



ドメイン間フェデレーションの構成ワークフロー

ここでは、ドメイン間フェデレーションの構成ワークフローについて説明します。

- [Office 365 Workflow \(Business to Business via Expressway\), on page 1](#)
- [Skype for Business Workflow, on page 2](#)
- [Microsoft Lync ワークフロー \(Expressway 経由の社内\) \(3 ページ\)](#)
- [Microsoft Lync Workflow \(Business to Business via Expressway\), on page 5](#)
- [Microsoft Lync Workflow \(Business to Business via ASA\), on page 6](#)
- [Microsoft OCS ワークフロー \(直接フェデレーション\) \(6 ページ\)](#)
- [Microsoft OCS ワークフロー \(ASA を介した Business to Business\) \(7 ページ\)](#)
- [SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフロー \(8 ページ\)](#)
- [AOL を使用した SIP フェデレーションの構成ワークフロー \(9 ページ\)](#)
- [XMPP フェデレーションのワークフロー \(9 ページ\)](#)

Office 365 Workflow (Business to Business via Expressway)

The IM and Presence Service supports interdomain SIP federation with Office 365 via Cisco Expressway session classification in a business to business configuration. With this integration, Office 365 hosts the Skype for Business deployment.



Note For interdomain federation with Skype for Business without Office 365, see [Skype for Business Workflow, on page 2](#).

IM and Presence Service Configuration

1. Start Federation services. See [フェデレーション サービスのオン](#).
2. Configure a public DNS SRV record for the IM and Presence domain. The SRV should resolve to the Expressway-E IP address. See [IM および Presence サービスの DNS SRV レコードの追加](#).

3. In the IM and Presence Service, add the Office 365 domain entry. See [IM and Presence サービスへの Office 365 ドメインの追加](#).
4. In the IM and Presence Service, configure a TLS static route to Expressway-C. See [Office 365 へのスタティック ルートの構成](#).
5. In the IM and Presence Service, assign Expressway-C as a TLS peer. See [TLS ピアとしての Expressway の追加](#).
6. In the IM and Presence Service, add the Expressway-E server to the inbound access control list. See [アクセス制御リストへの Expressway の追加](#).
7. Restart the Cisco XCP Router on all IM and Presence Service nodes. See [Cisco XCP ルータの再起動](#).
8. Exchange certificates between the servers in your deployment. For the IM and Presence Service, you will need to upload the Expressway-C certificate chain to the **cup-trust** store. See [Exchange Certificates](#).

Cisco Expressway Configuration

After interdomain federation is configured on the IM and Presence Service, set up Cisco Expressway for interdomain federation with Office 365. For Expressway configuration details, see *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

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

Skype for Business Workflow

The IM and Presence Service supports SIP federation with Skype for Business via Expressway in the following integrations:

- Business to Business via Expressway—Federation with a remote Skype for Business server that is located in another company's network.
- Single Enterprise Network—Federation with an on-premise Skype for Business server that is located in the same enterprise network as the IM and Presence Service, but which is in a different domain.



Note Skype for Business can also be hosted by Office 365. For Office 365 deployments, see [Office 365 Workflow \(Business to Business via Expressway\)](#), on page 1.

Following is an overview of the configuration process. For a detailed task flow, see [Skype for Business フェデレーションのタスク フロー](#).

IM and Presence Service Configuration

1. Turn on Federation Services. See [フェデレーション サービスのオン](#).

2. Configure a DNS SRV record for the IM and Presence domain. See [IM および Presence の DNS SRV の割り当て](#).
 - In business to business federations, it should be a public DNS SRV that points to Expressway-E.
 - For interdomain federation within a single enterprise, it can be an internal DNS SRV that points to Expressway-C.



Note You can still configure interdomain federation without the DNS SRV record, but you will have to add the route manually on the Skype for Business server.

3. In the IM and Presence Service, add the Skype for Business domain entry. See [IM および Presence へのフェデレーテッド ドメインの追加](#).
4. In the IM and Presence Service, configure a TLS static route to Expressway. See [IM and Presence のスタティック ルートの構成](#).
5. In the IM and Presence Service, assign Expressway-C as a TLS peer. See [TLS ピアとしての Expressway の追加](#).
6. In the IM and Presence Service, add the Expressway-C server to the inbound access control list. See [アクセス制御リストへの Expressway の追加](#).
7. Restart the Cisco XCP Router service on all IM and Presence nodes. See [Cisco XCP ルータの再起動](#).
8. Exchange certificates between the servers in your deployment. See [Exchange Certificates](#).

