Teamcenter Service Lifecycle for SFDC - Installation and Setup Guide

SIEMENS

© 2025 Siemens

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

Log in to Support Center to access software downloads and updates, product and release documentation, Knowledge Base articles, videos, other self-service resources, and to open support cases: **https://support.sw.siemens.com**.

If you do not have a Support Center login, register here: **https://support.sw.siemens.com/register**.

To 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 external client app 3-4
  - Configure TCSLMPhysicalStructure Microservice versions earlier than 2606 3-8
  - Configure TCSLMPhysicalStructure Microservice version 2512 3-9
  - Configure TCSLMPhysicalStructure Microservice versions 2606 and later 3-10
- Add trusted URLs 3-14
- Configure custom settings 3-14
- Update remote site settings 3-15
- Knowledge setup for users 3-15
- Enable lightning web security 3-18

Troubleshooting TCSLMPhysicalStructure Microservice 4-1
- Verify microservice health 4-1
- Resolve Deployment Center accessibility issues 4-3
- Resolve Salesforce embedded view access error 4-4
- Resolve deployment script execution failures 4-5
- Troubleshoot TCSLMPhysicalStructure microservice startup failures 4-5
- Resolve Salesforce connection errors 4-5
- Validate JSON configuration files 4-6
- Troubleshoot Active Workspace gateway connectivity 4-7
- Resolve proxy and firewall issues 4-7
- Resolve Deployment Center script generation issues 4-7
- Troubleshoot Teamcenter Process Manager service issues 4-8
- Resolve microservice version compatibility issues 4-8
- Resolve CORS errors in browser 4-9
- Troubleshoot Salesforce timeout errors 4-9

Contact and Support 5-1

© 2025 Siemens

© 2025 Siemens

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, TCSLMPhysicalStructure Microservice and specific versions of Teamcenter. It is crucial to align these versions for proper functionality.

App Version	TCSLMPhysicalStructure Microservice	Teamcenter
Teamcenter SLM 2606	2606 or latest patch	2606
	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 TCSLMPhysicalStructure Microservice 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 required TCSLMPhysicalStructure microservices using this link: **TCSLMPhysicalStructure-MS**

For information about configuring microservices using Deployment Center (DC), see the following topics:

- **Configure TCSLMPhysicalStructure Microservice versions earlier than 2606**
- **Configure TCSLMPhysicalStructure Microservice version 2512**
- **Configure TCSLMPhysicalStructure Microservice versions 2606 and later**

© 2025 Siemens

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.

© 2025 Siemens

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. Add specific attributes to the config.json file of your microservice gateway. You can find this file in the gateway folder inside the microservices folder. 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. Add ***.force.com** to both the **frame-src** and **frame-ancestors** arrays. To search for these arrays by their name, press Ctrl + F. Refer to the image below:

© 2025 Siemens



© 2025 Siemens

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!

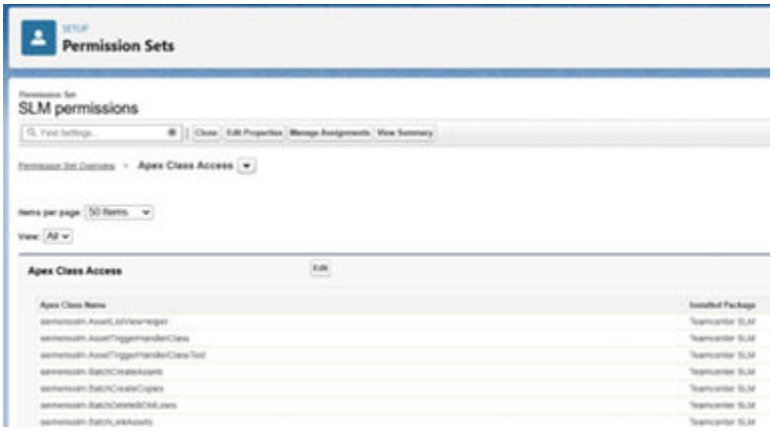
Create permission set

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**:
   - Work Plan Template
   - Work Step Template
   - Work Plan Template entry
   - 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**.

© 2025 Siemens



User management

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

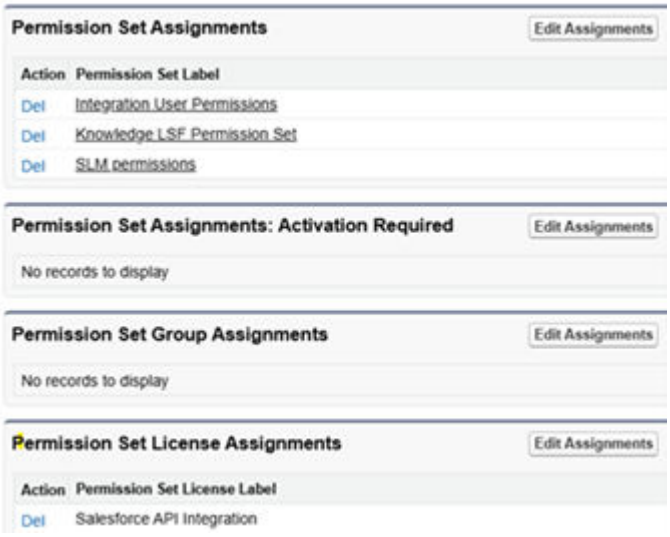
Create integration user

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**.

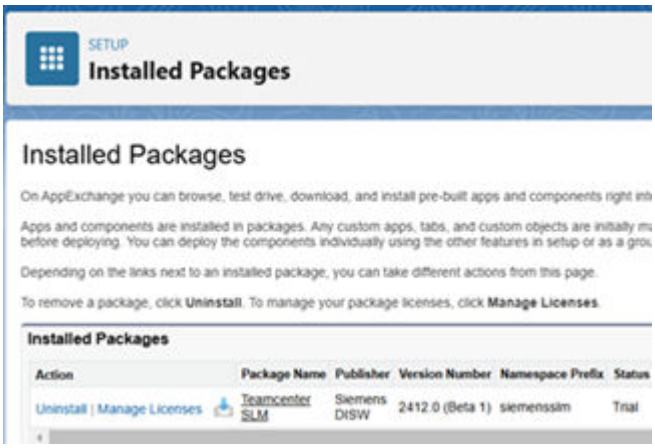
Procedure

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

© 2025 Siemens



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.

© 2025 Siemens

> **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 external client app

Configure OAuth authentication to enable secure access to Salesforce data without requiring users to manually log in for each integration request.

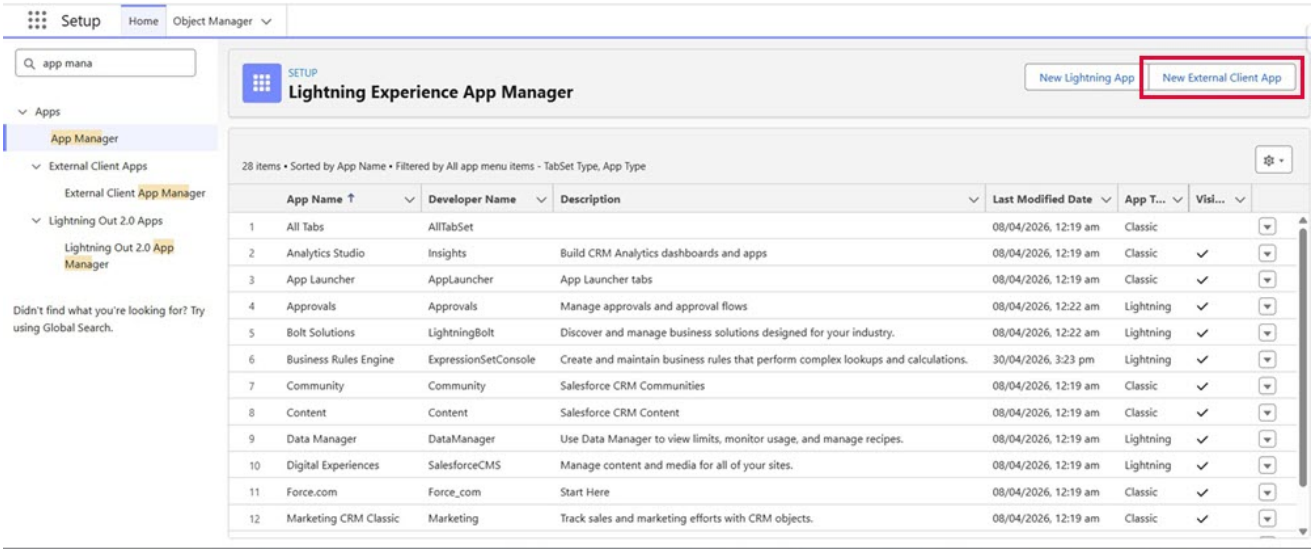
Prerequisites

- Access to Salesforce Setup with administrative privileges
- Integration user account created in Salesforce
- Production organization URL for production environments

