MRA 導入のアップグレード後のタスク

MRA アクセス制御設定を再構成するには

重要

- アップグレード後は、[内部認証の可用性の確認（Check for internal authentication availability）] 設定がオフになります。Unified CM の認証設定によっては、一部の Cisco Jabber ユーザによるリモートログインが妨げられる場合があります。
- X8.9 の [排他（Exclusive）] オプションの設定は、[認証パス（Authentication path）] で [SAML SSO 認証（SAML SSO authentication）] を指定することで設定します。これには、ユーザー名とパスワードによる認証禁止が適用されます。

始める前に

システムを再起動した後、MRA アクセス制御の設定を再設定する必要があります。

ステップ 1 で、[構成（Configuration）] > [Unified Communications] > [構成（Configuration）] > [MRAアクセス制御（MRA Access Control）] に移動します。

ステップ 2 次のいずれかを実行します。

- 新しい MRA アクセス制御方式を X8.10 から利用するには、このページで選択した方法で適切な値を設定します。どの値を適用するかについては、次の最初の表を参照してください。
- または、アップグレード前の認証方法を保持するには、このページで、 の以前の設定に合わせて適切な値を設定します。従来の の設定と同等の の新しい設定を調べるには、次の 2 番目の表を参照してください。

ステップ 3 自己記述トークン（[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]）を構成する場合は、Unified CM ノードを更新します。[構成（Configuration）] > **[Unified Communications]** > ***[UCサーバタイプ（UC server type）]*** に移動し、[サーバーの更新（Refresh servers）] をクリックします。

MRA アクセス制御の設定

Web UI で実際に表示されるフィールドは、MRA が有効かどうか（[Unified Communications モード（Unified Communications mode）] が [モバイルおよびリモート アクセス（Mobile and remote access）] に設定されているかどうか）、および選択された認証パスによって異なります。テーブル内のすべてのフィールドが必ずしも表示されるわけではありません。

表 *1 : MRA* アクセス制御の設定

フィールド	説明	デフォルト
認証パス（Authentication path）	MRA が有効になるまで非表示のフィールド。MRA 認証の制御方法を定義します。 SAML SSO 認証（SAML SSO authentication）：クライアントは外部 IdP によって認証されます。 UCM/LDAP Basic 認証（UCM/LDAP basic authentication）：クライアントは、Unified CM によって LDAP 資格情報に対してローカルに認証されます。 SAML SSO および UCM/LDAP（SAML SSO and UCM/LDAP）：どちらの方法も許可します。 なし（None）：認証は適用されません。これは、MRA が最初に有効になるまでのデフォルトです。単に MRA をオフにするのではなく [なし（None）]「」オプションが用意されているのは、展開によっては、実際には MRA ではない機能を許可するために MRA をオンにする必要があるためです。（Meeting Server の Web プロキシ、XMPP フェデレーションなど）。[なし（None）]「」は、そのような場合にのみ使用してください。 （注） 他のケースでは使用しないでください。	MRA をオンにするまでは [なし（None）] MRA をオンにした後は [UCM/LDAP]

フィールド	説明	デフォルト
OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）	このオプションでは、承認のための自己記述トークンが必要です。サポート用のインフラストラクチャを持つすべての展開で推奨される承認オプションです。 現在、この承認方法を使用できるのは Jabber クライアントだけです。他の MRA エンドポイントは現在サポートしていません。また、クライアントは、更新を伴う OAuth トークン承認モードにある必要があります。	[オン（On）]
OAuth トークンによる承認（Authorize by OAuth token）（以前は SSO モード）	[認証パス（Authentication path）] が [SAML SSO] または [SAML SSO および UCM/LDAP（SAML SSO and UCM/LDAP）] の場合に利用可能。 このオプションには、IdP を使用した認証が必要です。現在、Jabber クライアントのみがこの承認方法を使用できますが、他の MRA エンドポイントではサポートされていません。	[オフ（Off）]
ユーザ クレデンシャルによる承認（Authorize by user credentials）	[認証パス（Authentication path）] が [UCM/LDAP] または [SAML SSO および UCM/LDAP（SAML SSO and UCM/LDAP）] の場合に利用可能。 ユーザクレデンシャルによる認証を実行しようとするクライアントは、MRA によって許可されます。これには、Jabber、およびサポートされている IP フォンと TelePresence デバイスが含まれます。	オフ（Off）

