



Skype for Business とのドメイン間フェデレーション

このセクションでは、Skype for Business とのドメイン間フェデレーションについて説明します。

- [Skype for Business ドメイン間フェデレーション \(1 ページ\)](#)
- [Skype for Business フェデレーションのタスク フロー \(2 ページ\)](#)

Skype for Business ドメイン間フェデレーション

IM and Presence Service は、Expressway を介した Skype for Business サーバーとのドメイン間フェデレーションをサポートします。次の統合がサポートされています。

- Business to Business : 別の会社のネットワーク内のリモート Skype for Business サーバーとのフェデレーション
- 単一のエンタープライズネットワーク : 同じエンタープライズネットワーク内にあるが、異なるドメインにあるオンプレミスの Skype for Business サーバーとのフェデレーション。



(注) また、Office365 展開でホストされている Skype for Business サーバーとのフェデレーションを構成することもできます。構成情報を含む詳細については、「[Office 365 とのドメイン間フェデレーション](#)」を参照してください。

Skype for Business フェデレーションの例

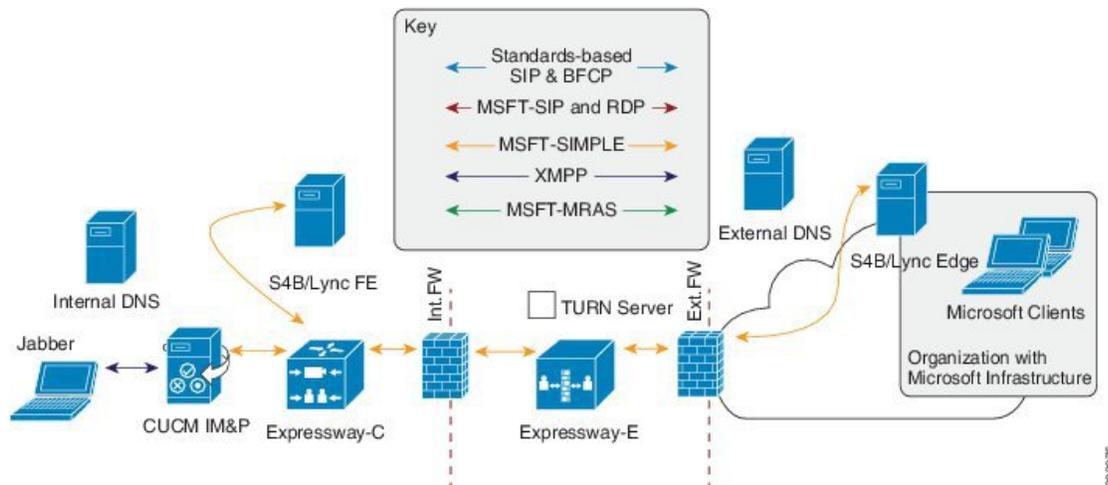
次の図は、Skype for Business サーバーのビジネス ツー ビジネス フェデレーションと単一エンタープライズ ネットワーク フェデレーションの両方を示しています。

- Business to Business フェデレーションでは、図の左側にある IM and Presence Service と、図の右側にある別の会社のネットワークにあるリモート Skype for Business サーバーの間で通信が行われます。この統合には、企業のファイアウォールを通過する通信が必要です。そ

のため、エンタープライズネットワーク内に展開されている Expressway-Cに加えて、ファイアウォールの DMZ 内に Expressway-E を展開する必要があります。

- 単一エンタープライズネットワークでは、オンプレミスの Skype for Business サーバーは企業ネットワーク内にありますが、別のドメインにあります。この図では、Skype for Business サーバーは内部ファイアウォール内にあります。この統合には Expressway-C が必要ですが、通信がファイアウォールを通過する必要がないため、Expressway-E は必要ありません。

図 1: Skype for Business とのフェデレーション



Skype for Business フェデレーションのタスク フロー

オンプレミスまたはリモートの Skype for Business サーバーとのドメイン間フェデレーションを設定するには、次のタスクを実行します。この設定を使用して、次の展開のいずれかを設定できます。

