## SAML の基本

## 導入

Coupa は、Coupa と ID 管理ソリューション間の SSO (シングル サインオン) サポートに SAML 2.0 (セキュリティ アサーション マークアップ言語) の使用をサポートしています。これにより、ユーザーは Coupa へのリンクをクリックし、SSO に既にログインしている場合は自動的にサインインできます。

COUPA サービスで SAML が有効になると、一部のユーザーが SAML をバイパスして、Coupa 認証情報を使用してログインできるようになります。これは、SAML サーバーがオフラインで、管理者が SAML を無効にするために Coupa へのアクセスを必要としている場合の安全策です。

## 利点

SAML を使用して Coupa インスタンスを統合すると、次のようないくつかの利点があります。

* ユーザーは、Coupa の新しいパスワードを覚えておく必要はありません。
* Coupaはパスワード情報を保存または維持しないため、監査/リスクの問題を軽減します。
* イントラネットおよび企業標準を通じてアカウント制御を一元化
* SAML は SSO の業界で受け入れられている標準です。

## ユーザー エクスペリエンス

1. ユーザーが Coupa インスタンスの Web ページにアクセスした場合。
2. Coupa は、認証のためにユーザーを SSO サイトにリダイレクトします。
3. SSO サイトは、ユーザーのブラウザーに対して、クーパが提供する URL に SAML 応答を投稿するように指示する Web ページを返します。
4. クーパは応答を検証します。成功すると、セッションがタイムアウトするまで、新しく認証されたユーザーは SSO サイトで再認証する必要はありません。セッション タイムアウトは管理者が設定できます。

## クーパ SAML SSO のセットアップ

## メソッド

1. [初期段階の SP メタデータ](https://s3.amazonaws.com/sso-metadata-us-east/metadata_stg.xml)([本番 SP メタデータ xml](https://s3.amazonaws.com/sso-metadata-us-east/metadata_prd.xml)) ファイルをステージ IdP サーバにインポートします。
   * IdP がメタデータ交換をサポートしていない場合は、xml ファイルを開いて情報を抽出してください。
   * クーパの推奨セットアップは SP-Init-SSO です。クーパは IdP-Init-SSO をセットアップすることもできますが、IdP-Init-SSO では、SAML 要求と共に**リレーステート**パラメータを送信する必要があります。これを行う 1 つの方法は、xml .接続を作成する前に xml を変更できます。/sp/ACS.saml2?RelayState=https://<coupa-instance-domain-name>/sessions/saml\_post
   * IdP で接続のセットアップを完了します。
2. 以下の情報を Coupa に送信します。
   * メタデータ: IdP からメタデータ xml をエクスポートします。
     + IdP がメタデータ交換をサポートしていない場合は、SAML 応答でデジタル署名を検証するために、エンティティ ID (別名接続 ID) と X509 証明書を指定してください。
   * ログイン URL: ユーザーの IdP ログイン ページ。IdP が SSO を開始する場合に必要です。詳細については、FAQ を参照してください。
   * ログアウト URL: Coupa アプリケーションからのユーザーログアウトとそのセッションがクリアされると、ページ Coupa が表示されます。これは、内部ページ、ホーム ページ、または顧客がホストする任意のランディング ページです。
   * テストユーザー: IdP でテストユーザーを作成し、接続をテストします。
3. Coupa は、IdP メタデータをインポートし、SP から IdP への接続を完了し、お客様に通知します。
4. 割り当てられた Coupa 管理者が、ユーザーが SAML を使用できるようにします。
   * SAML 認証を有効にするユーザー設定を変更する
   * 「シングルサインオンID」を設定し、これは、クーパにSAML要求で渡されたNameIDと同じである、NameIDがプロビジョニングされる方法については、システム管理者に確認してください。