Expressway Configuration

Configure Expressway for interdomain federation with Skype for Business. For Expressway configuration details, see the *Chat and Presence XMPP Federation and Microsoft SIP Federation using IM and Presence or Expressway* at:

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

Additional Configuration Details



Note For a more detailed view of the configuration tasks for Skype for Business, see [Skype for Business フェデレーションのタスク フロー](#).

Microsoft Lync ワークフロー (Expressway 経由の社内)

社内シナリオで Expressway を介して IM and Presence Service と Microsoft Lync 間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。

この設定は、チャットのための展開とチャット+コールの展開の両方をサポートします。

IM and Presence Service の設定

1. IM and Presence Service で、Microsoft Lync ドメインのフェデレーション ドメイン エントリを追加します。IM and Presence Service は、フェデレーテッドドメインエントリの着信 ACL を自動的に追加します。「[企業内での Microsoft Lync ドメインの追加](#)」を参照してください。
2. IM and Presence Service で、Microsoft Lync サーバドメインごとに個別の TLS スタティック ルートを設定します。各ルートは、特定の Microsoft フロント エンドサーバーを指す必要があります。「[IM and Presence から Lync へのスタティック ルートの構築](#)」を参照してください。



(注) TLS スタティック ルートを設定する必要があります。TCP は、Microsoft Lync とのフェデレーションではサポートされていません。

3. IM and Presence Service で、Lync サーバ証明書に署名する CA のルート証明書を IM and Presence Service にアップロードします。また、TLS ピアサブジェクトを設定します。「[Set up Certificates on IM and Presence for Federation with Lync](#)」を参照してください。

Expressway の設定

チャット+コール展開の場合のみ、Expressway ゲートウェイを追加します。ゲートウェイで、Microsoft の相互運用性と SIP ブローカを設定します。Expressway を構成するには、[Configure Expressway Gateway for Microsoft Lync Federation](#) に進みます。



(注) チャットのための展開では、Expressway ゲートウェイは必要ありません。

Expressway ゲートウェイの SIP ブローカを使用するチャット+コール展開の場合、サポートは社内シナリオのみに限定されます。ビジネスツービジネスはサポートされていません。

Lync の構成

1. Lync サーバーで、次のいずれかの手順を使用して TLS 静的ルートを構成します。
 1. チャット+コール展開の場合は、[Lync から IM および Presence へのスタティック ルートの構成](#)
 2. チャットのための展開の場合は、[Lync から Expressway ゲートウェイへの静的ルートの構成](#)
2. Lync サーバで、IM and Presence Service を信頼できるアプリケーションとして追加し、各 IM and Presence クラスタ ノードを信頼できるアプリケーション サーバー プールに追加します。「[Lync Server での信頼できるアプリケーションの構成](#)」を参照してください。

3. Lync サーバーで、トポロジをコミットします。「[トポロジの公開](#)」を参照してください。

Microsoft Lync Workflow (Business to Business via Expressway)



Note This deployment is supported for intracompany deployments only. Federation via Expressway Gateway SIP broker is not supported for business to business federation.

Complete the following tasks to set up interdomain federation between IM and Presence Service and Microsoft Lync in a business to business deployment via Expressway's session classification method.

This configuration supports both chat-only and chat+calling deployments.



Note The minimum IM and Presence Service release for this configuration is 11.5(1)SU2.

IM and Presence Service Configuration

1. In the IM and Presence Service, add a federated domain entry for the Microsoft Lync domain. The IM and Presence Service automatically adds the incoming ACL for the federated domain entry. See [企業内での Microsoft Lync ドメインの追加](#).
2. In the IM and Presence Service, configure an individual TLS static route for each Microsoft Lync server domain. Each route should point to a specific Microsoft front end server. See [IM and Presence から Lync へのスタティック ルートの構築](#).



Note You must configure TLS static routes. TCP is not supported for federation with Microsoft Lync.

3. In the IM and Presence Service, upload the root certificate for the CA that signs the Lync server certificates to IM and Presence Service. Also, set up TLS Peer subjects. See [Set up Certificates on IM and Presence for Federation with Lync](#).

Expressway Configuration

Configure Cisco Expressway session classification. Refer to your Cisco Expressway configuration documentation at <https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>. For Release X8.9.2, refer to *Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure*.

