TEAMCENTER

Teamcenter Security

Teamcenter 2412

SIEMENS

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: **support.sw.siemens.com**

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

Contents

1. Components of Teamcenter security

Using Teamcenter, you can share your company's data with internal and external users irrespective of their geographical location. To mitigate security risks during collaboration and sharing, Teamcenter provides functionality to secure your information on multiple levels.

- **Operating system**

  Users can only access files using the File Management System (FMS), which requires authorization through Teamcenter.

  Your metadata is stored in a Relational Database Management System (RDBMS), which is accessed by the Teamcenter server process. Users have no direct access.

- **Network**

  Secure your traffic by using Helmet, CORS, TLS, and other mechanisms.

  Proxy and reverse proxy capabilities are available for added security.

- **Users**

  Organize your users by using groups and roles for easy assignment of data permissions.

  Map workspaces to your groups and roles for easy assignment of user interface (UI) permissions.

  Use projects, programs, and licensing to provide special permissions based on other criteria.

- **Data**

  Use different data types to categorize your data.

  Assign different permissions to each data type.

The information here is focused on the Active Workspace client, which provides its own security capabilities in addition to those of the Teamcenter platform. Knowledge of both is required.

Where can I find the Teamcenter platform documentation?

The foundation of Teamcenter security, the concepts, tasks and reference information, is included in the *Security Administration* documentation.

2. Operating system

Back end user accounts

Create an operating system user account that will *only* be used for your deployment.

When installing Teamcenter and Active Workspace the operating system user account you use is important. The files stored on Teamcenter volumes are owned by this account, and any person or software that has access to the account has *direct and unrestricted* access to those files. Do not use a generic account that many have access to.

Refer to the *Create user accounts and directories* documentation:

- Teamcenter Installation on Windows Using TEM
- Teamcenter Installation on Linux Using TEM

3. Network

Working with proxies and Active Workspace

Following are key points to consider when using a proxy server with Active Workspace. This is not a step-by-step guide. There are so many variables that contribute to your specific environment, it would be impossible to document every permutation.

Configuration

The following items depend upon your choice of routing.

- **Active Workspace gateway is at the root**

  You have the proxy root context routed directly to the Active Workspace gateway.

  - Never block the **/tc** route from communicating with the gateway.
  - **Websocket** support will work by default.

- **Unique path**

  You have a unique route to the Active Workspace gateway.

  - The **urlPrefix** in the gateway's *config.json* file supports this if the proxy doesn't support path modification.
  - If using this configuration without **urlPrefix**, your cookie path must be updated to reflect this.

Other considerations

- **Common configuration requirements**

  The proxy must be configured for session affinity. This ensures that the request is routed through the same Active Workspace gateway and Teamcenter web tier. Ideally, this is determined by the Teamcenter web tier session cookie (**JSESSIONID** or **ASP.NET_SessionId**).

- **Cookies**

  The **path** attribute is critical. If the path of the proxy does not match the path of the Active Workspace gateway (**urlPrefix**) then the proxy should update the **path** attribute. Otherwise the browser may send the cookie to the incorrect route.

- **TLS**

If enabled on the proxy but *not* on the Active Workspace gateway, then the cookie will need its attributes maintained, including **Secure**, **SameSite** and **HttpOnly**.

If enabled on both the proxy *and* the Active Workspace gateway, the configuration is automatic.

- **Teamcenter Security Services SSO**

  - There are several settings that must be considered in the gateway's *config.json* file.

    - **tcSSOAppID** is the application ID used with Teamcenter Security Services Identity Service configuration. This is the indirect way that Teamcenter Security Services can redirect back to the the Active Workspace gateway after log in.

    - **tcSSOURL** is the URL for the Teamcenter Security Services log in service. This is used for the redirect during SSO log in.

    - **tcSSORedirectMethod** is defaulted to **POST** if unset. **GET** is the alternative value. This is not typically used.

    - **tcSSOLogoutURL** is used for redirection during log out. This can be used to avoid logging back in immediately upon log out.

    - **proxyServerUrl** is required when working with a proxy. This is the URL from the user's perspective for getting to the Active Workspace gateway.

    - **queryParams** is a collection of query parameters to add to the URL during SSO log in. This is not typically used.

      ```
      "sso": {
         "tcSSOAppID": "@Gateway.tcsso.AppID@",
         "tcSSOURL": "@Gateway.tcsso.URL@",
         "tcSSORedirectMethod": "",
         "tcSSOLogoutURL": "",
         "proxyServerUrl": "",
         "queryParams": ""
      },
      ```

  - The Teamcenter Security Services manages a map of application ids to service a URL. It must have the *full* URL to the Active Workspace gateway from the user's perspective.

    If working with a proxy, this will include both the proxy and the path (if defined).

    ```
    https://myproxy.xyz.com/awc
    ```

Proxies

This is not a comprehensive list. Consult the documentation for the load balancer you are using.

- **Apache httpd**

  https://httpd.apache.org/

  - The following required modules not enabled by default.

    ```
    LoadModule proxy_module modules/mod_proxy.so
    LoadModule proxy_http_module modules/mod_proxy_http.so
    LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
    ```

  - When using **TLS/https** and a **urlPrefix**, such as **/awc**.

    ```
    ProxyPass /awc https://myserver.xyz.com:3000/awc
    ProxyPassReverse /awc https://myserver.xyz.com:3000/awc
    ```

  - When using the httpd load balancer.

    ```
    # Load balancer configuration for WebSocket
    <Proxy balancer://ws_tc_int_awc>
    BalancerMember ws://myserver.xyz.com:3000 route=4    ttl=29
    ProxySet lbmethod=bybusyness nofailover=off stickysession=JSESSIONID
    </Proxy>
    ```

Using self-signed or unknown certificate authorities

If you are using a self-signed certificate or certificate from an unknown certificate authority, **node.js** provides two options: Add one of these two environment variables to your gateway service config file: **TC_ROOT**/*microservices/services_config/gateway.json*

- **Extend the root certificates at runtime**

  Add the **NODE_EXTRA_CA_CERTS** environment variable and point it to your own local file. This extends the *root* certificate authorities (from VeriSign, for example) to include your own certificates.

  The certificates contained in this local file must be in PEM format.

- **Skip the validation**

  Add the **NODE_TLS_REJECT_UNAUTHORIZED** environment variable and set its value to '0' (zero).

  > Warning:
  >
  > This makes TLS, and HTTPS by extension, insecure. This is for testing purposes only and should *never* be used in a production environment.

