Cisco Unity Connection クイック スタート ガイド

SAML SSO アクセス - リリース 10.0(1) 以降

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

- 「始めに」（P.2）
- 「サービス プロバイダーおよびアイデンティティ プロバイダーについて」（P.3）
- 「SAML プロトコルについて」（P.3）
- 「Unity Connection Web アプリケーションへのシングル サインオン（SSO）アクセスの必要性」（P.4）
- 「Unity Connection 10.0(1) 以降で SAML SSO を有効にするための要件」（P.5）
- 「Cisco Unity Connection 10.x での SAML SSO 機能の設定」（P.5）
- 「SAML SSO を使用した Cisco Unity Connection 10.x の Web アプリケーション ページへのアクセス」（P.6）
- 「Cisco Unity Connection の SAML SSO コマンド」（P.7）
- 「Cisco Unity Connection の SAML SSO のトラブルシューティング」（P.8）

発行日：2013 年 11 月

1 始めに

Cisco Unity Connection 10.0(1) 以降、オープンな業界標準プロトコルの SAML（Security Assertion Markup Language）を使用した拡張ログイン機能が導入されました（SAML は、HTTP リダイレクト バインディングおよび HTTP POST バインディングで動作する複数のバインディング プロトコルをサポートします）。Cisco Unity Connection 10.0(1) 以降のリリースでは、SAML シングル サインオンおよび OpenAM シングル サインオンの両方をサポートしていますが、一度に有効にできる SSO 機能は 1 つのみです。

（注） SAML バインディングは、標準のメッセージング フォーマットおよび通信プロトコルへの SAML プロトコル メッセージのマッピングです（例：リダイレクト バインディングおよび HTTP POST バインディング）。

SAML SSO では、次の Unified Communication 製品で、Unity Connection サブスクライバ Web インターフェイスを使用した管理 Web アプリケーション間のシングル サインオン アクセスが可能です。

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified IM/Presence

SAML SSO により、LDAP ユーザは、アイデンティティ プロバイダーで認証されるユーザ名とパスワードでログインできます。アイデンティティ プロバイダーの詳細については、以下を参照してください。

クイック スタート ガイドの「**サービス プロバイダーおよびアイデンティティ プロバイダーについて**」*の章*

SAML プロトコルの詳細については、以下を参照してください。

クイック スタート ガイドの「**SAML プロトコルについて**」*の章*

管理者権限を持つ非 LDAP ユーザは、リカバリ URL を使用して Cisco Unity Connection Administration にログインします。リカバリ URL は、ユーザ名とパスワードによる管理およびサービスアビリティ Web アプリケーションへの代替アクセスを提供します。非 LDAP ユーザは、リカバリ URL を使用して、Unity Connection の次の Web アプリケーションにアクセスできます。

- Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unified Serviceability

（注） LDAP ユーザは、Active Directory に統合されたユーザです。非 LDAP ユーザは、Unity Connection サーバにローカルに常駐するユーザです。

Unity Connection（LDAP または非 LDAP）ユーザは、SAML SSO を使用して、次の Unity Connection Web アプリケーションにシングル サインオン アクセスできません。

- Disaster Recovery System
- Cisco Unified Operating System Administration

Web アプリケーションへのシングル サインオン アクセスの詳細については、次のセクションを参照してください。

SAML SSO を使用した Cisco Unity Connection 10.x の Web アプリケーション ページへのアクセス

Unity Connection ユーザは、SAML SSO を使用して、Unified Communication の Web アプリケーションにシングル サインオン アクセスできます。SAML SSO では、1 回のログインで Web アプリケーションにアクセスできます。

Cisco Unity Connection で SAML SSO 機能を有効にするには、いくつかの要件を満たし、設定手順に従う必要があります。

SAML SSO の設定の要件の詳細については、次のセクションを参照してください。

Unity Connection 10.0(1) 以降で SAML SSO を有効にするための要件

SAML SSO の設定の詳細については、次のセクションを参照してください。

Cisco Unity Connection 10.x での SAML SSO 機能の設定

SAML SSO 機能は、Cisco Unity Connection Administration からのみ有効になりますが、一連のコマンドを備えた CLI インターフェイスから SSO ステータスをチェックしたり、SSO を無効にすることもできます。

