Microsoft Exchange の設定

予定表統合用の Microsoft Exchange の設定

オンプレミス Microsoft Exchange Server を展開する場合は、この章の手順を実行して、Microsoft Exchange を IM and Presence サービスと Microsoft Outlook 間の予定表統合用に設定します。IM and Presence サービスは、次の Microsoft 展開タイプのそれぞれと統合できます。

表 *1*：*IM and Presence* サービスとの予定表統合用の *Microsoft Exchange* の設定

Microsoft Exchange の展開	Microsoft の設定
Microsoft Exchange 2007	Microsoft Exchange 2007 設定タスク フロー，（1 ページ）
Microsoft Exchange 2010、2013、または 2016	Microsoft Exchange 2010/2013/2016 設定タスク フロー，（10 ページ）

Microsoft Exchange 2007 設定タスク フロー

IM and Presence サービスとの Outlook 予定表統合用に Microsoft Exchange 2007 展開を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Windows のセキュリティ設定の確認, （3 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	ユーザにローカルでサインインする権限を付与するように Exchange Server を設定します。 • Windows Server 2003 での Microsoft Exchange 2007 の設定, （4 ページ） • Windows Server 2008 での Microsoft Exchange 2007 の設定, （5 ページ）	（注） Exchange 偽装を機能させるには、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 レベルでの偽装権限の設定, （5 ページ）	権限は、サーバ、データベース、ユーザ、および連絡先のレベルで付与します。
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, （6 ページ）	偽装を実行するサービス アカウント用の権限は、クライアント アクセス サーバ（CAS）上で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 メールボックスへの Send As 権限の付与, （7 ページ）	サービス アカウントとユーザ 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 メールボックスへの偽装権限の付与, （8 ページ）	サービス アカウントとユーザ メールボックスに偽装権限を付与します。
ステップ 7	Microsoft Exchange 2007 アカウントの権限の確認, （9 ページ）	権限がメールボックス レベルに伝播することと、指定されたユーザがメールボックスにアクセスして、他のユーザのアカウントを偽装できることを確認します。
ステップ 8	Windows Server 2003 を実行する Exchange 2007 の認証の有効化, （10 ページ）	Exchange Server で認証を有効にします。
ステップ 9	Exchange Server 用の証明書の設定タスク フロー, （21 ページ）	Microsoft Exchange 展開用の証明書を設定するには、このタスク フローを実行します。

Windows のセキュリティ設定の確認

手順

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

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

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

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

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

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

b) [OK] をクリックします。

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

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

Windows Server 2003 での Microsoft Exchange 2007 の設定

手順

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

ステップ 2 左ペインの [Security Settings] 下で、[Local Policies] > [User Rights Assignments] に移動します。

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

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

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

ステップ 6 [OK] をクリックします。

次の作業

サーバ レベルでの偽装権限の設定, （5 ページ）

Windows Server 2008 での Microsoft Exchange 2007 の設定

手順

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

ステップ 2 [スタート（Start）] を選択します。

ステップ 3 gpmc.msc と入力します。

ステップ 4 [Enter] を選択します。

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

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

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

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

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

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

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

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

次の作業

サーバ レベルでの偽装権限の設定, （5 ページ）

サーバ レベルでの偽装権限の設定

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

はじめる前に

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

```
Get-OrganizationConfig
```

の文字列を下記に置き換えます。

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

ServerName は Exchange サーバの名前です。

例

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

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

手順

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

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

構文

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

例

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

次の作業

サービス アカウントの Active Directory サービス拡張権限の設定, （6 ページ）

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

はじめる前に

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

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

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

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

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

構文

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

例

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

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

構文

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

例

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

次の作業

サービス アカウントおよびユーザ メールボックスへの Send As 権限の付与, （7 ページ）

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

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

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

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

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

構文

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

例

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

次の作業

サービス アカウントおよびユーザ メールボックスへの偽装権限の付与, （8 ページ）

サービス アカウントおよびユーザ メールボックスへの偽装権限の付与

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

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

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

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

構文

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

例

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

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

次の作業

Microsoft Exchange 2007 アカウントの権限の確認, （9 ページ）

Microsoft Exchange 2007 アカウントの権限の確認

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

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（CAS）が、選択したサービス ノードに表示されていることを確認します。

