Cisco Unified Presence Release 8.5 統合ガイド（Microsoft Exchange 版）

Integration Guide for Configuring Cisco Unified Presence Release 8.5 with Microsoft Exchange

2011 年 3 月 16 日

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

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

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Unified Presence Release 8.5 統合ガイド（Microsoft Exchange 版）

CONTENTS

CHAPTER 1

Cisco Unified Presence と Microsoft Exchange の統合の計画

Cisco Unified Presence での Microsoft Exchange 予定表ステータス

Cisco Unified Presence に Microsoft Exchange を統合することによって、Microsoft Outlook の予定表 / 会議ステータスを Cisco Unified Presence のアベイラビリティ ステータスに取り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、Cisco Unified Presence において会議ステータス（Microsoft Outlook 予定表に表示される）と Cisco Unified Presence のユーザのアベイラビリティ ステータスがどのように対応付けられるかを示しています。

表 1-1　予定表ステータスに基づく集約されたアベイラビリティ ステータス

Microsoft Outlook のステータス	Cisco Unified Presence のステータス
空き時間 / 仮の予定	応対可能
取り込み中	アイドル / ビジー
外出中[1] 退席中[2]	退席中

1. Microsoft Oulook 2003 および 2007
2. Microsoft Outlook 2010

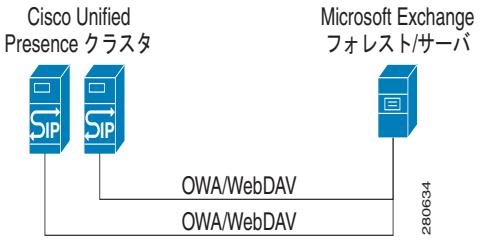
Cisco Unified Presence と Microsoft Exchange 2003 および 2007 の統合：WebDAV 経由

WebDAV インターフェイス経由での Exchange 統合の概要

Microsoft Exchange サーバ（バージョン 2003 および 2007）は、WebDav による予定表の統合をサポートしています。図 1 は、Exchange サーバによって公開される WebDAV インターフェイス上で Outlook Web Access（OWA）プロトコルを使用して Microsoft Exchange サーバ（バージョン 2003 および 2007）を Cisco Unified Presence に統合する方法を示しています。

Cisco Unified Presence は、1 つの WebDav フロントエンド Exchange サーバとのみ通信できます。Exchange フロントエンド サーバは、ユーザが Webdav のセットアップ時に設定する複数の Exchange バックエンド サーバと通信します。Microsoft Exchange は、Cisco Unified Presence 上の Exchange サーバに対して設定されたプレゼンス ゲートウェイを介して Cisco Unified Presence と通信します。

図 1　　Microsoft Exchange と Cisco Unified Presence アーキテクチャの統合



Exchange 2003 および 2007 の管理役割と権限

Microsoft Exchange 2003 および 2007 では、管理者が Exchange サーバ上のユーザ メールボックスへのサイン インをデフォルトで拒否されます。Cisco Unified Presence が Exchange サーバ上のメールボックス ストアに接続し、エンドユーザの予定表データを照会するためには、「Receive As」アカウントと呼ばれる、特別な権限を持つ Exchange アカウントが必要です。

次の作業

第 2 章「Cisco Unified Presence と統合（WebDAV 経由）するための Microsoft Exchange Server 2003 および 2007 の設定」

この統合に伴う既知の問題

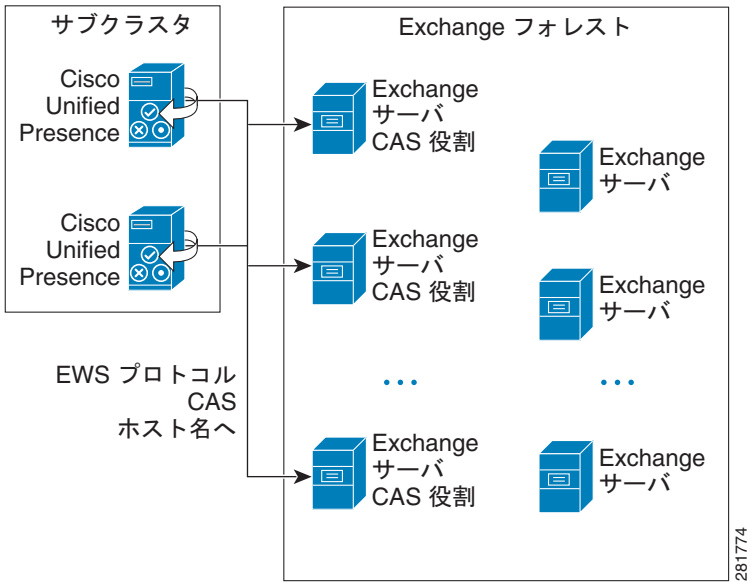
WebDAV による統合に影響することが明らかになっている問題については、このガイドの「Exchange 予定表統合のトラブルシューティング」を参照してください。「Microsoft Exchange の統合に影響することが確認されている問題」（P.6-5）を参照してください。

Cisco Unified Presence と Microsoft Exchange 2007 および 2010 の統合：Exchange Web サービス（EWS）経由

EWS インターフェイス経由での Exchange 統合の概要

Microsoft Exchange 2007 では、WebDAV に加え、Exchange Web Services（EWS; Exchange Web サービス）でも SOAP に似た Exchange サーバ インターフェイスを使用して予定表を統合できます。Microsoft Exchange 2010 では、WebDAV がサポートされなくなったため、EWS を使用する方法でのみ予定表を統合できます。

（注）　会議通知機能および Cisco IP Phone Messenger 機能は、Microsoft Exchange 2003 または 2007 を WebDAV 経由で統合した場合にのみ有効になります。EWS 統合では、Cisco IP Phone Messenger の [今日の会議（Today's Meeting）] 設定は機能しません。



Exchange 2007 および 2010 の管理役割と権限

すべてのユーザ アカウントにアクセスするために WebDAV アクセスに特別なアカウントが必要であるのと同じように、EWS でも同様の機能が必要となります。EWS では、指定アカウントに「役割」を割り当てることにより、この機能を管理します。この役割は偽装権限を持っています。

Microsoft Exchange Server 2007

呼び出し元が Exchange 2007 サーバ上の別のユーザの電子メール アカウントにアクセスするためには、EWS 統合に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、自身のアカウントに付与された権限ではなく偽装されたアカウントに付与された権限を使用してユーザ アカウントを偽装します。

偽装されたアカウントは、Exchange 2007 を実行する Client Access Server（CAS; クライアント アクセス サーバー）に対する **ms-Exch-EPI-Impersonation** 権限を取得する必要があります。これにより、呼び出し元は、CAS サーバを使用してユーザの電子メール アカウントを偽装する権限を得ることができます。さらに、呼び出し元は、メールボックス データベースとディレクトリ内の個々のユーザ オブジェクトのいずれかに対する **ms-Exch-EPI-MayImpersonate** 権限も取得する必要があります。

個々のユーザの Access Control List（ACL; アクセス コントロール リスト）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

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

- 管理役割グループ：Exchange のセットアップ プロセス中に 11 のデフォルト管理役割グループが提示されます。各グループには、その役割に固有の権限が関連付けられています。組み込まれている役割グループの例として、「受信者の管理」と「ヘルプ デスク」があります。通常、特定のタスクを実行する必要のあるスーパー ユーザは、該当する管理役割グループに割り当てられ、そのグループの権限を継承します。たとえば、製品サポート担当者は、Exchange 組織内のすべてのユーザの連絡先情報を変更できる必要があるため、ヘルプ デスク管理役割グループに割り当てます。
- 管理役割の割り当てポリシー：管理者やスーパー ユーザではない通常のユーザについては、管理役割の割り当てポリシーによって、変更できるメールボックスを決定します。**New-ManagementRoleAssignment** コマンドレットを使用してユーザに **ApplicationImpersonation** 役割を割り当てると、アカウントが組織内のユーザを偽装し、そのユーザの代わりにタスクを実行できます。役割の割り当ての適用範囲は、**New-ManagementScope** コマンドレットを使用して個別に管理され、特定の受信者またはサーバを対象としてフィルタリングできます。

（注）　RBAC では、Exchange Server 2007 で必要となる ACL の変更および管理は不要です。

Microsoft Exchange Server 2007 および 2010 と統合する場合のプレゼンス ゲートウェイの設定

多数のユーザをサポートするためには（EWS による予定表との統合を有効にした場合）、Cisco Unified Presence が EWS トラフィックの負荷を複数の CAS サーバに分散する必要があります。Cisco Unified Presence は、EWS を介して複数の CAS サーバに接続でき、このラウンド ロビン方式を使用してトラフィック負荷に対応します。

- 最初にユーザの予定表購読を有効にしたときには、そのユーザには管理者によって設定された対象 CAS ホストのプールから CAS が割り当てられます。
- ユーザへの割り当ては、そのユーザの予定表購読が失敗するまで保持されます。
- ユーザの予定表購読が失敗した場合は、対象 CAS ホストのプールから CAS サーバが再度割り当てられます。
- Cisco Unified Presence が中間証明書チェーンを信頼できるように、各 CAS に固有の中間証明書が必要です。

（注）　Cisco Unified Presence の本リリースは、Microsoft Exchange の自動検出サービスをサポートしていません。自動検出サービスは、CAS サーバにロードバランシング メカニズムが組み込まれていることを前提とします。

Cisco Unified Presence の管理画面で Exchange 統合用に EWS プレゼンス ゲートウェイを設定するときには、次の点に留意してください。

- WebDAV サーバと EWS サーバの混在環境を展開することはできません。1 つの WebDAV サーバと 1 つ以上の EWS サーバ ゲートウェイのいずれかを設定する必要があり、両方を設定することはできません。
- *1 つまたは複数の* EWS サーバを追加、更新、削除でき、サーバ数に上限はありません。ただし、[プレゼンス ゲートウェイ（Presence Gateway）] ウィンドウの [トラブルシュータ（Troubleshooter）] では、設定された EWS サーバのうち最初の 10 台についてのみステータスを確認および報告できます。
- EWS サーバ ゲートウェイは、EWS サーバ ゲートウェイに対して設定されたクレデンシャル（アカウント名とパスワード）を共有します。1 つの EWS サーバ ゲートウェイのクレデンシャルを変更すると、設定されている *すべての* EWS ゲートウェイのクレデンシャルが同じように変更されます。
- 1 つまたは複数の EWS サーバを追加、更新、または削除した *後* で、設定を有効にするために、Cisco UP プレゼンス エンジンを再起動する必要があります。複数の EWS サーバを 1 つずつ追加する場合は、Cisco UP プレゼンス エンジンを 1 回再起動するだけで、一度にすべての変更を有効にできます。

次の作業

第 3 章「Cisco Unified Presence と統合（EWS 経由）するための Microsoft Exchange Server 2007 および 2010 の設定」

この統合に伴う既知の問題

EWS による統合に影響することが明らかになっている問題については、このガイドの「Exchange 予定表統合のトラブルシューティング」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」（P.6-5）を参照してください。

必要な設定タスク

Microsoft Exchange の Cisco Unified Presence 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てください。

表 1-2　互換性マトリクス

コンポーネント	互換性のあるバージョン
Windows Server	• Windows Server 2003 の最新のサービス パック（SP2） • Windows Server 2008 の最新のサービス パック（SP2）
Cisco Unified Communications Manager	Release 6.x 以降
Cisco Unified Presence	Release 8.5
Microsoft Exchange Server 2003	Microsoft Exchange 2003 の最新のサービス パック（SP2）
Microsoft Exchange Server 2007	Microsoft Exchange 2007 の最新のサービス パック（SP1）
Microsoft Exchange Server 2010	Microsoft Exchange 2010 の最新のサービス パック（SP1）
Active Directory	• Active Directory 2003 with Windows Server 2003（SP2） -- または -- • Active Directory 2008 with Windows Server 2008（SP2） **（注）** Active Directory 内のユーザ名は、Cisco Unified Communications Manager に定義されたユーザ名と一致している必要があります。
サードパーティ証明書または証明書サーバ	証明書を作成するためには、これらのいずれかが必要。

関連事項

クライアント アプリケーションで予定表ステータスを設定するには、Cisco Unified Presence の [ユーザ オプション（User Options）] ページを使用します。

詳細な情報の取得

Cisco Unified Presence のマニュアル

http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

Cisco Unified Communications Manager のマニュアル

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

Microsoft Exchange 2003 のマニュアル

http://technet.microsoft.com/en-us/library/bb123872.aspx

Microsoft Exchange 2007 のマニュアル

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

- Exchange 2007 で Outlook Web アクセスに対して FBA を設定する方法については、次のサイトを参照してください。

  http://technet.microsoft.com/en-us/library/aa998867(EXCHG.80).aspx

Microsoft Exchange 2010 のマニュアル

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

Microsoft Active Directory のマニュアル

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

詳細な情報の取得

CHAPTER 2

Cisco Unified Presence と統合（WebDAV 経由）するための Microsoft Exchange Server 2003 および 2007 の設定

（注） このモジュールでは、**WebDAV 経由**での Cisco Unified Presence と Microsoft Exchange Server 2003 および 2007 の統合について説明します。Exchange Web Services（EWS; Exchange Web サービス）経由で Exchange Server 2007 または 2010 を統合する場合は、第 3 章「Cisco Unified Presence と統合（EWS 経由）するための Microsoft Exchange Server 2007 および 2010 の設定」を参照してください。2 種類の Exchange 統合の概要については、第 1 章「Cisco Unified Presence と Microsoft Exchange の統合の計画」を参照してください。