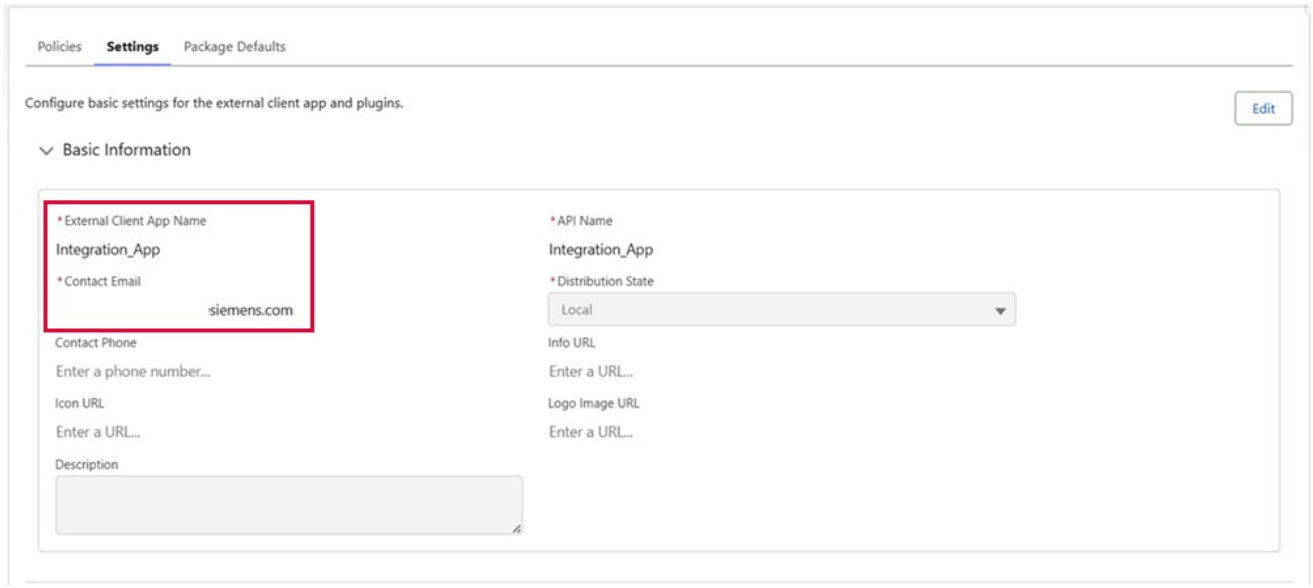
Procedure

1. In Salesforce, go to **Setup**.
2. In the **Quick Find** box, search for **App Manager**.
3. Click **New External Client App**.

© 2025 Siemens

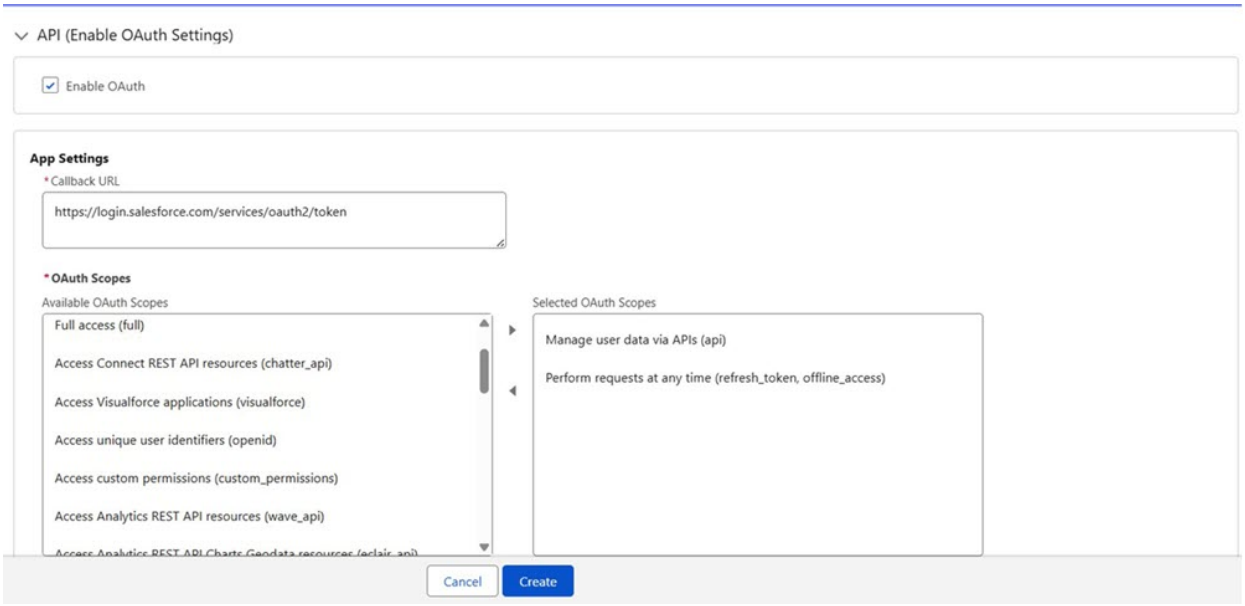


4. In the **Basic Information** section, do the following:
   a. In the **External Client App Name** field, enter the application name.
   b. In the **Contact Email** field, enter the contact email address for the application.



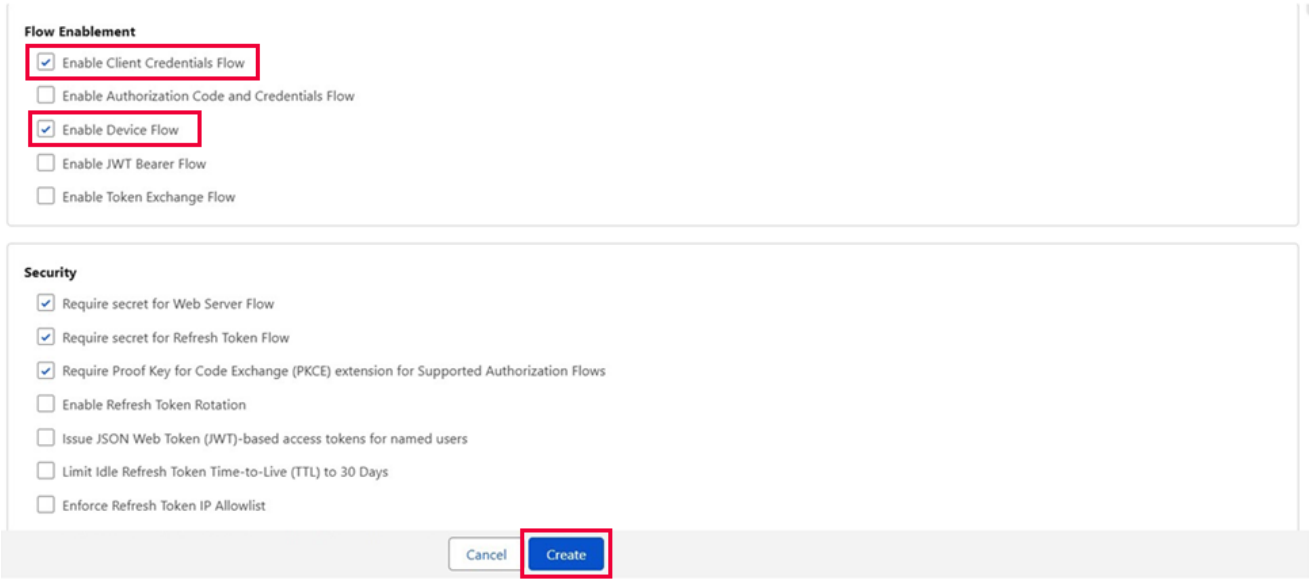
5. In the **API (Enable OAuth Settings)** section, do the following:
   a. Select **Enable OAuth**.
   b. In the **Callback URL** field, enter: *https://login.salesforce.com/services/oauth2/success*.
   c. In the **OAuth Scopes** field, select the required scopes for your integration.

© 2025 Siemens



d. Select **Enable Client Credentials Flow** and **Enable Device Flow** check boxes.

e. Click **Create**.

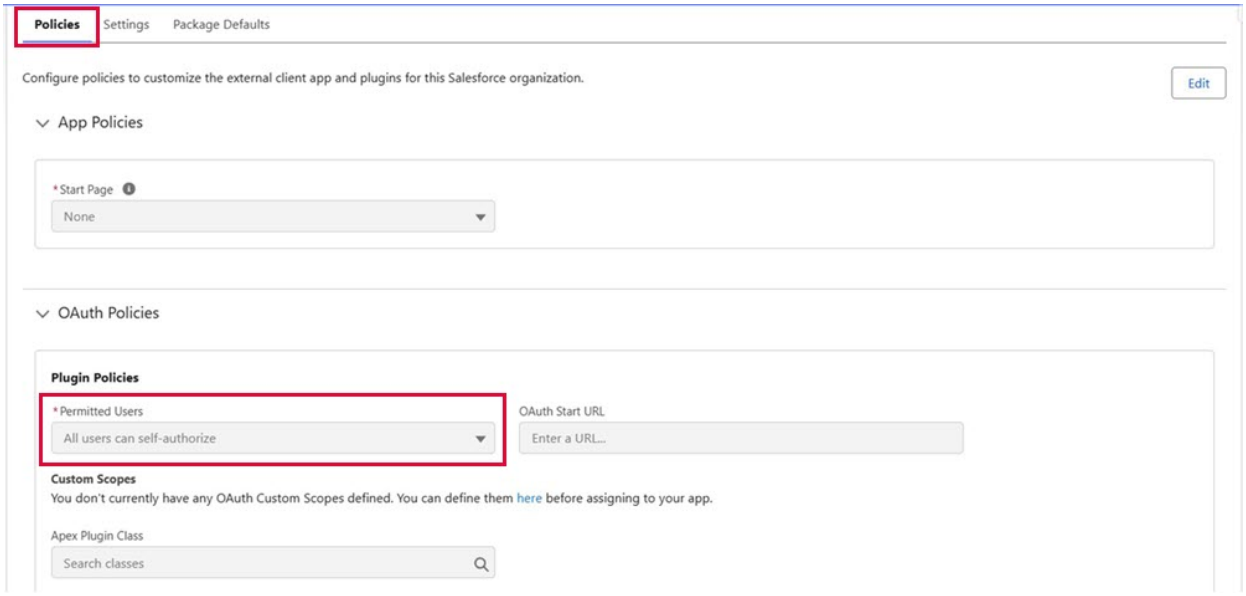


The external client app is created.