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

a) サービス アカウントがリストされている。

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

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

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

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

次の作業

Windows Server 2003 を実行する Exchange 2007 の認証の有効化, （10 ページ）

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

手順

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

ステップ 2 [Web サイト（Web Sites）] を選択します。

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

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

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

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

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

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

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

- 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。

次の作業

Exchange Server 用の証明書の設定タスク フロー, （21 ページ）

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

IM and Presence サービスとの Outlook 予定表統合用に Microsoft Exchange 2010、2013、または 2016 展開を設定するには、次のタスクを実行します。

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, （12 ページ）	Windows 統合認証（NTLM）用の Windows セキュリティ設定を確認します。
ステップ 2	お使いのリリース用の Exchange 権限を設定します。 • Exchange 2010 の特定のユーザまたはグループの Exchange 偽装権限の設定, （12 ページ） • Exchange 2013 または 2016 の特定のユーザまたはグループの Exchange 偽装権限の設定 , （14 ページ）	特定のユーザまたはユーザ グループ用の Exchange 偽装権限を設定します。
ステップ 3	お使いのリリース用の権限を確認します。 • Microsoft Exchange 2010 アカウントでの権限の確認, （16 ページ） • Microsoft Exchange 2013 または 2016 アカウントの権限の確認, （18 ページ）	権限がメールボックス レベルに伝播することと、指定されたユーザがメールボックスにアクセスして、他のユーザのアカウントを偽装できることを確認します。
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, （20 ページ）	基本認証と Windows 統合認証のどちらかまたはその両方を Exchange Server の EWS 仮想ディレクトリ（/EWS）で有効にする必要があります。
ステップ 5	Exchange Server 用の証明書の設定タスク フロー, （21 ページ）	Microsoft Exchange 展開用の証明書を設定するには、このタスク フローを実行します。

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で、[スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。

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

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

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

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

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

b) [OK] をクリックします。

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

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

Exchange 2010 の特定のユーザまたはグループの Exchange 偽装権限の設定

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

これらは、Exchange サーバ 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 の特定のユーザまたはグループの Exchange 偽装権限の設定 , （14 ページ）のステップに従います。

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 アカウントを偽装する権限を指定する既存のドメイン サービス アカウント（*Ex2010* など）に付与します。

構文

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

例

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

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

構文

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

例

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

ステップ 5 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 *2*：*Exchange* サーバ *2010* で推奨されるスロットル ポリシーの設定

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

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

注：サポートされる Exchange SP1 でのみ使用可能です。

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

構文

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

例

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

次の作業

Microsoft Exchange 2010 アカウントでの権限の確認, （16 ページ）

関連トピック

Exchange サーバ 2010
Exchange サーバ 2013

Exchange 2013 または 2016 の特定のユーザまたはグループの Exchange 偽装権限の設定

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

Exchange Server 2013 または 2016 のコマンドと設定を以下に示します。Exchange Server 2010 を使用している場合は、Exchange 2010 の特定のユーザまたはグループの Exchange 偽装権限の設定, （12 ページ）のステップに従います。

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、指定された既存のドメイン サービス アカウント（Ex2013 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: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権限が、Ex2013 アカウントに付与されます。

構文

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

例

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

ステップ 5 New-ThrottlingPolicy コマンドを実行し、下の表で定義された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 *3*：***Exchange Server 2013*** または ***2016*** で推奨されているスロットル ポリシー設定

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（**Unlimited**）
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 サーバ 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 で使用されたサービス アカウントを関連付けます。

構文

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

例

```
Set-ThrottlingPolicyAssociation -Identity ex2013 -ThrottlingPolicy IMP_ThrottlingPolicy
```

次の作業

Microsoft Exchange 2013 または 2016 アカウントの権限の確認, （18 ページ）

Microsoft Exchange 2010 アカウントでの権限の確認

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。

これらは、Exchange サーバ 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 アカウントの権限の確認, （18 ページ）のステップに従います。