## クーパで SSO を有効にする

1. 行きます。https://<your\_site>.coupahost.com/administration/security
2. **[SAML**を**使用してログイン**する] チェックボックスをオンにします。
3. 次の形式で "**ログイン ページ URL"**を指定します。
   * SP 開始ログインの場合:
     + テスト/ステージングの場合: https://sso-stg1.coupahost.com/sp/startSSO.ping?PartnerIdpId= <stage\_IdP\_entityid>&TARGET=https://<your-test\_site>.coupahost.com/sessions/saml\_post
     + 生産の場合: https://sso-prd1.coupahost.com/sp/startSSO.ping?PartnerIdpId= <prod\_IdP\_entityid>&TARGET=https://<your\_site>.coupahost.com/sessions/saml\_post
   * IdP 開始ログインの場合:
     + IdP ログイン URL を使用する
4. Coupa からログアウトするときにユーザーをリダイレクトする場合は、**ログアウト ページ URL を**指定します。
5. タイムアウト**URL**を指定します。**ログイン ページ**の URL と同じである必要があります。
6. 証明書はレガシ機能です。追加機能は提供されず、今後のリリースでは削除される予定です。ただし、まだ必要です。このダミー証明書[サーバー.crt](https://success.coupa.com/@api/deki/files/7860/server.crt?revision=1)を使用してください。ドロップダウンから証明書の種類として**DER**を選択します。アプリケーションは解析エラーを発生させますが、実際には証明書をアップロードします。証明書は、ドロップダウンでアクセスできるようになります。

## クーパ SAML に関するよくある質問

##### クーパでSAMLを設定するには?

構成を開始するには、この FAQ を読み、[構成セットアップ](https://success.coupa.com/Integrate/Technical_Documentation/SSO/02_Coupa_SSO_Setup)の手順 1 を完了してください。手順 2 に記載されている Coupa の実装担当者の要件を指定します。Coupaエンジニアは、クーパの終わりにIdP接続をセットアップするのに役立ちますが、セットアップは完全にセルフサービスではありません。Coupa 内の管理者は、SAML を無効にする自由を持っています, 変更ログイン URL, ログアウト URL とタイムアウト URL.

##### クーパはどの SAML プロトコルをサポートしていますか?

SAML V2.0

##### SAML V2.0 仕様はどこにありますか?

<http://saml.xml.org/saml-specifications>

##### SAML 応答 xml を検証する方法

XML を確認してください。 http://docs.oasis-open.org/security/saml/v2.0/saml-schema-protocol-2.0.xsd

    $ xmllint --noout --schema saml-schema-protocol-2.0.xsd saml\_response.xml

##### SAML 応答をデコードする方法は?

1 つのオンライン デコーダ[は次の](https://rnd.feide.no/simplesaml/module.php/saml2debug/debug.php)https://rnd.feide.no/simplesaml/modu...ebug/debug.php

##### SAML 応答を追跡および表示する方法

Firefox アドオン saml-tracer は HTTPS フローを追跡し、SAML 応答をデコードして解析します https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/

##### ログイン URL とは何ですか?

**[設定] > [セキュリティ制御**] の下のログイン URL は、単に HTTP 302 リダイレクトです。

IdP 開始 SSO の場合は、IdP ログイン画面のログイン URL を入力します。Coupa アプリケーションは、ユーザーを IdP ホストログイン ページにリダイレクトしてユーザーを認証します。ユーザーには、Coupa サインイン ページは表示されません。

SP で開始された SSO の場合、IdP でエンティティ ID がわかっている場合は、URL を構築できます。をクリックして、SPの開始を開始します。

###### *テスト/ステージング用*

https://sso-stg1.coupahost.com/sp/startSSO.ping?PartnerIdpId= <stage\_IdP\_entityid>&TARGET=https://{your-test\_site}.coupahost.com/sessions/saml\_post

###### *生産用*

https://sso-prd1.coupahost.com/sp/startSSO.ping?PartnerIdpId= <prod\_IdP\_entityid>&TARGET=https://{your\_site}.coupahost.com/sessions/saml\_post

##### Coupa にログアウト URL が必要な理由

Coupa アプリケーションからユーザーがログアウトすると、ユーザー セッションがクリアされ、[セットアップ] - > [セキュリティ制御] で構成されたログアウト URL にリダイレクトされます。SLO 実装ではなく、単純なリダイレクト。ユーザーが IdP からサインアウトする必要はありません。ログアウト URL は、Coupa アプリケーションを使用して完了すると、ユーザーの内部サイトまたは任意のランディング ページにすることができます。

##### タイムアウト URL とは何か、タイムアウトは SAML 実装でどのように機能しますか?

Coupa アプリケーションのセッション有効期限タイムアウトは、システム->セキュリティ制御の下に設定されています。セッションタイムアウト後、Coupa はタイムアウト URL にリダイレクトされます (ログイン URL と同じ) は、URL に基づいて IdP 開始または SP 開始 SSO を開始します。ほとんどの場合、タイムアウト URL はログイン URL と同じです。ユーザーには、ユーザーの「Coupa セッションの有効期限」および「IdP タイムアウト」に基づいてログインページが表示されます。

