



Teamcenter Service Lifecycle for SFDC - Installation and Setup Guide

This Documentation contains trade secrets or otherwise confidential information owned by Siemens Industry Software Inc. or its affiliates (collectively, "Siemens"), or its licensors. Access to and use of this Documentation is strictly limited as set forth in Customer's applicable agreement(s) with Siemens. This Documentation may not be copied, distributed, or otherwise disclosed by Customer without the express written permission of Siemens, and may not be used in any way not expressly authorized by Siemens.

This Documentation is for information and instruction purposes. Siemens reserves the right to make changes in specifications and other information contained in this Documentation without prior notice, and the reader should, in all cases, consult Siemens to determine whether any changes have been made.

No representation or other affirmation of fact contained in this publication shall be deemed to be a warranty or give rise to any liability of Siemens whatsoever.

If you have a signed license agreement with Siemens for the product with which this Documentation will be used, your use of this Documentation is subject to the scope of license and the software protection and security provisions of that agreement. If you do not have such a signed license agreement, your use is subject to the Siemens Universal Customer Agreement, which may be viewed at <https://www.sw.siemens.com/en-US/sw-terms/base/uca/>, as supplemented by the product specific terms which may be viewed at <https://www.sw.siemens.com/en-US/sw-terms/supplements/>.

SIEMENS MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS DOCUMENTATION INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY. SIEMENS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, LOST DATA OR PROFITS, EVEN IF SUCH DAMAGES WERE FORESEEABLE, ARISING OUT OF OR RELATED TO THIS DOCUMENTATION OR THE INFORMATION CONTAINED IN IT, EVEN IF SIEMENS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TRADEMARKS: The trademarks, logos, and service marks (collectively, "Marks") used herein are the property of Siemens or other parties. No one is permitted to use these Marks without the prior written consent of Siemens or the owner of the Marks, as applicable. The use herein of third party Marks is not an attempt to indicate Siemens as a source of a product, but is intended to indicate a product from, or associated with, a particular third party. A list of Siemens' Marks may be viewed at: <https://www.sw.siemens.com/en-US/trademarks/>. The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

About Siemens Digital Industries Software

Siemens Digital Industries Software is a global leader in the growing field of product lifecycle management (PLM), manufacturing operations management (MOM), and electronic design automation (EDA) software, hardware, and services. Siemens works with more than 100,000 customers, leading the digitalization of their planning and manufacturing processes. At Siemens Digital Industries Software, we blur the boundaries between industry domains by integrating the virtual and physical, hardware and software, design and manufacturing worlds. With the rapid pace of innovation, digitalization is no longer tomorrow's idea. We take what the future promises tomorrow and make it real for our customers today. Where today meets tomorrow. Our culture encourages creativity, welcomes fresh thinking and focuses on growth, so our people, our business, and our customers can achieve their full potential.

Support Center: <https://support.sw.siemens.com>

Send Feedback on Documentation: https://support.sw.siemens.com/doc_feedback_form

Table of Contents

- System Requirements..... 1-1
- Active Workspace Gateway configuration..... 2-1
- App Installation and Configuration..... 3-1
 - Salesforce knowledge settings.....3-1
 - Install the application.....3-1
 - Create permission set..... 3-1
 - User management.....3-2
 - Create integration user..... 3-2
 - Create or update end user.....3-3
 - Set up connected app.....3-4
 - Add trusted URLs..... 3-5
 - Configure custom settings..... 3-5
 - Update remote site settings..... 3-6
 - Knowledge setup for users.....3-6
 - Enable lightning web security.....3-7
- Contact and Support.....4-1

1. System Requirements

Before you begin the installation, ensure that your environment meets the following requirements:

1. Users must have the specified licenses and access permissions to utilize the full functionality.
 - **Service Technician Access (STA) License**—Required for viewing data from Teamcenter.
 - **Salesforce License**—Dependent on Service Cloud or Field Service.

User	Licenses
Siemens Technician	SLM for CRM (Basic)
Siemens Supervisor	SLM for CRM Asset Manager (Basic)

2. Version compatibility matrix

The following matrix shows the compatibility between versions of the Salesforce app and specific versions of Teamcenter. It is crucial to align these versions for proper functionality.

