Microsoft Exchange の設定

予定表統合のための Microsoft Exchange の構成

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

表 *1 : IM and Presence Service* との予定表統合のための *Microsoft Exchange* の構成

Microsoft Exchange の展開	Microsoft の構成
Microsoft Exchange 2007	Microsoft Exchange 2007 設定タスクフロー （2 ページ）
Microsoft Exchange 2010、2013 または 2016	Microsoft Exchange 2010/2013/2016 の設定タスクフロー （10 ページ）

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

Microsoft Exchange 2007 設定タスクフロー

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

手順

	コマンドまたはアクション	目的
ステップ 1	Windows セキュリティ設定の確認	NTLM 要件などの Windows セキュリティ設定を確認します。
ステップ 2	ローカルでサインインする権限をユーザーに付与するように Exchange Server を設定します。 • Windows Server 2003 での Microsoft Exchange 2007 の設定 • Windows Server 2008 での Microsoft Exchange 2007 の設定	（注） Exchange の偽装を正常に機能させるには、すべての Microsoft Exchange Server を Windows Authorization Access Group のメンバーにする必要があります。 サービスアカウントは、Exchange 管理グループのメンバーであってはなりません。Exchange は、これらのグループのすべてのアカウントの偽装を明示的に拒否します。
ステップ 3	サーバーレベルでの偽装権限の設定	データベース、ユーザー、連絡先レベルでアクセス許可を付与します。
ステップ 4	サービスアカウントの Active Directory サービス拡張権限の設定	これらのアクセス許可は、クライアントアクセスサーバー（CAS）上で、偽装を実行するサービスアカウントに対して設定する必要があります。
ステップ 5	サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与	サービスアカウントおよびユーザーメールボックスに Send As 権限を付与します。
ステップ 6	サービスアカウントおよびユーザーメールボックスへの偽装権限の付与	サービスアカウントおよびユーザーメールボックスへの偽装権限の付与
ステップ 7	Microsoft Exchange 2007 アカウントでのアクセス許可の確認	Exchange 2010 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザーのアカウン

	コマンドまたはアクション	目的
		トを偽装したりできることを確認する必要があります。
ステップ 8	Windows Server 2003 を実行する Exchange 2007 での認証の有効化	Exchange Server で認証を有効にします。
ステップ 9	Exchange Server の証明書の設定タスクフロー （20 ページ）	このタスクフローを完了して、Microsoft Exchange 展開用の証明書を設定します。

Windows セキュリティ設定の確認

手順

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

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

ステップ 3 [ネットワークセキュリティ：NTLM SSPベースクライアント（セキュアな RPC を含む）のサーバー向け最小セッションセキュリティ（Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers）] を選択します。

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

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

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

b) [OK] をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Exchange を実行している Windows ドメインコントローラとサーバーを再起動します。

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

Windows Server 2003 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange 表示専用管理者の役割を委任されたサービスアカウントを使用して Exchange Server 2007 ユーザーインターフェイスにログインします。

ステップ 2 左ペインの [セキュリティ設定（Security Settings）] から **[ローカルポリシー（Local Policies）] > [ユーザー権利の割り当て（User Rights Assignments）]** の順に選択します。

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

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

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

ステップ 6 [OK] をクリックします。

次のタスク

サーバーレベルでの偽装権限の設定

Windows Server 2008 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange 表示専用管理者の役割を委任されたサービスアカウントを使用して Exchange Server 2007 にログインします。

ステップ 2 [スタート（Start）] を選択します。

ステップ 3 gpmc.msc と入力します。

ステップ 4 [Enter] を選択します。

ステップ 5 Exchange Server で [ドメインコントローラセキュリティ設定（Domain Controller Security Settings）] ウィンドウを開きます。

ステップ 6 左ペインの **[セキュリティ設定（Security Settings）]** から **[ローカルポリシー（Local Policies）] > [ユーザー権利の割り当て（User Rights Assignments）] の順に選択します。**