フィールド	説明	デフォルト
内部認証の可用性の確認（**Check for internal authentication availability**）		[いいえ（No）]

フィールド	説明	デフォルト
	[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）] または [OAuth トークンによる承認（Authorize by OAuth token）] が有効になっている場合に利用可能。 最適なセキュリティとネットワーク トラフィックの削減のため、デフォルトは[いいえ（No）] です。 Expressway-C がホーム ノードをチェックするかどうかを選択することにより、Expressway-E がリモート クライアント認証リクエストにどのように反応するかを制御します。 リクエストは、クライアントが OAuth トークンによってユーザを認証しようとする可能性があるかどうかを尋ね、そのリクエストには Expressway-C がユーザのホーム クラスタを見つけるためのユーザ ID が含まれています。 はい（Yes）：*get_edge_sso* リクエストで、OAuth トークンがサポートされているかどうかをユーザのホーム Unified CM に確認します。ホーム Unified CM は、Jabber クライアントの *get_edge_sso* リクエストによって送信されたアイデンティティから判別されます。 いいえ（No）：Expressway が内部を参照しないように構成されている場合に、Edge の認証設定に応じて、すべてのクライアントに同じ応答が送信されます。 選択するオプションは、実装およびセキュリティ ポリシーによって異なります。すべての Unified CM ノードで OAuth トークンがサポートされている場合は、[いいえ（No）] を選択して応答時間とネットワーク全体のトラフィックを減らすことができます。または、ロールアウト中にクライアントがエッジ構成を取得するモードを使用するようにする場合や、すべてのノードでOAuthを保証できない場合は、[はい（Yes）] を選択します。 **注意** これを [はい（Yes）] に設定すると、認証されていないリモート クライアントからの不正なインバウ	

フィールド	説明	デフォルト
	ンドリクエストが許可される可能性があります。この設定に [いいえ（No）] を指定すると、Expressway は不正なリクエストを防止します。	

フィールド	説明	デフォルト
ID プロバイダー：**IdP の作成または変更（Identity providers: Create or modify IdPs**）		-

フィールド	説明	デフォルト
	[認証パス（Authentication path）] が [SAML SSO] または [SAML SSO および UCM/LDAP（SAML SSO and UCM/LDAP）] の場合に利用可能。 **ID プロバイダーの選択** シスコ コラボレーション ソリューションは、SAML 2.0（セキュリティ アサーション マークアップ言語）を使用して、ユニファイド コミュニケーション サービスを利用するクライアント用の SSO（シングル サインオン）を有効にします。 使用する環境に SAML ベース SSO を選択した場合は、次の点に注意してください。 • SAML 2.0 は、SAML 1.1 との互換性がないため、SAML 2.0 標準を使用する IdP を選択する必要があります。 • SAMLベースのアイデンティティ管理は、コンピューティングとネットワーキング業界のベンダーによって異なる方法で実装されています。したがって、SAML 標準に準拠するための幅広く受け入れられている規制はありません。 • 選択した IdP の設定や管理ポリシーは、Cisco TAC（テクニカル アシスタンス センター）のサポート対象外です。IdPベンダーとの関係とサポート契約を利用して、IdPを正しく設定する上での支援を得られるようにしてください。Cisco は IdP に関するエラー、制限、または特定の設定に関する責任を負いません。 シスコ コラボレーション インフラストラクチャは、SAML 2.0 への準拠を主張する他の IdP と互換性がある可能性もありますが、シスコ コラボレーション ソリューションでテストされているのは次の IdP だけです。 • OpenAM 10.0.1 • Active Directory Federation Services 2.0（AD FS 2.0）	

