Identity 実装ガイド

バージョン 38.0, Winter '17

@salesforcedocs

最終更新日: 2016/08/21

本書の英語版と翻訳版で相違がある場合は英語版を優先するものとします。

目次

第 1 章　Salesforce Identity とは?

Salesforce Identity は、Salesforce 組織のユーザを外部のアプリケーションやサービスと接続するとともに、ユーザアプリケーションおよび認証の監視、管理、およびレポートを行うための管理ツールを提供します。

Salesforce Identity は、次の機能を備えた Identity and Access Management (IAM) サービスです。

- クラウドベースのユーザディレクトリ。ユーザのアカウントと情報は 1 か所で保存、管理され、他のサービスやアプリケーションからも使用できます。
- ユーザを確認し、ユーザアクセス権に対する詳細な制御を維持するための認証サービス。各ユーザが使用できるアプリケーションの選択、2 要素認証の要求、個々のユーザがセッションを維持するために必要なログイン頻度の設定ができます。
- UI インテグレーションを含む、サードパーティアプリケーションのアクセス管理と認証。ユーザはアプリケーションとサービスを必要に応じていつでも使用できます。
- アプリケーションのプロビジョニングとプロビジョニング解除。ユーザが常に最新のアプリケーションを利用できるようにし、使用してはならないアプリケーションを削除します。
- Identity 機能のリリースを表示および管理するための API。
- Identity ユーザによるアプリケーションおよびサービスの利用状況のレポート。セキュリティを強化します。
- Salesforce Identity Connect。プロビジョニングおよび Microsoft Active Directory などのディレクトリサービスとのシングルサインオンインテグレーションのためのオンプレミス型コネクタです。

エディション

使用可能なエディション: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

Salesforce Identity を実装するには、次のいずれかを使用します。

Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) は、XML ベースの標準です。これを使用してサービス間で認証のやりとりを行うことができます。これは、さまざまな Web シングルサインオンソリューションをベースにしています。Salesforce は、企業ポータルまたは ID プロバイダから Salesforce へのシングルサインオンを行うために SAML をサポートします。

OAuth

OAuth は、アプリケーション間のセキュアな認証を可能にするオープンプロトコルで、シングルサインオンに使用します。OAuth 「フロー」には、Salesforce 組織に OAuth を実装するためのさまざまな方法を記述します。具体的なフローについての詳細は、*『Force.com REST API 開発者ガイド』* を参照してください。

OpenID Connect

Open ID Connect は、OAuth 2.0 に基づいた、サービス間の ID 検証用の認証プロトコルです。OpenID Connect を使用すると、Salesforce 組織は、Google などの別のサービスで実行された認証に基づいてユーザの ID を検証できます。

私のドメイン
: Salesforce 組織のカスタムドメイン名 (たとえば、*https://companyname.my.salesforce.com* など) を定義するには、[私のドメイン] を使用します。カスタムドメイン名によって、組織のログインと認証の管理が改善され、ログインページをカスタマイズできます。

接続アプリケーション
: 接続アプリケーションは、API を使用して、アプリケーションを Salesforce と統合します。接続アプリケーションでは、標準の SAML および OAuth プロトコルを使用して認証して、シングルサインオンを提供し、Salesforce API を使用してトークンを提供します。標準の OAuth 機能に加え、接続アプリケーションでは、システム管理者はさまざまなセキュリティポリシーを設定したり、対応するアプリケーションを使用できるユーザを明示的に制御したりできます。

アプリケーションランチャー
: アプリケーションランチャーは、Salesforce 組織からシングルサインオンアプリケーションを起動するユーザ操作を一元化します。Salesforce のアプリケーションランチャーでは、接続アプリケーションおよび標準アプリケーションにリンクするロゴがすべて 1 つのタブに表示されます。表示するには、ユーザに「Identity 機能を使用」が有効で [アプリケーションランチャー] が [参照可能] に設定されたプロファイルまたは権限セットが割り当てられている必要があります。その場合、アプリケーションランチャーは Force.com アプリケーションメニューにアプリケーションとして表示されます。

Identity ライセンス
: ユーザにアプリケーションランチャーなどの Identity 機能へのアクセスを許可します。アプリケーションランチャーを表示および使用するには、ユーザに「Identity 機能を使用」権限が必要です。

  Enterprise Edition、**Performance** Edition、および **Unlimited** Edition のすべての有料ユーザライセンスに含まれます。**Developer** Edition を使用する新規の各組織には、10 個の無償の Identity ユーザライセンスが含まれます。

External Identity ライセンス
: 外部ユーザにアプリケーションランチャーやシングルサインオンなどの Identity 機能を許可します。外部ユーザは、一般的に組織外の非従業員やコミュニティユーザであり、システム管理者がアクセスを管理して、組織へのアクセスを制限する必要があるユーザです。

  Enterprise Edition、**Performance** Edition、および **Unlimited** Edition のすべての有料ユーザライセンスに含まれます。**Developer** Edition を使用する新規の各組織には、5 個の無償の Identity ユーザライセンスが含まれます。

ID プロバイダおよびサービスプロバイダインテグレーション
: *ID プロバイダ*は、ユーザがシングルサインオンを使用して他の Web サイトにアクセスできるようにする信頼済みプロバイダです。*サービスプロバイダ*は、アプリケーションをホストする Web サイトです。Salesforce を ID プロバイダとして有効にして、1 つ以上のサービスプロバイダを定義できます。ユーザは、シングルサインオンを使用して Salesforce から他のアプリケーションに直接アクセスできます。シングルサインオンを使用すると、いくつものパスワードを覚える必要がなく、1つだけ覚えておけばよいため、ユーザは非常に助かります。さらに、アプリケーションをタブとして Salesforce 組織に追加できるため、ユーザはプログラムを切り替える必要がなくなります。

Salesforce Identity Connect
: Identity Connect は、Windows または Linux プラットフォームで実行するサービスを介して Active Directory と Salesforce のインテグレーションを実現します。このインテグレーションには、Salesforce にログインするときにシングルサインオン (SSO) Active Directory インテグレーション用の ID サービスプロバイダ (IDP) として機能する Identity Connect または Salesforce との Active Directory ユーザの同期が含まれます。

2 要素認証

2 要素認証を有効化すると、ユーザがログインするとき、ユーザ名とワンタイムパスワード (OTP) など、2 つの情報の入力が要求されます。Salesforce は、ユーザ定義の OTP と、ソフトウェアまたはハードウェアデバイスで生成された OTP をサポートしています。

これは Salesforce 組織内のユーザのアプリケーションランチャーのビューの一例です。このユーザは外部のアプリケーションおよびサービスを別々にログインせずに開けるように設定されたプロファイルまたは権限セットを持っています。

システム管理者の接続アプリケーションページでは、使用可能なアプリケーションごとに、プロファイルおよび権限セットに基づいてユーザを割り当てられます。

利用状況情報について詳細を取得する場合、システム管理者は Identity 利用状況レポートを設定して実行できます。レポートについての詳細は、「アプリケーションの監視とレポートの実行」を参照してください。

第 2 章　Salesforce Identity の使用方法

次の簡単なシナリオでは、会社でいくつかの Salesforce Identity 機能を組み合わせて、さまざまなアプリケーションの使用を管理統括しながら、従業員のユーザエクスペリエンスを向上させる方法を示しています。

Salesforce Identity により、従業員はシングルサインオン (SSO) で複数のアプリケーションにサインインして、作業を行うことができます。これらのアプリケーションは、Salesforce 組織に統合されている場合や、サードパーティの外部アプリケーションである場合があります。

次の例では、Salesforce Identity 機能を使用することで、Universal Containers という会社のニーズを満たす方法を示しています。

例: Universal Containers の従業員は、複数のアプリケーションにサインインして作業を行う必要があります。そこでシングルサインオン (SSO) ソリューションが必要だと判断し、そのために Salesforce を使用することを決定します。Salesforce を SSO プロバイダ (ID プロバイダとも呼ばれる) として設定するために、Universal Containers は Salesforce 組織で [私のドメイン] を使用してカスタムドメインを設定する必要があります。まず従業員がログインするカスタムドメインで独自の認証設定を作成して管理します。

次に、Security Assertion Markup Language (SAML) を使用して、ドメインとその他のプロバイダ間で認証情報を渡します。Universal Containers のカスタムドメインにログインしたユーザは、ログインし直さなくても外部アプリケーションを使用できます。反対に、これらのユーザは承認された外部アプリケーション (この場合は「ID プロバイダ」) を使用しているときに、ログインし直さずに Universal Containers のドメインにアクセスすることもできます。ユーザは、SAML 標準をサポートするアプリケーション (Google Apps など) 間をシングルサインオンアクセスできます。

次に、Universal Containers は、シングルサインオンを有効にすると同時に独自のセキュリティを強化することも決定します。2 要素認証を実装して、ログイン時にユーザに一意のワンタイムコードの入力を求めます。また、Universal Containers はログインページをカスタマイズして、企業ブランドとの整合性を高めたり、ログインするユーザが認証情報を入力する前に状況を把握しやすくしたりします。

Universal Containers は、アプリケーションランチャーを使用して、個々のユーザが使用できるアプリケーションやユーザのログイン回数を制御します。また、アプリケーションランチャーを使用して、モバイルユーザもモバイルブラウザや Chatter ネイティブモバイルアプリケーションを介してシングルサインオンを拡張できます。

ログインおよびユーザ管理については、企業データベースのユーザを Salesforce 組織に追加できるように、Identity Connect を使用して Active Directory を Salesforce と統合します。会社のアカウントを持つユーザは、Active Directory のログイン情報を使用して簡単に Salesforce 組織にログインできます。つまり、ユーザはデスクトップからシングルサインオンを使用することができます。さらに、Active Directory または Salesforce で行われるユーザへの変更は、2 つの環境間で統合されます。

システムが稼働したら、Universal Containers は、レポートおよびダッシュボードを作成して、ユーザのログイン履歴やアプリケーションの利用状況を追跡します。これらのレポートを使用して、システム管理者は認証された利用状況を追跡し、必要に応じて認証を調整できます。

第 3 章 クイックスタート: 自分のドメインの設定、接続アプリケーションの追加、およびアプリケーションランチャーの使用

トピック:

このクイックスタートは、複数の Salesforce Identity 機能を組み合わせることに習熟するためのハンズオンチュートリアルです。

重要: Winter '14 以降の*新しい* Developer Edition (DE) 組織を使用してください。アップグレードされた従来の DE 組織には、このクイックスタートに必要な機能がすべて揃っていない可能性があります。

