As an admin, you walk a fine line between making sure that your Salesforce org is secure and that your users can log in quickly and easily. The most effective way to protect your org and its data is to require that users provide more than just their username and password. Security experts call this multi-factor authentication, or MFA for short.

**What Is Multi-Factor Authentication?**

By the way, you may be more familiar with the terms two-factor authentication or 2FA. Not to worry! While 2FA is a subset of MFA, we’re effectively talking about the same thing.

So, what exactly are the multiple factors? They’re different types of evidence that users provide when logging in to confirm their identity.

* One factor is something users know. For Salesforce logins, that's a username and password combination.
* Other factors are verification methods that a user has in their possession, such as a mobile device with an authenticator app installed or a physical security key.

**How Multi-Factor Authentication Works**

MFA adds an extra step to your Salesforce login process.

1. A user enters their username and password, as usual.
2. Then the user is prompted to provide one of the verification methods that Salesforce supports.

You can allow any or all of these verification methods:

|  |  |
| --- | --- |
| Salesforce Authenticator | A free mobile app that integrates seamlessly into your login process. Users can quickly verify their identity via push notifications. We’ll talk more about this app in a bit. |
| Third-party TOTP authenticator apps | Apps that generate unique, temporary verification codes that users type in when prompted. This code is sometimes called a time-based one-time password, or TOTP for short. Users can pick from a wide variety of options, including Google Authenticator, Microsoft Authenticator, or Authy. |
| Security keys | Small physical tokens that look like a thumb drive. Logging in with this option is fast and easy — users simply connect the key to their computer then press the key’s button to verify their identity. Users can use any key that’s compatible with the FIDO Universal Second Factor (U2F) standard, such as Yubico’s YubiKey or Google’s Titan Security Key. |

## Turn On Multi-Factor Authentication for Every Login

**Step 1: Verify that the session security level is set for multi-factor authentication**

First, let’s make sure that the right security level is associated with the multi-factor authentication login method.  In most production orgs, this setting is already in place. But if it’s not, it’s important to do this step before you set up an MFA requirement for any admin users. Otherwise, you could prevent yourself or other admins from logging in.

1. From Setup, enter Session Settings in the Quick Find box, then select **Session Settings**.
2. Under Session Security Levels, make sure that Multi-Factor Authentication is in the High Assurance category.

**Step 2: Create a user**

1. From Setup, enter Users in the Quick Find box, then select **Users**.
2. Click **New User**.
3. For the first name and last name, enter Sia and Thripio, respectively.
4. Enter *your* email address in the Email field. This setting is to get user notifications for Sia.
5. Create a username for Sia and enter it in the Username field. It must be in email address format, but it doesn’t have to be a working email address. Make sure the email address is unique in your Trailhead Playground. We’re going to use Sia's first initial, last name, and current date in the username like this: SThripio.12202020@jedeye-tech.com.
6. Edit or accept the nickname value.
7. For User License, select **Salesforce Platform**.
8. For Profile, select **Standard Platform User**. While you’re here, deselect the options to receive Salesforce CRM content alerts. No need to clutter your inbox with unnecessary email from Salesforce.
9. Make sure that **Generate new password and notify user immediately** is selected—it’s way down at the bottom of the page. Salesforce emails you about Sia’s new user because you entered your email address in the Email field.
10. Click **Save**. Salesforce emails you a link to verify the user and set Sia’s password.  
    **Note:** If you get an error that the username exists, create a user with a different name.
11. Log in as Sia, and reset the password.

After you set the password,  it’s time to enable MFA for Sia’s user account.

**Step 3: Create a permission set for multi-factor authentication**

Enable MFA for users by assigning the **Multi-Factor Authentication for User Interface Logins** user permission. You can do this step by editing profiles or by creating a permission set that you assign to specific users.

A permission set is a collection of settings and permissions that gives users access to various Salesforce features. Let’s create a permission set with the MFA permission.

1. If you’re logged in as Sia, log out. Log in again as the system administrator of your Trailhead Playground.
2. From Setup, enter Permission in the Quick Find box, then select **Permission Sets**.
3. Click **New**.
4. Label the permission set “MFA Authorization for User Logins”.
5. Click **Save**.
6. Under System, click **System Permissions**.
7. Now you’re on the detail page for the MFA Authorization for User Logins permission set.
8. Click **Edit**.
9. Select **Multi-Factor Authentication for User Interface Logins**.
10. Click **Save,**then click **Save** again to confirm permission changes.

 You’re almost there! You just need to assign the permission set.

**Step 4: Assign the permission set to Sia’s user**

For now, we’ll assign the permission set just to Sia. Later, when you’re ready to roll out MFA more broadly, you can assign the same permission set to other users.