##### Coupa は IdP ユーザーを識別するためにどのような情報を使用しますか。

Coupa は、SAML 応答の NameID 値を使用して、対応する Coupa ユーザーを検索します。SAML ログインを成功させるには、ユーザーの作成時に「シングルサインオン ID」を指定する必要があります。シングル サインオン ID は、ユーザー インターフェイスでユーザーを編集するか、Coupa API を使用してユーザー統合を行うことによって構成できます。

##### クーパにアクセスしてSAMLをバイパスする方法はありますか?

Coupa は、SSO 認証プロセスをバイパスするこのサポート インターフェイスを提供します。URL は**です。**これは、通常のユーザーが作成されたときに Coupa のパスワードが設定されていない可能性があるため、管理者を対象としています。これにより、SSO 以外のログインができなくなります。必要に応じて、このサポート インターフェイスを介してログインする Coupa パスワードを持つユーザーを作成できます。これは、IdP の一部ではないが、まだ Coupa にアクセスする必要があるユーザーに便利です。https://{your-site}.coupahost.com/sessions/support\_login

##### クーパはいつ必要とリレーステートを必要としますか?

リレーステートは、IdP 開始 SSO に対して必須であり、SP で開始された SSO には必要ありません。RelayState は、顧客の Coupa インスタンスを識別するためにサービス プロバイダーが必要です。リレーステートは、SAML レスポンスに沿ってクエリ文字列または別の POST 変数として渡すことができます。リレーステート=https://<クーパインスタンスドメイン名>/セッション/saml\_post。簡単な方法の 1 つは、ステージまたは実稼働メタデータ xml で見つけたアサーション コンシューマー サービス URL にクエリ文字列として RelayState**を追加することです。**

##### IdP 開始 SSO および SP 開始 SSO の作業フローは何ですか。

<http://documentation.pingidentity.com/display/PF/IdP-Initiated+SSO--POST>

<http://documentation.pingidentity.com/display/PF/SP-Initiated+SSO--POST-POST>

##### ステージおよびプロダクションクーパインスタンスの SAML の設定方法

クーパ ステージのアサーション エンド ポイント URL (アサーション コンシューマー サービス) は、およびクーパの生産に対してです。SAML をステージとプロダクションの両方で動作させるためには、ステージ用とプロダクション用の 2 つの接続が必要です。ステージを持たない場合、生産 IdP しかない場合でも、クーパステージとクーパプロダクションインスタンスに対して 2 つの異なる接続を作成できます。リレーステートは、ステージとプロダクションの接続で異なります。https://sso-stg1.coupahost.com/sp/ACS.saml2https://sso-prd1.coupahost.com/sp/ACS.saml2

##### SAML を使用してユーザープロビジョニングを行うことはできますか?

現在の Coupa SAML の設定は、認証のみを目的とし、Coupa 内のユーザープロビジョニングではありません。承認は、Coupa ユーザー ロールを介して行われます。SAML ロールは、ユーザーを認証します。

##### クーパと統合されたIdPシステムは何ですか?

SAML 2.0 を実装する IdP システム。ADFS 2.0, PingFederate, ノベルアクセスマネージャー, オラクルアクセスマネージャ, チボリアクセスマネージャ, シボレスのようなオープンソースプロジェクト, カスタム構築ソリューション, など.現在、IdP サンプル コードは提供していませんが、オンラインおよびオープンソース プロジェクトから入手できます。

##### お客様がCoupaに提供するサンプルIdPメタデータをお探しです。

添付の[Test\_IDP\_Metadata.xml](https://success.coupa.com/@api/deki/files/2754/Test_IDP_Metadata.xml?revision=1)を参照してください。

##### 認証リクエストと SAML 応答のサンプルを探しています。

添付の[sample\_AuthnRequest\_and\_SAML\_response.xml](https://success.coupa.com/@api/deki/files/2755/sample_AuthnRequest_and_SAML_response.xml?revision=1)を参照してください。

##### "無効な応答属性 (Hg3Av.............FG) - 未承諾の応答には、応答不可のエラーを含めることはできません。

このようなエラーの 3 つの理由:

1. IdP 側からの SAML 応答が同じ認証トークンを使用して、SAML を再生しています
2. 同じログインページから SAML POST を複製します (たとえば、同じ SAML レスポンスを持つ 2 つの POST)。
3. ACS URL でリレーステートを使用して IdP 側に PingFederate を設定し、クーパで SP 開始を使用します。

1 と 2 は、Firefox とsaml\_tracerプラグインまたは任意の HTTP トラッキング ツールを使用して検出できます。3 は、PingFederate を使用して IdP 側の有効です、 彼らはクーパとの SP-Init セットアップのリレーステートを設定しないでください。

##### SSO 関連の問題をトラブルシューティングするための SAML トレースの収集

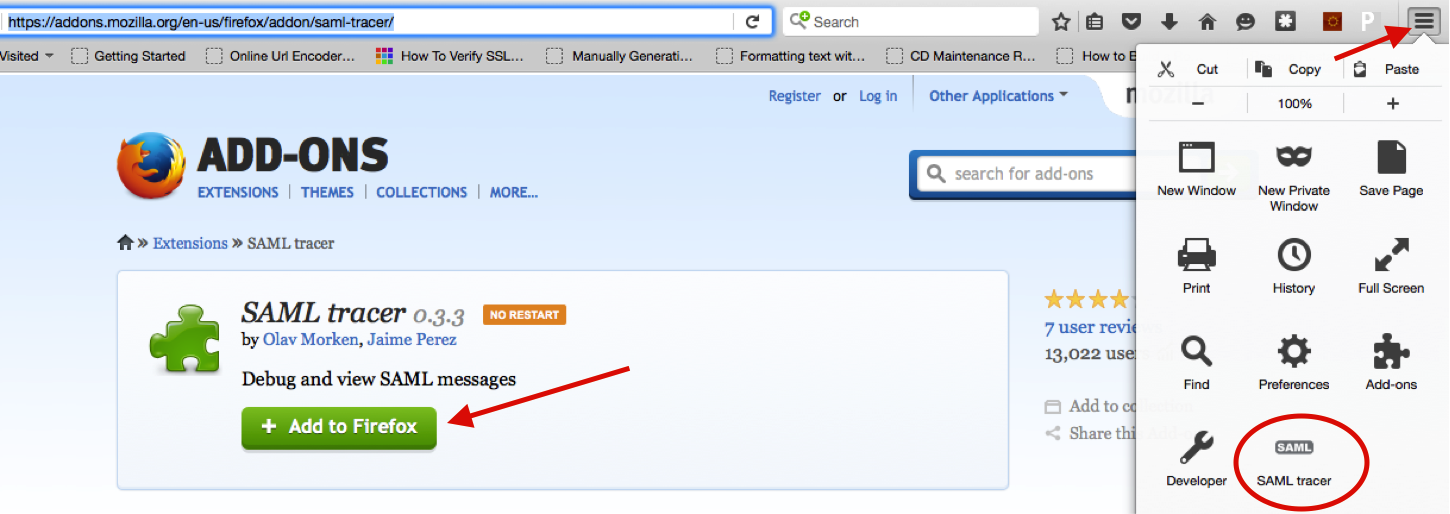
サポートの観点から、SAML / SSO 認証の失敗に関連するデータを収集する必要がある場合があります。