Microsoft Lync Workflow (Business to Business via ASA)

- Configure a federated domain on the IM and Presence Service for Microsoft Lync federation, see [SIP フェデレーテッド ドメインの追加](#).
- Configure the DNS SRV records, see [SIP フェデレーションの DNS 構成](#).
- Configure the routing on the IM and Presence Service for Microsoft Lync federation, see [IM および Presence サービスのルーティング構成](#)
- (Optional) Configure the email address for federation feature, see [フェデレーション用の電子メールをオンにする](#)
- Configure the TLS security settings on the IM and Presence Service, see [IM および Presence サービスでセキュリティ設定の構成](#)
- Configure the Cisco Adaptive Security Appliance for Microsoft Lync federation, see [SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフロー](#) and [TLS Proxy Configuration on the Cisco Adaptive Security Appliance](#).
- Configure certificate exchange for Microsoft Lync federation, see [Security Certificate Configuration on Lync Edge Server for TLS Federation](#).
- Configuration of Lync Server 2010 and Edge servers for interdomain federation differs from that outlined within this guide for OCS. For information on configuring the Lync enterprise for interdomain federation with the IM and Presence Service, see [Microsoft documentation](#).

Microsoft OCS ワークフロー（直接フェデレーション）

IM and Presence Service と Microsoft OCS 間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。この設定は、企業内で ASA ファイアウォールを使用しない SIP フェデレーション用です。

IM and Presence Service の設定

1. IM and Presence Service で、Microsoft OCS ドメインのフェデレーション ドメイン エントリを追加します。IM and Presence Service は、フェデレーテッド ドメイン エントリの着信 ACL を自動的に追加します。「[企業内での Microsoft OCS ドメインの追加](#)」を参照してください。
2. IM and Presence Service で、Microsoft OCS サーバ ドメインごとに個別のスタティック ルートを設定します。各ルートは、特定の Microsoft フロント エンド サーバーを指す必要があります。「[Microsoft サーバの IM および Presence サービスのスタティック ルートの構成](#)」を参照してください。



(注) OCS の場合、プロトコルタイプとして TCP または TLS を選択できます。

Microsoft OCS の構成

1. OCS サーバーで、IM and Presence Service ドメインを指す TCP または TLS スタティック ルートを設定します。各ルートは、特定の IM and Presence Service ノードを指している必要があります。「[OCS で IM および Presence サービスに向かうスタティック ルートの構成](#)」を参照してください。
2. IM and Presence Service で、ピア認証リスナーがポート 5061 として設定され、サーバー認証リスナーがポート 5061 ではないことを確認します。「[ピア認証リスナーの確認](#)」を参照してください。
3. OCS サーバーで、各 IM and Presence Service ノードのホスト認証エントリを設定します。TLS 暗号化を使用する場合は、各 IM and Presence ノードに 2 つのエントリを追加する必要があります。1 つはノード IP アドレスを含むエントリ、もう 1 つは FQDN を含むエントリです。「[OCS での IM and Presence サービス ノードのホスト認証エントリの追加](#)」を参照してください。
4. OCS と IM and Presence Service の間に TLS が設定されている場合は、IM and Presence Service とのドメイン間フェデレーション用に OCS で証明書を設定します。TLS を使用していない場合は、この手順をスキップできます。「[ドメイン間フェデレーション用の OCS での証明書の構成](#)」を参照してください。
5. OCS サーバーで、TLS (トランスポートは MTLS または TLS のいずれか) または TCP のリスナーポートが設定されていることを確認します。TLS の場合は、ポート 5061 を使用します。TCP の場合は、ポート 5060 を使用します。「[OCS サーバーでポート 5060/5061 を有効にする](#)」を参照してください。
6. TLS を使用している場合は、FIPS を使用するように OCS を設定します。「[FIPS を使用するための OCS の構成](#)」を参照してください。
7. TLS を使用している場合は、OCS サーバー証明書に署名する CA のルート証明書を IM and Presence Service にアップロードします。「[Set Up Certificates on the IM and Presence Service Node for Federation with Microsoft Server over TLS](#)」を参照してください。

Microsoft OCS ワークフロー (ASA を介した Business to Business)

- Microsoft OCS フェデレーション用の IM and Presence Service でフェデレーテッド ドメインを設定します。「[SIP フェデレーテッド ドメインの追加](#)」を参照してください。
- DNS SRV レコードの構成は、「[SIP フェデレーションの DNS 構成](#)」を参照してください。

- Microsoft OCS フェデレーションの IM and Presence Service でルーティングを構成します。「[IM および Presence サービスのルーティング構成](#)」を参照してください。
- (オプション) フェデレーション機能の電子メールアドレスを設定します。「[フェデレーション用の電子メールをオンにする](#)」を参照してください。
- IM and Presence サービスでのセキュリティを設定します。IM および Presence サービスで [セキュリティ設定の構成](#) を参照してください。
- Microsoft OCS フェデレーション用の Cisco 適応型セキュリティアプライアンスを構成します。SIP フェデレーション向け Cisco 適応型セキュリティアプライアンスのワークフローと Cisco 適応型セキュリティアプライアンスでの [TLS Proxy の構成](#) を参照してください。
- Microsoft OCS フェデレーションの証明書交換を設定します。「[SIP Federation Security Certificate Configuration with Cisco Adaptive Security Appliance](#)」を参照してください。
- Microsoft OCS サーバーを設定します。「[SIP フェデレーションの外部サーバー コンポーネントの構成](#)」を参照してください。
- (オプション) 冗長性のためにロードバランサを設定します。「[SIP フェデレーションの冗長性のためのロードバランサの構成](#)」を参照してください。
- Microsoft OCS フェデレーションのトラブルシューティング情報については、「[SIP フェデレーション統合のトラブルシューティング](#)」を参照してください。