If you’re not on the detail page for your new permission set, navigate back there.

1. On the detail page of the new permission set, click **Manage Assignments**.
2. Click **Add Assignments**. On the list of users, select the checkbox next to Sia’s user. (If you wanted, you could assign up to 1,000 users at a time.)
3. Click **Assign**.

**What Is My Domain?**

My Domain is sort of like creating your own empire within the Salesforce universe. It’s a Salesforce Identity feature that lets you personalize your Salesforce org by creating a subdomain (empire) within the Salesforce domain (universe).

How’s that? If your Salesforce org was created before Winter ’21, your users access your org through the instance URL that Salesforce assigns you, such as https://na30.salesforce.com. With My Domain, you give your users a nifty, personalized way to access Salesforce. Instead of the meaningless https://na30.salesforce.com URL, your URL can look like https://somethingReallycool.my.salesforce.com where:

* somethingReallycool Equals your My Domain: your personal subdomain within the Salesforce domain. Typically, it's your company name or whatever drives your brand.
* my.salesforce.com is the Salesforce domain name—domain, for short. My Domain login URLs all belong to this same domain.

Having a My Domain isn’t just about convenience and branding an org’s login experience. It's about having more control over your login process and simplifying authentication. In fact, Salesforce requires you to have a My Domain in place to:

* Work in multiple Salesforce orgs in the same browser
* Set up single sign-on (SSO) with external identity vendors
* Set up authentication providers, such as Google and Facebook, so that your users can log in to your Salesforce org with their social account credentials
* Use Lightning components in Lightning component tabs, Lightning page, the Lightning App Builder, or standalone apps

Because having a My Domain is so important, all production and Developer Edition orgs created in Winter ’21 and later get one by default.

## Create a My Domain

If your Developer Edition was created before the Winter ’21 release, the address bar shows that your new org uses an instance URL, such as https://na30.lightning.force.com. (If you just created a new Developer Edition org, My Domain is already enabled.)

1. From Setup, enter My Domain in the Quick Find box, then select **My Domain**.
2. Enter the name for your subdomain. Choose something fun that’s also unique.

**NOTE:** If you see "My Domain Settings" instead of "My Domain Step 1", then your org already has a deployed My Domain—probably because it was created in Winter ’21 or later. To rename your My Domain in a production org, click **Edit** in My Domain Settings. You can't rename the My Domain in your Developer Edition org, though. So jump ahead to After Deployment: Set My Domain Policies.

1. Click **Check Availability**. Salesforce checks whether this My Domain name is already in use.
2. When you get the green light (3), click **Register Domain** (4).
3. Sit back and watch for an email telling you that the process completed. Behind the scenes, Salesforce prepares your org's My Domain and updates its domain name registries.

## Test and Deploy Your My Domain

1. From the email you receive, click the link to get back to the My Domain wizard.
2. The link takes you to your Salesforce org. Notice the URL in the browser address bar shows your new My Domain name.
3. Click **Log in** to continue setting up My Domain. Enter the username and password you used when you signed up for your org.
4. Pretend that we’ve completed testing links. It’s time to make your My Domain available to all the users in your org.
5. Click **Deploy to Users**, and then click **OK**. Deploying a My Domain rolls out the new URL throughout your org. Now all your users see the My Domain URL in their browser address bar.  
   **Note:** This step is often overlooked, especially when you’re interrupted while working on this module. If you walked away, get yourself back to My Domain. From Setup, enter My Domain in the Quick Find box, then select **My Domain**. Salesforce takes you to the step in the My Domain wizard where you left off. If you’re still at Step 3, click **Deploy to Users**.
6. Click **OK**.

## After Deployment: Set My Domain Policies

1. If you’re not looking at the My Domain page, from Setup, enter My Domain in the Quick Find box, then select **My Domain**.
2. Under My Domain Settings, click **Edit**. Set login policies to control what happens when users try to log in from your old URL instead of from My Domain.
3. For now, keep the default settings, but let’s review the options.  
   **Login Policy**—You can require users to log in using your My Domain login page. This prevents users from attempting to log in with the generic https://login.salesforce.com/ URL.  
   **Redirect Policy**—You can choose between three redirect policies. That is, if someone selects a bookmark such as https://na30.salesforce.com, we redirect them to the My Domain equivalent.
   1. **Redirect to the same page within the domain**. Let users continue to log in from your URL as well as your My Domain login URL. This option might be convenient, but it’s like nothing has changed.
   2. **Redirected with a warning to the same page within the domain**. Reminds users to use your My Domain login URL when logging in. Yet it still redirects them to your org. This option is good for a few days after you deploy your My Domain to help users transition to your org's new login URL.
   3. **Not redirected**. Requires users to use your My Domain login URL when accessing your org. The training wheels are off. Expect that your users have transitioned to using the My Domain login URL. If they haven’t, they get an error when they try to use your instance URL or login in from login.salesforce.com.
4. **Rename your My Domain** lets you rename your My Domain, for example, if your company’s name or branding changes.