SAML SSO の CLI コマンドの詳細については、次のセクションを参照してください。

Cisco Unity Connection の SAML SSO コマンド

SAML SSO のトラブルシューティングの詳細については、次のセクションを参照してください。

Cisco Unity Connection の SAML SSO のトラブルシューティング

2 サービス プロバイダーおよびアイデンティティ プロバイダーについて

サービス プロバイダー（**SP**）は、Web アプリケーションを提供する Unity Connection 上の保護されたエンティティです。サービス プロバイダーは、認証と承認に信頼できるアイデンティティ プロバイダー（IdP）またはセキュリティ トークン サービス（STS）を利用します。

アイデンティティ プロバイダーは、セキュリティ トークンでユーザを認証するオンライン サービスまたは Web サイトです。アイデンティティ プロバイダーは、エンド ユーザを認証して SAML アサーションを返します。SAML アサーションは、はい（認証済み）または、いいえ（認証に失敗）の応答を表示します。

要求された Web アプリケーションにアクセスするには、ユーザ資格をアイデンティティ プロバイダーで認証する必要があります。いずれかの時点で認証が拒否された場合、ユーザは要求された Web アプリケーションにアクセスできません。認証が許可された場合、ユーザは要求された Web アプリケーションにシングル サインオン アクセスできます。

SAML SSO メカニズムの詳細については、以下を参照してください。

クイック スタート ガイドの「SAML プロトコルについて」のセクション

現在サポートされているアイデンティティ プロバイダーは、次のとおりです。

- OpenAM バージョン 10.1
- ADFS（Active Directory Federated Services）バージョン 2.0
- Ping Federate バージョン 6.10.0.4
- Oracle Identity Manager バージョン 11.0

上記のサービス プロバイダーおよびアイデンティティ プロバイダーの定義は、SAML プロトコル メカニズムの理解に役立ちます。

3 SAML プロトコルについて

Security Assertion Markup Language（SAML）は、データ交換用の XML ベースのオープンな標準データ フォーマットです。SAML は、サービス プロバイダーによってユーザの認証に使用される認証プロトコルです。セキュリティ認証情報は、アイデンティティ プロバイダーとサービス プロバイダーの間で渡されます。

SAML は、クライアント プラットフォームに関係なく、SAML 対応のコラボレーション（Unified Communication）サービスに対してクライアントによる認証を可能にするオープン標準です。

すべての Cisco Unified Communication Web インターフェイス（CUCM や Unity Connection など）は、SAML SSO 機能の SAML 2.0 プロトコルを使用します。LDAP ユーザを認証するために、Unity Connection は認証要求をアイデンティティ プロバイダーに委任します。Unity Connection によって生成されるこの認証要求が SAML 要求になります。

アイデンティティ プロバイダーは、認証して SAML アサーションを返します。SAML アサーションは、はい（認証済み）または、いいえ（認証に失敗）を表示します。

シングル SAML SSO メカニズム：

SAML 2.0 プロトコルは、コラボレーション サービス間のシングル サインオン アクセスを可能にし、コラボレーション サービスとカスタマーのアイデンティティ プロバイダー間の連携も可能にするビルディング ブロックです。

SSO が Cisco Unity Connection サーバで有効になると、サービス プロバイダーのメタデータとして機能する Cisco Unity Connection によって、**SPMetadata<Unity Connection のホスト名>.xml** という名前の .xml ファイルが生成されます。SAML SP メタデータは、SAML サービス プロバイダー（Unity Connection 上）からエクスポートし、アイデンティティ プロバイダー（ADFS）にインポートする必要があります。