手順

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

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

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

a) EMS で次のコマンドを実行します。

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

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

例：コマンド出力

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	ユーザ（User）	Direct	ex2010

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

a) EMS で次のコマンドを実行します。

Get-ManagementScope _suImpersonateScope

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

例：コマンド出力

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	いいえ（False）	ユーザ（User）	Direct	識別名（Distinguished Name）

ステップ 5 EMS で次のコマンドを実行して、ThrottlingPolicy パラメータが下の表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 *4*：*Exchange* サーバ *2010* で推奨されるスロットル ポリシーの設定

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

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

次の作業

Exchange 仮想ディレクトリの認証のイネーブル化

関連トピック

Exchange サーバ 2010
Exchange サーバ 2013

Microsoft Exchange 2013 または 2016 アカウントの権限の確認

Exchange 2013 または 2016 アカウントに権限を割り当てた後で、その権限がメールボックスのレベルまで伝播し、指定されたユーザがメールボックスにアクセスしたり別のユーザのアカウントを偽装したりできることを確認する必要があります。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。

（注） Exchange Server 2010 を使用している場合は、Microsoft Exchange 2010 アカウントでの権限の確認, （16 ページ）のステップに従います。

手順

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

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

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

a) EMS で次のコマンドを実行します。

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

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

例：コマンド出力

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	ユーザ（User）	Direct	ex2010

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

a) EMS で次のコマンドを実行します。

```
Get-ManagementScope _suImpersonateScope
```

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

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	いいえ （False）	ユーザ （User）	Direct	識別名 （Distinguished Name）

ステップ 5 EMS で次のコマンドを実行して、ThrottlingPolicy パラメータが下の表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 *5*：*Exchange Server 2013* または *2016* で推奨されているスロットル ポリシー設定

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（Unlimited）**
EwsRechargeRate	900000

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

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 [インターネット情報サービス（Internet Information Services）] を開き、サーバを選択します。

ステップ 2 [Web サイト（Web Sites）] を選択します。

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

ステップ 4 [EWS] を選択します。

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

ステップ 6 次の認証方法が有効になっていることを確認します。

- 匿名認証
- Windows 認証や基本認証

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

次の作業

Exchange Server 用の証明書の設定タスク フロー, （21 ページ）

関連トピック

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

SAN およびワイルドカード証明書のサポート

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

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

ワイルドカード証明書を使用すると、ドメインと無制限のサブドメインを提示できるようになります。これを行うには、ドメイン名にアスタリスク（*）を指定します。名前にはワイルドカード文字 * を含めることができます。ワイルドカードは単一のドメイン名コンポーネントに対応します。たとえば、*.a.com は foo.a.com と一致しますが、bar.foo.a.com とは一致しません。

（注） SAN 証明書については、保護されたホストが [サブジェクトの別名（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 [サブジェクトの代替名（Subject Alternative Name）] フィールドに表示されている保護されたホストと完全に一致している必要があります。
ワイルドカードは、標準証明書の場合は [共通名（CN）（Common Name (CN)）] フィールドに、SAN 証明書の場合は [サブジェクトの代替名（Subject Alternative Name）] フィールドに使用することができます。

Exchange Server 用の証明書の設定タスク フロー

Microsoft Exchange 展開用の証明書を設定するには、次のタスクを実行します。

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 サーバに認証局（CA）をインストールする。 • Windows Server 2003 での CA のインストール, （22 ページ） • Windows Server 2008 での CA のインストール, （23 ページ）	認証局（CA）は Exchange Server 上で動作することもできますが、サードパーティの証明書交換のセキュリティを強化するために、別の Windows サーバを CA として使用することをお勧めします。
ステップ 2	お使いのバージョンの Windows サーバ用の CSR を生成する。 • CSR の作成：Windows Server 2003 の実行, （24 ページ） • CSR の作成：Windows Server 2008 の実行, （26 ページ）	Exchange の IIS サーバで証明書署名要求（CSR）を作成する必要があります。作成した CSR は CA サーバによってその後署名されます。
ステップ 3	CA サーバ/認証局への CSR の提出, （27 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 サーバの完全修飾ドメイン名（FQDN）を使用し、IM and Presence サービスが信頼している認証局の署名を付けることを推奨します。この手順により、CA が Exchange IIS からの CSR に署名できます。