- オンプレミスの Skype for Business サーバーを展開している別の企業との企業間統合。
- 単一の企業内では、IM and Presence Service とオンプレミスの Skype for Business サーバ間のドメイン間フェデレーションを設定できます。



(注) Office 365 でホストされている Skype for Business 展開とのフェデレーションについては、[Office 365 とのドメイン間フェデレーション](#) を参照してください。

はじめる前に

デフォルトでは、フェデレーションルーティングパラメータは、インストール時にデータベースパブリッシャ ノードの FQDN に設定されます。この値をリセットする場合は、[フェデレーションルーティングパラメータの構成](#) に移動します。

	IM and Presence Service の設定	Expressway の設定	Skype for Business の構成	説明
ステップ 1	フェデレーションサービスのオン (4 ページ)			フェデレーションサービスが実行中であることを確認します。
ステップ 2	IM および Presence の DNS SRV の割り当て (5 ページ)			Skype for Business が IM and Presence Service にトラフィックをルーティングできるように、DNS SRV レコードを構成します。
ステップ 3	IM および Presence へのフェデレーションドメインの追加 (5 ページ)			すべての Skype for Business ドメインのドメインエントリを追加します。
ステップ 4	IM and Presence のスタティックルート構成 (6 ページ)			Expressway-C を指すスタティックルートを設定します。
ステップ 5	TLS ピアとしての Expressway の追加 (6 ページ)			Expressway-C を TLS ピアとして設定します。
ステップ 6	アクセス制御リストへの Expressway の追加 (7 ページ)			すべての Expressway-C サーバーをアクセス制御リストに追加します。
ステップ 7	Cisco XCP ルータの再起動 (8 ページ)			構成が完了したら、Cisco XCP ルータサービスを再起動します。

	IM and Presence Service の設定	Expressway の設定	Skype for Business の構成	説明
ステップ 8		Configure Expressway for Federation with Skype for Business (8 ページ)		ドメイン間フェデレーション用に Expressway を構成します。
ステップ 9			ユーザー信頼設定の構成 (9 ページ)	IM and Presence ユーザーの信頼設定を構成します。
ステップ 10			グローバルフェデレーションアクセス設定の構成 (10 ページ)	フェデレーションのグローバルアクセスエッジ設定を構成します。
ステップ 11			IM および Presence を許可ドメインとして追加 (10 ページ)	オプション。このタスクは、グローバルアクセスエッジ設定で IM and Presence ドメインが許可されていない場合にのみ実行します。
ステップ 12			IM および Presence の SIP フェデレーションプロバイダとして Expressway を追加 (11 ページ)	オプション。IM and Presence Service へのトラフィックのルーティングに DNS SRV を使用していない場合にのみ、このタスクを実行します。
ステップ 13	Exchange Certificates (12 ページ)			セットアップ内のサーバー間で証明書を交換します。

フェデレーションサービスのオン

Cisco XCP SIP Federation Connection Manager サービスをオンにします。これにより、プロビジョニングする各ユーザーの SIP フェデレーション機能がオンになります。このタスクは、クラスタ内の各ノードで実行する必要があります。

ステップ 1 Cisco Unified IM and Presence Serviceability のユーザーインターフェイスにログインします。[Tools (ツール)] > [Service Activation (サービス アクティベーション)] を選択します。

- ステップ 2 [サーバー (X8.9.2)] ドロップダウンから、IM and Presence ノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3 [IM and Presence Services] で、Cisco XCP SIP Federation Connection Manager サービスの横にあるオプションボタンがオンになっていることを確認します。
- ステップ 4 [保存 (Save)] をクリックします。
- ステップ 5 SIP フェデレーションが機能するには、Cisco SIP プロキシ サービスが実行されている必要があります。Cisco Unified IM and Presence Serviceability のユーザインターフェイスにログインします。[ツール (Tools)] > [機能サービス (Feature Services)] を選択し、Cisco SIP プロキシ サービスが実行されていることを確認します。

IM および Presence の DNS SRV の割り当て

IM and Presence Service の DNS SRV レコードを構成します。Skype for Business は、このレコードを使用して、Expressway 経由で IM and Presence Service にトラフィックをルーティングします。