Microsoft Exchange 2003 設定チェックリスト（WebDAV）

表 2-1 は、Microsoft Exchange 2003 サーバ上のメールボックスへのアクセスを設定するときに従う必要のあるチェックリストです。詳細については、Microsoft Server 2003 のマニュアル（http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx）を参照してください。

表 2-1　Microsoft Exchange 2003 コンポーネントの設定作業

作業	手順	重要な注意事項
サービス アカウントを作成し、「Exchange 表示専用管理者」セキュリティ グループのメンバとして追加する。	1. Exchange サーバの **Active Directory ユーザーとコンピュータ**（ADUC）で新しいサービス アカウントを作成します。 2. Exchange サーバの **Active Directory ユーザーとコンピュータ**（ADUC）で新しいセキュリティ グループを作成します。そのセキュリティ グループに「Exchange 表示専用管理者」という名前を付けます。 3. 作成した Exchange 表示専用管理者グループを右クリックし、[プロパティ（Properties）] を選択します。[メンバー（Members）] タブで、このグループに作成したサービス アカウントを追加します。 4. Exchange サーバでシステム マネージャを開き、[管理グループ（Administrative Groups）] で [Exchange 表示専用管理者（Exchange View Only Administrator）] グループまで移動します。 5. このグループを右クリックし、[制御の委任（Delegate Control）] を選択して、Exchange 管理委任ウィザードを開始します。 6. [追加（Add）] を選択し、作成したグループまで移動して選択します。 7. そのグループに Exchange 表示専用管理者の役割を割り当てます。	Exchange サーバに管理者アカウントが既に設定されている場合があります。その場合でも、デフォルトの管理者設定では Exchange サーバ上の他のユーザ アカウントにサイン インできないことがあるため、Exchange 統合用の管理者アカウントを別途作成することを推奨します。
ユーザ アカウントを作成し、そのユーザ アカウントに Exchange 表示専用管理者の権限を委任する。	1. Exchange サーバに新しいユーザ アカウントを作成します。 2. Exchange サーバでシステム マネージャを開き、[管理グループ（Administrative Groups）] で、作成したアカウントを追加する管理グループまで移動します。 3. このグループを右クリックし、[制御の委任（Delegate Control）] を選択して、Exchange 管理委任ウィザードを開始します。 4. [追加（Add）] を選択し、作成したユーザ アカウントまで移動して選択します。 5. そのアカウントに Exchange 表示専用管理者の役割を割り当てます。	Exchange 2003 環境では、管理者（Exchange 表示専用の権限を持つ）だけが Exchange サーバ上のユーザ アカウントにサインインして Exchange 設定を表示できるように、このユーザ アカウントに「Exchange 表示専用管理者」権限を委任する必要があります。 ユーザ アカウントは、一般の Exchange ユーザが使用する標準の Windows アカウントです。
ユーザ メールボックスに対する Receive As 権限を付与する。	1. Exchange サーバでシステム マネージャを開き、[管理グループ（Administrative Groups）] で、[最初の管理グループ（First Administrative Group）] > [サーバー（Servers）] > [最初のサーバー（First Server）] > [メールボックス ストア（Mailbox Store）] を選択します。 2. メールボックス ストアを右クリックし、[プロパティ（Properties）] を選択します。[セキュリティ（Security）] タブで、予定表の情報にアクセスする必要のあるアカウントの名前を入力します。 3. その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 Receive As 権限を割り当てます。	Cisco Unified Presence では、Exchange サーバ上のユーザの予定表を調べるために追加の Receive As アカウント権限が必要です。この権限を上位レベル（メール ストレージ グループなど）で割り当て、メール ストレージ グループ内のすべてのメールボックスに対する読み取り専用アクセスを有効にすることを推奨します。

トラブルシューティングのヒント

- Cisco Unified Presence は、Exchange サーバへの接続時にアカウントへのサイン インを可能にするためにのみ、そのアカウントに Receive As 権限を必要とします。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。
- Exchange サーバがダウンしていることを示すエラー メッセージが表示され、証明書が正しく設定されている場合は、Receive As アカウントが適切に設定されていません。上記の手順に従ってアカウントを再作成してください。

次の作業

「Exchange 2003 アカウントの権限の確認」（P.2-3）

Exchange 2003 アカウントの権限の確認

手順

ステップ 1　Internet Explorer を使用して次の URL に接続します。

https://server/exchange/user@domain

server にはサーバ名、user にはユーザ名（Receive As アカウント以外のユーザ）、domain には= Exchange ドメインをそれぞれ入力します。

ステップ 2　Receive As クレデンシャルを使用してサイン インします。このクレデンシャルによって OWA アカウントにアクセスできる場合は、権限が Exchange サーバまで正しく伝播されたことを意味します。

次の作業

「Microsoft Exchange と統合する場合の Cisco Unified Presence でのプレゼンス ゲートウェイの設定」（P.4-1）

トラブルシューティングのヒント

この手順は、Microsoft Exchange Server 2003 SP1 以降のリリースを対象とします。

Microsoft Exchange 2007 設定チェックリスト（WebDAV）

表 2-2 は、Microsoft Exchange 2007 サーバ上のメールボックスへのアクセスを設定するときに従う必要のあるチェックリストです。詳細については、Microsoft Server 2007 のマニュアル（http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx）を参照してください。

表 2-2　Microsoft Exchange 2007 コンポーネントの設定作業

作業	手順	重要な注意事項
Exchange 表示専用管理者アカウントにメールボックスを追加する。	1. Exchange 表示専用管理者の役割を委任されているアカウントを使用して Exchange 2007 サーバにサイン インします。 2. Exchange 2007 サーバ上で Exchange Management Console（EMC; Exchange 管理コンソール）を開きます。 3. コンソール ツリーで [受信者の構成（Recipient Configuration）] を選択します。 4. [メールボックスの新規作成（New Mailbox）] を選択し、[メールボックスの新規作成（New Mailbox）] ウィザードを完了します。 – [ユーザー ログオン名（ユーザー プリンシパル名）（User Logon Name (User Principal Name)）] には、ユーザ アカウントが属する Microsoft ドメインの名前に続けてユーザがメールボックスにサイン インするために必要な名前を入力します。 例：**msoft-domain-name¥username**	指定のストレージにメールボックスを持たないアカウントは機能せず、いずれかの段階でメールボックスを削除した場合、そのアカウントは機能を停止します。

アカウントに Exchange 表示専用管理者の権限を委任する。	**Exchange Management Console（EMC; Exchange 管理コンソール）を使用する場合**
	1. Exchange 2007 サーバ上で EMC を開きます。
	2. コンソール ツリーで [Organization Configuration] を右クリックします。
	3. [Exchange 管理者の追加（Add Exchange Administrator）] を選択し、作成したアカウントまで移動して選択します。
	4. そのアカウントに Exchange 表示専用管理者の役割を割り当てます。
	Exchange Management Shell（EMS; Exchange 管理シェル）を使用する場合
	1. コマンド ライン入力を行うために EMS を開きます。
	2. Run 行または EMS のコマンド プロンプトから、関連する引数を指定して Add-Exchange コマンドを実行します。
	このコマンドの構文と例を次に示します。
	構文
	`Add-ExchangeAdministrator -Role "role" -Identity "identity"`
	例
	`Add-ExchangeAdministrator -Role ViewOnlyAdmin -Identity CUPSAdmin`
		• Exchange 2007 環境では、管理者（Exchange 表示専用の権限を持つ）だけが Exchange サーバ上のユーザ アカウントにサイン インして Exchange 設定を表示できるように、このユーザ アカウントに「Exchange 表示専用管理者」権限を委任する必要があります。
		• ユーザ アカウントは、一般の Exchange ユーザが使用する標準の Windows アカウントです。

作業	手順	重要な注意事項

ユーザ メールボックスに対する Receive As 権限を付与する。	**Exchange Management Shell（EMS; Exchange 管理シェル）を使用する場合**
	1. コマンド ライン入力を行うために EMS を開きます。
	2. EMS で次のように Add-ADPermission コマンドを実行します。
	構文
	`Add-ADPermission -Identity "Mailbox Store" -User "Trusted User" -ExtendedRights Receive-As`
	例
	`Add-ADPermission -Identity "First Storage Group" -User CUPSAdmin -ExtendedRights Receive-As`
		この手順を実行するために、Exchange Management Console（EMC; Exchange 管理コンソール）を使用することはできません。

トラブルシューティングのヒント

- Cisco Unified Presence は、Exchange サーバへの接続時にアカウントへのサイン インを可能にするためにのみ、そのアカウントに Receive As 権限を必要とします。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。
- Exchange サーバがダウンしていることを示すエラー メッセージが表示され、証明書が正しく設定されている場合は、Receive As アカウントが適切に設定されていません。上記の手順に従ってアカウントを再作成してください。

次の作業

「Exchange 2007 アカウントの権限の確認」（P.2-5）

Exchange 2007 アカウントの権限の確認

Exchange 2007 アカウントに権限を割り当てた後で、その権限がメールボックス レベルまで伝播され、エンドユーザのメールボックスにアクセスできることを確認する必要があります。Exchange 2007 では、権限がメールボックスに伝播されるまでに時間を要します。

はじめる前に

- Exchange アカウントに適切な役割と Receive-As 権限を委任してください。「Microsoft Exchange 2007 設定チェックリスト」を参照してください。
- 次の手順の例では、Exchange アカウントが「cupsadmin」であり、メール ストレージ グループの名前が「First Storage Group」であることを前提とします。

手順

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

ステップ 2　次のように Exchange アカウントが「Exchange 表示専用管理者」グループのメンバであることを確認します。

a. EMS で次のコマンドを実行します。

```
([ADSI]"LDAP://CN=CUPS Admin,CN=Users,DC=r7,DC=com").memberof
```

（注）「CN=CUPS Admin,CN=Users,DC=r7,DC=com」は、Exchange アカウントの Distinguished Name（DN; 識別名）です。DN を確認するには、**adsiedit.msc** を使用します。また、必要な場合は Active Directory 管理者に DN を問い合わせてください。

b. 次のように、Exchange アカウントが「Exchange 表示専用管理者」グループのメンバであることがコマンド出力に示されていることを確認します。

例：コマンド出力

CN=Exchange View-Only Administrators,	OU=Microsoft Exchange Security Groups,	DC=r7,	DC=com

ステップ 3　次のように、Exchange アカウントにメール ストレージ グループに対する「Receive-As」権限があ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-ADPermission "First Storage Group" -user cupsadmin | Format-Table -AutoSize
```

（注）「First Storage Group」は、メール ストレージ グループの名前です。「cupsadmin」は、Exchange アカウントです。

b. 次のように、Exchange アカウントがメール ストレージ グループに対する「Receive-As」権限を持っていることがコマンド出力に示されていることを確認します。

例：コマンド出力

Identity ------	User ----	Deny ---	Inherited -------	Rights -----
HTLUO-MAIL¥First Storage Group	R7¥cupsadmin	False	False	Receive-As

ステップ 4　次のように、Exchange アカウントがエンドユーザのメールボックスに対する権限を持っ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-MailboxPermission jdoe -user cupsadmin | Format-Table -autosize
```

（注）「jdoe」は、エンドユーザのメールボックスです。「cupsadmin」は、Exchange アカウントです。

b. 次のように、Exchange アカウントが jdoe のメールボックスに対する FullAccess 権限を持っていることがコマンド出力に示されていることを確認します。

例：コマンド出力

Identity ------	User ----	AccessRights --------	IsInherited --------	Deny ---
r7.com/Dallas/John Doe	R7¥cupsadmin	{FullAccess}	True	False

トラブルシューティングのヒント

ユーザ メールボックスに対するフル アクセス権限は、最上位の権限（この例では「First Storage Group」）から継承されます。コマンド（ステップ 4 で実行したコマンド以外）が出力を返さない場合は、権限がメールボックスまで伝播されていないことを意味します。Exchange アカウントがエンド ユーザのメールボックスに対して FullAccess 権限を持つまで、*先に進まないでください*。

次の作業

「Microsoft Exchange と統合する場合の Cisco Unified Presence でのプレゼンス ゲートウェイの設定」（P.4-1）

Exchange 2003/2007 仮想ディレクトリの認証の有効化

Microsoft Office Outlook Web アクセスが正しく動作するためには、Exchange 仮想ディレクトリ（/exchange または /exchweb）の基本認証を有効にする必要があります。/exchange ディレクトリは、OWA および WebDAV へのメールボックス アクセス要求を処理します。/exchweb ディレクトリには、OWA および WebDAV が使用するリソース ファイルが含まれています。

次の手順は、Windows Server 2003 を実行する Exchange 2003 および Exchange 2007 サーバでの WebDAV 統合を対象とします。

手順

ステップ 1　[Administrative Tools] から [Internet Information Services] を開き、サーバを選択します。

ステップ 2　[Web Sites] を選択します。

ステップ 3　[Default Web Site] を選択します。

ステップ 4　[/exchange] または [/exchweb] を右クリックし、[Properties] を選択します。

ステップ 5　[Directory Security] タブを選択します。

ステップ 6　[Authentication and Access Control] で、[Edit] を選択します。

ステップ 7　[Authentication] で [Basic Authentication] チェックボックスと [Integrated Windows] チェックボックスがオンになっていることを確認します。

関連事項

- http://technet.microsoft.com/en-us/library/aa998849(EXCHG.80).aspx
- 既知の問題：「Exchange 2007 から「HTTP 503 サービス利用不可（HTTP 503 Service Unavailable）」エラーが返され、予定表の統合が失敗する」（P.6-9）を参照

CHAPTER 3

Cisco Unified Presence と統合（EWS 経由）するための Microsoft Exchange Server 2007 および 2010 の設定