管理者は、SAML メタデータを Cisco Unity Connection Administration からエクスポートし、そのメタデータをアイデンティティ プロバイダー上にインポートする必要があります。管理者は、SAML メタデータをアイデンティティ プロバイダーからエクスポートし、そのメタデータを Cisco Unity Connection Administration 上にインポートする必要もあります。これは、サービス プロバイダー（Unity Connection 上に常駐）と、SAML 認証に不可欠なアイデンティティ プロバイダーとの間の 2 ウェイ ハンドシェイクです。

SAML メタデータには、次の情報が含まれます。

- アイデンティティ プロバイダーおよびサービス プロバイダーの URL 情報。
- アイデンティティ プロバイダーに POST アサーションの場所を指示するサービス プロバイダーの Assertion Consumer Service（ACS）の URL。
- アイデンティティ プロバイダーおよびサービス プロバイダーの証明書情報。

SAML メタデータの交換は、アイデンティティ プロバイダーとサービス プロバイダー間の信頼関係を構築します。アイデンティティ プロバイダーは SAML アサーションを発行し、それにデジタル署名します。サービス プロバイダーは、SAML アサーションを受信すると、アサーションがアイデンティティ プロバイダーによって発行されたことを保証するアイデンティティ プロバイダーの証明書情報を使用して、アサーションを検証します。

4 Unity Connection Web アプリケーションへのシングル サインオン（SSO）アクセスの必要性

Cisco Unity Connection 8.6(2) 以降のリリースでは、OpenAM ベースのシングル サインオンを使用して、ユーザによる Web アプリケーションへのシングル サインオン（SSO）アクセスが可能です。Cisco Unity Connection の シングル サインオン（SSO）アクセスにより、エンド ユーザは Cisco Unity Connection Administration に 1 回ログインするだけで、次の Cisco Unity Connection アプリケーションに再度ログインすることなくアクセスできます。

- Cisco Unity Connection Serviceability
- Cisco Unified Serviceability
- Cisco Personal Communications Assistant
- Web Inbox

Unity connection 8.6(2) よりも前のリリースのシングル サインオン アクセス（SSO）では、OpenAM と Active Directory を同時に使用して Web アプリケーションにシングル サインオン アクセスしていました。

SSO の詳細については、セキュリティ ガイドの「Cisco Unity Connection のシングルサインオン」の章を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/security/guide/10xcucsec061.html

（注） グラフィカル ユーザ インターフェイス（GUI）のみを使用してシングル サインオン（OpenAM および SAML の両方）を有効にできるようになり、コマンドライン インターフェイス（CLI）で機能を有効にする操作はサポートされなくなりました。

SAML SSO の主な利点は、次の Unified Communication 製品の Web アプリケーション間でシングル サインオン アクセスできることです。

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified IM/Presence

SAML SSO を使用してユーザによってアクセスされる Web アプリケーションの詳細については、以下を参照してください。

*クイック スタート ガイド*の「SAML SSO を使用した Cisco Unity Connection 10.x の Web アプリケーション ページへのアクセス」のセクション

SAML SSO により、LDAP ユーザは、アイデンティティ プロバイダーで認証されるユーザ名とパスワードでログインできます。管理者権限を持つ非 LDAP ユーザは、リカバリ URL を使用して Cisco Unity Connection Administration にログインできます。SSO ログインに失敗すると（アイデンティティ プロバイダーまたは Active Directory が非アクティブの場合など）リカバリ URL がユーザ名とパスワードによる管理およびサービスアビリティ Web アプリケーションへの代替アクセスを提供します。

5 Unity Connection 10.0(1) 以降で SAML SSO を有効にするための要件

Cisco Unity Connection 10.x で SAML SSO 機能を設定するには、次の要件を満たしている必要があります。

- Cisco Unity Connection 10.0(1) 以降のリリースがクラスタ内の両方のサーバ上にある。
- Windows 2008 SP2 プラットフォームでアイデンティティ プロバイダーをインストールする。アイデンティティ プロバイダーは Unity Connection サーバと同じドメインに設定する必要があります。
- Unity Connection およびアイデンティティ プロバイダー（SAML SSO 用に選択）の時計が相互に同期されている。
- SSO モードを Cisco Unity Connection Administration から有効にする場合は、Unity Connection の管理者権限を持つ少なくとも 1 人の LDAP ユーザが SAML SSO の **SSO テストを実行する**必要があります。
- Unity Connection 管理および サービスアビリティ Web アプリケーションにアクセスできるように、システム管理者ロールをユーザ アカウントに割り当てる。