6. Navigate to the **Policies** tab and do the following:

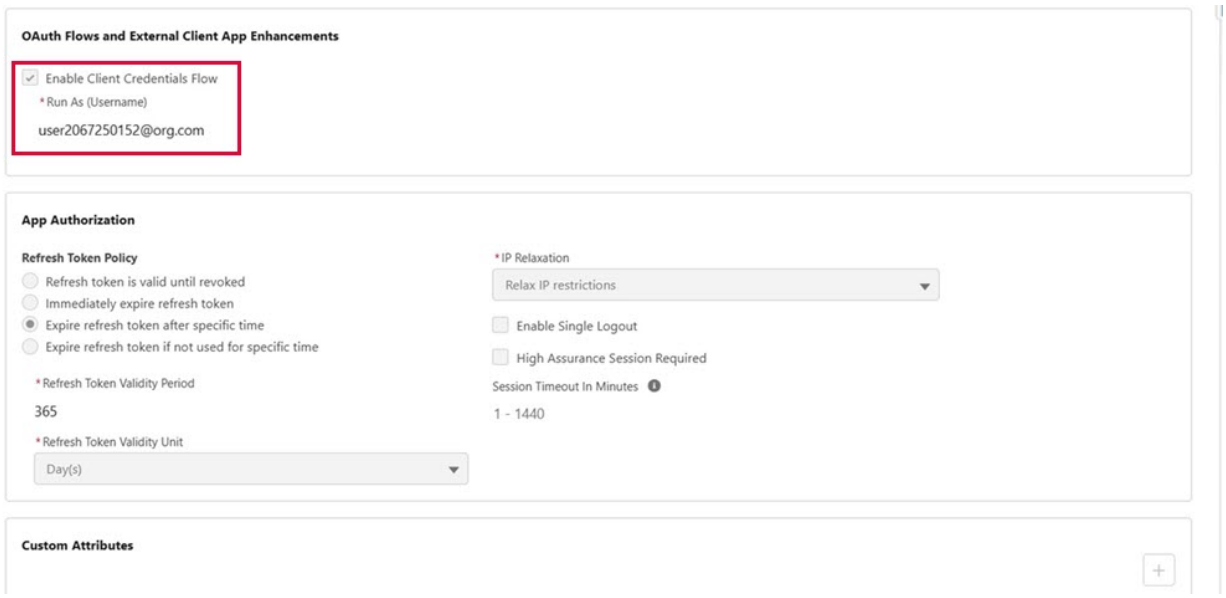
a. From the **Permitted Users** list, select **All users can self-authorize**.

© 2025 Siemens



b. Select the **Enable Client Credentials Flow** check box.

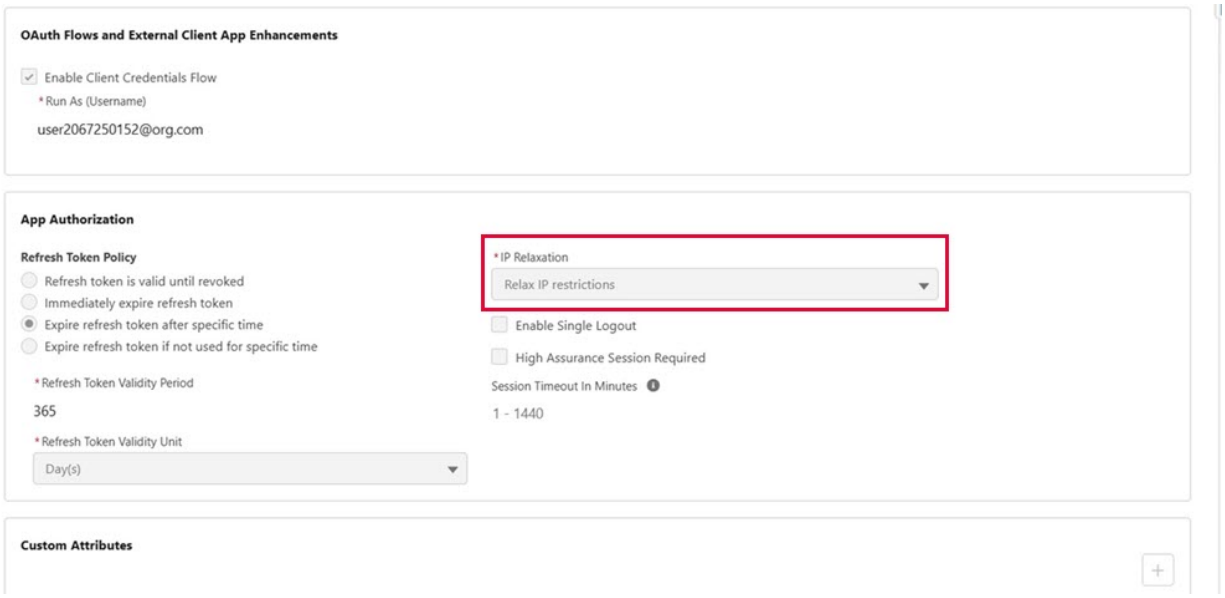
c. In the **Run As** field, enter the integration user's username.



d. From the **IP Relaxation** list, select **Relax IP restrictions**.

e. Click **Save**.

© 2025 Siemens



The policy settings are saved.

7. Navigate to the **Settings** tab and do the following:
   a. Click **OAuth Settings**, and then click **Consumer Key and Secret** to open the credentials.
   b. Copy the **Consumer Key** and **Consumer Secret** values and paste them into the custom settings.
8. To set the Consumer Key, Consumer Secret, and Salesforce URL properties based on your version requirements, see the following topics:
   - **Configure TCSLMPhysicalStructure Microservice versions earlier than 2606**
   - **Configure TCSLMPhysicalStructure Microservice version 2512**
   - **Configure TCSLMPhysicalStructure Microservice versions 2606 and later**

Configure TCSLMPhysicalStructure Microservice versions earlier than 2606

- Save the Salesforce Org's **Consumer Key**, **Consumer Secret**, and **Salesforce (SF) URL** in the JSON file at the following path:

  C:\Apps\tc\tc version folder\microservices folder\services_config folder\tcslmphysicalstructure.json as follows:

```
CONSUMER_KEY=<key>
CONSUMER_SECRET=<secret>
SF_URL=https://<My Domain URL>
```


© 2025 Siemens

Tip

To find your Salesforce My Domain URL, go to **Salesforce Setup** and search for domain > **My Domain** > **Current My Domain URL**.

Sample **tcslmphysicalstructure.json** file:

```
{
  "tcslmphysicalstructure_service": {
    "image": "tcslmphysicalstructure_service-2512",
    "environment": [
      "DSP=http://vc6s015:9090",
      "ENDPOINT_TC=http://vc6s015:8000/tc",
      "MSR=http://vc6s015:8787/eureka/v2/",
      "STORAGEMODE=FMS",
      "SF_URL=addyoursfurl.com",
      "CONSUMER_KEY=addyourkey123",
      "CONSUMER_SECRET=addyoursforgsecret456",
      "LOG_LEVEL=info",
      "NODE_ENV=production"
    ],
    "deploy": {
      "replicas": 1
    }
  }
}
```

Warning

Ensure that all quotation marks and commas are correct. Validate the file with a JSON linter before you save it.

Configure TCSLMPhysicalStructure Microservice version 2512

- Open the JSON file at the following path:

  C:\Apps\tc\tc version folder\microservices folder\services_config folder\tcslmphysicalstructure.json

- Add the **Salesforce Org's URL (SF URL)** to the JSON file:

  ```
  SF_URL= https://<My Domain URL>
  ```

- Save the file.

Sample JSON file:

© 2025 Siemens

```
{
  "tcslmphysicalstructure_service": {
    "image": "tcslmphysicalstructure_service-2606",
    "environment": [
      "DSP=http://vc6s015:9090",
      "ENDPOINT_TC=http://vc6s015:8000/tc",
      "MSR=http://vc6s015:8787/eureka/v2/",
      "STORAGEMODE=FMS",
      "VAULT_TLS_ROOT=C:/Apps/tc/tc2606/TR/tc_vault_tls",
      "SF_URL=https://test.com",
      "LOG_LEVEL=info",
      "NODE_ENV=production"
    ],
    "deploy": {
      "replicas": 1
    }
  }
}
```

Tip

To find your Salesforce My Domain URL, go to **Salesforce Setup** and search for domain > **My Domain** > **Current My Domain URL**.

Configure TCSLMPhysicalStructure Microservice versions 2606 and later

Set the Salesforce Org's **Consumer Key**, **Consumer Secret**, and **Salesforce (SF) URL** for microservice versions 2606 and later.

