FUJITSU Software
Systemwalker Service Catalog Manager V15.3.2

Release Notes

Contents

About this Manual

This manual describes new features and changes to existing features of FUJITSU Software Systemwalker Service Catalog Manager (CT-MG) V15.3.2 as compared to V15.3.1. In addition, this manual provides compatibility information and information on known restrictions.

CT-MG can be operated on the platforms specified in the *Installation Guide*.

This manual is structured as follows:

Chapter	Description
What's New? on page 6	Describes new features, changes, and enhancements.
Compatibility on page 12	Describes compatibility issues when upgrading an installation from a previous release of CT-MG.
Restrictions on page 16	Describes the known restrictions of this release.

Readers of this Manual

This manual is intended for operators who are responsible for installing CT-MG.

It assumes that you are familiar with the following:

- Administration of the operating systems in use, including the adaption and execution of batch files or shell scripts.
- Java EE technology, particularly as to the deployment on application servers.
- Relational databases and their administration, in particular the PostgreSQL database.
- CT-MG concepts as explained in the *Overview* manual.
- Installation and administration of Web servers.
- Installation and administration of the GlassFish application server.

Notational Conventions

This manual uses the following notational conventions:

Add	The names of graphical user interface elements like menu options are shown in boldface.
init	System names, for example command names and text that is entered from the keyboard, are shown in Courier font.
<variable>	Variables for which values must be entered are enclosed in angle brackets.
[option]	Optional items, for example optional command parameters, are enclosed in square brackets.
one | two	Alternative entries are separated by a vertical bar.
{one | two}	Mandatory entries with alternatives are enclosed in curly brackets.

Available Documentation

The following documentation on CT-MG is available:

- *Overview:* A PDF manual introducing CT-MG. It is written for everybody interested in CT-MG and does not require any special knowledge.
- *Online Help:* Online help pages describing how to work with the administration portal of CT-MG. The online help is intended for and available to everybody working with the administration portal.
- *Installation Guide (GlassFish):* A PDF manual describing how to install and uninstall CT-MG. It is intended for operators who set up and maintain CT-MG in their environment.
- *Operator's Guide:* A PDF manual for operators describing how to administrate and maintain CT-MG.
- *Technology Provider's Guide:* A PDF manual for technology providers describing how to prepare applications for usage in a SaaS model and how to integrate them with CT-MG.
- *Supplier's Guide:* A PDF manual for suppliers describing how to define and manage service offerings for applications that have been integrated with CT-MG.
- *Reseller's Guide:* A PDF manual for resellers describing how to prepare, offer, and sell services defined by suppliers.
- *Broker's Guide:* A PDF manual for brokers describing how to support suppliers in establishing relationships to customers by offering their services on a marketplace.
- *Marketplace Owner's Guide:* A PDF manual for marketplace owners describing how to administrate and customize marketplaces in CT-MG.
- *Developer's Guide:* A PDF manual for application developers describing the public Web service interface of CT-MG and how to integrate applications and external systems with CT-MG.
- *ServerView Resource Orchestrator Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual platforms and servers controlled by ServerView Resource Orchestrator through services in CT-MG.
- *Amazon Web Services Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual servers controlled by the Amazon Elastic Compute Cloud Web service through services in CT-MG.
- *OpenStack Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual systems controlled by OpenStack through services in CT-MG.
- Javadoc documentation for the public Web service interface of CT-MG and additional resources and utilities for application developers.

1 What's New?

This chapter describes changes and enhancements made in CT-MG since V15.3.1.

1.1 System Environment

Web Browsers

The CT-MG user interface supports the following Web browsers:
- Google Chrome 23.0 - 39.0
- Microsoft Internet Explorer 8.0, Microsoft Internet Explorer 9.0, 10.0, or 11.0 running in 8.0 compatibility mode
- Mozilla Firefox 24.0 - 33.0

Operating System

CT-MG has been tested with and can now be run with Red Hat Linux V7.

Search Indexer Application

The CT-MG search indexer application is now based on the most recent versions of Hibernate Search and Apache Lucene.