More information about **node.js** environment variables can be found on the node.js web site.

Configuring gateway security

The **Active Workspace Gateway** uses several middleware functions for security. These systems are defined in the gateway configuration file, located in the Active Workspace installation directory.

AW ROOT/*microservices*/*gateway*-**nnn**/*config.json*.

> Note:
>
> After making any changes to this file, you must restart the **gateway** to implement the changes.

helmet

Following is a list of some important notes for various features of **helmet**. Not all features in the file are listed here, and not all available features are in the file.

```
"security": {
    ...
    "helmet": {
        "contentSecurityPolicy": false,
        "frameguard": false,
        ...
    }
```

contentSecurityPolicy

Not enabled by default, and is not supported by Active Workspace at this time. Do not enable this feature.

frameguard

The frameguard option is used to set the X-Frame-Options header. This is disabled for Active Workspace by default. If you enable this feature, you will lose the capability of hosting Active Workspace within an iFrame by a host. iFrames are used by some embedded functionality

https://helmetjs.github.io/#x-frame-options

cors

Cross-Origin Resource Sharing (cors) is enabled in Active Workspace. However no whitelist sites are defined by default.

```
"security": {
    ...
    "cors": {
    }
```

To add a site, configure the **origin** parameter.

```
{
    security: {
        cors: {
            origin: [ 'http://example.com', 'http://example2.com' ]
        }
    }
}
```

> Caution:
>
> Siemens Digital Industries Software recommends **adding routes** instead of using **cors**.

csurf

Cross-Site Request Forgery (CSRF) defense is enabled in Active Workspace.

```
"security": {
    ...
    "csurf": {
        "cookie": true
    }
```

> Caution:
>
> If you write custom client code that calls any routes through the Active Workspace gateway, you should use the provided http services. If you use low-level JavaScript calls instead, you may be required to set the request header.

Configuring gateway SSO

The **Active Workspace Gateway** responds to several settings concerning Security Services single sign-on (SSO). These settings are defined in the gateway configuration file located in the Active Workspace installation directory.

AW ROOT/*microservices/gateway-***nnn**/*config.json*.

> Note:
>
> After making any changes to this file, you must restart the **gateway** to implement the changes.

sso

```
"sso": {
    "tcSSOAppID": "Teamcenter",
    "tcSSOURL": "",
    "tcSSORedirectMethod": "",
```

```
    "tcSSOLogoutURL": "",
    "proxyServerUrl": ""
},
```

tcSSOAppID

Use the Teamcenter Environment Manager (TEM) to change this property. Do not directly modify this setting in the **config.json** file.

tcSSOURL

Use the Teamcenter Environment Manager (TEM) to change this property. Do not directly modify this setting in the config file.

tcSSORedirectMethod

When Active Workspace is configured with Teamcenter Security Services, where Teamcenter Security Services is behind an authenticating gateway and request parameters are lost during HTTP Post method requests, use the following parameter to change the HTTP request method type to GET to prevent request parameters from being dropped.

tcSSOLogoutURL

A logout landing page must be configured when Active Workspace is configured with Security Services, which in turn is configured behind an authenticating gateway, such as SiteMinder, WebSeal, IIS, or Apache. In this scenario, the authentication is handled by the gateway. When a user clicks the logoff button, Active Workspace redirects the user to this landing page. This could be any page, such as an internal corporate site that provides access to various systems. To change the default logoff landing page, you must provide the URL for the server.

proxyServerUrl

The proxy server URL is typically a load balancer between the end user's browser & the SSO login service. This is the URL the user initially used to access the site. It is critical that this setting is correct because cookies are filtered by the browser based upon this.

Configuring gateway timeout

The **Active Workspace Gateway** responds to a setting concerning timeout. This setting is defined in the gateway configuration file located in the Active Workspace installation directory.

AW ROOT/*microservices*/*gateway*-**nnn**/*config.json*.

> Note:
>
> After making any changes to this file, you must restart the **gateway** to implement the changes.

timeout

```
"timeout": {
        "httpRequestResponse": 600000,
```

```
        "autoLogout": "2m",
    },
```

httpRequestResponse

Timeout on request **responses** originating with the server to the backend or a route.

autoLogout

This specifies the amount of time the gateway should wait before logging out the user session.

The gateway starts waiting when either:

- All Active Workspace browser tabs to that session are closed.
- The browser is completely closed.

Configuring gateway routing

The **Active Workspace Gateway** uses several middleware functions for security. These systems are defined in the gateway configuration file, located in the Active Workspace installation directory.

AW ROOT/*microservices*/*gateway*-**nnn**/*config.json*.

> Note:
>
> After making any changes to this file, you must restart the **gateway** to implement the changes.

routing

You can add new routes to the gateway, allowing the browser to use these routes instead of communicating directly with the backend server. The basic types of routes are:

- Direct endpoints for services that are *not* registered with the microservice framework. You specify this type of route by providing the **target** with a fully defined URL including protocol, host, and port. Do not set the **alias** property for this route type.
- Microservices registered services. These services are fully participating micro-services and support the service registry and service dispatcher as supplied by the microservice framework. Specify the microservice **alias** which is registered with the microservice framework. Do not set the **target** property for this route type

```
{
    "routes": {
        "example-basic": {
            "path": "/google",
            "target": "https://www.google.com"
        },
        "example-microservice": {
            "path": "/mymicroserver",
```

```
            "alias": "mymicroserver"
        },
        "example-graphql-service": {
            "path": "/mygraphqlservice",
            "target": "http://myhost:myport/mygraphqlservice",
            "graphQL": true,
            "noPing": true
        },
        "example-microservice-graphql": {
            "path": "/mymsgraphql",
            "alias": "mymsgraphql",
            "graphQL": true
        }
    }
}
```

Example:

The following route points to a hypothetical ERP service.

```
"erpsvc": {
        "path": "/erpsvc",
        "target": "http://1.2.3.4:8073",
        "noPing": true
      }
```

path (required)

The URL path on the gateway which this route will use. For example, **http://host:port/path**.

disableAuth (required)

By default, custom routes are blocked until the user logs in. They will receive a HTTP 403 Forbidden error. If you want to allow your users to access a route without logging in, add this option with a value of **true**.

target (must use this or alias, but not both)

The target endpoint for the redirect from the gateway.

alias (must use this or target, but not both)

The alias registered in the microservice dispatcher. This value is used for dynamic targeting of the backend service.

graphQL (optional)

Indicates to the gateway if this route should be registered in the federation GraphQL network managed by the gateway.

pingEnabled

If set to **false**, the service does *not* implement the ping interface and so will *not* block gateway initiation while starting up.

urlPrefix

If you work with load balancers, you may need to change the URL prefix for your site to a non-root context.

