Oracle Eloqua and Salesforce SSO

Configuration Guide

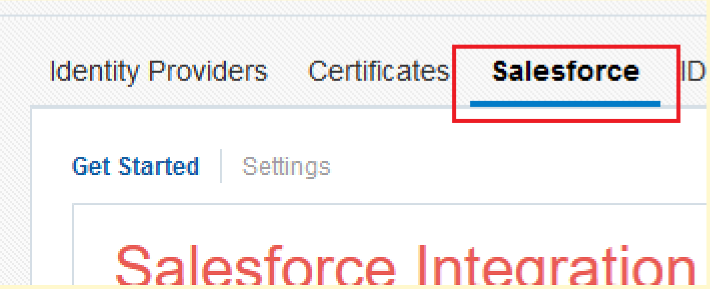
26-Jun-2024

Contents

Salesforce native SSO integration

☪

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



Using the Salesforce native SSO integration, you can enable single sign-on and automatically synchronize your Salesforce users with Oracle Eloqua.

In this setup, Salesforce is the identity provider and Oracle Eloqua is the service provider. Oracle Eloqua uses SAML 2.0 token authentication to allow users to access Oracle Eloqua using their Salesforce login credentials.

↖**Note**: Oracle Eloqua Identity Cloud Service for Salesforce only supports SHA-1 signed certificates.

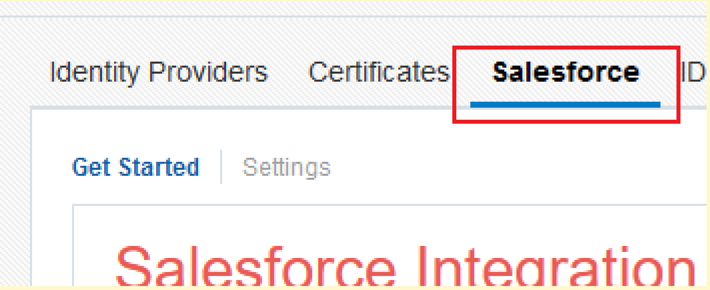
About service providers and identity providers

When planning to enable single sign-on, it is important to understand a few terms:

- Service Provider: A website that hosts applications. When you enable single sign-on, Oracle Eloqua is the service provider.
- Identity Provider: A trusted provider that can authenticate users and allow single sign-on to access other websites. The identity provider is your single sign-on vendor, in this case Salesforce.

Steps to enable Salesforce native SSO integration

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



As an administrator, you can enable single sign-on (SSO) for your Oracle Eloqua users. Single sign-on allows users to login to Oracle Eloqua with their Salesforce login credentials.

Enabling SSO requires you configure Oracle Eloqua and Salesforce. To complete the configuration, you will need administrative access to Salesforce and Oracle Eloqua.

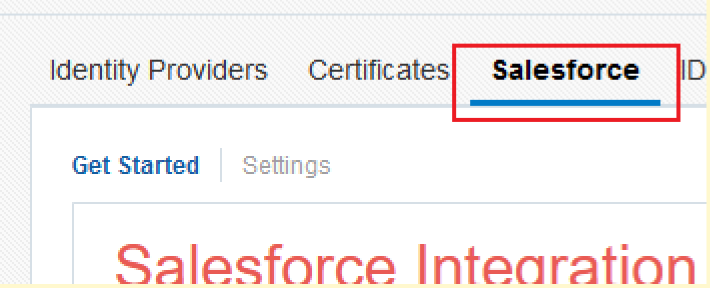
The following table shows the steps required to configure single sign-on with Salesforce.

Step	Description
Preliminary setup	In Salesforce, you must enable Salesforce as an identity provider and download the identity provider metadata. See Preliminary Salesforce setup for Salesforce native SSO integration.
Configure Oracle Eloqua as a connected app	Gather the information you need from Oracle Eloqua and then set up Oracle Eloqua as a SAML connected app in Salesforce. See Configuring Oracle Eloqua as a connected app for native SSO integration.
Configure the Salesforce single sign-on	Configure Salesforce as an identity provider in Oracle Eloqua by uploading metadata from Salesforce and configure an integration user to communicate with Salesforce. Configuring the Salesforce native SSO integration
Map Salesforce profiles to security groups	Map your Salesforce profiles to Oracle Eloqua security groups. See Mapping Salesforce profiles to Eloqua security groups for Salesforce native SSO integration and About synchronizing Salesforce users with Oracle Eloqua using the native SSO integration.
Test the setup	Test single sign-on access to Oracle Eloqua. See Testing Salesforce native SSO integration.