上記の要件が満たされると、Cisco Unity Connection サーバで SAML SSO 機能が設定されます。これについては、次のサブ セクションで説明します。

6 Cisco Unity Connection 10.x での SAML SSO 機能の設定

SAML SSO 機能をサポートするには、Cisco Unity Connection およびアイデンティティ プロバイダーを適切に設定する必要があります。このセクションでは、Unity Connection サーバでの SAML SSO の設定手順について説明します。

Unity Connection サーバ で SAML SSO 機能を設定するには、次の手順を実行する必要があります。

手順 1：Unity Connection サーバで SAML SSO を有効にするには、Cisco Unity Connection インターフェイスにログインします。

[システム設定] > [SAML シングルサインオン] に移動し、[SAML SSO の有効化] オプションを選択します。

SAML SSO オプションを選択すると、ウィザードが開きます。[すべての Web サーバ接続がリスタートされます] が表示されたら、[続行] を選択します。

（注） SAML SSO を Cisco Unity Connection から有効にする場合は、Unity Connection の管理者権限を持つ LDAP ユーザが少なくとも 1 人必要です。

手順 2：IdP メタデータ インポートを初期化するには、[IdP メタデータ信頼ファイルのインポート] を選択して、ウィザードの次のステップに移動します。次に、[参照] オプションを選択して、IdP メタデータをシステムからアップロードします。次に、[IdP メタデータのインポート] オプションを選択します。

メタデータのインポートが成功すると、[すべてのサーバでインポートが成功しました] のメッセージが表示されます。次に、[次へ] を選択してウィザードを続行します。

手順 3：SAML メタデータ交換で、[信頼メタデータファイルセットのダウンロード] オプションを選択します。

注意 信頼メタデータがインポートされなかった場合は、[このテストを実行する前に、IdP にサーバメタデータファイルをインストールする必要があります。] の警告メッセージが画面に表示されます。

次に [次へ] を選択します。**有効な管理者 ID** のウィンドウが表示され、管理者権限を持つ LDAP ユーザが自動的にウィンドウに入力されます。管理者権限を持つ LDAP ユーザが上記のウィンドウに自動的に入力されたことを確認したら、[SSO テストを実行 ...] を選択してテストを実行します。

手順 4：ウィザードが続行され、IdP へのユーザ ログインのウィンドウが表示されます。前のウィンドウに自動的に入力された、**管理者ロールを持つ LDAP ユーザの資格**を入力します。これにより、**SAML SSO 機能**が完全に有効になります。[終了] を選択して、設定ウィザードを終了します。

リカバリ URL を使用した Web アプリケーションへの SAML SSO アクセスの方法はもう 1 つあります。リカバリ URL は /ssosp/login を指します。管理者権限を持つ非 LDAP ユーザが製品ランディング ページでリカバリ URL のオプションを選択する場合、実際は /ssosp/login URL を選択しています。この URL は、要求を SSO サービス プロバイダー（SSOSP）に送信します。リカバリ URL オプションが無効の場合は、/ssosp/login URL をインターセプトするために ssosp で組み込まれた新しいフィルタが、要求をアイデンティティ プロバイダーにリダイレクトしますが、リカバリ URL オプションが有効の場合は、作成された新しいフィルタが要求を /cuadmin/recoveryurl.do にリダイレクトします。

（注） Unity Connection で SAML SSO の有効 / 無効を切り替えると、Web アプリケーションが適切に初期化されるまで約 2 ～ 3 分待機する必要があります。次に、Cisco Unity Connection Serviceability ページから（または CLI コマンドの **utils service restart Cisco Tomcat** を使用して）Tomcat サービスを再起動する必要があります。