- 企業間フェデレーションでは、レコードは Expressway-E の IP アドレスを指すパブリック DNS SRV である必要があります。
- 単一企業内のフェデレーションでは、Expressway-C の IP アドレスを指す内部 DNS を使用できます。フェデレーションは単一の企業内で行われるため、Expressway-E は必要ありません。

例：

```
nslookup
set type=srv
_sipfederationtls._tcp.expwye
```

ここで、expwye は Expressway-E のドメインです。



- (注) DNS SRV レコードがなくてもドメイン間フェデレーションを構成できますが、この場合は、Skype for Business サーバにルートを手動で追加する必要があります。これを行うことを選択した場合は、このタスクをスキップできます。

次のタスク

[IM および Presence へのフェデレーテッド ドメインの追加 \(5 ページ\)](#)

IM および Presence へのフェデレーテッド ドメインの追加

IM and Presence Service で、フェデレーションする Skype for Business ドメインごとにフェデレーション ドメイン エントリを追加します。

-
- ステップ 1 Cisco Unified CM IM およびプレザンス管理から、[プレザンス (Presence)] > [ドメイン間フェデレーション (Inter-Domain Federation)] > [SIP フェデレーション (SIP Federation)] を選択します。
 - ステップ 2 [新規追加 (Add New)] をクリックします。
 - ステップ 3 [ドメイン名 (Domain Name)] フィールドに、ドメイン名を入力します。
 - ステップ 4 ドメインの説明を入力します。たとえば、Skype for Business フェデレーションドメイン。
 - ステップ 5 [統合タイプ (Integration Type)] ドロップダウンから、[Inter-domain to OCS/Lync/S4B] を選択します。
 - ステップ 6 [保存 (Save)] をクリックします。
-

次のタスク

[Cisco XCP ルータの再起動 \(8 ページ\)](#)

IM and Presence のスタティック ルートの構成

IM and Presence Service で、Skype for Business ユーザーのスタティック ルートを構成します。スタティック ルートは TLS を使用し、Expressway-C を指している必要があります。

-
- ステップ 1 Cisco Unified CM IM and Presence 管理で、[プレゼンス (Presence)] > [ルーティング (Routing)] > [スタティック ルート (Static Routes)] を選択します。
 - ステップ 2 [新規追加 (Add New)] をクリックします。
 - ステップ 3 [接続先パターン (Destination Pattern)] フィールドに、Skype for Business の FQDN を逆の形式で入力します。たとえば、ドメインが s4b.com の場合は、.com.s4b.* と入力します。
 - ステップ 4 [次のホップ (Next Hop)] フィールドに、Expressway-C の IP アドレスまたは FQDN を入力します。
 - ステップ 5 [次のホップ ポート (Next Hop Port)] フィールドに 5061 と入力します。
 - ステップ 6 [ルート タイプ (Route Type)] ドロップダウンリストから、[ドメイン (Domain)] を選択します。
 - ステップ 7 [プロトコル タイプ (Protocol Type)] ドロップダウンリスト ボックスから、[TLS] を選択します。
 - ステップ 8 [保存 (Save)] をクリックします。
-

次のタスク

[TLS ピアとしての Expressway の追加 \(6 ページ\)](#)

TLS ピアとしての Expressway の追加

IM and Presence Service で次の手順を使用して、Expressway-C を TLS のピアとして設定します。

-
- ステップ 1 Expressway-C を TLS ピア サブジェクトとして追加します。

- a) Cisco Unified CM IM and Presence 管理 で、[システム (System)]>[セキュリティ (Security)]>[TLS ピア サブジェクト (TLS Peer Subject)]を選択します。
- b) [新規追加 (Add New)]をクリックします。
- c) [ピア サブジェクト名 (Peer Subject Name)]フィールドに、Expressway-C の Expressway-C の完全修飾ドメイン名を入力します。
- d) [説明 (Description)]を入力します。
- e) [保存 (Save)]をクリックします。