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

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

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

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

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

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

次のタスク

サーバーレベルでの偽装権限の設定

サーバーレベルでの偽装権限の設定

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

はじめる前に

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

  Get-OrganizationConfig

  を次の文字列に置き換えます。

  Get-ExchangeServer -Identity *ServerName*

  ここで、*ServerName* は Exchange Server の名前です。

  例

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

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

手順

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

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

構文

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

例

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

次のタスク

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

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

始める前に

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

- CAS がロードバランサの背後に配置されている場合は、ロードバランサの背後にあるすべての CAS の Microsoft Exchange 2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。
- お使いのメールボックス サーバーが CAS サーバーとは異なるマシン上にある場合は、すべてのメールボックスサーバーの Ex2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。
- このアクセス許可は、[Active Directoryサイトとサービス（Active Directory Sites and Services）] または [Active Directory ユーザーとコンピュータ（Active Directory Users and Computers）] ユーザーインターフェイスを使用して設定することもできます。

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

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

構文

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

例

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

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

構文

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

例

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

次のタスク

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

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

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

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

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

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

構文

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

例

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

次のタスク

サービスアカウントおよびユーザーメールボックスへの偽装権限の付与

サービスアカウントおよびユーザーメールボックスへの偽装権限の付与

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

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

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

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

構文

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

例

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

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

次のタスク

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

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

Exchange 2007 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザーのアカウントを偽装したりできることを確認する必要があります。Exchange 2007 では、アクセス許可がメールボックスに伝播されるまでに多少時間がかかります。

手順

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

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

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

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

ステップ 5 各 CAS サーバーの [プロパティ（Properties）] を表示し、[セキュリティ（Security）] タブで次の点を確認します。「」

a) サービス アカウントがリストされている。

b) サービスアカウントに付与されているアクセス許可が（チェックされているボックスにより）アカウントに Exchange Web サービスの偽装権限が付与されていることを示している。

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

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

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

次のタスク

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

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

手順

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

ステップ 2 [サイト（Web Sites）] を選択します。

ステップ 3 [既定の Web サイト（Default Web Site）] を選択します。

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

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

ステップ 6 [認証とアクセス制御（Authentication and Access Control）] で [編集（Edit）] をクリックします。

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

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

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

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

ステップ 9 [OK] をクリックします。

次のタスク

Exchange Server の証明書の設定タスクフロー （20 ページ）

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	Windows セキュリティ設定の確認 （11 ページ）	Windows 統合認証（NTLM）の Windows セキュリティ設定を確認します。
ステップ 2	使用するリリースの Exchange アクセス許可を設定します。 • Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定 • Exchange 2013 または 2016 の特定のユーザーまたはグループに Exchange の偽装権限を設定	特定のユーザーまたはユーザーグループに Exchange の偽装権限を設定する
ステップ 3	使用するリリースのアクセス許可を確認します。 • Microsoft Exchange 2010 アカウントのアクセス許可の確認 • Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認	Exchange 2010 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザーのアカウントを偽装したりできることを確認する必要があります。

	コマンドまたはアクション	目的
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	Exchange Server の EWS 仮想ディレクトリ (/EWS) で、基本認証、Windows 統合認証、またはその両方を有効にする必要があります。
ステップ 5	Exchange Server の証明書の設定タスクフロー （20 ページ）	このタスクフローを完了して、Microsoft Exchange 展開用の証明書を設定します。

Windows セキュリティ設定の確認

手順

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

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

ステップ 3 [ネットワークセキュリティ：NTLM SSPベースクライアント（セキュアなRPCを含む）のサーバー向け最小セッションセキュリティ（Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers）] を選択します。

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

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

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

b) [OK] をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Exchange を実行している Windows ドメインコントローラとサーバーを再起動します。

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

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

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

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

手順

ステップ 1 Active Directory でアカウントを作成します。

ステップ 2 コマンド ライン入力を行うために EMS を開きます。

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

構文

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

例

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

ステップ 4 この New-ManagementRoleAssignment コマンドを実行し、偽装権限が適用される範囲を定義します。この例では、指定された Exchange Server のすべてのアカウントを偽装する権限が、*Exch2010* アカウントに対して与えられます。