Preliminary Salesforce setup for Salesforce native SSO integration

☪

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



Before enabling sign-on with Salesforce, you first need to enable Salesforce as an identity provider.

The following steps outline the process to enable Salesforce as an identity provider, but for full details you should refer to the Salesforce help Enable Salesforce as an Identity Provider.

Note: Oracle Eloqua Identity Cloud Service for Salesforce only support SHA-1 signed certificates.

To enable Salesforce as an identity provider:

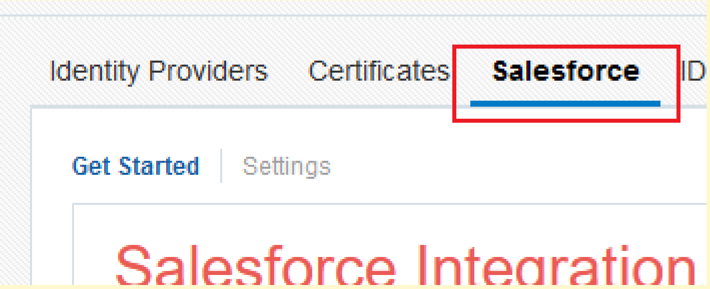
1. Choose an option:

Task	Option
If Salesforce is not already enabled as an identity provider	a. Set up a subdomain for your Salesforce instance and deploy it to your Salesforce users. This is a unique domain used only by your organization and is required before you can enable single sign-in using Salesforce. b. Enable Salesforce as an identity provider. c. Download the SAML metadata associated with your new identity provider. Later you will upload this to Oracle Eloqua.
If Salesforce is enabled as an identity provider	a. Download the SAML metadata associated with your new identity provider. Later you will upload this to Oracle Eloqua.

After you finish: Continue to Configuring Oracle Eloqua as a connected app for native SSO integration.

Configuring Oracle Eloqua as a connected app for native SSO integration

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



After you completed the preliminary Salesforce setup, you must configure Oracle Eloqua as a service provider. In Salesforce, service providers are configured by creating a SAML enabled connected app. The connected app identifies Oracle Eloqua as a trusted service provider and allows Salesforce and Oracle Eloqua to communicate with each other.

Before you begin:

When configuring the connect app, you’ll need to the following information from Oracle Eloqua:

- Oracle Eloqua's assertion consumer service (ACS) URL.
- Oracle Eloqua's entity ID that is unique for your instance.
- If you plan to allow Oracle Eloqua to initiate logins, you must download Oracle Eloqua's certificate.

To gather the information you need from Oracle Eloqua:

1. In Oracle Eloqua, click **Settings** ⚙.
2. Click **Single Sign-On** in the *Users and Security* area.
3. Click the **Salesforce** tab and then click the **Get Started** tab.
4. Click **Configuration Information** and copy the information provided.
5. If you plan to allow Oracle Eloqua to initiate login, click **Download Eloqua Certificate**.

To configure Oracle Eloqua as a SAML enabled connected app:

1. Gather the information you need from Oracle Eloqua.
2. In Salesforce, create a new SAML enabled connected app for Oracle Eloqua. For more information, see the Salesforce documentation.

   Use the following information when configuring the connected app:

Field	Setting
Entity ID	The entity ID you gathered earlier
ACS URL	The ACS URL you gathered earlier
Subject Type	Username
Name ID Format	Leave as default
Issuer	Leave as default
Enable SAML	Turn this setting on
Verify Request Signatures	If you plan to allow Oracle Eloqua to initiate logins, select this option and upload the certificate from Oracle Eloqua.

3. After creating the connected app, authorize users for Oracle Eloqua application. Later you define in Oracle Eloqua what access these users can have based on their profile.