App Version	SLM-Microservice	Teamcenter
Teamcenter SLM 2512	2512 or latest patch	2512
	2506 or latest patch	2506
	2412.0001 or latest patch	2412
	2406.0002 or latest patch	2406
	2312.0005 or latest patch	2312

Note

Ensure you use the corresponding SLM Microservice (SLM-MS) and Teamcenter (TC) or Active Workspace (AW) version based on the Salesforce app version you are installing.

Based on compatibility requirements, you can download the necessary SLM microservices from the following link: [SLM-MS](#)

3. The installation of the MFE Vis microservice is a prerequisite for enabling asset visualization within the Teamcenter Service Lifecycle for SFDC application.

Note

The MFE Vis microservice is included as part of the Active Workspace kit.

4. For secure communication and data transfer, Active Workspace must be HTTPS enabled.
5. Teamcenter needs to be exposed to the internet to facilitate communication with Salesforce.

2. Active Workspace Gateway configuration

This section outlines the necessary configurations for your Active Workspace Gateway.

Procedure

1. If you have not already set up your gateway configuration, please follow the instructions provided via [this link](#).
2. You need to add specific attributes to your microservice gateway config.json file. Locate the **additionalCookieAttributes** section and insert the following:

```
"additionalCookieAttributes": [  
  {  
    "cookieName": "XSRF-TOKEN",  
    "attributes": [ "Secure", "SameSite=None" ]  
  },  
  {  
    "cookieName": "_csrf",  
    "attributes": [ "Secure", "SameSite=None" ]  
  },  
  {  
    "cookieName": "JSESSIONID",  
    "attributes": [ "Secure", "SameSite=None", "Max-age=9999999999", "Expires=Session" ]  
  },  
  {  
    "cookieName": "TcSS-JSESSIONID",  
    "attributes": [ "Secure", "SameSite=None" ]  
  }  
]
```


3. App Installation and Configuration

Salesforce knowledge settings

Before installing the application, ensure that knowledge is enabled in the Salesforce org.

Procedure

1. Navigate to **Setup**.
2. Search for and select **Knowledge Settings**.
3. Enable Knowledge.

Install the application

You can install the application from the [Salesforce AppExchange](#).

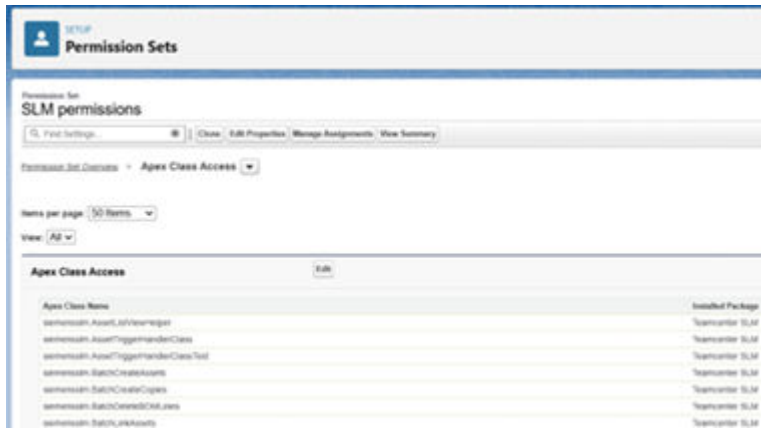
If you encounter any difficulties during this process, reach out to our support team using the contact information provided in this documentation. We are here to assist you!

Create permission set

You need to create a new permission set, for example, named **SLM Permissions**, and assign the necessary access levels.

Procedure

1. Assign full access to the following objects under **Object Settings**:
 - Knowledge Asset Junctions
 - Assets
2. Assign the following **System Permissions** within the permission set:
 - Author Apex
 - Customize Application
3. Assign all **siemensslm** namespace Apex classes under **Apex Class Access**.