構文

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

例

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

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

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100 -EwsPercentTimeInAD:50
-EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60 -EwsMaxSubscriptions:NULL
-EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

例

```
New-ThrottlingPolicy -Name:IM_and_Presence_ThrottlingPolicy -EwsMaxConcurrency:100
-EwsPercentTimeInAD:50 -EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60
-EwsMaxSubscriptions:NULL -EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

表 *2 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：**Exchange Server 2010**
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000

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

[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリングポリシー値で十分でした。ただし、Client Access Server（CAS）への EWS リクエストの負荷が高い場合は、パラメータを 100 に引き上げることを推奨します。

注：サポートされる Exchange SP1 でのみ使用可能です。

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

構文

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

例

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

次のタスク

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

関連トピック

Exchange Server 2010
Exchange Server 2013

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

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

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

手順

ステップ 1 Active Directory でアカウントを作成します。

ステップ 2 コマンド ライン入力を行うために EMS を開きます。

ステップ 3 EMS で New-ManagementRoleAssignment コマンドを実行し、他のユーザーアカウントを偽装するアクセス許可を指定サービスアカウント（*Ex2013* など）に付与します。

構文

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

例

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2013@contoso.com
```

ステップ 4 この New-ManagementRoleAssignment コマンドを実行し、偽装権限が適用される範囲を定義します。この例では、指定された Exchange Server のすべてのアカウントを偽装するアクセス許可が、*Exch2013* アカウントに対して与えられます。

構文

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

例

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

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

構文

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

例

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

表 *3 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

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

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

注：サポートされる Exchange SP1 でのみ使用可能です。

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

構文

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

例

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

次のタスク

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

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

Exchange 2010 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザーのアカウントを偽装したりできることを確認する必要があります。Exchange 2010 では、アクセス許可がメールボックスに伝播されるまでに多少時間がかかります。

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

手順

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

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

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

a) EMS で次のコマンドを実行します。

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

b) コマンド出力で、次のように、指定アカウントに対する役割「ApplicationImpersonation」の割り当てが示されることを確認します。

コマンド出力の例

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

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

a) EMS で次のコマンドを実行します。

```
Get-ManagementScope _suImpersonateScope
```

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

コマンド出力の例

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

ステップ 5 次のコマンドを EMS で実行して、ThrottlingPolicy パラメータが EMS で定義されている内容と一致することを確認します。

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

表 *4 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

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

[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリングポリシー値で十分でした。ただし、Client Access Server（CAS）への EWS リクエストの負荷が高い場合は、パラメータを 100 に引き上げることを推奨します。

次のタスク

Exchange 仮想ディレクトリでの認証の有効化

関連トピック

Exchange Server 2010
Exchange Server 2013

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

Exchange 2013 または 2016 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザーのアカウントを偽装したりできることを確認する必要があります。アクセス許可がメールボックスに伝播されるまでには多少の時間がかかります。

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

手順

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

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

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

a) EMS で次のコマンドを実行します。

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

b) コマンド出力で、次のように、指定アカウントに対する役割「ApplicationImpersonation」の割り当てが示されることを確認します。

コマンド出力の例

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

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

a) EMS で次のコマンドを実行します。

```
Get-ManagementScope _suImpersonateScope
```

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

コマンド出力の例

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

ステップ 5 次のコマンドを EMS で実行して、ThrottlingPolicy パラメータが EMS で定義されている内容と一致することを確認します。

```
Get-ThrottlingPolicy -Identity IMP_ThrottlingPolicy | Format-List | findstr ^Ews
```

表 *5 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

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

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

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

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

Windows Server 2008 を実行する Exchange 2010、2013 または 2016 の認証の有効化

手順

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

ステップ 2 [サイト（Web Sites）] を選択します。

ステップ 3 [既定の Web サイト（Default Web Site）] を選択します。

ステップ 4 [EWS] を選択します。

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

ステップ 6 次の認証方法が有効になっていることを確認します。

- [匿名認証（Anonymous Authentication）]
- [Windows 認証（Windows Authentication）] および [Basic 認証（Basic Authentication）]（両方またはどちらか）