Note:

For example, if you want your prefix to be **myprefix**, then change the entry as follows.

Original	Modified
... "maxAge": 15552000, "urlPrefix": "/", "routes": { ...	... "maxAge": 15552000, "urlPrefix": "/**myprefix**", "routes": { ...

After making the change, remember to restart the **gateway**.

Configuring multiple application IDs

In a single sign-on Teamcenter deployment, you can configure a single instance of a Teamcenter server to support more than one web tier. For example, an Active Workspace client and a traditional rich client can be deployed for the same server instance. Each client needs a distinct application ID (**AppID**) configured in Security Services to associate with their return URL. To accommodate this situation, the Security Services identity server supports compound **AppID**s.

For example, an Active Workspace client uses an **AppID** named **TCAWC** and a Teamcenter rich client uses an **AppID** named **TCrich**. In the *tc_profilevars* file, configure the compound **AppID** as **TCAWC,TCrich** or **TCAWC TCrich**. The comma or space separates the individual **AppID**s. The Teamcenter server sends that entire string as a token validation call parameter.

In addition to making the change in the *tc_profilevars* file, in the Security Services Identity Service you must configure an **AppID** for each of the clients (for example, **TCAWC** and **TCrich**) and include the appropriate return URLs.

Configuring load balancer time-outs

The Teamcenter web tier and Teamcenter Security Services Login Service maintain client session information. This leads to two important considerations when deploying Teamcenter behind a third-party load balancer:

- When deployed behind a load balancer, it is important that all requests from a given client are routed to the same back-end web tier or Login Service instance. Load balancers typically have a *stickiness* or affinity setting, and this must be set in the load balancer configuration for these Teamcenter web applications.

- Ensure that the load balancer's session time-out interval is equal to or greater than the Teamcenter session time-out values. The Teamcenter time-outs are set in the Login Service and web tier using the Web Application Manager by typing the time-out value in the **Session time-out** box in the **Modify Web Application Information** dialog box. Otherwise, the load balancer time-out eclipses the Teamcenter time-out.

Either of these can lead to apparently random and unexpected behavior as the load balancer switches between or abandons active web application instances.

4. User

Configure sequence of the postlogon stages

You can configure the sequence of the postlogon stages displayed on the Active Workspace client after successful authentication by setting the **AWC_PostLoginStages** preference.

PickGeography	Displays the **Geography** entry on the postlogon page.

Configure logoff for Active Workspace

There are three possible scenarios for Active Workspace logoff. The logoff behavior changes based on whether Teamcenter Security Services is being configured or not, and if so, how it is configured for authentication.

If Active Workspace is being configured to use Teamcenter Security Services behind an authenticating gateway such as SiteMinder, WebSeal, IIS or Apache, this is a special case that requires additional configuration.

This is the default behavior to expect for each scenario.

- Active Workspace is using Teamcenter authentication without Teamcenter Security Services:

  1. User clicks the **logout** button.
  2. Teamcenter clears the **tcserver** session.
  3. Active Workspace presents its logon page after successful logout.

- Active Workspace is configured using Teamcenter Security Services, and Teamcenter Security Services is configured to authenticate using an LDAP server:

  - Active Workspace is launched in standalone:

    1. User clicks the **logout** button.
    2. Teamcenter clears the **tcserver** session and the Teamcenter Security Services session.
    3. Active Workspace presents the logon page after successful logoff.

  - Active Workspace is participating in a Single Sign-On session with another Teamcenter client that has launched a session agent applet:

1. User clicks the **logout** button.
2. Teamcenter clears the **tcserver** session.
3. User is presented a page stating **You are logged out of Teamcenter application however your TcSS session is still active**.
4. This page will also have a **Login Again** button. When the user clicks this button, they are directed to Active Workspace home page without challenge as long as Teamcenter Security Services session is still valid.

- Active Workspace is configured with Teamcenter Security Services, and Teamcenter Security Services is behind an authenticating gateway:

1. User clicks the **logout** button.
2. Teamcenter clears the **tcserver** session, but it does not close the authenticating gateway session by default.

> Caution:
>
> Because the authenticating gateway session is not closed by default, the single sign-on session is still active. Unless the user specifically logs off from the authenticating gateway session or closes all instances of the browser, the session remains active and can pose a security risk.

3. Active Workspace does not present a page by default.

> Note:
>
> The third scenario requires additional configuration during the initial installation of Active Workspace. You must **configure a logout URL** on the gateway.

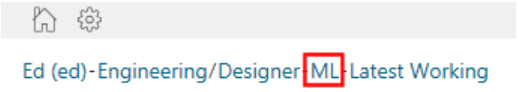
Configuring location codes

Introduction to location codes

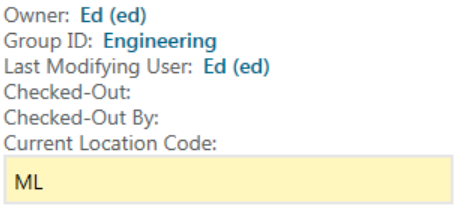
CAGE stands for Commercial And Government Entity. A CAGE Code is a government assigned number given to a supplier on a location basis. It is used to uniquely identify the design source and location for parts and engineering documentation. Documents and parts must be identified with a CAGE Code.

Using Teamcenter, administrators can create and assign location and CAGE codes to users to uniquely identify the design source (location) for parts and engineering documentation. For example, as an administrator, you have designers using Active Workspace in both Europe and the United States. Because management wants to track the location where parts are created, you want to use the location code functionality in Active Workspace.

Each user's location code displays next to their name at the top of the Active Workspace page.



When an Active Workspace user creates a part or a document, their location code appears as a value in the **Current Location Code** (**fnd0CurrentLocationCode**) property on that part or document revision, and in the **Original Location Code** (**fnd0OriginalLocationCode**) property on the part or document. Users can edit this property to change the value.



> Note:
>
> To display the **fnd0CurrentLocationCode** property, you must modify XML rendering style sheet datasets.