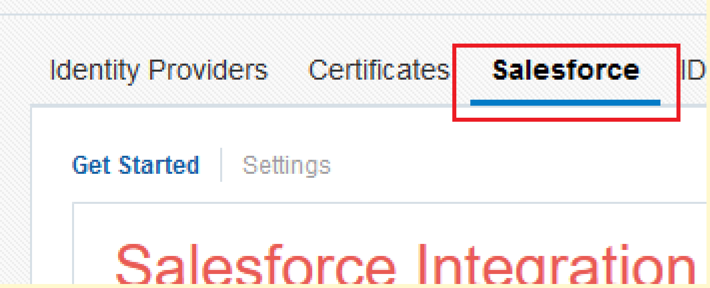
> ⦿ **Tip**: If you want to test the connection before authorizing all users, select only the Salesforce profiles that you want to use for testing purposes.

After you finish: Continue to Configuring the Salesforce native SSO integration.

Configuring the Salesforce native SSO integration

☪

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



After enabling Salesforce as an identity provider, you can upload the Salesforce metadata file and configure the connection to Salesforce.

Before you begin:

- You will need the SAML metadata file that you downloaded from Salesforce. See Preliminary Salesforce setup for Salesforce native SSO integration for more information.

- Identify the Salesforce account that will be used to synchronize user accounts. This could be the same user set up for the CRM integration. This user must have access to the User Entity and Profile Entity in Salesforce.

Uploading the Salesforce SAML metadata to Oracle Eloqua

Upload the Salesforce SAML metadata to start the single sign-on configuration process.

To upload the Salesforce SAML metadata to Oracle Eloqua:

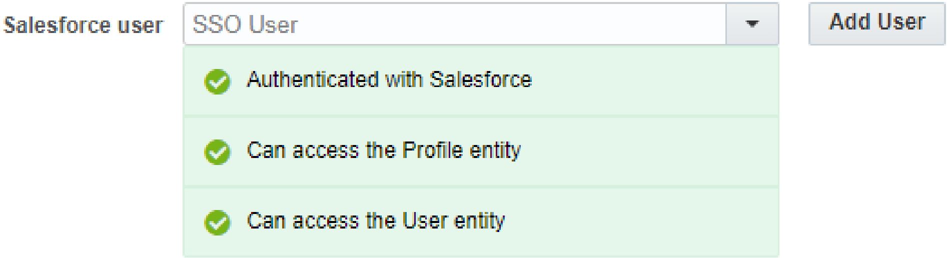
1. Click **Settings** ⚙.
2. Click **Single Sign-On** in the *Users and Security* area.
3. Click the **Salesforce** tab.
4. On the **Get Started** tab, click **Upload Salesforce metadata file** in step 2 and upload the metadata file you downloaded earlier. After the upload completes, a confirmation appears and the *Settings* tab opens. If this tab does not open, open it so that you can continue the setup below.

Setting up the Salesforce integration user

The integration user is used to connect to and communicate with Salesforce. This is usually the same user set up for the CRM integration. This user must have access to the user entity and profile entity in Salesforce.

To setup the Salesforce integration user and security profile mappings:

1. In the *Single Sign-On* area of Oracle Eloqua, click the **Salesforce** tab, and then click the **Settings** tab.
2. Select the Salesforce user that Oracle Eloqua authenticates with from the **Salesforce user** list.
3. After you select a user, Oracle Eloqua verifies that the user can authenticate with Salesforce, access the user entity and access the profile entity and shows you the results of the tests.



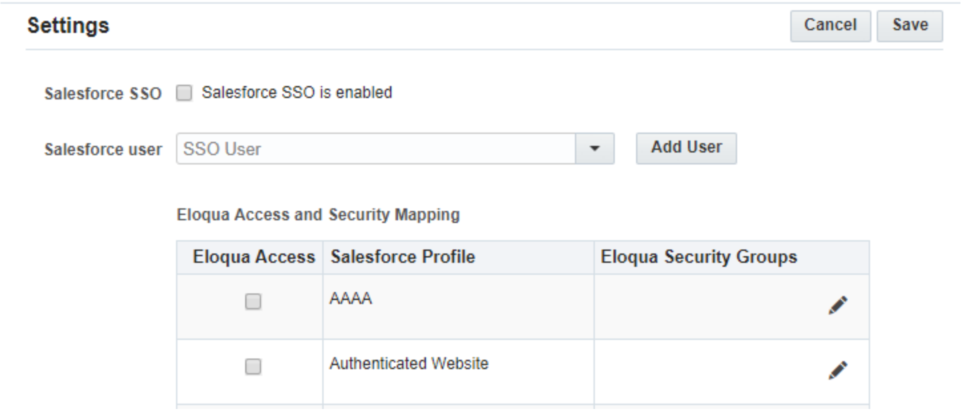
Salesforce user: SSO User

✓ Authenticated with Salesforce

✓ Can access the Profile entity

✓ Can access the User entity

4. Click **Save**. The window refreshes and shows the *Eloqua Access and Security Mapping* settings. This is a listing of the Salesforce profiles available.