User management

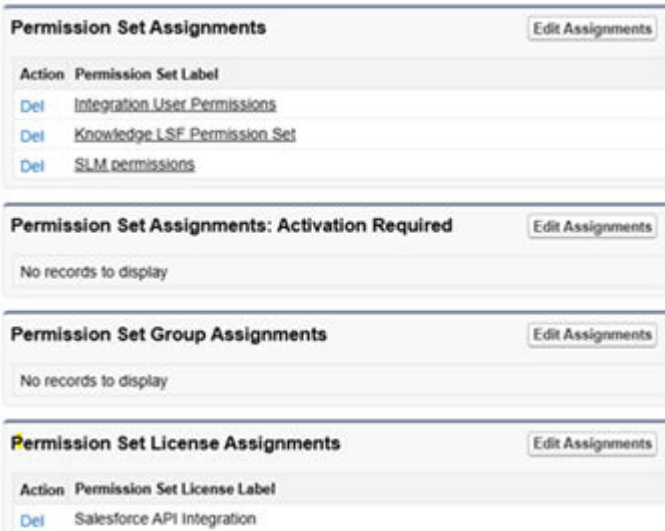
User setup is crucial for the application's functionality. This involves creating an integration user and end users.

Create integration user

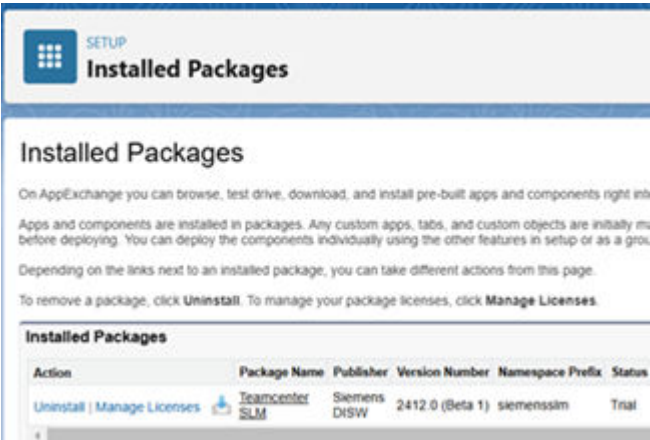
To facilitate background communication with Teamcenter, create a user with the user license as **Salesforce Integration** and the profile as **Minimum Access - API Only Integrations**.

Procedure

1. After creating the user license and profile, assign the **Salesforce API Integration** permission set license to this user.
2. Assign the following permission sets:
 - Integration Users Permissions
 - SLM Permissions



- 3. Assign the SLM app license to the integration user:
 - a. Go to **Installed Packages**.
 - b. Select **Manage Licenses**.
 - c. Click **Add Users**, select the integration user, and click **Add**.



Create or update end user

Now, configure the actual users who will be interacting with the application. You can either create new users or modify existing ones.

Procedure

- 1. Technician user setup:
 - a. Create a new user.

Note

This user must be a Knowledge user.

- b. Assign the **Siemens Technician** and **SLM Permissions** permission sets.

Tip

You can also apply these settings to an existing user.

2. Supervisor user setup:

- a. Create a new user.

Note

This user must be a Knowledge user.

- b. Assign the **Siemens Supervisor** and **SLM Permissions** permission sets.

Note

You can also apply these settings to an existing user.

Set up connected app

Create a connected app in Salesforce, for example, named **SLM Connected App**, with the following configurations:

Procedure

1. Enable **OAuth Settings**.
2. Enable **Device Flow**.
3. Enable **Client Credentials Flow**.
4. Add the following OAuth scopes to the **Selected OAuth Scopes** column:
 - Manage user data via APIs (api)
 - Manage user data via Web browsers (web)
 - Perform requests at any time (refresh_token, offline_access)
 - **Save** the changes.
5. Go to **Manage→Policies→IP relaxation** and set it to **Relax IP Restrictions**.
6. For **Client Credentials Flow**, choose **Run As** and select the integration user.
7. **Save** the changes.
8. Open the connected app and navigate to **Manage Consumer Details**.

9. Get the **Consumer Key** and **Consumer Secret**.
10. Save the **Consumer Key** and **Consumer Secret** in the microservices .env file as follows:

```
CONSUMER_KEY=<key>
CONSUMER_SECRET=<secret>
DEV_MODE=0
SF_URL=<my domain>
```

Tip

To find your Salesforce my domain, go to Salesforce Setup and search for domain → my domain.