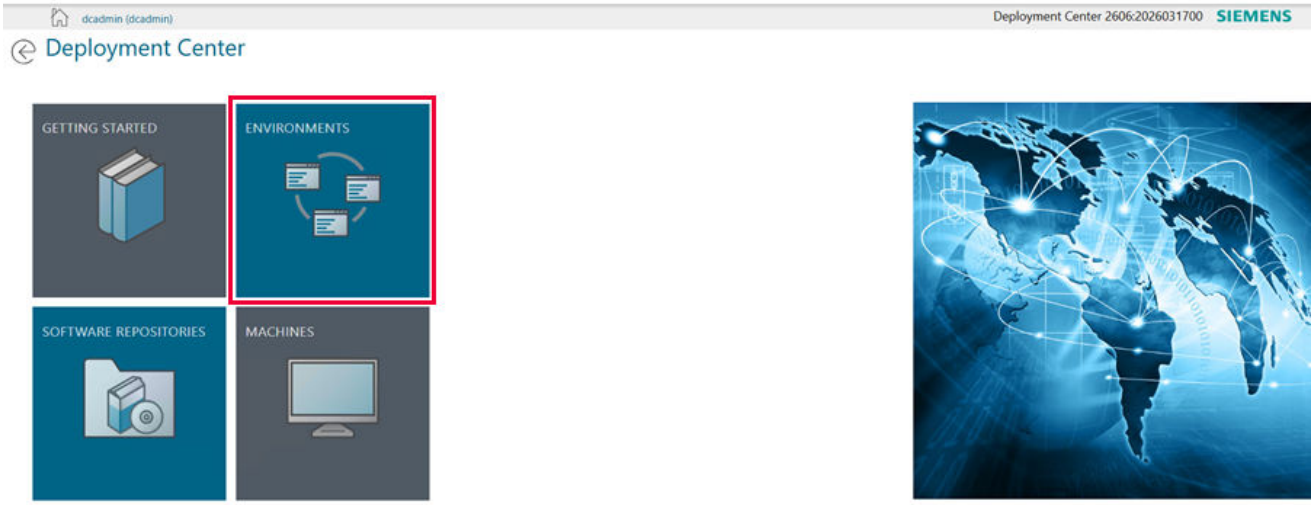
Prerequisites

Install the TCSLMPhysicalStructure Microservice before you continue. If you have not installed it, see the *Installation of TCSLMPhysicalStructure Microservice* guide.

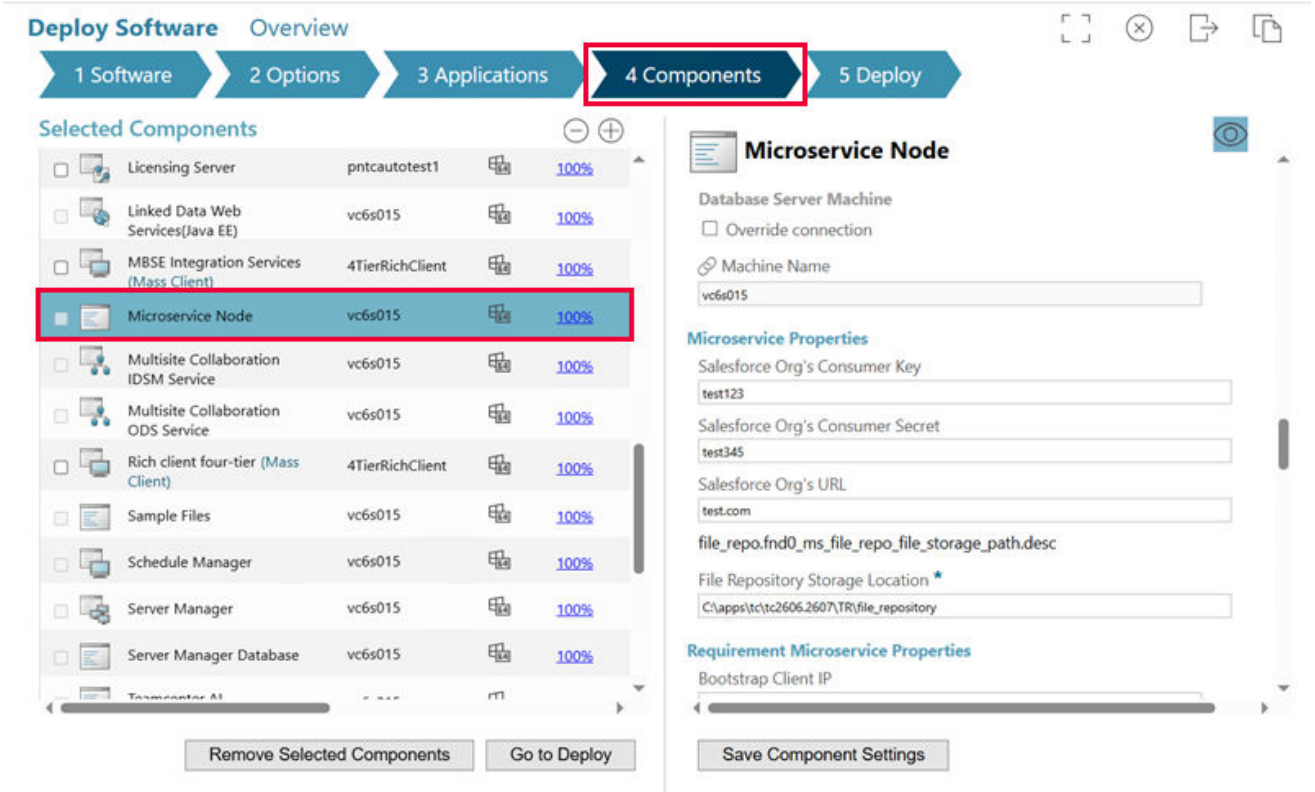
Procedure

1. Log on to Deployment Center and select the environment to which you want to add the Microservice Node.

© 2025 Siemens



2. On the **Environments** page, go to the **Components** tab.
3. In the **Selected Components** list, search for **Microservice Node** and select it.

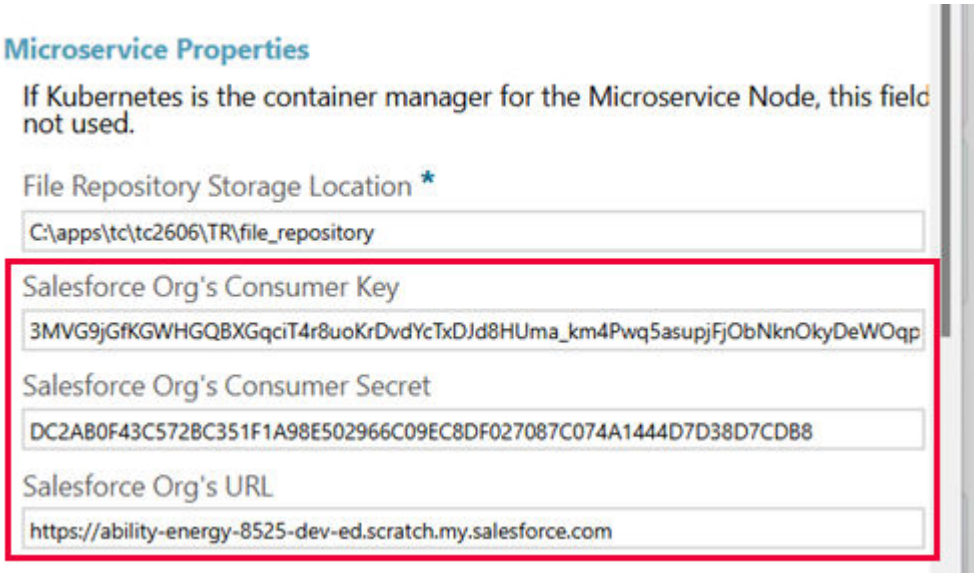


4. In the **Microservice Node** panel, in the **Microservice Properties** section, enter the credentials for the **Salesforce Org's Consumer Key**, **Salesforce Org's Consumer Secret** and **Salesforce Org's URL**.

© 2025 Siemens

Tip

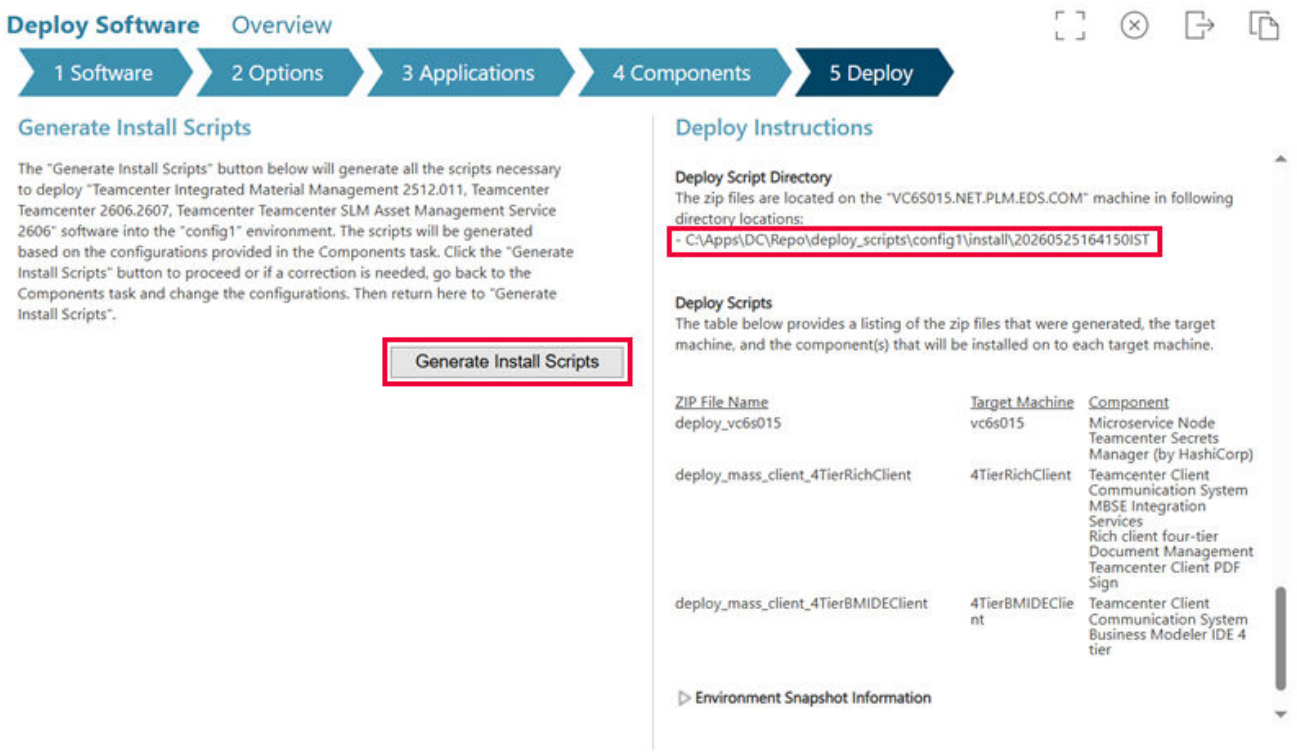
To find your Salesforce My Domain URL, go to **Salesforce Setup** and search for domain > **My Domain** > **Current My Domain URL**.