1.2 Installation

The setup scripts, installation structures, and configuration files have been optimized and unified for the following packages delivered with CT-MG:
- Installation Package, `fujitsu-bss-install-pack.zip`
- Integration Package, `fujitsu-bss-integration-pack.zip`
- Payment Service Provider Integration Package, `fujitsu-bss-integration-psp-pack.zip`
- Integration Package for Asynchronous Provisioning (APP), `fujitsu-bss-integration-app-pack.zip`
- ROR Integration Package, `fujitsu-bss-ror-install-pack.zip`
- AWS Integration Package, `fujitsu-bss-aws-install-pack.zip`
- OpenStack Integration Package, `fujitsu-bss-openstack-install-pack.zip`

The structure of the packages has been unified as follows:
- `databases/<dbName>_db` subdirectory:

  Configuration files for setting up the databases:
  - `db.properties`
  - `configsettings.properties`
  - For APP and all service controllers: `configsettings_controller.properties`
  - For CT-MG: `sso.properties`

  Note that the properties file content has also been unified and optimized.

- `doc` subdirectory:

  Documentation on the package.

- `domains/<domainName>_domain` subdirectory:

  The configuration files for setting up the application server resources as well as the archive files containing the applications to be installed:

  - `glassfish.properties`.

    Note that the properties file content has also been unified and optimized.

  - `applications` subdirectory containing the `.ear` and `.war` files that can be deployed.

- `install` subdirectory:

  XML files that support you in setting up the databases and application server resources for the applications to be deployed.

  Note that the target names in the installation calls have changed. The CT-MG *Installation Guide*, the APP documentation, as well as the ROR, AWS, and OpenStack Integration manuals describe the new installation process in detail.

1.3   Integration of Subscription Approval Process

The integration of an approval process that is automated with an external process control system has been enhanced:

On marketplaces, a subscription owner (an administrator or a subscription manager of the customer organization) can now view the current status of a subscription (**My Subscriptions** page and **Account --> Subscriptions** page). The status **Started** informs him that the action was initialized on the platform, the status **Waiting for reply** informs him that the subscription still has to be approved before his users can start working with the underlying service.

If the execution of an action is aborted, the process control system is now automatically informed about the abortion of the action, so that it can stop processing the request for approval.

The Notification Service interface has been extended by the method `onCancelAction`. It can be used for automatically informing the external process control system about the abortion of a trigger process.

1.4   User Management

Restriction of Service Access Via User Groups

The administrator of an organization can define user groups to restrict the access to services on marketplaces.

A user group is a set of users with access to specific services. When a user logs in to the platform, he has access only to the services that are visible to the user groups to which he belongs. Administrators of organizations are responsible for managing user groups.

A user can be a member of multiple groups. Group hierarchies are not supported. Each organization can have any number of groups.

For each organization, there is a so-called default group. It is automatically created when the organization is created. All users of the organization automatically belong to the default group. Users cannot be removed from the default group, and the default group cannot be deleted.

Note that user groups have no effect on subscriptions. An administrator can individually assign any user to a subscription, irrespective of the user groups to which the user belongs.

Definition of a Maximum Number of Registered Users

The platform operator can define the maximum number of users that can be registered within his CT-MG installation.

The `configsettings.properties` file has been extended by two settings:

*   `TIMER_INTERVAL_USER_COUNT`
*   `MAX_NUMBER_ALLOWED_USERS`

The **Manage users** page of the administration portal has been extended and now indicates the current number of registered users (including the platform operator) as well as the configured maximum number of registered users. At regular intervals (default: 12 hours), the system checks the number of registered users. The platform operator is informed by email when this check returns that the allowed number of registered users is exceeded.

1.5   Service Controllers

AWS Integration

CT-MG comes with an integration package for the Amazon Elastic Compute Cloud Web service (Amazon EC2), a major component of Amazon Web Services (AWS): `fujitsu-bss-aws-install-pack.zip`.

AWS is a collection of remote computing services that together make up a Cloud computing platform offered by Amazon. Amazon Elastic Compute Cloud (Amazon EC2) is one of the central Web services of AWS. It provides computing capacities in the Cloud and allows you to quickly scale these capacities as your computing requirements change.

The integration of AWS with CT-MG provides for an Infrastructure as a Service (IaaS) solution that leverages the features of both products: Through services, which are published on a marketplace in CT-MG, users can request and use virtual servers in Amazon EC2. The usage costs can be calculated and charged by means of the CT-MG billing and payment services.

The AWS integration package provided with CT-MG includes all components required for connecting an existing CT-MG installation with AWS. A new manual, *Systemwalker Service Catalog Manager Amazon Web Services Integration (GlassFish)*, is available describing how to deploy this package and how to create and use services for AWS on a CT-MG marketplace.