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

次のタスク

Exchange Server の証明書の設定タスクフロー （20 ページ）

関連トピック

Outlook Web App の仮想ディレクトリの管理

Exchange Web サービス仮想ディレクトリの SSL を有効または無効にする

SAN およびワイルドカード証明書のサポート

IM and Presence Service では、Microsoft Exchange との予定表統合をセキュリティ保護するために、X.509 証明書を使用します。IM and Presence Service では、標準の証明書とともに、SAN およびワイルドカード証明書をサポートしています。

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

ワイルドカード証明書を使用すると、ドメイン名にアスタリスクを指定することにより、ドメインと無制限のサブドメインを表すことができます。名前にはワイルドカード文字 * を含めることができます。ワイルドカードは単一のドメイン名コンポーネントに対応します。たとえば、*.a.com は foo.a.com と一致しますが、bar.foo.a.com とは一致しません。

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

ワイルドカードは、[標準証明書の共通名（CN）（Common Name (CN)）]と、SAN 証明書の [サブジェクトの別名（Subject Alternative Name）] に使用することができます。

Exchange Server の証明書の設定タスクフロー

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

手順

	コマンドまたはアクション	目的
ステップ 1	お使いのバージョンの Windows Server のバージョンに認証局 (CA) をインストールします • Windows Server 2003 での CA のインストール （21 ページ） • Windows Server 2008 での CA のインストール （22 ページ）	認証局（CA）は Exchange Server 上で実行することもできますが、サードパーティの証明書交換のセキュリティを強化するために、別の Windows Server を CA として使用することをお勧めします。
ステップ 2	お使いのバージョンの Windows Server の証明書署名要求を生成します。 • 証明書署名要求の生成：Windows Server 2003 を実行している場合 （23 ページ） • 証明書署名要求の生成：Windows Server 2008 を実行している場合 （24 ページ）	Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバーによって署名されます。
ステップ 3	CA サーバー/認証局への証明書署名要求の送信 （26 ページ）	IIS で Exchange 用に作成されるデフォルトの SSL 証明書には、Exchange Server の完全修飾ドメイン名（FQDN）を使用し、IM and Presence Service が信頼している認証局の署名を付けることを推奨します。この手順により、CA が Exchange IIS からの証明書署名要求に署名できます。
ステップ 4	署名付き証明書のダウンロード （27 ページ）	署名付き証明書をダウンロードします。
ステップ 5	署名付き証明書をお使いのバージョンの Windows Server にアップロードします。 • 署名付き証明書のアップロード：Windows 2003 を実行している場合 （28 ページ）	ここでは、署名付き証明書署名要求を IIS にアップロードする手順を説明します。

	コマンドまたはアクション	目的
	• 署名付き証明書のアップロード：Windows 2008 を実行している場合（29 ページ）	
ステップ 6	ルート証明書のダウンロード （30 ページ）	CA サーバーからルート証明書をダウンロードします。
ステップ 7	IM and Presence Service ノードへのルート証明書のアップロード （31 ページ）	ルート証明書を IM and Presence Service にアップロードします。