5. Click **Save Component Settings** in the **Microservice Node** panel.
6. Click **Go to Deploy** to navigate to the **Deploy** tab.
7. Click **Generate Install Scripts** to generate the deployment script.

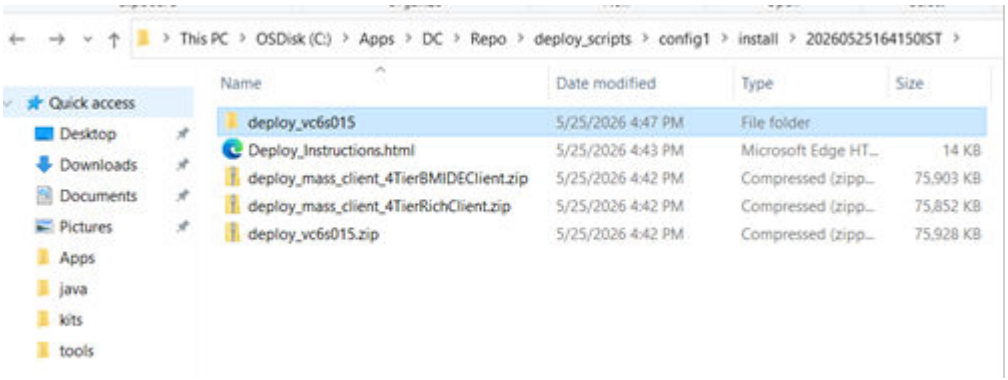
   When script generation is complete, in the **Deploy Instructions** panel, under **Deploy Script Directory** section, copy the directory location.

© 2025 Siemens



8. In Windows File Explorer, go to the deployment script directory path that you copied.
9. Unzip and open the deploy_hostname folder.

> **Note**
>
> To check the host name, open a command prompt and enter the hostname command.

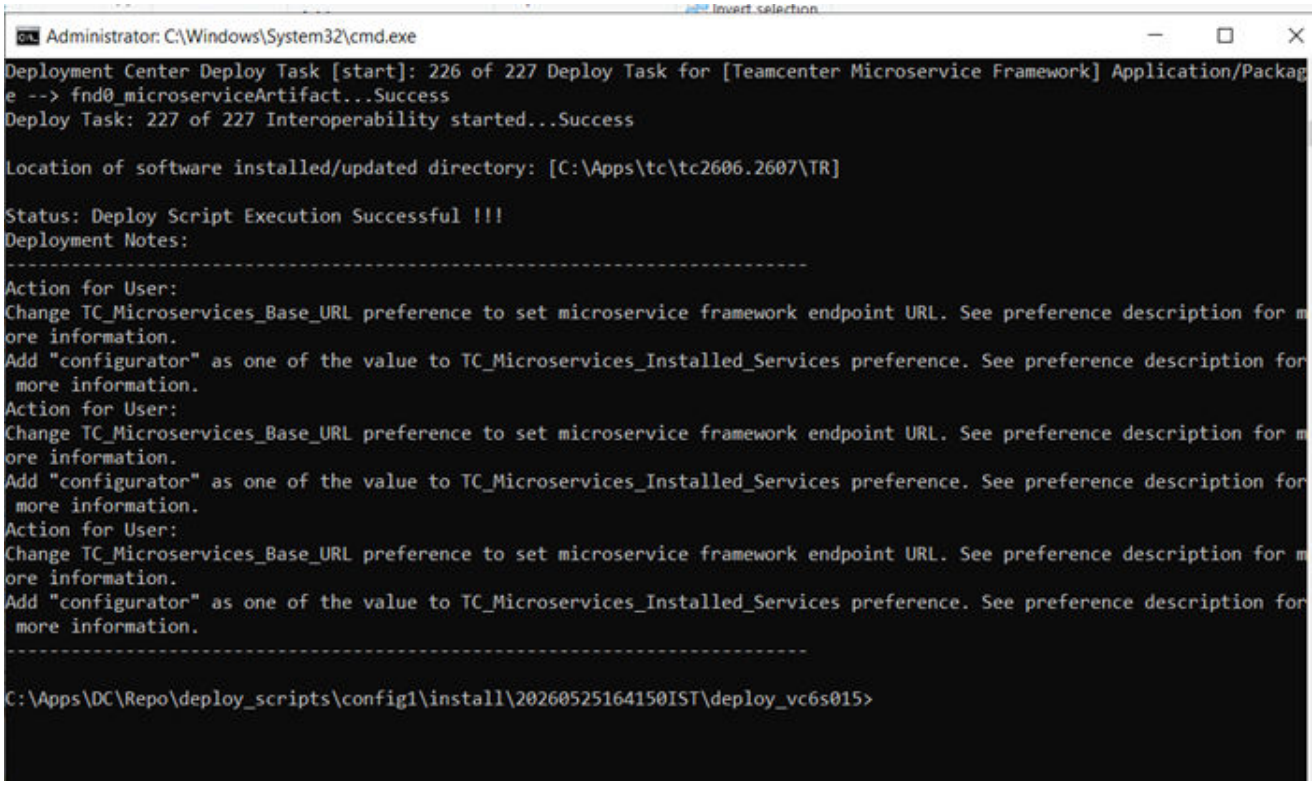


10. To run the deployment script, open a command prompt in administrator mode in the deploy_hostname folder and run:

```
deploy.bat -softwareLocation=C:\Apps\DC\Repo\Software
-dcusername=dcadmin -dcpassword=dcadmin
```

11. Wait until the tcslmphysicalstructure microservice deploys successfully.

© 2025 Siemens



12. After the TCSLMPhysicalStructure microservice is configured successfully, start the **Teamcenter Process Manager** service from **Windows Services** (services.msc) to start the TCSLMPhysicalStructure microservice.

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.

© 2025 Siemens

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

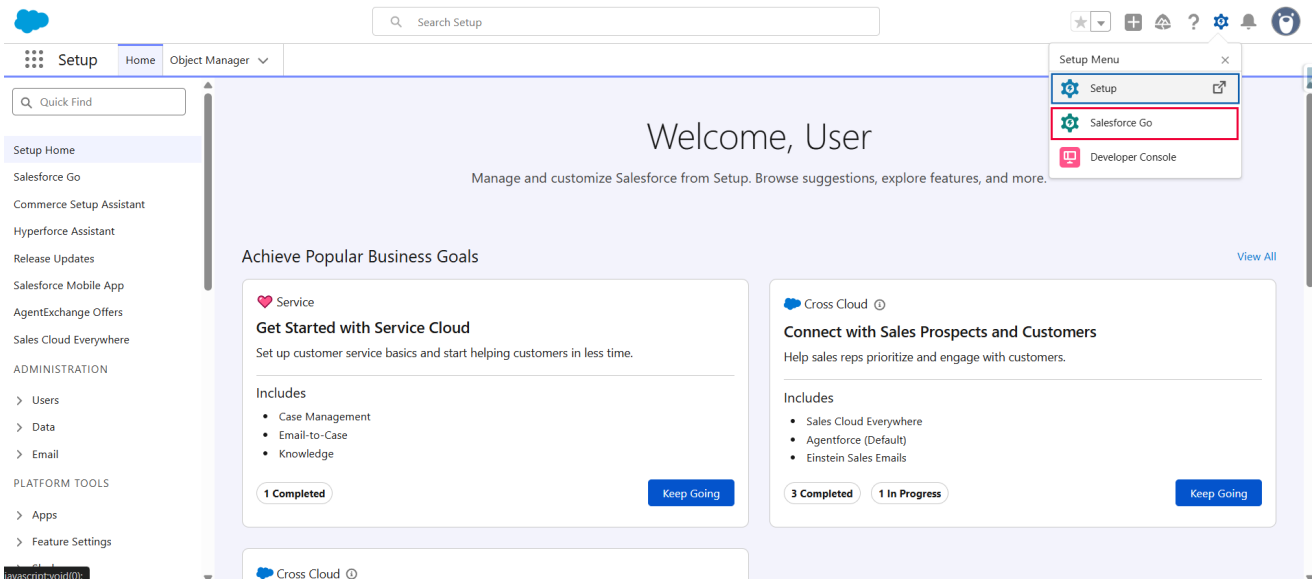
1. Go to **Setup**.
2. Search for **Remote Site Settings**.
3. Click the **TeamcenterEnv** row.
4. Remove the test URL from the **Remote Site URL** field.
5. Enter your Active Workspace **Domain Name URL**.
6. Click **Save**.