Identity 機能の使用を開始するのに必要なのは、[私のドメイン] を使用して作成した Salesforce カスタムドメイン、Salesforce 組織から起動する接続アプリケーション、許可された接続アプリケーションの適切なユーザに対して設定されたアプリケーションランチャーのみです。

[私のドメイン] を使用して独自のドメイン名を作成する

Salesforce 組織ドメインをカスタマイズします。

[私のドメイン] の使用方法を学習している間は、本番組織で次の手順を実行しないでください。Developer Edition 組織 (Winter '14 以降) を使用してください。新しいドメイン名をリリースした後、その組織で名前を元に戻すことはできません。

カスタムドメイン名を使用すると、組織でのログインや認証の管理を次のような複数の方法で改善することができます。たとえば、

- 一意のドメイン URL でビジネスアイデンティティを強調する
- ログイン画面のブランド設定および右フレームのコンテンツのカスタマイズを行う
- 新しいドメイン名を使用しないページ要求をブロックまたはリダイレクトする
- 複数の Salesforce 組織で同時に作業する
- カスタムログインポリシーを設定してユーザの認証方法を決定する
- ユーザがログインページで Google や Facebook などのソーシャルアカウントを使用してログインできるようにする
- ユーザが 1 回ログインするだけで外部サービスにアクセスできるようにする

次の手順では、例として会社名「universal containers」を使用します。ただし、[私のドメイン] は各自固有にする必要があるため、この練習問題では、独自の名前を選択して使用する必要があります。

1. [設定] から、[クイック検索] ボックスに「*私のドメイン*」と入力し、[私のドメイン] を選択します。
2. サンプル URL で使用するサブドメイン名を入力します。たとえば、Universal Containers という会社が `universalcontainers` というサブドメインを使用するとします。この会社のログイン URL は、`https://universalcontainers.my.salesforce.com/` となります。名前は 40 字以下で、文字、数字、ハイフンを使用できます。

   次の予約語は、サブドメインには使用できません。

   - www
   - salesforce
   - heroku

   ドメイン名の先頭を次のものにすることはできません。

   - root
   - status
   - ハイフン
3. [使用可能か調べる] をクリックします。名前がすでに使用されている場合、別の名前を選択します。
4. [契約条件] をクリックして契約を確認し、チェックボックスをオンにします。
5. [ドメインの登録] をクリックします。
6. ドメイン名のテストの準備ができると、通知メールが送信されます この処理に最大 3 分かかることがあります。

ドメインをテストします。

1. [設定] から、[クイック検索] ボックスに「私のドメイン」と入力し、[私のドメイン] を選択します。
2. [こちらをクリックしてログインしてください] をクリックします。
3. サブドメインにリダイレクトされたことを確認します。

   UI をクリックしていくと、各ページですべて新しいサブドメインが使用されているのがわかります。

ドメインをリリースします。

1. [設定] から、[クイック検索] ボックスに「私のドメイン」と入力し、[私のドメイン] を選択します。
2. [ユーザにリリース] をクリックします。

これで、[私のドメインの設定] で新しいドメインのログインポリシーを編集したり、ログインページをカスタマイズしたりできるようになりました。

新しい接続アプリケーションを作成する

Salesforce 組織に接続アプリケーションとして表示される Heroku アプリケーションを作成します。

接続アプリケーションは、API を使用して Salesforce と統合します。接続アプリケーションでは、標準の SAML および OAuth プロトコルを使用して認証して、シングルサインオンを提供し、Salesforce API を使用してトークンを提供します。標準の OAuth 機能に加え、接続アプリケーションでは、システム管理者はさまざまなセキュリティポリシーを設定したり、対応するアプリケーションを使用できるユーザを明示的に制御したりできます。

次の手順では、「セキュリティワークブック」で使用するために設計された特殊な Heroku アプリケーションを使用して、組織に設定可能な接続アプリケーションを生成します。

このセクションの内容:

ステップ 1: OAuth アプリケーションを作成する

アプリケーションで OAuth を使用する前に、環境を設定する必要があります。

1. 新しいブラウザタブで、Web サイト https://securityworkbook.herokuapp.com/ にアクセスします。
2. [Get Started with Spring MVC (Spring MVC を始める)] をクリックします。

   「AGI」アプリケーションのアクセスを許可するように要求される場合があります。その場合は、[Allow (許可)] をクリックしてこのチュートリアルを続行します。
3. Heroku ログイン情報を入力します。ログイン情報がない場合は、[Sign Up (サインアップ)] をクリックして Heroku アカウントを作成し、この手順をやり直してください。
4. 新しい Heroku アプリケーションの名前をメモします。
5. [登録] をクリックします。

   新しいタブが開いて Salesforce ログイン画面が表示されます。

6. システム管理者のログイン情報を使用して Developer Edition 組織にログインします。

   一時的に [リモートアクセス] ページが表示された後、[アプリケーション] ページにリダイレクトされます。Summer'13 リリースで、リモートアクセスアプリケーションは接続アプリケーションに置き換わり、既存のリモートアクセスアプリケーションは接続アプリケーションに自動的に移行されました。

ステップ 2: 接続アプリケーションを作成する

Heroku からアプリケーションを接続アプリケーションのリストに追加します。

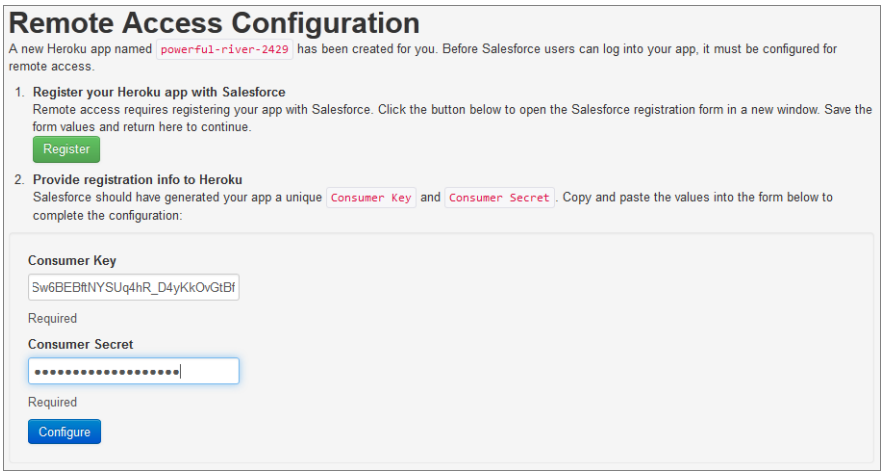
1. [アプリケーション] ページで、[接続アプリケーション] 関連リストまでスクロールダウンし、[新規] をクリックします。
2. [接続アプリケーション名] に、Heroku アプリケーションの名前を入力します。
3. [API 参照名] に、*ダッシュをアンダースコアに置き換えるか、ダッシュを削除した* Heroku アプリケーションの名前を入力します。Heroku ではアプリケーション名にダッシュが必須ですが、Salesforce では API 名にダッシュを使用できません。
4. [取引先責任者 メール] に、システム管理者のメールアドレスを入力します。
5. [OAuth 設定の有効化] を選択します。
6. [コールバック URL] に、Heroku アプリケーションへの URL (`/_auth` を含む) を入力します。

   たとえば、`https://arcane-crag-2451.herokuapp.com/_auth` のようにします。
7. [選択した OAuth 範囲] には、以下を追加します。
   a. フルアクセス
   b. ユーザに代わっていつでも要求を実行 (refresh_token、offline_access)
8. [保存] をクリックします。

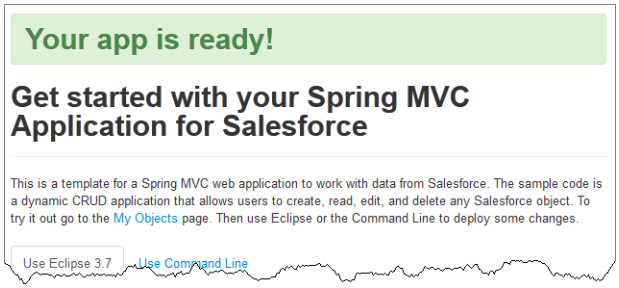
ステップ 3: OAuth アプリケーションを終了する

ここでは、Heroku アプリケーションを Salesforce OAuth プロバイダと接続します。

1. [接続アプリケーションの詳細] ページで、[コンシューマ鍵] の値をコピーします。
2. ブラウザの Heroku タブに戻り、[Consumer Key (コンシューマ鍵)] に貼り付けます。
3. ブラウザの Salesforce タブに戻ります。
4. [コンシューマの秘密] をクリックして表示します。
5. [コンシューマの秘密] をコピーします。
6. ブラウザの Heroku タブに戻り、[Consumer Secret (コンシューマの秘密)] に貼り付けます。

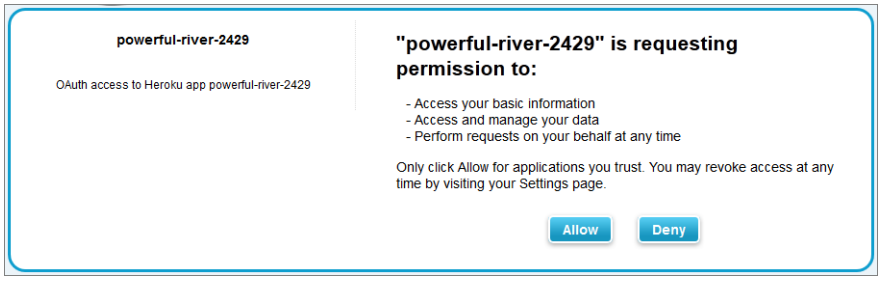


7. [設定] をクリックします。
   これには数分かかる場合があります。
8. ページの最初のパラグラフにある [My Objects (私のオブジェクト)] リンクをクリックします。



   Salesforce OAuth 画面にリダイレクトされます。ページの右上隅で Developer Edition 組織のシステム管理者としてログインしていることを確認します。

9. [許可] をクリックします。



   いずれかのオブジェクトをクリックすると、プラットフォームとロール設定に基づいてアクセス権を持つレコードが表示されます。たとえば、[Invoice Statement (請求書)] をクリックすると、Invoice オブジェクトが表示されます。

Salesforce アプリケーションランチャーから接続アプリケーションを起動する

接続アプリケーションに Salesforce 組織からのシングルサインオンを設定し、アプリケーションランチャーに追加します。

Salesforce のアプリケーションランチャーでは、接続アプリケーションおよび標準アプリケーションにリンクするロゴがすべて 1 つのタブに表示されます。表示するには、ユーザに「Identity 機能を使用」が有効で [アプリケーションランチャー] が [参照可能] に設定されたプロファイルまたは権限セットが割り当てられている必要があります。その場合、アプリケーションランチャーは Force.com アプリケーションメニューにアプリケーションとして表示されます。DE 組織のシステム管理者には、すでにアプリケーションランチャーへのアクセス権があります。