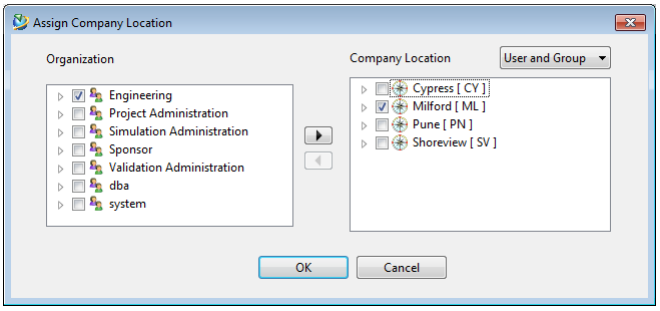
Create location codes

If you set the **Fnd0DisplayLocationCodeLOV** global constant to **true** to display location codes as a list of values, you must create the list of company locations.

1. Administrators create location codes in the rich client with My Teamcenter by choosing **File→New→Other→Company Location**.

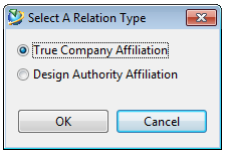
2. After you create the location codes, use My Teamcenter to assign the location codes to groups, roles, and users.

   Choose **Tools→Assign Company Location** to select the organization and company location to assign to it.



3. Click the arrow between the panes to assign the company location.

   The **Select a Relation Type** dialog box is displayed.



4. Select one of the following that describes the user assignment:

   - **True Company Affiliation**

     Users acts as employees of the company.

   - **Design Authority Affiliation**

     Users act as vendors of the company.

5. Click **OK**.

   The company location is assigned to the selected groups, roles, and users.

6. When users log on to Active Workspace, they see the location code next to their user name on the home page. And when they create parts or documents in Active Workspace, this location code appears in the **Current Location Code** (**fnd0CurrentLocationCode**) property on that part or document.

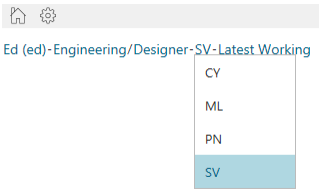
Changing the location code display with global constants

As an administrator, you can set the following global constants in the Business Modeler IDE to determine how the location code is displayed and selected by Active Workspace users:

- **Fnd0DisplayLocationCodeLOV**

  Determines if the **Current Location Code** (**fnd0CurrentLocationCode**) property should be a text box or display a list of values (LOV) with CAGE codes. By default, the value is set to **false**, making it a text box. Set it to **true** to have the box display a list of values.

  If you set this constant to **true**, users click the location code next to their name to change their location. (The **Set or Clear Location Code** button does not appear on the **Profile** page.)

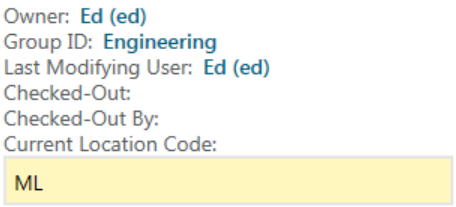


- **Fnd0AllowSuggestiveLocationCode**

  Determines if an end user is allowed to enter a location code that does not exist on any company location. By default, the value of the constant is **true**, and they can enter any location code they want, even if it does not exist yet in the system. If the value of the constant is **false**, the end user must select from the list of existing location codes.

Restricting the changing of location for parts and documents

When an Active Workspace user creates a part or a document, their location code appears as a value in the **Current Location Code** (**fnd0CurrentLocationCode**) property on that part or document revision, and in the **Original Location Code** (**fnd0OriginalLocationCode**) property on the part or document. Users can edit this property to change the value.



You can restrict changing the location for parts and documents in the following ways:

- Allow only existing location codes.

  If you want to restrict what can be entered to **Current Location Code** box to only those location codes that are already set up in the system, set the **Fnd0AllowSuggestiveLocationCode** global constant to **false** in the Business Modeler IDE.

- Make the location code property read-only for specific pages.

  If you want to make the **Current Location Code** (**fnd0CurrentLocationCode**) property read-only on specific pages, such as summary pages, make the property read-only in the XML rendering style sheet datasets.

  For example, on the **Awp0ItemRevSummary.xml** style sheet file, add **modifiable="false"** to the property tag, for example:

  ```
  <property name="fnd0CurrentLocationCode" modifiable="false"/>
  ```

- Make the location code property read-only globally.

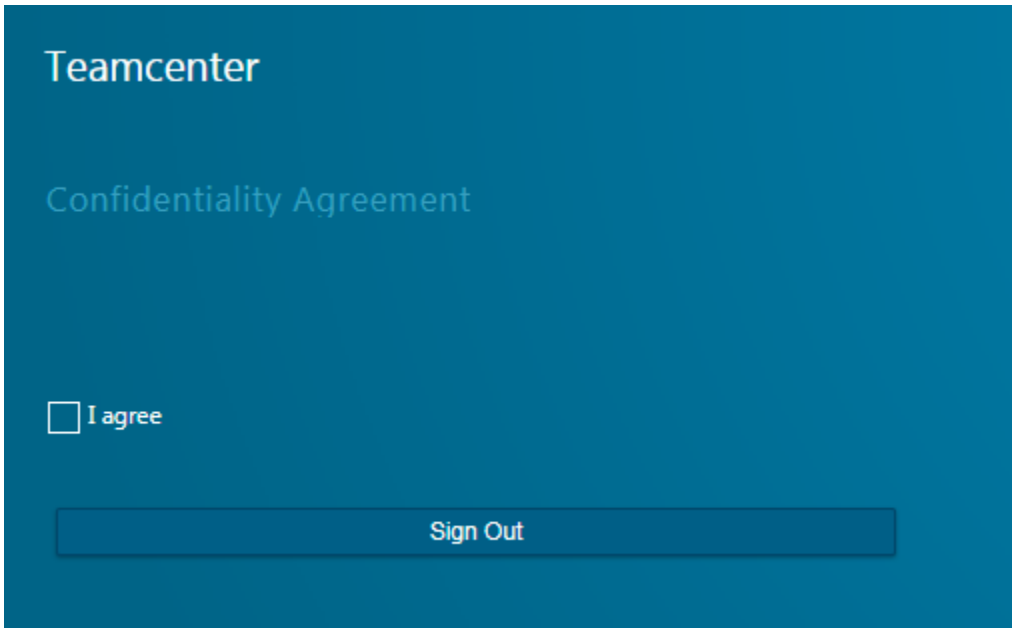
  If you want to make the **Current Location Code** (**fnd0CurrentLocationCode**) property read-only throughout the system so that users cannot change the location code for any already-created part or document, in the Business Modeler IDE set the **Modifiable** property constant for the property to **Read** or **Write Only If Null**.