Windows Server 2003 での CA のインストール

始める前に

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

手順

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

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

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

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

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

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

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

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

ステップ 4 インターネットインフォメーション サービスを停止するように求められたら [はい（Yes）] を選択します。

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

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

次のタスク

証明書署名要求の生成：Windows Server 2003 を実行している場合　（23 ページ）

Windows Server 2008 での CA のインストール

手順

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

ステップ 2 コンソールツリーで、[役割（Roles）] を選択します。

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

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

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

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

c) [概要（Introduction）] ウィンドウで、[次へ（Next）] をクリックします。

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

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

e) [セットアップの種類の指定（Specify Setup Type）] ウィンドウで、[スタンドアロン（Standalone）] をクリックします。

f) [CAの種類の指定（Specify CA Type）] ウィンドウで、[ルートCA（Root CA）] をクリックします。

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

h) [CAの暗号化を構成（Configure Cryptography for CA）] ウィンドウで、デフォルトの暗号化サービスプロバイダーを選択します。

i) [CA名を構成（Configure CA Name）] ウィンドウで、CA を識別する共通名を入力します。

j) [有効期間の設定（Set Validity Period）] ウィンドウで、CA 用に生成された証明書の有効期間を設定します。

（注） CA が発行する証明書は、ここで指定した期日まで有効になります。

k) [証明書データベースを構成（Configure Certificate Database）] ウィンドウで、デフォルトの証明書データベースの場所を選択します。

l) [インストールオプションの確認（Confirm Installation Selections）] ウィンドウで、[インストール（Install）] をクリックします。

m) [インストールの結果（Installation Results）] ウインドウで、すべてのコンポーネントに対して「インストールが正常に完了しました（Installation Succeeded）」というメッセージが表示されていることを確認し、[閉じる（Close）] をクリックします。

（注） サーバーマネージャに役割の 1 つとして [Active Directory証明書サービス（Active Directory Certificate Services）] が表示されます。

次のタスク

証明書署名要求の生成：Windows Server 2008 を実行している場合 （24 ページ）

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

Exchange の IIS で証明書署名要求（CSR）を生成する必要があります。生成した証明書署名要求は CA サーバーによって署名されます。証明書の [サブジェクトの別名（Subject Alternative Name (SAN)）] フィールドに値が入力されている場合、その値は証明書の共通名（CN）と一致している必要があります。

始める前に

自己署名証明書：必要に応じて証明書 CA サービスをインストールします。

手順

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

a) [既定のWebサイト（Default Web Site）] を右クリックします。

b) [プロパティ（Properties）] を選択します。

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

ステップ 3 [サーバー証明書（Server Certificate）] を選択します。

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

ステップ 5 **サーバー証明書ウィザード**を完了します。

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

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

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

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

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

（注） ここで入力する IIS 証明書の一般名は、IM and Presence Service でプレゼンスゲートウェイを設定するときに使用されるため、接続先のホスト（URI または IP アドレス）と一致している必要があります。

f) [地理情報（Geographical Information）] ウィンドウで次のように地理情報を入力し、[次へ（Next）] を選択します。

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

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

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

h) [要求ファイルの概要（Request File Summary）] ウィンドウに表示されている情報に誤りがないことを確認し、[次へ（Next）] を選択します。

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

次のタスク

CA サーバー/認証局への証明書署名要求の送信 （26 ページ）

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

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

手順

ステップ 1 [管理ツール（Administrative Tools）] から [インターネットインフォメーションサービス（IIS）マネージャ（Internet Information Services (IIS) Manager）] ウィンドウを開きます。

ステップ 2 IIS マネージャの左ペインの [接続（Connections）] の下で、[Exchange Server] を選択します。

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

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

ステップ 5 **証明書の要求**ウィザードを完了します。

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

- [共通名（Common Name）] フィールドに Exchange Server ホスト名または IP アドレスを入力します。
- [組織（Organization）] フィールドに会社名を入力します。
- [組織単位（Organizational Unit）] フィールドに部署名を入力します。

b) 地理情報を次のように入力し、[次へ（Next）] をクリックします。

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

（注） ここで入力する IIS 証明書の一般名は、IM and Presence Service でプレゼンスゲートウェイを設定するときに使用されるため、接続先のホスト（URI または IP アドレス）と一致している必要があります。

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

d) [証明書要求ファイル名（Certificate Request File Name）] ウィンドウで証明書要求の適切なファイル名を入力し、[次へ（Next）] を選択します。

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

e) [要求ファイルの概要（Request File Summary）] ウィンドウに表示されている情報に誤りがないことを確認し、[次へ（Next）] を選択します。