Knowledge setup for users

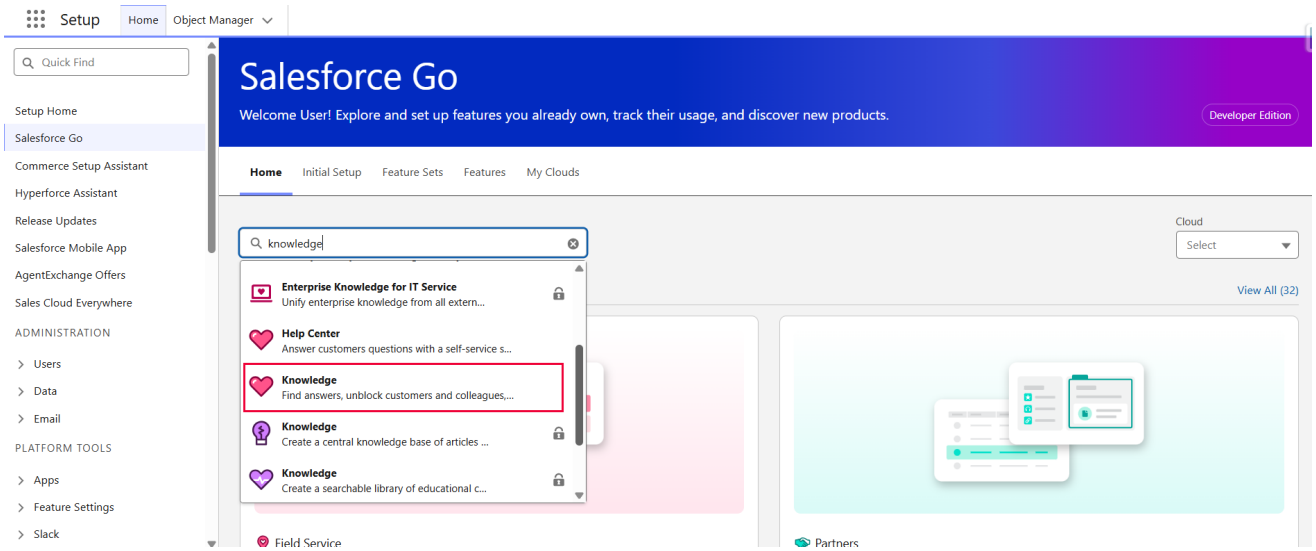
Procedure

1. For each user who needs access to Knowledge, navigate to the user profile and select the option that marks them as a **Knowledge user**.
2. Click the **Gear** icon beside your profile.
3. In **Setup**, click **Salesforce Go**.

© 2025 Siemens

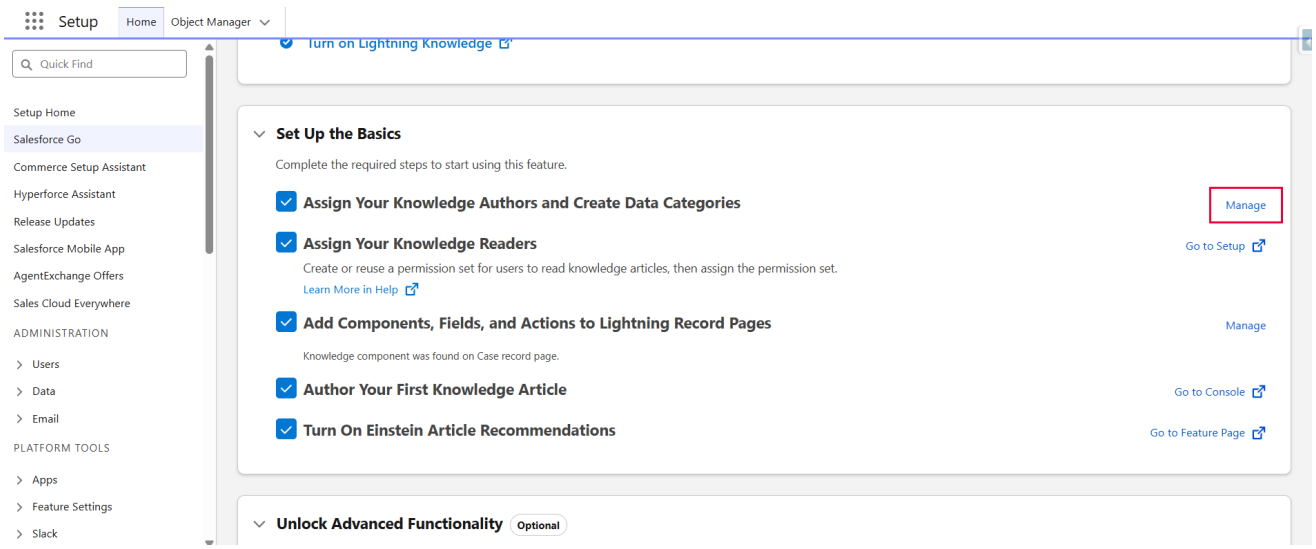


4. In the **Salesforce Go** page, search for **Knowledge** in the search box.

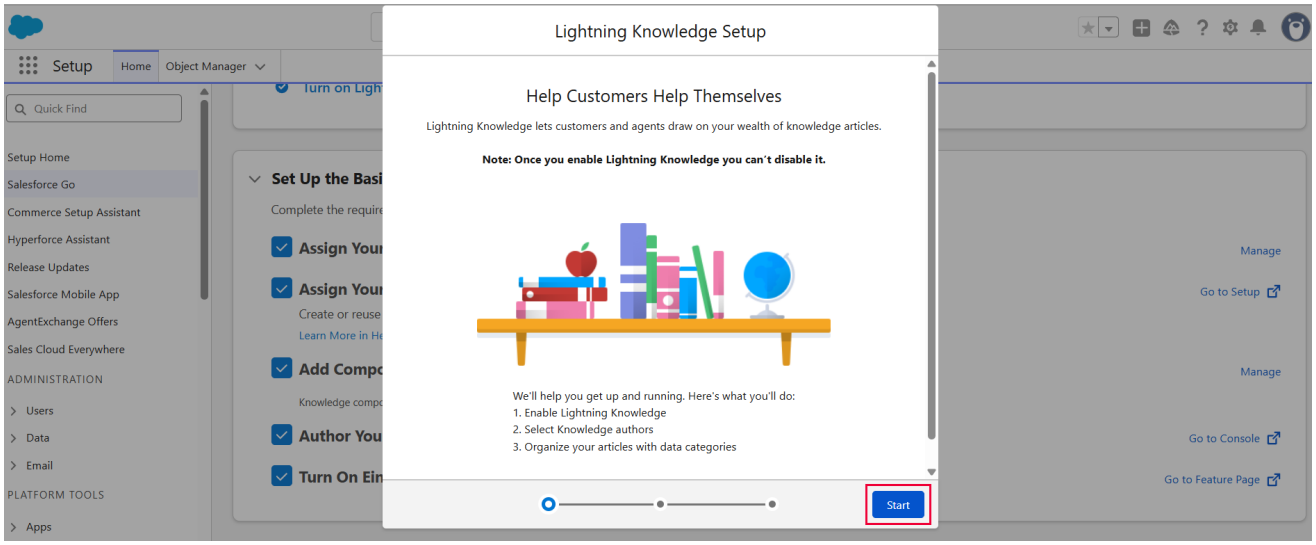


5. Click **Manage**. Follow the setup wizard, click **Next**, and then click **Finish**.

© 2025 Siemens



6. In the **Knowledge Setup** window, click **Start** and follow the steps.



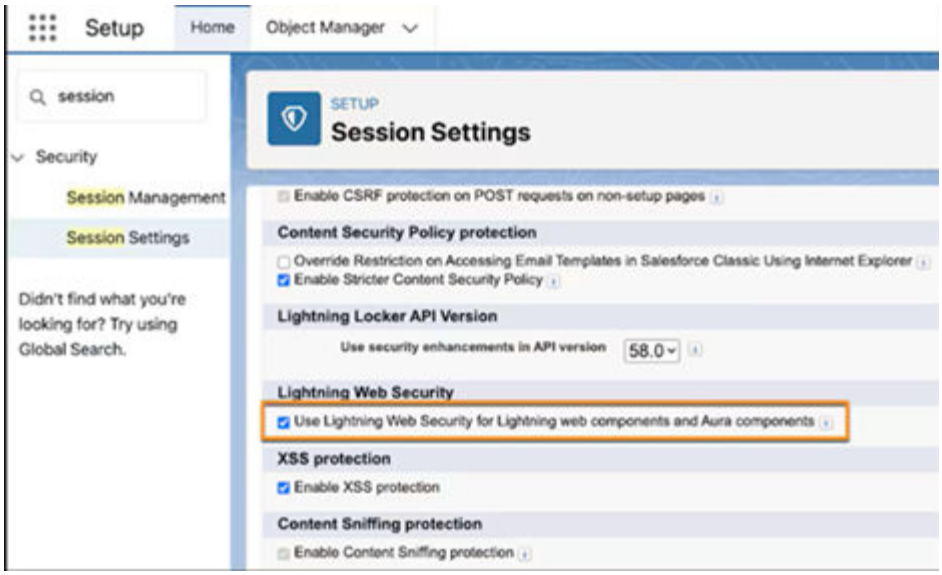
7. Go to **Object Manager**.
8. Open the **Answer** field.
9. Click **Set Field-Level Security**.
10. Select the **Visible** column for All and click **Save**.
11. Go to **Page Layouts**.
12. Open the **Knowledge Layout**.
13. Drag the **Answer** field to a position below the **URL Name** field.
14. Click **Save**.

© 2025 Siemens

Enable lightning web security

Procedure

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



© 2025 Siemens

4. Troubleshooting TCSLMPhysicalStructure Microservice

Verify microservice health

Verify that the TCSLMPhysicalStructure microservice is running and properly registered with the service registry by using health check URLs and reviewing service status.