Confidentiality agreement configuration

Overview of confidentiality agreement

The stand-alone confidentiality agreement, which must be configured, appears during post logon. When the user selects **I agree** and clicks **Continue**, it ensures that the user has accepted the agreement and is then able to gain access to the client. By selecting **I agree**, the user agrees to comply with the confidentiality agreement.

> Note:
>
> The acceptance of the confidentiality agreement is not recorded anywhere in the system.
>
> However, if you require your users to agree to a confidentiality agreement, for example, for authorized data access (ADA) requirements, **you can configure a custom confidentiality agreement statement to be displayed following the selection of their current working location**. This information can be stored so you can generate a report for audit purposes.



Configure the stand-alone confidentiality agreement

To configure the stand-alone confidentiality agreement, you must use the **AWC_PostLoginStages** preference. This preference lists the postlogon stages in the sequence displayed on the Active Workspace client after successful authentication. You must add the string **ConfidentialityAgreement** when defining this preference. Doing so displays the confidentiality agreement page after the user successfully logs on.

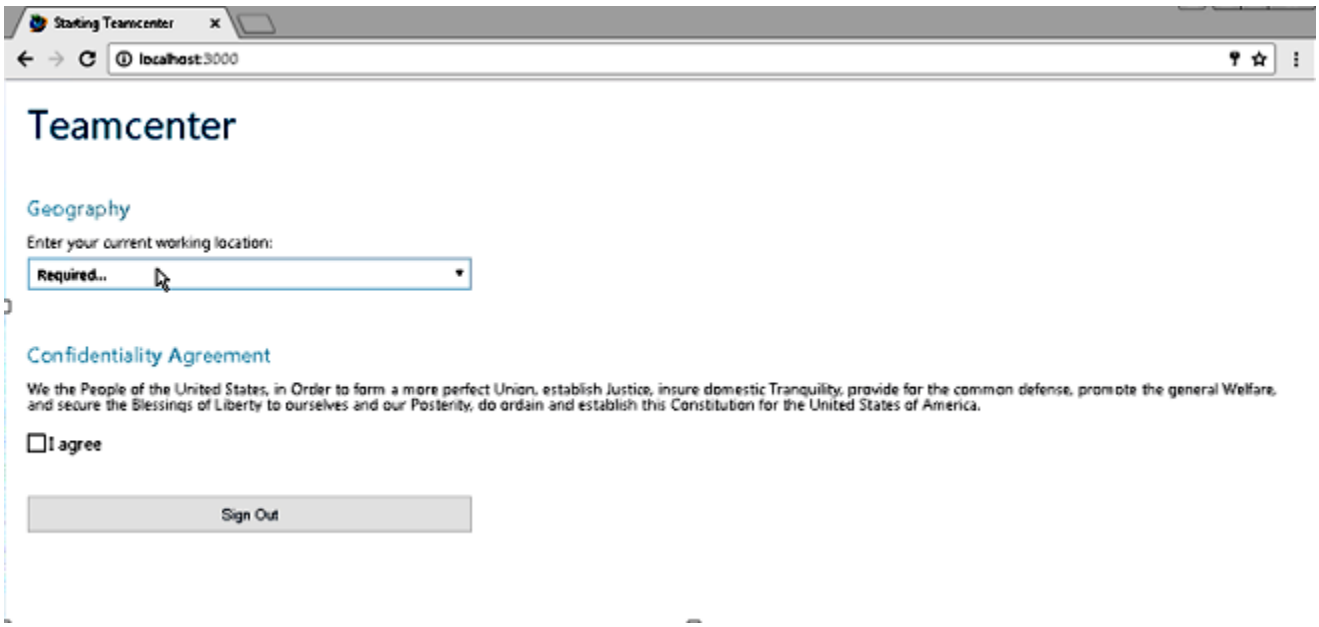
Geography access configuration

Overview of geography access

Geography access allows you to configure both a geography entry and a custom confidentiality agreement prior to users logging on to an Active Workspace session.

For example, in the following Active Workspace session, users must first select the country in which they are currently located before the home page is displayed. If the user does not select a country, the only other option is to log off.

If you require your users to agree to a confidentiality agreement, for example, for authorized data access (ADA) requirements, you can configure a custom confidentiality agreement statement to be displayed following the selection of their current working location. The **I agree** button is unavailable until a valid country is selected in the drop-down list.



You can run a report, **License Login Report**, that displays the logon information. This report is displayed in My Teamcenter by choosing **Tools→Reports→Report Builder Reports→License Login Report**.

Configure geography access

1. Update the site geography.

   You can assign geography to a site using the **site_util** utility.

   > Note:
   >
   > You can also assign site geography using the Organization application.

2. Configure the geography list using the Business Modeler IDE.

   By default, Teamcenter attaches the **Fnd0CountryCodes** list of values (LOV) on the **User.Geography** attribute.

   > Note:
   >
   > If you add a custom LOV to the **User.Geography** attribute, you must remove it before starting a Teamcenter upgrade.

3. Update the user geography.

   You can assign geography to a single user using the **-Geography** argument of the **make_user** utility. To change the geography for all users at the same time, you can perform a batch mode change using the **-allUserDeclaredGeography** argument and the two-character ISO 3166 country code; for example, to set geography to Germany (DE) for all users, enter:

   ```
   -allUserDeclaredGeography=DE
   ```

   > Note:
   >
   > You can also assign user geography using the Organization application.

4. Configure preferences for logon entry of geography:

   - **LoginCountry_selection_enabled**

     Enables the **Country Selection** dialog box for users to select the country from which they are logging in.

True	Displays the **Country Selection** dialog box.
False	Allows the logon process to continue and display the user's home page.

   - **AWC_PostLoginStages**

Lists the postlogon stages in the sequence displayed on the Active Workspace client after successful authentication.

Setting this preference ensures the user cannot bypass the postlogon page.

PickGeography	Displays the **Geography** entry on the postlogon page.

- **LoginCountry_save_previous_selection**

  Allows/denies the ability to save the previous country selection in the **Country Selection** dialog box. If users are logging on from the same site each time, you can configure it so the user does not have to make the country selection each time.

  > Note:
  >
  > This preference is ignored when **LoginCountry_selection_enabled** is set to **False**.

