明と推奨される処置
SSL 接続/証明書の確認成功	Exchange Server との SSL 接続が IM and Presence Service 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 Server とのセキュアな接続を確立するために IM and Presence Service で必要な証明書がない。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）]をクリックして証明書ビューアを開きます。 **2.** [証明書チェーンをそのまま使用（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 Server からダウンロードします。 **2.** IM and Presence Service 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 Server 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** でアップロードする必要があります。 • [Cisco Unified IM and Presence OS

テスト	ステータスの説明と推奨される処置
	Administration] とユーザー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 ユーザーインターフェイス下の[プレゼンスゲートウェイの設定（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 [確認が成功しました（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。 • **Cisco Unified IM and Presence Serviceability** のユーザーインターフェイスにログインします。 • **[Tools（ツール）] > [Service Activation（サービス アクティベーション）]** 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 Service が Exchange Server 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/証明書の確認ステータスが [確認が成功しました（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 - 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 Service 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、サーバーに 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 Server 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/証明書の確認ステータスが [確認が成功しました（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別名（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 Service 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、サーバーに 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別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 Server 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/証明書の確認ステータスが [確認が成功しました（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 Server が証明書を再生成したが、IM and Presence Service サーバー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 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 Administration 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 Service が SSL 接続を確認できません。 Exchange Server へのネットワーク接続を検証し、適切な IP アドレスとポート番号で Exchange Server に接続できることを確認するようお勧めします。
SSL 接続/証明書の確認に失敗	不明確な原因または IM and Presence Service が到達可能性テストを実行できないことにより、確認が失敗しました。 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。

Microsoft Exchange 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 Server 2007、2010、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 Service と Exchange カレンダーの統合は、予定表プレゼンスをサブスクライブするユーザーの最大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）を行うユーザーの最大 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、下記の表を参照してください。

表 *18 :* 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	予定表プレゼンスにサブスクライブするユーザーの %	予定表の同時移行を行うユーザーの %
8.5(1)	50	30
8.5(2) 以降	100	50

ユーザーが Microsoft Exchange Server 間を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 Server 間でユーザーを移動すると、そのユーザーの予定表ステータスの変更が更新されません。

原因

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

解決策

IM and Presence Service の管理者またはユーザーは、Exchange 管理者がユーザーを Exchange Server 間で移動した後に、そのユーザー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 ユーザーの削除が IM and Presence Service にレプリケートされるまで 24 時間以上かかる

問題

LDAP からユーザーを削除すると、そのユーザーのステータスが Cisco Unified Communications Manager で [非アクティブ（Inactive）] 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ー認証は失敗します。ただし、Cisco Unified Communications Manager が LDAP との間で変更を同期すると、管理者による強制的な同期またはスケジュールされた同期が実行された後 24 時間、ユーザー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 Service の Cisco Sync Agent は、ユーザーが削除されるまでユーザーのステータス変更を同期しません。それまで、ユーザーは Cisco Unified Communications Manager 上に存在し続け、すべての IM and Presence Service 機能（Exchange カレンダーのサブスクリプションを含む）のライセンスは24時間そのユーザーに与えられたままになります。この遅延は、LDAP から削除される前に Cisco Jabber にログインしていたユーザーが自動的にログアウトされないことを意味します。ユーザーの既存の予定表ステータス（連絡可能、取り込み中）は、ユーザーがクライアントからログアウトするまで IM and Presence Service で保持されます。

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。ユーザーがLDAPから削除されると、そのユーザーの予定表のサブスクリプションは少なくとも 24 時間は IM and Presence Service 上に設定されたまま更新され続けます。

解決策

ユーザーがLDAPから削除された場合に、そのユーザーのライセンスを手動で削除すると、IM and Presence Service が Exchange カレンダーのサブスクリプションをただちに終了し、ユーザーをクライアント アプリケーションからサインアウトします。手動で削除しない場合、24 時間の遅延が生じることがあります。

Microsoft Exchange Server URL に「Calendar」の訳語が含まれることの確認

予定表の統合をローカライズする場合は、Exchange Server の URL に「Calendar」の訳語が含まれていることを確認します。

手順

ステップ 1 IM and Presence Service と Cisco Unified Communications Manager の両方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 でのロケールのインストールの詳細については、予定表統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 Service ノードを再起動し、**Cisco Unified CM IM and Presence Administration** ユーザーインターフェイスにログインします。

ステップ 3 予定表で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（Presence）] > [ゲートウェイ（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 Service と Cisco Unified Communications Manager の両方にロケールがインストールされた後、必要に応じて Cisco Unified Communications Manager のユーザーロケールを切り替え、ユーザーロケールが設定されていることを確認します。

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。