（注） このモジュールでは、**Exchange Web Services（EWS; Exchange Web サービス）経由での** Cisco Unified Presence と Microsoft Exchange Server 2007 および 2010 の統合について説明します。WebDAV 経由で Exchange Server 2003 または 2007 を統合する場合は、第 2 章「Cisco Unified Presence と統合（WebDAV 経由）するための Microsoft Exchange Server 2003 および 2007 の設定」を参照してください。2 種類の Exchange 統合の概要については、第 1 章「Cisco Unified Presence と Microsoft Exchange の統合の計画」を参照してください。

Microsoft Exchange 2007 設定チェックリスト（EWS）

はじめる前に

Exchange 2007 サーバの設定手順は、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。

表 3-1 は、Windows Server 2003 および Window Server 2008 で実行される Microsoft Exchange 2007 サーバ上のメールボックスへのアクセスを設定するときに従う必要のあるチェックリストです。詳細については、Microsoft Server 2007 のマニュアル（http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx）を参照してください。

表 3-1　Microsoft Exchange 2007 コンポーネントの設定作業

作業	手順	重要な注意事項
ユーザにサービス アカウントにローカルでサイン インするための権限を付与する。	**Windows Server 2003 上の Exchange 2007 設定** **1.** Exchange 表示専用管理者の役割を委任されているサービス アカウントを使用して Exchange 2007 サーバにサイン インします。 **2.** Exchange サーバで [ドメイン コントローラ セキュリティの設定（Domain Controller Security Settings）] ウィンドウを開きます。 **3.** 左側のフレームの [セキュリティ設定（Security Settings）] で [ローカル ポリシー（Local Policies）] > [ユーザー権利の割り当て（User Rights Assignments）] を選択します。 **4.** コンソールの右側のフレームで [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。 **5.** [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。 **6.** [名前の確認（Check Names）] を選択し、指定されたユーザが正しいことを確認します。[OK] をクリックします。 **Windows Server 2008 上の Exchange 2007 設定** **1.** Exchange 表示専用管理者の役割を委任されているサービス アカウントを使用して Exchange 2007 サーバにサイン インします。 **2.** [開始（Start）] を選択します。 **3.**「gpmc.msc」と入力します。 **4.** Enter を押します。 **5.** Exchange サーバで [ドメイン コントローラ セキュリティの設定（Domain Controller Security Settings）] ウィンドウを開きます。 **6.** 左側のフレームの [セキュリティ設定（Security Settings）] で [ローカル ポリシー（Local Policies）] > [ユーザー権利の割り当て（User Rights Assignments）] を選択します。 **7.** コンソールの右側のフレームで [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。 **8.** [これらのポリシーの設定を定義する（Define these policy settings）] チェックボックスがオンになっていることを確認します。 **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。[OK] をクリックします。 **10.** [名前の確認（Check Names）] を選択し、指定されたユーザが正しいことを確認します。[OK] をクリックします。 **11.** [ローカル ログオンを許可する（Allow Log On Locally）] を右クリックして [プロパティ（Properties）] を選択し、表示されるダイアログ ボックスで [適用（Apply）] と [OK] をクリックします。 **12.** ユーザ SMTP アドレスが *alias @ FQDN* であることを確認します。そうでない場合は、User Principal Name（UPN; ユーザー プリンシパル名）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。	• Exchange 偽装が動作するためには、すべての Exchange サーバが Windows Authorization Access Group のメンバであることが必要です。 • サービス アカウントは、Exchange 管理グループのメンバ*であってはなりません*。Microsoft Exchange は、Exchange 管理グループに属するすべてのアカウントについて、偽装を明示的に拒否します。

作業	手順	重要な注意事項

偽装権限をサーバ レベルで設定する。	**Exchange Management Shell（EMS; Exchange 管理シェル）を使用する場合**
	1. コマンド ライン入力を行うために EMS を開きます。
	2. 次の Add-ADPermission コマンドを実行してサーバに対する偽装権限を追加します。
	構文
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -AccessRights GenericAll -InheritanceType Descendents`
	例
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -AccessRights GenericAll -InheritanceType Descendents`
		• これらのコマンドレットは、偽装権限をサーバ レベルで付与します。データベース、ユーザ、および連絡先のレベルで権限を付与することもできます。
		• 複数のサーバがある場合は、各サーバ（またはデータベース）への偽装権限を付与する必要があります。Exchange 2007 には、システム全体を対象とする偽装権限の機能はありません。
		• ユーザの SMTP アドレスが alias@FQDN と定義されていることを確認します。そうでない場合は、User Principal Name（UPN; ユーザー プリンシパル名）を使用してユーザ アカウントを偽装する必要があります。

サービス アカウントの Active Directory サービス拡張権限を設定する。	**Exchange Management Shell（EMS; Exchange 管理シェル）を使用する場合**
	1. 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（Exch2007 など）のサーバに対する偽装権限を追加します。
	構文
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation`
	例
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation`
	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-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate`
	例
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate`
		• これらの権限は、偽装を実行するサービス アカウントについて（Client Access Server（CAS; クライアント アクセス サーバー）上で）設定する必要があります。
		• CAS がロード バランサの背後に位置する場合は、ロード バランサの背後にある *すべての* CAS サーバについて、Ex2007 アカウントに **ms-Exch-EPI-Impersonation** 権限を付与します。
		• メールボックス サーバが CAS とは異なるマシン上にある場合は、すべてのメールボックス サーバについて、Ex2007 アカウントに **ms-Exch-EPI-Impersonation** 権限を付与します。
		• この権限は、[Active Directory サイトとサービス（Active Directory Sites and Services）] または [Active Directory ユーザーとコンピュータ（Active Directory Users and Computers）] ユーザ インターフェイスを使用して設定することもできます。

作業	手順	重要な注意事項

サービス アカウントおよびユーザ メールボックスに Send As 権限を付与する。	**Exchange Management Shell（EMS; Exchange 管理シェル）を使用する場合**
	EMS で次の Add-ADPermission コマンドを実行して、サービス アカウントおよび関連するすべてのユーザ メールボックス ストアに Send As 権限を付与します。
	構文
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -ExtendedRights Send-As`
	例
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRights Send-As`
		この手順を実行するために、Exchange Management Console（EMC; Exchange 管理コンソール）を使用することはできません。

サービス アカウントおよびユーザ メールボックスに Receive As 権限を付与する。	**Exchange Management Shell（EMS; Exchange 管理シェル）を使用する場合**
	EMS で次の Add-ADPermission コマンドを実行して、サービス アカウントおよび関連するすべてのユーザ メールボックス ストアに Receive As 権限を付与します。
	構文
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity User | select-object).identity -ExtendedRights Receive-As`
	例
	`Add-ADPermission -Identity (get-exchangeserver).DistinguishedName -User (Get-User -Identity Ex2007 | select-object).identity -ExtendedRights Receive-As`
		この手順を実行するために、Exchange Management Console（EMC; Exchange 管理コンソール）を使用することはできません。

トラブルシューティングのヒント

Cisco Unified Presence は、Exchange サーバへの接続時にアカウントへのサイン インを可能にするためにのみ、そのアカウントに Receive As 権限を必要とします。このアカウントは、通常、メールを受信しないため、領域の割り当てについて考慮する必要はありません。

次の作業

「Exchange 2007 アカウントの権限の確認」（P.3-4）

Exchange 2007 アカウントの権限の確認

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

はじめる前に

Exchange アカウントに適切な権限を委任してください。「Microsoft Exchange 2007 設定チェックリスト（EWS）」を参照してください。

手順

ステップ 1　Exchange 2007 サーバの 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　選択したサービス ノードに CAS が含まれていることを確認します。

ステップ 5　各 CAS サーバの [プロパティ（Properties）] を表示し、[セキュリティ（Security）] タブで次のことを確認します。

a. サービス アカウントが表示されている。

b. サービス アカウントに付与されている権限が（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。

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

トラブルシューティングのヒント

- アカウントまたは偽装権限がステップ 5 に示すとおりに表示されていない場合は、サービス アカウントを再作成し、そのアカウントに必要な偽装権限を付与することが必要となることがあります。
- 変更を有効にするために、Exchange サーバの再起動が必要となる場合があります。これはテストによって確認されています。

次の作業

「Exchange 2007/2010 仮想ディレクトリの認証を有効にする方法」（P.3-8）

Microsoft Exchange 2010 設定チェックリスト（EWS）

表 3-3 は、Microsoft Exchange 2010 サーバ上のメールボックスへのアクセスを設定するときに従う必要のあるチェックリストです。詳細については、Microsoft Server 2010 のマニュアル（http://technet.microsoft.com/en-us/library/bb124558.aspx）を参照してください。

はじめる前に

Microsoft Exchange 2010 サーバを EWS 経由で Cisco Unified Presence に統合する前に、Exchange サーバで次のスロットル ポリシー パラメータ値を設定してください。これらの値は、EWS 経由での Cisco Unified Presence との予定表統合が機能するために必要です。これらのパラメータ値を*変更しない*ことを推奨します。

表 3-2　Microsoft Exchange の推奨スロットル ポリシー パラメータ値

パラメータ	推奨設定値
EWSMaxConcurrency	シスコが実施したテストにおいて、このスロットル ポリシー パラメータはデフォルト値のままで予定表を使用する 50% のユーザをサポートするために十分であることが確認されました。ただし、CAS に対する EWS 要求の負荷が高い場合は、このパラメータを 100 に設定することを推奨します。
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60
EWSMaxSubscriptions	5000
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000

表 3-3　Microsoft Exchange 2010 コンポーネントの設定作業

作業	手順	重要な注意事項

特定のユーザまたはユーザのグループに Exchange 偽装権限を設定する。	**Exchange Management Shell（EMS; Exchange 管理シェル）を使用する場合**
	1. コマンド ライン入力を行うために EMS を開きます。
	2. EMS で New-ManagementRoleAssignment コマンドを実行し、指定したサービス アカウント（Ex2010 など）に他のユーザ アカウントを偽装する権限を付与します。
	構文
	`new-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation -User:user@domain`
	例
	`new-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation -User:Ex2010@domain`
	3. 次の New-ManagementRoleAssignment コマンドを実行して、偽装権限の適用範囲を定義します。この例では、Exch2010 アカウントに指定した Exchange サーバ上のすべてのアカウントを偽装する権限を付与します。
	構文
	`new-ManagementScope -Name:_suImpersonateScope -ServerList:<server name>`
	例
	`new-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227`
		EWS 自動検出サービスを使用するためには、Cisco Unified Communications Manager から Cisco Unified Presence に同期できるように、偽装ユーザに対して LDAP で明示的にメール ID が設定されていることが*必要*です。

次の作業

「Exchange 2010 アカウントの権限の確認」（P.3-7）

関連事項

Microsoft Exchange サーバ パラメータの詳細については、
http://technet.microsoft.com/en-us/library/dd351045.aspx を参照してください。

Exchange 2010 アカウントの権限の確認

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

はじめる前に

- Exchange アカウントに適切な権限を委任してください。「Microsoft Exchange 2010 設定チェックリスト（EWS）」を参照してください。

手順

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

ステップ 2　サービス アカウントに必要な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. 次のように、指定されたアカウントに役割「ApplicationImpersonation」が割り当てられていることがコマンド出力に示されていることを確認します。

例：コマンド出力

Name ------	Role ----	RoleAssigneeName ------------	RoleAssignee Type ------	Assignment Method -----	EffectiveUser Name ----------
_suImpersonate RoleAsg	ApplicationImpe rsonation	ex 2010	User	Direct	ex 2010

ステップ 3　サービス アカウントに適用される管理適用範囲が正しいことを確認します。

a. EMS で次のコマンドを実行します。

```
Get-ManagementScope _suImpersonateScope
```

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

例：コマンド出力

Name ------	ScopeRestrictionType ----	Exclusive --------	RecipientRoot ------	Recipient Filter -----	ServerFilter ----------
_suImpersonate Scope	ServerScope	False			Distinguished Name

次の作業

「Exchange 2007/2010 仮想ディレクトリの認証を有効にする方法」（P.3-8）

Exchange 2007/2010 仮想ディレクトリの認証を有効にする方法

Microsoft Office Outlook Web アクセスが正しく動作するためには、Exchange 仮想ディレクトリ（/exchange または /exchweb）の基本認証を有効にする必要があります。/exchange ディレクトリは、OWA および WebDAV へのメールボックス アクセス要求を処理します。/exchweb ディレクトリには、OWA および WebDAV が使用するリソース ファイルが含まれています。

- 「Windows Server 2003 を実行する Exchange 2007 の認証の有効化」（P.3-8）
- 「Windows Server 2008 を実行する Exchange 2010 の認証の有効化」（P.3-9）

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

手順

ステップ 1　[Administrative Tools] から [Internet Information Services] を開き、サーバを選択します。

ステップ 2　[Web Sites] を選択します。

ステップ 3　[Default Web Site] を選択します。

ステップ 4　[Exchange] または [Exchweb] ディレクトリ フォルダを右クリックし、[Properties] を選択します。

ステップ 5　[Directory Security] タブを選択します。

ステップ 6　[Authentication and Access Control] で、[Edit] を選択します。

ステップ 7　[Authentication] で、次のチェックボックスがオンになっていることを確認します。

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

次の作業

「Microsoft Exchange と統合する場合の Cisco Unified Presence でのプレゼンス ゲートウェイの設定」（P.4-1）

Windows Server 2008 を実行する Exchange 2010 の認証の有効化

手順

ステップ 1　Exchange 管理コンソールで、統合 Windows 認証を有効にする仮想ディレクトリに移動します。

ステップ 2　[Server Configuration] を選択します。

ステップ 3　[Client Access] を選択します。

ステップ 4　Outlook Web App 仮想ディレクトリをホストしているサーバを選択します。

ステップ 5　[Outlook Web App] タブを選択します。

ステップ 6　作業ウィンドウで、統合 Windows 認証を有効にする仮想ディレクトリを選択して右クリックします。

ステップ 7　[Properties] を選択します。

ステップ 8　[Authentication] タブを選択します。

ステップ 9　[Use one or more standard authentication methods] を選択します。

ステップ 10　[Basic Authentication (password is sent in clear text)] をオンにします。

ステップ 11　[OK] を選択します。

次の作業

「Microsoft Exchange と統合する場合の Cisco Unified Presence でのプレゼンス ゲートウェイの設定」（P.4-1）

関連事項

- http://technet.microsoft.com/en-us/library/aa998849.aspx
- http://technet.microsoft.com/en-us/library/ee633481.aspx