OpenStack Integration

CT-MG comes with an integration package for OpenStack, a cloud computing software platform: `fujitsu-bss-openstack-install-pack.zip`.

OpenStack is an open-source cloud operating system that controls large pools of processing, storage, and networking resources throughout a data center. It is managed by the OpenStack Foundation.

The integration of OpenStack with CT-MG provides for an Infrastructure as a Service (IaaS) solution that leverages the features of both products: Through services, which are published on a marketplace in CT-MG, users can request and use instantiated resources, such as networks, servers, or storage in OpenStack. The usage costs can be calculated and charged by means of the CT-MG billing and payment services.

The OpenStack integration package provided with CT-MG includes all components required for connecting an existing CT-MG installation with OpenStack. A new manual, *Systemwalker Service Catalog Manager OpenStack Integration (GlassFish)*, is available describing how to deploy this package and how to create and use services for OpenStack on a CT-MG marketplace.

ROR Integration

In addition to configuring the ROR integration software via configuration files, it can be configured via a user interface.

This user interface is the same for all service controllers (AWS, OpenStack, and ROR). It is recommended that you use the configuration files during the installation process, and that the configuration files are deleted afterwards. Service controller configuration settings should only be updated using the user interface.

Access to Instances Maintained by Service Controllers

Apart from having access to the overall service controller configuration settings, a service controller implementation can now also access the list of instances maintained by the service controller and the respective service instance details.

This data can be made available to the individual service controllers via the `APPlatformService` interface, which is included in the APP integration package.

The `APPlatformService` interface has been extended by the following methods:

- `authenticate()` for authenticating a user as a technology manager for a specific service controller
- `requestControllerSettings()` for requesting APP callbacks
- `listServiceInstances()` for retrieving the list of service instance IDs known in the context of a specific service controller
- `getServiceInstanceDetails()` for retrieving the settings of a given service instance

To ensure that every service controller has access to its own instance data only, a callback function has been implemented in the `APPlatformController` interface: `setControllerSettings()`.

Interruption of Operation Processing

The technology manager of an organization responsible for an AWS or OpenStack service controller can now control the provisioning or deprovisioning of resources so that manual actions can be performed.

If the technology manager specifies the new `MAIL_FOR_COMPLETION` parameter in technical service definitions, the service controller interrupts the processing of each operation before its completion and waits for a notification about the execution of a manual action. The `MAIL_FOR_COMPLETION` parameter defines the email address to which emails are to be sent that describe the manual steps required to complete an operation.

AWS Service Controller Configuration Settings

In the `configsettings_controller.properties` file for the AWS service controller, you can now specify the AWS access keys.

For security reasons, it is recommended that you delete the file as soon as you have successfully installed and configured the AWS integration software.

1.6 Asynchronous Execution of Service Operations

Since service operations can be long-running tasks, for example in backup or restore scenarios, asynchronous execution of such operations is now supported. CT-MG can collect information on the status of the execution of an asynchronous service operation.

It is possible

- for standard users to check the status of an operation for a subscription they are assigned to.
- for administrators to check the status of the operations for all subscriptions of their organization.
- for subscription managers to check the status of the operations for the subscriptions they own.

The operation service API interface included in the CT-MG integration package has been extended so that feedback about the status of a service operation can be passed back to CT-MG. The version number of the operation service API has been increased to V1.3.

A new class, `OperationResult`, has been implemented in the operation service API for specifying whether a service operation is executed asynchronously or synchronously.

The `OperationResult` class also serves to notify CT-MG about the type of execution and possible errors. This information can be retrieved using the `executeServiceOperation()` method of the `OperationService` interface.

A new method in the `SubscriptionService` interface allows for updating the status of a certain service operation in CT-MG: `updateAsyncOperationProgress()`. This method can be called by technology managers.

Changes to the Technical Service Definition

The `type` attribute of the `Operation` element has been removed. Whether an operation is to be executed synchronously or asynchronously is defined by using `true` or `false` when calling the `OperationResult.setAsyncExecution()` method.

Changes to the Asynchronous Provisioning Platform (APP)

APP now stores the transaction ID to be passed to CT-MG. The transaction ID is also included in APP log messages. The service instance list in APP provides a function for completing the pending execution of a service operation.

Every service controller implementation (AWS, OpenStack, and ROR) can now indicate that an operation is pending.