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

次のタスク

CA サーバー/認証局への証明書署名要求の送信 （26 ページ）

CA サーバー/認証局への証明書署名要求の送信

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

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

始める前に

Exchange Server の IIS で証明書署名要求を生成します。

手順

ステップ 1 証明書要求ファイルを CA サーバーにコピーします。

ステップ 2 次のいずれかの URL にアクセスします。

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

または

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

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

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

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

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

ステップ 7 次の行から、

-----BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST-----

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

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

ステップ 10 [送信（Submit）] をクリックします。

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

ステップ 12 要求を右クリックし、次の操作を実行します。

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

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

次のタスク

署名付き証明書のダウンロード （27 ページ）

署名付き証明書のダウンロード

始める前に

自己署名証明書：CA サーバーに証明書署名要求（CSR）を送信します。

サードパーティ証明書：認証局に証明書署名要求を要求します。

手順

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

ステップ 2 その要求を右クリックし、[開く（Open）] を選択します。

ステップ 3 [詳細（Details）] タブを選択します。

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

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

ステップ 6 **証明書のエクスポート**ウィザードを完了します。

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

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

c) [証明書エクスポートウィザードの完了（Certificate Export Wizard Completion）] ウィンドウで、概要を確認し、エクスポートが成功したことを確認して [完了（Finish）] を選択します。

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

次のタスク

使用するサーバータイプ用の署名付き証明書をアップロードします。

- 署名付き証明書のアップロード：Windows 2003 を実行している場合 （28 ページ）
- 署名付き証明書のアップロード：Windows 2008 を実行している場合 （29 ページ）

署名付き証明書のアップロード：Windows 2003 を実行している場合

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

始める前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

ステップ 1 [管理ツール（Administrative Tools）] から**インターネットインフォメーションサービス（Internet Information Services）**を開きます。

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

a) [既定のWebサイト（Default Web Site）] を右クリックします。

b) [プロパティ（Properties）] を選択します。

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

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

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

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

ステップ 5 **サーバー証明書ウィザード**を完了します。

a) [保留中の証明書の要求（Pending Certificate Request）] ウィンドウで、[保留中の要求を処理し、証明書をインストールする（Process the pending request and install the certificate）] を選択し、[次へ（Next）] をクリックします。

b) [保留中の証明書を処理（Process a Pending Request）] ウィンドウで、[参照（Browse）] をクリックして証明書を検索し、適切なパスとファイル名に移動します。

c) [SSLポート（SSL Port）] ウィンドウで、SSL ポートに 443 を入力し、[次へ（Next）] をクリックします。

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

Tip

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

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

次のタスク

ルート証明書のダウンロード （30 ページ）

署名付き証明書のアップロード：Windows 2008 を実行している場合

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

始める前に

自己署名証明書：署名付き証明書をダウンロードします。

サードパーティ証明書：認証局から署名付き証明書が提供されます。

手順

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

ステップ 2 IIS マネージャの左ペインの [接続（Connections）] の下で、[Exchange Server] を選択します。

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

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

ステップ 5 [証明機関の応答を指定します（Specify Certificate Authority Response）] ウィンドウで次の操作を実行します。

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

ステップ 6 [インターネット インフォメーション サービス（Internet Information Services）] ウィンドウで次の手順を実行し、証明書をバインドします。

a) [既定の Web サイト（Default Web Site）] を選択します。
b) IIS マネージャの右ペインにある [操作（Actions）] ウィンドウで [バインディング（Bindings）] を選択します。

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

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

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

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

次のタスク

ルート証明書のダウンロード （30 ページ）

ルート証明書のダウンロード

始める前に

署名付き証明書を Exchange IIS にアップロードします。

手順

ステップ 1 CA サーバーのユーザーインターフェイスにログインし、Web ブラウザを開きます。

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

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

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

ステップ 4 [エンコード方式（Encoding Method）] で、[Base 64] を選択します。

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

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

Tip

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

次のタスク

IM and Presence Service ノードへのルート証明書のアップロード （31 ページ）

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

始める前に

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

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** の [証明書インポートツール（Certificate Import Tool）] を使用して、次の操作を行います。

