TeamConnect Enterprise® 6.3.1

Release Notes **Document ID: tce_63_m_1**

This document details the upgrade information, new features, resolved issues, and known issues that are included in TeamConnect Enterprise® 6.3.1

1 System Requirements

Before you begin to install TeamConnect 6.3.1, ensure that your system meets the requirements. For a full list of requirements, refer to the Installation Requirements in the *TeamConnect Enterprise 6.3.1 Installation Guide*.

The following versions of TeamConnect can be upgraded to TeamConnect 6.3.1

TeamConnect 5.0 (through 5.0.10)
TeamConnect 5.1 (through 5.1.1)
TeamConnect 5.2 (through 5.2.10)
TeamConnect 6.0 (through 6.0.2)
TeamConnect 6.1 (through 6.1.2)
TeamConnect 6.2 (through 6.2.6)
TeamConnect 6.3

TeamConnect 6.3.1 is designed to pair with the following versions of modules (notes below reflect the available versions as of the TeamConnect 6.3.1 release date):

AP Link 5.0 Patch 3
CSM 6.2.5
Data Warehouse 6.3
Financial Management 6.3.1
Legal Matter Management 5.0.1 Patches 1-6
Office Suite 3.2.1+
Screen Designer 5.2.1+
Service of Process (SOP) Manager 5.1.1+

The following changes to the system requirements should be noted for both new installations and upgraded instances:

Third Party Changes

Oracle DB – 19c (dropped support of 12c)
SQL Server – 2019 (dropped support of 2017)
Weblogic – bumped to java 8 build 261
Websphere – moved to Liberty and now support openjdk11
Elasticsearch – 7.10
Mac OS X – Catalina (10.15.6)

To upgrade to TeamConnect Enterprise® 6.3, run the TeamConnect Installer as described in the *TeamConnect Enterprise 6.3 Installation Guide.*

2 Upgrade Considerations

Third Party Changes

Oracle DB – 19c (dropped support of 12c)
SQL Server – 2019 (dropped support of 2017)
Weblogic – bumped to java 8 build 261
Websphere – moved to Liberty and now support openjdk11
Elasticsearch – 7.10
Mac OS X – Catalina (10.15.6)

Elasticsearch 7.10 Upgrade

Build a new Elasticsearch instance with 7.10 and cut over to it. This will require a reindex.

3 New Features

The list of new features is described below. The following new or updated articles have been published in the Client Success Center to accompany this release:

The following new features have been released in the TeamConnect Enterprise® 6.3.1. Each feature is documented in the following format:

- Feature Name
- Feature Description
- Each enhancement under that feature
- Internal Tracking Code

TeamConnect Security Enhancements

Enhancement: Enhance TeamConnect's security options by adding Multi-factor authentication (MFA)
Description: Multi-factor Authentication (MFA) adds an additional layer of security to your TeamConnect accounts. Verifying your identity using a second factor of authentication such as your phone, or security token prevents anyone but you from logging in to the application, even if they know your password.

Multi-factor Authentication offers the following values to users:

- **Improved Security**- It adds an additional layer of security, keeping user accounts secure even if the password is compromised or hacked by an unauthorized entity.
- **Increased Flexibility and Employee Productivity**- TeamConnect users can securely access the application from virtually any device or location without any risk of identity theft or unauthorized access.
- **Highly Scalable**- New users, clients, and devices can easily be added to benefit from this secure technology without requiring any significant effort, IT infrastructure change, or training.

For more information, refer to TeamConnect - Multi-Factor Authentication.

Tracking Code: TC-35002

Enhancement: Allow admin to enable MFA for standard login
Description: Navigate to *Admin* > *Admin Settings* > *Security* > *Multi-factor Authentication* to configure the MFA settings in TeamConnect.
Tracking Code: TC-35004

Enhancement: Require MFA for groups

Description: New option "REQUIRE MULTI-FACTOR AUTHENTICATION FOR STANDARD LOGIN" added to the group to enable MFA only to the user(s) associated with the group.
Tracking Code: TC-35006

Enhancement: Bypass MFA for system user

Description: For Out-of-the-box admin users (TeamConnect Admins and SYSTEM Users), MFA settings are not applicable.

Tracking Code: TC-37752

Enhancement: End user login using device token registration

Description: To display the QR code on the MFA screen, allow users to scan and register their device for receiving the token.

Tracking Code: TC-35012

Enhancement: End user login using email token and provide auto-login link

Description: Auto-triggering of email with token and providing an auto-login link in an email to access the application.

Tracking Code: TC-35015, TC-35440

Enhancement: Update password expiry / force change password workflow to check for MFA

Description: MFA screen should be displayed for the user to authenticate their identify at the time of login when admin performs any of the following action:

1) Enable USER MUST CHANGE PASSWORD AT NEXT LOG IN in user's profile
2) Define the Password parameters to set the validity for the password and the user's password gets expired.

Tracking Code: TC-36875

Enhancement: Update forgot password workflow to include token

Description: User has to authenticate their identity by providing the token received on their authorized registered device or on email before proceeding to change password screen.

Tracking Code: TC-35030

Enhancement: Update reset password workflow to include MFA
Description: User has to authenticate their identity to change their login password by providing the token received on their authorized registered device or on email.
Tracking Code: TC-35018

Enhancement: Notify admin to reset auth app registration
Description: New option “Notify Admin to reset my authorized device” provided on the MFA screen for the user to request admin to reset the registered authorized device of the user.
Tracking Code: TC-35031

Enhancement: Reset the registered authorized device
Description: New option added in the user’s profile for the admin to reset the registered authorized device of the user.
Additional Information: For more information, refer to How to reset the user's MFA authorized device?
Tracking Code: TC-35032

4 Known Issues

The following items are known issues in the TeamConnect Enterprise® 6.3.1 release. Each issue is documented in the following format:

- A description of the issue
- Internal tracking code

Issue:
Description:
Workaround:
Tracking Code:

Issue: Navigating back from the Multi-Factor Authentication (MFA) screen and logging in with another user still logs in with previous user
Workaround: Do not click the browser back button in authentication workflows and always logout from the application properly.
Tracking Code: TC-37416

Issue: Default Category filter value set to blank in Essentials OOTB native reports.
Description: Running OOTB reports shows blank results because the Default Category value is set to blank to all the Data Series in OOTB reports.
Workaround: To generate the report correctly, edit the report to specify a value for Default Category.
Tracking Code: TC-37862