Configuring Salesforce

https://campus.barracuda.com/doc/84313785/

Creating a Custom Profile in Salesforce

You must create a new user with System Administrator privileges in Salesforce that is used exclusively by the Service Center integration to send ticket updates and asset information to Salesforce. To avoid interruptions in service from forced password changes, you must create a new profile in Salesforce that has all the access of the System Administrator profile, without password changes enforced.

To create a custom profile

1. Login to Salesforce using an Administrator account.
2. Click your user name in the top right, then click **Setup**.
3. Under the **Administration Setup** menu, expand **Manage Users** and click **Profiles**.
4. Locate the **System Administrator** profile from the list and click **Clone**.
5. Type *MW Integration* as the profile name and click **Save**.
6. The page for the new profile opens. Click **Edit**.
7. Under **Administrative Permissions**, check **Password Never Expires**.
8. Click **Save**.

Creating an Integration User in Salesforce

Next, create a dedicated user for the integration and apply the MW Integration profile.

To create an integration user

1. Login to Salesforce using an Administrator account.
2. Click your user name in the top right, then click **Setup**.
3. Under the **Administration Setup** menu, expand **Manage Users**, then click Users.
4. Click **New User.**
5. Fill out the required fields under **General information** as follows:
    1. **Role**: Choose as appropriate for your organization
    2. **Last Name:** Type MWIntegration.
    3. **User License**: Choose **Salesforce**.
    4. **Alias**: Type **MWI**.
    5. **Profile**: Choose **MW Integration**.
    6. **Email**: Enter a valid email address for your organization. The initial password will be sent to this address, so make sure you have access to the mailbox.
    7. **Username**: The email you entered will auto-populate. The username must be in the form of an email but is not required to be associated with an actual mailbox. Update if required.

8. **Nickname**: This will auto-populate. Update if required.
6. Fill out the required fields under **Locale Settings** as follows:
    1. **Time Zone**: Choose your time zone.
    2. **Locale**: Choose your locale.
    3. **Language**: Choose your language.
7. Fill out the required fields under **Approver Settings** as follows:
    1. Receive Approval Request Emails: Never
8. Check **Generate new password and notify user immediately**.
9. Click **Save**.
10. An email is sent to the address entered. Retrieve the email and click the confirmation link.
11. Type and verify your new password.
12. Choose a security question and type the answer.
13. Click **Save**.

Recording the Security Token

Salesforce assigns each user a security token, which functions to maintain a session identifier for communications. It is for this reason that the account used for the integration with Barracuda Managed Workplace must not be shared with a human user. You enter this token into Service Center when completing the integration, using the configuration wizard for the Salesforce service desk module.

To generate a security token

1. Login to Salesforce using the credentials for the MW Integration user you just created.
2. Click your user name in the top right, then click **Setup**.
3. Under the **Personal Setup** menu, expand **My Personal Information**, then click Reset My Security Token.
4. Click **Reset Security Token**.
5. An email is sent to the address entered. This email contains the security token you will use to complete the Service Center portion of the integration.

Authorizing Service Center for Salesforce Access

Salesforce security settings restrict API access to entities that have been expressly permitted. You must provide both the IP address and domain for your Service Center to fulfill the security requirements.

To configure security

1. Login to Salesforce using an Administrator account.

2. Click your user name in the top right, then click **Setup**.
3. Under the **Administration Setup** menu, expand **Security Controls**, then click **Network Access**.
4. Beside **Trusted IP Ranges**, click **New**.
5. Type the Internet-facing IP address of your Service Center in the **Start IP Address** and **End IP Address** fields.
6. Click **Save**.
7. Under the **Security Controls** menu, click **Remote Site Settings**.
8. Click **New Remote Site**.
9. Type SC in the **Remote Site Name** field.
10. Type the address of your Service Center in the **Remote Site URL** field.
    Note: If your Service Center address is sc.yourcompany.com, you should use the scmessaging URL (scmessaging.yourcompany.com) in the Remote
    Site URL as these are separate sites that must each be granted access.
    Caution: Do not include any subdirectories in the URL you enter. For example, if your Service Center address is https://mwcloudplatform.com/sc, enter https://mwcloudplatform.com only.
11. If your Service Center does not use SSL, check **Disable Protocol Security**.
    Note: We strongly recommend using SSL to protect your end-client's data.
12. Add a description if you wish.
13. Check the **Active** check box.
14. Click **Save**.

Suspending Salesforce Case Validation Rules

Certain validation rules for the case object in Salesforce may prevent a successful push of the Barracuda Managed Workplace Apex programming objects to Salesforce. If you have any validation rules configured in Salesforce for the Case object, these should be temporarily disabled when saving the integration configuration in Service Center to ensure a successful push.

Important:

- If Working or New are not available statuses for case objects, the connector will fail to save, displaying "An error occurred compiling trigger/class - step 1".
- If the CaseComment Salesforce object is unavailable/disabled the connector will fail to save, displaying "An error occurred compiling trigger/class - step 1".

To check for Case Validation Rules

1. Login to Salesforce using an Administrator account.
2. Click your user name in the top right, then click **Setup**.
3. Under the **App Setup** menu, expand **Customize**.
4. Expand **Cases**, then click **Validation Rules**.
5. Click **Edit** next to the name of the rule you wish to disable.

6. Clear the **Active** check box.
7. Click **Save**.
8. Repeat Steps 5-7 for every validation rule you wish to disable.

Note: When enabling the rules after a successful push of the configuration, ensure no rules comply with the ticketing parameters set by Service Center. For example, if you have fields in the Case object that are required, but have no default value, the push will not succeed.

Confirming the Apex Test Coverage

Salesforce does not allow new Apex programming objects to be uploaded if the total test coverage for all objects is less than 75%.

To determine your test coverage

1. Login to Salesforce using an Administrator account.
2. Click your user name in the top right, then click **Setup**.
3. Under the **App Setup** menu, expand **Develop**, then click **Apex Classes**.
4. If there are no objects listed, the integration will be successful and you may proceed.
5. If there are objects present, click **Run All Tests**.

If the results show you have a test coverage of less than 75%, please consult the Salesforce knowledgebase or Technical Support team to resolve before proceeding.