Settings

Salesforce SSO: □ Salesforce SSO is enabled

Salesforce user: SSO User

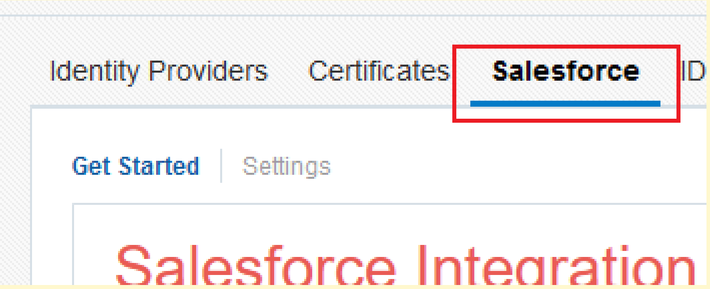
Eloqua Access and Security Mapping

Eloqua Access	Salesforce Profile	Eloqua Security Groups
□	AAAA	✎
□	Authenticated Website	✎

After you finish: Continue to Mapping Salesforce profiles to Eloqua security groups for Salesforce native SSO integration.

Mapping Salesforce profiles to Eloqua security groups for Salesforce native SSO integration

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



After you enabled single sign-on and specified the Salesforce user account, you can map Salesforce profiles to Oracle Eloqua security groups.

Before you begin:

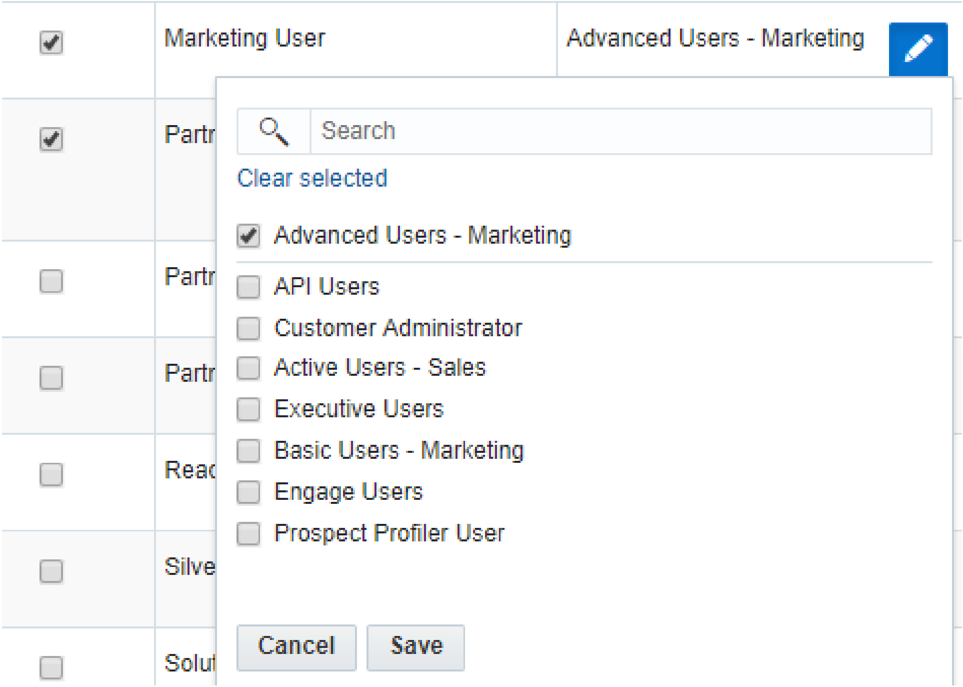
- Configure the Salesforce single sign-on integration by uploading the Salesforce metadata and setting the Salesforce integration user.