フィールド	説明	デフォルト
	• PingFederate® 6.10.0.4	
ID プロバイダー：SAML データのエクスポート（Identity providers: Export SAML data）	[認証パス（Authentication path）] が [SAML SSO] または [SAML SSOおよびUCM/LDAP（SAML SSO and UCM/LDAP）] の場合に利用可能。 SAMLデータの操作の詳細については、「*Edge* 経由の *SAML SSO* 認証」を参照してください。	-
Jabber iOS クライアントによる組み込みの Safari の使用の許可（Allow Jabber iOS clients to use embedded Safari）	デフォルトでは、IdP または Unified CM の認証ページは、iOS デバイスの組み込み Web ブラウザ（Safariブラウザではない）に表示されます。このデフォルトのブラウザは iOS の信頼ストアにアクセスできないので、デバイスに導入された証明書を使用することはできません。 この設定では、オプションで、iOS デバイス上の Jabber がネイティブの Safari ブラウザを使用することができます。Safari ブラウザでは、デバイスの信頼ストアにアクセスできるため、OAuth 導入時にパスワードレス認証または二要素認証を有効化できるようになりました。 このオプションには潜在的なセキュリティの問題が存在します。認証が完了した後で、Safari から Jabber にブラウザ制御を返す機能は、カスタムプロトコルハンドラを呼び出すカスタム URL 方式を使用します。Jabber 以外の別のアプリケーションがこの方式を妨害し、iOS から制御を取得できます。この場合、アプリケーションはURL の OAuth トークンへアクセスできます。 すべてのモバイル デバイスが管理されているなどの理由で、iOS デバイスに Jabber のカスタムURL形式を登録する他のアプリケーションがないと確信する場合、オプションを有効にしても安全です。別のアプリケーションがカスタム Jabber URL を妨害する可能性が心配な場合、組み込み Safari ブラウザを有効にしないでください。	[いいえ（No）]

フィールド	説明	デフォルト
SIP トークンの余分なパケット存続時間（SIP token extra time to live）	[OAuth トークンによる承認（Authorize by OAuth token）] が [オン（On）] の場合に利用可能。 必要に応じて、簡単な OAuth トークンの存続可能時間（秒）を延長します。クレデンシャルの有効期限が切れた後、コールを受け入れるための短い時間枠をユーザに提供します。ただし、潜在的なセキュリティ リスクが増加します。	0 秒

アップグレードによって適用されるMRAアクセス制御値

表 *2:* アップグレードによって適用される *MRA* アクセス制御値

オプション	アップグレード後の値	従来	現在
認証パス（Authentication path）	アップグレード前の設定が適用されます （注） [SSOモード（SSO mode）]：X8.9 の [オフ（Off）] は、X8.10 の 2 つの設定になります。 • **認証パス（Authentication path）** = *UCM/LDAP* • **ユーザ ログイン情報による承認（Authorize by user credentials）** = オン（*On*） [SSOモード（SSO mode）]：X8.9 の [排他（Exclusive）] は、X8.10 では 2 つの設定になっています。 • **認証パス（Authentication path）** = *SAML SSO* • **OAuth トークンによる承認（Authorize by OAuth token）** = オン（*On*） [SSOモード（SSO mode）]：X8.9 の [オン（On）] は、X8.10 では 2 つの設定になっています。 • **認証パス（Authentication path）** = *SAML SSO* および *UCM/LDAP* • **OAuth トークンによる承認（Authorize by OAuth token）** = オン（*On*） • **ユーザ ログイン情報による承認（Authorize by user credentials）** = オン（*On*）	両方	Expressway-C

オプション	アップグレード後の値	従来	現在
OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）	[オン（On）]	-	Expressway-C
OAuth トークンによる承認（Authorize by OAuth token）（以前は SSO モード）	アップグレード前の設定が適用されます	両方	Expressway-C
ユーザ クレデンシャルによる承認（Authorize by user credentials）	アップグレード前の設定が適用されます	両方	Expressway-C
内部認証の可用性の確認（Check for internal authentication availability）	[いいえ（No）]	Expressway-E	Expressway-C
ID プロバイダー：IdP の作成または変更（Identity providers: Create or modify IdPs）	アップグレード前の設定が適用されます	Expressway-C	Expressway-C（変更なし）
ID プロバイダー：SAML データのエクスポート（Identity providers: Export SAML data）	アップグレード前の設定が適用されます	Expressway-C	Expressway-C（変更なし）

オプション	アップグレード後の値	従来	現在
Jabber iOS クライアントによる組み込みの Safari の使用の許可（Allow Jabber iOS clients to use embedded Safari）	[いいえ（No）]	Expressway-E	Expressway-C
SIP トークンの余分なパケット存続時間（SIP token extra time to live）	アップグレード前の設定が適用されます	Expressway-C	Expressway-C（変更なし）

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。