ステップ 2 設定した Expressway TLS ピア サブジェクトを含む TLS コンテキストを作成します。

- a) [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)]から [システム (System)]>[セキュリティ (Security)]>[TLS コンテキスト構成 (TLS Context Configuration)]の順に選択します。
- b) [検索 (Find)]をクリックします。
- c) [Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。
- d) [TLS 暗号マッピング (TLS Cipher Mapping)]で、矢印を使用して目的の TLS 暗号を [選択した TLS 暗号 (Selected TLS Ciphers)]ボックスに移動します。ただし、ほとんどの場合、デフォルト設定のままです。
- e) [TLS ピア サブジェクト マッピング (TLS Peer Subject Mapping)]で、矢印を使用して、作成した TLS ピア サブジェクトを [選択した TLS ピア サブジェクト (Selected TLS Peer Subjects)]リストボックスに移動します。
- f) [保存 (Save)]をクリックします。

アクセス制御リストへの Expressway の追加

IM and Presence Service で、Expressway-C が認証なしで IM and Presence Service にアクセスできるように、各 Expressway-C サーバのインバウンドアクセス制御リスト (ACL) エントリを追加します。マルチクラスタ展開の場合は、各クラスタでこの手順を実行します。



- (注) グローバルアクセスを提供する ACL ([すべての許可 (Allow from all)])、または Expressway-C サーバが存在するドメインへのアクセスを提供する ACL (たとえば、[company.com からの許可 (Allow from company.com)]) がある場合は、Expressway-C サーバの ACL エントリを追加する必要はありません。

ステップ 1 IM and Presence Service のパブリッシャ ノードにログインします。

ステップ 2 Cisco Unified CM IM and Presence 管理で、[システム (System)]>[セキュリティ (Security)]>[受信 ACL (Incoming ACL)]を選択します。

ステップ 3 ACL エントリを作成します。

- a) [新規追加 (Add New)]をクリックします。

- b) 新しい ACL エントリの **[説明 (Description)]** を入力します。たとえば、Expressway-C を介した Skype for Business フェデレーション。
- c) Expressway-C の IP アドレスまたは FQDN へのアクセスを提供する **[アドレス パターン (Address Pattern)]** を入力します。たとえば、Allow from 10.10.10.1 または Allow from expwyc.company.com です。
- d) **[保存 (Save)]** をクリックします。
- e) この一連の手順を繰り返して、別の ACL エントリを作成します。サーバーアクセスを提供するには、サーバー IP アドレスを含む ACL とサーバー FQDN を含む ACL の 2 つのエントリが必要です。

ステップ 4 Cisco SIP Proxy サービスを再開します。

- a) **[プレゼンス (Presence)]** > **[ルーティング (Routing)]** > **[設定 (Settings)]** を選択します。
- b) **[すべてのプロキシ サービスの再開 (Restart All Proxy Services)]** をクリックします。

次のタスク

[Cisco XCP ルータの再起動 \(8 ページ\)](#)

Cisco XCP ルータの再起動

設定が完了したら、**Cisco XCP ルータ**を再起動します。

- ステップ 1** [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、**[ツール (Tools)]** > **[コントロールセンター-ネットワークサービス (Control Center - Network Services)]** を選択します。
- ステップ 2** サーバー ドロップダウン リスト ボックスで、IM and Presence データベース パブリッシャ ノードを選択して、**[移動 (Go)]** をクリックします。
- ステップ 3** **[IM and Presence サービス (IM and Presence Services)]** の下で、**[Cisco XCP Router]** サービスを選択します。
- ステップ 4** **[再起動 (Restart)]** をクリックします。
- ステップ 5** すべての IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

次のタスク

[IM and Presence のスタティック ルートの構成 \(6 ページ\)](#)

Configure Expressway for Federation with Skype for Business

After interdomain federation is configured on the IM and Presence Service, set up Expressway for interdomain federation with Skype for Business.

- For business to business interdomain federation, you must deploy both Expressway-C and Expressway-E.

- For interdomain federation with a Skype for Business server that is located within your enterprise network, you can deploy an Expressway-C cluster only as the communication does not need to extend across the WAN.

For Expressway configuration details, see the *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

<http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>.



Note Make sure that your Expressway-C zone configuration points to the port that is associated with TLS Peer Authentication on the IM and Presence Service. You can confirm the correct port on Cisco Unified CM IM and Presence Administration by going to **System > Application Listeners** and confirming the port associated to **Default Cisco SIP Proxy TLS Listener - Peer Auth**. The default is **5062**.