Changes to the Marketplace Functionality

A new menu option, **Operations**, has been added to the **Account** menu.

Standard users can view the execution status of all operations they initiated for the subscriptions to which they are assigned. Users with administrative rights can view the execution status of the operations for all subscriptions of their organization, including the ones they initiated as users assigned to a subscription. Subscription managers can view the execution status of the operations for the subscriptions they own, including the ones they executed as users assigned to a subscription.

Synchronous operations are shown in state COMPLETED and the column "status description" is left empty.

Users can delete the status entries for selected operations.

1.7 Documentation

All manuals and online help pages as well as the marketplace FAQs have been revised to reflect the newly introduced or changed features.

Two new manuals are available:

- *Amazon Web Services Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual servers controlled by the Amazon Elastic Compute Cloud Web service through services in CT-MG.
- *OpenStack Integration (GlassFish):* A PDF manual for operators describing how to offer and use virtual systems controlled by OpenStack through services in CT-MG.

2 Compatibility

This chapter describes compatibility issues when upgrading to CT-MG V15.3.2.

Public Web Service Interface

If applications integrated with CT-MG rely on pure HTTP calls, you need to change their setup to use HTTPS.

CT-MG V15.3.2 comes with a **compatibility layer** so that applications (clients) implemented with CT-MG V15.0, V 15.1, V15.2, V15.2.1, V15.3, or V15.3.1 can still be used without having to be rewritten. Versions older than V15.0 are not supported.

A Web service client accesses exactly one version of the public Web service interface. The versioning pattern is as follows:

Web service version	CT-MG version
Platform services: v1.2 Notification service API: v1.2 Provisioning service API: v1.2 Operation service API: v1.1 PSP integration service: v1.2	V15.0
Platform services: v1.3 Notification service API: v1.3 Provisioning service API: v1.3 Operation service API: v1.1 PSP integration service: v1.3	V15.1
Platform services: v1.4 Notification service API: v1.4 Provisioning service API: v1.3 Operation service API: v1.1 PSP integration service: v1.4	V15.2, V15.2.1
Platform services: v1.5 Notification service API: v1.5 Provisioning service API: v1.4 Operation service API: v1.1 PSP integration service: v1.5	V15.3
Platform services: v1.6 Notification service API: v1.6 Provisioning service API: v1.5 Operation service API: v1.2 PSP integration service: v1.6	V15.3.1
Platform services: v1.6 Notification service API: v1.7	V15.3.2 (this release)

Web service version	CT-MG version
Provisioning service API: v1.5 Operation service API: v1.3 PSP integration service: v1.6	

A WSDL URL is used to address a specific Web service. For new Web service calls, this is the current version of the Web services with basic, certificate-based, or security token service authentication (`BASIC`, `CLIENTCERT`, or `STS`). In the case that existing Web service calls are to be upgraded to the current release, the version information provided in the WSDL URLs in question must be updated to the corresponding versions.

If CT-MG is installed in INTERNAL authentication mode, Web services with the `BASIC` or `CLIENTCERT` suffix can be used. If CT-MG is installed in SAML_SP mode, Web services with the `STS` or `CLIENTCERT` suffix can be used.

The WSDL URL of a specific service can be found out as follows:

1. In the GlassFish administration console, go to **Common Tasks** -> **Applications** -> **fujitsu-bss**.

2. On the **Descriptor** tab, open the `META_INF/sun-ejb-jar.xml` descriptor file of the `fujitsu-adm-um-webservices.jar` subcomponent.

   For every Web service, the endpoint address URI shows the Web service name, its version, and whether it is to be addressed through basic authentication (`BASIC`), certificate-based authentication (`CLIENTCERT`), or a security token service (`STS`).

   The URL pointing to the WSDL definition of a platform service is constructed as follows:

   `<base_URL_HTTPS>/<endpoint-address-uri>?wsdl`

   `<base_URL_HTTPS>` points to the server and port where the CT-MG Web services have been deployed.

   `<endpoint-address-uri>` is the address as defined in the `sun-ejb-jar.xml` descriptor file.

   `?wsdl` is the suffix to be used for identifying a WSDL file.