	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, （28 ページ）	署名付き証明書のコピーをダウンロードします。
ステップ 5	お使いのバージョンの Windows サーバに署名付き証明書をアップロードする。 • 署名付き証明書のアップロード：Windows 2003 の実行, （29 ページ） • 署名付き証明書のアップロード：Windows 2008 の実行, （31 ページ）	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。
ステップ 6	ルート証明書のダウンロード, （32 ページ）	CA サーバ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 サービス ノードへのルート証明書のアップロード, （32 ページ）	IM and Presence サービスにルート証明書をアップロードします。

Windows Server 2003 での CA のインストール

はじめる前に

- CA をインストールするには、まず Windows Server 2003 コンピュータにインターネット 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（□）] > [プログラムの追加と削除（Add or Remove Programs）] の順に選択します。

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

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

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

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

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

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

d) [Certificate Database Settings] ウィンドウで、デフォルト設定を受け入れて [Next] をクリックします。

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

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

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

次の作業

CSR の作成：Windows Server 2003 の実行, （24 ページ）

Windows Server 2008 での CA のインストール

手順

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

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

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

ステップ 4 [Add Roles] ウィザードを完了します。

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

b) [サーバ ロールを選択（Select Server Roles）] ウィンドウで、[Active Directory 証明書サービス（Active Directory Certificate Services）] チェックボックスをオンにして、[次へ（Next）] をクリックします。

c) [イントロダクション ウィンドウ（Introduction Window）] ウィンドウで、[次へ（Next）] をクリックします。

d) [ロール サービスを選択（Select Role Services）] ウィンドウで、次のチェックボックスをオンにし、[次へ（Next）] をクリックします。

- Certificate Authority
- Certificate Authority Web Enrollment
- Online Responder

e) [セットアップ タイプを指定（Specify Setup Type）] ウィンドウで、[スタンドアロン（Standalone）] をクリックします。

f) [CA タイプを指定（Specify CA Type）] ウィンドウで、[ルート CA（Root CA）] をクリックします。
g) [プライベート キーのセット アップ（Set Up Private Key）] ウィンドウで、[新しいプライベート キーを作成（Create a new private key）] をクリックします。
h) [CA の暗号化を設定（Configure Cryptography for CA）] ウィンドウで、デフォルトの暗号化サービス プロバイダーを選択します。
i) [CA 名を設定（Configure CA Name）] ウィンドウで、CA を識別する共通名を入力します。
j) [有効期間を設定（Set Validity Period）] ウィンドウで、CA 用に生成された証明書の有効期間を設定します。

（注） CA がここで指定した期日まで有効な証明書を発行します。

k) [証明書データベースを設定（Configure Certificate Database）] ウィンドウで、デフォルトの証明書データベースの場所を選択します。
l) [インストールの選択を確認（Confirm Installation Selections）] ウィンドウで、[インストール（Install）] をクリックします。
m) [インストール結果（Installation Results）] ウインドウで、すべてのコンポーネントに対して「インストールが完了しました（Installation Succeeded）」というメッセージが表示されていることを確認し、[閉じる（Close）] をクリックします。

（注） Server Manager での役割の 1 つとして [Active Directory 証明書サービス（Active Directory Certificate Services）] が表示されます。

次の作業

CSR の作成：Windows Server 2008 の実行, （26 ページ）

CSR の作成：Windows Server 2003 の実行

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

はじめる前に

自己署名証明書：必要に応じて証明書 CA サービスをインストールします。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット 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 [サーバ証明書] を選択します。