CHAPTER 4

Microsoft Exchange サーバと統合するための Cisco Unified Presence の設定

Microsoft Exchange と統合する場合の Cisco Unified Presence でのプレゼンス ゲートウェイの設定

Microsoft Exchange サーバ（Microsoft Outlook）を予定表情報の交換用のプレゼンス ゲートウェイとして設定する必要があります。Exchange ゲートウェイによって、Cisco Unified Presence サーバは、アベイラビリティ情報（予定表 / 会議ステータス）をユーザ単位でアベイラビリティ ステータスに反映できます。

この手順の設定オプションは、ネットワーク環境と次のうちどの統合を行うかによって異なります。

- Exchange 2003 を WebDAV 経由で Cisco Unified Presence に統合
- Exchange 2007 を WebDAV または Exchange Web Services（EWS; Exchange Web サービス）経由で Cisco Unified Presence に統合
- Exchange 2010 を EWS 経由で Cisco Unified Presence に統合

（注） それぞれの Exchange 統合の概要については、第 1 章「Cisco Unified Presence と Microsoft Exchange の統合の計画」を再読することを推奨します。

はじめる前に

1 つの WebDav サーバまたは複数の EWS サーバを設定できます。展開環境に WebDAV サーバと EWS サーバを混在させることは *できません*。

手順

ステップ 1 Cisco Unified Presence の管理画面にログインします。

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

ステップ 3　[新規追加（Add New）] を選択します。

ステップ 4　適切なプレゼンス ゲートウェイ タイプを選択し、Microsoft Exchange サーバを予定表情報の交換用のプレゼンス ゲートウェイとして設定します。

統合形式	選択するプレゼンス ゲートウェイ タイプ	設定手順
Exchange 2003 または 2007 サーバを WebDAV 経由で統合	**Exchange -- WebDAV**	**1.** [説明（Description）] フィールドに、複数のタイプ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 インスタンスの区別に役立つ意味のある説明を入力します。 **2.** [プレゼンス ゲートウェイ（Presence Gateway）] フィールドには、プレゼンス ゲートウェイのサーバの場所を入力します。これは、Exchange サーバの IIS 証明書の件名 Common Name（CN; 共通名）と一致している必要があります。Microsoft Exchange サーバに接続するには、次のいずれかの値を使用する必要があります。 – FQDN – DNS SRV FQDN – IP アドレス 詳細については、「トラブルシューティングのヒント」を参照してください。 **3.** [アカウント名（Account Name）] フィールドには、Cisco Unified Presence が Microsoft Exchange サーバに接続するときに使用する Receive-As アカウントの名前を <domain>¥<username> の形式で入力します。このとき、次の点に留意してください。 – Exchange サーバがデフォルト ドメインを指定する設定になっている場合は、ユーザ名にドメインを含める必要がない可能性があります。 – それ以外の場合は、証明書エラー（401 および 404 認証応答）の発生を防ぐために、アカウント名の前にドメインを指定してください。 詳細については、「トラブルシューティングのヒント」を参照してください。 **4.** Cisco Unified Presence が Microsoft Exchange サーバに接続するために必要となる Microsoft Exchange アカウント パスワードを入力し、確認します。確認のためもう一度パスワードを入力します。この値は、Microsoft Exchange サーバ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。 **5.** Microsoft Exchange サーバとの接続に使用するポートを入力します。Cisco Unified Presence と Microsoft Exchange との統合は、セキュアな HTTP 接続を介して行う必要があります。ポート 443（デフォルト ポート）を使用し、それ以外のポートに変更しないことを推奨します。

統合形式	選択するプレゼンス ゲートウェイ タイプ	設定手順
Exchange 2007 または 2010 サーバを EWS 経由で統合し、Exchange サーバのアドレスを指定する	**Exchange -- EWS Server**	1. [説明（Description）] フィールドに、複数のタイプ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 インスタンスの区別に役立つ意味のある説明を入力します。 2. [プレゼンス ゲートウェイ（Presence Gateway）] フィールドには、プレゼンス ゲートウェイのサーバの場所を入力します。これは、Exchange サーバの IIS 証明書の件名 Common Name（CN; 共通名）と一致している必要があります。Microsoft Exchange サーバに接続するには、次のいずれかの値を使用する必要があります。 – FQDN – DNS SRV FQDN – IP アドレス 詳細については、「トラブルシューティングのヒント」を参照してください。 3. Cisco Unified Presence が Microsoft Exchange サーバに接続するときに使用する偽装アカウントの名前を e-mail address: user@domain の形式で入力します。 詳細については、「トラブルシューティングのヒント」を参照してください。 4. Cisco Unified Presence が Microsoft Exchange サーバに接続するために必要となる Microsoft Exchange アカウント パスワードを入力し、確認します。確認のためもう一度パスワードを入力します。この値は、Microsoft Exchange サーバ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。 5. Microsoft Exchange サーバとの接続に使用するポートを入力します。Cisco Unified Presence と Microsoft Exchange との統合は、セキュアな HTTP 接続を介して行う必要があります。ポート 443（デフォルト ポート）を使用し、それ以外のポートに変更しないことを推奨します。

次の作業

Outlook をプレゼンス ゲートウェイ タイプとして設定したら、次の点を確認してください。

1. Cisco Unified Presence と Exchange サーバとの接続は成功しましたか。[プレゼンス ゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [トラブルシュータ（Troubleshooter）] に接続ステータスが表示されます。修正が必要な場合は、「Exchange サーバ接続ステータスのトラブルシューティング」（P.6-1）を参照してください。
2. Exchange SSL 証明書チェーンのステータスは正しい（[確認が成功しました（Verified）]）ですか。[プレゼンス ゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [トラブルシュータ（Troubleshooter）] に証明書件名 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 / 証明書ステータスのトラブルシューティング」（P.6-2）を参照してください。
3. [任意] Cisco IP Phone Messenger 対応の電話機にユーザのスケジュールされた会議が表示されますか。詳細については、「Microsoft Exchange の統合に影響することが確認されている問題」（P.6-5）を参照してください。

4. [任意] 統合した予定表をローカライズする場合、Exchange サーバの URL に「Calendar」の訳語が含まれていますか。修正が必要な場合は、「Microsoft Exchange の統合に影響することが確認されている問題」（P.6-5）を参照してください。

トラブルシューティングのヒント

- [プレゼンス ゲートウェイ（Presence Gateway）] フィールドを設定するときには（WebDAV および EWS の設定）、次の要件に留意してください。
  - Cisco Unified Presence 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。Cisco Unified Presence は Subject Alternative Names（SAN; サブジェクトの別名）証明書をサポートしていないことに注意してください。そのため、1 つの SSL 証明書にホスト名のリストを指定することはできません。
  - [プレゼンス ゲートウェイ（Presence Gateway）] フィールドを設定するときには、Exchange サーバから受け取る証明書の件名と一致する FQDN を入力する必要があります。これは、証明書チェーンのリーフ証明書の件名 Common Name（CN; 共通名）値です。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。
- [アカウント名（Account Name）] フィールドと [パスワード（Password）] フィールドを設定するときには（EWS の設定）、次の要件に留意してください。
  - EWS サーバを追加し、さらに別のサーバを追加する場合、[アカウント名（Account Name）] フィールドと [パスワード（Password）] フィールドには、最初のサーバで入力したクレデンシャルがデフォルト値として入力されます。
  - EWS サーバでアカウント名とパスワードを変更すると、それらのクレデンシャルが設定済みのすべての EWS サーバに反映されます。
  - EWS サーバを追加、更新、または削除した場合、設定の変更を有効にするためには、Cisco UP プレゼンス エンジンを再起動する必要があります。複数の EWS サーバを 1 つずつ追加する場合は、Cisco UP プレゼンス エンジンを 1 回再起動するだけで、一度にすべての変更を有効にできます。サービスの再起動が必要なときには Cisco Unified Presence から通知があり（自動通知）、Cisco Unified サービスアビリティへ移動して Cisco UP プレゼンス エンジンを再起動できます（[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [ツール（Tools）] > [コントロール センタ - 機能サービス（Control Center - Feature Services）] の順に選択します）。
- DNS の設定については、次の点に留意してください。
  - Cisco Unified Presence で DNS を設定した場合は、リーフ証明書の件名 CN 値は FQDN または IP アドレスのいずれかになると考えられます。[プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値は、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。
  - Cisco Unified Presence で DNS を設定していない場合は、リーフ証明書の件名 CN 値は IP アドレスになります。件名 CN 値が IP アドレスでない場合は、件名 CN 値が Exchange サーバの IP アドレスになるようにこの Exchange 証明書を生成し直す必要があります。[プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値は、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。

[任意] EWS 経由で送信される Microsoft Exchange 予定表通知の頻度の設定

この手順は、Microsoft Exchange サーバ 2007 または 2010 を EWS 経由で統合する場合にのみ必要となります。予定表を WebDAV 経由で統合する場合、この手順を実行する*必要はありません*。

[EWS Status Frequency] パラメータは、Exchange サーバが Cisco Unified Presence 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。Cisco Unified Presence 上のプレゼンス エンジンがサブスクリプションを失ったことを 60 分（デフォルト）よりも短い間隔で検出する必要がある場合は、この間隔をデフォルト値より小さい値に変更してください。この間隔を短くすると、エラーの検出能力は向上しますが、それに伴って Exchange サーバおよび Cisco Unified Presence サーバへの負荷も増加します。

手順

ステップ 1　[Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [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（Server）] メニューから Cisco Unified Presence Server を選択します。

ステップ 3　[サービス（Service）] メニューから [Cisco UP プレゼンス エンジン（アクティブ）（Cisco UP Presence Engine (Active)）] を選択します。

ステップ 4　[EWS Status Frequency] フィールドのパラメータ値を編集します。このパラメータのデフォルト値は 60 分です。

ステップ 5　[保存（Save）] を選択します。

次の作業

[EWS Status Frequency] パラメータの変更は、ユーザ単位で予定表の統合が発生するたびに付加的に更新されます。ただし、すべてのユーザについてパラメータの変更を有効にするために、Cisco UP プレゼンス エンジンを再起動することを推奨します。[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [Tools] > [Service Activation] の順に選択します。

トラブルシューティングのヒント

このパラメータの最大値は 1440 分です。

[任意] 予定表を統合する場合の多言語サポートの設定方法

この手順は、Microsoft Exchange サーバ 2003 または 2007 を WebDAV 経由で統合する場合にのみ必要となります。予定表を EWS 経由で統合する場合、この手順を実行する*必要はありません*。

ユーザ ロケールは各国に固有であり、ユーザ ロケール ファイルには、ユーザ アプリケーションおよびユーザ Web ページの特定ロケールでの翻訳テキストが含まれています。Microsoft Exchange の展開環境を複数言語対応に拡張する場合は、予定表の統合で使用するユーザ ロケールをサポートするように Cisco Unified Communications Manager と Cisco Unified Presence を設定する必要があります。サポートされる言語の数に制限はありません。

- 「Cisco Unified Communications Manager へのロケール インストーラのインストール」（P.4-6）
- 「Cisco Unified Presence へのロケール インストーラのインストール」（P.4-7）
- 「多言語の予定表と統合する場合のユーザ ロケールの設定」（P.4-8）

Cisco Unified Communications Manager へのロケール インストーラのインストール

この手順を開始する前に、次の点に注意してください。

- Cisco Unified Communications Manager ロケール インストーラをインストールする前に、クラスタ内の各サーバに Cisco Unified Communications Manager（Release 6.x 以降）をインストールする必要があります。
- インストールされるロケールのデフォルト設定は、[English United States] です。Cisco Unified Communications Manager に適切な言語 / ロケールをインストールし、ユーザが最初にサイン インするときに Exchange サーバで適切な言語 / ロケールを選択することを強く推奨します。次の考慮事項は WebDAV 統合のみが対象となります。
  - Cisco Unified Communications Manager に別の言語 / ロケールがインストールされているときにエンド ユーザの Exchange メールボックスにデフォルト言語（英語）を設定した場合、それ以降にそのユーザのロケールを変更することはできません。この問題の詳細については、「WebDAV 経由で予定表との統合を行う場合のローカリゼーションに関する注意事項」（P.6-7）を参照してください。
  - 英語以外のロケールを設定する場合は、Cisco Unified Communications Manager と Cisco Unified Presence の*両方*に適切な言語インストーラをインストールする必要があります。クラスタ内のすべてのサーバにロケール インストーラをインストールしてください（パブリッシャ サーバにインストールしてからサブスクライバ サーバにインストールします）。
- 適切なすべてのロケール インストーラが*両方*のシステムにロードされるまで、ユーザ ロケールを*設定しない*でください。ロケール インストーラが Cisco Unified Communications Manager にロードされた*後*であっても、Cisco Unified Presence にロードされる*前*にユーザがユーザ ロケールを設定してしまうと、予定表が正しく動作しないことがあります。問題が報告された場合は、各ユーザに対し、Cisco Unified Communications Manager の [ユーザ オプション（User Options）] ページにサイン インし、ロケールを現在の設定から [英語（English）] に変更してから適切な現在に戻すように指示することを推奨します。BAT ツールを使用してユーザ ロケールを適切な現在に同期させることもできます。
- 変更を有効にするためには、サーバを再起動する必要があります。ロケールのインストール手順がすべて完了したら、クラスタ内の各サーバを再起動してください。クラスタ内のすべてのサーバを再起動するまで、システム内で更新は行われません。サーバの再起動後にサービスが再開されます。
- クラスタ内のすべてのサーバに同じコンポーネントをインストールしてください。