- Review this information about synchronizing Salesforce users with Oracle Eloqua.
- In Salesforce, identify the Salesforce profiles that can access to the Oracle Eloqua connected app.
- Consider how Salesforce profiles should map to Oracle Eloqua security groups. Security groups control the level of access that users have to Oracle Eloqua features and assets. The default security groups and access settings are available on Topliners. If you need to change the security group settings, consider doing that before you map the Salesforce profiles.

To setup the Salesforce integration user and security profile mappings:

1. In Oracle Eloqua, click **Settings** ⚙.
2. Click **Single Sign-On** in the *Users and Security* area.
3. Click the **Salesforce** tab and then click the **Settings** tab.

4. For each Salesforce profile that you want to allow access to Oracle Eloqua, do the following:
   a. Select the **Eloqua Access** check box.
   b. Click ✎ and select the **Eloqua Security Groups**. Save your changes.



☑	Marketing User	Advanced Users - Marketing
☑	Partr	
□	Partr	
□	Partr	
□	Reac	
□	Silve	
□	Solut	

Search

Clear selected

☑ Advanced Users - Marketing

□ API Users

□ Customer Administrator

□ Active Users - Sales

□ Executive Users

□ Basic Users - Marketing

□ Engage Users

□ Prospect Profiler User

Note: If you do not see the list of Salesforce profiles, ensure that you set up the integration user.

5. After you map all of the Salesforce profiles to Oracle Eloqua security groups, click **Save**.

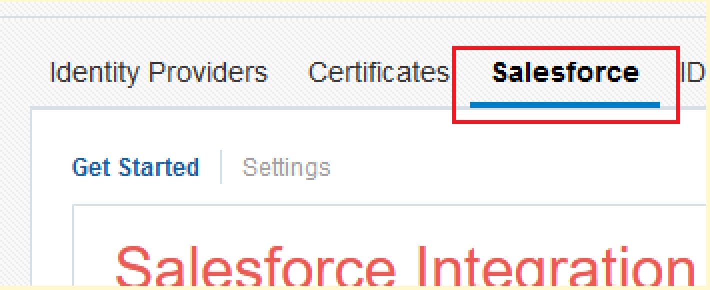
6. When you are ready to turn on SSO with Salesforce, click the **Salesforce SSO** check box and then click **Save**.

After up finish: Continue to Testing Salesforce native SSO integration.

Testing Salesforce native SSO integration

☪

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



After you've set up the Salesforce and Oracle Eloqua for single sign-on, you are ready to test. In addition to the information below, Salesforce offers additional testing tools.

Before you begin:

- Complete the steps to enable single sign-on with Salesforce.
- Identify the Salesforce user account you are going to use for testing. We recommend using an account that has an administrator profile. Ensure the user's profile is mapped to Oracle Eloqua security groups.

- Make sure that the Salesforce profiles have been mapped to the appropriate Oracle Eloqua security groups. See mapping Salesforce profiles to Oracle Eloqua security groups.

To test single sign-on:

1. In a browser, navigate to https://login.eloqua.com, then click **Sign in with single sign-on or another account**.
2. Enter your company name and click **Sign In**.

   This should redirect you to the Salesforce login page. If you are already logged in to Salesforce, you will be logged in directly to Oracle Eloqua. Otherwise, login with your Salesforce user credentials.
3. You know that single sign-on worked if you are directed to Oracle Eloqua. If not, refer to the troubleshooting information.

Troubleshooting

> ⬉**Note**: You cannot use Oracle Eloqua's debug mode to test single sign-on with Salesforce.

If you cannot login using your Salesforce single sign-on credentials, you can try the following solutions:

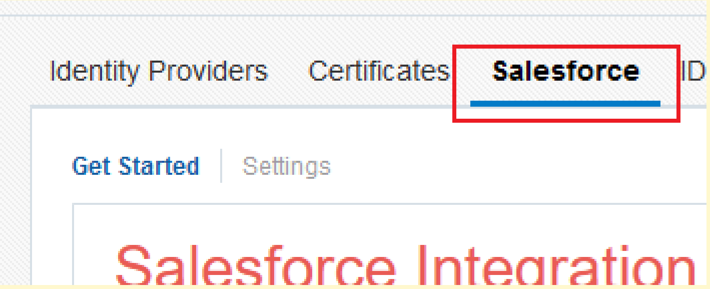
- In Salesforce, verify the Salesforce identity provider configuration. Verify that you are able to login to other SAML enabled connected apps using the Salesforce login credentials.