これには、ブラウザベースのツールが 2 つ用意されています。

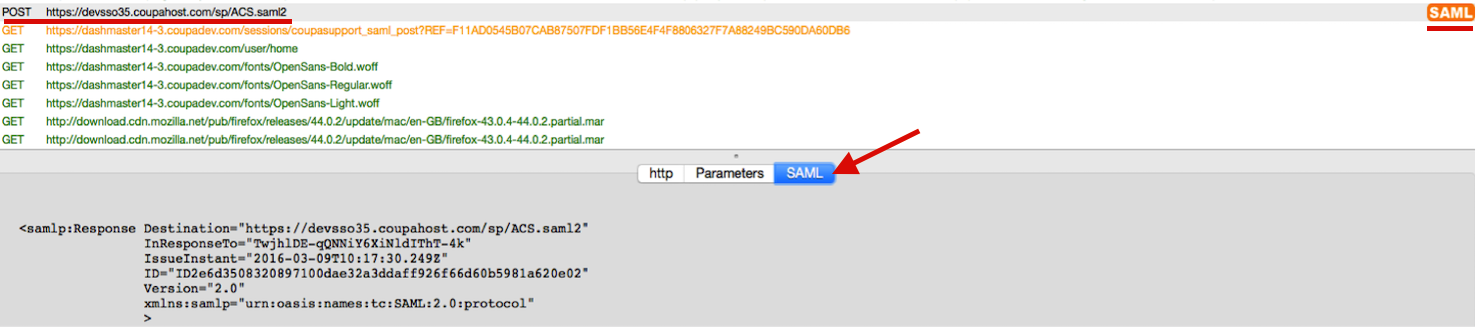
###### *Firefox*

SAML トレーサー: <https://addons.mozilla.org/en-us/firefox/addon/saml-tracer/>

インストールすると、次のスクリーンショットのように表示され、SSO接続を行っている間に開く必要があります。



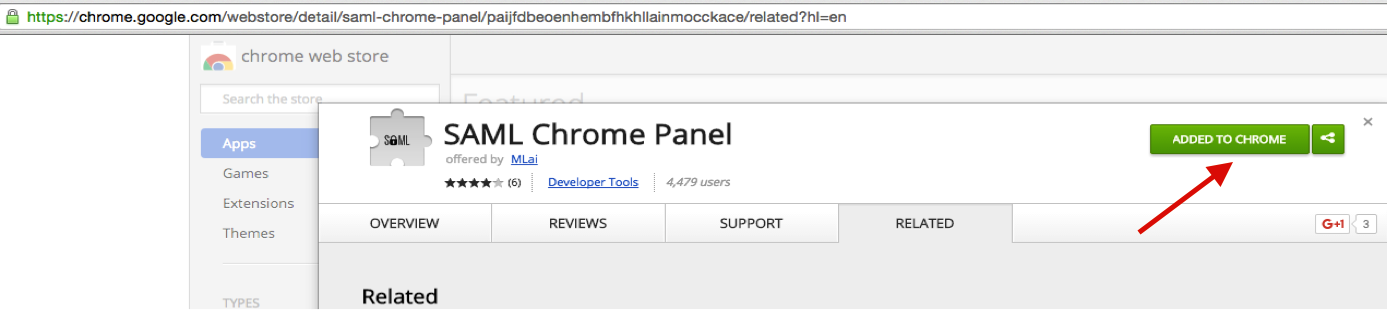
収集する必要があるデータは、SAML タブの下に POST\* として見つかります。

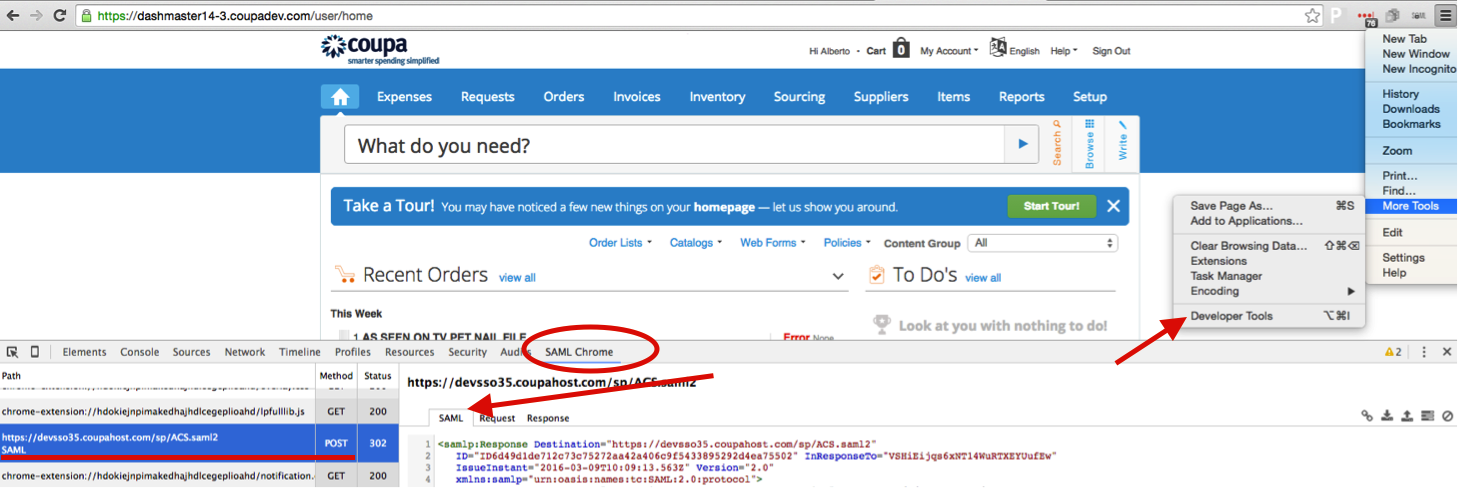


###### *クロム*

SAML トレーサー: <https://chrome.google.com/webstore/detail/saml-chrome-panel/paijfdbeoenhembfhkhllainmocckace?hl=en>