1. Salesforce 組織から接続アプリケーションを起動するには、開始 URL を設定する必要があります。
2. Salesforce 組織で、[設定] から [クイック検索] ボックスに「接続アプリケーション」と入力し、接続アプリケーションを管理するオプションを選択します。
   新しい接続アプリケーションのリストが表示されます。
3. 接続アプリケーション名の横にある [編集] をクリックします。
4. [基本情報] セクションで、アプリケーションに [開始 URL] を指定します。
   たとえば、アプリケーションが「glacial-temple-2472」の場合、URL は *https://glacial-temple-2472.herokuapp.com/* になります。

   メモ: *https://* プレフィックスを含めてください。
5. [新規] をクリックします。
6. [アプリケーションランチャー] タブをクリックするか、ドロップダウンアプリケーションメニューから [アプリケーションランチャー] を選択します。[アプリケーションランチャー] タブに、追加した接続アプリケーションが表示されます。アプリケーションをクリックして起動できます。

接続アプリケーションにカスタムロゴを指定し、アプリケーションランチャーでの外観をカスタマイズできます。次に、レポートですべてのユーザの接続アプリケーション利用状況を監視し、必要に応じてセキュリティ設定を調整します。

第 4 章　私のドメイン

トピック:

Salesforce の [私のドメイン] 機能を使用して、カスタムドメインを Salesforce 組織の URL に追加します。カスタムドメインを持つことで、独自のブランドが強調され、組織がより安全になります。カスタムドメインを使用すれば、ログインページをカスタマイズすることができるので便利です。

[私のドメイン] を使用すると、Salesforce ドメインの一部であるカスタムドメインを定義できます。カスタムドメインは、実際にはプライマリドメインのサブドメインです。たとえば、`developer` は `salesforce.com` ドメインのサブドメインです。カスタムドメインを使用すると、`https://yourInstance.salesforce.com/` のような Salesforce が割り当てた URL を、`https://somethingcool.my.salesforce.com` のような自分が選択した名前に置き換えることができます。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

カスタムドメイン名を使用すると、組織でのログインや認証の管理を次のような複数の方法で改善することができます。たとえば、

- 一意のドメイン URL でビジネスアイデンティティを強調する
- ログイン画面のブランド設定および右フレームのコンテンツのカスタマイズを行う
- 新しいドメイン名を使用しないページ要求をブロックまたはリダイレクトする
- 複数の Salesforce 組織で同時に作業する
- カスタムログインポリシーを設定してユーザの認証方法を決定する
- ユーザがログインページで Google や Facebook などのソーシャルアカウントを使用してログインできるようにする
- ユーザが 1 回ログインするだけで外部サービスにアクセスできるようにする

次の Salesforce 機能を使用するには [私のドメイン] が必要です。

- 外部 ID プロバイダを使用したシングルサインオン (SSO)
- Google や Facebook などの認証プロバイダを使用したソーシャルサインオン
- Lightning コンポーネントタブ、Lightning ページ、Lightning アプリケーションビルダー、またはスタンドアロンアプリケーションの Lightning コンポーネント

Sandbox 環境でも [私のドメイン] を使用できます。

メモ: [私のドメイン] には、追加の利用規約が適用されます。

ドメイン名には、次のような標準 URL 形式を使用します。

- プロトコル: https://
- サブドメインのプレフィックス: ブランドまたは用語
- ドメイン: my.salesforce.com

名前は40字以下で、文字、数字、ハイフンを使用できます。ドメイン名の先頭は、root、status、またはハイフンにはできません。

ドメイン名を決定する前に、複数の名前を試して使用可能かどうかを確認できます。

Salesforce は、ドメインの作成時に ID プロバイダとして有効になります。ドメインをリリースした後で、ドメインのログインポリシーをカスタマイズして、ID プロバイダを追加または変更したり、組織のセキュリティを強化したりできます。

重要: ドメインはリリース直後に有効になり、元の URL を使用した要求は新しいドメインにリダイレクトされます。リリース後は、Salesforce カスタマーサポートのみが、ドメイン名を無効化または変更できます。

ドメイン名の設定

カスタムドメイン名は、すばやく簡単に実装できます。

1. 使用可能なドメイン名を見つけてサインアップします。
2. ログインページのロゴ、背景色、および右フレームの内容をカスタマイズします。
3. ログインページで使用できる ID プロバイダを追加または変更します。
4. ドメイン名をテストして組織全体にリリースします。
5. ユーザがページにアクセスするときのログインポリシーを設定します。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

ユーザ権限

ドメイン名を設定する
- 「アプリケーションのカスタマイズ」

ドメイン名の定義

組織のカスタムドメイン名をサインアップします。登録する前に、名前を試用して利用可能かどうか確認できます。

カスタムドメイン名の設定では最初に組織に固有のドメイン名を見つけてサインアップします。名前は慎重に選択します。登録すると、Salesforce がドメイン名を使用してそのドメイン名レジストリを更新します。登録した後は、Salesforce カスタマーサポートしかドメイン名を無効化または変更できません。

1. [設定] から、[クイック検索] ボックスに「*私のドメイン*」と入力し、[私のドメイン] を選択します。
2. サンプル URL で使用するサブドメイン名を入力します。たとえば、Universal Containers という会社が `universalcontainers` というサブドメインを使用するとします。この会社のログイン URL は、`https://universalcontainers.my.salesforce.com/` となります。名前は 40 字以下で、文字、数字、ハイフンを使用できます。

   次の予約語は、サブドメインには使用できません。

   - www
   - salesforce
   - heroku

   ドメイン名の先頭を次のものにすることはできません。

   - root

エディション

使用可能なインターフェース: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

ユーザ権限

ドメイン名を定義する
- 「アプリケーションのカスタマイズ」

- status
- ハイフン

3. [使用可能か調べる] をクリックします。名前がすでに使用されている場合、別の名前を選択します。
4. [契約条件] をクリックして契約を確認し、チェックボックスをオンにします。
5. [ドメインの登録] をクリックします。
6. ドメイン名のテストの準備ができると、通知メールが送信されます この処理に最大 3 分かかることがあります。

ドメイン名をテストしてリリースしたら、ユーザが新しいドメイン名を使用できます。

ログインページのブランド設定のカスタマイズ

背景色、ロゴ、および右側のコンテンツを追加して、ログインページの外観をカスタマイズします。ログインページをカスタマイズして自社のブランドに関連付けると、ユーザがページを見分けやすくなります。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

ユーザ権限

ログインページをカスタマイズする
- 「アプリケーションのカスタマイズ」

1. [設定] から、[クイック検索] ボックスに「*私のドメイン*」と入力し、[私のドメイン] を選択します。
2. [認証設定] で [編集] をクリックします。
3. ロゴをカスタマイズするには、画像をアップロードします。

   画像には、最大 100 KB の .jpg、.gif、または .png ファイルを使用できます。最大サイズは 250px × 125px です。
4. ログインページの背景をカスタマイズするには、 をクリックするか、有効な 16 進数の色コードを入力します。
5. iOS ユーザのために高度な認証方式をサポートするには、[iOS でのユーザ認証にネイティブブラウザを使用] を選択します。

   このオプションにより、iOS デバイスで Salesforce1 と Mobile SDK のアプリケーションを使用しているユーザのために、Kerberos、Windows NT LAN Manager (NTLM)、証明書ベースの認証などの認証方式がサポートされます。このオプションを選択すると、iOS デバイスのユーザは、カスタムドメインへのシングルサインオン認証を使用するときにネイティブブラウザにリダイレクトされます。他のオペレーティングシステムの場合、Salesforce1 や、Mobile SDK バージョン 3.1 以降を使用しているアプリケーションがモバイルデバイス管理 (MDM) ソフトウェアと統合されていれば、これらのアプリケーションで証明書ベースの認証を使用できます。
6. ログインページの右側の iFrame に入れるファイルの URL を入力します。

   右側の iFrame のコンテンツは、ページの約半分を占めるようにサイズ変更できます。SSL 暗号化と https:// 接頭辞を使用する URL にコンテンツをホストする必要があります。反応型 Web 設計を使用して右側の iFrame に独自のカスタムコンテンツページを作成するには、私のドメインサンプルテンプレートを使用します。

   例: `https://c.salesforce.com/login-messages/promos.html`

7. 必要に応じて、ログインページの ID プロバイダとして認証サービスを選択します (Google や Facebook のようなソーシャルサインオンプロバイダなど)。これにより、ユーザはソーシャルアカウントのログイン情報を使用してログインできるようになります。認証サービスを [設定] の [認証プロバイダ] として設定します。
8. [保存] をクリックします。

ログインページへの ID プロバイダの追加

ユーザが代替 ID プロバイダオプションを使用してログインページから直接認証できるようにします。シングルサインオンを有効にして SAML を設定しているか、[設定] で [認証プロバイダ] として外部認証プロバイダを設定している場合、ドメインのログインページでそれらの ID プロバイダへのリンクを提供できます。ユーザは ID プロバイダのログイン画面に送られて認証された後、Salesforce にリダイレクトして戻されます。

メモ: Janrain を除き、SAML シングルサインオン ID プロバイダまたは外部認証プロバイダとして設定されているすべてのプロバイダを認証サービスとして使用できます。Janrain を使用して、ログインページから認証することはできません。

1. [設定] から、[クイック検索] ボックスに「*私のドメイン*」と入力し、[私のドメイン] を選択します。
2. [認証設定] で [編集] をクリックします。
3. ID プロバイダとして、1 つ以上の設定済み認証サービスを選択します。
4. [保存] をクリックします。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

ユーザ権限

ログインページに ID プロバイダを追加する
- 「アプリケーションのカスタマイズ」

[私のドメイン] のログインポリシーの設定

ドメインのログインポリシーをカスタマイズして、ログインのセキュリティを確保します。

ログインポリシーをカスタマイズして、組織のセキュリティレイヤを追加します。デフォルトでは、ユーザはドメイン固有のログインページをスキップして、一般的な Salesforce ログインページからログインできます。また、ユーザはドメイン名を使用せずにページ要求を行うこともできます(以前のブックマークを使用する場合など)。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