What to do next

After Expressway is configured, proceed with the Skype for Business setup:

[ユーザー信頼設定の構成, on page 9](#)

ユーザー信頼設定の構成

Skype for Business サーバーで、Federated IM and Presence ユーザーのユーザー信頼設定を構成します。

ステップ 1 Skype for Business サーバーにログインします。

ステップ 2 左側のナビゲーションバーで、[フェデレーションと外部アクセス (**Federation and External Access**)] をクリックします。

ステップ 3 ヘッダーバーで、[外部アクセス ポリシー (**EXTERNAL ACCESS POLICY**)] をクリックします。

ステップ 4 [新規 (**New**)] をクリックし、[ユーザー ポリシー (**User Policy**)] を選択します。

ステップ 5 [名前 (**Name**)] フィールドに、IM and Presence ドメインを入力します。

ステップ 6 次のいずれかのオプションを選択します。

- フェデレーテッドユーザーとの通信を有効にする
- リモートユーザーとの通信を有効にする
- パブリックユーザーとの通信を有効にする

ステップ 7 [確定する (**Commit**)] をクリックします。

次のタスク

[グローバルフェデレーションアクセス設定の構成 \(10 ページ\)](#)

グローバル フェデレーション アクセス設定の構成

Skype for Business サーバーで、SIP フェデレーションのグローバルアクセス エッジ設定を構成します。

- ステップ 1** 左側のナビゲーションバーで、[フェデレーションと外部アクセス (Federation and External Access)] をクリックします。
- ステップ 2** ヘッダーバーで、[アクセス エッジ構成 (ACCESS EDGE CONFIGURATION)] をクリックします。
- ステップ 3** [グローバル (Global)] を選択します。
- ステップ 4** すべてのドメインへのアクセスをグローバルに許可する場合は、次の各オプションを選択します。それ以外の場合は、許可するオプションを選択します。

- フェデレーションとパブリック IM 接続の有効化
- [パートナー ドメイン検出の有効化 (Enable partner domain discovery)] : パブリック DNS SRV レコードを使用してトラフィックを IM and Presence Service にルーティングするには、このオプションを選択します。DNS SRV レコードを使用しない場合、または DNS SRV レコードがない場合は、このオプションをオフのままにします。
- リモートユーザー アクセスの有効化
- 会議への匿名ユーザ アクセスの有効化

(注) アクセスをグローバルに許可しない場合は、IM and Presence を許可ドメインおよび SIP フェデレートッドプロバイダーとして手動で追加する必要があります。

- ステップ 5** [確定する (Commit)] をクリックします。

次のタスク

制限付きアクセスを設定した場合 (つまり、一部のグローバルオプションをオフのままにした場合)、[IM および Presence を許可ドメインとして追加 \(10 ページ\)](#)。

グローバルにアクセスを許可しているが、IM and Presence Service にルーティングするためのパブリック DNS SRV レコードがない場合は、[IM および Presence の SIP フェデレートッドプロバイダーとして Expressway を追加 \(11 ページ\)](#)。

それ以外の場合、グローバルにアクセスを許可し、IM and Presence Service にトラフィックをルーティングするパブリック DNS SRV レコードがある場合は、[Exchange Certificates \(12 ページ\)](#)。

IM および Presence を許可ドメインとして追加

Skype for Business サーバのグローバル アクセス エッジ設定ですべてのドメインが許可されていない場合は、この手順を使用します。この場合、IM and Presence Service ドメインの特定のエントリーを追加します。

- ステップ 1 左側のナビゲーションバーで、[フェデレーションと外部アクセス (Federation and External Access)] をクリックします。
- ステップ 2 ヘッダーバーで、[SIP フェデレーション ドメイン (SIP FEDERATED DOMAINS)] をクリックします。
- ステップ 3 [新規 (New)] をクリックし、[許可されたドメイン (Allowed domain)] を選択します。
- ステップ 4 [ドメイン名 (Domain name)] フィールドに、IM and Presence ドメインを入力します。
- ステップ 5 [アクセスエッジサービス (FQDN) (Access Edge Service (FQDN))] フィールドで、Expressway-E 完全修飾ドメイン名を入力します。
- ステップ 6 [確定する (Commit)] をクリックします。