7 SAML SSO を使用した Cisco Unity Connection 10.x の Web アプリケーション ページへのアクセス

SAML SSO により、LDAP ユーザは、アイデンティティ プロバイダーで認証されるユーザ名とパスワードを使用して、クライアント アプリケーションにログインできます。SAML SSO 機能を有効にすると、Unified Communication 製品でサポートされている Web アプリケーションのユーザー ログインで、Unity Connection の次の Web アプリケーション（Cisco Unified Communications Manager および Cisco Unified CM IM/Presence を除く）にもアクセスできます。

Unity Connection ユーザ	Web アプリケーション
管理者権限を持つ LDAP ユーザ	• Unity Unity Connection Administration • Cisco Unity Connection Serviceability • Cisco Unified Serviceability • Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox（デスクトップ バージョン）
管理者権限を持たない LDAP ユーザ	• Cisco Personal Communications Assistant • Web Inbox • Mini Web Inbox（デスクトップ バージョン）

（注） Web Inbox および Mini Web Inbox にアクセスするには、メールボックスを持つユーザが必要です。また、[Unity Connection Administration] > [サービス クラス] > [ライセンス済み機能] に移動し、[Web Inbox、Messaging Inbox および RSS フィードの使用をユーザに許可する] 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。

管理者ロールを持つ非 LDAP ユーザは、リカバリ URL を使用して Cisco Unity Connection Administration にログインできます。**リカバリ URL** オプションは、Unity Connection 製品導入の選択ウィンドウの **Cisco Unity Connection** オプションの直下にあります。SSO ログインに失敗すると（アイデンティティ プロバイダーまたは Active Directory が非アクティブの場合）リカバリ URL がユーザ名とパスワードによる管理およびサービスアビリティ Web アプリケーションへの代替アクセスを提供します。

8 Cisco Unity Connection の SAML SSO コマンド

SAML SSO 機能では、前述の 3 つのコマンドに加えて、次のコマンドが導入されています。

- utils sso enable
- utils sso disable
- utils sso status
- utils sso recovery-url enable
- utils sso recovery-url disable
- set samltrace level < トレース レベル >
- show samltrace level

- **utils sso enable**

このコマンドを実行すると、管理者はグラフィカル ユーザ インターフェイス（GUI）からのみ SSO 機能を有効にできる旨の情報テキスト メッセージが返されます。OpenAM SSO および SAML SSO を CLI インターフェイスから有効にすることはできません。

- **utils sso disable**

このコマンドは、（OpenAM ベースおよび SAML ベースの）SSO モードを無効にします。クラスタ内では、両方のノードでコマンドを実行する必要があります。グラフィカル ユーザ インターフェイス（GUI）から SSO を無効にすることもできます。この場合は、特定の SSO モードで [無効] オプションを選択します。

（注） Unity Connection のグラフィカル ユーザ インターフェイス（GUI）から SSO を無効にすると、クラスタの場合に両方のノードで SSO モードが無効になります。

- **utils sso status**

このコマンドは、各ノードの SSO ステータス（有効または無効）を表示します。このコマンドは、各ノードで個別に実行されます。

- **utils sso recovery-url enable**

このコマンドは、リカバリ URL SSO モードを有効にします。また、この URL が正常に機能していることを検証します。クラスタ内では、両方のノードでコマンドを実行する必要があります。

- **utils sso recovery-url disable**

このコマンドは、対象の接続ノードでリカバリ URL SSO モードを無効にします。

- **set samltrace level <トレース レベル>**

このコマンドは、指定されたトレースで次の情報を特定できます。

  - エラー
  - 警告
  - デバッグ
  - 重大
  - 情報

- **show samltrace level**

このコマンドは、SAML SSO で選択したログを表示します。

9 Cisco Unity Connection の SAML SSO のトラブルシューティング

SAML SSO では、次の Unified Communication 製品で ユーザによる Web アプリケーションへのシングル サインオン アクセスが可能です。