この手順を Cisco Unified Communications Manager で実行する方法については、次の URL にある『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/8_0_1/cucos/iptpch7.html#wp1054072

次の作業

「Cisco Unified Communications Manager へのロケール インストーラのインストール」（P.4-6）

Cisco Unified Presence へのロケール インストーラのインストール

はじめる前に

- Cisco Unified Communications Manager にロケール インストーラをインストールします。英語以外のロケールを使用する場合は、Cisco Unified Communications Manager と Cisco Unified Presence の*両方*に適切な言語インストーラをインストールする必要があります。
- Cisco Unified Presence クラスタに複数のノードがある場合は、クラスタ内のすべてのサーバにロケール インストーラをインストールしてください（パブリッシャ サーバにインストールしてからサブスクライバ サーバにインストールします）。
- 適切なすべてのロケール インストーラが*両方*のシステムにロードされるまで、ユーザ ロケールを*設定しない*でください。ロケール インストーラが Cisco Unified Communications Manager にロードされた*後*であっても、Cisco Unified Presence にロードされる*前*にユーザがユーザ ロケールを設定してしまうと、予定表が正しく動作しないことがあります。問題が報告された場合は、各ユーザに対し、Cisco Unified Communications Manager の [ユーザ オプション（User Options）] ページにサイン インし、ロケールを現在の設定から [英語（English）] に変更してから適切な現在に戻すように指示することを推奨します。BAT ツールを使用してユーザ ロケールを適切な現在に同期させることもできます。
- 変更を有効にするためには、サーバを再起動する必要があります。ロケールのインストール手順がすべて完了したら、クラスタ内の各サーバを再起動してください。クラスタ内のすべてのサーバを再起動するまで、システム内で更新は行われません。サーバの再起動後にサービスが再開されます。

手順

ステップ 1　Cisco Unified Presence ロケール インストーラを入手するには、Cisco.com の次のページにアクセスします。

http://tools.cisco.com/support/downloads/go/ReleaseType.x?optPlat=&isPlatform=Y&mdfid=281820245&sftType=Unified+Presence+Locale+Installer&treeName=Voice+and+Unified+Communications&modelName=Cisco+Unified+Presence+Version+7.0&mdfLevel=Software%20Version/Option&treeMdfId=278875240&modifmdfid=null&imname=&hybrid=Y&imst=N

ステップ 2　作業環境に適した Cisco Unified Presence ロケール インストーラ バージョンを選択します。

ステップ 3　ファイルをダウンロードしたら、ハード ドライブに保存し、ファイルの保存場所をメモします。

ステップ 4　SFTP をサポートするサーバにこのファイルをコピーします。

ステップ 5　管理者のアカウントとパスワードを使用して Cisco Unified OS の管理画面にログインします。

ステップ 6　[ソフトウェア アップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）] を選択します。

ステップ 7　ソフトウェアの入手先として [リモート ファイル システム（Remote File System）] を選択します。

ステップ 8　[ディレクトリ（Directory）] フィールドにファイルの保存場所（/tmp など）を入力します。

ステップ 9　ロケール インストーラ ファイルが保存されているサーバ（ステップ 4 で指定したサーバ）の名前を入力します。これにより、ロケール インストーラ ファイルが Cisco Unified Presence サーバにコピーされ、インストールできるようになります。

ステップ 10　[ユーザ名（User Name）] フィールドと [ユーザ パスワード（User Password）] フィールドに自分のユーザ名とパスワードを入力します。

ステップ 11　[転送プロトコル（Transfer Protocol）] で [SFTP] を選択します。

ステップ 12　[次へ（Next）] を選択します。

ステップ 13　検索結果のリストから Cisco Unified Presence ロケール インストーラを選択します。

ステップ 14　[次へ（Next）] を選択してインストーラ ファイルをロードし、検証します。

ステップ 15　ロケールのインストールが完了したら、クラスタ内の各サーバを再起動します。

ステップ 16　インストールされるロケールのデフォルト設定は、[English United States] です。Cisco Unified Presence の再起動中に、必要に応じて、ダウンロードしたインストーラのロケールに合わせてブラウザの言語を変更してください。

使用するブラウザ	設定手順
Internet Explorer バージョン 6.x	**a.** [ツール（Tools）] > [インターネット オプション（Internet Options）] を選択します。 **b.** [全般（General）] タブを選択します。 **c.** [言語（Languages）] を選択します。 **d.** [上へ（Move Up）] ボタンを使用して、優先する言語をリストの先頭に移動します。 **e.** [OK] を選択します。
Mozilla Firefox バージョン 3.x	**a.** [ツール（Tools）] > [オプション（Options）] を選択します。 **b.** [コンテンツ（Content）] タブを選択します。 **c.** [言語（Languages）] セクションの [言語設定（Choose）] を選択します。 **d.** [上へ（Move Up）] ボタンを使用して、優先する言語をリストの先頭に移動します。 **e.** [OK] を選択します。

ステップ 17　ユーザがサポートされている製品のロケールを選択できることを確認します。

トラブルシューティングのヒント

クラスタ内のすべてのサーバに同じコンポーネントをインストールしてください。

次の作業

「多言語の予定表と統合する場合のユーザ ロケールの設定」（P.4-8）

多言語の予定表と統合する場合のユーザ ロケールの設定

はじめる前に

- 使用可能なすべての言語が含まれている、Cisco Unified Communications Manager および Cisco Unified Presence のロケール インストーラをインストールします。適切なすべてのロケール インストーラが*両方*のシステムにロードされるまで、ユーザ ロケールを*設定しない*でください。
- インストールされるロケールのデフォルト設定は、[English United States] です。Cisco Unified Communications Manager に適切な言語 / ロケールをインストールし、ユーザが最初にサイン インするときに Exchange サーバで適切な言語 / ロケールを選択することを強く推奨します。Cisco Unified Communications Manager に別の言語 / ロケールがインストールされているときにエ

ンド ユーザの Exchange メールボックスにデフォルト言語（英語）を設定した場合、それ以降にそのユーザのロケールを変更することはできません。この問題の詳細については、「WebDAV 経由で予定表との統合を行う場合のローカリゼーションに関する注意事項」（P.6-7）を参照してください。

- ロケール インストーラが Cisco Unified Communications Manager にロードされた*後*であっても、Cisco Unified Presence にロードされる*前*にユーザ ロケールを設定してしまうと、予定表が正しく動作しないことがあります。システムが適切な言語を使用するようにするには、Cisco Unified Communications Manager のユーザ ページにサイン インし、ユーザ ロケールを現在の設定から英語に変更することを推奨します。その後、ロケールを必要な言語に戻します。

手順

ステップ 1　次の表のうち自分のロール（管理者またはユーザ）に対応する手順を実行します。

ロール	設定手順
Administrator	**a.** 管理者のアカウントとパスワードを使用して Cisco Unified Communications Manager の管理画面にログインします。 **b.** [ユーザ管理（User Management）] > [エンド ユーザ（End User）] の順に選択します。 **c.** 検索と一覧表示機能を使用して、必要なユーザを検索します。 **d.** 必要なユーザの [ユーザ ID（User ID）] ハイパーリンクを選択します。 **e.** [ユーザ ロケール（User Locale）] ドロップダウン リストからユーザの適切な言語を選択します。 **f.** [保存（Save）] を選択します。
User	**a.** ユーザのアカウントおよびパスワードを使用して [Cisco Unified Communications Manager のユーザ オプション（Cisco Unified Communications Manager User Options）] にサイン インします。 **b.** [ユーザ オプション（User Options）] > [ユーザ設定（User Settings Configuration）] を選択します。 **c.** [ユーザ ロケール（User Locale）] ドロップダウン リストからユーザの適切な言語を選択します。 **d.** [保存（Save）] を選択します。

関連事項

- 「Cisco Unified Communications Manager へのロケール インストーラのインストール」（P.4-6）
- 「Cisco Unified Presence へのロケール インストーラのインストール」（P.4-7）

[任意] Microsoft Exchange 通知ポートの設定

このトピックは、プレゼンス エンジンにおいて Exchange サーバからの通知をネットワーク設定に固有の別のポートで受信する場合にのみ当てはまります。この手順は、WebDAV と EWS の両方の Exchange 設定を対象とします。

WebDAV 統合では、HTTPU 通知の受信にデフォルトで UDP ポート 50020 が使用されます。EWS 統合では、HTTP 通知の受信にデフォルトで TCP ポートが使用されます。

はじめる前に

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

手順

ステップ 1　[Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [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（Server）] メニューから Cisco Unified Presence Server を選択します。

ステップ 3　[サービス（Service）] メニューから [Cisco UP プレゼンス エンジン（アクティブ）（Cisco UP Presence Engine (Active)）] を選択します。

ステップ 4　[Presence Engine Configuration] セクションの [Microsoft Exchange Notification Port] フィールドのパラメータ値を編集します。WebDAV 設定の場合、このパラメータのデフォルト値は 50020 です。

ステップ 5　[保存（Save）] を選択します。

次の作業

一度にすべてのユーザのパラメータ変更を有効にするために、Cisco UP プレゼンス エンジンを再起動することを推奨します。[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [Tools] > [Service Activation] の順に選択します。

トラブルシューティングのヒント

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

[任意] Microsoft Exchange 予定表通知の接続時間の設定

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

はじめる前に

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

手順

ステップ 1　[Cisco Unified Presence の管理（Cisco Unified Presence Administration）] > [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（Server）] メニューから Cisco Unified Presence Server を選択します。

ステップ 3　[サービス（Service）] メニューから [Cisco UP プレゼンス エンジン（アクティブ）（Cisco UP Presence Engine (Active)）] を選択します。

ステップ 4　[Calendar Spread] フィールドのパラメータ値を編集します。このパラメータのデフォルト値は 50 です。

ステップ 5　[保存（Save）] を選択します。

次の作業

[Calendar Spread] パラメータの変更は、ユーザ単位で予定表の統合が発生するたびに付加的に更新されます。ただし、すべてのユーザについてパラメータの変更を有効にするために、Cisco UP プレゼンス エンジンを再起動することを推奨します。[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [Tools] > [Service Activation] の順に選択します。

トラブルシューティングのヒント

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

CHAPTER 5

Cisco Unified Presence と Microsoft Exchange 間でのセキュアな証明書交換の設定

自己署名証明書およびサードパーティ証明書の交換管理チェックリスト

自己署名証明書およびサードパーティ証明書のセキュアな交換を設定する手順の概要を表 5-1 に示します。

表 5-1　自己署名証明書およびサードパーティ証明書チェックリスト

設定手順		設定方法
ステップ 1	証明書 CA サービスをインストールする。	**自己署名証明書** 「認証局（CA）サービスのインストール方法」（P.5-2）
ステップ 2	Exchange サーバの IIS で CSR を作成する。	**自己署名証明書** 「Exchange Server の IIS 上での CSR の作成方法」（P.5-5） **サードパーティ証明書** 「Exchange Server の IIS 上での CSR の作成方法」（P.5-5）

表 5-1　自己署名証明書およびサードパーティ証明書チェックリスト（続き）

設定手順		設定方法
ステップ 3	CA サーバ/認証局に CSR を提出する。	**自己署名証明書** 「CA サーバ/認証局への CSR の提出」（P.5-9） **サードパーティ証明書** 認証局に CSR を要求します。
ステップ 4	署名付き証明書をダウンロードする。	**自己署名証明書** 「署名付き証明書のダウンロード」（P.5-10） **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。
ステップ 5	署名付き証明書を Exchange IIS にアップロードする。	**自己署名証明書** 「署名付き証明書の Exchange IIS へのアップロード方法」（P.5-11） **サードパーティ証明書** 「署名付き証明書の Exchange IIS へのアップロード方法」（P.5-11）
ステップ 6	ルート証明書をダウンロードする。	**自己署名証明書** 「ルート証明書のダウンロード」（P.5-13） **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。
ステップ 7	ルート証明書を Cisco Unified Presence サーバにアップロードします。	**自己署名証明書** 「Cisco Unified Presence サーバへのルート証明書のアップロード」（P.5-13） **サードパーティ証明書** CA 署名付きのサードパーティ Exchange サーバ証明書がある場合は、証明書チェーン内のすべての CA 証明書を Cisco Unified Presence 信頼証明書（cup-trust）として Cisco Unified Presence にアップロードする必要があります。

認証局（CA）サービスのインストール方法

CA は Exchange サーバ上で動作しますが、サードパーティ証明書の交換におけるセキュリティを高めるために、別の Windows サーバを Certificate Authority（CA; 認証局）として使用することを推奨します。

- 「Windows Server 2003 への CA のインストール」（P.5-3）
- 「Windows Server 2008 への CA のインストール」（P.5-4）

Windows Server 2003 への CA のインストール

はじめる前に

- CA をインストールするためには、まず Windows Server 2003 コンピュータに Internet Information Services（IIS; インターネット インフォメーション サービス）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 ディスクを用意してください。