- Verify that the Oracle Eloqua connected app is configured correctly in Salesforce. See Configuring Oracle Eloqua as a connected app for native SSO integration for more information.
- Verify that the Salesforce user you are using for testing has a user profile mapped to Oracle Eloqua security groups. See Mapping existing Oracle Eloqua users to Salesforce for Salesforce native SSO integraiton for more information.
- If you receive the error "Your request either didn't include a SAML response or the SAML response was malformed", then verify that the Oracle Eloqua connected app is configured correctly in Salesforce. The entity ID is case sensitive. See Configuring the Salesforce native SSO integration for more information.
- Ensure that certificates have not expired. If your certificate has expired, your users would not be able to login to Oracle Eloqua using single sign-on. Learn more about checking for and updating expired certificates.
- First Name, Last Name, and Email Address are required fields for an Oracle Eloqua user. If these fields are not defined, you will receive an error when synching user details to Oracle Eloqua. Please ensure that First Name, Last Name, and Email Address are defined for a Salesforce user.

About synchronizing Salesforce users with Oracle Eloqua using the native SSO integration

☪

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



Using the Salesforce native SSO integration, you can synchronize your Salesforce users with Oracle Eloqua so that they can login using their single sign-on.

User account creation process

During the single sign-on configuration process, a Salesforce account is used for communication between Salesforce and Oracle Eloqua. Typically, this is the same

Salesforce account set up for CRM integration. You map Salesforce profiles to Oracle Eloqua security groups to ensure your Salesforce users have the correct access to Oracle Eloqua.

After you complete the single sign-on setup, the following occurs:

- Any user with a Salesforce profile mapped to a security group in Oracle Eloqua can login to Oracle Eloqua using their Salesforce single sign-on credentials.
- When the Salesforce user logs in to Oracle Eloqua using the single sign-on (including accessing Oracle Eloqua Profiler from within Salesforce), Oracle Eloqua automatically creates a user account for that user in Oracle Eloqua.
- Oracle Eloqua links the user account and the Salesforce account using the Salesforce user ID. The user is granted the appropriate security group access based on the user's Salesforce profile.
- Oracle Eloqua updates the user account every time the Salesforce user accesses Oracle Eloqua. This update also occurs if a user opens Oracle Eloqua Profiler in Salesforce. This update ensures that the user always has the appropriate access to Oracle Eloqua based on their Salesforce user profile.

User account maintenance

After enabling single sign-on with Salesforce, you continue to maintain your users in Salesforce. Oracle Eloqua synchronizes the Salesforce account with the Oracle Eloqua account every time the user logs in to Oracle Eloqua. If you disable or delete an account in Salesforce, that user will no longer have access to Oracle Eloqua.

You can continue to create Oracle Eloqua user accounts. For example, if you have users that should only have access to Oracle Eloqua, you can set up a user account in

Oracle Eloqua and keep it independent of Salesforce. In this case, the user would access Oracle Eloqua from the https://login.eloqua.com login using your site's company name and their Oracle Eloqua login credentials.

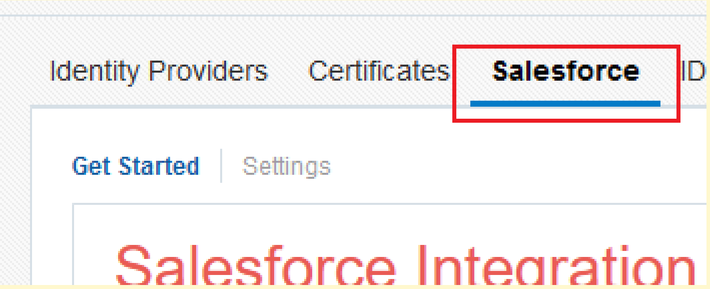
If you have existing Oracle Eloqua accounts that should be linked to a Salesforce account for single sign-on, you can manually create that linkage too. See Mapping existing Oracle Eloqua users to Salesforce for Salesforce native SSO integraiton for more information.