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

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

a) [サーバ証明書（Server Certificate）] ウィンドウで、[新しい証明書を作成する（Create a New Certificate）] を選択し、[次へ（Next）] をクリックします。

b) [証明書の要求の送信方法（Delayed or Immediate Request）] ウィンドウで、[証明書の要求を作成して後で送信する（Prepare the request now, but send it later）] を選択し、[次へ（Next）] をクリックします。

c) [名前とセキュリティの設定（Name and Security Settings）] ウィンドウで、デフォルトの Web サイトの証明書名を受け入れ、ビット長に [1024] を選択し、[次へ（Next）] をクリックします。

d) [組織情報（Organization Information）] ウィンドウで、[組織（Organization）] フィールドに会社名を、[組織部門（Organizational Unit）]フィールドに会社の組織部門を入力し、[次へ（Next）] をクリックします。

e) [サイトの一般名（Your Site's Common Name）] ウィンドウで、Exchange サーバ のホスト名または IP アドレスを入力し、[次へ（Next）] をクリックします。

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

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

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

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

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

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

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

次の作業

CA サーバ/認証局への CSR の提出, （27 ページ）

CSR の作成：Windows Server 2008 の実行

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

手順

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

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

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

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

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

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

- [共通名（Common Name）] フィールドに、Exchange サーバのホスト名または IP アドレスを入力します。
- [組織（Organization）] フィールドに、会社名を入力します。
- [組織部門（Organization Unit）] フィールドに、会社が属する組織部門を入力します。

b) 地理情報を次のように入力し、[次へ（Next）] をクリックします。

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

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

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

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

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

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

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

次の作業

CA サーバ/認証局への CSR の提出, （27 ページ）

CA サーバ/認証局への CSR の提出

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

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

はじめる前に

Exchange サーバの IIS で CSR を生成します。

手順

ステップ 1 証明書要求ファイルを CA サーバにコピーします。

ステップ 2 次のいずれかの URL にアクセスします。

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

または

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

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

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

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

PKCS #7 ファイルを使用した更新要求を提出（Submit a renewal request by using a base-64-encoded PKCS #7 file）] を選択します。

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

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

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST-----

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

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

ステップ 10 [送信（Submit）] をクリックします。

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

ステップ 12 要求を右クリックし、次の操作を実行します。

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

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

次の作業

署名付き証明書のダウンロード, （28 ページ）

署名付き証明書のダウンロード

はじめる前に

自己署名証明書：CA サーバに証明書署名要求（CSR）を送信します。

サードパーティ証明書：認証局に CSR を要求します。

手順

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

ステップ 2 その要求を右クリックし、[開く（Open）] を選択します。

ステップ 3 [詳細（Details）] タブを選択します。

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

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

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

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

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

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

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

次の作業

お使いのサーバ 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 の実行, （29 ページ）
- 署名付き証明書のアップロード：Windows 2008 の実行, （31 ページ）

署名付き証明書のアップロード：Windows 2003 の実行

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

はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネット 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 [インターネット情報サービス（Internet Information Services）] ウィンドウで次の手順を実行します。

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

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

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

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

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

ヒント

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

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

次の作業

ルート証明書のダウンロード, （32 ページ）

署名付き証明書のアップロード：Windows 2008 の実行

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

はじめる前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

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

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

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

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

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

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

ステップ 6 [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、次の手順を実行して証明書をバインドします。

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

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

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

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

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

次の作業

ルート証明書のダウンロード, （32 ページ）

ルート証明書のダウンロード

はじめる前に

署名付き証明書を Exchange IIS にアップロードします。

手順

ステップ 1 CA サーバにログインし、Web ブラウザを開きます。

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

a) Windows Server 2003：http://127.0.0.1/certserv

b) Windows Server 2008：https://127.0.0.1/certsrv

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

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

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

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

ヒント

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

次の作業

IM and Presence サービス ノードへのルート証明書のアップロード, （32 ページ）

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

はじめる前に

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

手順

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

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

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

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

ステップ 3 証明書のインポート ツール（ステップ 1, （33 ページ））に戻り、すべてのステータス テストが成功したことを確認します。

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

ヒント

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

次の作業

IM and Presence サービスの設定