手順

ステップ 1　[Start] > [Control Panel] > [Add/Remove Programs] の順に選択します。

ステップ 2　[Add/Remove Programs] ウィンドウの [Add/Remove Windows Components] を選択します。

ステップ 3　[Windows Components Wizard] が表示されます。

ウィンドウ	設定手順
[Windows Components] ウィンドウ ページ 1	**a.** [Components] のリストで [Certificate Services] をオンにします。 **b.** ドメイン メンバーシップとコンピュータ名の変更の制約に関する警告が表示されたら、[Yes] を選択します。
[CA Type] ウィンドウ ページ 2	**a.** [Stand-alone Root CA] を選択します。 **b.** [Next] を選択します。
[CA Identifying Information] ウィンドウ ページ 3	**a.** CA サーバの [Common Name] フィールドにサーバ名を入力します。DNS がない場合は、IP アドレスを入力してください。 **b.** [Next] を選択します。
[Certificate Database Settings] ウィンドウ ページ 4	**a.** デフォルト設定をそのまま使用します。 **b.** [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かどうかを確認するメッセージが表示されたら、[Yes] を選択します。

ステップ 5　Active Server Pages（ASP）を有効にするかどうかを確認するメッセージが表示されたら、[Yes] を選択します。

ステップ 6　インストール プロセスが完了したら、[Finish] を選択します。

トラブルシューティングのヒント

CA はサードパーティの認証局であることに注意してください。CA の共通名は、CSR の作成に使用される共通名と*同じであってはなりません*。

次の作業

「CA サーバ/認証局への CSR の提出」（P.5-9）

Windows Server 2008 への CA のインストール

手順

ステップ 1　[Start] > [Administrative Tools] > [Server Manager] の順に選択します。

ステップ 2　コンソール ツリーで [Roles] を選択します。

ステップ 3　[Action] > [Add Roles] の順に選択します。

ステップ 4　[Add Roles] ウィザードを完了します。

ウィンドウ	設定手順
[Before You Begin] ウィンドウ 1/13 ページ	**a.** ウィンドウに表示されている前提条件をすべて満たしていることを確認します。 **b.** [Next] を選択します。
[Select Server Roles] ウィンドウ 2/13 ページ	**a.** [Active Directory Certificate Services] をオンにします。 **b.** [Next] を選択します。
[Introduction] ウィンドウ 3/13 ページ	[Next] を選択します。
[Select Role Services] ウィンドウ 4/13 ページ	**a.** 次のチェックボックスをオンにします。 – [Certificate Authority] – [Certificate Authority Web Enrollment] – [Online Responder] **b.** [Next] を選択します。
[Specify Setup Type] ウィンドウ 5/13 ページ	[Standalone] を選択します。
[Specify CA Type] ウィンドウ 6/13 ページ	[Root CA] を選択します。
[Set Up Private Key] ウィンドウ 7/13 ページ	[Create a new private key] を選択します。
[Configure Cryptography for CA] ウィンドウ 8/13 ページ	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。
[Configure CA Name] ウィンドウ 9/13 ページ	CA を識別する共通名を入力します。
[Set Validity Period] ウィンドウ 10/13 ページ	この CA で作成される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です。

ウィンドウ	設定手順
[Configure Certificate Database] ウィンドウ 11/13 ページ	証明書データベースの場所をデフォルトのままにします。
[Confirm Installation Selections] ウィンドウ 12/13 ページ	[Install] を選択します。
[Installation Results] ウィンドウ 13/13 ページ	**a.** すべてのコンポーネントについて、[Installation Succeeded] というメッセージが表示されていることを確認します。 **b.** [Close] を選択します。 **（注）** サーバー マネージャに役割の 1 つとして [Active Directory Certificate Services] が表示されます。

次の作業

「Exchange Server の IIS 上での CSR の作成方法」（P.5-5）

Exchange Server の IIS 上での CSR の作成方法

CSR の作成：Windows Server 2003 の実行

Exchange の IIS で Certificate Signing Request（CSR; 証明書の署名要求）を作成する必要があります。作成した CSR は CA サーバによって署名されます。

はじめる前に

自己署名証明書：必要に応じて証明書 CA サービスをインストールします。

手順

ステップ 1　[Administrative Tools] から [Internet Information Services] を開きます。

ステップ 2　Internet Information Services（IIS; インターネット インフォメーション サービス）マネージャで次の操作を実行します。

a. [Default Web Site] を右クリックします。

b. [Properties] を選択します。

ステップ 3　[Directory Security] タブを選択します。

ステップ 4　[Server Certificate] を選択します。

ステップ 5　[Web Server Certificate Wizard] ウィンドウが表示されたら、[Next] を選択します。

ステップ 6　Web Server Certificate Wizard を完了します。

（注） 証明書の [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 Common Name（CN; 共通名）と一致している必要があります。

ウィンドウ	設定手順
[Server Certificate] ウィンドウ 1/9 ページ	**a.** [Create a New Certificate] を選択します。 **b.** [Next] を選択します。
[Delayed or Immediate Request] ウィンドウ 2/9 ページ	**a.** [Prepare the Request Now, But Send It Later] を選択します。 **b.** [Next] を選択します。
[Name and Security Settings] ウィンドウ 3/9 ページ	**a.** Web サイトの証明書のデフォルト名をそのまま使用します。 **b.** ビット長として [1024] を選択します。 **c.** [Next] を選択します。
[Organization Information] ウィンドウ 4/9 ページ	**a.** [Organization] フィールドに会社名を入力します。 **b.** [Organization Unit] フィールドに部署名を入力します。 **c.** [Next] を選択します。
[Your Site's Common Name] ウィンドウ 5/9 ページ	**a.** [Common Name] フィールドには、Exchange サーバのホスト名または IP アドレスを入力します。 **（注）** ここで入力する IIS 証明書の一般名は、Cisco Unified Presence 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。 **b.** [Next] を選択します。
[Geographical Information] ウィンドウ 6/9 ページ	**a.** 次の地理情報を入力します。 – [Country/Region]（国 / 地域） – [State/province]（都道府県） – [City/locality]（市区町村） **b.** [Next] を選択します。
[Certificate Request File Name] ウィンドウ 7/9 ページ	**a.** 証明書要求のファイル名を入力し、CSR の保存先のパスとファイル名を指定します。 **b.** [Next] を選択します。 **（注）** CSR は拡張子（.txt）なしで保存してください。この CSR ファイルを後で探す必要があるため、保存場所を覚えておいてください。このファイルを開くには、必ずメモ帳を使用します。

ウィンドウ	設定手順
[Request File Summary] ウィンドウ 8/9 ページ	**a.** [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ます。 **b.** [Next] を選択します。
[Server Certificate Completion] ウィンドウ 9/9 ページ	[Finish] を選択します。

次の作業

「CA サーバ/認証局への CSR の提出」（P.5-9）

CSR の作成：Windows Server 2008 の実行

Exchange の IIS で Certificate Signing Request（CSR; 証明書の署名要求）を作成する必要があります。作成した CSR は CA サーバによって署名されます。

はじめる前に

手順

ステップ 1　[Administrative Tools] から [Internet Information Services (IIS) Manager] を開きます。

ステップ 2　IIS マネージャの左側のフレームにある [Connections] ウィンドウで [Exchange Server] を選択します。

ステップ 3　[Server Certificates] をダブルクリックします。

ステップ 4　IIS マネージャの右側のフレームにある [Actions] ウィンドウで [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。

ウィンドウ	設定手順
[Distinguished Name Properties] ウィンドウ 1/5 ページ	**a.** [Common Name] フィールドには、Exchange サーバのホスト名または IP アドレスを入力します。 **（注）** ここで入力する IIS 証明書の一般名は、Cisco Unified Presence 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。 **b.** [Organization] フィールドに会社名を入力します。 **c.** [Organization Unit] フィールドに部署名を入力します。 **d.** 次の地理情報を入力します。 – [City/locality]（市区町村） – [State/province]（都道府県） – [Country/Region]（国 / 地域） **e.** [Next] を選択します。
[Cryptographic Service Provider Properties] ウィンドウ 2/5 ページ	**a.** デフォルトの暗号化サービス プロバイダーをそのまま使用します。 **b.** ビット長として [1024] を選択します。 **c.** [Next] を選択します。
[Certificate Request File Name] ウィンドウ 3/5 ページ	**a.** 証明書要求のファイル名を入力します。 **b.** [Next] を選択します。 **（注）** CSR は拡張子（.txt）なしで保存してください。この CSR ファイルを後で探す必要があるため、保存場所を覚えておいてください。このファイルを開くには、必ずメモ帳を使用します。
[Request File Summary] ウィンドウ 4/5 ページ	**a.** [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ます。 **b.** [Next] を選択します。
[Request Certificate Completion] ウィンドウ 5/5 ページ	[Finish] を選択します。

次の作業

「CA サーバ / 認証局への CSR の提出」（P.5-9）

CA サーバ/認証局への CSR の提出

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

- Exchange 証明書
- Cisco Unified Presence の管理画面にある、Exchange プレゼンス ゲートウェイの [プレゼンス ゲートウェイ（Presence Gateway）] フィールド

はじめる前に

Exchange サーバの IIS で CSR を作成します。

手順

ステップ 1　証明書要求ファイルを CA サーバにコピーします。

ステップ 2　次の URL を開きます。

http://*local-server*/certserv

または、

http://127.0.0.1/certsrv

ステップ 3　[Request a certificate] を選択します。

ステップ 4　[advanced certificate request] を選択します。

ステップ 5　[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] を選択します。

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

ステップ 7　次の行から、

-----BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST-----

ステップ 8　CSR の内容を [Certificate Request] テキストボックスに貼り付けます。

ステップ 9　（任意）[Certificate Template] ドロップダウン リストのデフォルト値は [Administrator] テンプレートです。このテンプレートでは、サーバの認証に適した有効な署名付き証明書が作成されることもあれば、作成されないこともあります。エンタープライズのルート CA がある場合は、[Certificate Template] ドロップダウン リストから [Web Server] 証明書テンプレートを選択してください。[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 設定を既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　[Submit] を選択します。

ステップ 11　[Start] > [Administrative Tools] > [Certification] > [Authority] > [CA name] > [Pending request] の順に選択します。[Certificate Authority] ウィンドウの [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。

- [All Tasks] を選択します。
- [Issue] を選択します。

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

次の作業

「署名付き証明書のダウンロード」（P.5-10）

署名付き証明書のダウンロード

はじめる前に

自己署名証明書：CA サーバに CSR を提出します。

サードパーティ証明書：認証局に CSR を要求します。

手順

ステップ 1　[Administrative Tools] から [Certification Authority] を開きます。先ほど発行した証明書の要求が [Issued Requests] に表示されます。

ステップ 2　その要求を右クリックし、[Open] を選択します。

ステップ 3　[Details] タブを選択します。

ステップ 4　[Copy to File] を選択します。

ステップ 5　[Certificate Export Wizard] が表示されたら、[Next] を選択します。

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。

ウィンドウ	設定手順
[Export File Format] ウィンドウ 1/3 ページ	**a.** [Base-64 encoded X.509] を選択します。 **b.** [Next] を選択します。
[File to Export] ウィンドウ 2/3 ページ	**a.** 証明書の保存場所を入力します。証明書の名前には **cert.cer** を使用します（*c:¥cert.cer* など）。 **b.** [Next] を選択します。
[Certificate Export Wizard Completion] ウィンドウ 3/3 ページ	**a.** 表示されている概要情報に目を通し、エクスポートが成功したことを確認します。 **b.** [Finish] を選択します。

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

次の作業

「署名付き証明書の Exchange IIS へのアップロード方法」（P.5-11）

署名付き証明書の Exchange IIS へのアップロード方法

署名付き証明書のアップロード：Windows 2003 の実行

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

はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

ステップ 1　[Administrative Tools] から [Internet Information Services] を開きます。

ステップ 2　[Internet Information Services] ウィンドウで次の手順を実行します。

a. [Default Web Site] を右クリックします。

b. [Properties] を選択します。

ステップ 3　[Default Web Site] ウィンドウで次の手順を実行します。

a. [Directory Security] タブを選択します。

b. [Server Certificate] を選択します。

ステップ 4　[Web Server Certificate Wizard] ウィンドウが表示されたら、[Next] を選択します。

ステップ 5　Web Server Certificate Wizard を完了します。

ウィンドウ	設定手順
[Pending Certificate Request] ウィンドウ 1/4 ページ	**a.** [Process the pending request and install the certificate] を選択します。 **b.** [Next] を選択します。
[Process a Pending Request] ウィンドウ 2/4 ページ	**a.** [Browse] を選択して証明書を指定します。 **b.** 正しいパスおよびファイル名に移動します。 **c.** [Next] を選択します。
[SSL Port] ウィンドウ 3/4 ページ	**a.** SSL ポートを「443」と入力します。 **b.** [Next] を選択します。
[Server Certificate Completion] ウィンドウ 4/4 ページ	[Finish] を選択します。

トラブルシューティングのヒント

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

- [Directory Security] タブで [View Certificate] を選択します。
- [Details] > [Highlight root certificate] の順に選択し、[View] を選択します。
- ルート証明書の [Details] タブを選択し、証明書をインストールします。

次の作業

「ルート証明書のダウンロード」（P.5-13）

署名付き証明書のアップロード：Windows 2008 の実行

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

はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

ステップ 1　[Administrative Tools] から [Internet Information Services (IIS) Manager] を開きます。

ステップ 2　IIS マネージャの左側のフレームにある [Connections] ウィンドウで [Exchange Server] を選択します。

ステップ 3　[Server Certificates] をダブルクリックします。

ステップ 4　IIS マネージャの右側のフレームにある [Actions] ウィンドウで [Complete Certificate Request] を選択します。