## Single Sign-On

With a custom domain and login page, you make it easy for employees to log in to your Salesforce org with a secure, easy-to-remember URL.

Do you want to make it even easier so that they don’t have to log in at all? Then set up single sign-on (SSO).

SSO has lots of advantages.

* You spend less time managing passwords.
* Your employees save time when they don’t have to manually log in to Salesforce. Did you know that users take 5–20 seconds to log in to an online application? Those seconds add up.
* More people use Salesforce. Users can send out links to Salesforce records and reports, and their recipients can open them in a single click.
* You can manage access to sensitive information from one place.

## Configure Inbound SSO with a Third-Party Identity Provider

Is this starting to sound difficult? It’s not, really. Let’s break it down into simple steps.

1. Create a Federation ID for each user.
2. Set up SSO settings in Salesforce.
3. Set up Salesforce settings in the SSO provider.
4. Make sure it all works.

## Step 1: Create a Federation ID

1. From Setup, enter Users in the Quick Find box, then select **Users**.
2. Click **Edit** next to Sia’s name.
3. Under Single Sign On Information, enter the Federation ID: sia@jedeye-tech.com. **Tip** : A Federation ID must be unique for each user in an org. That’s why the username is handy. But if the user belongs to multiple orgs, use the same Federation ID for the user in each org.
4. Click **Save**.

## Step 2: Set Up Your SSO Provider in Salesforce

**Tip** : You’re going to work in both your Salesforce Dev org and the Axiom app. Keep them open in separate browser windows so that you can copy and paste between the two.

1. In a new browser window, go to [http://axiomsso.herokuapp.com](http://axiomsso.herokuapp.com/Home.action).
2. Click **SAML Identity Provider & Tester**.
3. Click **Download the Identity Provider Certificate**. You upload this certificate later to your Salesforce org, so remember where you save it.
4. In your Salesforce org, from Setup, enter Single in the Quick Find box, and then select **Single Sign-On Settings**.
5. Click **Edit**.
6. Select **SAML Enabled**.
7. Click **Save**.
8. In SAML Single Sign-On Settings:
   1. Click **New**.
   2. Enter the following values.
      * Name: Axiom Test App
      * Issuer: http://axiomsso.herokuapp.com
      * Identity Provider Certificate: Choose the file you downloaded in step 3.
      * Request Signature Method: Select **RSA-SHA1**.
      * SAML Identity Type: Select **Assertion contains the Federation ID from the User object**.
      * SAML Identity Location: Select **Identity is in the NameIdentifier element of the Subject statement**.
      * Service Provider Initiated Request Binding: Select **HTTP Redirect**.
      * Entity ID: Enter your My Domain name, which you can copy from the subdomain name that you set up in the “Customize Your Login Process with My Domain” unit. Make sure that entity ID includes "https" and references the Salesforce domain. It should look something like this: https://mydomain-dev-ed.my.salesforce.com.
9. Click **Save** and leave the browser page open.

## Step 3: Link Your Identity Provider to Salesforce

1. Return to the Axiom web app. If you don’t have the app open in a browser window, go to [http://axiomsso.herokuapp.com](http://axiomsso.herokuapp.com/Home.action).
2. Click **SAML Identity Provider & Tester**.
3. Click **generate a SAML response**.
4. Enter the following values. Leave the other fields as is.
   * SAML Version: 2.0
   * Username or Federated ID: The Federation ID from the Sia's Salesforce User page
   * Issuer: http://axiomsso.herokuapp.com
   * Recipient URL: The URL from the Salesforce SAML Single Sign-On Settings page. Don’t see it? It’s at the bottom labeled **Salesforce Login URL**.
   * Entity Id: The Entity ID from the Salesforce SAML Single Sign-On Settings page

## Step 4: Make Sure It All Works

OK, now that everything’s all configured, let’s make sure that it works. What’s the proof? A successful login, of course.

1. In the Axiom settings browser window, click **Request SAML Response**. (It’s way down at the bottom.)
2. Axiom generates the SAML assertion in XML. Does it look like language used by a robot communicating with desert outpost moisture evaporators? Look again. You can see that it doesn’t look all that bad. To get to the interesting information, scroll through the XML.
3. Click **Login**.

If everything’s OK, you’re logged in as Sia at your Salesforce home page. The Axiom application logs you in to your Salesforce org as the user with the assigned Federation ID.