証明書のアップロード方法	アクション
Cisco Unified CM IM and Presence Administration の [証明書インポートツール（Certificate Import Tool）] [証明書インポートツール（Certificate Import Tool）] は、信頼証明書を IM and Presence Service にインストールするプロセスを簡略化するもので、証明書交換の主要な方法です。このツールでは、Exchange Server のホストとポートを指定すると、サーバーから証明書チェーンがダウンロードされます。承認すると、欠落している証明書が自動的にインストールされます。 （注） この手順では、**Cisco Unified CM IM and Presence Administration** の [証明書インポート ツール（Certificate Import Tool）] にアクセスし、設定する方法を 1 つ紹介します。特定のタイプの予定表統合のために Exchange プレゼンスゲートウェイを設定する場合は、**Cisco Unified Presence Administration** 内の証明書インポートツールのカスタマイズされたバージョンを表示することもできます（**Cisco Unified CM IM and Presence Administration** にログインし、**[プレゼンス（Presence）] > [ゲートウェイ（Gateways）]** を選択します）。	

証明書のアップロード方法	アクション
	1. **Cisco Unified CM IM and Presence Administration** のユーザーインターフェイスにログインします。 2. **[システム（System）] > [セキュリティ（Security）] > [証明書のインポートツール（Certificate Import Tool）]** を選択します。 3. 証明書をインストールする証明書信頼ストアとして [IM and Presence(IM/P) Trust] を選択します。このストアには、Exchange の統合に必要な Presence Engine 信頼証明書が保存されます。 4. Exchange Server に接続するために、次のいずれかの値を入力します。 • IP アドレス • Hostname • FQDN この [ピアサーバー（Peer Server）] フィールドに入力する値は、Exchange Server の IP アドレス、ホスト名、または FQDN と完全に一致している必要があります。 5. Exchange Server との通信に使用するポートを入力します。この値は、Exchange Server の使用可能なポートと一致している必要があります。 6. [送信（Submit）] をクリックします。ツールが完了すると、テストごとに次の状態が報告されます。 • ピアサーバーの到達可能性ステータス：IM and Presence Service が Exchange Server に到達（ping）できるかどうかを示します。「Exchange Server の接続ステータスに関するトラブルシューティング」を参照してください。 • SSL 接続/証明書の確認ステータス：証明書のインポートツールが指定されたピアサーバーから証明書をダウ

証明書のアップロード方法	アクション
	ンロードすることに成功したかどうかと、IM and Presence Service とリモートサーバーの間にセキュアな接続が確立されたかどうかを示します。「SSL 接続と証明書のステータスのトラブルシューティング」を参照してください。

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

証明書のアップロード方法	アクション
Cisco Unified IM およびプレゼンス オペレーティング システムの管理 Exchange Server が SSL/TLS ハンドシェイク中に証明書を提供しない場合、それらの証明書は証明書のインポートツールではインポートできません。この場合、証明書管理ツールを使用して手動で欠落している証明書をインポートする必要があります（**Cisco Unified IM and Presence Operating System Administration** にログインし、**[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します）。	1. IM and Presence Service ノードの管理に使用するコンピュータに、**certnew.cer** 証明書ファイルをコピーするか、FTP で送信します。 2. **Cisco Unified IM and Presence Operating System Administration** ユーザーインターフェイスにログインします。 3. **[Security（セキュリティ）]** > **[Certificate Management（証明書管理）]** を選択します。 4. [証明書の一覧（Certificate List）] ウィンドウで、[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。 5. [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ダイアログボックスが開いたら、次の操作を実行します。 • [証明書名（Certificate Name）] ドロップダウンリストから [cup-xmpp-trust] を選択します。 • 拡張子を付けずにルート証明書の名前を入力します。 6. [参照（Browse）] をクリックし、[certnew.cer] を選択します。 7. [ファイルのアップロード（Upload File）] をクリックします。

ステップ 3 証明書のインポート ツール（ステップ 1 （31 ページ））に戻り、すべてのステータス テストが成功したことを確認します。

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

ヒント

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

次のタスク

IM and Presence 予定表統合のタスクフロー

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