SIP フェデレーション向け Cisco 適応型セキュリティ アプライアンスのワークフロー

- Cisco 適応型セキュリティアプライアンスと IM and Presence Service (内部インターフェイス) 間の証明書を構成します。「[IM および Presence サービスと Cisco 適応型セキュリティアプライアンス間のセキュリティ証明書の交換](#)」を参照してください。
- Cisco 適応型セキュリティアプライアンスとフェデレーションドメイン (外部インターフェイス) 間の証明書を構成します。「[Microsoft CA を使用した Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge \(外部インターフェイス\) 間のセキュリティ証明書の交換](#)」を参照してください。
- プライベートからパブリックへのメッセージングの PAT ルールを設定します。「[ポートアドレス変換 \(PAT\)](#)」を参照してください。
- パブリックからプライベートへのメッセージング用のスタティック PAT を設定します。「[スタティック PAT コマンドの例](#)」を参照してください。
- 必要なアクセスリストを構成します。「[アクセスリストの構成要件](#)」を参照してください。
- TLS プロキシインスタンスを構成します。「[TLS プロキシインスタンスの構成](#)」を参照してください。

- アクセスリストを TLS プロキシに関連付けます。「[クラスマップを使用したアクセスリストと TLS プロキシインスタンスの関連付け](#)」を参照してください。

AOL を使用した SIP フェデレーションの構成ワークフロー

- AOL フェデレーションを有効にするには、AOL ライセンスを確立します。「[AOL フェデレーションのライセンス要件](#)」、「[AOL ルーティング情報の要件](#)」、および「[AOL プロビジョニング情報の要件](#)」を参照してください。
- AOL フェデレーション用に IM and Presence Service でフェデレーテッド ドメインを構成します。[SIP フェデレーテッド ドメインの追加](#)」を参照してください。
- DNS SRV レコードの構成は、「[SIP フェデレーションの DNS 構成](#)」を参照してください。DNS を使用していない場合は、次の手順を参照してください。
- AOL フェデレーションのルーティングを構成します。「[TLS を使用したスタティック ルートの構成](#)」を参照してください。
- (オプション) AOL でホストされているドメインのデフォルト フェデレーション ルーティング ドメインを確認して構成します。
- (オプション) フェデレーション機能の電子メールアドレスを設定します。「[フェデレーション用の電子メールをオンにする](#)」を参照してください。
- IM and Presence Service で TLS セキュリティ設定と証明書を構成します。「[IM および Presence サービスでセキュリティ設定の構成](#)」および「[Cisco 適応型セキュリティ アプライアンスと AOL SIP アクセス ゲートウェイ間のセキュリティ証明書の交換](#)」を参照してください。
- AOL の Cisco 適応型セキュリティ アプライアンス for AOL を構成します。AOL FQDN、サーバポート、およびパブリック IP アドレスの詳細については、[AOL SIP アクセス ゲートウェイ](#) を参照してください。
- (オプション) 冗長性のためにロードバランサを設定します。「[SIP フェデレーションの冗長性のためのロード バランサの構成](#)」を参照してください。

XMPP フェデレーションのワークフロー



-
- (注) Webex、IM and Presence Service、および IBM Sametime については、このワークフローに従います。
-
- XMPP フェデレーション用に IM and Presence Service を設定します。「[XMPP フェデレーションの IM および Presence サービス構成](#)」を参照してください。

- XMPP フェデレーションのセキュリティを設定します。「[XMPP フェデレーションのセキュリティ証明書の構成](#)」を参照してください。
- (オプション) フェデレーション機能の電子メールアドレスを設定します。「[フェデレーション用の電子メールをオンにする](#)」を参照してください。
- XMPP フェデレーションサービスをオンにします。「[XMPP フェデレーションサービスをオンにする](#)」を参照してください。
- XMPP フェデレーション用に Cisco 適応型セキュリティアプライアンスを設定します。「[XMPP フェデレーション用の Cisco 適応型セキュリティアプライアンスの構成](#)」を参照してください。
- XMPP フェデレーションのトラブルシューティング情報については、「[XMPP フェデレーション統合のトラブルシューティング](#)」を参照してください。

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。