True	Downloads the previously selected country and fills in the combination box in the **Country Selection** dialog box with the value stored on the **User.Geography** attribute. The user selects **Agree** to accept the previously entered country.
False	Causes the **Country Selection** dialog box to not save the previous geography entry. This forces all users who log on to enter a new country when logging on. The initial value in the selection box is blank and the **Agree** button is unavailable until the user selects a country.

5. After the geography access is enabled for users, you can generate the **License Login Report**. This report, which is also helpful for audit purposes, displays the following data:

   - User ID
   - Month
   - Year
   - Geography
   - Intellectual property (IP)

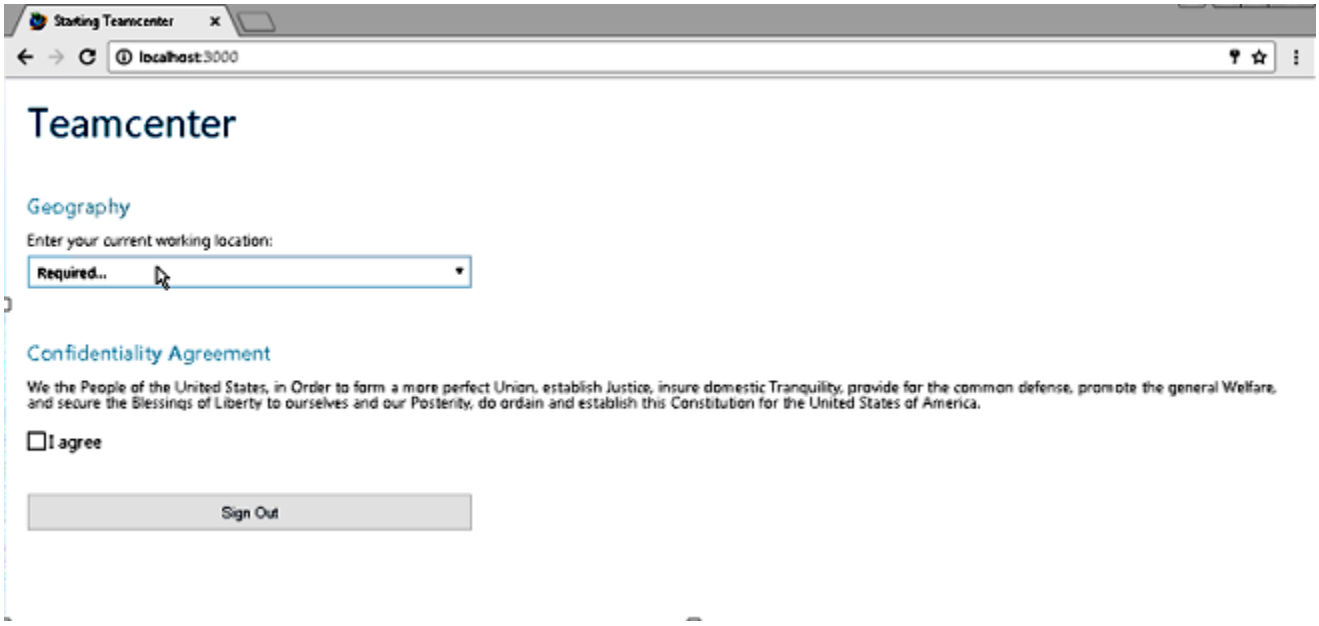
   This report documenting logon information of users can be stored and used for future reference.

Configure confidentiality agreement

> Note:
>
> By default, there is no confidentiality agreement configured.

In Active Workspace, you can configure a custom confidentiality agreement statement to be displayed following logon.

- If **AWC_PostLoginStages** is set with value **PickGeography**, then users must select their current geography.
- If **AWC_PostLoginStages** is set with value **ConfidentialityAgreement** only, then users are not required to select their current geography.



To modify the **LoginCountry_confidentiality_statement** text message, perform the following steps:

1. Create a untranslatable resource file, *custom-name*_**text.xml**.
2. Add the existing key (**LoginCountry_confidentiality_statement**) located in the **tc_text_locale.xml** file to the *custom-name*_**text.xml** file.
3. Add the custom file to the **TC_USER_MSG_DIR***language_locale* directory.

   > Note:
   >
   > *language_locale* is the JAVA standard language name. For example, **fr_FR**.

4. Modify the **LoginCountry_confidentiality_statement** in the **TC_USER_MSG_DIR***language_locale**custom-name*_**text.xml** file.

Following are tips for creating a confidentiality statement:

- Create the new language directory in a location other than *TC_ROOT* or *TC_DATA* to prevent its loss during migrating or patching. A typical custom structure might be:

```
d:\custom-localizations\
     en_US\
          conf_messages_test.xml
     fr_FR\
          conf_messages_test.xml
     de_DE\
          conf_messages_test.xml
```

- The **conf_messages_test.xml** file has different contents in each directory. For example:
  - English (**en_US**) file:

```
<?xml version="1.0" encoding="us-ascii" standalone="yes"?>
<textsrv filename="tc_text_locale.xml">
    <key id="LoginCountry_confidentiality_statement">Your 8859 character set English
        Confidentiality Statement goes here.</key>
</textsrv>
```

  - German (**de_DE**) file:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<textsrv filename="tc_text_locale.xml">
    <key id="LoginCountry_confidentiality_statement">Your 8859 character set German
        Confidentiality Statement goes here.</key>
</textsrv>
```

  - French (**fr_FR**) file:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<textsrv filename="tc_text_locale.xml">
    <key id="LoginCountry_confidentiality_statement">Your 8859 character set French
        Confidentiality Statement goes here.</key>
</textsrv>
```

- Make certain your environment variable is set correctly:

```
set TC_USER_MSG_DIR=d:\custom-localizations
```

Format using HTML

Optionally, you can use HTML to format the page displayed in the Active Workspace. Use the following HTML formatting tags in both the **Geography** and **Confidentiality Agreement** sections of the post-logon page.

> Note:
>
> These HTML formatting tags are *not* supported in the rich client.

HTML tag	Function
This is a unilateral non-disclosure agreement	Indicates a heading on a website appears in the color Tomato. By default, this tag states: This is a unilateral non-disclosure agreement.
	Indicates the paragraph appears in bold font.
	Indicates the paragraph text appears in italic font.
	Indicates the paragraph text is underlined.
	Indicates a paragraph.
	Indicates the text in the paragraph appears in the specified font family, for example, arial.
<p style="font-size;>	Indicates the text in the paragraph is of a certain font size, for example, 12 point.
<p style="color;>	Indicates the paragraph contents displays a certain color, for example, Tomato.
Know more about Siemens PLM	Indicates the placement of a link.
 	Indicates a line break.
	Indicates an image element. You must copy the image into your Active Workspace installation **/assets/image** folder.