ユーザ権限

ドメインのログインポリシーを設定する
- 「アプリケーションのカスタマイズ」

1. [設定] から、[クイック検索] ボックスに「*私のドメイン*」と入力し、[私のドメイン] を選択します。
2. [私のドメインの設定] で、[編集] をクリックします。
3. ドメイン固有のログインページを使用しないユーザの認証をオフにするには、ログインポリシーを選択します。ポリシーを選択することで、たとえば、一般的な `https://<instance>.salesforce.com/` ログインページでユーザがログインしたり、ログイン後にページにリダイレクトされることを回避できます。このオプションを使用すると、ドメイン名を知らないユーザによるログイン試行を回避できるため、セキュリティが向上します。
4. リダイレクトポリシーを選択します。
   a. ドメイン名を含まない URL を引き続き使用することをユーザに許可するには、[ドメイン内の同じページにリダイレクト] を選択します。このオプションを選択すると、組織のセキュリティは向上しません。

      メモ: パートナーポータルに [ドメイン内の同じページにリダイレクト] オプションが選択されている場合はブックマークが機能しません。既存のブックマークを手動で変更し、Salesforce インスタンス名をカスタムドメイン名に置き換えることによって、新しいドメイン URL を参照するようにします。たとえば、ブックマークの URL にある *`https://yourInstance.salesforce.com/`* を *`https://yourDomain.my.salesforce.com/`* に置き換えます。

   b. ドメイン名を使用するようにユーザに要求するには、[ドメイン内の同じページに警告付きでリダイレクト] を選択します。ユーザは、警告を読んだ後ページを表示できます。このオプションを数日間または数週間に設定しておくことで、ユーザは新しいドメイン名に移行しやすくなりますが、組織のセキュリティは向上しません。
   c. ページを表示するときにドメイン名を使用するようにユーザに要求するには、[リダイレクトしない] を選択します。これは、最もセキュリティレベルが高いオプションです。
5. [保存] をクリックします。

[私のドメイン] の URL の変更

組織のドメイン名を設定すると、Visualforce ページの URL を含め、すべてのアプリケーション URL も変更されます。ドメイン名をリリースする前に、すべてのアプリケーション URL を更新していることを確認します。たとえば、Chatter アンサーの [メール通知 URL] 項目を更新しないと、古い URL で通知を内部ユーザに送信し続けます。次の表に変更内容を示します。

URL の種類	古い URL	新しい URL
ログイン	`https://login.salesforce.com`	`https://<subdomain>.my.salesforce.com`
アプリケーションページまたはタブ	*https://yourInstance.salesforce.com/<pageID>*	`https://<subdomain>.my.salesforce.com/<pageID>`
名前空間を含まない Visualforce ページ	*https://c.visual.force.com/apex/<pagename>*	`https://<subdomain>--c.visual.force.com/apex/<pagename>`
名前空間を含む Visualforce ページ	`https://<yournamespace101>.visual.force.com/apex/<pagename>`	`https://<subdomain>--<yournamespace>.visual.force.com/apex/<pagename>`

エディション

使用可能なインターフェース: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

メモ: Sandbox 環境で [私のドメイン] を実装すると、URL 形式は `https://<subdomain>--<sandboxname>.<instance>.my.salesforce.com` になります。Sandbox 環境では名前空間を使用できないため、Sandbox のすべての Visualforce ページの URL の形式は `https://<subdomain>--<sandboxname>.<instance>.my.salesforce.com/apex/<pagename>` です。

新しいドメイン名のテストおよびリリース

ドメイン名を設定した後、それをテストしてユーザにロールアウトします。テストでは、ドメイン名を試すことができます。さらに、ドメインをユーザにロールアウトする前に、ページのアドレスを検証できます。

重要: ドメインはリリース直後に有効になり、元の URL を使用した要求は新しいドメインにリダイレクトされます。リリース後は、Salesforce カスタマーサポートのみが、ドメイン名を無効化または変更できます。

1. ドメインのログインをテストします。[設定] から、[クイック検索] ボックスに「*私のドメイン*」と入力し、[私のドメイン]、[こちらをクリックしてログインしてください] の順に選択します。または、DE 組織からログアウトし、カスタムドメイン名を使用して Salesforce にログインします。受信したアクティベーションメールに記載されたログインリンクをクリックしても、ログインは可能です。

   ドメインをユーザにリリースする前に、ドメインのログインページをカスタマイズして認証サービス (ソーシャルサインオンなど) を追加できます。ドメインを Sandbox 環境でテストすることもできます。

2. タブとリンクをクリックして、新しいドメイン名をテストします。すべてのページに新しいドメイン名が表示されます。

   カスタムボタンや Visualforce ページなどの機能によって Salesforce UI をカスタマイズした場合、カスタム要素を徹底的にテストしてから新しいドメイン名をリリースしてください。カスタマイズにハードコードされた参照やインスタンスベースの URL がないか確認します。ある場合は、代わりにカスタムドメイン URL を使用します。

3. 新しいドメイン名を組織にロールアウトするには、[設定] から、[クイック検索] ボックスに「*私のドメイン*」と入力し、[私のドメイン] を選択してから、[ユーザにリリース]、[OK] の順にクリックします。

ドメインはリリース直後に有効になり、新しいドメインアドレスのページにすべてのユーザがリダイレクトされます。ドメインをリリースした後に表示される [ドメインの設定] セクションでログインポリシーを設定できます。たとえば、ユーザが login.salesforce.com からログインできないように設定できます。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

ユーザ権限

ドメイン名を設定する
- 「アプリケーションのカスタマイズ」

[私のドメイン] を実装するためのガイドラインとベストプラクティス

次のヒントは、新しいドメイン名に円滑に移行するのに役立ちます。

- リリースする前に今後の変更をユーザに通知します。
- トラフィックが少ないときにトラブルシューティングができるように、組織で受信するトラフィックが最小になるタイミング (週末など) に新しいドメインをリリースします。
- リリースする前にまず、ログインポリシーのカスタマイズ、カスタム UI 機能、Visualforce ページ、アプリケーション URL の変更を Sandbox 環境でテストします。
- カスタムボタンや Visualforce ページなどの機能によって Salesforce UI をカスタマイズした場合、カスタム要素を徹底的にテストしてから新しいドメイン名をリリースしてください。カスタマイズにハードコードされた参照やインスタンスベースの URL がないか確認します。ある場合は、代わりにカスタムドメイン URL を使用します。
- ドメイン名をリリースする前に、すべてのアプリケーション URL を更新していることを確認します。たとえば、Chatter アンサーの [メール通知 URL] 項目を更新しないと、古い URL で通知を内部ユーザに送信し続けます。
- ドメインが登録されたが、まだリリースされていない場合に [私のドメイン] ログインページからログインすると、URL にカスタムドメイン名が示されます。ただし、ワークフローメールなど非同期で送信されるメールに埋め込まれている差し込み項目から作成されたリンクには、依然として古い URL が使用されます。ドメインのリリース後は、上記のようなリンクにも新しい [私のドメイン] URL が表示されます。
- 頻繁に使用するページ (ログインページなど) へのリンクを提供して、ユーザが新しいドメイン名の使用を開始できるようにサポートします。ログインポリシーが変更されたことをユーザに通知して、ユーザが初めてリダイレクトされたときにブックマークを更新するように促します。
- リダイレクトポリシーの [ドメイン内の同じページに警告付きでリダイレクト] オプションを選択して、ユーザがブックマークを新しいドメイン名に更新する猶予期間を設けます。数日または数週間が経過したら、ポリシーを [未リダイレクト] に変更します。このオプションは、ページを表示するときにドメイン名を使用するようユーザに要求します。これはセキュリティレベルが最も高いオプションです。
- [https://login.salesforce.com からログインできないようにする] は、カスタムドメインを認識していないユーザがそのドメインを使用するのではないかと懸念される場合にのみ使用します。それ以外の場合は、ユーザが新しいドメイン名に慣れるまでの間このオプションを使用できるようにしておきます。
- パートナーポータルに [ドメイン内の同じページにリダイレクト] オプションが選択されている場合はブックマークが機能しません。既存のブックマークを手動で変更し、Salesforce インスタンス名をカスタムドメイン名に置き換えることによって、新しいドメイン URL を参照するようにします。たとえば、ブックマークの URL にある *https://yourInstance.salesforce.com/* を *https://yourDomain.my.salesforce.com/* に置き換えます。
- 新しい Salesforce ドメイン名 URL を使用していないアプリケーションページ要求をブロックする場合は、ユーザに、以前のブックマークを更新するか、ログインページの新しいブックマークを作成する必要があることを通知します。ユーザはアプリケーション内のタブやリンクも更新する必要があります。ログインリダ

エディション

使用可能なインターフェース: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

イレクトポリシーを［未リダイレクト］に変更する場合は、ユーザが直ちに新しいURLを使用する必要があります。

- [私のドメイン]を使用する場合は、いつどのユーザが新しいログインURLでログインしているかを識別できます。[設定]から、［クイック検索］ボックスに「*ログイン履歴*」と入力し、[ログイン履歴]を選択して、[ユーザ名]列と[ログインURL]列を表示します。
- `login.salesforce.com`ページで、ユーザは[カスタムドメインにログインする]をクリックし、カスタムドメイン名を入力してログインできます。この場合、ユーザがドメイン名を認識している必要があります。安全を期すために、カスタムドメインのログインページへのダイレクトリンクをユーザに配布します。

所有する要素	実行する操作
組織へのAPIインテグレーション	APIクライアントがサーバエンドポイントを直接参照しているかどうかを確認します。APIクライアントは、ハードコードされたサーバURLを使用する代わりに、ログイン要求で返されたLoginResult.serverURL値を使用する必要があります。 カスタムドメインがリリースされた後は、Salesforceがドメインを含むサーバURLを返します。リダイレクトポリシー設定がAPIコールに影響することはありません。つまり、インスタンスURLへの従来のコールも継続して機能します。ただし、ベストプラクティスは、Salesforceから返された値を使用することです。
メールテンプレート	組織のインスタンスURLへの参照をカスタムドメインに置き換えます。
カスタムVisualforceページまたはカスタムForce.comアプリケーション	組織のインスタンスURLへの参照をカスタムドメインに置き換えます。「How to find hard-coded references with the Force.com IDE」を参照してください。
Chatter	Chatterグループの左側のナビゲーションでブックマークを更新するようにユーザに通知します。
コミュニティのゾーン(アイデア/アンサー/Chatterアンサー)	［メール通知 URL］を手動で更新します。 URLを更新するには、既存のURLをクリアして項目を空白にし、ページを保存します。その後、システムが項目に新しい[私のドメイン]のURLを入力します。