ステップ 5　[Specify Certificate Authority Response] ウィンドウで次の操作を実行します。

a. 省略記号 [...] を選択して証明書を指定します。

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] を選択します。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　[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. [Default Web Site] を選択します。

b. IIS マネージャの右側のフレームにある [Actions] ウィンドウで [Bindings] を選択します。

ステップ 7　[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. [Edit] をクリックします。

ステップ 8　[Edit Site Binding] ウィンドウで次の手順を実行します。

a. SSL 証明書のリスト ボックスから、作成した証明書を選択します。証明書に付けた「わかりやすい名前」が表示されます。

b. [OK] を選択します。

次の作業

「ルート証明書のダウンロード」（P.5-13）

ルート証明書のダウンロード

はじめる前に

署名付き証明書を Exchange IIS にアップロードします。

手順

ステップ 1　CA サーバにサイン 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。

- Windows server 2003：http://127.0.0.1/certsrv
- Windows server 2008：https://127.0.0.1/certsrv

ステップ 3　[Download a CA certificate, certificate chain, or CRL] を選択します。

ステップ 4　[Encoding Method] で、[Base 64] を選択します。

ステップ 5　[Download CA Certificate] を選択します。

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。

トラブルシューティングのヒント

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

次の作業

「Cisco Unified Presence サーバへのルート証明書のアップロード」（P.5-13）

Cisco Unified Presence サーバへのルート証明書のアップロード

はじめる前に

- 自己署名証明書：ルート証明書をダウンロードします。
- サードパーティ証明書：認証局にルート証明書を要求します。CA 署名付きのサードパーティ Exchange サーバ証明書がある場合は、証明書チェーン内のすべての CA 証明書を Cisco Unified Presence の信頼証明書（cup-trust）として Cisco Unified Presence 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 Presence の管理画面にある証明書インポート ツールを使用して、証明書をアップロードします。

証明書のアップロード方法	動作
Cisco Unified Presence の管理画面にある証明書インポート ツール 証明書インポート ツールは、信頼証明書を Cisco Unified Presence にインストールするプロセスを簡略化するもので、証明書交換の主要な方法です。このツールでは、Exchange サーバのホストとポートを指定すると、サーバから証明書チェーンがダウンロードされます。承認すると、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 Presence の管理画面の証明書インポート ツールにアクセスし、インストールする方法を説明します。いずれかの形式で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した場合（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] の順に選択）、カスタマイズされた証明書インポート ツールを表示することもできます。	**a.** Cisco Unified Presence の管理画面で、[システム（System）] > [セキュリティ（Security）] > [証明書インポート ツール（Certificate Import Tool）] の順に選択します。 **b.** 証明書をインストールする証明書信頼ストアとして [CUP の信頼性（CUP Trust）] を選択します。この証明書信頼ストアには、Exchange の統合に必要なプレゼンス エンジン信頼証明書が保存されます。 **c.** Exchange サーバに接続するために、次のいずれかの値を入力します。 – IP アドレス – ホスト名 – FQDN この [ピア サーバ（Peer Server）] フィールドに入力する値は、Exchange サーバの IP アドレス、ホスト名、または FQDN と完全に一致している必要があります。 **d.** Exchange サーバとの通信に使用するポートを入力します。この値は、Exchange サーバの使用可能なポートと一致している必要があります。 **e.** [送信（Submit）] を選択します。ツールが完了すると、テストごとに次の状態が報告されます。 – ピア サーバの到達可能性ステータス : Cisco Unified Presence が Exchange サーバに到達（ping）できるかどうかを示します。「Exchange サーバ接続ステータスのトラブルシューティング」（P.6-1）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 サーバから証明書をダウンロードすることに成功したかどうかと、Cisco Unified Presence とリモート サーバの間にセキュアな接続が確立されたかどうかを示します。「SSL 接続 / 証明書ステータスのトラブルシューティング」（P.6-2）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	動作
Cisco Unified オペレーティング システムの管理画面 Exchange サーバが SSL/TLS ハンドシェイク中に証明書を送信しない場合、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。その場合は、Cisco Unified オペレーティング システムの管理画面にある証明書の管理ツール（[セキュリティ（Security）] > [証明書の管理（Certificate Management）] の順に選択）を使用して、欠落している証明書を手動でインポートする必要があります。	**a.** Cisco Unified Presence サーバ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。 **b.** Cisco Unified Presence の管理画面のログイン ウィンドウで、[ナビゲーション（Navigation）] メニューから [Cisco Unified OS の管理（Cisco Unified OS Administration）] を選択し、[移動（Go）] を選択します。 **c.** Cisco Unified オペレーティング システムの管理画面用のユーザ名とパスワードを入力して、[ログイン（Login）] を選択します。 **d.** [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。 **e.** [証明書の一覧（Certificate List）] ウィンドウで [証明書のアップロード（Upload Certificate）] を選択します。 **f.** [証明書のアップロード（Upload Certificate）] ポップアップ ウィンドウが表示されたら、次の操作を実行します。 – [証明書の名前（Certificate Name）] リスト ボックスから [cup-trust] を選択します。 – 拡張子を付けずにルート証明書の名前を入力します。 **g.** [参照（Browse）] を選択し、[certnew.cer] を選択します。 **h.** [ファイルのアップロード（Upload File）] を選択します。

ステップ 3　証明書のインポート ツール（ステップ 1）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 UP プレゼンス エンジンと SIP プロキシ サービスを再起動します。[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [Tools] > [Service Activation] の順に選択します。

トラブルシューティングのヒント

- Cisco Unified Presence では、Exchange サーバの信頼証明書を件名 Common Name（CN; 共通名）あり / なしのどちらでもアップロードできます。
- 会議通知機能および Cisco IP Phone Messenger 機能は、ネットワークを WebDAV 経由で統合した場合にのみ有効です。これらの機能は EWS 統合ではサポートされません。
- 会議通知機能を使用する場合は、すべての種類の証明書についてプレゼンス エンジンと SIP プロキシを再起動する必要があります。証明書をアップロードしたら、[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] へ移動し、まずプレゼンス エンジン、次に SIP プロキシを再起動します。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。

CHAPTER 6

Exchange 予定表統合のトラブルシューティング

Exchange サーバ接続ステータスのトラブルシューティング

Exchange サーバの接続ステータスは、WebDAV または EWS 経由で予定表を統合するために Exchange プレゼンス ゲートウェイを設定した場合（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] の順に選択）、Cisco Unified Presence の管理画面に表示されます。[プレゼンス ゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [トラブルシュータ（Troubleshooter）] には、Cisco Unified Presence と Exchange サーバとの接続のステータスが表示されます。

（注） *1 つまたは複数の* EWS サーバを追加、更新、削除でき、サーバ数に上限はありません。ただし、[プレゼンス ゲートウェイ（Presence Gateway）] ウィンドウの [トラブルシュータ（Troubleshooter）] では、設定された EWS サーバのうち最初の 10 台についてのみステータスを確認および報告できます。

テスト	ステータスの説明と推奨される対処法
Exchange の到達可能性（ping 可能）	Cisco Unified Presence が Exhange サーバへの到達（ping）に成功しました。
Exchange の到達可能性（到達不可能）	Cisco Unified Presence が Exhange サーバの ping に失敗しました。フィールド値が誤っているか、またはお客様のネットワークに何らかの問題（ケーブリングなど）があるため、サーバが到達不可になっていると考えられます。 この問題を解決するには、ネットワークを介して Exchange サーバに到達できるように [Exchange Server] 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）] フィールドの値が件名 CN 値である必要がないことに注意してください。IP アドレスまたは解決可能なホスト名を入力できます。ただし、後の設定プロセスで、この値によって件名 CN 値が解決されます。 Exchange サーバとの接続に問題がある場合は、Cisco Unified Presence の管理画面の [システム トラブルシュータ（System Troubleshooter）] も参照し、推奨される解決策を実行してください。[診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）] の順に選択します。

SSL 接続 / 証明書ステータスのトラブルシューティング

[SSL 接続 / 証明書の確認（SSL Connection/Certificate Verification）] のステータスは、WebDAV または EWS 経由で予定表を統合するために Exchange プレゼンス ゲートウェイを設定した場合（[プレゼンス（Presence）] > [ゲートウェイ（Gateways）] の順に選択）、Cisco Unified Presence の管理画面に表示されます。[プレゼンス ゲートウェイの設定（Presence Gateway Configuration）] ウィンドウの [トラブルシュータ（Troubleshooter）] に証明書件名 CN の不一致があるかどうかが示されます。

（注）　*1 つまたは複数の* EWS サーバを追加、更新、削除でき、サーバ数に上限はありません。ただし、[プレゼンス ゲートウェイ（Presence Gateway）] ウィンドウの [トラブルシュータ（Troubleshooter）] では、設定された EWS サーバのうち最初の 10 台についてのみステータスを確認および報告できます。

テスト	ステータスの説明と推奨される対処法
SSL 接続/証明書の確認：確認に成功	Cisco Unified Presence が Exchange サーバとの SSL 接続を確認しました。証明書の詳細を表示するには、[表示（View）] をクリックします。
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）** 対処法の手順では、証明書のインポート ツールのカスタマイズ バージョンを使用しています。接続のステータスを確認するだけである場合は、確認されたステータスが示され、[保存（Save）] は選択できません。	Exchange へのセキュアな接続を確立するために Cisco Unified Presence が必要とする 1 つまたは複数の証明書が欠落しています。証明書ビューアを使用すると、欠落している証明書の詳細を表示できます。 欠落している証明書を表示するには、証明書ビューアを使用して次の手順を実行します。 **1.** [設定（Configure）] を選択して証明書ビューアを開きます。 **2.** [証明書チェーンをそのまま使用（Accept Certificate Chain）] をオンにします。 **3.** [保存（Save）] を選択します。 **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。 **6.** 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。 　**a.** 欠落している証明書ファイルを Exchange サーバからダウンロードします。 　**b.** Cisco Unified Presence 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。 　**c.** Cisco Unified OS の管理画面を使用して、欠落している必要な証明書をアップロードします。 トラブルシューティングのヒント • 証明書ビューアに証明書が表示されない場合は、欠落している証明書を Exchange サーバから手動でダウンロードしてインストールし、Cisco Unified OS の管理画面で次のようにアップロードする必要があります。 　– 必要に応じ、Cisco Unified OS の管理画面を開き、証明書をアップロードして証明書チェーンを完成させてください。 　– Cisco Unified Presence の管理画面の [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、再び証明書ビューアを開いて、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 信頼証明書をアップロードした後で、Cisco UP プレゼンス エンジンを再起動する必要があります。[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [Tools] > [Service Activation] の順に選択します。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 ビューアを開き、証明書チェーンの詳細を確認してください。Cisco Unified Presence が Exchange サーバからダウンロードした証明書チェーンに問題（前述したように証明書が欠落しているなど）がある場合は、[設定（Configure）] ボタンが表示されます。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対処法
SSL 接続/証明書の確認に失敗：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。この問題を解決するには、証明書ビューアを使用して手動で対処するか、または [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します。 [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。Cisco Unified Presence 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の ping を行います。入力したホスト（FQDN または IP アドレス）は、IIS 証明書の件名 CN と完全に一致している必要があります。 **2.** [保存（Save）] を選択します。 証明書ビューアを使用して件名 CN の不一致を解決する場合は、次の手順を実行します。 **1.** [設定（Configure）] を選択して証明書ビューアを開きます。 **2.** [証明書チェーンをそのまま使用（Accept Certificate Chain）] をオンにします。 **3.** [保存（Save）] を選択します。 **4.** [閉じる（Close）] を選択して証明書ビューアを閉じます。証明書ビューアを閉じると、[プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値が変更されることを知らせるメッセージが表示され（値を更新した場合）、[プレゼンス ゲートウェイ（Presence Gateway）] ページが更新されます。 **5.** [プレゼンス ゲートウェイ（Presence Gateway）] フィールドの値が更新されたことを確認します。 **6.** [SSL 接続/証明書の確認（SSL Connection/Certificate Verification）] の値が [確認が成功しました（Verified）] であることを確認します。 **トラブルシューティングのヒント** [設定（Configure）] または [表示（View）] を選択して証明書チェーン ビューアを開き、証明書チェーンの詳細を確認してください。Exchange サーバからダウンロードされた証明書チェーンに問題（前述したように証明書が欠落しているなど）がある場合は、[設定（Configure）] ボタンが表示されます。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対処法
SSL 接続/証明書の確認に失敗：証明書が不正	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。考えられる原因として、Exchange サーバが証明書を再作成した後も Cisco Unified Presence サーバに以前の証明書が残っていることがあります。 この問題を解決するには、次の手順を実行します。 • ログを選択して、このエラーの原因を特定します。 • このエラーの原因が不正な署名である場合は、Cisco Unified OS の管理画面を使用して、古い証明書を Cisco Unified Presence から削除し、新しい証明書をアップロードする必要があります。 • 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である場合は、Cisco Unified OS の管理画面を使用して、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、Cisco Unified Presence が SSL 接続を確認できません。 Exchange サーバへのネットワーク接続を検証し、Exchange サーバが正しい IP アドレスとポート番号を使用してに接続を受け入れることを確認するよう推奨します。
SSL 接続/証明書の確認に失敗	不明確な原因または Cisco Unified Presence 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 のバージョン（2003、2007、2010）に共通または特有の既知の問題について説明します。

- 「予定表統合のスケールの制限」（P.6-6）
- 「ユーザが Exchange サーバ間で移動すると、予定表ステータスが更新されない」（P.6-6）
- 「LDAP ユーザの削除が Cisco Unified Presence に反映されるまでに最低 24 時間かかる」（P.6-6）
- 「WebDAV 経由で予定表との統合を行う場合のローカリゼーションに関する注意事項」（P.6-7）
- 「Exchange サーバの URL に「Calendar」の訳語が含まれている必要がある」（P.6-7）
- 「Cisco IP Phone Messenger 対応の電話機のプレゼンス ゲートウェイ設定の確認」（P.6-8）
- 「Microsoft HotFix KB841561 の適用」（P.6-8）
- 「Exchange 2007 から「HTTP 503 サービス利用不可（HTTP 503 Service Unavailable）」エラーが返され、予定表の統合が失敗する」（P.6-9）
- 「会議通知および Cisco IP Phone Messenger のサポート」（P.6-11）