User account limits

Depending on your Oracle Eloqua purchase agreement, there may be a limit on the number of user accounts. This includes all types of users (sales and marketing). If you exceed the limit, your account manager will contact you. If you need to reduce the number of Oracle Eloqua users, you can unlink the Salesforce user from their Oracle Eloqua account and disable the account in Oracle Eloqua. See Unlinking Salesforce SSO users for more information.

Mapping existing Oracle Eloqua users to Salesforce for Salesforce native SSO integraiton

Important: The Salesforce native SSO integration page (highlighted below) requires the use of the deprecated Salesforce native CRM integration. Since this native CRM integration was deprecated, and the use of the Salesforce Integration app is encouraged, use the Identity Provider setup instead. Learn more.



After you have setup single sign-on, if you have existing Oracle Eloqua users that you want to change to single sign-on users you can manually map those users to their Salesforce account.

To map a single user:

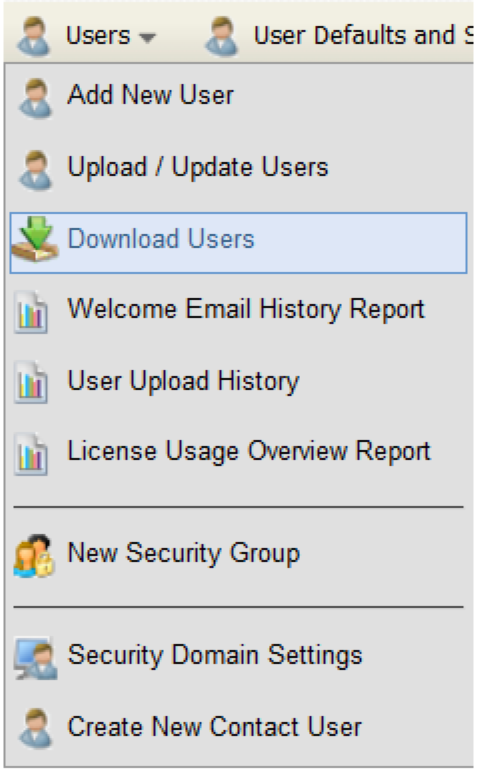
1. Log on to Oracle Eloqua, then click **Settings** ⚙.
2. Click **Users** in the *Users and Security* section.
3. Open the user account you want to update.
4. Enter the 18 digit **Salesforce User ID** in the *CRM Details* section. Click **Save**.

> **Note**: You can use this toggle to unlink individual synchronized users from SSO if you want to make them stand-alone Oracle Eloqua users with their own credentials.
>
> For more information, see Unlinking Salesforce SSO users.

To map users in bulk:

1. Log on to Oracle Eloqua, then click **Settings** ⚙.
2. Click **Users** in the *Users and Security* section.

3. Click **Users > Download Users**



4. Click the **Export** menu and choose the export format.
5. Open the downloaded file and update the **Salesforce User ID** with the Salesforce user ID.
6. In Oracle Eloqua, navigate back to *Users and Security*, and select **Users > Upload / Update Users**.
7. Complete the **User Upload / Update** wizard.
8. To complete the mapping, contact My Oracle Support to link the Oracle Eloqua users in bulk to their corresponding Salesforce users.

Unlinking Salesforce SSO users

You can remove the link between an Oracle Eloqua user account and a Salesforce account. After you remove the link, the user is no longer able to access Oracle Eloqua using their Salesforce login credentials. For example, you might have reached a user account limit and want to disable user accounts.

> ⇖**Note**: The account linkage between Oracle Eloqua and Salesforce only applies if your organization purchased the Oracle Eloqua Identity Cloud Service for Salesforce.

To unlink an Oracle Eloqua user account from Salesforce:

1. Click **Settings** ⚙.
2. Click **Users** in the *Users and Security* section.
3. Open the user you want to update.
4. At the bottom of the screen, click **Unlink from Salesforce**.

   After you remove the link, you cannot restore it without having the user's Salesforce ID.

To remove the Salesforce account link from multiple accounts:

1. Download the user accounts to a .csv file.
2. Update the file to include only the accounts you want to update and remove the *SFDC User Id*.

> ⦿ **Tip**: You can remove any other settings from the file that you are not changing.

3. . Upload the updated .csv file to Oracle Eloqua.