次のタスク

Skype for Business から IM and Presence Service にトラフィックをルーティングするためにパブリック DNS SRV レコードを使用しているかどうかを確認します。

- DNS SRV レコードを使用していない場合は、IM and Presence の SIP プロバイダーとして Expressway を手動で追加します。「[IM および Presence の SIP フェデレーテッドプロバイダとして Expressway を追加 \(11 ページ\)](#)」を参照してください。
- DNS SRV レコードを使用している場合は、[Exchange Certificates \(12 ページ\)](#) を選択します。

IM および Presence の SIP フェデレーテッドプロバイダとして Expressway を追加

Skype for Business からのトラフィックをルーティングするために DNS SRV レコードを使用していない場合は、Skype for Business サーバーでこの手順を使用します。この場合、IM and Presence Service の SIP フェデレーションプロバイダとして Expressway を手動で追加する必要があります。



(注) IM and Presence Service の DNS SRV レコードがある場合は、このタスクをスキップできます。

- ステップ 1 Skype for Business サーバーで、[フェデレーションおよび外部アクセス (Federation and External Access)] をクリックします。
- ステップ 2 [SIP フェデレーション プロバイダ (SIP FEDERATED PROVIDERS)] をクリックします。
- ステップ 3 [新規 (New)] をクリックし、[ホステッドプロバイダ (Hosted provider)] を選択します。
- ステップ 4 [プロバイダ名 (Provider name)] フィールドに、IM and Presence ドメインを入力します。
- ステップ 5 [Access Edge service (FQDN)] フィールドに、Expressway-E サーバの完全修飾ドメイン名を入力します。

ステップ 6 [確定する (Commit)] をクリックします。

次のタスク

[Exchange Certificates \(12 ページ\)](#)

Exchange Certificates

Follow this process to exchange certificates among the servers in your Interdomain Federation with Skype for Business deployment.



Note External Edge certificates from the Skype for Business edge server must have the following OID values under Enhanced Key Usage:

- Server Authentication: (1.3.6.1.5.5.7.3.1)
- Client Authentication: (1.3.6.1.5.5.7.3.2)

ステップ 1 Download certificates from each system in the deployment:

- IM and Presence Service (internal certificate can be self-signed)
- Expressway-C (internal certificate can be self-signed)
- Expressway-E (external certificate must be CA-signed). Note that the Expressway-E is required for Business to Business federation only. Expressway-E is not used for single enterprise network.
- Skype for Business edge server (External Edge certificate must be CA-signed)

Note In this context, if any of the certificates, such as Expressway-E and Skype for Business, are signed by a Certificate Authority, it is the Root CA certificate that is actually added in the relevant far end trust store. Only in the scenario of self-signed certificates should themselves be added to the far end trust stores.

ステップ 2 On the IM and Presence Service, upload the Expressway-C certificate to **cup-trust**.

ステップ 3 On the Expressway-C, upload the IM and Presence Service certificate and, (for Single Enterprise Network federation only) the Skype for Business certificate.

ステップ 4 Upload the Skype for Business certificate as follows:

- (Single Enterprise Network). On the Expressway-C, upload the Skype for Business certificate
- (Business to Business only) On the Expressway-E, upload the Skype for Business External Edge certificate.

ステップ 5 On the Skype for Business edge server, upload the Expressway-E external certificate (for Business to Business) or the Expressway-C certificate (for federation within a single enterprise).

Certificate Notes

- For IM and Presence Service, you can download and upload certificates from the **Certificate Management** window in Cisco Unified IM OS Administration (choose **Security** >

Certificate Management). For detailed procedures, see the "Security Configuration" chapter of the *Configuration and Administration Guide for IM and Presence Service* at <http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html>.

- For Expressway certificate management, see the *Cisco Expressway Administrator Guide* at <http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html>.
- For Skype for Business certificates, you can use the Skype for Business Deployment Wizard to install or download certificates. Run the wizard and select the **Request, Install or Assign Certificates** option. For details, see your Microsoft Skype for Business documentation.

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。