Following snippet shows some of the available tags.

```
<key id="LoginCountry_confidentiality_statement">
<![CDATA[<html><body>
   <h1 style="color:Tomato;">This is a unilateral non-disclosure agreement</h1>
   <p style="font-weight: bold;">Employee should keep information confidential</p>
   <p style="text-decoration: underline;">
      <a href="http//www.siemens.com/plm"
         title="Siemens PLM">Know more about Siemens PLM</a></p>
```

```
   <p style=color:MediumSeaGreen;">In certain circumstances ...
   <br>Detailed confidentiality obligations:
   <br>1. an indemnity protecting the disclosure
   <br>2. non-publicity provisions
   <br>3. a data processor clause
   </p>
</body> </html>]]>
</key>
```

5. Data

Digital signature configuration

Digital signature configuration tasks

What is digital signature?

A digital signature is a mathematical stamp on an object used to confirm that the object has not been modified since the signature was applied. It also identifies who applied the digital signature.

Why configure digital signature?

After installing digital signature using Teamcenter Environment Manager (TEM), it is not fully functional unless you configure it. You must **perform additional steps to enable digital signature**.

What do I need to do before configuring?

Before you can configure digital signature, you must install the features. Install the following from the **Features** panel of Teamcenter Environment Manager (TEM):

- **Digital Signatures** (client)

  Installs the user interface elements for viewing digital signatures in Active Workspace.

  Select **Active Workspace→Client→Digital Signatures**.

- **Digital Signatures** (server)

  Installs the server-side definitions for digital signatures.

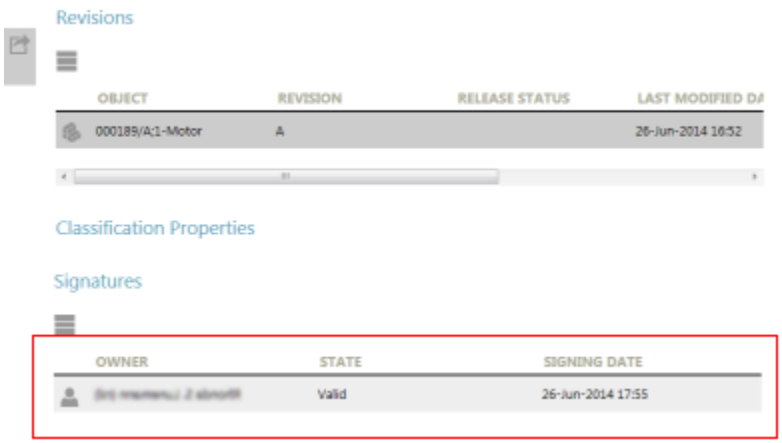
  Select **Active Workspace→Server Extensions→Digital Signatures**.

Where can I find out more about digital signature?

See *Security Administration* in the Teamcenter documentation.

What does a digital signature look like?

Following is an example of a digital signature applied to a workspace object in Active Workspace.



Enable digital signature

A *digital signature* is a mathematical stamp on an object used to indicate if that object has been modified after the signature was applied. It also identifies who applied the digital signature. You must use public key infrastructure (PKI) authentication when applying the digital signature.

You must have administrative privilege to perform these steps.

1. Install and configure your Teamcenter four-tier server for digital signature as described in Teamcenter *Security Administration*.

2. Patch your environment to a version of Teamcenter. Refer to the general patch instructions in the Teamcenter documentation, as well as the readme file for the patch.

   For information about installing patches on a Teamcenter server, see the appropriate server installation guide (for *Teamcenter Installation on Windows Using TEM* or *Teamcenter Installation on Linux Using TEM*).

3. Install Active Workspace and include the digital signature features shown in the Teamcenter Environment Manager (TEM) **Features** panel:

   - **Active Workspace Client**
   - **Digital Signatures** (client) for Active Workspace

     Enables Active Workspace to support digital signature functionality. This includes applying and voiding digital signatures to Teamcenter objects that are configured to support it and digitally signing data upon workflow task completion.

   - **Active Workspace Indexer**
   - **Active Workspace** (server)

- **Digital Signatures** (server) for Active Workspace

  Installs the Active Workspace style sheet to support applying digital signatures on objects.

4. Configure your system by adding the following code to all style sheets specific to Active Workspace.

   Note:

   Generally, these style sheet names begin with the prefix **Awp0** (for example, **Awp0DatasetSummary**). The **Awp0** and **Summary** are standard for each style sheet to be modified. The middle portion denotes the object type to be updated, for this example, **Dataset**).

```
<section title=”Signatures”>
   <objectobjectSet source = "Fnd0DigitalSignatureRel.Fnd0DigitalSignature"
       sortdirection = "ascending" sortby = "object_string"
       defaultdisplay = "listDisplay">
      <tableDisplay>
                <property name = "owning_user"/>
         <property name = "fnd0State"/>
         <property name = "creation_date"/>
      </tableDisplay>
      <thumbnailDisplay/>
      <listDisplay/>
      <command actionKey = "addDigitalSignatureAction"
           commandId = "com.teamcenter.rac.applyDigitalSign"
           renderingHint = "commandbutton"/>
      <command actionKey = "voidDigitalSignatureAction"
           commandId = "com.teamcenter.rac.voidDigitalSign"
           renderingHint = "commandbutton"/>
      </objectSet>
    </section>
```

5. Install Teamcenter Security Services Session Agent on each client with digital signature support enabled.

License attachment configuration

Overview of license attachment

Note:

Users of this feature must have administrative privileges. Generally, this feature is used by project managers.

To provide time-limited grants or denials of access to users who do not have access to classified data based on their clearance level, you can attach and detach licenses to workspace objects. For example, you can restrict access of ITAR-controlled items to only those users in the United States.

Use the **Attach Licenses** command to add one of the following licenses to a workspace object:

- **ITAR**

  The ITAR license grants discretionary access to specific users or groups to workspace objects with International Traffic in Arms Regulations (ITAR) classifications for a specified period of time.

- **IP**

  The IP license grants discretionary access to specific users or groups to workspace objects that have intellectual property (IP) classification. It grants the access for a specified period of time.