   Example: `https://myserver:8081/AccountService/v1.6/BASIC?wsdl`

The following table shows which subcomponent contains the descriptor file for which CT-MG version:

Subcomponent	Descriptor file for CT-MG version
`fujitsu-adm-um-webservices-v1_2.jar`	V15.0
`fujitsu-adm-um-webservices-v1_3.jar`	V15.1
`fujitsu-adm-um-webservices-v1_4.jar`	V15.2, V15.2.1
`fujitsu-adm-um-webservices-v1_5.jar`	V15.3
`fujitsu-adm-um-webservices.jar`	V15.3.1, V15.3.2

With CT-MG V 15.3, SAML_SP authentication mode had been introduced. Therefore the following applies:

Subcomponent	Descriptor file for CT-MG version
`fujitsu-adm-um-webservices-v1_5.jar`	V15.3

Subcomponent	Descriptor file for CT-MG version
`fujitsu-adm-um-webservices.jar`	V15.3.1, V15.3.2

The CT-MG integration package (`fujitsu-bss-integration-pack.zip`) contains archive files in the `doc/en` subdirectory, where you can find detailed information on changes to the Web services. Use the `changes.html` file of every package for viewing the respective documentation.

Java 5 Client Applications with Certificate-Based Authentication

If applications integrated with CT-MG are implemented with JDK 5 and use certificate-based authentication, you need to set the following security property for GlassFish 3.1.2.2 in the JVM options of the `bes-domain` domain:

`sun.security.ssl.allowUnsafeRenegotiation=true`

This setting is required because the handshake protocol has changed since JDK 5. However, it is not recommended. It is safer to migrate your applications to a higher Java version.

If credentials are passed for a Web service call, although certificate-based authentication is defined, authentication takes place using the user name and password. In order to use certificate-based authentication, the applications must be changed in a way that no user name and password is sent via HTTP headers. With GlassFish 2.1 and JDK 5, the credentials were not evaluated.

Update Installation of CT-MG

An update installation is possible from a CT-MG 15.3.1 installation to this release. If you want to upgrade from a previous release, you need to uninstall CT-MG and restart with a new installation following the instructions in the *Installation Guide*.

Due to the migration of the CT-MG search indexer application to the most recent versions of Hibernate Search and Apache Lucene, it is necessary to change settings in the VM options of the application server. The index directories must be deleted before starting an update installation. For details, refer to the *Installation Guide*.

Update Installation of APP and Controllers

The platform operator and technology managers must make sure that the following rules are observed when updating CT-MG, APP and/or controllers (AWS, OpenStack, or ROR):

The CT-MG version must be higher or equal to the APP version. The APP version must be equal to the controller version.

Example: If you want to use the AWS controller included in this release (V15.3.2), you must upgrade CT-MG and APP to V15.3.2 first.

Manual Migration of Technical Services for Asynchronous Provisioning

With V15.3.2 (this release), APP implements HTTPS client authentication for Web services in APP (both, the Provisioning Service and the Operation Service). The Web service endpoints in APP have been configured for CLIENTCERT authentication.

In case you have implemented and provided technical service definitions using the HTTP protocol for provisioning service calls in APP, you must manually migrate the technical services so that the HTTPS protocol is used:

1. Export the relevant service definition.

2. Adapt the `provisioningUrl` attribute of the `TechnicalService` element to use the HTTPS protocol.

3. Adapt the `actionURL` attribute of the `Operation` element.

4. Import the service definition in CT-MG.

The Web applications (APP and controller user interface) work as before.

Asynchronous Provisioning - Assigning Users to a Subscription in the Pending State

With CT-MG V15.3.1, a customer can subscribe to a service and afterwards instantly assign users to the subscription, even if the subscription has not yet been provisioned (if CT-MG is running in asynchronous mode) or has not yet been approved (if an approval process is implemented).

With CT-MG V15.3.2, a customer can subscribe to a service, and users can be assigned as soon as the subscription has been successfully provisioned or approved.

3   Restrictions

This chapter describes known restrictions of this CT-MG release.

Java Version

CT-MG requires a Java Development Kit (JDK), version 7, 64 bit. Deployment of CT-MG with JDK 7, Update 20, has been tested and is recommended.

As of JDK, version 7, Update 25, sending a newly created HashMap over a remote EJB call in GlassFish and adding an entry to the HashMap in the EJB method throws an `ArrayIndexOutOfBoundsException`. Workaround: Add and remove an entry before sending the HashMap in the EJB call.

Due to a CORBA library change which is incompatible with Oracle GlassFish Server version 3.1.2.2, CT-MG cannot be deployed with JDK 7, Update 55, and higher.

Note: Third-party tools that you integrate with CT-MG may require a different Java version.