予定表統合のスケールの制限

Cisco Unified Presence と Exchange の予定表の統合は、予定表プレゼンスを購読するユーザの最大 X% と予定表の同時移行（会議への同時出席または同時退席など）を行うユーザの最大 Y% について検証されています。Cisco Unified Presence Release 8.5 の場合、X および Y の値は次のとおりです。

- X = 50
- Y = 30

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

問題

Exchange を統合した環境で、Exchange 管理者がユーザをある Exchange サーバから別の Exchange サーバへ移動すると、そのユーザについては予定表ステータスの変更が更新されません。

原因

この問題は、ユーザを別のサーバへ移動したことを Exchange サーバが通知しないために発生します。

ソリューション

Cisco Unified Presence 管理者またはユーザは、Exchange 管理者がユーザをある Exchange サーバから別の Exchange サーバへ移動した*後*で、そのユーザの予定表統合をいったん無効にし、再び有効にする必要があります。

LDAP ユーザの削除が Cisco Unified Presence に反映されるまでに最低 24 時間かかる

問題

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

Cisco Unified Presence 上の Cisco UP Sync Agent は、ユーザが削除されるまでユーザ ステータスの変更を同期しません。それまでの間、そのユーザは Cisco Unified Communications Manager に存在し、すべての Cisco Unified Presence 機能（Exchange 予定表の購読を含む）がそのユーザに対して 24 時間にわたり有効なままとなります。このような遅延が生じるのは、そのユーザが LDAP から削除される*前に*クライアント アプリケーション（Cisco Unified Personal Communicator）にサイン インしたユーザが自動的にサイン アウトされないことを意味します。そのユーザの以前の予定表ステータス（応対可能、取り込み中）は、ユーザがクライアントからサイン アウトするまで Cisco Unified Presence に残存します。

原因

この問題は、Cisco Unified Communications Manager を設定し、LDAP 認証を使用している場合に発生します。LDAP からユーザを削除した場合、そのユーザの予定表の購読は、最低 24 時間 Cisco Unified Presence 上に存続し、更新されます。

ソリューション

LDAP からユーザを削除する場合、Cisco Unified Presence が Exchange 予定表の購読をただちに停止し、削除されたユーザをクライアント アプリケーションからサイン アウトするように、そのユーザのライセンスを手動で削除できます。そうしない場合、24 時間の遅延が発生する可能性があることに注意してください。

WebDAV 経由で予定表との統合を行う場合のローカリゼーションに関する注意事項

問題

Cisco Unified Communications Manager に別の言語/ロケールがインストールされている場合に、ユーザの Exchange メールボックスの言語をデフォルト（英語）のままにすると、予定表が英語のデフォルト名となり、そのユーザの言語/ロケールは変更できません。予定表の購読について 404 エラーが返されます。

原因

この問題は、WebDAV 経由のローカライズされた Exchange 2003/2007 統合でのみ発生します。この問題は EWS 統合には影響しません。

ソリューション

- この問題の発生を防ぐには、Exchange の設定時に言語を正しく設定することを推奨します。Cisco Unified Communications Manager に適切な言語/ロケールをインストールし、ユーザが最初にサイン インするときに Exchange サーバで適切な言語/ロケールを選択します。
- ユーザの Exchange メールボックスの言語を英語に設定し、Cisco Unified Communications Manager に別の言語/ロケールがインストールされている場合は、そのユーザについて Cisco Unified Communications Manager の言語/ロケールを英語に戻す必要があります。この設定の手順については、「多言語の予定表と統合する場合のユーザ ロケールの設定」（P.4-8）を参照してください。

Exchange サーバの URL に「Calendar」の訳語が含まれている必要がある

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

手順

ステップ 1　Cisco Unified Presence と Exchange サーバに同じ言語ロケールをインストール（ロケール インストーラをロード）します。Cisco Unified Presence にロケールをインストールする方法の詳細については、「[任意] 予定表を統合する場合の多言語サポートの設定方法」（P.4-5）を参照してください。

ステップ 2　Cisco Unified Presence サーバを再起動し、Cisco Unified Presence の管理画面にログインします。

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

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。

Cisco IP Phone Messenger 対応の電話機のプレゼンス ゲートウェイ設定の確認

Receive-As アカウント クレデンシャルと証明書の交換が正しく設定されている場合、Cisco IP Phone Messenger 対応の電話機にはユーザのスケジュールされた会議が表示されます。Outlook プレゼンス ゲートウェイが正しく設定されていることを確認するには、適切に設定された電話機で次の手順を実行します。

手順

ステップ 1　[サービス（Services）] を選択します。

ステップ 2　[PhoneMessenger] を押します。

ステップ 3　IP Phone Messenger サービスにサイン インします。

ステップ 4　[1 今日の会議（1 Today's meetings）] を選択します。

ステップ 5　ユーザの当日の会議が表示されることを確認します。

Microsoft HotFix KB841561 の適用

この問題は Microsoft Exchange 2003 でのみ発生します。Exchange 2003 サーバで問題が発生し、「500 内部サーバー エラー（500 Internal Server Error）」が表示された場合は、Microsoft HotFix KB841561 を適用してください。

手順

ステップ 1　Windows Server 2003 および Microsoft Exchange 2003 の SP2 をアンインストールします。

ステップ 2　Windows Server 2003 および Exchange 2003 の SP1 をインストールします。

ステップ 3　KB841561 を http://www.microsoft.com/downloads/details.aspx?familyid=050be883-11fc-4045-b988-c737e79c65d0&displaylang=en からダウンロードしてインストールします。

ステップ 4　Windows Server 2003 および Microsoft Exchange 2003 の SP2 をインストールします。

Exchange 2007 から「HTTP 503 サービス利用不可（HTTP 503 Service Unavailable）」エラーが返され、予定表の統合が失敗する

この問題は Microsoft Exchange 2007 でのみ発生します。

問題

Exchange 2007 以降においては、Outlook Web アクセスの URL が **/exchange** から **/owa** に変更されています。これは、OWA が Exchange 2007 メールボックス サーバ上のメールボックスにアクセスするときに使用する仮想ディレクトリです。ところが、WebDAV 経由での Exchange 2007 との統合では以前の URL が使用されているため、Cisco Unified Presence は SUSCRIBE 要求を常に **/exchange** 仮想ディレクトリに送信します。Exchange Server 2007（SP1）でのテストでは、http://<server>/exchange を http://<server>/owa にリダイレクトすると、Exchange 2007 のインターネット インフォメーション サービス（IIS; Internet Information Services）マネージャ コンソールにエラー（HTTP 503 サービス利用不可（HTTP 503 Service Unavailable））が表示されることが確認されています。

原因

この問題は、Exchange 2007 SP1 を使用していて、Exchange 仮想ディレクトリのターゲット アドレスを Web メール用のデフォルト OWA ディレクトリにリダイレクトした場合に発生します。

ソリューション

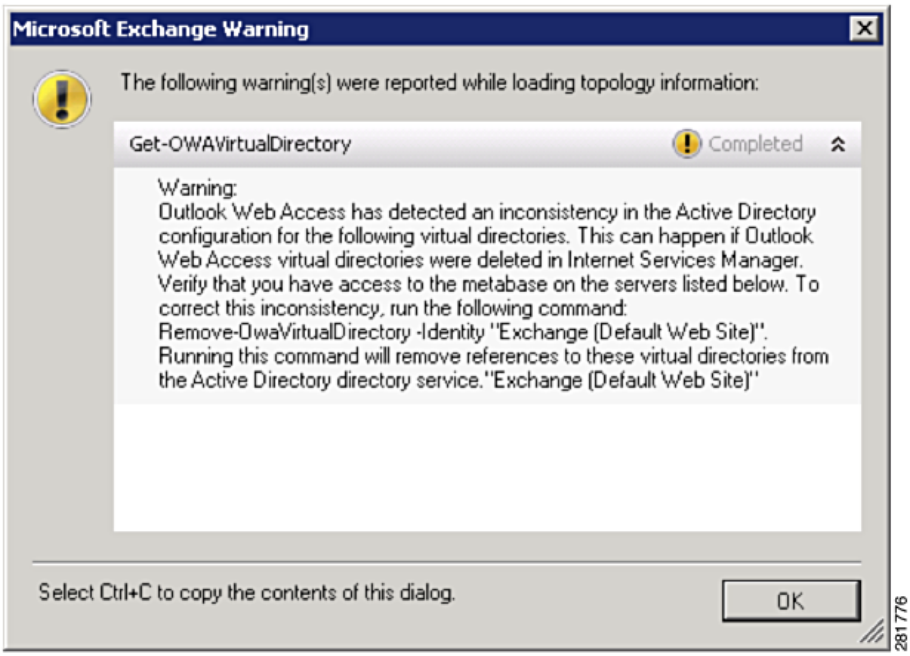
「503 サービス利用不可（503 Service Unavailable）」エラー メッセージが表示された場合は、次の手順を実行してください。

手順

ステップ 1　[Administrative Tools] から [Internet Information Services] を開きます。

ステップ 2　IIS の Microsoft Exchange 仮想ディレクトリを削除します。

ステップ 3　表示される警告を確認し、推奨されているコマンドレットを Exchange Management Shell（EMS; Exchange 管理シェル）で実行します。



ステップ 4　このコマンドレットを EMS で実行することにより、Exchange 仮想ディレクトリが正しく設定されていることを確認し、ディレクトリを再度 IIS に追加します。

Syntax

```
New-OwaVirtualDirectory -name exchange -OWAVersion Exchange2003or2000
-VirtualDirectoryType mailboxes
```

ステップ 5　Exchange サーバによって仮想ディレクトリが IIS に設定されるのを待ちます。

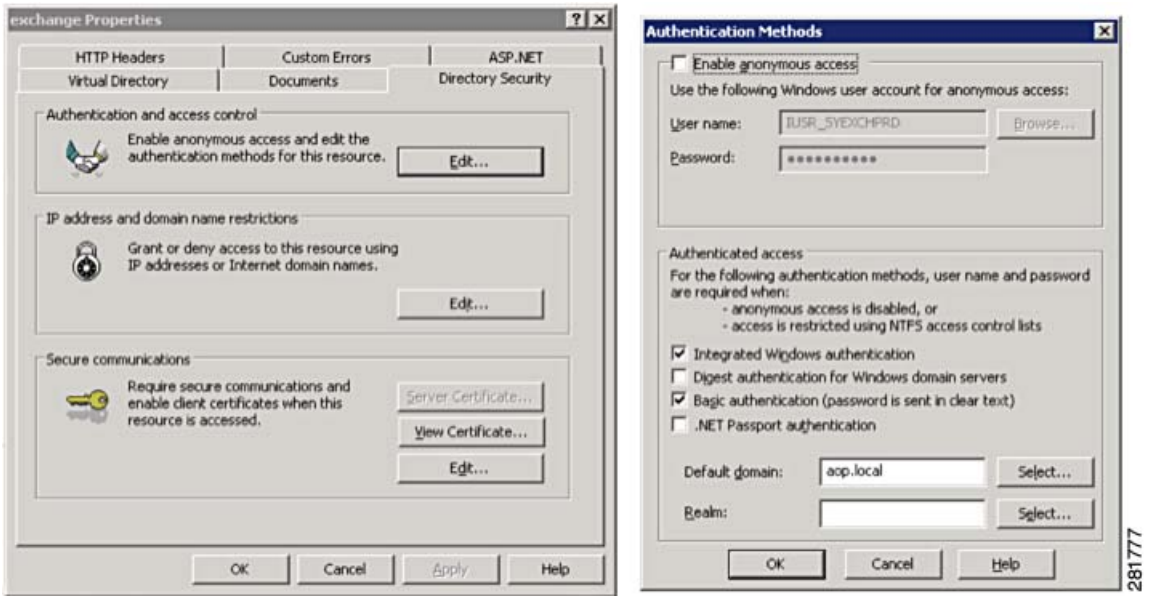
ステップ 6　IIS を再起動します。

ステップ 7　完全なターゲット アドレス（http://mail.contoso.com/exchange/user@contoso.com/calendar など）を使用して、http://<server>/exchange/<user email address>/calendar をテストします。

ステップ 8　ユーザ名とパスワードの入力を求めるメッセージが表示されることを確認します。これは、WebDAV が有効であり、仮想ディレクトリに正しく設定されていることを示します。Active Directory のクレデンシャルを入力します。

ステップ 9　Cisco Unified Presence の IIS ログが表示されたら、内容を確認します。

ステップ 10　ログに 401 認証の問題が報告されている場合は、アクセスを認証するドメインを追加します。



ステップ 11　IIS を再起動します。

ステップ 12　[Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] > [Tools] > [Service Activation] の順に選択し、Cisco UP プレゼンス エンジンを再起動します。

ステップ 13　再度 IIS ログを調べ、予定表に関して正しい SUBSCRIBE メッセージが含まれていることを確認します。

トラブルシューティングのヒント

この手順は、Microsoft Entourage 2008 を使用して電子メールを表示するために WebDAV を必要とする Apple MAC ユーザも対象となります。

会議通知および Cisco IP Phone Messenger のサポート

会議通知機能および Cisco IP Phone Messenger 機能は、ネットワークを WebDAV 経由で統合した場合にのみ有効です。そのため、この問題は Microsoft Exchange 2003 または 2007 でのみ発生します。これらの機能は EWS 統合ではサポートされません。