- **Exclude**

  The Exclude license denies specific users or groups access to the attached workspace objects for a period of time.

Adding the License List panel to custom XRT pages

Active Workspace ships with the **License List** panel visible on the following XRT style sheets:

- **Awb0ItemRevSummaryForShowObjectLocation.xml**
- **Awp0ItemRevSummary.xml**

To add the **License List** panel to your custom XRT pages, insert the following line in the XRT style sheet:

```
<inject type="dataset" src="LicenseListInfo"/>
```

```
// All Rights Reserved.
// ***************************************************
// @<COPYRIGHT>@
-->
<!-- Default style sheet for displaying item rev summary. -->
<rendering>
    <header>
        <image source="type"/>
        <property name="owning_user"/>
        <property name="last_mod_date"/>
        <property name="release_status_list" renderingHint="label"/>
        <property name="object_type"/>
    </header>
    <page titleKey="tc_xrt_Overview" visibleWhen="ActiveWorkspace:SubLocation != com.siemens.splm.client.occmgmt:OccurrenceManagementSubLocation">
        <column>
            <section titleKey="tc_xrt_properties">
                <property name="item_id" renderingHint="label"/>
                <property name="item_revision_id" renderingHint="label"/>
                <property name="object_name"/>
                <property name="object_desc"/>
                <property name="object_type"/>
                <property name="release_status_list" renderingHint="label"/>
                <property name="date_released" renderingHint="label"/>
                <property name="effectivity_text" renderingHint="label"/>
                <break/>
                <property name="owning_user" renderingHint="objectlink" modifiable="false"/>
                <property name="owning_group" renderingHint="objectlink" modifiable="false"/>
                <property name="last_mod_user"/>
                <property name="checked_out" renderingHint="label"/>
                <property name="checked_out_user"/>
                <command commandId="com.teamcenter.rac.properties" titleKey="tc_xrt_moreProperties"/>
            </section>
            <inject type="dataset" src="S2clScalarRatingOverview"/>
            <content visibleWhen="ics_classified!=null">
                <section titleKey="tc_xrt_ClassificationProperties">
                    <classificationProperties/>
                </section>
            </content>
            <inject type="dataset" src="ProjectListInfo"/>
            <inject type="dataset" src="LicenseListInfo"/>
        </column>
        <column>
            <section titleKey="tc_xrt_Preview">
                <image source="thumbnail"/>
            </section>
```

Attaching licenses

Using licenses

> Note:
>
> Users of this feature must have administrative privileges. Generally, this feature is used by project managers.

To provide time-limited grants or denials of access to users who do not have access to classified data based on their clearance level, you can attach and detach licenses to workspace objects. For example, you can restrict access of ITAR-controlled items to only those users in the United States.

Use the **Attach Licenses** command to add one of the following licenses to a workspace object:

- **ITAR**

  The ITAR license grants discretionary access to specific users or groups to workspace objects with International Traffic in Arms Regulations (ITAR) classifications for a specified period of time.

- **IP**

  The IP license grants discretionary access to specific users or groups to workspace objects that have intellectual property (IP) classification. It grants the access for a specified period of time.

- **Exclude**

  The Exclude license denies specific users or groups access to the attached workspace objects for a period of time.

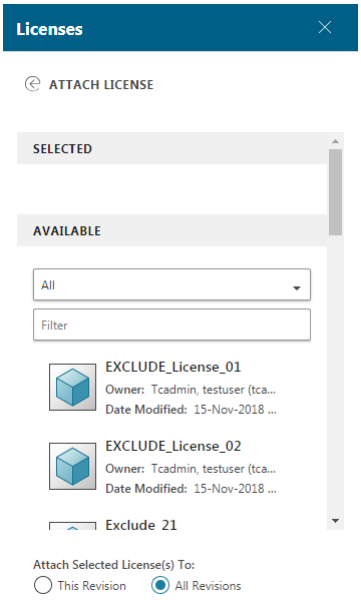
Attach licenses

> Note:
>
> Using this feature requires ADA administrative privileges. Generally, this feature is used by Data Security Administrators or Controllers.

1. Select a workspace object and click **Manage** > **Attach Licenses**.

   The **Licenses** panel displays.

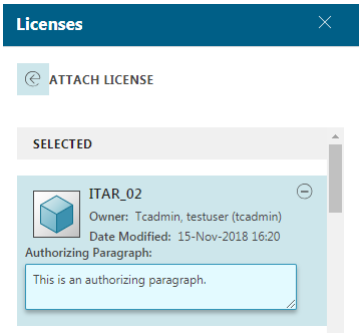
2. Click **Attach License** ⊕ to select the available licenses (**ITAR License**, **IP License**, **Exclude License**, or a custom license type).



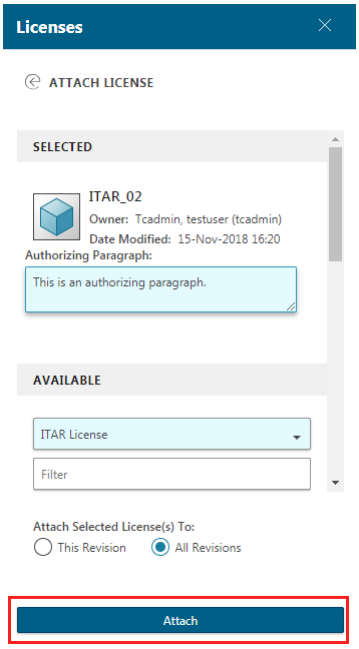
3. Select a license type and license and click **Add** ⊕.

   If you select **ITAR License**, you must edit the **Authorizing Paragraph** for the license before adding the license.

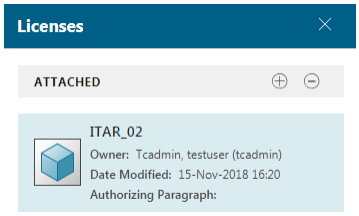
4. (Optional) Type the authorizing paragraph.



5. Select **This Revision** or **All Revisions**. Then, click **Attach** to attach the selected license(s).



You can confirm the selected license(s) were successfully added by clicking **Manage** > **Attach Licenses**.



Detach licenses

> Note:
>
> Using this feature requires ADA administrative privileges. Generally, this feature is used by Data Security Administrators and Controllers.

1. Select a workspace object and click **Manage** > **Attach Licenses**.

   The **Licenses** panel displays.

2. Select any license to detach and click **Detach License** ⊖. This detaches the license(s) from the selected items.