[私のドメイン] を使用したシステムパフォーマンス情報とメンテナンス情報の取得

Salesforce カスタマーは、`trust.salesforce.com` からシステムパフォーマンス情報とメンテナンス情報を取得します。パフォーマンス情報は、組織のインスタンスに基づいてレポートされます。組織で使用しているインスタンスは、私のドメインを設定していなければ、ブラウザのアドレスバーに表示されます。ベストプラクティスに従って私のドメインを設定した場合は、ドメインルックアップツールを使用してインスタンスを取得してください。

ドメイン名を使用して、システムの状況の情報を取得する方法を次に示します。

1. システムの状況を確認できる trust.salesforce.com に移動します。
2. trust.salesforce.com/trust/domainLookupLaunch/ に移動し、検索バーにドメイン名を入力してインスタンスを取得します。
   URL 全体ではなく、ドメイン名を入力してください。たとえば、`https://yourDomain.my.salesforce.com/` ではなく *yourDomain* を使用します。
3. [すべてのインスタンスが利用可能] を選択し、インスタンスのエントリを探してください。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

ユーザ権限

ドメイン名の設定に必要な権限

- 「アプリケーションのカスタマイズ」

第 5 章　アプリケーションランチャーの設定および使用

トピック:

アプリケーションランチャーでは、社内アプリケーション、接続アプリケーション、および Salesforce アプリケーションにリンクするロゴがすべて 1 つの統合ユーザインターフェースに表示されます。システム管理者は、組織のアプリケーションのデフォルトの表示順を設定できます。

すべての Lightning Experience ユーザは、アプリケーションランチャーを使用できます。

Salesforce Classic ユーザには「Identity 機能を使用」権限が必要であり、ユーザプロファイルの [アプリケーションランチャー] オプションが [参照可能] に設定されている必要があります。ユーザには、表示権限のあるアプリケーションのみが表示されます。

Salesforce Classic では、システム管理者プロファイルを持つシステム管理者には、アプリケーションランチャーへのアクセス権が自動的に付与されます。システム管理者プロファイルからコピーされたプロファイルを使用するシステム管理者には、アクセス権は付与されません。

「クイックスタート:自分のドメインの設定、接続アプリケーションの追加、およびアプリケーションランチャーの使用」に示すように、アプリケーションランチャーは接続アプリケーションへのアクセスを管理する場合に特に便利です。また、AppMenuItem API を使用すれば、アプリケーションランチャーのアプリケーションをプログラムで制御できます。

Salesforce Classic でのプロファイルを使用したアプリケーションランチャーの有効化

アプリケーションランチャーにアクセスできるようにプロファイルを作成してユーザに割り当てます。

メモ: 次の手順は、Salesforce Classic で動作します。Lightning Experience では、画面上部のナビゲーションバーの左側に [アプリケーションランチャー] アイコン ( ) が表示されます。Salesforce Classic では、このアイコンは表示されません。

Salesforce Classic では、システム管理者プロファイルを持つシステム管理者には、アプリケーションランチャーへのアクセス権が自動的に付与されます。システム管理者プロファイルからコピーされたプロファイルを使用するシステム管理者には、アクセス権は付与されません。

エディション

使用可能なエディション: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

1. [設定] から、[クイック検索] ボックスに「*プロファイル*」と入力し、[プロファイル] を選択します。
2. [新規プロファイル] をクリックします。
3. 新規プロファイルのベースとして既存のプロファイルを選択します。
   たとえば、[標準ユーザ] を選択します。
4. 新規プロファイルの名前を入力します。
   たとえば、「`Standard User Identity`」(標準ユーザ ID) と入力します。
5. [保存] をクリックします。
6. 新規プロファイルの詳細ページで、[編集] をクリックします。
7. [カスタムアプリケーション設定] で、[アプリケーションランチャー] を [参照可能] に設定します (まだ設定していない場合)。
   [タブの設定] で、[アプリケーションランチャー] タブが [デフォルトで表示] に設定されていることを確認します。
8. [システム管理者権限] の下で、[Identity 機能を使用] を選択します。
9. [保存] をクリックします。
10. [設定] から、[クイック検索] ボックスに「*ユーザ*」と入力し、[ユーザ] を選択します。
11. アプリケーションランチャーにアクセスする各ユーザの横にある [編集] をクリックします。
12. ユーザの [プロファイル] 項目で、[Identity 機能を使用] が有効になっている新規プロファイルを選択します。
    たとえば、`[Standard User Identity (標準ユーザ ID)]` プロファイルを使用できます。
13. [保存] をクリックします。
    選択したユーザとしてログインすると、アプリケーションランチャーがドロップダウンアプリケーションメニューに表示されます。

Salesforce Classic での権限セットを使用したアプリケーションランチャーの有効化

アプリケーションランチャーにアクセスできるように権限セットを作成してユーザに割り当てます。

エディション

使用可能なエディション: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

メモ: 次の手順は、Salesforce Classic で動作します。Lightning Experience では、画面上部のナビゲーションバーの左側に [アプリケーションランチャー] アイコン ( ) が表示されます。Salesforce Classic では、このアイコンは表示されません。

1. [設定] から、[クイック検索] ボックスに「*権限セット*」と入力し、[権限セット] を選択します。
2. [新規] をクリックします。
3. 新しい権限セットの表示ラベルを入力します。

   たとえば、「*Identity Features*」(ID 機能) と入力します。
4. 必要に応じて、この権限セットの使用を特定のユーザライセンスに制限します。
5. [保存] をクリックします。
6. [システム権限] をクリックします。
7. [編集] をクリックします。
8. [Identity 機能を使用] を選択します。
9. [保存] をクリックします。
10. [設定] から、[クイック検索] ボックスに「ユーザ」と入力し、[ユーザ] を選択します。
11. アプリケーションランチャーへのアクセス権を付与する既存のユーザの名前をクリックします。
12. [権限セットの割り当て] 関連リストで、[割り当ての編集] をクリックします。
13. Identity 機能に対して作成した新しい権限セットを [有効化された権限セット] に追加します。
14. [保存] をクリックします。

    選択したユーザとしてログインすると、アプリケーションランチャーがドロップダウンアプリケーションメニューに表示されます。

    メモ: アプリケーションランチャーが表示されない場合は、ユーザに関連付けられたプロファイルで、アプリケーションランチャー設定の [参照可能] を選択します。

アプリケーションの並び替え

組織のSalesforceアプリケーション、カスタムアプリケーション、接続アプリケーションのデフォルトの順序を並び替えます。アプリケーションランチャーでアプリケーションを非表示にすることもできます。

システム管理者は、組織のユーザに表示されるアプリケーションのデフォルトの並び替え順を制御します。この対象は、Salesforce マーケティングアプリケーションやコールセンターアプリケーションなどのSalesforceの標準アプリケーションと、組織のカスタムアプリケーションです。組織で接続アプリケーションを使用していることもあります。接続アプリケーションには、Gmail™・や Microsoft Office 365™・などの生産性アプリケーションや、ユーザの業務遂行を支援するその他のアプリケーションがあります。

組織に設定する並び替え順は、ユーザのデフォルトビューになります。ユーザは組織のデフォルトビューから開始して、最も頻繁に使用するアプリケーションにすばやくアクセスできるようにアプリケーションの順序を並び替えることができます。

エディション

使用可能なエディション: Lightning Experience と Salesforce Classic の両方

使用可能なエディション: **Contact Manager** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

このセクションの内容:

Salesforce Classic での Force.com アプリケーションメニューとアプリケーションランチャーの並び替え

アプリケーションが Force.com アプリケーションメニューに表示される順序を変更できます。

Force.com アプリケーションメニューは、各アプリケーションページの上部に表示されるドロップダウンリストです。アプリケーションランチャーが有効になっていると、オンプレミス型アプリケーション、接続アプリケーション、および Salesforce アプリケーションにリンクするロゴが表示されます。

1. [設定] から、次のいずれかの操作を実行します。
   a. [クイック検索] ボックスに「アプリケーション」と入力し、[アプリケーション] を選択して、[並び替え] をクリックします。
   b. [クイック検索] ボックスに「アプリケーションメニュー」と入力し、[アプリケーションメニュー] を選択します。
2. 必要に応じて、リストのアプリケーションをドラッグして順序を変更します。変更はその場で有効になります。
3. 必要に応じて、[参照可能] または [非表示] をクリックすると、組織のすべてのユーザに対してアプリケーションランチャーの個々のアプリケーションを表示または非表示にできます。

組織にインストールされたすべてのアプリケーションは、並び替え用に表示されます。ただし、Force.com アプリケーションメニューとアプリケーションランチャーに表示されるアプリケーションは、各アプリケーションの表示設定とユーザ権限によって異なります。たとえば、システム管理者には通常、標準ユーザより多くのアプリケーションが表示されます。ユーザ権限がありプロファイルで参照可能になっているすべてのアプリケーションが表示されます。アプリケーションランチャー、接続アプリケーション、およびサービスプロバイダでは、開始URLがリストされている必要があります。

エディション

使用可能なエディション: Salesforce Classic

使用可能なエディション: **Contact Manager** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

アプリケーションを参照する
- 「設定・定義を参照する」

アプリケーションを管理する
- 「アプリケーションのカスタマイズ」

Salesforce Lightning Experience でのアプリケーションランチャーのアプリケーションの並び替え

アプリケーションランチャーに表示されるアプリケーションの組織のデフォルトの表示設定や順序を変更できます。

アプリケーションランチャーには、ユーザが使用可能なすべての Salesforce アプリケーションと、システム管理者が組織にインストールした接続アプリケーションが表示されます。システム管理者は、アプリケーションランチャーを使用して、組織のアプリケーションのデフォルトの並び替え順と表示を設定できます。ユーザは、アプリケーションランチャー内で自分のビューを並び替えることができます。

1. [設定] から、次のいずれかの操作を実行します。
   a. ［クイック検索］ボックスに「アプリケーション」と入力し、[アプリケーション] を選択して、[並び替え] をクリックします。
   b. ［クイック検索］ボックスに「アプリケーションメニュー」と入力し、[アプリケーションメニュー] を選択します。
2. 必要に応じて、リストのアプリケーションをドラッグして順序を変更します。変更はその場で有効になります。
3. [参照可能] または [非表示] をクリックすると、組織のすべてのユーザに対してアプリケーションランチャーの個々のアプリケーションを表示または非表示にできます。

組織にインストールされたすべてのアプリケーションは、並び替え用に表示されます。ただし、アプリケーションランチャーに表示されるアプリケーションは、各アプリケーションの表示設定とユーザ権限によって異なります。たとえば、システム管理者には通常、標準ユーザより多くのアプリケーションが表示されます。ユーザ権限がありプロファイルで参照可能になっているすべてのアプリケーションが表示されます。接続アプリケーションおよびサービスプロバイダでは、開始 URL がリストされている必要があります。