Add trusted URLs

Create two trusted URLs (one for HTTP and one for HTTPS) with the following configurations enabled:

- connect-src (scripts)
- font-src (fonts)
- frame-src (iframe content)

Configure custom settings

Procedure

1. Go to **Setup**.
2. Search for **Custom Settings**.
3. Click **Manage** for the TC_Settings row.
4. Click **New**.
5. Enter the following login URL details (These are dummy details for your reference):
 - a. Set AWC_Path_c to awc.
 - b. Set MS_Path_c to tc/micro. The microservice path, such as **micro** or **sd**, will be configured according to the Active Workspace gateway config.json.
 - c. Set TC_SF_Route_c to tc/micro/tcslmassetmgmt/coc. The microservice path, such as **micro** or **sd**, will be configured according to the Active Workspace gateway config.json.
 - d. For TcX, set TC_SF_Route_c to tc/micro/tcslmassetmgmt/tcxcoc. The microservice path, such as **micro** or **sd**, will be configured according to the Active Workspace gateway config.json.
 - e. Set TC_URL_c to <Active Workspace gateway URL>.

Example

https://albsf-tc2312.eu-central-1.elb.amazonaws.com

Update remote site settings

Procedure

1. Go to **Setup**.
2. Search for **Remote Site Settings**.
3. Click the **TeamcenterEnv** row.
4. Remove the test URL from the **Remote Site URL** field.
5. Enter your Active Workspace **Domain Name URL**.
6. Click **Save**.

Knowledge setup for users

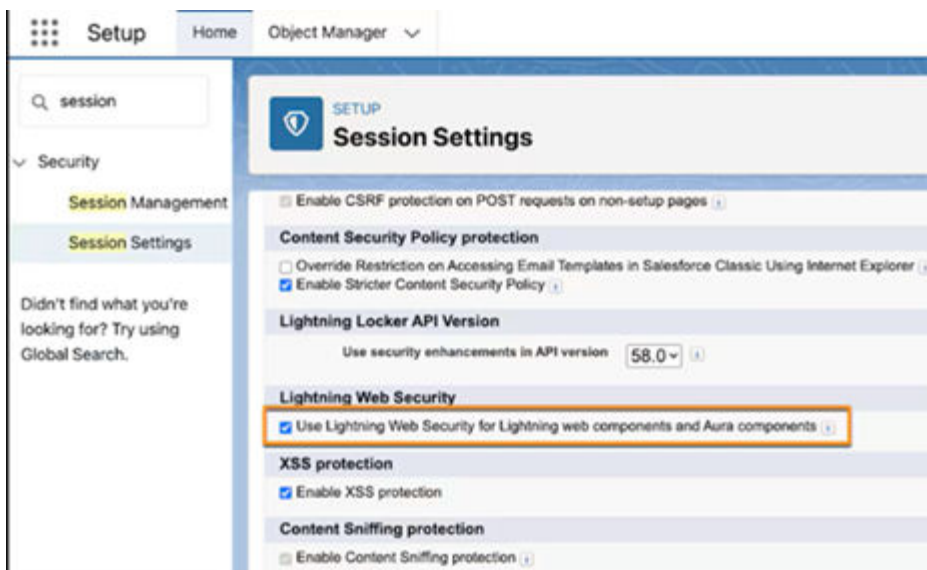
Procedure

1. For all users who need access to Knowledge, navigate to their user profile and ensure they are marked as a **Knowledge user**.
2. Search for **Knowledge Setup**, select it, and then follow the instructions.
3. Go to **Object Manager** (within Service Setup).
4. Open **Knowledge** (siemensslm_Knowledge_kav).
5. Go to **Fields & Relationships**.
6. Open the **Answer** field.
7. Click **Set Field-Level Security**.
8. Select the **Visible** column for All and click **Save**.
9. Go to **Page Layouts**.
10. Open the **Knowledge Layout**.
11. Drag the **Answer** field to a position below the **URL Name**.
12. Click **Save**.

Enable lightning web security

Procedure

1. Open **Setup**.
2. Navigate to **Session Settings**.
3. Select the **Lightning Web Security** checkbox.



4. Contact and Support

For technical support, you can email the following experts:

1. **Name:** Bhupendrasing Patil
Email: bhupendrasing.patil@siemens.com
2. **Name:** Chetan Attarde
Email: chetan.attarde@siemens.com
3. **Name:** Ajay Dahibhate
Email: ajay.dahibhate@siemens.com