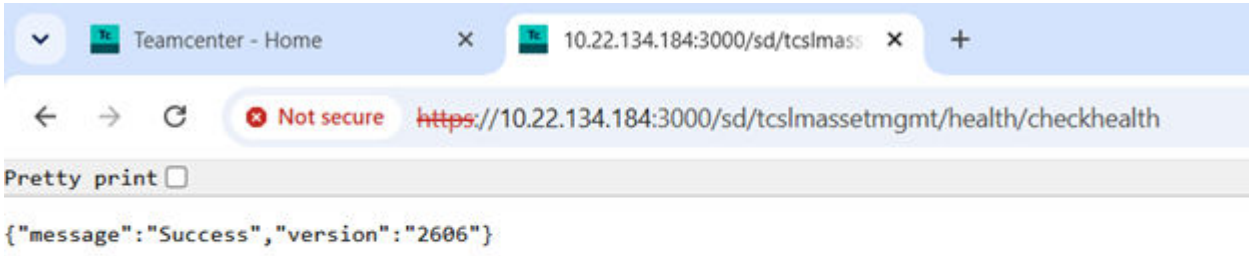
Procedure

1. Check the microservice health status by accessing **one of the following URLs**:

   Note
   Ensure that you are logged in to Active Workspace before you proceed.

   - **<awc_url>/sd/tcslmassetmgmt/health/checkhealth**
   - **<awc_url>/tc/micro/tcslmassetmgmt/health/checkhealth**

   Expected output:

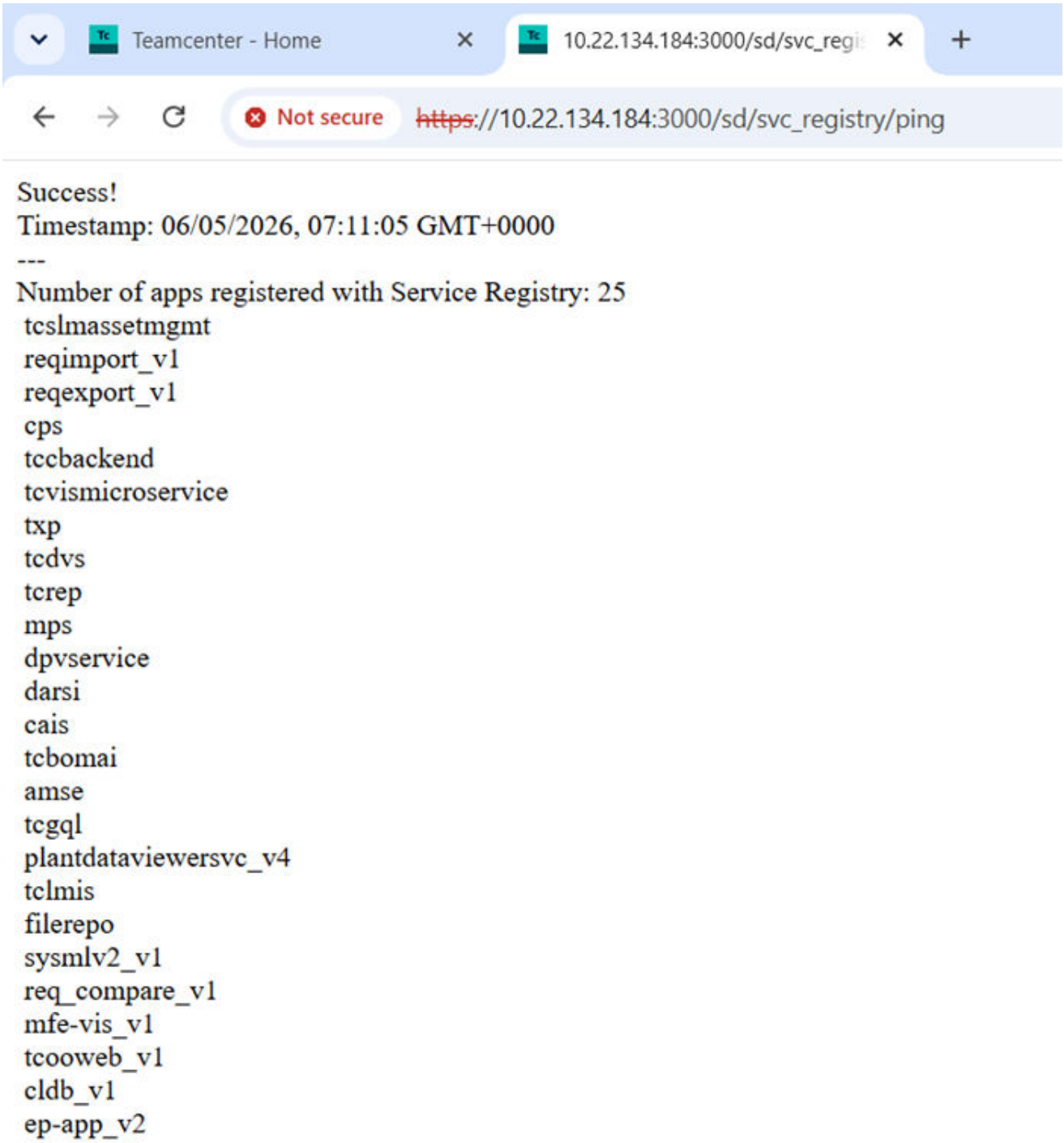


2. Verify the service registry ping by accessing the following URL:

   - **<awc_url>/sd/svc_registry/ping**

   Expected output:

© 2025 Siemens



3. Verify the service registration in the Eureka registry by accessing the following URL:
   - **http://<eureka_host>:<eureka_port>/eureka/v2/apps**

Results

The following results indicate successful microservice health:

© 2025 Siemens

- The service registry ping returns a successful response.
- The health check endpoints return a **200 OK** status with service health details.
- The Eureka applications endpoint lists **tcslmassetmgmt** as a registered application.

What to do next

If the health checks fail, perform the following actions:

- Verify that the microservice is running by checking the Teamcenter Process Manager or the service status.
- Confirm that the microservice port is not blocked or already in use.
- Check the microservice logs to ensure that it registered successfully with Eureka.
- Verify network connectivity between the Active Workspace gateway and the microservice host.

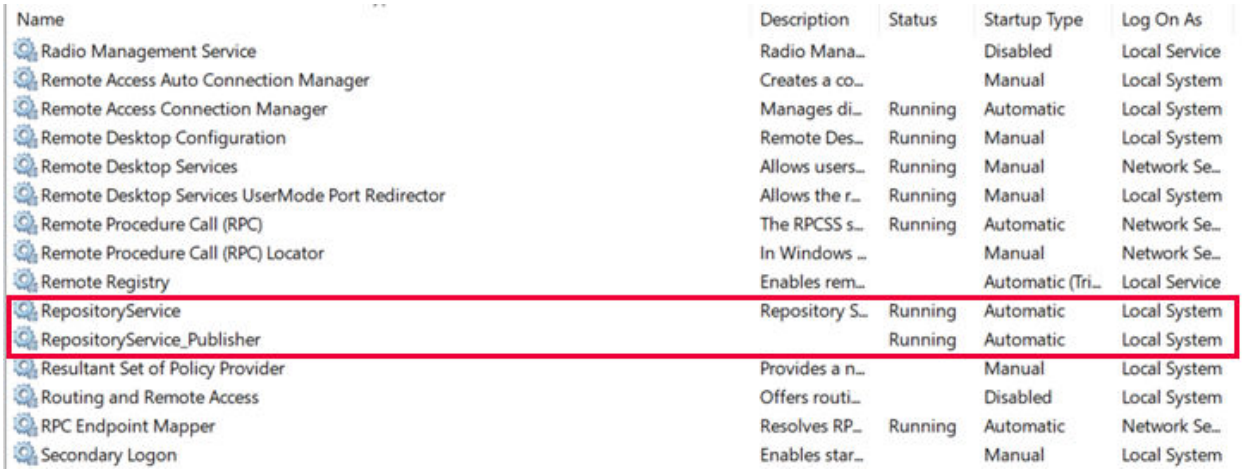
> **Note**
>
> Replace **<awc_url>** with your Active Workspace client URL, for example, **http://10.22.134.95:3000**.
> Replace **<eureka_host>:<eureka_port>** with your Eureka server address, for example, **10.22.134.172:8787**.

Resolve Deployment Center accessibility issues

If Deployment Center is not accessible through a browser in a Windows environment, ensure that the following four services are running.