エディション

使用可能なエディション: Lightning Experience

使用可能なエディション: **Contact Manager** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

アプリケーションを参照する
- 「設定・定義を参照する」

アプリケーションを管理する
- 「アプリケーションのカスタマイズ」

第 6 章 Google Apps へのシングルサインオンの設定

トピック:

Salesforce 組織のユーザが Google Apps (Google Drive、Gmail、および Gcal など) にシングルサインオンアクセスできるようにします。

Google Apps では、シングルサインオン用の SAML が使用されるため、Google に個別にログインすることなく、Salesforce アプリケーションランチャーから Google Apps を起動するように組織を設定できます。このプロセスはクイックスタートのプロセスと類似しており、Salesforce 組織のユーザが Google Apps (Google Drive、Gmail、および Gcal など)にシングルサインオンアクセスできるようにすることができます。組織で Google Apps を設定するには、以下が必要です。

1. カスタムドメイン ([私のドメイン])。
2. Google 管理コンソールへのアクセス権がある Google Apps 管理者アカウント。
3. [Identity 機能を使用] が有効になっているプロファイルまたは権限セット。

独自のカスタムドメインを設定する手順は、「クイックスタート:自分のドメインの設定、接続アプリケーションの追加、およびアプリケーションランチャーの使用」を参照してください。[Identity 機能を使用] が有効になっているプロファイルまたは権限セットを設定する手順は、「アプリケーションランチャーの設定および使用」を参照してください。

Salesforce ID プロバイダの証明書の取得

ID プロバイダの証明書をダウンロードして保存します。

Salesforce 組織で次の手順を実行します。

1. [設定] から、[クイック検索] ボックスに「*ID プロバイダ*」と入力し、**[ID プロバイダ]** を選択します。

   [ID プロバイダの設定] セクションで SAML アサーションを署名する証明書を取得します。必要に応じて、自己署名証明書を署名機関によって発行された本番証明書に変更できます。証明書についての詳細は、オンラインヘルプの「証明書と鍵のペアの作成」を参照してください。

2. **[証明書のダウンロード]** をクリックします。

   この証明書で署名が検証されたら、Google 管理者アカウントに証明書をアップロードする必要があります。保存場所を覚えておいてください。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Developer** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Database.com** Edition

Google 管理者のシングルサインオンオプションの設定

Google 管理者アカウントで、シングルサインオンの値を設定します。

https://admin.google.com で管理者として Google Apps アカウントにサインインする必要があります。

1. Google 管理者アカウントで、**[その他のコントロール]** > **[セキュリティ]** > **[詳細設定]** > **[シングル サインオン (SSO) の設定]** をクリックします。
2. 次の値を入力します。
   a. サインインページの URL: *https://yourdomain.my.salesforce.com/idp/endpoint/HttpRedirect*

      yourdomain は、カスタムドメイン名で置き換えてください。

   b. サインアウトページの URL: *https://yourdomain.my.salesforce.com*

      yourdomain は、カスタムドメイン名で置き換えてください。

   c. パスワードの URL を変更: *https://yourdomain.my.salesforce.com/_ui/system/security/ChangePassword*

      yourdomain は、カスタムドメイン名で置き換えてください。

   d. 検証証明書: 「Salesforce ID プロバイダの証明書の取得」で保存した ID プロバイダの証明書ファイルをアップロードします。

   e. **[ドメイン固有の発行元を使用]** を選択します。
3. **[変更を保存]** をクリックします。

Gmail の接続アプリケーションの作成

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Developer** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Database.com** Edition

次の手順は、Gmail 接続アプリケーションの設定方法を示しています。

Salesforce 組織で次の手順を実行します。

1. [設定] から、[クイック検索] ボックスに「アプリケーション」と入力し、[アプリケーション] を選択します。
2. [接続アプリケーション] セクションで、[新規] をクリックします。
3. [基本情報] セクションで、次の値を入力します。
   a. 接続アプリケーション名: *Gmail*。
   b. 連絡先メール: システム管理者のメールアドレス。
   c. ロゴ画像 URL:[いずれかのサンプルロゴを選択] を選択し、対象のロゴを特定してクリックします。次に、ログ URL をコピーします。[ロゴ画像 URL] 項目に値を貼り付けます。または、独自の URL を入力します。
4. [Web アプリケーション設定] セクションで、次の値を入力します。
   a. 開始 URL: *https://gmail.google.com*。
   b. [SAML の有効化] を選択します。
   c. エンティティ ID: 「*google.com/a/yourGoogleAppDomainName*」と入力します。
      yourGoogleAppDomainName は、実際の Google ドメイン名で置き換えてください。
   d. ACS URL: [エンティティ ID] と同じですが、プレフィックスとして「https」、サフィックスとして「acs」が付きます (例: *https://google.com/a/yourGoogleAppDomainName/acs*)。
   e. 件名種別: ユーザの識別方法を選択します。
      この項目には、ユーザの Google Apps のメールアドレスを含める必要があります。

   設定を変更する必要がある場合を除き、その他の項目はそのままにしておきます。
5. [保存] をクリックします。
6. [設定] から、[クイック検索] ボックスに「接続アプリケーション」と入力し、接続アプリケーションを管理するオプションを選択します。
7. 接続アプリケーションの名前 (この場合は「Gmail」) をクリックします。
8. [Idp-init のログイン URL] の値をコピーします。
9. [編集] をクリックします。
10. [開始 URL] 項目で、[Idp-init のログイン URL] 項目の値を貼り付け、次の文字列を追加します。
    [Idp-init のログイン URL] 項目からコピーした値 + *&RelayState=http%3A%2F%2Fmail.google.com%2Fa%2FyourGoogleAppDomainName*
    yourGoogleAppDomainName は、実際の Google ドメインで置き換えてください。次のような値になります。

```
https://identitydemo.my.salesforce.com/idp/login?app=0sp30000000000k
&RelayState=http%3A%2F%2Fmail.google.com%2Fa%2Fidentitydemo.com
```

11. [保存] をクリックします。

    これで、この接続アプリケーションをプロファイルまたは権限セットに追加できるようになりました。そのプロファイルまたは権限セットをユーザに適用すると、ユーザは Gmail 接続アプリケーションを使用できるようになります。同じ基本プロセスを実行して、他の Google Apps をインストールできます。

第 7 章　2 要素認証ログイン要件の設定

Salesforce システム管理者は、ユーザがログインするときに、認証の 2 番目の要素を使用するように要求できます。

ユーザが Salesforce ([私のドメイン] を使用して作成されたカスタムドメインがある組織を含む) にユーザ名とパスワードを使用してログインするたびに 2 要素認証が必要になるように設定できます。この要件を設定するには、ユーザプロファイル (コピーされたプロファイルのみ) または権限セットの「ユーザインターフェースへのログインの 2 要素認証」権限を選択します。

段階的な手順: 2 要素認証によってログインを保護する

「ユーザインターフェースログインの2要素認証」権限があるユーザは、Salesforce へのログインのたびに、モバイル認証アプリケーションや U2F セキュリティ鍵などの 2 つ目の要素を入力する必要があります。

また、プロファイルベースのポリシーを使用して、特定のプロファイルに割り当てられたユーザに 2 要素認証要件を設定することもできます。次の認証方式のユーザに 2 要素認証要件を設定する場合はプロファイルポリシーを使用します。

- シングルサインオンの SAML
- Salesforce 組織またはコミュニティへのソーシャルサインオン
- コミュニティへのユーザ名およびパスワード認証

ユーザ名とパスワード、代理認証、SAML シングルサインオン、および認証プロバイダ経由のソーシャルサインオンなどの、すべての Salesforce ユーザインターフェース認証方式がサポートされています。ユーザプロファイルで、[ログインに必要なセッションセキュリティレベル] 項目を [高保証] に設定します。次に、組織のセッションの設定で、特定のログイン方法にポリシーを適用するようにセッションセキュリティレベルを設定します。組織のセッションの設定では、セッションのセキュリティレベルで、[2 要素認証] が [高保証] にあることも確認します。

警告: [2 要素認証] が [標準] 列にある場合、標準レベルセキュリティを付与する方法を使用してログインすると、エラーが発生します。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Contact Manager** Edition、**Group** Edition、**Professional** Edition、**Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

プロファイルと権限セットを編集する

- 「プロファイルと権限セットの管理」

このセクションの内容:

ID 検証のためのワンタイムパスワードジェネレータアプリケーションまたはデバイスの関連付け

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: すべてのエディション

Salesforce Authenticator や Google Authenticator などのワンタイムパスワードジェネレータアプリケーションをアカウントに関連付けることができます。Salesforce で ID を確認する必要があるときには、アプリケーションによって生成される確認コード (「時間ベースのワンタイムパスワード」とも呼ばれる) を使用します。セキュリティ強化のためにログイン時、接続済みアプリケーションへのアクセス時、またはレポートやダッシュボードへのアクセス時に 2 要素認証が必要な場合は、アプリケーションからコードを使用します。アプリケーションを接続する前に 2 要素認証が必要になった場合は、次に Salesforce にログインしたときにアプリケーションを接続するよう求められます。まだ 2 要素認証が必要でない場合は、引き続き個人設定からアプリケーションをアカウントに接続できます。

1. デバイスのタイプに応じて、サポートされる認証アプリケーションをダウンロードします。Salesforce Authenticator for iOS、Salesforce Authenticator for Android、Google Authenticator など、時間ベースのワンタイムパスワード (TOTP) アルゴリズム (IETF RFC 6238) をサポートしている認証アプリケーションであれば、どれでも使用できます。
2. [個人設定] から、［クイック検索］ボックスに「*高度なユーザの詳細*」と入力し、[高度なユーザの詳細] を選択します。結果が得られない場合は、［クイック検索］ボックスに「*個人情報*」と入力し、[個人情報] を選択します。
3. [アプリケーション登録: ワンタイムパスワードジェネレータ] を見つけ、[接続] をクリックします。
4. セキュリティ上の理由で、アカウントにログインするように要求されます。
5. モバイルデバイスで、認証アプリケーションを使用して QR コードをスキャンします。

   または、ブラウザで [QR コードをスキャンできません] をクリックすると、セキュリティキーが表示されます。認証アプリケーションで、ユーザ名と表示されたキーを入力します。
6. Salesforce で、認証アプリケーションによって生成されたコードを、[確認コード] 項目に入力します。

   確認コードは、認証アプリケーションによって定期的に新しく生成されます。現在のコードを入力します。
7. [接続] をクリックします。

アカウントの安全を確保するため、新しいID検証方法がSalesforceアカウントに追加されるたびに、メール通知が送信されます。自分がその方法を追加したか、Salesforceのシステム管理者が自分の代わりに追加したかに関係なく、メールは送信されます。