これをインストールすると Chrome の開発者ツールにタブが追加され、POST\* が表示され、[SAML] タブを確認する必要があります。





\*POSTコールは、サンドックス  
とプロダクションインスタンスの開発環境  
に対して行われます。https://devsso35.coupahost.comhttps://prdsso40.coupahost.com

## LDAP を使用したアクティブ ディレクトリ

## 導入

クーパは、認証に外部 LDAP またはマイクロソフトの ActiveDirectory サーバーの使用をサポートしています。これにより、ユーザーは、イントラネット アプリケーションへのアクセスを許可するのと同じ資格情報を使用して Coupa にサインインできます。

Coupa は、一度に 1 つの LDAP と統合できます。複数の LDAP を使用するお客様は、複数の LDAP の上に仮想/プロキシレイヤーを作成する必要があります。

### 利点

Coupa インスタンスをディレクトリサーバーと統合すると、次のような利点があります。

* ユーザーは、Coupa の新しいパスワードを覚えておく必要はありません。
* パスワードの変更が、すぐにクーパに反映される
* ディレクトリ サーバーで定義されているパスワード ポリシーを適用する
* ディレクトリ サーバーを使用してアカウント制御を集中化する

## 実装の詳細

1. 指定された特権のないアカウントとしてディレクトリ サーバーにログインします。
2. サインインしようとしているユーザーの検索を実行します。
   1. Coupa は、ユーザーが提供する資格情報と一致します。sAMAccountName
   2. クーパは次の試合に一致します。 objectClassorganizationalPerson
3. Coupa は、見つかったユーザーの識別名とユーザーによって提供されたパスワードを使用して、ディレクトリ サーバーにバインドします。
4. 手順 3 が成功した場合は、ユーザーを Coupa に入れましょう。

### 必要な情報

| 情報 | 詳細 | 提供する人 |
| --- | --- | --- |
| クーパ サーバー IP アドレス | 顧客が接続する特定の Coupa IP。IP アドレスを使用して、ファイアウォールの規則を可能な限り制限します。 | カット |
| ホスト | 接続先のサーバー IP とホスト名 | 顧客 |
| ポート | 接続先のポート。Coupa は、ポート 636 を介して一般的に LDAPS 接続を使用します。LDAPS が正しく機能するには、TLS 証明書が必要です。 | 顧客 |
| ベース | LDAP を検索するための基本 DN | 顧客 |
| ドメイン | アクティブ ディレクトリ ドメイン | 顧客 |
| 名 | ログインするユーザーのユーザー名は、このユーザーはバインドして検索する以外に権限を持つべきではありません | 顧客 |
| パスワード | 上記のユーザーのパスワード | 顧客 |

## 制限

私たちの経験は、あなたの組織にとって懸念されるかもしれないし、ないかもしれないいくつかの制限を発見しました:

* ファイアウォールで保護されたイントラネット内に Coupa Server が存在する場合、ディレクトリ サーバーに接続できるようにするために、ファイアウォール規則を作成する必要がある場合があります。
* 認証を実行するには、Coupa Server がディレクトリ サーバーにバインドするために、特権のないアカウントを作成する必要があります。
* 資格情報はイントラネットの外部に送信されます (ただし、Coupa とのネットワーク通信はすべて、高レベルの  
  SSL 暗号化で保護されています)

Coupa R23 から LDAP サーバー接続の証明書検証を実施します。つまり、LDAP 経由で接続する IP アドレスをユーザーにすることはできませんが、有効な FQDN (myldapserver.mydomain.com) を使用する必要があります。

これは、接続先のコンピュータ上に存在する証明書がサーバーの名前と一致する必要があることを意味します。

社内の IT に関する問題を検証し、質問がサポート チケットを開いた場合は、実稼働インスタンスを R23 にアップグレードしてください。

また、シングル サインオン (SSO) の FAQ 記事もお願いします。