Certificate-Based Authentication

Certificate-based authentication cannot be used when calling CT-MG functions whose execution requires that a user role be specified. The user role determines whether the calling user is allowed to execute the function. Instead, you must use basic authentication for such Web service calls.

If you need to use certificate-based authentication in such scenarios, contact your FUJITSU support organization.

Web Browsers

Concurrent Sessions

CT-MG does not support multiple sessions in Web browsers. This means that you cannot run and log in to CT-MG using several tabs or instances of the same Web browser. If you want to use multiple sessions, run CT-MG in different Web browsers, for example, in Microsoft Internet Explorer and Mozilla Firefox.

Caching in Internet Explorer 8

If an administrator logs in to the CT-MG administration portal and, during the same session, accesses a marketplace, he is logged out as soon as he wants to return to the administration portal (for example, by entering the respective URL again - `http(s)://<domain>/<context-root>/`). This behavior is due to a setting in Internet Explorer 8 which controls the Web page caching. In order to avoid this behavior and to ensure that the administrator stays logged in:

In Internet Explorer, select **Tools** -> **Internet Options**. On the **General** tab, in the **Browsing history** section, click **Settings**. In the **Check for newer versions of stored pages** section, make sure that **Every time I visit the webpage** is selected.

Back Button

CT-MG does not support the usage of the "Back" button in Web browsers. This means that you must use the CT-MG buttons for moving forward and backward between the CT-MG pages.

HTTP or HTTPS Configuration

CT-MG can be configured to use the HTTP or the HTTPS protocol. If you use both protocols at the same time, PSP (payment service provider) integration will not work.

We recommend to configure the HTTPS protocol for all URLs used by CT-MG.

Report Error Messages

The following reports require input parameters, for example a billing data key or dates:

- Supplier revenue report (can be generated by platform operators)
- Detailed billing report for an existing invoice of a customer (can be generated by suppliers and operators)
- Detailed billing report for an existing invoice (can be generated by customers)

When the input parameter is entered in a wrong or invalid format, e.g. `My<>Key` as a billing data key or `2012.5.12` as a date, the error message generated by the report engine does not contain text explaining the reason for the error. If you receive an error message when trying to generate a report, check the input parameter(s) and ensure that they are in the correct format. For example, you can find the date format in the dialog for entering the start and end date for a report; the billing data key is printed on the invoice.

ROR Integration

If CT-MG is integrated with ServerView Resource Orchestrator (ROR), it is recommended that you use the CT-MG user interface for subscribing to services and that the ROR user interface is used for problem-solving purposes only.

Otherwise, the following situation may occur:

A user requests the provisioning of a platform or a server on an existing platform in ROR and assigns a specific name. ROR deploys the new platform or server instance. If another user decides to use the CT-MG user interface for subscribing to a service for provisioning a platform or a server and assigns the same name, the CT-MG ROR controller assumes that the service instance has been created by APP. The pending subscription in CT-MG is successfully completed (based on the existing platform or server).

Asynchronous Provisioning - Termination of Subscription

When a supplier or reseller terminates a customer's subscription and APP is used for asynchronous provisioning, an email is sent to the technology provider of the underlying service as well as to the customer's administrator or subscription manager. The email contains information that the subscription has been terminated as well as the reason why. In case, the technology manager uses a default language in his profile different from the one of the administrator or subscription manager, the email to the customer's administrator or subscription manager will show the text of the reason in the technology manager's language.

Logout Error with Active Directory Federation Services in Internet Explorer 11

An error occurs when a user working with CT-MG tries to log out by clicking **Logout** in the administration portal or on a marketplace. This is true for a specific system configuration:

- CT-MG is installed in SAML_SP authentication mode so that Web browser single sign-on can be used.
- Windows Active Directory Federation Services is installed and used as Identity Provider (IdP).
- In CT-MG, the `SSO_IDP_AUTHENTICATION_REQUEST_METHOD` configuration setting is defined as `POST`.
- CT-MG is accessed using Internet Explorer 11.

- Internet Explorer is set up for integrated Windows authentication (IWA) so that no authentication is required when logging in to CT-MG.

The correct behavior would be that the Web browser is refreshed and the user is automatically logged in again. To achieve this, either use Mozilla Firefox or Google Chrome as the Web browser, or set the `SSO_IDP_AUTHENTICATION_REQUEST_METHOD` setting to `GET`.