関連トピック:

Salesforce ヘルプ: Salesforce 環境のカスタマイズ

第 8 章　独自のブランドを使用したログインページのカスタマイズ

背景色、ロゴ、および右側の iFrame のコンテンツを追加して、カスタムドメインのログインページの外観を変更します。

ログインページの外観を変更する前に、[私のドメイン]を使用してドメインを設定する必要があります。詳細は、「クイックスタート:自分のドメインの設定、接続アプリケーションの追加、およびアプリケーションランチャーの使用」(ページ 5)を参照してください。

カスタムログインページを使用すると、会社のブランドに合わせたり、ユーザに追加情報を提供したり、組織を識別したりできます。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

使用可能なエディション: **Performance** Edition、**Unlimited** Edition、**Enterprise** Edition、**Developer** Edition、**Professional** Edition、および **Group** Edition

1. [設定] から、[クイック検索] ボックスに「*私のドメイン*」と入力し、[私のドメイン] を選択します。
2. [認証設定] で [編集] をクリックします。
3. ロゴをカスタマイズするには、画像をアップロードします。

   画像には、最大 100 KB の .jpg、.gif、または .png ファイルを使用できます。最大サイズは 250px × 125px です。
4. ログインページの背景をカスタマイズするには、 をクリックするか、有効な 16 進数の色コードを入力します。
5. iOS ユーザのために高度な認証方式をサポートするには、[iOS でのユーザ認証にネイティブブラウザを使用] を選択します。

   このオプションにより、iOS デバイスで Salesforce1 と Mobile SDK のアプリケーションを使用しているユーザのために、Kerberos、Windows NT LAN Manager (NTLM)、証明書ベースの認証などの認証方式がサポートされます。このオプションを選択すると、iOS デバイスのユーザは、カスタムドメインへのシングルサインオン認証を使用するときにネイティブブラウザにリダイレクトされます。他のオペレーティングシステムの場合、Salesforce1 や、Mobile SDK バージョン 3.1 以降を使用しているアプリケーションがモバイルデバイス管理 (MDM) ソフトウェアと統合されていれば、これらのアプリケーションで証明書ベースの認証を使用できます。
6. ログインページの右側の iFrame に入れるファイルの URL を入力します。

   右側の iFrame のコンテンツは、ページの約半分を占めるようにサイズ変更できます。SSL 暗号化と https:// 接頭辞を使用する URL にコンテンツをホストする必要があります。反応型 Web 設計を使用して右側の iFrame に独自のカスタムコンテンツページを作成するには、私のドメインサンプルテンプレートを使用します。

   例: `https://c.salesforce.com/login-messages/promos.html`
7. 必要に応じて、ログインページの ID プロバイダとして認証サービスを選択します (Google や Facebook のようなソーシャルサインオンプロバイダなど)。これにより、ユーザはソーシャルアカウントのログイン情報を使用してログインできるようになります。認証サービスを [設定] の [認証プロバイダ] として設定します。
8. [保存] をクリックします。

例: たとえば、[右フレームの URL] として *`https://sfdclogin.herokuapp.com/news.jsp`* を追加できます。

第 9 章 Identity Connect を使用した Salesforce と Active Directory のユーザの同期

トピック:

Identity Connect を使用して Active Directory から Salesforce 組織にユーザデータをアップロードして同期できます。

Identity Connect をインストールして設定すると、ユーザを管理および同期するための管理コンソールを利用できます。統合 Windows 認証 (IWA) と Kerberos を使用してシングルサインオンを設定することで、デスクトップ環境にサインインしたユーザは、別途ログインしなくても Salesforce を使用できるようになります。

Identity Connect をテストするには、Force.com トライアル組織にサインアップします。Developer Edition 組織と Force.com トライアル組織の違いについての詳細は、この FAQ を参照してください。

Identity Connect について

Identity Connect によって、Active Directory を統合できます。

Identity Connect は、Windows または Linux プラットフォームで実行するサービスを介して Active Directory と Salesforce のインテグレーションを実現します。このインテグレーションには、Salesforce にログインするときにシングルサインオン (SSO) Active Directory インテグレーション用の ID サービスプロバイダ (IDP) として機能する Identity Connect または Salesforce との Active Directory ユーザの同期が含まれます。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

有料オプションで使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition **Developer** Edition には 10 個の Identity Connect 権限セットライセンスが含まれます。

Identity Connect のインストール

組織に少なくとも 1 つの Identity Connect ライセンスが必要です。Identity Connect を取得するには、Salesforce にお問い合わせください。

通常、Identity Connect ソフトウェアは、IT 部門がサーバにインストールします。各ユーザが Identity Connect を個別にインストールする必要はありません。

1. [設定] から、[クイック検索] ボックスに「`Identity Connect`」と入力し、**[Identity Connect]** を選択します。

   メモ: **[Identity Connect]** は、組織にこの機能が追加されていない場合は [設定] には表示されません。

2. オペレーティングシステムに対応するダウンロードリンクをクリックします。
3. 『Salesforce Identity Connect Implementation Guide』に従ってソフトウェアをインストールします。

エディション

使用可能なエディション: Salesforce Classic と Lightning Experience の両方

有料オプションで使用可能なエディション: **Enterprise** Edition、**Performance** Edition、および **Unlimited** Edition **Developer** Edition には 10 個の Identity Connect 権限セットライセンスが含まれます。

ユーザ権限

Identity Connect をインストールする
- 「ユーザの管理」

第 10 章　チュートリアル: 外部 ID プロバイダからのシングルサインオンのテスト

トピック:

このチュートリアルでは、サードパーティ ID プロバイダからのシングルサインオン (SSO) を実装する方法と、そのプロバイダからの SAML アサーションをトラブルシューティングする方法を説明します。

Salesforce では、サードパーティ ID プロバイダの SSO がサポートされます。SSO を機能させるには、ID プロバイダとサービスプロバイダが SAML アサーションを使用して認証および承認情報を連携する必要があります。外部 ID プロバイダからの SSO の設定をテストし、SAML アサーションをトラブルシューティングするには、該当する手順を実行します。このチュートリアルが終了すると、外部アプリケーションから Salesforce 組織にログインできるようになります。

統合 ID を設定する

このシングルサインオン実装のために、Salesforce 組織と外部アプリケーション間をリンクするユーザ属性を設定します。

1. [設定] から、［クイック検索］ボックスに「ユーザ」と入力し、[ユーザ] を選択します。
2. 現在のユーザの横にある [編集] をクリックします。
3. [シングルサインオン情報] セクションの [統合 ID] に「`admin@universalcontainers.com`」と入力します。

   この例では、適宜、架空の統合 ID を作成します。統合 ID は、複数のアプリケーション間で共有できる、各ユーザの一意のユーザ名です。ユーザの従業員 ID を使用する場合もあります。統合 ID で重要なのは、1 つの Salesforce 組織内の複数のユーザ間で重複しないことです (複数の Salesforce 組織で同じユーザに同じ統合 ID を設定することはできます)。
4. [保存] をクリックします。

ID プロバイダを設定する

ID プロバイダを設定する手順を実行するには、Heroku でホストされているシングルサインオンテストアプリケーションの Axiom を使用します。

Axiom アプリケーションから ID プロバイダ証明書を取得し、Salesforce 組織に設定します。

ヒント: Axiom アプリケーションと DE 組織をそれぞれ別のブラウザウィンドウで開いたままにし、2 つの間で簡単に切り取りと貼り付けができるようにします。

1. 新しいブラウザウィンドウで http://axiomsso.herokuapp.com にアクセスします。
2. [SAML Identity Provider & Tester (SAML ID プロバイダ & テスタ)] をクリックします。
3. [Download the Identity Provider Certificate (ID プロバイダの証明書をダウンロード)] をクリックします。

   証明書によって署名が検証されたら、証明書を Salesforce 組織にアップロードする必要があります。保存場所を覚えておいてください。
4. Salesforce 組織で、[設定] から［クイック検索］ボックスに「*シングルサインオン設定*」と入力し、[シングルサインオン設定] を選択します。
5. [編集] をクリックします。
6. [SAML を有効化] を選択します。
7. [保存] をクリックします。
8. [SAML シングルサインオン設定] で、[新規] をクリックします。
9. 次の値を入力します。
   a. 名前: `Axiom Test App`
   b. 発行者: `http://axiomsso.herokuapp.com`
   c. ID プロバイダの証明書: ステップ 3 でダウンロードしたファイルを選択します。

d. 証明書署名要求: 証明書を選択します。使用できる証明書がない場合は、`Generate self-signed certificate` を選択します。

e. SAML ID 種別: [アサーションには、ユーザオブジェクトの統合 ID が含まれます] を選択します。

f. SAML ID の場所: [ID は、Subject ステートメントの NameIdentifier 要素にあります] を選択します。

g. サービスプロバイダの起動要求バインド: [HTTP リダイレクト] を選択します。

h. エンティティ ID: [私のドメイン] の名前を「https」も含めて入力します (*`https://universalcontainers.my.salesforce.com`* など)。

10. [保存] をクリックし、ブラウザのページは開いたままにしておきます。

SAML を生成する

Axiom は、割り当てられた統合 ID を使用して Salesforce 組織にログインするための SAML アサーションを生成します。

ヒント: Axiom アプリケーションと DE 組織をそれぞれ別のブラウザウィンドウで開いたままにし、2 つの間で簡単に切り取りと貼り付けができるようにします。

1. Axiom (http://axiomsso.herokuapp.com) に戻ります。
2. [Generate a SAML Response (SAML レスポンスを生成)] をクリックします。
3. 次の値を入力します (他の項目は空白のままでもかまいません)。
   a. SAML 2.0
   b. ユーザ名または統合 ID: *`admin@universalcontainers.com`*
   c. 発行者: *`http://axiomsso.herokuapp.com`*
   d. 受信 URL: Salesforce SAML の [シングルサインオン設定] ページから取得します (ページを閉じてしまった場合は、[設定] から [クイック検索] ボックスに「*シングルサインオン設定*」と入力し、[シングルサインオン設定] を選択し、[Axiom Test App (Axiom テストアプリケーション)] をクリックします)。[Salesforce ログイン URL] の値を使用します。
   e. エンティティ ID: こちらも Salesforce [SAML シングルサインオン設定] から取得します。
4. Axiom に戻り、[Request SAMLResponse (SAMLResponse を要求)] をクリックします。
   Axiom が SAML アサーションを生成します。
5. [ログイン] をクリックします。
   Axiom アプリケーションは、割り当てられた統合 ID を使用して、Salesforce 組織にユーザとしてログインします。