- Cisco Unified Communications Manager
- Cisco Unity Connection
- Cisco Unified IM/Presence

SAML SSO では、Web ブラウザがアクティブになるまで、ユーザが Web アプリケーションにシングル サインオン アクセスできます。

SAML SSO モードを有効にしている間は、すべての要件とチェックリストを満たしていることを確認してください。SAML SSO の要件およびチェックリストの詳細については、*クイック スタート ガイド*の「**Unity Connection 10.0(1) 以降で SAML SSO を有効にするための要件**」のセクションを参照してください。

（注） SAML SSO を有効にするには、Cisco Unity Connection でドメイン ネーム サーバ（DNS）を設定する必要があります。SAML SSO は、完全修飾ドメイン名（FQDN）がないと機能しません。

Unity Connection の SAML SSO の問題をトラブルシューティングするためのタスク リスト

Unity Connection の SAML SSO が正常に動作しない場合は、次の方法を実行して問題を解決してください。

- **エラー 1）IdP へのリダイレクトが失敗する**
- **エラー 2）IdP 認証に失敗する**
- **エラー 3）Unity Connection へのリダイレクトに失敗する**
- **エラー 4）パブリッシャ サーバとサブスクライバ サーバの SAML ステータスが一致していない**

エラー 1）IdP へのリダイレクトが失敗する

エンド ユーザが Unity Connection サポートの Web ブラウザを使用して、SAML 対応の Web アプリケーションにログインしようとした場合に、設定したアイデンティティ プロバイダー（IdP）にリダイレクトされず、認証の詳細情報を入力できません。

解決方法

次の条件が満たされていることを確認してください。

- アイデンティティ プロバイダー（IdP）が稼働している。
- 正しい IdP メタデータ ファイル（idp.xml）が Cisco Unity Connection にアップロードされている。
- Unity Connection および IdP が同じ時間のサイクル（およびタイムゾーン）で同期されているかどうかを確認する。

エラー 2）IdP 認証に失敗する

エンド ユーザが IdP によって認証されていません。

解決方法

次の条件が満たされていることを確認してください。

- LDAP ディレクトリが IdP にマップされている。
- ユーザーが LDAP ディレクトリに追加されている、問題が解決しない場合は、Unity Connection およびアイデンティティ プロバイダーに関連付けられている NTP サーバを確認してください。これらのサーバに関連付けられている NTP サーバの時刻は同期されている必要があります。
- LDAP アカウントがアクティブになっている。
- 正しい ユーザ ID とパスワードになっている。

エラー 3）Unity Connection へのリダイレクトに失敗する

IdP によって認証された後でも、ユーザが SAML SSO 対応の Web アプリケーションにリダイレクトされません。

解決方法

- Unity Connection および IdP の時計が同期されている。時計の同期については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection*』の「NTP 設定」のセクションを参照してください。
- 必須属性 UID が IdP に設定されている。
- 正しい Unity Connection サーバ メタデータ ファイルが IdP にアップロードされている。
- 必要な権限がユーザにある。

エラー 4）パブリッシャ サーバとサブスクライバ サーバの SAML ステータスが一致していない

Unity Connection のパブリッシャ サーバとサブスクライバ サーバの SAML ステータスが一致していません。

解決方法

- IdP メタデータ がサブスクライバ サーバで正しいかどうかを確認します。正しくない場合は、[SAML シングルサインオン] Web ページから [メタデータの再インポート] オプションを選択します。
- 問題が解決しない場合は、[すべての無効なサーバの修正] オプションを選択します。

（注） Unity Connection クラスタの場合は、パブリッシャ サーバのメタデータの再インポートのオプションはありません。

SAML SSO アクセスの問題の診断トレース

これとは別のすべての SAML SSO 関連の問題については、次のコマンドを使用して SSO ログを有効にします。

admin: **set samltrace level < トレース レベル >**

定義されるトレースは、デバッグ、情報、警告、エラー、重大です。

トレースは、Unity Connection の次の場所から収集されます。

/var/log/active/tomcat/logs/ssosp

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/