© 2025 Siemens

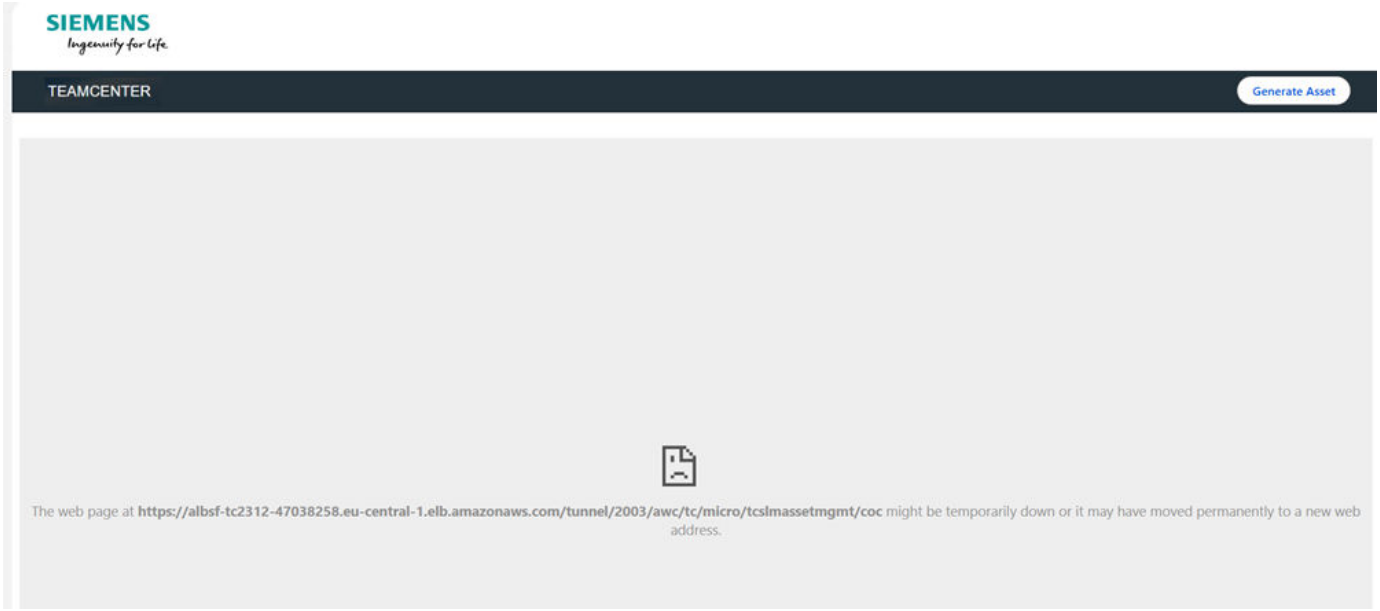


Name	Description	Status	Startup Type	Log On As
Radio Management Service	Radio Mana...		Disabled	Local Service
Remote Access Auto Connection Manager	Creates a co...		Manual	Local System
Remote Access Connection Manager	Manages di...	Running	Automatic	Local System
Remote Desktop Configuration	Remote Des...	Running	Manual	Local System
Remote Desktop Services	Allows users...	Running	Manual	Network Se...
Remote Desktop Services UserMode Port Redirector	Allows the r...	Running	Manual	Local System
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Network Se...
Remote Procedure Call (RPC) Locator	In Windows ...		Manual	Network Se...
Remote Registry	Enables rem...		Automatic (Tri...	Local Service
RepositoryService	Repository S...	Running	Automatic	Local System
RepositoryService_Publisher		Running	Automatic	Local System
Resultant Set of Policy Provider	Provides a n...		Manual	Local System
Routing and Remote Access	Offers routi...		Disabled	Local System
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network Se...
Secondary Logon	Enables star...		Manual	Local System

Resolve Salesforce embedded view access error

If the Salesforce embedded view displays a **page might be temporarily down or moved permanently** error, open the tunnel URL in a new browser tab to establish the connection.

When you access the embedded Salesforce view, the error message appears.



Perform the following steps to resolve the error.

Procedure

1. Copy the tunnel URL from the iframe source.

   The URL format is similar to: **https://<awc_url>/tunnel/2003/awc/tc/micro/tcslmassetmgmt/coc**

© 2025 Siemens

2. Open a new browser tab and paste the copied URL into the address bar.
   If the page loads correctly in the new tab, the embedded Salesforce view should now function properly in Active Workspace.

Resolve deployment script execution failures

1. Ensure that the following Teamcenter services are stopped during deployment and installation:
   - **Teamcenter Process Manager**
   - **Teamcenter Server Manager config1_PoolA**
   - **Tomcat_tc_AdminServer**
2. Restart these services after the deployment completes successfully.

Troubleshoot TCSLMPhysicalStructure microservice startup failures

When the TCSLMPhysicalStructure microservice fails to start, the issue is typically related to configuration errors, port conflicts, or missing runtime dependencies. Use the following steps to diagnose and resolve the startup failure.

Procedure

1. Check the microservice logs for errors.

   Log file location (Windows): *C:\Apps\tc\<version>\microservices\logs\tcslmphysicalstructure.log*
2. Verify that the port configured for the microservice is not already in use.

   Run the following command on Windows:

   ```
   netstat -ano | findstr :<port_number>
   ```
3. Ensure the Java or Node.js runtime required by the microservice is installed and available in the system PATH.

Resolve Salesforce connection errors

Fix connection issues between the TCSLMPhysicalStructure microservice and Salesforce when you encounter 401 Unauthorized or Connection Refused errors.

Procedure

1. Verify that the **Consumer Key** and **Consumer Secret** are correct and have not been rotated or revoked in the **Salesforce Connected App** settings.

© 2025 Siemens

2. Confirm that the SF_URL value matches your Saleforce My Domain exactly.

   Note

   Ensure that the URL is in the format **https://yourcompany.my.salesforce.com** and does not include a trailing slash.

3. Check that the OAuth scopes for the Salesforce Connected App are enabled:
   - **full**
   - **refresh_token**
   - **api**
4. Check that the Salesforce Connected App **IP Relaxation** policy is set appropriately, or go to **Setup** > **Network Access** and verify that the server IP address hosting the TCSLMPhysicalStructure microservice is whitelisted.

Validate JSON configuration files

Check the tcslmphysicalstructure.json configuration file for syntax errors, special characters, and formatting issues that can prevent the microservice from starting.

Procedure

1. Validate the tcslmphysicalstructure.json file with a JSON validator to find syntax errors.

   Use one of the following tools:
   - **jsonlint**
   - **Online JSON validator**

   The validator identifies errors such as missing commas, mismatched brackets, or trailing commas.
2. Check for special characters or invisible Unicode characters that might have been introduced during copy-paste operations.
   a. Open the file in a plain-text editor such as Notepad++ or Visual Studio Code (VS Code).
   b. Enable the **Show All Characters** option to display non-printable characters.
   c. Remove any invisible or special characters that should not be in the file.
3. Confirm that credential values do not contain unescaped special characters.

   Special characters such as double quotes ("), backlashes (\), and other reserved JSON characters must be properly escaped.

© 2025 Siemens

Troubleshoot Active Workspace gateway connectivity

Resolve connectivity issues between the Active Workspace gateway and the TCSLMPhysicalStructure microservice by verifying configuration, testing network connectivity, and validating SLL/TLS certificates.

Procedure

1. Verify that the **config.json** file for the gateway is saved correctly and that you restarted the gateway service after making changes.
2. Confirm that the microservice URL configured in the gateway is reachable from the gateway host.

   Run the following URL to test connectivity to the microservice health check endpoint:

   <awc_url>/sd/tcslmassetmgmt/health/checkhealth
3. If you use HTTPS, ensure that the SLL/TLS certificates are valid and trusted by the gateway.

   Self-signed certificates must be added to the trust store.

Resolve proxy and firewall issues

Configure proxy settings and firewall rules to allow the microservices to communicate with Salesforce through corporate network security controls.

Procedure

1. Configure proxy settings for the microservice if the environment is behind a corporate proxy.
   - Set the HTTP_PROXY and HTTPS_PROXY environment variables, or
   - Configure the proxy settings in the microservice configuration file.
2. Add Salesforce domains to the firewall allow-list.

   Ensure that the following domains are allowed through the firewall:
   - ***.salesforce.com**
   - ***.force.com**
   - **login.salesforce.com**
3. Verify that outbound traffic on port 443 (HTTPS) is not blocked between the microservice host and Salesforce.

Resolve Deployment Center script generation issues

Fix issues that prevent Deployment Center from generating installation scripts by verifying configuration, service availability, and system resources.

© 2025 Siemens

Procedure

1. Ensure that all mandatory fields are filled in before you click **Generate Install Scripts**.

   Verify that the following fields contain valid values:
   - **Consumer Key**
   - **Consumer Secret**
   - **SF URL**
2. Check that the DC Vault service is running and accessible.

   For more information, see **Resolve Deployment Center accessibility issues**.
3. Verify sufficient disk space is available in the Deployment Script Directory path.
4. Review the Deployment Center logs for errors.

   Log file location (Windows): *C:\Apps\DC\Server\logs*

Troubleshoot Teamcenter Process Manager service issues

Resolve issues that prevent the Teamcenter Process Manager service from starting or initiating the microservice process by verifying service configuration, reviewing logs, and checking permissions.

Procedure

1. Open Windows Services by running **services.msc** and verify that the **Teamcenter Process Manager** service is configured for **Automatic** startup.
2. Check the **Process Manager** logs for errors related to starting the microservice process.
3. Ensure that the service account running **Teamcenter Process Manager** has sufficient permissions to access the microservice installation directory and configuration files.

Resolve microservice version compatibility issues

Ensure that the TCSLMPhysicalStructure Microservice version is compatible with the Teamcenter version and properly deployed to prevent version-related startup and runtime failures.

Procedure

1. Confirm that the installed TCSLMPhysicalStructure Microservice version matches the Teamcenter version based on the compatibility matrix in the System Requirements section.
2. If you are upgrading, ensure that the previous microservice version is fully uninstalled or stopped before you deploy the new version.

© 2025 Siemens

3. Clear any cached configuration by deleting temporary files in the microservice working directory before deployment.

Resolve CORS errors in browser

Fix Cross-Origin Resource Sharing (CORS) errors that prevent the browser from connecting to Salesforce by verifying gateway configuration, allowed origins, and clearing browser data.

Procedure

1. Verify that the additionaCookieAttributes section in the gateway **config.json** file is configured correctly, as described in the Active Workspace gateway configuration section.
2. Ensure that the Salesforce domain is included in the allowed origins configuration of the gateway.
3. Clear the browser cache and cookies, and then retry the connection.

Troubleshoot Salesforce timeout errors

Resolve timeout errors when connecting to Salesforce by checking network latency, adjusting timeout values, and verifying Salesforce service status.

Procedure

1. Check network latency between the microservice host and Salesforce.

   Use ping or traceroute to test connectivity to login.salesforce.com
2. Increase the connection timeout values in the microservice configuration if the default values are too low for the network conditions.
3. Verify that Salesforce is not experiencing service disruptions by checking **status.salesforce.com**.

© 2025 Siemens

© 2025 Siemens

5. 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

© 2025 Siemens