SAML アサーションをトラブルシューティングする

Salesforce SAML 検証を使用して、SAML アサーションをテストおよび修正します。

クイックスタートの手順を実行しているとき、Axiom アプリケーションで組織へのログインが行われない場合は、Salesforce SAML 検証を使用して SAML アサーションをトラブルシューティングできます。SAML アサーションのトラブルシューティング中、Axiom アプリケーションをブラウザウィンドウで開いたままにします。Axiom を再度開く必要がある場合は、http://axiomsso.herokuapp.com にアクセスします。

1. Salesforce 組織で、[設定] から［クイック検索］ボックスに「*シングルサインオン設定*」と入力し、[シングルサインオン設定] を選択します。
2. **[SAML アサーション検証]** をクリックします。

   +SAML 検証に、最後に記録された SAML ログインエラーとエラーの理由を説明する詳細が表示されます。
3. Axiom アプリケーションからの SAML アサーションをテストするには、Axiom アプリケーションから **[Formatted SAML Response (書式化された SAML レスポンス)]** をコピーします。
4. Salesforce SAML 検証で、ページ下部にある **[SAML レスポンス]** ボックスに SAML アサーションを貼り付けます。
5. **[検証]** をクリックします。

   ページに、アサーションのトラブルシューティングに役立つ結果が表示されます。たとえば、アサーションが生成されてからログインに使用されるまでしばらく時間が空いた場合、タイムスタンプの有効期限が切れてログインが無効になります。その場合は、SAML アサーションを再生成して再試行してください。

第 11 章 アプリケーションの監視とレポートの実行

トピック:

接続アプリケーションを監視し、アプリケーションの利用状況をユーザ、アプリケーション、時間、またはその他の値別に追跡するレポートを設定します。

Identity ユーザの接続アプリケーションを設定した後は、組織全体の接続アプリケーションの利用状況監視、アプリケーションの使用頻度調査、アプリケーションの詳細にドリルダウンして接続アプリケーション設定の変更、セキュリティニーズの変化に応じた特定のアプリケーションのブロックまたはブロック解除を行うことができます。

接続アプリケーションの利用状況を監視する

エディション

使用可能なエディション: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

システム管理者は、組織の [接続アプリケーションの OAuth の利用状況] ページでインストール済み接続アプリケーションの利用状況を監視できます。

組織内の任意の接続アプリケーションの利用状況に関する情報を表示するには、[設定] から［クイック検索］ボックスに「*接続アプリケーションの OAuth の利用状況*」と入力し、[接続アプリケーションの OAuth の利用状況] を選択します。接続アプリケーションと各アプリケーションに関する情報のリストが表示されます。

接続アプリケーション
: アプリケーションの名前。インストール済みであってもまだ使用されていない接続アプリケーションは、リストに表示されません。

アプリケーション情報を参照
: [アプリケーション情報を参照] をクリックすると、接続アプリケーションの詳細ページに移動します。または、接続アプリケーションがまだインストールされていない場合は、[インストール] をクリックします。

ユーザ数
: アプリケーションを実行したことがあるユーザの数。[ユーザ数] の値をクリックすると、各ユーザに関する次のような情報が表示されます。

  - アプリケーションを初めて使用した日時
  - アプリケーションを最後に使用した日時
  - アプリケーションを使用した回数の合計

  接続アプリケーションユーザの [利用状況] ページで、そのユーザの行にある [取り消し] アクションをクリックすると、現在のセッションへのユーザのアクセスを終了できます。または、ページの上部にある [すべて取り消し] ボタンをクリックすると、現在接続アプリケーションを使用している全ユーザをログアウトさせることができます。

アクション
: [ブロック] をクリックすると、接続アプリケーションを使用する現在のすべてのユーザセッションが終了し、すべての新しいセッションがブロックされます。アプリケーションのブロックは永続的ではありません。[ブロック解除] をクリックして、ユーザが次回アプリケーションにログインし、アクセスできるようにできます。

Identity ユーザのレポートを作成する

エディション

使用可能なエディション: Salesforce Classic

使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、**Developer** Edition、および **Database.com** Edition

Salesforce で管理されている ID イベントログを使用して、システム管理者はレポートやダッシュボードを作成し、そこからシングルサインオンと接続アプリケーションの利用状況に関する特定の情報にドリルダウンできます。

次の手順では、Identity ユーザのレポートを設定します。同じレポートタイプの複数のバリエーションを設定する場合や、レポートのダッシュボードを作成する場合にも、同じ手順を使用します。ダッシュボードについての詳細は、Salesforce ヘルプの「ダッシュボードの使用開始」を参照してください。

新しいレポートタイプを設定する

1. [設定]から、[クイック検索] ボックスに「*レポートタイプ*」と入力し、[レポートタイプ] を選択します。
2. [新規カスタムレポートタイプ] をクリックします。
3. 次の値を入力します。
   a. 主オブジェクト: [ユーザ]
   b. レポートタイプの表示ラベル: 固有の表示ラベル (「*Identity Users (Identity ユーザ)*」など)。
   c. レポートタイプ名: この項目には自動的に表示ラベルが使用されます。別の名前にする場合は変更します。
   d. 説明: 他のユーザが見てわかりやすい説明を入力します。
   e. カテゴリに格納: このレポートのカテゴリを選択します ([管理レポート] など)。
   f. リリース状況:他のユーザが表示できるようにこのレポートをリリースする準備ができるまで、[開発中] のままにします。
4. [次へ] をクリックします。
5. [クリックして他のオブジェクトと関連付ける] を選択します。
6. [ID イベントログ (ユーザ)] を選択します。
7. [保存] をクリックします。

レポートを作成する

1. [レポート] タブをクリックします。
2. [新規レポート...] をクリックします。
3. [管理レポート] で、[Identity Users (ID ユーザ)] を選択します。
4. [作成]をクリックします。
5. 必要に応じて項目をレポートにドラッグアンドドロップします。

   たとえば、このレポートに役立つ項目として、*ユーザ名*、*ユーザ ID*、*アプリケーション*：*接続アプリケーション名*、*タイムスタンプ*、*利用状況の種別*があります。
6. [保存] をクリックします。

7. **レポート名を入力します**(「*Identity Connected App Usage (Identity 接続アプリケーション利用状況)*」など)。
8. **[保存] をクリックします**(または **[レポートを保存して実行] をクリックしてすぐに結果を表示します**)。

第 12 章　External Identity を使用した新規ユーザへの組織の拡張

External Identity は、お客様やパートナーに低コストの Identity and Access Management (IAM) サービスを提供する新しい種類の Salesforce ライセンスです。このライセンスは、カスタマーコミュニティやパートナーコミュニティライセンスにアップグレードできます。

External Identity ライセンスによって、カスタマーコミュニティライセンスを使用することなく、柔軟にコミュニティサイトにユーザを追加できます。External Identity ライセンスは、カスタマーコミュニティライセンスより低コストでユーザを追加できます。ただし、ケースやナレッジなど、コミュニティの重要な機能にはアクセスできません。これらのユーザの保存および管理、ユーザ名とパスワード、シングルサインオン、ソーシャルサインオン (Facebook、Google+、LinkedIn、その他の認証プロバイダの ID を使用) による認証を行います。新規ユーザの効率的なプロビジョニングのためにユーザにセルフ登録を許可します。これらのユーザは通常、ビジネスの利用者、パートナー、販売店、患者、およびその他の顧客です。

次の表に、External Identity ライセンスとカスタマーコミュニティライセンスを持つユーザが使用できる機能を示します。

機能	External Identity	カスタマーコミュニティ
取引先	✓ 参照、編集	✓ 参照、編集
納入商品	✓ 参照、作成、編集	✓ 参照、作成、編集
Chatter	✓	✓
取引先責任者	✓ 参照、作成、編集	✓
ID	✓	✓
ケース		✓ 自分のケースの作成と管理が可能
商品		✓ 参照のみ
注文		✓

エディション

使用可能なエディション: Salesforce Classic

External Identity ライセンスを使用可能なエディション: **Enterprise** Edition、**Performance** Edition、**Unlimited** Edition、および **Developer** Edition

ユーザ権限

External Identity ユーザを割り当ておよび管理する
- 「ユーザの管理」

コミュニティを有効化する
- 「アプリケーションのカスタマイズ」

機能	External Identity	カスタマーコミュニティ
ファイル	✅	✅
Chatter アンサー		✅
アイデア		✅
ナレッジ		✅ 参照のみ
ToDo		✅ 参照のみ
カスタムオブジェクト	✅ ライセンスあたりに2個のカスタムオブジェクト (管理パッケージ内のカスタムオブジェクトは、この制限にカウントされません)	✅ ライセンスあたりに 10 個のカスタムオブジェクト (管理パッケージ内のカスタムオブジェクトは、この制限にカウントされません)
メモと添付ファイル		✅ メモ: [メモと添付ファイル]関連リストは、取引先と取引先責任者で使用できません。
追加ストレージ	150 MB (25,000 個の有効なユーザライセンス) 2 GB (250,000 個の有効なユーザライセンス) 10 GB (1,000,000 個の有効なユーザライセンス) 60 GB (5,000,000 個の有効なユーザライセンス)	

コミュニティ内の External Identity ライセンスユーザ数が 1 か月に 1000 万ユニークユーザを超えないようにすることをお勧めします。この制限を超えて追加のユーザライセンスが必要な場合は、Salesforce のアカウントエグゼクティブにお問い合わせください。この制限を超えると、追加料金および機能の低下が生じる可能性があります。

コミュニティを設定して External Identity ライセンスユーザをサポートする方法についての詳細は、『Salesforce Communites 実装ガイド』および『Community Templates for Self-Service Implementation Guide』を参照してください。

第 13 章　Salesforce Identity、シングルサインオン、およびセキュリティに関する詳細情報の取得

Salesforce Identity に関する詳細情報のソースへのリンクです。

Salesforce Identity では、ポータルアクセス用に外部 ID もサポートします。また、パートナーや顧客を Identity ユーザとして有効化できます。外部 ID の使用方法についての詳細は、以下を参照してください。

次のリンクから役に立つ関連リソースを参照できます。

- Salesforce Identity Web ページ
- Salesforce Identity の「How-to」動画
- Security Single Sign-On Implementation Guide (セキュリティシングルサインオン実装ガイド) [PDF]
- 『Force.com REST API 開発者ガイド』の「認証について」
- Salesforce Identity Connect User Guide (Salesforce Identity Connect ユーザガイド)
- developer.salesforce.com Identity のホームページ
- Salesforce セキュリティ早見表